Versión Current Release de XenMobile Server

Contents

Notas de versión de los parches graduales 3

Notas de versión del parche gradual 3 de XenMobile Server 10.14 4

Notas de versión del parche gradual 6 de XenMobile Server 10.13 4

Notas de versión del parche gradual 11 de XenMobile Server 10.12 4

Notas de versión del parche gradual 10 de XenMobile Server 10.12 4

Notas de versión del parche gradual 2 de XenMobile Server 10.14 5

Notas de versión del parche gradual 5 de XenMobile Server 10.13 5

Notas de versión del parche gradual 1 de XenMobile Server 10.14 6

Notas de versión del parche gradual 9 de XenMobile Server 10.12 8

Notas de versión del parche gradual 4 de XenMobile Server 10.13 8

Notas de versión del parche gradual 8 de XenMobile Server 10.12 9

Notas de versión del parche gradual 3 de XenMobile Server 10.13 10

Novedades en XenMobile Server 10.14 10

Novedades en XenMobile Server 10.13 16

Novedades en XenMobile Server 10.12 28

Novedades en XenMobile Server 10.11 37

Avisos legales de terceros 48

Elementos retirados 49

Problemas resueltos 62

Problemas conocidos 64

Arquitectura 64

Requisitos del sistema y compatibilidad 68

Compatibilidad de XenMobile 71

Sistemas operativos compatibles 73

Requisitos de puertos 75

Escalabilidad y rendimiento 86

Licencias 89

Cumplimiento del estándar FIPS 140-2 96

Idiomas disponibles 97

Instalación y configuración 99

Configurar FIPS con XenMobile 114

Configurar la agrupación en clústeres 117

Guía de recuperación ante desastres 128

Habilitar servidores proxy 129

Configurar SQL Server 132

Propiedades de servidor 135

Opciones de la interfaz de línea de comandos 150

Flujos de trabajo iniciales en la consola de XenMobile 167

Certificados y autenticación 171

Citrix Gateway y XenMobile 187

Autenticación con dominio o dominio y token de seguridad 197

Autenticación con certificado de cliente o certificado y dominio 205

Entidades PKI 228

Proveedores de credenciales 256

Certificados APNs 265

SAML para Single Sign-On en Citrix Files 274

Azure Active Directory como proveedor de identidades 285

Credenciales derivadas **298**

Actualizar **319**

Inscripción, roles y cuentas de usuario **324**

Perfiles de inscripción **341**

Configurar roles con RBAC **346**

Notificaciones **369**

Dispositivos **381**

ActiveSync Gateway **390**

Migrar de la administración de dispositivos a Android Enterprise **392**

Android Enterprise **399**

Distribuir aplicaciones de Android Enterprise **450**

Android Enterprise heredado para clientes de Google Workspace (anteriormente G Suite) **479**

iOS **519**

macOS **539**

Inscribir en bloque dispositivos Apple **546**

Propiedades de cliente **554**

Implementar dispositivos mediante el Programa de implementación de Apple **565**

Inscribir dispositivos **578**

Firebase Cloud Messaging **605**

Integración en funciones de Apple Educación **609**

Distribuir aplicaciones de Apple **650**

Control de acceso de red **679**

Samsung Knox **686**

Inscribir en bloque dispositivos Samsung Knox **689**

Acciones de seguridad **695**

Dispositivos compartidos **710**

XenMobile AutoDiscovery Service (ADS) **715**

Directivas de dispositivo **721**

Directivas de dispositivo por plataforma **742**

Directiva de duplicación AirPlay **743**

Directiva de AirPrint **746**

Directiva Configuraciones administradas por Android Enterprise **747**

Permisos de aplicación de Android Enterprise **758**

Directiva de APN **760**

Directiva de acceso a aplicaciones **763**

Directiva de atributos de aplicación **764**

Directiva de configuración de aplicaciones **764**

Directiva de inventario de aplicaciones **766**

Directiva de bloqueo de aplicaciones **767**

Directiva de uso de red de las aplicaciones **770**

Directiva de notificaciones de aplicaciones **771**

Directiva de restricciones a aplicaciones **772**

Directiva de túnel de aplicaciones **773**

Directiva de desinstalación de aplicaciones **777**

Directiva de restricciones de desinstalación de aplicaciones **778**

Directiva de dispositivo para actualizar automáticamente aplicaciones administradas **779**

Directiva de BitLocker **780**

Directiva de explorador web **785**

Directiva de calendario (CalDAV) **786**

Directiva de red de telefonía móvil **787**

Directiva de administrador de conexiones **788**

Directiva de programación de conexiones **789**

Directiva de contactos (CardDAV) **791**

Directiva de control de actualizaciones de SO **793**

Directiva de copia de aplicaciones al contenedor de Samsung **798**

Directiva Credenciales **799**

Directiva de XML personalizado **806**

Directiva de Defender **807**

Directiva de eliminación de archivos y carpetas **809**

Directiva de eliminación de valores y claves del Registro **809**

Directiva de Device Health Attestation **810**

Directiva de nombre de dispositivo **811**

Directiva de configuración de la educación **812**

Directiva de hub empresarial **814**

Directiva de Exchange **815**

Directiva de archivos **823**

Directiva de FileVault **826**

Directiva de fuentes **828**

Directiva de diseño de pantalla de inicio **829**

Directiva de importación de perfiles de iOS y macOS **831**

Directiva de dispositivos de administración de Keyguard **833**

Directiva de quiosco **836**

Directiva de configuración del Launcher **840**

Directiva de LDAP **841**

Directiva de localización geográfica **843**

Directiva de correo **850**

Directiva de dominios administrados **853**

Directiva de opciones de MDM **856**

Directiva de información de la organización **857**

Directiva de código de acceso **858**

Directiva de hotspot personal **873**

Directiva de eliminación de perfiles **873**

Directiva de perfil de datos **874**

Directiva de eliminación de perfiles de datos **875**

Directiva de proxy **876**

Directiva de Registro **878**

Directiva de asistencia remota **879**

Directiva de restricciones **880**

Directiva de itinerancia **935**

Directiva de clave de licencia MDM de Samsung **937**

Directiva de firewall para Samsung SAFE **939**

Directiva de SCEP **940**

Directivas de Siri y dictado **944**

Directiva de cuenta SSO **946**

Directiva de cifrado de almacenamiento **947**

Directiva de tiendas **948**

Directiva de calendarios suscritos **949**

Directiva de términos y condiciones **950**

Directiva de VPN **950**

Directiva de fondo de pantalla **1001**

Directiva de filtro de contenido web **1003**

Directiva de clip web **1005**

Directiva Wi-Fi **1007**

Directiva de certificado de Windows CE **1022**

Directiva de Windows Information Protection **1023**

Directiva de opciones de XenMobile **1028**

Directiva de desinstalación de XenMobile **1032**

Agregar aplicaciones **1032**

Tipos de conectores de aplicaciones **1074**

Actualizar la versión de aplicaciones MDX o de empresa **1074**

Citrix Launcher **1076**

Compras por volumen de Apple **1079**

Virtual Apps and Desktops a través de Citrix Secure Hub **1083**

Usar Citrix Content Collaboration con XenMobile **1084**

SmartAccess para aplicaciones HDX **1100**

Agregar contenido multimedia **1119**

Implementar recursos **1123**

Macros **1139**

Acciones automatizadas **1170**

Supervisar y ofrecer asistencia **1179**

Anonimato de datos en paquetes de asistencia **1182**

Comprobaciones de conectividad **1183**

Customer Experience Improvement Program **1186**

Registros **1188**

Proveedor de servicios móviles **1196**

Informes **1197**

Supervisión SNMP **1202**

Paquetes de asistencia **1211**

Opciones de asistencia y Remote Support **1221**

Syslog **1230**

Ver archivos de registros en XenMobile **1231**

Herramienta XenMobile Analyzer **1233**

API de REST **1248**

Conector de Endpoint Management para Exchange ActiveSync **1250**

Conector de Citrix Gateway para Exchange ActiveSync **1303**

Conceptos avanzados **1319**

Interacción del XenMobile instalado localmente con Active Directory **1320**

Implementar XenMobile **1324**

Modos de administración **1326**

Requisitos de dispositivo **1334**

Seguridad y experiencia del usuario **1334**

Aplicaciones **1355**

Comunidades de usuarios **1363**

Estrategia de correo electrónico **1372**

Integración de XenMobile **1381**

Requisitos multisitio **1390**

Integración en Citrix Gateway y Citrix ADC **1392**

Consideraciones sobre SSO y proxies para aplicaciones MDX **1403**

Autenticación **1408**

Arquitectura de referencia para implementaciones locales **1426**

Propiedades de servidor **1437**

Directivas de aplicación y de dispositivo **1441**

Opciones de inscripción de usuarios **1454**

Ajustar las operaciones de XenMobile **1457**

Aprovisionar y desaprovisionar aplicaciones **1466**

Operaciones del panel de mandos **1470**

Control de acceso basado en roles y asistencia en XenMobile **1472**

Supervisar sistemas **1474**

Recuperación ante desastres **1482**

Proceso de asistencia de Citrix **1486**

Enviar invitaciones de inscripción a grupos en XenMobile **1488**

Configurar un servidor Device Health Attestation local **1490**

Configurar la autenticación por certificado en EWS para notificaciones push de Secure Mail **1500**

Integrar la administración de dispositivos móviles (MDM) de XenMobile en Cisco Identity Services Engine (ISE) **1504**

Notas de versión de los parches graduales

January 4, 2022

Esta sección contiene las notas de versión de parches graduales más recientes de XenMobile Server. Haga clic en el enlace que hay a continuación para ver los problemas resueltos y los conocidos, los cambios en las funciones y las acciones necesarias por su parte.

El parche gradual más reciente contiene todas las correcciones de los parches graduales anteriores de la misma versión.

Notas de versión de los parches de la versión actual	Fecha de publicación
10.14, parche gradual 3	22 de diciembre de 2021
10.14, parche gradual 2	15 de diciembre de 2021
10.14, parche gradual 1	19 de noviembre de 2021

Notas de versión de los parches de versiones anteriores	Fecha de publicación
10.13, parche gradual 6	21 de diciembre de 2021
10.13, parche gradual 5	15 de diciembre de 2021
10.13, parche gradual 4	11 de agosto de 2021
10.13, parche gradual 3	13 de mayo de 2021
10.13, parche gradual 2	25 de febrero de 2021
10.13, parche gradual 1	8 de enero de 2021
10.12, parche gradual 11	21 de diciembre de 2021
10.12, parche gradual 10	16 de diciembre de 2021
10.12, parche gradual 9	8 de octubre de 2021
10.12, parche gradual 8	2 de junio de 2021
10.12, parche gradual 7	29 de marzo de 2021
10.12, parche gradual 6	26 de enero de 2021
10.11, parche gradual 7	18 de noviembre de 2020
10.10, parche gradual 6	22 de julio de 2020

Notas de versión del parche gradual 3 de XenMobile Server 10.14

January 4, 2022

Estas notas de versión describen mejoras y problemas resueltos y conocidos del parche gradual 3 de XenMobile Server 10.14.

Esta versión incluye correcciones de errores.

Para obtener información sobre los parches graduales anteriores de XenMobile Server 10.14.0, consulte Notas de versión de los parches graduales.

Notas de versión del parche gradual 6 de XenMobile Server 10.13

January 4, 2022

Estas notas de versión describen mejoras y problemas resueltos y conocidos del parche gradual 6 de XenMobile Server 10.13.

Esta versión incluye correcciones de errores.

Para obtener información sobre los parches graduales anteriores de XenMobile Server 10.13.0, consulte Notas de versión de los parches graduales.

Notas de versión del parche gradual 11 de XenMobile Server 10.12

January 4, 2022

Estas notas de versión describen mejoras y problemas resueltos y conocidos del parche gradual 11 de XenMobile Server 10.12.

Esta versión incluye correcciones de errores.

Para obtener información sobre los parches graduales anteriores de XenMobile Server 10.12.0, consulte Notas de versión de los parches graduales.

Notas de versión del parche gradual 10 de XenMobile Server 10.12

January 4, 2022

Estas notas de versión describen mejoras y problemas resueltos y conocidos del parche gradual 10 de XenMobile Server 10.12.

Esta versión incluye correcciones de errores.

Para obtener información sobre los parches graduales anteriores de XenMobile Server 10.12.0, consulte Notas de versión de los parches graduales.

Notas de versión del parche gradual 2 de XenMobile Server 10.14

January 4, 2022

Estas notas de versión describen mejoras y problemas resueltos y conocidos del parche gradual 2 de XenMobile Server 10.14.

Para obtener información sobre los parches graduales anteriores de XenMobile Server 10.14.0, consulte Notas de versión de los parches graduales.

Problema resuelto

En XenMobile Server, se observa un uso elevado de la CPU en los nodos del servidor en las horas de máxima actividad. [CXM-102568]

Notas de versión del parche gradual 5 de XenMobile Server 10.13

January 4, 2022

Estas notas de versión describen mejoras y problemas resueltos y conocidos del parche gradual 5 de XenMobile Server 10.13.

Novedades

- **Compatibilidad con dispositivos con Windows 11.** Ahora puede usar XenMobile Server para administrar dispositivos con Windows 11. Para obtener más información, consulte Lista de compatibilidad de sistemas operativos. [CXM-99998]
- **Configure el modo de conexión y la prioridad de red para macOS.** En la directiva Wi-Fi, habilite la configuración **Modo de conexión** para dispositivos macOS si quiere decidir cómo se conectarán los usuarios a la red. El dispositivo puede utilizar las credenciales del sistema o credenciales introducidas en la ventana de inicio de sesión para autenticar al usuario. Si tiene

varias redes, escriba un número en el campo **Prioridad** para establecer la prioridad de la conexión de red. El dispositivo elige la red que tenga el número de prioridad más bajo. Para obtener más información, consulte los parámetros de macOS en Directiva Wi-Fi. [CXM-100533]

- XenMobile Server no podrá sincronizar licencias de grupo con Google porque Google ya no admite licencias de grupo en dispositivos Android Enterprise. Para obtener más información, consulte este artículo. [CXM-101309]

Para obtener información sobre los parches graduales anteriores de XenMobile Server 10.13.0, consulte Notas de versión de los parches graduales.

Problemas resueltos

- Después de inscribir dispositivos con iOS 15 o macOS 12, el perfil de configuración de MDM aparece como "No verificado". [CXM-99380]
- Las aplicaciones de compras por volumen de Apple instaladas en dispositivos se actualizan automáticamente a la versión más reciente cuando el parámetro **Actualización automática de aplicaciones** está inhabilitado. [CXM-99723]
- En la consola de XenMobile Server, al modificar los parámetros de una aplicación para borrar todas las plataformas y guardar, la aplicación no aparece en **Configurar > Aplicaciones**. [CXM-99850]
- En algunos dispositivos Android Enterprise, los grupos de entrega y las directivas o aplicaciones asignadas no se aplican de forma intermitente. [CXM-101554]
- En XenMobile Server, se observa un uso elevado de la CPU en los nodos del servidor en las horas de máxima actividad. [CXM-102450]
- En los dispositivos iOS inscritos en el modo de solo MDM, no se pueden agregar aplicaciones a través de exploradores abiertos por Secure Hub desde el App Store. Aparece este error: **Su sesión ha caducado. Vuelva a iniciar sesión para continuar.** [CXM-102604]
- En la versión 10.13 de XenMobile Server, no puede conectar ni configurar el controlador de zonas de almacenamiento solamente con conectores de zonas de almacenamiento. [CXM-102655]
- A partir de la versión 10.13 RP1 de XenMobile Server, no funciona la captura de conectividad entre nodos de XenMobile de la supervisión de SNMP. [CXM-102788]

Notas de versión del parche gradual 1 de XenMobile Server 10.14

January 4, 2022

Estas notas de versión describen mejoras y problemas resueltos y conocidos del parche gradual 1 de XenMobile Server 10.14.

Novedades

- **Compatibilidad con dispositivos con Windows 11.** Ahora puede usar XenMobile para administrar dispositivos con Windows 11. Para obtener más información, consulte Lista de compatibilidad de sistemas operativos. [CXM-99999]
- **Configure el modo de conexión y la prioridad de red para macOS.** En la directiva Wi-Fi, habilite la configuración **Modo de conexión** para dispositivos macOS si quiere decidir cómo se conectarán los usuarios a la red. El dispositivo puede utilizar las credenciales del sistema o credenciales introducidas en la ventana de inicio de sesión para autenticar al usuario. Si tiene varias redes, escriba un número en el campo **Prioridad** para establecer la prioridad de la conexión de red. El dispositivo elige la red que tenga el número de prioridad más bajo. Para obtener más información, consulte los parámetros de macOS en Directiva Wi-Fi. [CXM-100879]
- XenMobile Server no podrá sincronizar licencias de grupo con Google porque Google ya no admite licencias de grupo en dispositivos Android Enterprise. Para obtener más información, consulte este artículo. [CXM-101209]

Problemas conocidos

Es posible que los dispositivos inscritos cuya versión se haya actualizado de macOS 11 o una anterior a macOS 12, o bien los dispositivos recién inscritos en macOS12, se muestren como “No verificados” en **Preferencias del Sistema > Perfiles** del dispositivo. Para obtener más información y una solución temporal, consulte este artículo de asistencia.[CXM-101843]

Problemas resueltos

- Después de inscribir un dispositivo con iOS 15 o macOS 12, el perfil de configuración de MDM aparece como **No verificado**. [CXM-99379]
- En la consola de XenMobile Server, al modificar los parámetros de una aplicación para borrar todas las plataformas y guardar, la aplicación no aparece en **Configurar > Aplicaciones**. [CXM-99851]
- No puede salir de Citrix Launcher en la plataforma Android Enterprise. Aparece este error: **Contraseña incorrecta**. [CXM-100975]
- En la versión 10.14 de XenMobile Server, no puede modificar la directiva Importar perfil de iOS y macOS. [CXM-102393]

Notas de versión del parche gradual 9 de XenMobile Server 10.12

January 4, 2022

Estas notas de versión describen mejoras y problemas resueltos y conocidos del parche gradual 9 de XenMobile Server 10.12.

Novedades

Compatibilidad con Android 12. Ahora XenMobile Server admite Android 12 en dispositivos Android Enterprise. Para obtener un resumen de las ventajas en seguridad y privacidad, consulte la documentación de Google sobre Android. [CXM-97765]

Compatibilidad con dispositivos con Windows 11. Ahora puede usar XenMobile Server para administrar dispositivos con Windows 11. Para obtener más información, consulte Lista de compatibilidad de sistemas operativos. [CXM-99995]

Problemas resueltos

Las aplicaciones de compras por volumen de Apple instaladas en dispositivos se actualizan automáticamente a la versión más reciente cuando el parámetro **Actualización automática de aplicaciones** está inhabilitado. [CXM-95985]

En la versión 10.12 de XenMobile Server, aparece un error al acceder a **Detalles del dispositivo**. Este error se produce cuando la propiedad de dispositivo tiene un valor en **”“**. [CXM-97953]

En la consola de XenMobile Server, al modificar los parámetros de una aplicación para desmarcar todas las plataformas y guardar, la aplicación no aparece en **Configurar > Aplicaciones**. [CXM-99708]

Notas de versión del parche gradual 4 de XenMobile Server 10.13

September 19, 2021

Estas notas de versión describen mejoras y problemas resueltos y conocidos del parche gradual 4 de XenMobile Server 10.13.

Novedades

Compatibilidad con Android 12. Ahora XenMobile Server admite actualizaciones de dispositivos Android Enterprise a Android 12. Para obtener un resumen de las ventajas en seguridad y privacidad, consulte la documentación de Android.

Para obtener información sobre los parches graduales anteriores de XenMobile Server 10.13.0, consulte Notas de versión de los parches graduales.

Problemas resueltos

- La propiedad de servidor `ios.mdm.apns.connectionPoolSize` se oculta cuando cambia a la API basada en HTTP/2 para APNs. [CXM-95479]
- En XenMobile Server 10.12, no se pueden modificar las propiedades del programa VPP en determinadas aplicaciones. [CXM-96854]
- Las aplicaciones web requeridas no consiguen instalarse automáticamente en dispositivos MDM únicamente. [CXM-97477]
- En la versión 10.13 de XenMobile Server, al configurar el servidor proxy desde la **interfaz de la línea de comandos**, no puede enviar notificaciones al Secure Hub activo en dispositivos iOS. [CXM-97807]
- En la versión 10.13 de XenMobile Server, aparece un error al acceder a **Detalles del dispositivo**. Este error se produce cuando la propiedad de dispositivo tiene un valor en **”“**. [CXM-97951]

Notas de versión del parche gradual 8 de XenMobile Server 10.12

June 11, 2021

Estas notas de versión describen mejoras y problemas resueltos y conocidos del parche gradual 8 de XenMobile Server 10.12.

Novedades

Renovación del certificado APNs de Secure Hub El certificado del servicio de notificaciones push de Apple (APNs) de Secure Hub para XenMobile Server 10.12 caduca el 17 de junio de 2021. Esta actualización renueva el certificado APNs de Secure Hub, que caducará el 7 de mayo de 2022. [CXM-94513]

Problemas resueltos

- Justo después de inscribir un dispositivo con macOS 10.14 o una versión posterior, las propiedades del dispositivo no siempre se rellenan en la consola de XenMobile Server. Una vez reiniciado el dispositivo, sus propiedades aparecen como es debido. [CXM-94221]
- En XenMobile Server 10.12, a veces ShareFile no puede establecer una conexión. [CXM-95419]

Notas de versión del parche gradual 3 de XenMobile Server 10.13

May 20, 2021

Estas notas de versión describen mejoras y problemas resueltos y conocidos del parche gradual 3 de XenMobile Server 10.13.

Novedades

Renovación del certificado APNs de Secure Hub El certificado del servicio de notificaciones push de Apple (APNs) de Secure Hub para XenMobile Server 10.13 caduca el 17 de junio de 2021. Esta actualización renueva el certificado APNs de Secure Hub, que caducará el 7 de mayo de 2022. [CXM-94070]

Puerto alternativo para las notificaciones de APNs. Ahora XenMobile Server permite usar el puerto 2197 como alternativa al puerto 443. Utilice el puerto 2197 para enviar notificaciones de APNs y recibir comentarios de `api.push.apple.com`. El puerto utiliza la API del proveedor de APNs basada en HTTP/2. El valor predeterminado de la propiedad `apns.http2.alternate.port.enabled` del servidor es **`false`**. Para utilizar el puerto alternativo, actualice la propiedad del servidor y, a continuación, reinicie el servidor. [CXM-93911]

Problemas resueltos

Justo después de inscribir un dispositivo con macOS 10.14 o una versión posterior, las propiedades del dispositivo no siempre se rellenan en la consola de XenMobile Server. Una vez reiniciado el dispositivo, sus propiedades aparecen como es debido. [CXM-94150]

Si habilita las configuraciones **Habilitar aplicaciones del sistema** e **Inhabilitar aplicaciones** para la misma aplicación en la directiva Restricciones, la aplicación aparece en el perfil de trabajo. [CXM-94097]

Al agregar usuarios de SNMP a la consola de XenMobile Server, los usuarios no aparecen en la lista **Usuarios de supervisión SNMP** o los agentes de SNMP quedan inactivos. [CXM-93199]

En XenMobile Server, las comprobaciones de conectividad de NetScaler Gateway no muestran ningún resultado. [CXM-93134]

En la consola de XenMobile Server, no se muestra la fecha de caducidad correcta del certificado raíz. [CXM-93133]

Novedades en XenMobile Server 10.14

January 4, 2022

Las directivas clásicas se retiran de Citrix ADC

Citrix anunció recientemente la retirada de algunas funcionalidades basadas en directivas clásicas a partir de la compilación 56.20 de Citrix ADC 12.0. Los avisos de retirada de Citrix ADC no afectan a las integraciones existentes de XenMobile Server con Citrix Gateway. XenMobile Server sigue siendo compatible con las directivas clásicas y no es necesario hacer nada.

Servicio XenMobile Migration Service

Si utiliza XenMobile Server local, nuestro servicio XenMobile Migration Service puede ayudarle a comenzar a usar el servicio Endpoint Management. La migración desde XenMobile Server a Citrix Endpoint Management no requiere reinscribir dispositivos.

Para iniciar la migración, póngase en contacto con un representante de ventas local de Citrix o con un socio de Citrix. Consulte Servicio XenMobile Migration Service.

Anuncios de retirada

Para obtener información avanzada sobre las funciones de Citrix XenMobile que se están retirando gradualmente, consulte Elementos retirados.

Antes de actualizar la versión de los dispositivos de punto final a iOS 14.5

Antes de actualizar la versión de un dispositivo de punto final a iOS 14.5, Citrix recomienda lo siguiente para mitigar cierres inesperados de las aplicaciones:

- Actualice la versión de Citrix Secure Mail y Secure Web a 21.2.X o a una posterior. Consulte Actualizar la versión de aplicaciones MDX o de empresa.
- Si utiliza MDX Toolkit, empaquete todas las aplicaciones iOS de terceros con MDX Toolkit 21.3.X o una versión posterior. Compruebe la página de descargas de MDX Toolkit para asegurarse de que dispone de la versión más reciente.

Antes de actualizar la versión de un Citrix ADC local

La actualización de un Citrix ADC local a ciertas versiones puede dar lugar a un error de Single Sign-on. El inicio de sesión Single Sign-on en Citrix Files o la URL del dominio de ShareFile en un explorador con la opción **Inicio de sesión de empleados** genera un error. El usuario no puede iniciar sesión.

Para evitar este problema: Si aún no ha ejecutado este comando desde la CLI de ADC en Citrix Gateway, ejecútelo para habilitar el SSO global:

```
1 `set vpn parameter SSO ON`
2 `bind vpn vs <vsName> -portalTheme X1`
```


Para obtener más información, consulte:

- Citrix ADC Release (Feature Phase) 13.0, compilación 67.39/67.43
- Configuraciones de SSO afectadas

Después de completar la solución temporal, los usuarios podrán autenticarse mediante Single Sign-On (SSO) en Citrix Files o en la URL del dominio de ShareFile desde un explorador con la opción Inicio de sesión de empleados. [CXM-88400]

Antes de actualizar la versión de XenMobile a la 10.14 (instalación local)

Han cambiado algunos requisitos del sistema. Para obtener información, consulte Requisitos del sistema y compatibilidad y Compatibilidad de XenMobile.

1. Si la máquina virtual con XenMobile Server que quiere actualizar tiene menos de 8 GB de RAM, se recomienda aumentarla a, por lo menos, 8 GB.
2. Actualice Citrix License Server a la versión 11.16 o a una posterior antes de actualizarlo a la versión más reciente de XenMobile Server 10.14.

   La versión más reciente de XenMobile requiere Citrix License Server 11.16 (versión mínima).

   > **Nota:**
   >
   > La fecha de Customer Success Services (anteriormente, fecha de Subscription Advantage) en XenMobile 10.14 es el 15 de septiembre de 2021. La fecha de Customer Success Services de su licencia de Citrix debe ser posterior a esta fecha.
   >
   > Puede ver la fecha junto a la licencia en el servidor de licencias. Si conecta la versión más reciente de XenMobile a un entorno de servidor de licencias anterior, la comprobación de conectividad falla y no se puede configurar el servidor de licencias.

   Para renovar la fecha que consta en la licencia, descargue el archivo de licencias más reciente del Portal de Citrix y cárguelo en el servidor de licencias. Consulte Customer Success Services.
3. Para un entorno en clúster, las implementaciones de aplicaciones y directivas iOS a dispositivos iOS 11 y posterior presentan el siguiente requisito. Si Citrix Gateway está configurado para la persistencia de SSL, debe abrir el puerto 80 en todos los nodos de XenMobile Server.
4. Recomendación: Antes de instalar una actualización de XenMobile, utilice las funcionalidades de la máquina virtual (VM) para tomar una instantánea del sistema. Asimismo, realice una copia de seguridad de la base de datos de configuración del sistema. Si tiene problemas durante la actualización, las copias de seguridad completas le permitirán recuperar los datos.

Para actualizar la versión

Con esta versión, XenMobile es compatible con VMware ESXi 7.0. Asegúrese de actualizar a la versión 10.14 antes de instalar o actualizar ESXi 7.0.

Puede actualizar directamente la versión 10.13.x o 10.12.x de XenMobile a 10.14. Para actualizar la versión, descargue el último binario disponible en https://www.citrix.com/downloads. Vaya a **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. En el mosaico del software XenMobile Server para su hipervisor, haga clic en **Download File** (Descargar archivo).

Para cargar la actualización de la versión, utilice la página **Administración de versiones** de la consola de XenMobile. Consulte Para actualizar desde la página “Administración de versiones”.

Después de actualizar la versión

Si la funcionalidad relacionada con las conexiones de salida deja de funcionar y no ha cambiado la configuración de las conexiones, busque errores similares a los siguientes en el registro de XenMobile Server: “No se puede conectar con el servidor del programa VPP: El nombre de host ‘192.0.2.0’ no coincide con el sujeto de certificado suministrado por el servidor homólogo”.

- Si recibe el error de validación de certificado, inhabilite la verificación de nombres de host en el XenMobile Server.
- De forma predeterminada, la verificación de nombres de host está habilitada en las conexiones salientes, excepto para el servidor PKI de Microsoft.
- Si la verificación de nombre de host deja inoperativa la implementación, cambie la propiedad de servidor `disable.hostname.verification` a **`true`**. El valor predeterminado de esta propiedad es **`false`**.

Actualizaciones sobre compatibilidad de plataforma

- **iOS 15:** Las aplicaciones móviles de productividad de XenMobile Server y Citrix son compatibles con iOS 15, pero no son compatibles actualmente con las nuevas funcionalidades de iOS 15.
- **Android 12:** XenMobile Server es compatible con Android 12. Consulte Migrar de la administración de dispositivos a Android Enterprise para obtener información sobre cómo afecta la retirada de las API de administración de dispositivos de Google a los dispositivos con Android 10 o una versión posterior. Consulte también este blog de Citrix.

Directivas de dispositivo

- Hemos agregado dos parámetros a todos los modos de inscripción de Android Enterprise para ajustarse mejor a los parámetros de Google y simplificar la configuración.

  - **Permitir la opción Compartir Bluetooth:** Si no está activado, los usuarios no pueden establecer la opción Compartir Bluetooth saliente en sus dispositivos.
  - **Permitir la desinstalación de aplicaciones:** Permite a los usuarios desinstalar aplicaciones desde Google Play Store administrado.

  Además, hemos trasladado la opción **Permitir actualización inalámbrica** de la directiva Restricciones a la directiva Actualización de SO.

  Para obtener más información sobre estos cambios, consulte Directiva de restricciones y Directiva de actualización del SO.

- La configuración de las restricciones de Android Enterprise se ha reorganizado para ofrecer una mayor claridad. A veces, se han realizado cambios menores en los nombres de los parámetros. Para obtener más información sobre la reorganización, consulte Parámetros de Android Enterprise.
- Ahora puede actualizar automáticamente aplicaciones administradas en dispositivos Android Enterprise. Para obtener más información, consulte Directiva de dispositivo para actualizar automáticamente aplicaciones administradas.
- Puede configurar una lista de tipos de archivo que pueden cargarse mediante la directiva de archivos. Estos tipos de archivo no se pueden cargar aunque los agregue a esta lista de permitidos:
  - .cab
  - .appx
  - .ipa
  - .apk
  - .xap
  - .mdx
  - .exe

  Para obtener información, consulte Propiedades de servidor.

Inscripción de dispositivos

- Ahora puede crear perfiles de inscripción diferentes para dispositivos iOS y Android. XenMobile Server admite una serie de perfiles de inscripción con diferentes tipos de inscripción. Para obtener más información, consulte Perfiles de inscripción.
- Dispositivos con Android 11 o una versión posterior totalmente administrados se inscriben en el perfil de trabajo en el modo de dispositivos propiedad de la empresa. El nuevo modo separa aún más los perfiles personales y de trabajo en los dispositivos. Este cambio ofrece un mayor control a la organización sobre el perfil administrado y otorga a los usuarios una mayor privacidad sobre

su perfil personal. Para obtener más información, consulte Android Enterprise y Propiedades de servidor.

- Ahora puede especificar más pantallas de configuración que omitir cuando los usuarios configuran dispositivos iOS o macOS.
  - iOS
    - **Restauración completada:** Impide que los usuarios vean si una restauración se completa durante la instalación. Para iOS 14.0 y versiones posteriores.
    - **Actualización completada:** Impide que los usuarios vean si una actualización de software se completa durante la instalación. Para iOS 14.0 y versiones posteriores.
  - macOS
    - **Accesibilidad:** Impide que el usuario escuche VoiceOver automáticamente. Solo está disponible si el dispositivo está conectado a Ethernet. Para macOS 11 y versiones posteriores.
    - **Biometría:** Impide que el usuario configure Touch ID y Face ID. Para macOS 10.12.4 y versiones posteriores:
    - **True Tone:** Impide que los usuarios establezcan sensores de cuatro canales para ajustar dinámicamente el balance de blancos de la pantalla. Para macOS 10.13.6 y versiones posteriores.
    - **Apple Pay:** Impide que los usuarios configuren Apple Pay. Si se desactiva esta opción, los usuarios deben configurar Touch ID y Apple ID. Asegúrese de que los parámetros **ID de Apple** y **Biometría** estén desactivados. Para macOS 10.12.4 y versiones posteriores:
    - **Screen Time:** Impide que los usuarios activen Screen Time. Para macOS 10.15 y versiones posteriores:

  Para obtener más información sobre las opciones de configuración, consulte Implementar dispositivos mediante el Programa de implementación de Apple.

Mostrar archivos de registros de actualizaciones

Hay disponible una nueva opción llamada **Display update log file** en la interfaz de línea de comandos de **Logs** del **menú Troubleshooting**. Esta opción permite ver una lista del contenido de los registros de actualizaciones e incrementa la eficiencia de la solución de problemas. Para obtener más información acerca de las herramientas de interfaz de línea de comandos, consulte Opciones de la interfaz de línea de comandos.

Archivo de registros de errores

Al ver los registros de **Troubleshooting and Support > Logs**, ahora puede ver un registro que muestra los errores filtrados del registro de depuración. Para obtener más información, consulte Ver archivos

de registros en XenMobile.

Propiedades de servidor

- Puede decidir si las aplicaciones de Android antiguo se entregan a Android Enterprise mediante la configuración de la propiedad de servidor `afw.allow.legacy.apps`. Para obtener información, consulte Propiedades de servidor.
- Ahora XenMobile Server permite usar el puerto 2197 como alternativa al puerto 443. Utilice el puerto 2197 para enviar y recibir notificaciones de APNs procedentes de `api.push.apple.com`. El puerto utiliza la API del proveedor de APNs basada en HTTP/2. El valor predeterminado de la propiedad `apns.http2.alternate.port.enabled` del servidor es **`false`**. Para utilizar el puerto 2197, actualice la propiedad del servidor y, a continuación, reinicie el servidor.
- La validación de contraseñas evita que los usuarios usen contraseñas débiles. Cuando la propiedad `enable.password.strength.validation` se establece en **`true`**, no se pueden crear usuarios locales con contraseñas débiles.

Mejora de la lista de servidores virtuales de VPN

Si el nombre del servidor de VPN no incluye `_XM_XenMobileGetway`, XenMobile Server selecciona el primer servidor virtual de VPN disponible de la lista.

Compatibilidad con Citrix Launcher

XenMobile Server admite Citrix Launcher en dispositivos Android Enterprise. Para obtener más información, consulte Directiva de configuración de Launcher.

Nuevos colores para XenMobile Server

XenMobile Server se adhiere a los nuevos colores de la marca Citrix.

Novedades en XenMobile Server 10.13

January 4, 2022

XenMobile Server 10.13 (Descarga en PDF)

Las directivas clásicas se retiran de Citrix ADC

Citrix anunció recientemente la retirada de algunas funcionalidades basadas en directivas clásicas a partir de la compilación 56.20 de Citrix ADC 12.0. Los avisos de retirada de Citrix ADC no afectan a las integraciones existentes de XenMobile Server con Citrix Gateway. XenMobile Server sigue siendo compatible con las directivas clásicas y no es necesario hacer nada.

Servicio XenMobile Migration Service

Si utiliza XenMobile Server local, nuestro servicio XenMobile Migration Service puede ayudarle a comenzar a usar el servicio Endpoint Management. La migración desde XenMobile Server a Citrix Endpoint Management no requiere que vuelva a inscribir los dispositivos.

Para iniciar la migración, póngase en contacto con un representante de ventas local de Citrix o con un socio de Citrix. Consulte Servicio XenMobile Migration Service.

Anuncios de retirada

Para obtener información avanzada sobre las funciones de Citrix XenMobile que se están retirando gradualmente, consulte Elementos retirados.

Antes de actualizar la versión de los dispositivos de punto final a iOS 14.5

Citrix recomienda que, antes de actualizar la versión de un dispositivo de punto final a iOS 14.5, haga lo siguiente para mitigar cierres inesperados de las aplicaciones:

- Actualice la versión de Citrix Secure Mail y Secure Web a 21.2.X o a una posterior. Consulte Actualizar la versión de aplicaciones MDX o de empresa.
- Si utiliza MDX Toolkit, empaquete todas las aplicaciones iOS de terceros con MDX Toolkit 21.3.X o una versión posterior. Compruebe la página de descargas de MDX Toolkit para asegurarse de que dispone de la versión más reciente.

Antes de actualizar la versión de un Citrix ADC local

La actualización de un Citrix ADC local a ciertas versiones puede dar lugar a un error de Single Sign-on. El inicio de sesión Single Sign-on en Citrix Files o la URL del dominio de ShareFile en un explorador con la opción **Inicio de sesión de empleados** genera un error. El usuario no puede iniciar sesión.

Para evitar este problema: Si aún no ha ejecutado este comando desde la CLI de ADC en Citrix Gateway, ejecútelo para habilitar el SSO global:

```
1 `set vpn parameter SSO ON`
2 `bind vpn vs <vsName> -portalTheme X1`
```


Para obtener más información, consulte:

- Citrix ADC Release (Feature Phase) 13.0, compilación 67.39/67.43
- Configuraciones de SSO afectadas

Después de completar la solución temporal, los usuarios podrán autenticarse mediante Single Sign-On (SSO) en Citrix Files o en la URL del dominio de ShareFile desde un explorador con la opción Inicio de sesión de empleados. [CXM-88400]

Antes de actualizar la versión de XenMobile a la 10.13 (instalación local)

Han cambiado algunos requisitos del sistema. Para obtener información, consulte Requisitos del sistema y compatibilidad y Compatibilidad de XenMobile.

1. Si la máquina virtual con XenMobile Server que quiere actualizar tiene menos de 8 GB de RAM, se recomienda aumentarla a, por lo menos, 8 GB.
2. Actualice Citrix License Server a la versión 11.16 o a una posterior antes de actualizarlo a la versión más reciente de XenMobile Server 10.13.

   La versión más reciente de XenMobile requiere Citrix License Server 11.16 (versión mínima).

   > **Nota:**
   >
   > La fecha de Customer Success Services (anteriormente, fecha de Subscription Advantage) en XenMobile 10.13 es el 29 de septiembre de 2020. La fecha de Customer Success Services de su licencia de Citrix debe ser posterior a esta fecha.
   >
   > Puede ver la fecha junto a la licencia en el servidor de licencias. Si conecta la versión más reciente de XenMobile a un entorno de servidor de licencias anterior, la comprobación de conectividad falla y no se puede configurar el servidor de licencias.

   Para renovar la fecha que consta en la licencia, descargue el archivo de licencias más reciente del Portal de Citrix y cárguelo en el servidor de licencias. Consulte Customer Success Services.
3. Para un entorno en clúster, las implementaciones de aplicaciones y directivas iOS a dispositivos iOS 11 y posterior presentan el siguiente requisito. Si Citrix Gateway está configurado para la persistencia de SSL, debe abrir el puerto 80 en todos los nodos de XenMobile Server.
4. Recomendación: Antes de instalar una actualización de XenMobile, utilice las funcionalidades de la máquina virtual (VM) para tomar una instantánea del sistema. Asimismo, realice una copia de seguridad de la base de datos de configuración del sistema. Si tiene problemas durante la actualización, las copias de seguridad completas le permitirán recuperar los datos.

Para actualizar la versión

Con esta versión, XenMobile es compatible con VMware ESXi 7.0. Asegúrese de actualizar a la versión 10.13 antes de instalar o actualizar ESXi 7.0.

Puede actualizar directamente la versión 10.12.x o 10.11.x de XenMobile a 10.13. Para actualizar la versión, descargue el último binario disponible en https://www.citrix.com/downloads. Vaya a **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. En el mosaico del software XenMobile Server para su hipervisor, haga clic en **Download File** (Descargar archivo).

Para cargar la actualización de la versión, utilice la página **Administración de versiones** de la consola de XenMobile. Consulte Para actualizar desde la página "Administración de versiones".

Después de actualizar la versión

Si la funcionalidad relacionada con las conexiones de salida deja de funcionar y no ha cambiado la configuración de las conexiones, busque errores similares a los siguientes en el registro de XenMobile Server: "No se puede conectar con el servidor del programa VPP: El nombre de host '192.0.2.0' no coincide con el sujeto de certificado suministrado por el servidor homólogo".

- Si recibe el error de validación de certificado, inhabilite la verificación de nombres de host en el XenMobile Server.
- De forma predeterminada, la verificación de nombres de host está habilitada en las conexiones salientes, excepto para el servidor PKI de Microsoft.
- Si la verificación de nombre de host deja inoperativa la implementación, cambie la propiedad de servidor `disable.hostname.verification` a **`true`**. El valor predeterminado de esta propiedad es **`false`**.

Actualizaciones sobre compatibilidad de plataforma

- **iOS 14:** Las aplicaciones móviles de productividad de XenMobile Server y Citrix son compatibles con iOS 14, pero no son compatibles actualmente con las nuevas funcionalidades de iOS 14. Use MDX Toolkit 20.8.5 o una versión posterior o prepare las aplicaciones con el SDK de MAM.
- **Android 11:** XenMobile Server es compatible con Android 11. Consulte Migrar de la administración de dispositivos a Android Enterprise para obtener información sobre cómo afecta la retirada de las API de administración de dispositivos de Google a los dispositivos con Android 10 o una versión posterior. Consulte también este blog de Citrix.

Configurar diferentes modos de administración de dispositivos y aplicaciones en un mismo entorno

Ahora puede configurar un único sitio de XenMobile para ofrecer varias configuraciones de inscripción. El rol de los perfiles de inscripción se ha ampliado para incluir parámetros de inscripción para la administración de dispositivos y aplicaciones.

Los perfiles de inscripción admiten diferentes casos de uso y rutas de migración de dispositivos en una sola consola de XenMobile. Entre los casos de uso, se incluyen:

- Administración de dispositivos móviles (solo MDM)
- MDM+Administración de aplicaciones móviles (MAM)
- Solo MAM
- Inscripciones de propiedad de la empresa
- Inscripciones BYOD (con la posibilidad de excluir la inscripción en MDM)
- Migración de inscripciones en administrador de dispositivos Android a inscripciones en Android Enterprise (totalmente administrado, perfil de trabajo, dispositivo dedicado)

Los perfiles de inscripción sustituyen a la propiedad del servidor ahora retirada, `xms.server.mode`. Este cambio no afecta a los grupos de entrega existentes ni a los dispositivos inscritos.

Si no necesita inscribir dispositivos dedicados, puede inhabilitar esta funcionalidad estableciendo la propiedad de servidor `enable.multimode.xms` en **`false`**. Consulte Propiedades de servidor.

En la tabla siguiente, se muestra la ruta de migración automatizada desde el modo de propiedad del servidor existente a la nueva función de perfil de inscripción:

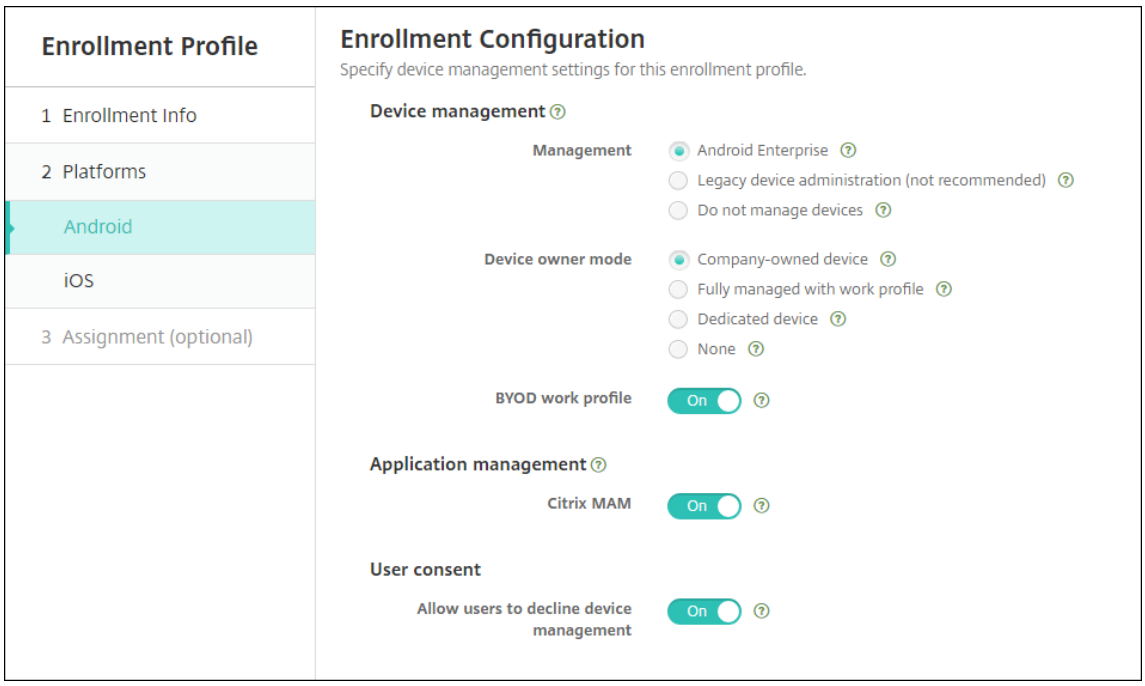
Propiedad de servidor existente	Nuevo modo de administración
Modo ENT (iOS)	Inscripción de dispositivos Apple con Citrix MAM
Modo ENT (Android)	Administrador de dispositivos antiguos con Citrix MAM
Modo ENT (Android Enterprise)	Perfil de trabajo en totalmente administrados (anteriormente COPE), con Citrix MAM
Modo MAM (iOS y Android)	Citrix MAM
Modo MDM (iOS)	Inscripción de dispositivos Apple
Modo MDM (Android)	Administrador de dispositivos antiguos
Modo MDM (Android Enterprise)	Perfil de trabajo en totalmente administrados

Al crear un grupo de entrega, puede adjuntar un perfil de inscripción al grupo. Si no adjunta un perfil

de inscripción, XenMobile adjunta el perfil de inscripción Global.

Los perfiles de inscripción proporcionan las siguientes funcionalidades de administración de dispositivos:

- **Migración más fácil desde el modo de administrador de dispositivos Android (AD) a Android Enterprise.** Para los dispositivos Android Enterprise, la configuración incluye un modo propietario del dispositivo, como: totalmente administrado, perfil de trabajo en totalmente administrado o dedicado. Consulte Android Enterprise.



  Para esta actualización de versión, los parámetros actuales de XenMobile para el modo de servidor y **Configuración > Android Enterprise** se asignan a los nuevos parámetros del perfil de inscripción como se indica a continuación.

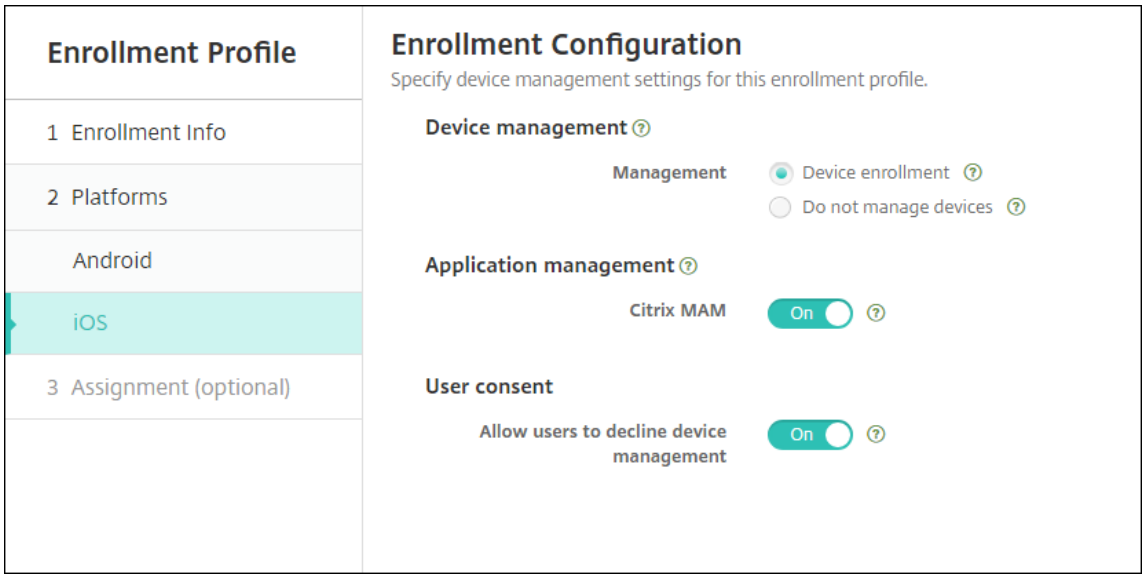
Configuración actual	Parámetro de administración	Parámetro del modo propietario del dispositivo	Parámetro de Citrix MAM
MDM. Google Play administrado (Android Enterprise)	Android Enterprise	Perfil de trabajo en totalmente administrados	No
MDM; G Suite (AD heredado)	AD heredado	no aplicable	No
MAM	No administrar dispositivos	no aplicable	Sí

Configuración actual	Parámetro de administración	Parámetro del modo propietario del dispositivo	Parámetro de Citrix MAM
MDM+MAM. Google Play administrado (Android Enterprise)	Android Enterprise*	Perfil de trabajo en totalmente administrados	Sí
MDM+MAM; G Suite (AD heredado)	AD heredado*	no aplicable	Sí

* Si la inscripción es necesaria, **Permitir a los usuarios rechazar la administración de dispositivos** está **desactivado**.

Después de la actualización, los perfiles de inscripción actuales reflejan esas asignaciones. Considere si quiere crear otros perfiles de inscripción para gestionar nuevos casos de uso a medida que abandona el AD heredado.

- **Gestión de iOS más sencilla.** Para los dispositivos iOS, la configuración incluye la posibilidad de inscribir los dispositivos como administrados o no administrados.



Para esta actualización de versión, las configuraciones anteriores se asignan a la nueva configuración del perfil de inscripción como se indica a continuación.

Modo de servidor	Parámetro de administración	Parámetro de Citrix MAM
MDM	Inscripción de dispositivos	No
MAM	No administrar dispositivos	Sí

Modo de servidor	Parámetro de administración	Parámetro de Citrix MAM
MDM+MAM	Inscripción de dispositivos	Sí

Si la inscripción es necesaria, **Permitir a los usuarios rechazar la administración de dispositivos** está **desactivado**.

Para los perfiles de inscripción mejorados, existen las siguientes limitaciones:

- La funcionalidad de perfil de inscripción mejorado no está disponible para invitaciones de inscripción con autenticación de dos factores o PIN de un solo uso.

Consulte Perfiles de inscripción.

Compatibilidad con la última API de proveedor de APNs basada en HTTP/2

Apple dejará desarrollar el protocolo binario heredado del servicio de notificaciones push (APNs) el 31 de marzo de 2021. Apple recomienda que se utilice en su lugar la API del proveedor de APNs basada en HTTP/2. XenMobile Server ahora es compatible con la API basada en HTTP/2. Para obtener más información, consulte la actualización de noticias “Apple Push Notification Service Update” en https://developer.apple.com/. Para obtener ayuda sobre cómo comprobar la conectividad con APNs, consulte Comprobaciones de conectividad.

Las siguientes versiones de XenMobile Server habilitan la compatibilidad con la API basada en HTTP/2 de forma predeterminada:

- XenMobile Server 10.13
- Parche gradual 5 y posteriores de XenMobile Server 10.12

Si utiliza las siguientes versiones de XenMobile Server, debe agregar la propiedad de servidor **apple.apns.http2** para habilitar la compatibilidad:

- Parches graduales 2-4 y posteriores de XenMobile Server 10.12
- Parche gradual 5 y posteriores de XenMobile Server 10.11

Ya no se admite XenMobile Server 10.11 y se recomienda actualizar a la versión más reciente.

Usar una VPN IPSec basada en certificados de dispositivo con muchos dispositivos iOS

En vez de configurar una directiva de VPN y una directiva de credenciales para cada dispositivo iOS que requiera una VPN IPSec basada en certificados de dispositivo, automatice el proceso.

1. Configure una directiva de VPN para iOS con el tipo de conexión **Always on IKEv2**.
2. Seleccione **Certificado de dispositivo basado en la identidad del dispositivo** como método de autenticación del dispositivo.

3. Seleccione el **Tipo de identidad del dispositivo** que quiera utilizar.
4. Importe en bloque los certificados de dispositivo con la API de REST.

Para obtener más información sobre cómo configurar la directiva de redes VPN, consulte Directiva de redes VPN. Para obtener información sobre cómo importar certificados en bloque, consulte Cargar certificados en bloque con la API de REST).

Actualizaciones automáticas para aplicaciones de compras por volumen de Apple

Al agregar una cuenta de compras por volumen (**Ajustes > Ajustes de iOS**), ahora puede habilitar las actualizaciones automáticas para todas las aplicaciones iOS. Consulte el parámetro **Actualización automática de aplicaciones** en Compras por volumen de Apple.

Requisitos de contraseña para una cuenta de usuario local

Cuando agregue o modifique una cuenta de usuario local en la consola de XenMobile, asegúrese de que sigue los requisitos de contraseña más recientes.

Para obtener más información, consulte Para agregar una cuenta de usuario local.

- **Requisitos de contraseña:** Cuando agregue o modifique una cuenta de usuario local en la consola de XenMobile Server, siga los requisitos de contraseña más recientes. Consulte Para agregar una cuenta de usuario local.
- **Bloqueo de cuenta de usuario local:** Si un usuario alcanza el número máximo de intentos consecutivos de inicio de sesión no válidos, la cuenta de usuario local se bloquea durante 30 minutos. El sistema deniega todos los intentos de autenticación hasta que transcurra el período de bloqueo. Para desbloquear la cuenta en la consola de XenMobile Server, vaya a **Administrar > Usuarios**, seleccione la cuenta de usuario y haga clic en **Desbloquear usuario local**. Consulte Para desbloquear una cuenta de usuario local.

Directivas de dispositivo

Se han agregado nuevas directivas y configuraciones de directivas para dispositivos Android Enterprise.

Ocultar el icono de la barra de la bandeja en dispositivos Android Enterprise

Ahora puede seleccionar si el icono de la barra de la bandeja estará oculto o visible para dispositivos Android Enterprise. Consulte Directiva de opciones de XenMobile.

Más funciones de administración de certificados para dispositivos Android Enterprise en modo de perfil de trabajo o en modo totalmente administrado

Además de instalar entidades de certificación en el almacén de claves administrado, ahora puede administrar las siguientes funcionalidades:

- **Configurar los certificados utilizados por aplicaciones administradas específicas.** La directiva de credenciales para Android Enterprise ahora incluye el parámetro **Aplicaciones que usan los certificados**. En esta directiva, puede especificar qué aplicaciones utilizan los certificados de usuario emitidos por el proveedor de credenciales seleccionado. Las aplicaciones obtienen acceso en modo silencioso a los certificados en tiempo de ejecución. Para utilizar los certificados con todas las aplicaciones, deje la lista de aplicaciones en blanco. Consulte Directiva Credenciales.
- **Quitar en modo silencioso los certificados del almacén de claves administrado o desinstalar todos los certificados de CA que no sean del sistema.** Consulte Directiva Credenciales.
- **Impedir que los usuarios modifiquen las credenciales almacenadas en el almacén de claves administrado.** La directiva de restricciones para Android Enterprise ahora incluye el parámetro **Permitir que el usuario configure las credenciales de usuario**. De forma predeterminada está **activado**. Consulte Directiva de restricciones.

Uso más fácil de alias de certificado en configuraciones administradas de Android Enterprise

Utilice la nueva configuración de **alias de certificado** en la directiva **Credenciales** con la directiva **Configuraciones administradas por Android Enterprise**. Al hacerlo, las aplicaciones pueden autenticarse en la VPN sin intervención por parte del usuario. En lugar de buscar el alias de credenciales en los registros de la aplicación, cree el alias de credenciales. Para crear el alias de credenciales, escríbalo en el campo **Alias de certificado** de la directiva **Configuraciones administradas por Android Enterprise**. A continuación, escriba el mismo alias de certificado en la configuración **Alias de certificado**, en la directiva **Credenciales**. Consulte Directiva Configuraciones administradas por Android Enterprise y Directiva de credenciales.

Control del parámetro "Use one lock" en dispositivos Android Enterprise

El nuevo parámetro **Habilitar código de acceso unificado** en la directiva de dispositivo **Código de acceso** permite controlar si un dispositivo requiere códigos de acceso diferentes para el dispositivo y el perfil de trabajo. Antes de este parámetro, los usuarios controlaban este comportamiento con la opción **Usar un bloqueo** en el dispositivo. Cuando la opción **Habilitar código de acceso unificado** está **activada**, los usuarios pueden usar el mismo código de acceso para el dispositivo y el perfil de trabajo. Si la opción **Enable unified passcode** está **desactivada**, los usuarios no pueden utilizar un mismo código de acceso para el dispositivo y el perfil de trabajo. Está **desactivado** de forma predeterminada. La opción para habilitar el bloque unificado (**Enable unified lock**) está disponible para

dispositivos Android Enterprise con Android 9.0 o una versión posterior. Consulte Directiva de código de acceso.

Mostrar las aplicaciones y accesos directos en dispositivos Android Enterprise que no cumplen los requisitos

La directiva de código de acceso para Android Enterprise tiene un nuevo parámetro, **Mostrar aplicaciones y accesos directos mientras el código de acceso no cumpla los requisitos**. Al habilitar este parámetro, las aplicaciones y los accesos directos permanecen visibles cuando el código de acceso del dispositivo no cumple los requisitos. Citrix recomienda crear una acción automatizada para marcar el dispositivo como no conforme cuando el código de acceso no cumpla los requisitos. Consulte Directiva de código de acceso.

Inhabilitar la capacidad de imprimir en los dispositivos de perfil de trabajo o dispositivos totalmente administrados Android Enterprise

En la directiva Restricciones, la configuración **No permitir la impresión** permite especificar si los usuarios pueden imprimir en cualquier impresora accesible desde el dispositivo Android Enterprise. Consulte Parámetros de Android Enterprise.

Permitir aplicaciones en dispositivos dedicados agregando el nombre del paquete en la directiva de quiosco

Ahora puede introducir el nombre del paquete que quiere permitir en la plataforma Android Enterprise. Consulte Parámetros de Android Enterprise.

Administrar las funciones de Keyguard para los dispositivos de perfil de trabajo y totalmente administrados de Android Enterprise

Android Keyguard administra las pantallas de bloqueo del dispositivo y de Work Challenge. Utilice la directiva de dispositivos de administración de Keyguard para controlar:

- Administración de Keyguard en dispositivos de perfil de trabajo. Puede especificar las funciones disponibles para los usuarios antes de que desbloqueen el Keyguard del dispositivo y el Keyguard de Work Challenge. Por ejemplo, de forma predeterminada, los usuarios pueden usar desbloqueo mediante huella digital y ver notificaciones sin redactar en la pantalla de bloqueo. También puede usar la directiva de administración de Keyguard para inhabilitar toda la autenticación biométrica para dispositivos con Android 9.0 y versiones posteriores.
- Administración de Keyguard en dispositivos dedicados y totalmente administrados. Puede especificar las funciones disponibles, como agentes de confianza y cámara segura, antes de que

desbloqueen la pantalla de Keyguard. O bien, puede optar por desactivar todas las funciones de Keyguard.

Consulte Directiva de dispositivos de administración de Keyguard.

Publicar aplicaciones empresariales para Android Enterprise en la consola de XenMobile

Ya no es necesario registrarse con una cuenta de desarrollador de Google Play al agregar una aplicación privada de Android Enterprise. La consola de XenMobile abre una interfaz de usuario de la tienda administrada de Google Play para que pueda cargar y publicar el archivo APK. Para obtener información más detallada, consulte Agregar una aplicación de empresa.

Publicar aplicaciones web para Android Enterprise en la consola de XenMobile

Ya no es necesario ir a Google Play administrado o al portal Google Developer si quiere publicar aplicaciones web de Android Enterprise para XenMobile. Al hacer clic en **Cargar** en **Configurar > Aplicaciones > Enlace web**, se abrirá una interfaz de usuario de Google Play Store administrado para cargar y guardar el archivo. La aprobación y publicación de la aplicación pueden tardar unos 10 minutos. Para obtener más información, consulte Agregar un enlace web.

Cargar certificados en bloque dispositivos iOS con la API de REST de XenMobile Server

Si no es práctico cargar los certificados de uno en uno, utilice la API de REST de XenMobile Server para cargar en bloque los dispositivos iOS.

1. Configure una directiva de VPN para iOS con el tipo de conexión **Always on IKEv2**.
2. Seleccione **Certificado de dispositivo basado en la identidad del dispositivo** como método de autenticación del dispositivo.
3. Seleccione el **Tipo de identidad del dispositivo** que quiera utilizar.
4. Importe en bloque los certificados de dispositivo con la API de REST.

Para obtener información sobre cómo configurar la directiva de redes VPN, consulte Directiva de redes VPN. Para obtener información sobre cómo importar certificados en bloque, consulte Cargar en bloque certificados en dispositivos iOS con la API de REST.

Actualizar claves de cifrado

La opción **Actualizar claves de cifrado** se agrega en los Parámetros avanzados de la interfaz de línea de comandos de XenMobile. Puede utilizar esta opción para actualizar las claves de cifrado de un nodo a la vez. Consulte Opciones de System.

Compatibilidad con ESXi 7.0

Con esta versión, XenMobile es compatible con VMware ESXi 7.0. Asegúrese de actualizar a la versión 10.13 antes de instalar o actualizar ESXi 7.0.

Nuevas propiedades de servidor

Las siguientes propiedades de servidor ya están disponibles:

- **Permitir nombres de host para enlaces de App Store de iOS:** Si quiere agregar aplicaciones de tienda pública de aplicaciones para iOS mediante las API públicas, en lugar de la consola, configure una lista de nombres de host permitidos.
- **Límite de bloqueo de cuentas de usuario local:** Configure el número de intentos de inicio de sesión que tiene un usuario local antes de que se bloquee su cuenta.
- **Tiempo de bloqueo de cuenta de usuario local:** Configure cuánto tiempo se bloquea la cuenta de un usuario local después de demasiados intentos de inicio de sesión fallidos.
- **Restricción sobre tamaño máximo para carga de archivos habilitada:** Permite habilitar la restricción de tamaño máximo de los archivos cargados.
- **Tamaño máximo permitido para carga de archivos:** Establezca el tamaño máximo de los archivos cargados.

Para obtener información más detallada acerca de estas propiedades, consulte Propiedades de servidor.

Limpieza de autoservicio del disco

Hay disponible una nueva opción de interfaz de línea de comandos, denominada **Disk Usage**, en el **menú Troubleshooting**. Esta opción le permite ver una lista de archivos de volcado principal y de tipo paquetes de asistencia. Después de ver la lista, puede optar por eliminar todos esos archivos desde la línea de comandos. Para obtener más información acerca de las herramientas de interfaz de línea de comandos, consulte Opciones de la interfaz de línea de comandos.

Novedades en XenMobile Server 10.12

January 4, 2022

XenMobile Server 10.12 (Descarga en PDF)

Servicio XenMobile Migration Service

Si utiliza XenMobile Server local, nuestro servicio XenMobile Migration Service puede ayudarle a comenzar a usar el servicio Endpoint Management. La migración desde XenMobile Server a Citrix Endpoint Management no requiere que vuelva a inscribir los dispositivos.

Para iniciar la migración, póngase en contacto con un representante de ventas local de Citrix o con un socio de Citrix. Para obtener más información, consulte Servicio XenMobile Migration Service.

Anuncios de retirada

Para obtener información avanzada sobre las funciones de Citrix XenMobile que se están retirando gradualmente, consulte Elementos retirados.

Preparar los dispositivos Android para cambios futuros

Estas retiradas anunciadas anteriormente afectan a los dispositivos Android y Android Enterprise:

- Inscripciones de administrador de dispositivos para Android 10:
  - **31 de julio de 2020:** Citrix considera obsoletas las nuevas inscripciones para el modo de administración de dispositivos Android heredados.
  - **1 de noviembre de 2020:** Google retira la API de administración de dispositivos heredados. Los dispositivos Android 10 que se ejecutan en el modo de administración de dispositivos heredados ya no funcionarán.
- Cifrado MDX:
  - **1 de agosto de 2020:** Citrix comienza a aplicar la migración del cifrado MDX al cifrado de plataforma para las aplicaciones móviles de productividad de Citrix y las aplicaciones MDX de terceros.
  - **1 de septiembre de 2020:** El cifrado MDX llega al final de su vida útil.

Para dispositivos inscritos en la administración de dispositivos heredados

- Si no utiliza el cifrado MDX, no se requiere ninguna acción.
- Si usa el cifrado MDX, migre los dispositivos Android a Android Enterprise antes del 31 de julio de 2020. Los dispositivos Android 10 deben inscribirse o reinscribirse con Android Enterprise. Este requisito incluye los dispositivos Android en modo de solo MAM. Consulte Migrar de la administración de dispositivos a Android Enterprise.

Para dispositivos ya inscritos en Android Enterprise a partir del 31 de julio

- Si ha publicado las aplicaciones desde la plataforma Android Enterprise, el cifrado ya se gestiona a través de Android Enterprise. No se requiere ninguna acción.

- Si ha publicado las aplicaciones desde la plataforma Android heredada, vuelva a publicar las aplicaciones desde Android Enterprise antes del 31 de julio de 2020.

Antes de actualizar la versión de XenMobile a la 10.12 (instalación local)

Han cambiado algunos requisitos del sistema. Para obtener información, consulte Requisitos del sistema y compatibilidad y Compatibilidad de XenMobile.

1. Actualice Citrix License Server a la versión 11.16 o a una posterior antes de actualizarlo a la versión más reciente de XenMobile Server 10.12.

   La versión más reciente de XenMobile requiere Citrix License Server 11.16 (versión mínima).

   > **Nota:**
   >
   > Si quiere utilizar su propia licencia para Preview, tenga en cuenta que la fecha de Customer Success Services (anteriormente, la fecha de Subscription Advantage) en XenMobile 10.12 es el 20 de enero de 2020. La fecha de Customer Success Services de su licencia de Citrix debe ser posterior a esta fecha.
   >
   > Puede ver la fecha junto a la licencia en el servidor de licencias. Si conecta la versión más reciente de XenMobile a un entorno de servidor de licencias anterior, la comprobación de conectividad falla y no se puede configurar el servidor de licencias.

   Para renovar la fecha que consta en la licencia, descargue el archivo de licencias más reciente del Portal de Citrix y cárguelo en el servidor de licencias. Para obtener más información, consulte Customer Success Services.

2. Para un entorno en clúster, las implementaciones de aplicaciones y directivas iOS a dispositivos iOS 11 y posterior presentan el siguiente requisito. Si Citrix Gateway está configurado para la persistencia de SSL, debe abrir el puerto 80 en todos los nodos de XenMobile Server.
3. Si la máquina virtual que ejecuta XenMobile Server que quiere actualizar tiene menos de 4 GB de RAM, debe aumentarla a por lo menos 4 GB. Tenga en cuenta que la memoria RAM mínima recomendada es de 8 GB para entornos de producción.
4. Recomendación: Antes de instalar una actualización de XenMobile, utilice las funcionalidades de la máquina virtual (VM) para tomar una instantánea del sistema. Asimismo, realice una copia de seguridad de la base de datos de configuración del sistema. Si tiene problemas durante la actualización, las copias de seguridad completas le permitirán recuperar los datos.

Para actualizar la versión

Puede actualizar directamente la versión 10.11.x o 10.10.x de XenMobile a 10.12. Para actualizar la versión, descargue el último binario disponible en https://www.citrix.com/downloads. Vaya a **Citrix**

Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10. En el mosaico del software XenMobile Server para su hipervisor, haga clic en **Download File** (Descargar archivo).

Para cargar la actualización de la versión, utilice la página **Administración de versiones** de la consola de XenMobile. Para obtener más información, consulte Para actualizar desde la página "Administración de versiones".

Después de actualizar la versión

Después de actualizar la versión de XenMobile a la 10.12 (instalación local):

Si la funcionalidad relacionada con las conexiones de salida deja de funcionar y no ha cambiado la configuración de las conexiones, busque errores similares a los siguientes en el registro de XenMobile Server: "No se puede conectar con el servidor del programa VPP: El nombre de host '192.0.2.0' no coincide con el sujeto de certificado suministrado por el servidor homólogo".

Si recibe el error de validación de certificado, inhabilite la verificación de nombres de host en el XenMobile Server. De forma predeterminada, la verificación de nombres de host está habilitada en las conexiones salientes, excepto para el servidor PKI de Microsoft. Si la verificación de nombre de host deja inoperativa la implementación, cambie la propiedad de servidor `disable.hostname.verification` a **`true`**. El valor predeterminado de esta propiedad es **`false`**.

Compatibilidad adicional con iOS 13

XenMobile Server admite dispositivos actualizados a iOS 13. La actualización afecta a los usuarios de la siguiente manera:

- Durante la inscripción, aparecen nuevas pantallas de opciones del Asistente de configuración de iOS. Apple ha agregado a iOS 13 nuevas pantallas de opciones del Asistente de configuración de iOS. Las nuevas opciones se incluyen en la página **Parámetros > Programa de inscripción de dispositivos de Apple (DEP)** de esta versión. Puede configurar XenMobile Server para omitir esas pantallas. Esas páginas aparecen a los usuarios en los dispositivos iOS 13.
- Algunas configuraciones de la directiva Restricciones que estaban disponibles en dispositivos supervisados o no supervisados para versiones anteriores de iOS solo están disponibles en dispositivos supervisados para versiones posteriores a iOS 13. El texto actual de ayuda en la consola de XenMobile Server aún no indica que estos parámetros son solo para dispositivos supervisados posteriores a iOS 13.
  - Permitir controles del hardware:
    - FaceTime
    - Instalar aplicaciones
  - Permitir aplicaciones

        * iTunes Store
        * Safari
        * Safari > Autorrelleno
    - Red: Permitir acciones de iCloud
        * Datos y documentos de iCloud
    - Parámetros solo para dispositivos supervisados: Permitir
        * Game Center > Añadir amigos
        * Game Center > Juegos multijugador
    - Contenido multimedia: Permitir
        * Música, podcasts y contenido de iTunes U explícito

Estas restricciones se aplican de la siguiente manera:

- Si un dispositivo con iOS 12 (o una versión anterior) ya está inscrito en XenMobile Server y, a continuación, se actualiza a iOS 13, las restricciones anteriores se aplican a los dispositivos no supervisados y supervisados.
- Si un dispositivo no supervisado con una versión posterior a iOS 13 se inscribe en XenMobile Server, las restricciones anteriores solo se aplican a los dispositivos supervisados.
- Si un dispositivo supervisado con una versión posterior a iOS 13 se inscribe en XenMobile Server, las restricciones anteriores solo se aplican a los dispositivos supervisados.

Migración del Programa de compras por volumen de Apple a Apple Business Manager (ABM) y Apple School Manager (ASM)

Las empresas e instituciones que utilizan el Programa de compras por volumen de Apple deben migrar a aplicaciones y libros en Apple Business Manager o Apple School Manager antes del 1 de diciembre de 2019.

Antes de migrar cuentas VPP en XenMobile, consulte este artículo de soporte de Apple.

Si su organización o centro educativo solo utiliza el Programa de compras por volumen (VPP), puede inscribirse en ABM/ASM e invitar a los compradores de VPP actuales a su nueva cuenta de ABM/ASM. Para ASM, vaya a https://school.apple.com. Para ABM, vaya a https://business.apple.com.

Para actualizar su cuenta de VPP 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 **Parámetros**.
2. Haga clic en **Parámetros de iOS**. Aparecerá la página de configuración del **Programa de Compras por Volumen**.
3. Asegúrese de que su cuenta de ABM o ASM tenga la misma configuración de aplicación que su cuenta VPP anterior.
4. En el portal de ABM o ASM, descargue un token actualizado.

5. En la consola de XenMobile, haga lo siguiente:
    a) Modifique la cuenta de compras por volumen existente con la información actualizada del token para esa ubicación.
    b) Modifique sus credenciales de ABM o ASM. No cambie el sufijo.
    c) Haga clic en **Guardar** dos veces.

Para obtener más información, consulte:

- Programa de implementación de Apple
- Inscribir en bloque dispositivos Apple

Compatibilidad con dispositivos COPE de Android Enterprise

XenMobile Server es compatible con dispositivos Android Enterprise totalmente administrados con perfiles de trabajo, antes conocidos como dispositivos COPE (propiedad de la empresa con acceso privado). Estos son dispositivos de tipo Android Enterprise totalmente administrados que además tienen un perfil de trabajo. Puede aplicar parámetros de directiva independientes al dispositivo y al perfil de trabajo. Para esta versión:

- Puede aplicar configuraciones independientes al dispositivo y al perfil de trabajo mediante estas directivas de dispositivo: Credenciales, Código de acceso y Restricciones.
- Puede aplicar el parámetro de modo de ubicación de la directiva de dispositivo Ubicación al propio dispositivo COPE, pero no al perfil de trabajo del dispositivo COPE. Otras opciones de configuración de la directiva de dispositivo Ubicación no están disponibles para los dispositivos COPE.
- Puede aplicar la acción de seguridad Bloquear por separado al dispositivo o al perfil de trabajo.

Directivas de dispositivo

En el caso de los dispositivos totalmente administrados con perfiles de trabajo (dispositivos COPE) Android Enterprise, algunas directivas de dispositivo pueden aplicar configuraciones diferentes a todo el dispositivo y al perfil de trabajo. En la consola de XenMobile Server, algunas directivas de dispositivo le permiten aplicar las distintas configuraciones. También puede usar otras directivas de dispositivo para aplicar una configuración solo a todo el dispositivo o solo al perfil de trabajo.

Acciones de seguridad

Para dispositivos Android Enterprise totalmente administrados con perfiles de trabajo (dispositivos COPE), puede aplicar:

- La acción de seguridad Bloquear por separado al dispositivo o al perfil de trabajo.
- Todas las demás acciones de seguridad al dispositivo.

Los perfiles de inscripción controlan las opciones de inscripción de los dispositivos Android

Los perfiles de inscripción ahora controlan el método de inscripción de los dispositivos Android si Android Enterprise está habilitado para su implementación de XenMobile. Los perfiles de inscripción determinan si los dispositivos Android están inscritos en el modo predeterminado de Android Enterprise (completamente administrado o perfil de trabajo) o en el modo antiguo (administrador de dispositivos).

De forma predeterminada, el perfil de inscripción global registra los dispositivos Android Enterprise nuevos y de restablecimiento de fábrica como dispositivos totalmente administrados e inscribe los dispositivos BYOD Android Enterprise como dispositivos de perfil de trabajo. Para obtener más información, consulte Android Enterprise.

Preparación de dispositivos Android antiguos para Android Enterprise como inscripción predeterminada

Google va a retirar el modo de administrador de dispositivos de la administración de dispositivos y anima a los clientes a gestionar todos los dispositivos Android en el modo de propietario del dispositivo o en el modo de propietario del perfil (consulte Retirada del administrador de dispositivos en las guías para desarrolladores de Google Android Enterprise). Para adaptarse a este cambio, Android Enterprise es ahora la opción de inscripción predeterminada de los dispositivos Android.

Este cambio significa que si Android Enterprise está habilitado para la implementación de XenMobile, todos los dispositivos Android recién inscritos (o que se han inscrito de nuevo) se inscriben como dispositivos Android Enterprise.

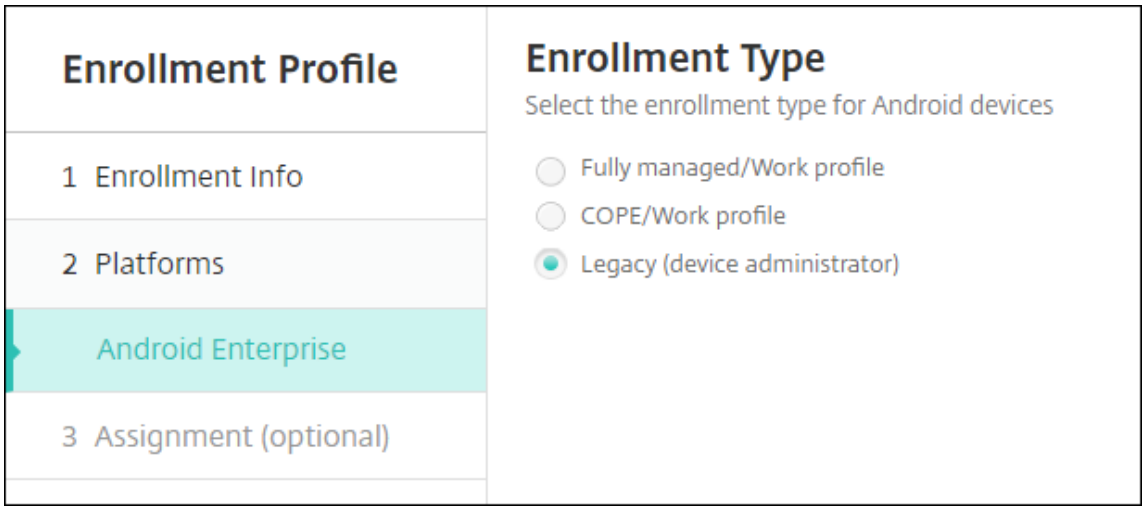
Para prepararse para este cambio, XenMobile ahora le permite crear perfiles de inscripción que controlan la forma en que se inscriben los dispositivos Android.

Es posible que su organización no esté preparada para comenzar a administrar dispositivos Android antiguos en modo de propietario del dispositivo o en modo de propietario del perfil. En ese caso, puede seguir administrándolos en el modo de administrador de dispositivos. Cree un perfil de inscripción para los dispositivos antiguos y vuelva a inscribir todos los dispositivos antiguos que ya están inscritos.

Para crear un perfil de inscripción para los dispositivos antiguos:

1. En la consola de XenMobile, vaya a **Configurar > Perfiles de inscripción**.
2. Para agregar un perfil de inscripción, haga clic en **Agregar**. En la página “Información de inscripción”, escriba un nombre para el perfil de inscripción.
3. Haga clic en **Siguiente** o seleccione **Android Enterprise** en **Plataformas**. Aparecerá la página Configuración de inscripción.

4. Establezca **Administración** en **Antigua (administración de dispositivos)**. Haga clic en **Siguiente** o seleccione **Asignación (optativa)**. Aparecerá la pantalla Asignación de grupos de entrega.



5. Elija un grupo o varios grupos de entrega que contengan los administradores que inscriben los dispositivos dedicados. A continuación, haga clic en **Guardar**.

Para seguir administrando dispositivos antiguos en el modo de administrador de dispositivos, inscríbalos o vuelva a inscribirlos con este perfil. Para inscribir dispositivos de administrador de dispositivos similares a los dispositivos de perfil de trabajo, los usuarios deben descargar Secure Hub y proporcionar una URL de servidor de inscripción.

Para obtener más información acerca de la compatibilidad de Endpoint Management con la transición a Android Enterprise, consulte el blog Android Enterprise as default for Citrix Endpoint Management service.

Administración simplificada de aplicaciones para Android Enterprise

Ya no es necesario ir a Google Play administrado o al portal Google Developers para aprobar o publicar aplicaciones para XenMobile Server. Como resultado, la aprobación y publicación de aplicaciones tardan unos 10 minutos, en lugar de horas.

Aprobar aplicaciones de Android Enterprise para la tienda pública de aplicaciones en la consola de XenMobile Server. Ahora puede aprobar aplicaciones de la tienda administrada de Google Play sin salir de la consola de XenMobile Server. Después de introducir un nombre de aplicación en el campo de búsqueda, se abrirá la interfaz de usuario de Google Play Store administrado con instrucciones para que apruebe y guarde la aplicación. A continuación, la aplicación aparece en los resultados para que pueda configurar los detalles. Consulte Agregar una aplicación de la tienda pública de aplicaciones.

Agregar aplicaciones MDX para Android Enterprise. La consola de XenMobile Server ahora admite

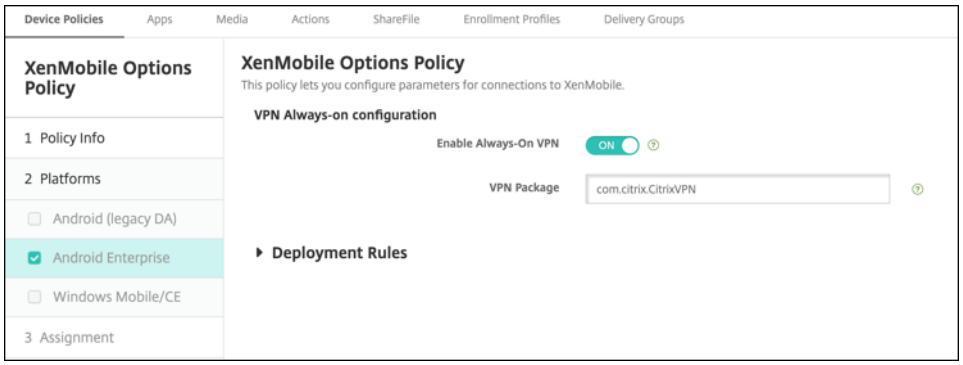
Android Enterprise como plataforma para la implementación de aplicaciones MDX. Consulte Agregar una aplicación MDX.

Aprobar aplicaciones MDX para Android Enterprise en la consola de XenMobile Server. Ahora puede aprobar aplicaciones de la tienda administrada de Google Play para Android Enterprise sin salir de la consola de XenMobile Server. Después de cargar un archivo MDX, se abrirá la interfaz de usuario de Google Play Store administrado con instrucciones para que apruebe y guarde la aplicación. Consulte Agregar una aplicación MDX.

Compatibilidad con VPN permanente para Android Enterprise

La directiva de dispositivos de XenMobile Server ahora le permite habilitar VPN permanente para Android Enterprise.

Al configurar perfiles de VPN para Android Enterprise, en **Perfil de VPN predeterminado**, introduzca el nombre del perfil de VPN. XenMobile utiliza este perfil cuando los usuarios tocan en el botón de conexión de la interfaz de usuario de la aplicación Citrix SSO, en lugar de tocar en un perfil específico. Si este campo se deja vacío, se utiliza el perfil principal para la conexión. Si solo se configura un perfil, este se marca como perfil predeterminado. Para la VPN permanente, este campo debe establecerse en el nombre del perfil de VPN que se utilizará para establecer la VPN permanente.



Configurar el seguimiento del producto para las aplicaciones de Android Enterprise

Al agregar una aplicación de la tienda pública o una aplicación MDX para Android Enterprise, configure el tipo de seguimiento de producto que quiere enviar a los dispositivos de usuario. Por ejemplo, si tiene un seguimiento diseñado para prueba, puede seleccionarlo y asignárselo a un grupo de entrega específico. Para obtener más información sobre cómo implementar una versión, consulte el Centro de ayuda de Google Play. Para obtener información sobre cómo configurar el seguimiento del producto, consulte Agregar una aplicación MDX o Agregar una aplicación de la tienda pública de aplicaciones.

Forzar un restablecimiento del código de acceso para usuarios de macOS

Cuando un dispositivo macOS recibe un perfil de configuración con una directiva de código de acceso, los usuarios deben proporcionar un código de acceso conforme a los parámetros de la directiva. Ahora puede forzar el restablecimiento de un código de acceso la próxima vez que un usuario se autentique. En la directiva de dispositivo Código de acceso para macOS (10.13 y versiones posteriores), habilite el nuevo parámetro **Forzar el restablecimiento del código de acceso**. Para obtener más información sobre la directiva, consulte Directiva de código de acceso.

Novedades en XenMobile Server 10.11

January 4, 2022

XenMobile Server 10.11 (Descarga en PDF)

Servicio XenMobile Migration Service

Si utiliza XenMobile Server local, nuestro servicio XenMobile Migration Service puede ayudarle a comenzar a usar el servicio Endpoint Management. La migración desde XenMobile Server a Citrix Endpoint Management no requiere que vuelva a inscribir los dispositivos.

Para iniciar la migración, póngase en contacto con un representante de ventas local de Citrix o con un socio de Citrix. Para obtener más información, consulte Servicio XenMobile Migration Service.

Migración del Programa de compras por volumen de Apple a Apple Business Manager (ABM) y Apple School Manager (ASM)

Las empresas e instituciones que utilizan el Programa de compras por volumen de Apple deben migrar a aplicaciones y libros en Apple Business Manager o Apple School Manager antes del 1 de diciembre de 2019.

Antes de migrar cuentas VPP en XenMobile, consulte este artículo de soporte de Apple.

Si su organización o centro educativo solo utiliza el Programa de compras por volumen (VPP), puede inscribirse en ABM/ASM e invitar a los compradores de VPP actuales a su nueva cuenta de ABM/ASM. Para ASM, vaya a https://school.apple.com. Para ABM, vaya a https://business.apple.com.

Para actualizar su cuenta de compras por volumen (anteriormente llamada VPP) 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 **Parámetros**.

2. Haga clic en **Compras por volumen**. Aparecerá la página de configuración de **Compras por volumen**.
3. Asegúrese de que su cuenta de ABM o ASM tenga la misma configuración de aplicación que su cuenta VPP anterior.
4. En el portal de ABM o ASM, descargue un token actualizado.
5. En la consola de XenMobile, haga lo siguiente:
   a) Modifique la cuenta de compras por volumen existente con la información actualizada del token para esa ubicación.
   b) Modifique sus credenciales de ABM o ASM. No cambie el sufijo.
   c) Haga clic en **Guardar** dos veces.

Compatibilidad adicional con iOS 13

> **Importante:**
>
> Con respecto a las actualizaciones de dispositivos a una versión posterior a iOS 12, tenga en cuenta que el tipo de conexión VPN de Citrix en la directiva VPN para iOS no admite versiones posteriores a iOS 12. Por eso, debe eliminar la directiva VPN existente y crear otra directiva VPN con el tipo de conexión Citrix SSO.
>
> La conexión Citrix VPN seguirá funcionando en dispositivos implementados anteriormente después de que elimine la directiva VPN. La nueva configuración de la directiva VPN surte efecto en XenMobile Server 10.11, durante la inscripción de usuario.

XenMobile Server admite dispositivos actualizados a iOS 13. La actualización afecta a los usuarios de la siguiente manera:

- Durante la inscripción, aparecen nuevas pantallas de opciones del Asistente de configuración de iOS. Apple ha agregado a iOS 13 nuevas pantallas de opciones del Asistente de configuración de iOS. Las nuevas opciones no se incluyen en la página **Parámetros > Programa de inscripción de dispositivos de Apple (DEP)** de esta versión. Por eso, no se puede configurar XenMobile Server para omitir esas pantallas. Esas páginas aparecen a los usuarios en los dispositivos iOS 13.
- Algunas configuraciones de la directiva Restricciones que estaban disponibles en dispositivos supervisados o no supervisados para versiones anteriores de iOS solo están disponibles en dispositivos supervisados para versiones posteriores a iOS 13. El texto actual de ayuda en la consola de XenMobile Server aún no indica que estos parámetros son solo para dispositivos supervisados posteriores a iOS 13.
  - Permitir controles del hardware:
    * FaceTime

        * Instalar aplicaciones
    - Permitir aplicaciones
        * iTunes Store
        * Safari
        * Safari > Autorrelleno
    - Red: Permitir acciones de iCloud
        * Datos y documentos de iCloud
    - Parámetros solo para dispositivos supervisados: Permitir
        * Game Center > Añadir amigos
        * Game Center > Juegos multijugador
    - Contenido multimedia: Permitir
        * Música, podcasts y contenido de iTunes U explícito

Estas restricciones se aplican de la siguiente manera:

- Si un dispositivo con iOS 12 (o una versión anterior) ya está inscrito en XenMobile Server y, a continuación, se actualiza a iOS 13, las restricciones anteriores se aplican a los dispositivos no supervisados y supervisados.
- Si un dispositivo no supervisado con una versión posterior a iOS 13 se inscribe en XenMobile Server, las restricciones anteriores solo se aplican a los dispositivos supervisados.
- Si un dispositivo supervisado con una versión posterior a iOS 13 se inscribe en XenMobile Server, las restricciones anteriores solo se aplican a los dispositivos supervisados.

Requisitos para certificados de confianza en iOS 13 y macOS 15

Apple tiene nuevos requisitos para certificados de servidor TLS. Verifique que todos los certificados cumplen los nuevos requisitos de Apple. Consulte la publicación de Apple: https://support.apple.com/en-us/HT210176. Para obtener ayuda sobre la administración de certificados, consulte Cargar certificados en XenMobile.

Actualizar la versión de GCM a la versión de FCM

El 10 de abril de 2018 Google retiró Google Cloud Messaging (GCM). El 29 de mayo de 2019 Google eliminó las API de servidores y clientes de GCM.

> **Requisitos importantes:**
>
> - Actualice a la versión más reciente de XenMobile Server.
> - Actualice a la versión más reciente de Secure Hub.

Google recomienda actualizar la versión de GCM a Firebase Cloud Messaging (FCM) de inmediato para empezar a disfrutar de las nuevas funciones que ofrece FCM. Para obtener información procedente de

Google, consulte https://developers.google.com/cloud-messaging/faq y https://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.html.

Para que las notificaciones push sigan estando disponibles en sus dispositivos Android: Si utiliza GCM con XenMobile Server, pásese a FCM. Luego, actualice XenMobile Server con la nueva clave de FCM disponible en Firebase Cloud Messaging Console.

Los pasos siguientes reflejan el flujo de trabajo de las inscripciones cuando se utilizan certificados de confianza.

Pasos de la actualización:

1. Siga las instrucciones de Google para actualizar la versión de GCM a la versión de FCM.
2. En Firebase Cloud Messaging Console, copie la nueva clave de FCM. La necesitará en el siguiente paso.
3. En la consola de XenMobile Server, vaya a **Parámetros > Firebase Cloud Messaging** y configure los parámetros como quiera.

Los dispositivos se pasarán a FCM la próxima vez que se conecten con XenMobile Server y actualicen sus directivas. Para obligar a que Secure Hub actualice las directivas: En Secure Hub, vaya a **Preferencias > Información del dispositivo** y toque **Actualizar directiva**.
Para obtener más información sobre la configuración de FCM, consulte Firebase Cloud Messaging.

Servicio XenMobile Migration Service

Si utiliza XenMobile Server local, nuestro servicio XenMobile Migration Service puede ayudarle a comenzar a usar el servicio Endpoint Management. La migración desde XenMobile Server a Citrix Endpoint Management no requiere que vuelva a inscribir los dispositivos.

Para obtener más información, contacte con el representante de ventas, el ingeniero de sistemas o Partner de Citrix local. En estos artículos de blog, se comenta el servicio XenMobile Migration Service:

New XenMobile Migration Service

Making the Case for XenMobile in the Cloud

Antes de actualizar la versión de XenMobile a la 10.11 (instalación local)

Han cambiado algunos requisitos del sistema. Para obtener información, consulte Requisitos del sistema y compatibilidad y Compatibilidad de XenMobile.

1. Actualice Citrix License Server a la versión 11.15 o a una posterior antes de actualizarlo a la versión más reciente de XenMobile Server 10.11.

   La versión más reciente de XenMobile requiere Citrix License Server 11.15 (versión mínima).

> **Nota:**
>
> Si quiere utilizar su propia licencia para Preview, tenga en cuenta que la fecha de Customer Success Services (anteriormente, la fecha de Subscription Advantage) en XenMobile 10.11 es el 9 de abril de 2019. La fecha de Customer Success Services de su licencia de Citrix debe ser posterior a esta fecha.
>
> Puede ver la fecha junto a la licencia en el servidor de licencias. Si conecta la versión más reciente de XenMobile a un entorno de servidor de licencias anterior, la comprobación de conectividad falla y no se puede configurar el servidor de licencias.

Para renovar la fecha que consta en la licencia, descargue el archivo de licencias más reciente del Portal de Citrix y cárguelo en el servidor de licencias. Para obtener más información, consulte Customer Success Services.

2. Para un entorno en clúster, las implementaciones de aplicaciones y directivas iOS a dispositivos iOS 11 y posterior presentan el siguiente requisito. Si Citrix Gateway está configurado para la persistencia de SSL, debe abrir el puerto 80 en todos los nodos de XenMobile Server.
3. Si la máquina virtual que ejecuta XenMobile Server que quiere actualizar tiene menos de 4 GB de RAM, debe aumentarla a por lo menos 4 GB. Tenga en cuenta que la memoria RAM mínima recomendada es de 8 GB para entornos de producción.
4. Recomendación: Antes de instalar una actualización de XenMobile, utilice las funcionalidades de la máquina virtual (VM) para tomar una instantánea del sistema. Asimismo, realice una copia de seguridad de la base de datos de configuración del sistema. Si tiene problemas durante la actualización, las copias de seguridad completas le permitirán recuperar los datos.

Para actualizar la versión

Puede actualizar directamente la versión 10.10.x o 10.9.x de XenMobile a 10.11. Para actualizar la versión, descargue el último binario disponible en https://www.citrix.com/downloads. Vaya a **Citrix Endpoint Management (y Citrix XenMobile Server) > XenMobile Server (local) > Software de producto > XenMobile Server 10**. En el mosaico del software XenMobile Server para su hipervisor, haga clic en **Download File** (Descargar archivo).

Para cargar la actualización de la versión, utilice la página **Administración de versiones** de la consola de XenMobile. Para obtener más información, consulte Para actualizar desde la página "Administración de versiones".

Después de actualizar la versión

Después de actualizar la versión de XenMobile a la 10.11 (instalación local):

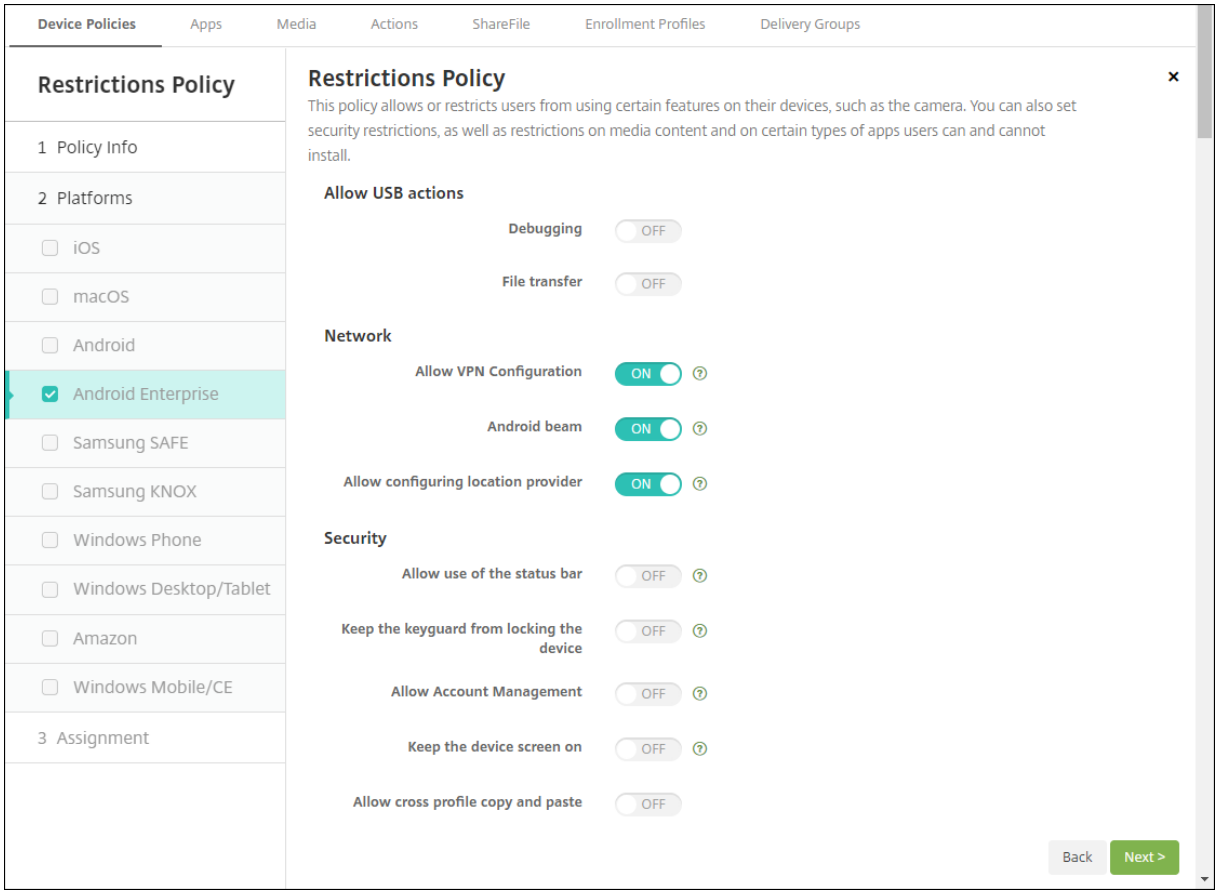
Si la funcionalidad relacionada con las conexiones de salida deja de funcionar y no ha cambiado la configuración de las conexiones, busque errores similares a los siguientes en el registro de XenMobile Server: "No se puede conectar con el servidor del programa VPP: El nombre de host '192.0.2.0' no coincide con el sujeto de certificado suministrado por el servidor homólogo".

Si recibe el error de validación de certificado, inhabilite la verificación de nombres de host en el XenMobile Server. De forma predeterminada, la verificación de nombres de host está habilitada en las conexiones salientes, excepto para el servidor PKI de Microsoft. Si la verificación de nombre de host deja inoperativa la implementación, cambie la propiedad de servidor `disable.hostname.verification` a **`true`**. El valor predeterminado de esta propiedad es **`false`**.

Configuraciones de directiva nuevas y actualizadas para dispositivos Android Enterprise

Directivas unificadas de Samsung Knox y Android Enterprise. Para dispositivos Android Enterprise con Samsung Knox 3.0 o posterior y Android 8.0 o posterior, Knox y Android Enterprise se han combinado en una solución unificada de administración de perfiles y dispositivos.
Defina la configuración de Knox en la página Android Enterprise de las siguientes directivas de dispositivo:

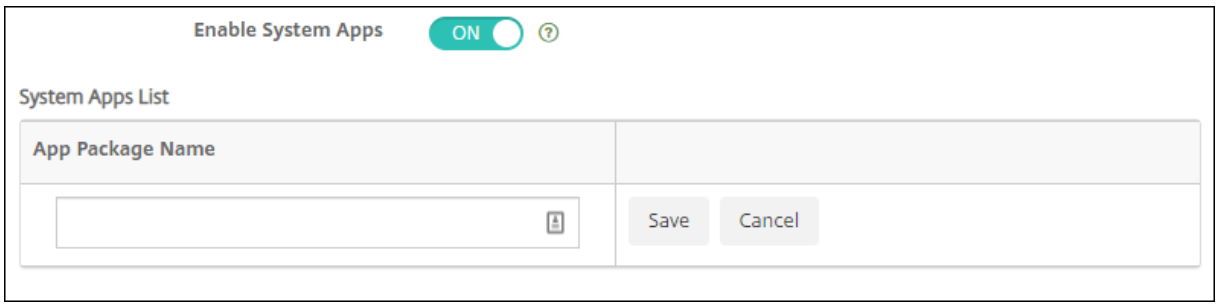
- **Directiva de actualización de SO de dispositivo.** Incluye configuraciones para las actualizaciones de Samsung Enterprise FOTA.
- **Directiva de código de acceso.**
- **Directiva de clave de licencia MDM de Samsung.** Configura la clave de licencia para Knox.
- **Configuraciones de la directiva Restricciones.**



Directiva de inventario de aplicaciones para Android Enterprise. Ahora, puede recopilar un inventario de las aplicaciones Android Enterprise que haya presentes en los dispositivos administrados. Consulte Directiva de inventario de aplicaciones.

Acceder a todas las aplicaciones de Google Play en Google Play Store administrado. La propiedad de servidor **Access all apps in the managed Google Play store** permite acceder a todas las aplicaciones de Google Play Store público desde Google Play Store administrado. Al establecer esta propiedad en **true**, se permiten las aplicaciones de la tienda pública de Google Play para todos los usuarios de Android Enterprise. A continuación, los administradores pueden usar la directiva de restricciones para controlar el acceso a estas aplicaciones.

Habilitar aplicaciones del sistema en dispositivos Android Enterprise. Para permitir que los usuarios ejecuten aplicaciones del sistema preinstaladas en el modo de perfil de trabajo o en el modo totalmente administrado de Android Enterprise, configure la directiva de restricciones. Esa configuración otorga a los usuarios acceso a las aplicaciones predeterminadas de los dispositivos, como la cámara, la galería y otras. Para restringir el acceso a una aplicación concreta, establezca los permisos de aplicación mediante la directiva de permisos de aplicación de Android Enterprise.



Se admiten dispositivos dedicados Android Enterprise. Ahora XenMobile admite la administración de dispositivos dedicados, anteriormente denominados dispositivos de uso único y propiedad de la empresa (COSU).

Los dispositivos Android Enterprise dedicados son dispositivos totalmente administrados que se destinan a cumplir un solo caso de uso. Así, restringe estos dispositivos a una aplicación o a un pequeño conjunto de aplicaciones que permitan realizar las tareas necesarias para este caso de uso. También impide que los usuarios habiliten otras aplicaciones o realicen otras acciones en el dispositivo.

Para obtener información sobre el aprovisionamiento de dispositivos Android Enterprise, consulte Aprovisionar dispositivos Android Enterprise dedicados.

Directiva renombrada. Para mayor concordancia con la terminología de Google, la directiva Restricciones a aplicaciones para Android Enterprise ahora se denomina Configuraciones administradas de Android Enterprise. Consulte Directiva Configuraciones administradas por Android Enterprise.

Bloquear y restablecer contraseña para Android Enterprise

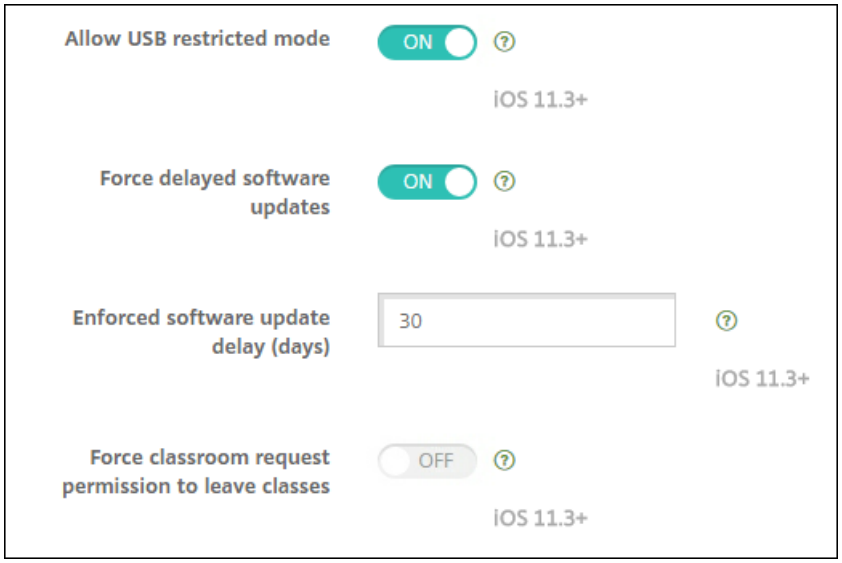
Ahora XenMobile admite la acción de seguridad Bloquear y restablecer contraseña para dispositivos Android Enterprise. Esos dispositivos deben estar inscritos en el modo perfil de trabajo con Android 8.0 o posterior.

- El código de acceso enviado bloquea el perfil de trabajo. El dispositivo no se bloquea.
- Si no se envía ningún código de acceso o el código enviado no cumple los requisitos de código de acceso:
  - Si aún no hay ningún código de acceso establecido en el perfil de trabajo, el dispositivo se bloquea.
  - Si ya hay un código de acceso establecido en el perfil de trabajo, el perfil de trabajo se bloquea pero el dispositivo no.

Para obtener más información sobre las acciones de seguridad de bloqueo y restablecimiento de contraseña, consulte Acciones de seguridad.

Nuevas configuraciones de la directiva Restricciones para iOS o macOS

- **Las aplicaciones no administradas pueden leer contactos administrados:** Opcional. Solo disponible si **Documentos de aplicaciones administradas en aplicaciones no administradas** está desactivado. Si esta directiva está habilitada, las aplicaciones no administradas pueden leer datos de los contactos de las cuentas administradas. Está **desactivado** de forma predeterminada. Disponible a partir de iOS 12.
- **Las aplicaciones administradas pueden registrar contactos no administrados:** Opcional. Si está habilitado, se permite que las aplicaciones administradas agreguen contactos a los contactos de cuentas no administradas. Si **Documentos de aplicaciones administradas en aplicaciones no administradas** está habilitado, esta restricción no tiene efecto. Está **desactivado** de forma predeterminada. Disponible a partir de iOS 12.
- **Autorrelleno de contraseñas:** Opcional. Si está inhabilitado, los usuarios no pueden usar las funciones de autorrelleno de contraseñas o sugerencias de contraseñas seguras. De forma predeterminada, está **activado**. Disponible a partir de iOS 12 y macOS 10.14.
- **Solicitud de contraseña a los contactos cercanos:** Opcional. Si está inhabilitado, los dispositivos de los usuarios no solicitan contraseñas de los dispositivos cercanos. De forma predeterminada, está **activado**. Disponible a partir de iOS 12 y macOS 10.14.
- **Compartir contraseña:** Opcional. Si está inhabilitado, los usuarios no pueden compartir sus contraseñas mediante la función de contraseñas de AirDrop. De forma predeterminada, está **activado**. Disponible a partir de iOS 12 y macOS 10.14.
- **Forzar fecha y hora automáticas:** Supervisado. Si está activada, los usuarios no pueden desactivar la opción **General > Fecha y hora > Establecer automáticamente**. Está **desactivado** de forma predeterminada. Disponible a partir de iOS 12.
- **Permitir modo restringido de USB:** Solo disponible para dispositivos supervisados. Si está desactivado, el dispositivo siempre se puede conectar a accesorios USB mientras está bloqueado. De forma predeterminada, está **activado**. Disponible a partir de iOS 11.3.
- **Forzar demora de actualizaciones de software:** Solo disponible para dispositivos supervisados. Si se **activa**, el usuario ve las actualizaciones de software más tarde. Con esta restricción activada, el usuario no verá una actualización de software hasta que transcurra la cantidad especificada de días después de la fecha de publicación de la actualización. Está **desactivado** de forma predeterminada. Disponible a partir de iOS 11.3 y macOS 10.13.4.
- **Demora forzosa para actualizaciones de software (días):** Solo disponible para dispositivos supervisados. Esta restricción permite al administrador establecer la demora de una actualización de software en el dispositivo. El valor máximo es de 90 días y el valor predeterminado es **30**. Disponible a partir de iOS 11.3 y macOS 10.13.4.
- **Forzar permiso del aula para abandonar clases:** Solo está disponible para dispositivos supervisados. Si está **activado**, un alumno matriculado en un curso no gestionado con Aula debe solicitar el permiso del profesor cuando intenta abandonar el curso. Está **desactivado** de forma predeterminada. Disponible a partir de iOS 11.3.



Consulte Directiva de restricciones.

Actualizaciones en la directiva de Exchange para iOS o macOS

Más parámetros de cifrado y de firma S/MIME Exchange a partir de iOS 12. Ahora la directiva de Exchange incluye configuraciones para definir el cifrado y la firma S/MIME.

Para la firma S/MIME:

- **Credencial de identidad para firma.** Seleccione la credencial de firma que se va a usar.
- **Firma S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden activar y desactivar la firma S/MIME en la configuración de sus dispositivos. Está **desactivado** de forma predeterminada.
- **UUID de certificado de firma S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden seleccionar, en la configuración de sus dispositivos, la credencial de firma que se va a usar. Está **desactivado** de forma predeterminada.

Para el cifrado S/MIME:

- **Credencial de identidad para cifrado.** Seleccione la credencial de cifrado que se va a usar.
- **Habilitar cambio de opción S/MIME para cada mensaje:** Cuando se **activa**, los usuarios ven una opción para activar o desactivar el cifrado S/MIME para cada mensaje que escriban. Está **desactivado** de forma predeterminada.
- **Cifrado S/MIME predeterminado reemplazable por el usuario:** Si se **activa**, los usuarios pueden, en la configuración de sus dispositivos, seleccionar si S/MIME está activado de forma predeterminada. Está **desactivado** de forma predeterminada.
- **UUID de certificado de cifrado S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden activar y desactivar el cifrado S/MIME y la identidad del cifrado S/MIME en la configuración de sus dispositivos. Está **desactivado** de forma predeterminada.

Configuraciones de OAuth en la directiva Exchange a partir de iOS 12. Ahora puede configurar la conexión con Exchange para usar OAuth en la autenticación.

Configuraciones de OAuth en la directiva Exchange a partir de macOS 10.14. Ahora puede configurar la conexión con Exchange para usar OAuth en la autenticación. Para la autenticación mediante OAuth, puede especificar la URL de inicio de sesión para una instalación que no utilice la detección automática.

Consulte Directiva de Exchange.

Actualizaciones en la directiva Correo para iOS

Más parámetros de cifrado y de firma S/MIME Exchange a partir de iOS 12. La directiva Correo incluye más configuraciones para definir el cifrado y la firma S/MIME.

Para la firma S/MIME:

- **Habilitar firma S/MIME:** Seleccione si esta cuenta admite la firma S/MIME. Está **activado** de forma predeterminada. Si se **activa**, aparecen los siguientes campos.
  - **Firma S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden activar y desactivar la firma S/MIME en la configuración de sus dispositivos. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.
  - **UUID de certificado de firma S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden seleccionar, en la configuración de sus dispositivos, la credencial de firma que se va a usar. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.

Para el cifrado S/MIME:

- **Habilitar cifrado S/MIME:** Seleccione si esta cuenta admite el cifrado S/MIME. Está **desactivado** de forma predeterminada. Si se **activa**, aparecen los siguientes campos.
  - **Habilitar cambio de opción S/MIME para cada mensaje:** Cuando se **activa**, los usuarios ven una opción para activar o desactivar el cifrado S/MIME para cada mensaje que escriban. Está **desactivado** de forma predeterminada.
  - **Cifrado S/MIME predeterminado reemplazable por el usuario:** Si se **activa**, los usuarios pueden, en la configuración de sus dispositivos, seleccionar si S/MIME está activado de forma predeterminada. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.
  - **UUID de certificado de cifrado S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden activar y desactivar el cifrado S/MIME y la identidad del cifrado S/MIME en la configuración de sus dispositivos. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.

Consulte Directiva de correo.

Actualizaciones en la directiva Notificaciones de aplicaciones para iOS

A partir de iOS 12, están disponibles las siguientes configuraciones en la directiva Notificaciones de aplicaciones.

- **Mostrar en CarPlay:** Si está **activado**, se muestran notificaciones en Apple CarPlay. De forma predeterminada, está **activado**.
- **Habilitar alerta crítica:** Si está **activado**, permite que una aplicación marque una notificación como crítica, con lo que esa aplicación ignora los parámetros de No molestar y de tono. Está **desactivado** de forma predeterminada.

Consulte Directiva de notificaciones de aplicaciones.

Compatibilidad con iPads compartidos utilizados con Apple Education

La integración de XenMobile con las funciones de Apple Education ahora admite iPads compartidos. Varios alumnos de un aula pueden compartir un iPad para las diferentes materias o asignaturas impartidas por uno o varios profesores.

O usted o los profesores inscriben los iPads compartidos y luego implementan directivas de dispositivo, aplicaciones y archivos multimedia en ellos. A continuación, los alumnos proporcionan sus credenciales administradas de ID de Apple para iniciar sesión en un iPad compartido. Si implementó anteriormente una directiva de configuración de la educación en los dispositivos de los alumnos, no es necesario que inicien sesión como “Otro usuario” para compartir esos dispositivos.

Requisitos previos para iPads compartidos:

- Cualquier iPad Pro, iPad de 5.ª generación, iPad Air 2 o posterior y iPad mini 4 o posterior
- Al menos 32 GB de almacenamiento
- Supervisado

Para obtener más información, consulte Configurar iPads compartidos.

Cambio en los permisos del control de acceso por roles (RBAC)

Ahora el permiso RBAC Agregar/Eliminar usuarios locales se divide en dos permisos: Agregar usuarios locales y Eliminar usuarios locales.

Para obtener información, consulte Configurar roles con RBAC.

Avisos legales de terceros

January 4, 2022

Esta versión de XenMobile puede incluir software de terceros con licencias definidas en los términos de los siguientes documentos:

Avisos legales de terceros para XenMobile

Elementos retirados

January 4, 2022

Los anuncios de este artículo tienen por objeto avisarle por adelantado acerca de las funciones de XenMobile Server que se están retirando progresivamente. Proporcionamos esta información de modo que pueda tomar a tiempo las decisiones empresariales pertinentes. Citrix examina el uso que hacen los clientes de una función que está por retirar y los comentarios que tengan sobre la eliminación de la función para determinar cuándo retirarla. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas. Para obtener información detallada acerca del soporte técnico de la vida útil del producto, consulte el artículo Política de soporte técnico de la vida útil del producto.

Elementos eliminados y obsoletos

En la lista siguiente se muestran las funciones de XenMobile Server que se han retirado o eliminado.

Los elementos *obsoletos* no se eliminan inmediatamente. Citrix sigue ofreciendo los elementos retirados hasta eliminarlos en una versión futura.

Los elementos *eliminados* se quitan (o dejan de desarrollarse) en XenMobile Server.

Para obtener información sobre las aplicaciones móviles de productividad que han alcanzado el fin de su vida, consulte Fin de vida y aplicaciones retiradas.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Knox Mobile Enrollment (AD heredado)	Knox Mobile Enrollment (KME) se retiró del modo de administrador de dispositivos heredado en todas las versiones de Android.	4 de mayo de 2021	Objetivo: 30 de junio de 2021	Utilice KME para inscribirse en el modo Android Enterprise. Android 8, 9, 10 y 11 admiten Android Enterprise.
Aplicaciones móviles de Citrix y aplicaciones Workspace para Android 7.x y iOS 12.x	Ya no se admiten las versiones de Android 7.x y iOS 12.x de Secure Hub, Secure Mail, Secure Web y la aplicación Citrix Workspace.	Abril de 2021	Objetivo: Junio de 2021	Use, como mínimo, la versión actual y la anterior de todas las plataformas de los sistemas operativos principales. Los dispositivos antiguos siguen inscritos. Sin embargo, Citrix no prueba ni admite los dispositivos heredados.
Credenciales derivadas	Desarrollo detenido de las credenciales derivadas y de la aplicación Citrix Derived Credentials Manager.	25 de marzo de 2021	Objetivo: Segundo trimestre de 2021	Consulte iOS para obtener una lista de los tipos de autenticación admitidos en iOS.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Internet Explorer 11	Se retiró la compatibilidad de Internet Explorer con la consola de XenMobile Server.	Enero de 2021	Enero de 2021	Utilice la versión más reciente de estos exploradores web: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari
Compatibilidad con token de software de RSA para Android	Se retiró la importación directa de tokens de software de RSA en Secure Hub para Android.	Enero de 2021	Febrero de 2021	Puede importar el token de software de RSA en la aplicación RSA SecurID disponible en Google Play. A continuación, puede usar el token para la autenticación de Citrix Gateway.
Android Sony	Ya no se admiten los dispositivos Android Sony ni las directivas específicas de Sony.	Enero de 2021	Febrero de 2021	Use Android Enterprise.
Android HTC	Ya no se admiten los dispositivos Android HTC ni las directivas específicas de HTC.	Enero de 2021	Febrero de 2021	Use Android Enterprise.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Componente de terceros del panel de mandos de XenMobile	Retiraremos un componente de terceros que forma parte del panel de mandos de XenMobile.	Diciembre de 2020	Enero de 2021	Para seguir usando el panel de mandos, actualice la versión de XenMobile a 10.12 o a una posterior.
Aplicaciones publicadas para el modo Administrador de dispositivos heredado en dispositivos Android Enterprise	Ya no entregamos aplicaciones publicadas para la plataforma AD heredada a los dispositivos inscritos en Android Enterprise.	Octubre de 2020	Noviembre de 2020	Para los dispositivos Android Enterprise, debe publicar aplicaciones para la plataforma Android Enterprise. Para continuar publicando aplicaciones en modo AD heredado para dispositivos en modo AD, cree un grupo de entrega aparte para esas aplicaciones.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Puertos de salida del servicio de notificaciones push de Apple (APNs)	Apple dejará de desarrollar el protocolo binario heredado de APNs a partir del 31 de marzo de 2021. Apple recomienda que se utilice en su lugar la API del proveedor de APNs basada en HTTP/2. Como parte de este cambio, no se admitirán los puertos 2195 ni 2196, utilizados para enviar notificaciones de APNs a `*.push.apple.com`.	Octubre de 2020	Objetivo: Abril de 2021	Utilice el puerto 443 o 2197 en su lugar. Consulte Abrir puertos de XenMobile para administrar dispositivos.
Contenedor SEAMS de Samsung	Ya no se admite el contenedor SEAMS de Samsung.	Junio de 2020	Agosto de 2020	Utilice la aplicación Samsung Knox Service Plug-in (KSP) para Android Enterprise. Consulte Agregar la aplicación Knox Service Plugin.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Certificados SSL (capa de sockets seguros) autofirmados	Se retiró el soporte para certificados SSL autofirmados de todas las plataformas de dispositivos.	Mayo de 2020		Reemplace el certificado autofirmado existente por un certificado SSL de confianza procedente de una entidad de certificación (CA) conocida.
Algoritmos de firma de autenticación basados en certificados (no FIPS y cifrados débiles)	Se retiró el soporte de los siguientes algoritmos de firma: SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA SHA1withDSA, RIPEMD160withRS RIPEMD128withRS RIPEMD256withRS	Mayo de 2020	Enero de 2021	Al crear una solicitud de firma de certificado (CSR) para un proveedor de credenciales en la consola de XenMobile (**Configuración > Proveedores de credenciales > Solicitud de firma de certificado**), elija un cifrado más sólido.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Servidores de bases de datos	Funcionalidad retirada para Microsoft SQL Server 2014 y versiones anteriores.	Octubre de 2021	Agosto de 2022	Actualice el sistema a una de estas versiones compatibles: Microsoft SQL Server 2016 SP2, Microsoft SQL Server 2017 CU 13 o Microsoft SQL Server 2019 CTP 3.2. Consulte la lista de servidores compatibles en Requisitos del sistema y compatibilidad.
Hipervisores	Se ha retirado la compatibilidad con Citrix XenServer 6.5.x y versiones anteriores, así como con VMware ESXi 5.5 Update 3 y versiones anteriores, e Hyper-V 2012.	Mayo de 2020	Agosto de 2020	Actualice el sistema a una de las siguientes versiones compatibles: Citrix Hypervisor 8.0 o una versión posterior, Citrix XenServer 7.0 o una versión posterior, VMware (ESXi 6.0, ESXi 6.5.0 Update 3, ESXi 6.7 Update 2, parche 10 o ESXi 7.0) o Hyper-V (Windows Server 2016 o Windows Server 2019).

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Citrix Launcher	Ya no se admite la aplicación Citrix Launcher.	Mayo de 2020	Objetivo: Agosto de 2020 (eliminar de la tienda de aplicaciones)	Aprovisionar dispositivos como quioscos (dispositivos dedicados). Para obtener más información, consulte Sustitución de Citrix Launcher.
Aplicaciones móviles de Citrix y aplicaciones Workspace para Android 6.x y iOS 11.x	Ya no se admiten las versiones de Android 6.x y iOS 11.x de Secure Hub, Secure Mail, Secure Web y la aplicación Citrix Workspace.	Abril de 2020	Junio de 2020	Use, como mínimo, la versión actual y la anterior de todas las plataformas de los sistemas operativos principales.
MDX Toolkit y MDX Service	Se ha retirado la funcionalidad para MDX Toolkit y MDX Service en favor del SDK de Mobile App Management (MAM). Durante esta transición, podrá usar aplicaciones MDX empaquetadas y aplicaciones desarrolladas por el SDK de MAM.	Marzo de 2020	Objetivo: Marzo de 2022 (para MDX Toolkit) y septiembre de 2021 (para MDX Service)	Para seguir administrando sus aplicaciones de empresa, use el SDK de MAM.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
MDX: Servidor de Gateway alternativo	Se retiró la autenticación de nivel superior para dispositivos iOS y Android.	Marzo de 2020	Objetivo: Septiembre de 2021	No hay alternativa
MDX: Micro VPN (modo de túnel completo)	Se retiró el túnel completo de red privada virtual (VPN) para dispositivos iOS y Android.	Marzo de 2020	Objetivo: Septiembre de 2021	Utilice el modo SSO web del SDK de MAM o cree una directiva VPN por aplicación con el tipo de conexión Citrix SSO.
MDX: Compatibilidad con archivos PAC	Se retiró el archivo de configuración automática de proxy (PAC) con una implementación de túnel completo de VPN para los dispositivos iOS y Android.	Marzo de 2020	Objetivo: Septiembre de 2021	Utilice Citrix Gateway para conectarse a través de un servidor proxy para acceder a redes internas.
Compatibilidad con dispositivos MDX compartidos	Se retiró la compatibilidad con dispositivos compartidos para las aplicaciones MDX.	Marzo de 2020	Objetivo: Septiembre de 2021	Para Android Enterprise, use la compatibilidad con dispositivos compartidos para MDM. Para iOS, use Apple School Manager o GroundControl.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Nuevas inscripciones de administrador de dispositivos para Android 10	Se retiró el soporte para nuevas inscripciones o reinscripciones en el modo de administrador de dispositivos antiguos en dispositivos Android 10. Los dispositivos ya inscritos continúan funcionando.	Febrero de 2020	Septiembre de 2020	Inscriba los nuevos dispositivos Android 10 (o una versión posterior) en Android Enterprise.
Modo de administrador de dispositivos heredado para dispositivos Android 10	Google ha retirado algunas API de Administrador de dispositivos. Citrix no admite dispositivos Android 10 inscritos en el modo Administrador de dispositivos después de actualizar la versión de Citrix Secure Hub al nivel 29 de la API de Android.	Febrero de 2020	Noviembre de 2020	Migre los dispositivos Android 10 a Android Enterprise.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Cifrado MDX	Se han retirado el cifrado MDX y la función de cifrado MDX de la consola de XenMobile.	Octubre de 2019	Septiembre de 2020	Habilite el cifrado de plataformas iOS o Android mediante nuestra función de administración de cifrados con comprobación adicional de cumplimiento de normas. Debe probar y planificar la migración del cifrado MDX antes de julio de 2020.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Directiva de código de acceso: La configuración **Sin restricciones** para Android Enterprise	Los dispositivos Android Enterprise con Android 7 o una versión posterior solo admiten códigos de acceso creados sin restricciones de caracteres. Si había establecido **Caracteres requeridos** en **No hay restricciones**, esta actualización cambia el valor a **Solo números**.	Febrero de 2019	Abril de 2019	Este cambio no afecta a la experiencia actual de inicio de sesión de los usuarios.
Remote Support	El cliente Remote Support para implementaciones de XenMobile Server en clústeres locales ya no está disponible.	Enero de 2019	Agosto de 2020	No hay alternativa

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Extensiones de red de Secure Hub para iOS	En Secure Hub 20.3.0 se retiró el marco de extensión de red que le permitía personalizar funciones de red para dispositivos iOS.	Octubre de 2018	Marzo de 2020	No hay alternativa
Versiones 1.0 y 1.1 de TLS	Para mejorar la seguridad de XenMobile, Citrix bloqueará cualquier comunicación a través de Transport Layer Security (TLS) 1.0 y 1.1. Debido al debilitamiento de su seguridad, PCI Council va a retirar TLS 1.0 y TLS 1.1.	Junio de 2018	Marzo de 2019	Actualice a TLS 1.2.
Windows Mobile/CE	Ya no se admiten dispositivos Windows Mobile/CE.	Abril de 2018	Septiembre de 2020	Use equipos de escritorio y portátiles Windows 10.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Android TouchDown	DigiCert dejó de admitir Android TouchDown. Citrix retirará la página de la plataforma Android TouchDown de la directiva de dispositivo de Exchange.	Julio de 2018	2021	Recomendación: Utilice Citrix Secure Mail.

Problemas resueltos

September 19, 2021

Se han resuelto los siguientes problemas en XenMobile 10.14:

- Después de actualizar la versión de XenMobile Server a 10.12, hay problemas con la vista del panel de mandos en la consola de XenMobile Server. [CXM-88918]
- La inscripción de programas de implementación de Apple (antes denominados DEP) falla en dispositivos Apple cuando está configurado el protocolo PKI genérico. [CXM-89978]
- Se requieren permisos adicionales para modificar los perfiles de inscripción cuando se inicia sesión con el control de acceso por roles (RBAC). [CXM-89985]
- En la consola de XenMobile Server, no se puede modificar la directiva **Configuraciones administradas por Android Enterprise** para la aplicación de Chrome. [CXM-89986]
- En la plataforma iOS, al modificar una directiva de VPN cuyo tipo de conexión es **Configuración dual AlwaysOn IKEv2**, se produce un error. [CXM-90010]
- La inscripción de dispositivos Android Enterprise con **SamAccountName** falla y aparece este error: “Work profile deleted, wiping profile”. [CXM-90049]
- La base de datos no acepta nombres de usuario que empiezan por “u” minúscula. [CXM-90722]
- La consola de XenMobile Server muestra el ID de tarjeta con circuito integrado (ICCID) en el caso de dispositivos que no tienen ninguna tarjeta SIM insertada. [CXM-90845]

- La inscripción del programa de inscripción de dispositivos (DEP) de Apple falla en dispositivos con iOS 14. [CXM-91697]
- En la consola de XenMobile Server, no se muestra la fecha de caducidad correcta del certificado raíz. [CXM-91961]
- En XenMobile Server, las comprobaciones de conectividad de NetScaler Gateway no muestran ningún resultado. [CXM-93129]
- Al agregar usuarios de SNMP a la consola de XenMobile Server, los usuarios no aparecen en la lista *Usuarios de supervisión SNMP* o los agentes de SNMP quedan inactivos. [CXM-93197]
- Si habilita las configuraciones **Habilitar aplicaciones del sistema** e **Inhabilitar aplicaciones** para la misma aplicación en la directiva de restricciones, la aplicación sigue apareciendo en el perfil de trabajo. [CXM-93671]
- La propiedad de servidor `ios.mdm.apns.connectionPoolSize` se oculta cuando cambia a la API basada en HTTP/2 para APNs. [CXM-95478]
- En XenMobile Server 10.12, no se pueden modificar las propiedades del programa VPP en determinadas aplicaciones. [CXM-96796]
- Las aplicaciones de compras por volumen de Apple instaladas en dispositivos se actualizan automáticamente a la versión más reciente cuando el parámetro **Actualización automática de aplicaciones** está inhabilitado. [CXM-96855]
- En la versión 10.13 de XenMobile Server, al configurar el servidor proxy desde la **interfaz de la línea de comandos**, no puede enviar notificaciones al Secure Hub activo en dispositivos iOS. [CXM-97609]
- En la versión 10.13 de XenMobile Server, aparece un error al acceder a **Detalles del dispositivo**. Este error se produce cuando la propiedad de dispositivo tiene un valor en **”“**. [CXM-97952]
- Para ver los problemas resueltos en la versión de los parches graduales de la versión 10.13.0, consulte:
  - Parche gradual 4 de XenMobile Server 10.13.0
  - Parche gradual 3 de XenMobile Server 10.13.0
  - Parche gradual 2 de XenMobile Server 10.13.0

Información relacionada

- Support Knowledge Center de XenMobile

Actualizaciones sobre compatibilidad de plataforma

Problemas conocidos

January 4, 2022

A continuación, se describe un problema conocido de XenMobile 10.14.

- Después de importar la imagen de XenMobile Server 10.8 o 10.9 en VMware ESXi 6.7 o 6.5 Update 2 y reiniciar la VM, la aplicación de configuración no se inicia, XenMobile Server entra en modo de recuperación y se borran las configuraciones de IP. Para solucionar este problema, cree una máquina virtual con una NIC de VMXNET3 y únala a la base de datos de aquella máquina virtual que entró en el modo de recuperación. [CXM-54581]
- Después de inscribir un dispositivo con iOS 15 o macOS 12, el perfil de configuración de MDM aparece como “No verificado”. [CXM-98525]
- Después de actualizar el sistema operativo a Android 12, los dispositivos reinscritos en el modo de perfil de trabajo aparecen dos veces en la tabla de administración de dispositivos. [CXM-99712]
- Después de enviar un comando de localización geográfica a un dispositivo inscrito en MDM con Android 12, los usuarios ven una pantalla blanca que se carga infinitamente al iniciar Secure Hub. [CXM-99878]-
- Para ver los problemas conocidos relacionados con las aplicaciones móviles de productividad, consulte Secure Hub, Secure Mail y Secure Web.
- Para ver los problemas conocidos en la versión más reciente de los parches graduales de la versión 10.13.0, consulte:
  - Notas de versión del parche gradual 4 de XenMobile Server 10.13

Información relacionada

- Support Knowledge Center de XenMobile

Arquitectura

January 4, 2022

Los requisitos de administración de dispositivos o de aplicaciones que tenga la organización son los que determinan los componentes de XenMobile que incluirá su arquitectura de XenMobile. Los

componentes de XenMobile son módulos y se construyen unos sobre otros. Por ejemplo, su implementación incluye Citrix Gateway:

- Citrix Gateway proporciona a los usuarios acceso remoto a las aplicaciones móviles y realiza un seguimiento de los tipos de dispositivos de los usuarios.
- XenMobile es el lugar donde se administran esas aplicaciones y dispositivos.

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 Citrix Gateway. Esa conexión proporciona acceso a aplicaciones y escritorios de la red interna.
- Inscripción de dispositivos. Los usuarios pueden inscribir dispositivos móviles en XenMobile para que estos se puedan administrar en la consola de XenMobile que se conecta a los recursos de red.
- Aplicaciones móviles, web, SaaS. Los usuarios pueden acceder a sus aplicaciones web, SaaS y móviles desde XenMobile mediante Secure Hub.
- Escritorios virtuales y aplicaciones Windows. Los usuarios pueden conectarse mediante Citrix Receiver o un explorador web para acceder a escritorios virtuales y aplicaciones de Windows desde StoreFront o desde la Interfaz Web.

Para conseguir estas funciones en una instancia local de XenMobile Server, Citrix recomienda implementar los componentes de XenMobile en el siguiente orden:

- Citrix Gateway. Puede configurar parámetros en Citrix 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 Citrix 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 móviles. Las aplicaciones móviles pueden incluir aplicaciones procedentes del App Store o de Google Play. Los usuarios también pueden conectarse a aplicaciones móviles empaquetadas con MDX Toolkit y cargadas en la consola.
- SDK de MAM o MDX Toolkit. La tecnología de empaquetado MDX está programada para alcanzar el final de su vida útil (EOL) en marzo de 2022. Para seguir administrando sus aplicaciones empresariales, debe incorporar el SDK de MAM.

  El SDK de administración de aplicaciones móviles (MAM) proporciona funcionalidad MDX que no cubren las plataformas iOS y Android. Puede habilitar MDX y proteger las aplicaciones iOS o Android. Puede hacer que esas aplicaciones estén disponibles en un almacén interno o en tiendas públicas de aplicaciones. Consulte SDK de aplicaciones MDX.

- StoreFront (opcional). Puede proporcionar acceso a aplicaciones y escritorios virtuales de Windows desde StoreFront a través de conexiones con Receiver.
- Citrix Files (opcional). Si implementa Citrix Files, 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 sobre la configuración de proveedores de identidades para Citrix Content Collaboration, consulte el sitio de asistencia de Content Collaboration.

XenMobile ofrece la administración de dispositivos y la administración de aplicaciones desde la consola de XenMobile. En esta sección se describe la arquitectura de referencia para la implementación de XenMobile.

En un entorno de producción, Citrix recomienda implementar la solución XenMobile en una configuración de clúster. Con ello, se obtiene escalabilidad y redundancia de servidores. Además, utilizar la funcionalidad de la descarga de SSL de Citrix ADC puede reducir más la carga de XenMobile Server y aumentar el rendimiento. Para obtener más información sobre cómo instalar una agrupación en clústeres en XenMobile configurando dos direcciones IP virtuales de equilibrio de carga en Citrix ADC, consulte Agrupar en clústeres.

Para obtener más información sobre cómo configurar XenMobile para una implementación de recuperación ante desastres, consulte el artículo Recuperación ante desastres del manual de implementación. Ese artículo contiene un diagrama de las arquitecturas.

En las siguientes secciones, se describen las diferentes arquitecturas de referencia para la implementación de XenMobile. Para ver diagramas de referencia de las arquitecturas, consulte los artículos Arquitectura de referencia para implementaciones locales y Arquitectura del manual de implementación de XenMobile. Para obtener una lista completa de los puertos, consulte Requisitos de puertos (local) y Requisitos de puertos (en la nube).

Modo de administración de dispositivos móviles (MDM)

> **Importante:**
>
> Si configura el modo MDM y después cambia al modo ENT, debe utilizar la misma autenticación (Active Directory). XenMobile no admite cambiar el modo de autenticación después de haber inscrito a los usuarios. Para obtener más información, consulte Actualizar desde XenMobile MDM Edition a Enterprise Edition.

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

- Implementar aplicaciones y directivas de dispositivo.

- Obtener inventarios de activos.
- Llevar a cabo acciones en los dispositivos, como borrados.

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

Modo de administración de aplicaciones móviles (MAM)

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

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

En este modo, los dispositivos no se pueden inscribir en MDM.

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

Modo MDM+MAM

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

- Administrar dispositivos de empresa a través de MDM
- Implementar aplicaciones y directivas de dispositivo
- Obtener un inventario de activos
- Borrar dispositivos
- Entregar aplicaciones móviles de empresa
- Bloquear aplicaciones y borrar los datos en los dispositivos

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

XenMobile en la red interna: Otra opción de implementación consiste en colocar un servidor de XenMobile Server local en la red interna, en lugar de la zona DMZ. Esta implementación se usa cuando

las directivas de seguridad impiden colocar otros dispositivos, que no sean dispositivos de red, en la zona DMZ. En esta implementación, XenMobile Server no está en la zona DMZ. Por lo tanto, no es necesario abrir puertos en el firewall interno para permitir el acceso a los servidores SQL Server y PKI desde la zona DMZ.

Requisitos del sistema y compatibilidad

January 4, 2022

> **Nota:**
>
> En este artículo, se indican los requisitos del sistema y la compatibilidad con XenMobile Server 10.14. Para conocer los requisitos del sistema para Endpoint Management, consulte Requisitos del sistema.

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

- Compatibilidad de XenMobile
- Sistemas operativos compatibles
- Requisitos de puertos
- Escalabilidad
- Licencias
- Cumplimiento del estándar FIPS 140-2
- Idiomas disponibles

Para ejecutar XenMobile 10.14, debe cumplir los siguientes requisitos mínimos:

- Alguno de los siguientes:
  - Citrix Hypervisor 8.1 u 8.0 o Citrix XenServer (versiones compatibles: 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2); para obtener información detallada, consulte XenServer.
  - VMware (versiones compatibles: ESXi 6.0, ESXi 6.5.0 Update 3 o ESXi 6.7 Update 2 patch 10, ESXi 7.0 Update 2a); para obtener información detallada, consulte Solución temporal de ESXi 6.7 y VMware.
  - Hyper-V (versiones compatibles: Windows Server 2016 y Windows Server 2019). Para obtener información detallada, consulte Hyper-V.
- Conector de Endpoint Management para Exchange ActiveSync 10.1.10 o conector de Citrix Gateway para Exchange ActiveSync 8.5.3.19
- Procesador de doble núcleo
- Cuatro unidades CPU virtuales

- 8 GB de RAM para entornos de producción; 4 GB de RAM para pruebas de concepto y entornos de prueba
- 50 GB de espacio en disco
- Citrix License Server 11.16.

  Actualice el servidor de licencias antes de actualizar XenMobile Server.

Solución temporal de ESXi 6.7

Para que ESXi 6.7 funcione, debe utilizar la siguiente solución temporal.

1. Con la herramienta OVF suministrada por VMware, extraiga el archivo OVA descargado de citrix.com. Puede obtener la herramienta OVF de la página de VMware (https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491).
2. De los tres archivos extraídos, cargue el archivo VMDK en su almacén de datos.
3. Cree una máquina virtual.
   a) Dé un nombre a la máquina virtual y seleccione **ESX/ESXi 4.x virtual machine** como opción de compatibilidad.
   b) Para la familia de sistema operativo invitado, seleccione **Linux**.
   c) Para la versión del SO invitado, seleccione **Other 2.6.x Linux (64-bit)**.
   d) Para el almacén de datos, seleccione **Default**.
   e) Durante la personalización, quite el disco duro, el controlador USB y la unidad de CD o DVD predeterminados.
   f) En “Network”, como tipo de adaptador, seleccione **VMXNET3**.
   g) En ESXi, si los discos son locales, seleccione **SCSI Controller** y **LSI Logic Parallel**. Si está utilizando un disco compartido, seleccione **VMware Paravirtual**.
   h) Haga clic en “Next” para finalizar la creación de VM.
4. Vaya al almacén de datos y copie el archivo VMDK que cargó anteriormente. Cópielo en el directorio de la VM que creó para XenMobile.
5. Desde la interfaz Web de ESXi, seleccione la máquina virtual y modifique la configuración.
6. Haga clic en **Add Hard disk**.
7. Seleccione el archivo VMDK copiado anteriormente y adjúntelo a la máquina virtual.
8. Haga clic en **Guardar**.
9. Encienda la máquina virtual.

Requisitos de sistema de Citrix Gateway

Para ejecutar Citrix Gateway con XenMobile 10.14, debe cumplir los siguientes requisitos mínimos.

- Citrix Gateway (local). Versiones compatibles: 12.1 o superior

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

Requisitos de base de datos para XenMobile 10.14

XenMobile requiere una de las siguientes bases de datos:

- Microsoft SQL Server

  XenMobile admite una base de datos de Microsoft SQL Server que se ejecute en una de las siguientes versiones compatibles. Para obtener más información acerca de las bases de datos de Microsoft SQL Server y sus requisitos de hardware, consulte la documentación de Microsoft.

  - Microsoft SQL Server 2014 SP3
  - Microsoft SQL Server 2016 SP2
  - Microsoft SQL Server 2017 CU 25
  - Microsoft SQL Server 2019 CU 12

  Los requisitos de la base de datos de Microsoft SQL Server también dependen del tamaño de la implementación. Para obtener más información acerca de los requisitos de base de datos de Microsoft SQL Server para la implementación, consulte Escalabilidad.

  XenMobile admite los grupos de disponibilidad de SQL Basic (grupos de disponibilidad AlwaysOn) y los clústeres de SQL para una alta disponibilidad de base de datos.

  Citrix recomienda usar Microsoft SQL de forma remota.

  Para obtener información sobre la actualización de versiones de Microsoft SQL, consulte el artículo Actualizar SQL Server de Microsoft.

- PostgreSQL (para entornos de prueba únicamente) PostgreSQL se incluye con XenMobile. Puede usarlo de forma local o remota en entornos de prueba. No se admite 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.

  Todas las ediciones de XenMobile admiten Remote PostgreSQL 9.5.1 y 9.5.11 para Windows, con las siguientes limitaciones: No se recomienda para entornos de producción. Se admite un máximo de 300 dispositivos Utilice instalaciones de SQL Server locales si tiene más de 300 dispositivos. No se admite la agrupación en clústeres.

Requisitos de cuenta de servicio de SQL Server

Compruebe que la cuenta de servicio de SQL Server que se va a usar en XenMobile tiene el permiso del rol `DBcreator`. Debe recordar la contraseña de la cuenta del servidor SQL que especifique durante la instalación de XenMobile Server. Esa contraseña será necesaria para clonar la base de datos de XenMobile durante la recuperación de XenMobile Server.

Proteja sus bases de datos de SQL Server mediante cifrado transparente de datos (TDE). No permita el acceso externo a los puertos de SQL Server, como se muestra en la arquitectura de referencia en Arquitectura de referencia para implementaciones locales.

Para obtener más información acerca de las cuentas de servicio de SQL Server, consulte las siguientes páginas del sitio de documentación de Microsoft. Estos enlaces hacen referencia a la información de SQL Server 2014. Si usa otra versión de servidor, selecciónela en la lista **Otras versiones**:

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

Compatibilidad con Virtual Apps and Desktops

- Virtual Apps and Desktops 7.15 LTSR CU3
- Virtual Apps and Desktops 7.1811
- Virtual Apps and Desktops 7 1906
- Virtual Apps and Desktops 7 1909
- Virtual Apps and Desktops 7 2006

Compatibilidad de StoreFront

- StoreFront 3.12.2
- StoreFront 7 1811
- StoreFront 7 1906
- StoreFront 7 1909
- StoreFront 7 2006

Compatibilidad con otros elementos

- Conector de Endpoint Management para Exchange ActiveSync 10.1.10
  - No se han probado versiones anteriores
- Conector de Citrix Gateway para Exchange ActiveSync 8.5.3.19
  - No se han probado versiones anteriores

Compatibilidad de XenMobile

January 4, 2022

> **Nota:**
>
> En este artículo, se indica la compatibilidad con XenMobile Server. Para conocer los componentes probados con Endpoint Management, consulte Compatibilidad con Endpoint Management.

Para utilizar las nuevas funciones, soluciones y actualizaciones de directivas, Citrix recomienda instalar la versión más reciente de:

- Citrix recomienda integrar el SDK de administración de aplicaciones móviles (MAM) con las aplicaciones de empresa para iOS y Android a fin de proporcionar funcionalidades MDX a dichas aplicaciones.

  MDX Toolkit está programado para alcanzar el final de su vida útil (EOL) en marzo de 2022. Para seguir administrando sus aplicaciones empresariales, debe incorporar el SDK de MAM.

En este artículo, se resumen las versiones de los componentes de XenMobile compatibles que se pueden integrar.

Rutas de compatibilidad y de actualización de versiones

Las versiones más recientes de Secure Hub, MDX Toolkit y las aplicaciones móviles de productividad son compatibles con la versión actual y la versión anterior de XenMobile Server.

La versión más reciente de las aplicaciones de productividad móvil requiere la versión más reciente de Secure Hub. Las dos versiones anteriores de las aplicaciones son compatibles con la versión más reciente de Secure Hub. Para obtener más información, consulte la tabla de productos de Citrix.

Citrix admite la distribución de aplicaciones de productividad de XenMobile solo desde una tienda pública de aplicaciones.

XenMobile Server (instalación local)

- Citrix admite actualizaciones desde las dos últimas versiones de XenMobile Server.
- Versión más reciente de XenMobile Server: XenMobile Server 10.14
- Actualizar versión desde:
  - XenMobile Server 10.13.x
  - XenMobile Server 10.12.x

Aplicaciones móviles de productividad

Los usuarios acceden a las aplicaciones móviles de productividad desde las tiendas públicas de aplicaciones. La versión más reciente de las aplicaciones de productividad móvil requiere la versión más

reciente de Secure Hub. Las dos versiones anteriores de las aplicaciones son compatibles con la versión más reciente de Secure Hub.

Para obtener más información acerca del ritmo de publicación por fases cada dos semanas previsto para las aplicaciones móviles de productividad, consulte Calendario de versiones. Para obtener información de asistencia, consulte Compatibilidad con aplicaciones móviles de productividad.

SDK de MAM

El SDK de MAM proporciona funcionalidad MDX que no cubren las plataformas iOS y Android. Puede hacer que esas aplicaciones estén disponibles en un almacén interno o en tiendas públicas de aplicaciones. Consulte SDK de aplicaciones MDX.

MDX Toolkit

La tecnología de empaquetado MDX está programada para alcanzar el final de su vida útil (EOL) en septiembre de 2021. Para seguir administrando sus aplicaciones empresariales, debe incorporar el SDK de MAM.

Citrix admite las tres versiones más recientes (n.n.n) de MDX Toolkit. Consulte Novedades en MDX Toolkit.

Compatibilidad con exploradores web

La consola de XenMobile Server requiere uno de los siguientes exploradores web compatibles:

- La versión más reciente de Google Chrome
- La versión más reciente de Mozilla Firefox
- La versión más reciente de Microsoft Edge
- La versión más reciente de Apple Safari

Sistemas operativos compatibles

January 4, 2022

> **Nota:**
>
> En este artículo, se indican los sistemas operativos compatibles con XenMobile Server 10.13. Para conocer los sistemas operativos de dispositivo admitidos en Endpoint Management, consulte Sistemas operativos admitidos.

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

La información sobre plataformas compatibles de este artículo también se aplica al conector de XenMobile para Exchange ActiveSync y al conector de Citrix Gateway para Exchange ActiveSync.

Para obtener las versiones más recientes de las aplicaciones móviles de productividad, así como los dispositivos compatibles para el cifrado MDX, consulte Aplicaciones móviles de productividad admitidas.

> **Nota:**
>
> Citrix es compatible, como mínimo, con la versión actual y la anterior de todas las plataformas de los sistemas operativos principales. No todas las funciones de la versión más reciente de Endpoint Management funcionan en versiones más antiguas de las plataformas.
>
> Para ver los anuncios de elementos retirados, consulte Elementos retirados.

Lista de compatibilidad de sistemas operativos

Citrix XenMobile admite los siguientes sistemas operativos:

> **Nota:**
>
> En abril de 2021, dejaron de admitirse las versiones de Android 7.x y iOS 12.x de Secure Hub, Secure Mail, Secure Web y la aplicación Citrix Workspace.

- **Android:** 8.x, 9.x, 10.x, 11.x, 12.x

  A partir de Android 10, consulte Consideraciones sobre Android.

- **iOS:** 13.x, 14.x, 15.x

  Las aplicaciones móviles de XenMobile y Citrix son compatibles con iOS 14.x, pero no son compatibles actualmente con todas las nuevas funcionalidades de iOS 14.x. Para empaquetar aplicaciones de empresa internas para iOS 14.x, use MDX Toolkit 21.8.5 o una versión posterior o prepare las aplicaciones con el SDK de MAM.

- **iPadOS:** 13.x, 14.x, 15.x

  Las aplicaciones móviles de XenMobile y Citrix son compatibles con iPadOS 14.x, pero no son compatibles actualmente con todas las nuevas funcionalidades de iPadOS 14.x.

- **macOS:** 10.13x, 10.14x, 10.15x, 11.x

  Las aplicaciones móviles de XenMobile y Citrix son compatibles con macOS 11, pero no son compatibles actualmente con todas las nuevas funcionalidades de macOS 11.

- **Escritorios y tabletas Windows:** (Solo para MDM) Windows 10 y Windows 11
- **Windows Phone:** (solo MDM). Windows Phone 8.1, Windows Phone 10, Windows 10 RS4 y RS5
- **Windows Mobile/CE:** (solo MDM) A partir del segundo trimestre de 2018, ya no se admiten dispositivos Windows Mobile/CE.
- **Samsung SAFE y Samsung Knox:** En dispositivos Samsung compatibles, XenMobile admite y extiende directivas de Samsung for Enterprise (SAFE) y Samsung Knox. XenMobile requiere que se habiliten las API de SAFE antes de implementar directivas de SAFE y directivas de restricciones. Para ello, implemente la clave integrada de Samsung Enterprise License Management (ELM) en un dispositivo. Consulte Directiva de clave de licencia MDM de Samsung.

Consideraciones sobre Android

Antes de actualizar el sistema operativo a Android 10 o a una versión posterior: Consulte Migrar de la administración de dispositivos a Android Enterprise para obtener información sobre cómo afecta la retirada de las API de administración de dispositivos de Google a los dispositivos con Android 10.

- Citrix recomienda evitar la inscripción de dispositivos Android 10 en el modo de administración de dispositivos antiguos. Google está retirando las API de administración de dispositivos, lo que afecta a los dispositivos con Android 10 o una versión posterior. Una vez retiradas las API, la inscripción de dispositivos Android 10+ en el modo de administración de dispositivos antiguos fallará. Citrix no admite la inscripción de dispositivos Android 11 en el modo de administración de dispositivos.
- Citrix recomienda usar Android Enterprise para dispositivos Android 10. Para obtener más información, consulte Migrar de la administración de dispositivos a Android Enterprise.
- El cambio en las API de Google no afecta a los dispositivos inscritos en el modo solo MAM.

Antes de actualizar:

- Compruebe que la infraestructura de su servidor cumple los requisitos de los certificados de seguridad que tienen un nombre de host coincidente en la extensión subjectAltName (SAN).
- Para verificar un nombre de host, el servidor debe presentar un certificado con un SAN correspondiente. Citrix confía en los certificados solamente si contienen un nombre SAN que coincida con el nombre del host.

Requisitos de puertos

January 4, 2022

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

Abrir puertos para que Citrix Gateway y XenMobile administren aplicaciones

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

- XenMobile
- StoreFront
- Citrix Virtual Apps and Desktops
- Conector de Citrix Gateway para Exchange ActiveSync
- Otros recursos de red interna, como los sitios web de intranet

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

Para obtener más información sobre Citrix Gateway, consulte la documentación de Citrix Gateway. Esa documentación contiene información sobre las direcciones IP de Citrix ADC (NSIP), las direcciones IP virtuales (VIP) y las direcciones IP de subred (SNIP).

Puerto TCP	Descripción	Origen	Destino
21 o 22	Se usa para enviar paquetes de asistencia a un servidor FTP o SCP.	XenMobile	Servidor SCP o FTP
53 (TCP y UDP)	Se utiliza para las conexiones DNS.	Citrix Gateway, XenMobile	Servidor DNS
80	Citrix Gateway transfiere la conexión VPN al recurso de la red interna a través del segundo firewall. Por regla general, esta situación ocurre si los usuarios inician sesión con Citrix Gateway Plug-in.	Citrix Gateway	Sitios web de la intranet

Puerto TCP	Descripción	Origen	Destino
80 u 8080, 443	El puerto XML y Secure Ticket Authority (STA) se usa para la enumeración, la generación de tíquets y la autenticación. Citrix recomienda el uso del puerto 443.	Tráfico de red XML de StoreFront y la Interfaz Web; Citrix Gateway STA	Virtual Apps o Virtual Desktops
123 (TCP y UDP)	Se usa para los servicios del protocolo de tiempo de red (NTP).	Citrix Gateway; XenMobile	Servidor NTP
389	Se usa para conexiones de protocolo LDAP no seguras.	Citrix 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 Virtual Apps and Desktops.	Internet	Citrix Gateway
443	Se utiliza para las conexiones a XenMobile con el objetivo de entregar aplicaciones web, aplicaciones para móvil y aplicaciones SaaS.	Internet	Citrix Gateway

Puerto TCP	Descripción	Origen	Destino
443	Se utiliza para la comunicación general del dispositivo con XenMobile Server.	XenMobile	XenMobile
443	Se usa para las conexiones desde dispositivos móviles hacia XenMobile para la inscripción.	Internet	XenMobile
443	Se usa para las conexiones desde XenMobile al conector de Citrix Gateway para Exchange ActiveSync.	XenMobile	Conector de Citrix Gateway para Exchange ActiveSync
443	Se usa para las conexiones desde el conector de Citrix Gateway para Exchange ActiveSync a XenMobile.	Conector de Citrix Gateway para Exchange ActiveSync	XenMobile
443	Se usa para la URL de respuesta en implementaciones sin la autenticación de certificado.	XenMobile	Citrix 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.	Citrix Gateway; XenMobile	Servidor de autenticación LDAP o Active Directory

Puerto TCP	Descripción	Origen	Destino
1494	Se usa para las conexiones ICA a aplicaciones Windows en la red interna. Citrix recomienda mantener este puerto abierto.	Citrix Gateway	Virtual Apps o Virtual Desktops
1812	Se utiliza para las conexiones RADIUS.	Citrix 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.	Citrix Gateway	Virtual Apps o Virtual Desktops
3268	Se usa para conexiones LDAP no seguras del catálogo global de Microsoft.	Citrix Gateway; XenMobile	Servidor de autenticación LDAP o Active Directory
3269	Se usa para conexiones seguras LDAP del catálogo global de Microsoft.	Citrix Gateway; XenMobile	Servidor de autenticación LDAP o Active Directory
9080	Se usa para el tráfico HTTP entre Citrix ADC y el conector de Citrix Gateway para Exchange ActiveSync.	Citrix ADC	Conector de Citrix Gateway para Exchange ActiveSync

Puerto TCP	Descripción	Origen	Destino
30001	Una API de administración para la organización inicial del servicio HTTPS	LAN interna	XenMobile Server
9443	Se usa para el tráfico HTTPS entre Citrix ADC y el conector de Citrix Gateway para Exchange ActiveSync.	Citrix ADC	Conector de Citrix Gateway para Exchange ActiveSync
45000; 80	Se utiliza para la comunicación entre dos máquinas virtuales de XenMobile cuando se implementan en un clúster. El puerto 80 es para la comunicación entre los nodos y para la descarga de SSL.	XenMobile	XenMobile
8443	Se utiliza para la inscripción, XenMobile Store y la administración de aplicaciones móviles (MAM).	XenMobile; Citrix Gateway; Dispositivos; Internet	XenMobile

Puerto TCP	Descripción	Origen	Destino
4443	Se utiliza para que un administrador acceda a la consola de XenMobile a través del explorador. También se utiliza para la descarga de registros y paquetes de asistencia de todos los nodos en clúster de XenMobile desde un nodo.	Punto de acceso (explorador web); 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
161	Se usa para el tráfico SNMP mediante el protocolo UDP.	SNMP Manager	XenMobile
162	Se usa para enviar las alertas de captura SNMP al SNMP Manager desde XenMobile. El origen es XenMobile y el destino es el SNMP Manager.	XenMobile	SNMP Manager

Abrir puertos de XenMobile para administrar dispositivos

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

Puerto TCP	Descripción	Origen	Destino
25	El puerto SMTP predeterminado para el servicio de notificaciones de XenMobile. Si el servidor SMTP utiliza otro puerto, compruebe que el firewall no bloquea ese puerto.	XenMobile	Servidor SMTP
80 y 443	Conexión de la tienda de aplicaciones empresariales al iTunes Store de Apple, a Google Play (se debe usar el puerto 80) o a la Tienda Windows Phone. Se utiliza para las compras por volumen de Apple. Se utiliza para publicar aplicaciones de las tiendas de aplicaciones de iOS, Secure Hub para Android o Secure Hub para Windows Phone.	XenMobile	`ax.apps.apple.com` y `*.mzstatic.com`; `vpp.itunes.apple.com`; `login.live.com`; `*.notify.windows.com`; `play.google.com`, `android.clients.google.com`, `android.l.google.com`
80 o 443	Se utiliza para las conexiones salientes entre XenMobile y la retransmisión de notificaciones SMS de Nexmo.	XenMobile	Servidor de retransmisión de SMS de Nexmo

Puerto TCP	Descripción	Origen	Destino
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
443	Se utiliza para la inscripción y la instalación de agentes en el caso de dispositivos Android y Windows y el cliente Remote Support para la administración MDM.	Wi-Fi y LAN	XenMobile
1433	Se utiliza para las conexiones a un servidor remoto de bases de datos (optativo).	XenMobile	Servidor SQL
443 o 2197	Se utiliza para enviar notificaciones del servicio de notificaciones push de Apple (APNs) a `*.push.apple.com`	XenMobile	Internet (hosts APNs con la dirección IP pública 17.0.0.0/8)
5223	Se usa para las conexiones salientes de APNs desde dispositivos iOS a `*.push.apple.com`.	Dispositivos iOS	Internet (hosts APNs con la dirección IP pública 17.0.0.0/8)

Puerto TCP	Descripción	Origen	Destino
8081	Se utiliza para los túneles de aplicaciones desde el cliente optativo Remote Support Client para MDM. El valor predeterminado es 8081.	Cliente Remote Support	XenMobile
8443	Utilizado para la inscripción de dispositivos iOS y Windows Phone.	Internet; LAN y Wi-Fi	XenMobile

Requisito de puerto para la conectividad con AutoDiscovery Service

Esta configuración de puerto garantiza que los dispositivos Android que se conectan desde Secure Hub para Android puedan acceder al servicio de detección automática de Citrix ADS (AutoDiscovery Service) desde dentro de la red interna. Necesita acceso a ADS para descargar las actualizaciones de seguridad disponibles a través de ADS.

> **Nota:**
>
> Puede que las conexiones ADS no admitan su servidor proxy. En este caso, permita que la conexión ADS circunvale el servidor proxy.

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

- **Obtener certificados de XenMobile Server y Citrix ADC.** 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.

La fijación de certificados requiere que los dispositivos se conecten al servicio ADS antes de que el dispositivo se inscriba. Ese requisito garantiza que Secure Hub disponga de la información de seguridad más actualizada. Para que Secure Hub inscriba un dispositivo, éste debe contactar con el servicio ADS. Por lo tanto, la apertura del acceso al servicio ADS dentro de la red interna es vital para permitir la inscripción de dispositivos.

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

FQDN	IP address	Port	Uso de IP y puerto
ads.xm.cloud.com	34.194.83.188	443	Secure Hub - Comunicación ADS
ads.xm.cloud.com	34.193.202.23	443	Secure Hub - Comunicación ADS

> **Nota:**
>
> Para versiones de Secure Hub anteriores a 10.6.15, el FQDN es discovery.mdm.zenprise.com . Abra el puerto 443 para las direcciones IP 52.5.138.94 y 52.1.30.122.

Requisitos de red de Android Enterprise

Para obtener información sobre las conexiones salientes que se deben tener en cuenta al configurar entornos de red para Android Enterprise, consulte el artículo Android Enterprise Network Requirements de la asistencia técnica de Google.

Requisitos de puertos para XenMobile

Estos hosts de destino deben ser accesibles desde la red para crear un Google Play Enterprise administrado y acceder al Google Play iFrame administrado. Google ha puesto el iFrame Managed Play a disposición de los desarrolladores de EMM para simplificar la búsqueda y la aprobación de aplicaciones. Para usar el iFrame Managed Play, el explorador web desde el que se accede a la consola de XenMobile debe tener acceso a Google Play.

Host de destino	**Port**	**Descripción**
play.google.com	TCP/443	Se utiliza para el registro en Google Play Store y Play Enterprise
*.googleapis.com	TCP/443	Se utiliza para la administración de Google Mobile, las API de Google y las API de Google Play Store
accounts.youtube.com, accounts.google.com	TCP/443	Se utiliza para la autenticación de cuentas
apis.google.com	TCP/443	Se utiliza para GCM y otros servicios web de Google

Host de destino	Port	Descripción
ogs.google.com	TCP/443	Se utiliza para elementos de la IU de iFrame
notifications.google.com	TCP/443	Se utiliza para notificaciones móviles y de escritorio
fonts.googleapis.com, *.gstatic.com, *.googleusercontent.com	TCP/443	Se utiliza para el contenido generado por los usuarios de Google Fonts. Por ejemplo, los iconos de la aplicación en el almacén
cri.pki.goog, ocsp.pki.goog	TCP/443	Se utiliza para la validación de certificados

Escalabilidad y rendimiento

January 4, 2022

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.

La escalabilidad se define aquí en términos de la capacidad que tienen los dispositivos ya inscritos en la implementación de 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* se define como la tasa máxima a la que los dispositivos existentes pueden volver a conectarse a la implementación.

Los datos de este artículo se derivan de pruebas realizadas en implementaciones que van desde 10 000 hasta 75 000 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 con Citrix Gateway 8200. Un dispositivo Citrix ADC con igual o mayor capacidad puede producir una escalabilidad y rendimiento similar o superior.

A continuación se presenta un resumen de los resultados de las pruebas de escalabilidad.

Resumen de los resultados de las pruebas de escalabilidad para implementaciones de hasta 75 000 dispositivos

Tasa de inicio de sesión (tasa de reconexión de usuarios existentes): hasta 9 375 dispositivos por hora

Configuración utilizada:

- Citrix Gateway
- MPX 8200
- XenMobile Enterprise Edition
- Clúster de 7 nodos de XenMobile Server
- Base de datos: externa de Microsoft SQL Server

Resultados de las pruebas según cantidad de dispositivos y configuración de hardware

Cantidad de dispositivos	12 500	30 000	60 000	75 000
Tasa de reconexión de dispositivos existentes por hora	1250	3750	7500	9375
Modo de XenMobile Server	Autónomo	Clúster	Clúster	Clúster
Clúster de XenMobile Server	N/D	3	5	7
XenMobile Server: dispositivo virtual	Memoria = 8 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
Active Directory	Memoria = 4 GB de RAM; Unidades vCPU = 2	Memoria = 8 GB de RAM; Unidades vCPU = 4	Memoria = 16 GB de RAM; Unidades vCPU = 4	Memoria = 16 GB de RAM; Unidades vCPU = 4

Cantidad de dispositivos	12 500	30 000	60 000	75 000
Base de datos externa de Microsoft SQL Server	Memoria = 8 GB de RAM; Unidades vCPU = 4	Memoria = 16 GB de RAM; Unidades vCPU = 8	Memoria = 24 GB de RAM; Unidades vCPU = 16	Memoria = 24 GB de RAM; Unidades vCPU = 16

Perfil de escalabilidad

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

Configuración de XenMobile Server	Total	Por usuario
Directivas	20	20
Aplicaciones	270	50
Aplicación pública	200	0
MDX	50	30
Web y 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	

Actividades de aplicaciones y conexiones de dispositivos

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

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

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

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

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

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

Arquitectura de referencia

Para consultar la arquitectura de referencia para las implementaciones de las pruebas de escalabilidad, consulte “Arquitectura principal de referencia para MAM y MDM” en Arquitectura de referencia para implementaciones locales.

Advertencias y limitaciones

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

- No se ha probado la plataforma Windows.
- El envío de directivas se ha probado en dispositivos iOS y Android.
- Cada nodo de XenMobile Server admite un máximo de 12 000 dispositivos de forma simultánea.

Licencias

January 4, 2022

> **Importante:**
>
> El proceso de devolución y modificación de licencias de Citrix ha cambiado a partir del 4 de noviembre de 2020. Para obtener información acerca de los cambios realizados en el portal "Manage Licenses" (Administrar licencias) de Citrix.com y "My Licensing Tools" (Mis herramientas de licencia) en Partner Central, consulte el artículo de Citrix Support https://support.citrix.com/article/CTX285157.

XenMobile usa Citrix Licensing para administrar las licencias. XenMobile Server y Citrix Gateway requieren licencias.

Para obtener información sobre las licencias de Citrix Gateway, consulte la documentación de Citrix Gateway. Para obtener más información acerca de Citrix Licensing, consulte El sistema de licencias de Citrix.

Al adquirir XenMobile Server, 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 Licencias de XenMobile.

Requisitos

- Actualice su Citrix License Server a 11.16.x o versiones posteriores antes de actualizar a la versión más reciente de XenMobile Server. Las versiones anteriores de Citrix Licensing no admiten la versión más reciente 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.
- 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, necesita los archivos de licencia originales.

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

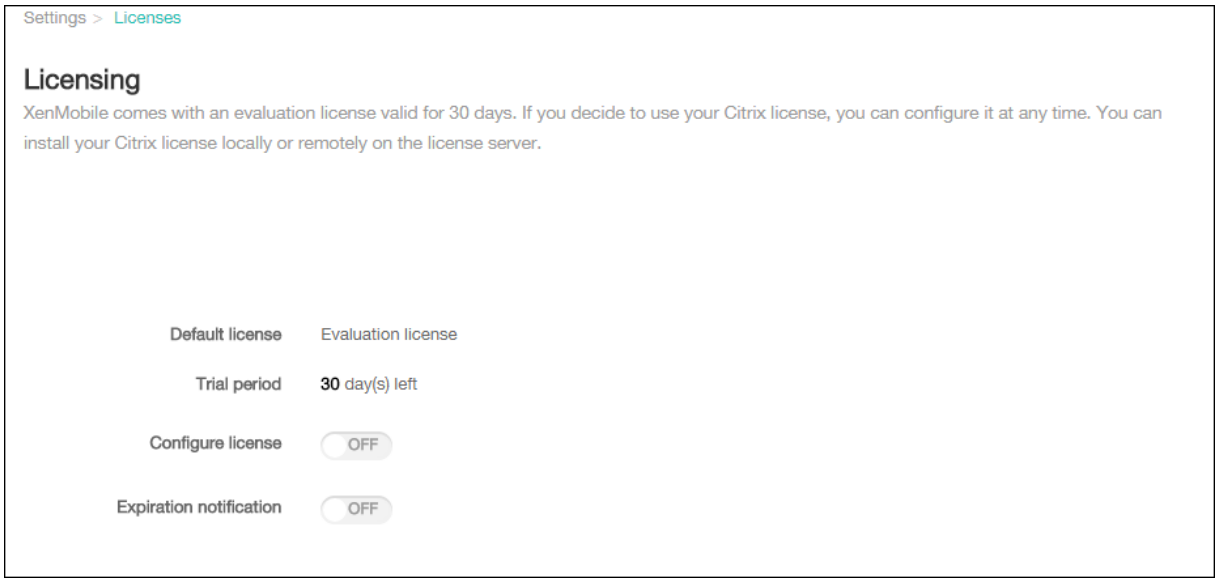
Si no dispone de licencia, XenMobile opera en modo de prueba con todas sus funcionalidades durante un período de gracia de 30 días. Este modo de prueba solo se puede usar una vez, y el período de 30 días comienza a partir de la instalación de XenMobile. El acceso a la consola Web de XenMobile no se bloquea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

Para encontrar la página "Licencias" en la consola de XenMobile

Cuando la página **Licencias** 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.



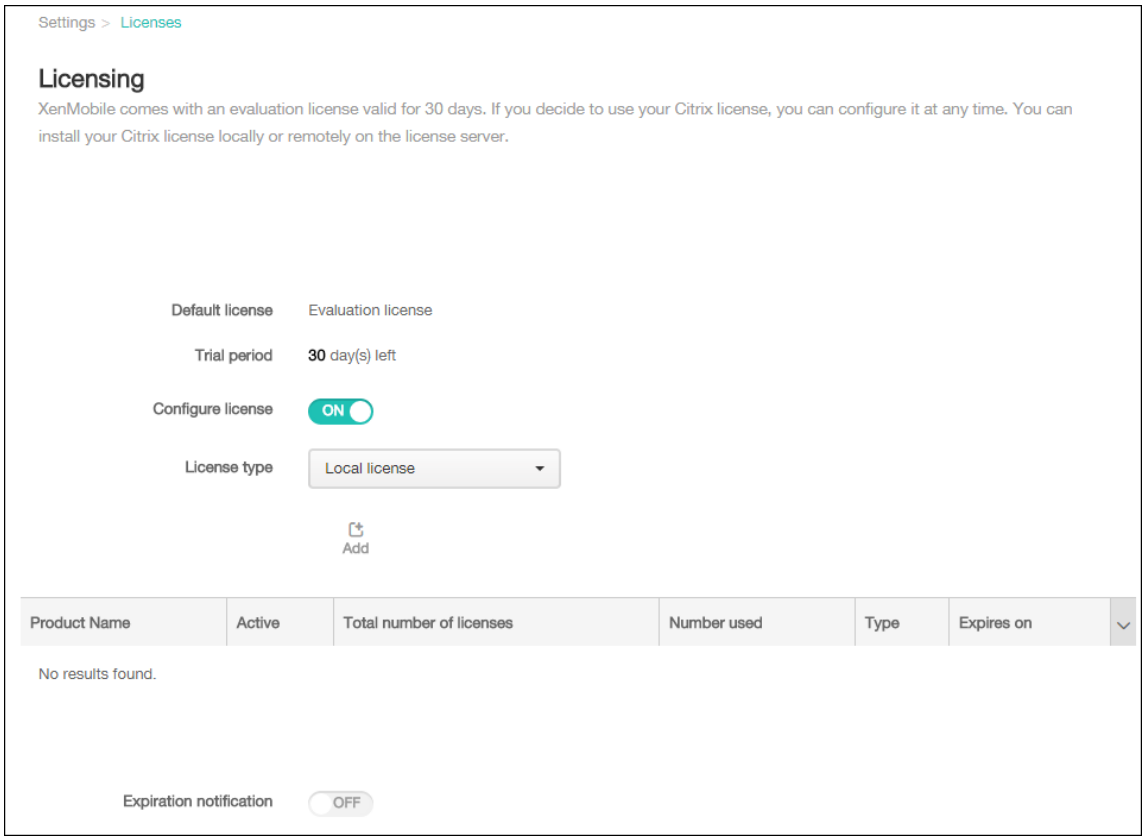
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Haga clic en **Licencias**. Aparecerá la página **Licencias**.

Para agregar una licencia local

Tras agregar nuevas licencias, 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, dichas licencias aparecen en una sola fila de la tabla. En estos casos, **Número total de licencias** y **Número utilizado** reflejan la cantidad total conjunta de licencias comunes. La fecha indicada en **Caduca** muestra la última fecha de caducidad de las licencias comunes.

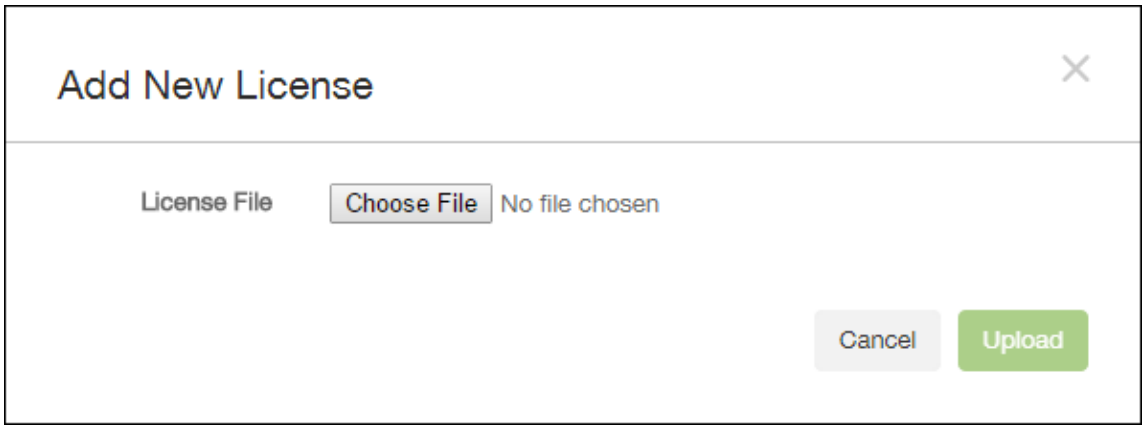
Puede administrar todas las licencias locales a través de la consola de XenMobile.

1. Los archivos de licencias pueden obtenerse del servicio Simple License Service desde la consola License Administration Console o directamente desde su cuenta, en Citrix.com. Para obtener información más detallada, consulte la documentación de Citrix Licensing.
2. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
3. Haga clic en **Licencias**. Aparecerá la página **Licencias**.
4. Establezca **Configurar licencia** en **Sí**. Aparecerán la lista **Tipo de licencia**, el botón **Agregar** y la tabla **Licencias**. La tabla **Licencias** contiene las licencias que ha utilizado con XenMobile. Si aún no ha agregado ninguna licencia de Citrix, la tabla estará vacía.

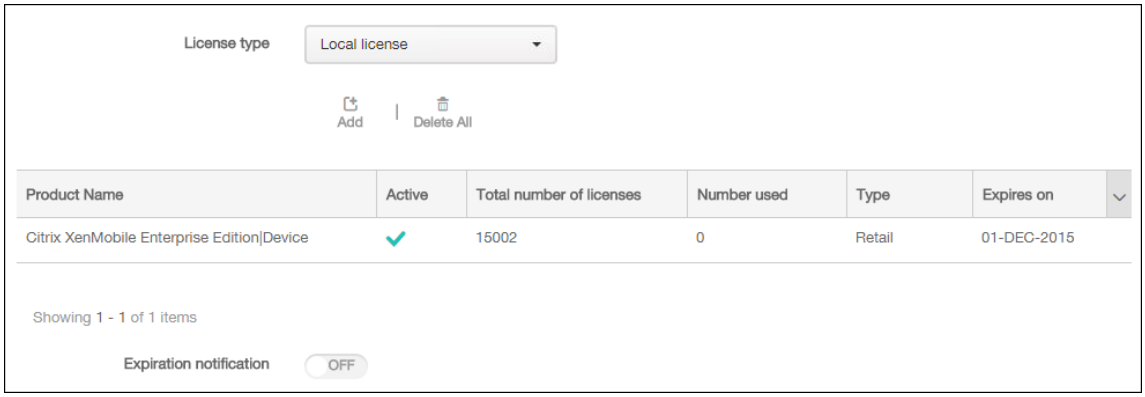


5. Compruebe que **Tipo de licencia** está establecido en **Licencia local**. A continuación, haga clic

en **Agregar**. Aparecerá el cuadro de diálogo **Agregar nueva licencia**.



6. En el cuadro de diálogo **Agregar nueva licencia**, haga clic en **Elegir archivo** y, a continuación, vaya a la ubicación del archivo de su licencia.
7. Haga clic en **Cargar**. La licencia se cargará de forma local y aparecerá en la tabla.



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

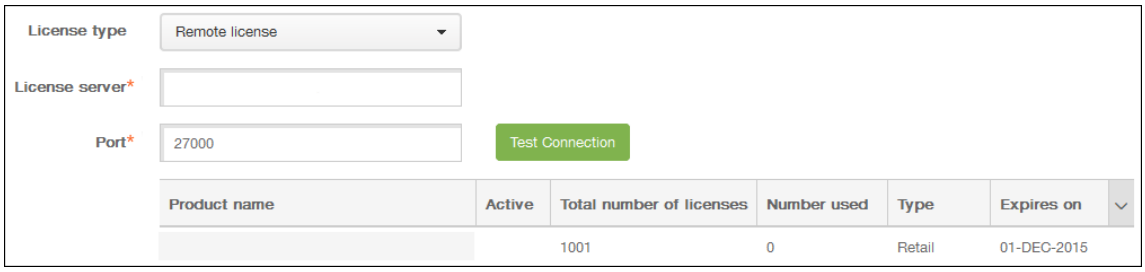
Para agregar una licencia remota

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. Importe el certificado del servidor de licencias en XenMobile Server (**Parámetros > Certificados**).
2. De forma predeterminada, la verificación de nombres de host está habilitada en las conexiones salientes, excepto para el servidor PKI de Microsoft. Si la verificación de nombres de host deja inoperativa la implementación, cambie la propiedad de servidor **disable.hostname.verification** a **true**. El valor predeterminado de esta propiedad es **false**.

Cuando se produce un error en la verificación de nombres de host, el registro del servidor contiene errores del tipo: “No se puede conectar con el servidor de compras por volumen: El nombre de host ‘192.0.2.0’ no coincide con el sujeto de certificado suministrado por el servidor homólogo”

3. En la página **Licencias**, establezca **Configurar licencia** en **Sí**. Aparecerán la lista **Tipo de licencia**, el botón **Agregar** y la tabla **Licencias**. La tabla **Licencias** contiene las licencias que ha utilizado con XenMobile. Si aún no ha agregado ninguna licencia de Citrix, la tabla estará vacía.
4. Establezca **Tipo de licencia** en **Licencia remota**. El botón **Agregar** se reemplaza por los campos **Servidor de licencias** y **Puerto** y el botón **Probar conexión**.

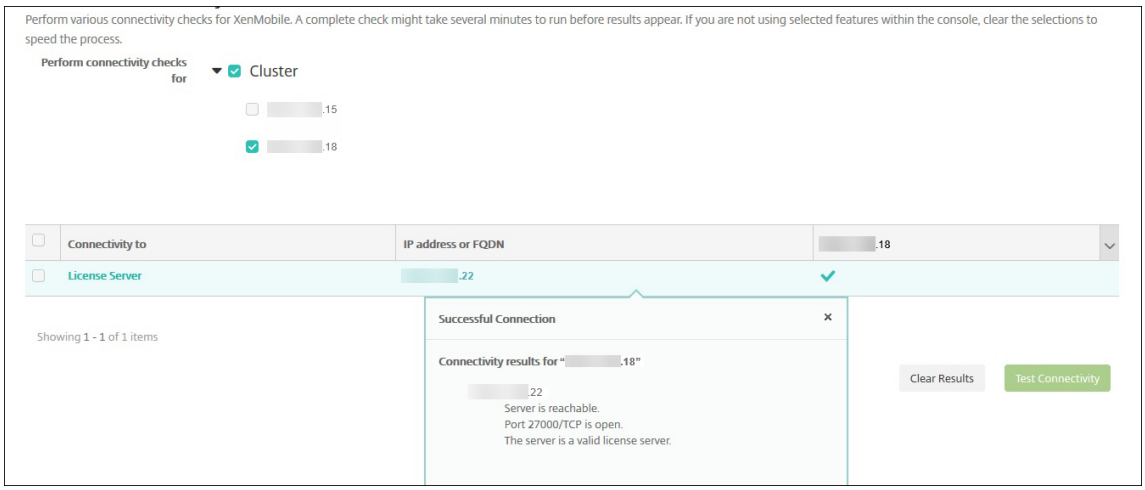


5. Configure estos parámetros:
   - **Servidor de licencias:** Escriba la dirección IP o el nombre de dominio completo (FQDN) del servidor de licencias remoto.
   - **Puerto:** Acepte el puerto predeterminado o escriba el número de puerto utilizado para comunicarse con el servidor de licencias.
6. Haga clic en **Probar conexión**. Si la conexión es satisfactoria, XenMobile se conecta al servidor de licencias, y la tabla “Licencias” se rellena con las licencias disponibles. Si solo hay una licencia, esta se activa automáticamente.

   Cuando haga clic en **Probar conexión**, XenMobile confirmará lo siguiente:

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

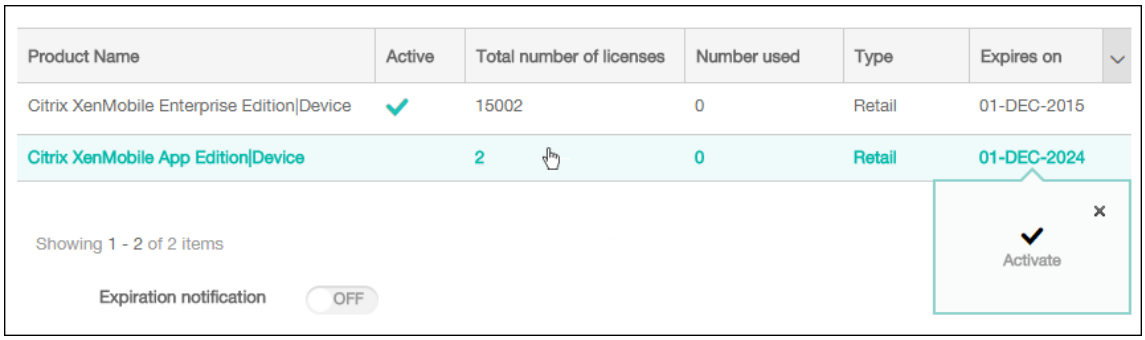
   Si la conexión no se consigue establecer, lea con atención el mensaje de error que aparece, haga las correcciones necesarias y haga clic en **Probar conexión**.



Para activar otra licencia

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

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



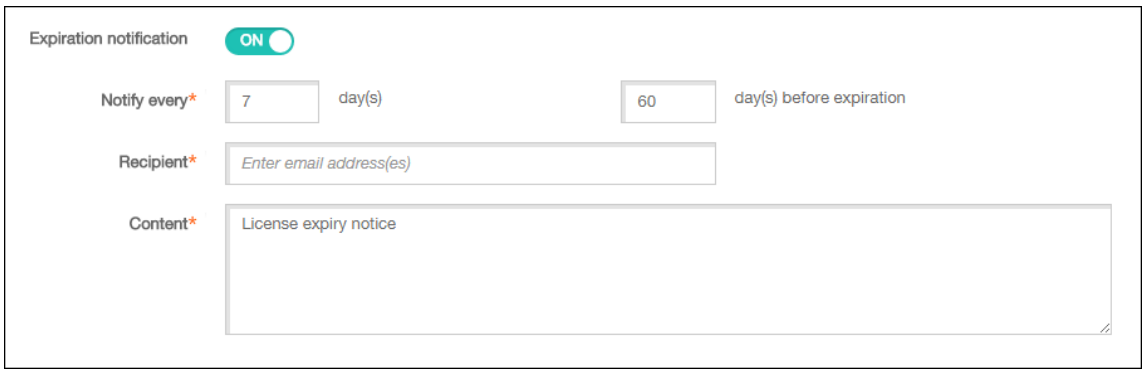
2. Haga clic en **Activar**. Aparecerá el cuadro de diálogo **Activar**.
3. Haga clic en **Activar**. Se activa la licencia seleccionada.

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

Para automatizar una notificación de caducidad

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

1. En la página **Licencias**, establezca **Notificación de caducidad** en **Sí**. Aparecerán nuevos campos relacionados con la notificación.



2. Configure estos parámetros:
   - En **Notificar cada**, 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.
   - **Destinatario:** Escriba su propia dirección de correo electrónico o la de la persona responsable de la licencia.
   - **Contenido:** Escriba el mensaje de notificación de caducidad que el destinatario verá en la notificación.
3. Haga clic en **Guardar**. Según los parámetros que haya definido, XenMobile comienza a enviar mensajes de correo electrónico con el texto que haya proporcionado en **Contenido** al destinatario que haya indicado en **Destinatario**. Las notificaciones se envían con la frecuencia que haya establecido.

Cumplimiento del estándar FIPS 140-2

January 4, 2022

US National Institute of Standards and Technologies (Instituto nacional de estándares y tecnologías de EE. UU., NIST) emite los estándares Federal Information Processing Standard (estándares federales de procesamiento de la información, conocidos por sus siglas en inglés, FIPS). Estos estándares FIPS 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 sobre los módulos FIPS 140 validados por el instituto NIST, consulte NIST Computer Security Resource Center.

> **Importante:**
>
> - Solo puede habilitar el modo FIPS de XenMobile durante la instalación inicial.

> - Los modos de XenMobile de solo administración de dispositivos móviles (MDM) o de solo administración de aplicaciones para móvil (MAM), así como XenMobile MDM+MAM, cumplen el estándar FIPS siempre que no se usen aplicaciones HDX.

Todas las operaciones de cifrado de datos en reposo (data at rest) y datos en tránsito (data in transit) en iOS utilizan módulos de cifrado validados por FIPS que proporcionan Citrix y Apple. En Android, todas las operaciones de cifrado de datos en reposo (data at rest) utilizan módulos de cifrado validados por FIPS que proporcionan los módulos de cifrado de la plataforma que proporciona el fabricante del dispositivo. Póngase en contacto con su representante de Citrix para obtener más información sobre los módulos de los fabricantes de dispositivos.

En los dispositivos Windows compatibles, todas las operaciones de cifrado de datos en reposo y datos en tránsito para la administración de dispositivos móviles (MDM) utilizan módulos de cifrado validados por FIPS que proporciona Microsoft.

Todas las operaciones de cifrado de datos en reposo y datos en tránsito para XenMobile MDM utilizan módulos de cifrado validados por FIPS. Todos los datos en reposo y los datos en tránsito para flujos de MDM utilizan módulos de cifrado conformes con FIPS de extremo a extremo. Esa seguridad incluye las operaciones de cifrado descritas anteriormente para dispositivos móviles, más las operaciones de cifrado entre dispositivos móviles y Citrix Gateway.

El almacén MDX Vault cifra aplicaciones MDX empaquetadas y los datos en reposo asociados en dispositivos iOS y Android mediante módulos criptográficos validados por FIPS.

Idiomas disponibles

January 4, 2022

Las aplicaciones móviles de productividad y la consola de XenMobile están adaptadas para poder utilizarse en otros idiomas además del inglés. En la disponibilidad de idiomas se incluyen entradas de teclado y caracteres 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 la globalización de todos los productos Citrix, consulte https://support.citrix.com/article/CTX119253.

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

Consola de XenMobile y Self Help Portal

- Francés
- Alemán
- Español
- Japonés

- Coreano
- Portugués
- Chino simplificado

Aplicaciones móviles de productividad

Una “X” indica que la aplicación está disponible en ese idioma concreto.

iOS y Android

Idioma	Secure Hub	Secure Mail	Secure Web	QuickEdit
Japonés	X	X	X	X
Chino simplificado	X	X	X	X
Chino tradicional	X	X	X	X
Francés	X	X	X	X
Alemán	X	X	X	X
Español	X	X	X	X
Coreano	X	X	X	X
Portugués	X	X	X	X
Neerlandés	X	X	X	X
Italiano	X	X	X	X
Danés	X	X	X	X
Sueco	X	X	X	X
Hebreo	X	X	X	Solo iOS
Árabe	X	X	X	X
Ruso	X	X	X	X
Turco	X	X	Solo Android	-
Polaco	X	X	X	-

Windows

Idioma	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

Idiomas disponibles con escritura de derecha a izquierda

En la tabla siguiente se resume el texto disponible en idiomas de Europa Central en cada aplicación. X indica que la función está disponible para esa plataforma. Los idiomas escritos de derecha a izquierda no están disponibles para dispositivos Windows.

Aplicación	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
QuickEdit	X	X

Instalación y configuración

January 4, 2022

Antes de comenzar

Puede usar esta lista de verificación para, antes de instalar, anotar los requisitos previos y los parámetros de la instalación local 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 completo, consulte XenMobile Deployment Handbook.

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

Lista de verificación previa a la instalación

Conectividad básica con la red

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

Requisito previo o parámetro	Componente o función	Escriba el parámetro
———————–	———–	——-
Escriba el nombre de dominio completo (FQDN) al que se conectan los usuarios remotos.	XenMobile y Citrix Gateway
Anote la dirección IP pública y local.
Necesita estas direcciones IP para configurar el firewall y definir la traducción de direcciones de red (NAT).	XenMobile y Citrix Gateway	
Anote la máscara de subred.	XenMobile y Citrix Gateway	
Anote las direcciones IP del DNS.	XenMobile y Citrix Gateway	
Escriba las direcciones IP del servidor WINS (si corresponde).	Citrix Gateway	
Identifique y anote el nombre de host de Citrix Gateway.	Citrix Gateway Este elemento no es el 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 Citrix Gateway.	Citrix Gateway	
Anote la dirección IP de XenMobile. Reserve una dirección IP si instala una instancia de XenMobile. Si configura un clúster, escriba todas las direcciones IP que necesita.	XenMobile	
Una dirección IP pública configurada en Citrix Gateway	Citrix Gateway	
Una entrada DNS externa para Citrix Gateway	Citrix Gateway
Anote 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).	Citrix Gateway	Puede utilizar el nombre sAMAccountName o el nombre principal de usuario (UPN) al configurar el nombre de usuario para el proxy web.	XenMobile y Citrix Gateway	
Escriba la dirección IP de la puerta de enlace predeterminada.	XenMobile y Citrix Gateway	
Escriba la dirección IP del sistema (NSIP) y la máscara de subred.	Citrix Gateway	
Escriba la dirección IP de subred (SNIP) y la máscara de subred.	Citrix Gateway	
Escriba la dirección IP y el nombre de dominio completo (FQDN) del servidor virtual de Citrix Gateway suministrados en el certificado. Para configurar varios servidores virtuales, escriba todas las direcciones IP virtuales y los nombres FQDN de los certificados.	Citrix Gateway	
Escriba las redes internas a las que pueden acceder los usuarios a través de Citrix Gateway. Ejemplo: 10.10.0.0/24. Introduzca todas las redes internas y los segmentos de red a los que deben acceder los usuarios cuando se conectan a Secure Hub o Citrix Gateway Plug-in si la opción de túnel dividido

está activada. | Citrix Gateway | |
| Compruebe que la conectividad de red entre XenMobile Server, Citrix Gateway, el servidor SQL Server externo de Microsoft y el servidor DNS está operativa. | XenMobile y Citrix Gateway | |

Licencias

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

Requisito previo	Componente	Escriba la ubicación
Obtenga licencias universales del sitio web de Citrix. Para obtener información detallada, consulte Licencias en la documentación de Citrix Gateway.	Citrix Gateway, XenMobile y Citrix License Server	

Certificados

XenMobile y Citrix 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 y certificados en la documentación de XenMobile.

Requisito previo	Componente	Notas
———	———	—–
Obtenga los certificados necesarios e instálelos.	XenMobile y Citrix Gateway	

Ports

Abra puertos para permitir la comunicación con los componentes de XenMobile.

Requisito previo	Componente	Notas
Puertos abiertos para XenMobile	XenMobile y Citrix Gateway	

Base de datos

XenMobile requiere que se configure la conexión a la base de datos. El repositorio de XenMobile requiere una base de datos de Microsoft SQL Server que se ejecute en una de las versiones compatibles indicadas en Requisitos del sistema y compatibilidad. Citrix recomienda usar Microsoft SQL de forma remota. PostgreSQL se incluye con XenMobile. Use PostgreSQL local o remoto *solamente* en entornos de prueba.

De forma predeterminada, XenMobile utiliza el controlador de base de datos jTDS. Para utilizar el controlador JDBC de Microsoft en instalaciones locales de XenMobile Server, consulte Controladores de SQL Server.

Requisito previo	Componente	Notas
Puerto y dirección IP de Microsoft SQL Server. Compruebe que la cuenta de servicio de SQL Server que se va a usar en XenMobile tiene el permiso del rol DBcreator.	XenMobile	

Parámetros de Active Directory

Requisito previo	Componente	Notas
———	———	——————-
Escriba el puerto y la dirección IP de Active Directory de los servidores principales y secundarios. Si utiliza el puerto 636, instale un certificado raíz de una entidad de certificación en XenMobile y cambie la opción “Usar conexión segura” a “Sí”.	XenMobile y Citrix Gateway
Escriba el nombre de dominio de Active Directory.	XenMobile y Citrix Gateway
Escriba la cuenta de servicio de Active Directory, que requiere un ID de usuario, una contraseña y un alias de dominio.
La cuenta de servicio de Active Directory es la cuenta que XenMobile utiliza para enviar consultas a Active Directory.	XenMobile y Citrix Gateway	
Escriba el DN base de usuario; es el nivel de directorio en el que se encuentran los usuarios. Por ejemplo: `cn=users,dc=ace,dc=com`. Citrix Gateway y XenMobile usan este DN base de usuario para enviar consultas a Active Directory.	XenMobile y Citrix Gateway	
Escriba el DN base de grupo; es el nivel de directorio en el que se encuentran los grupos. Citrix Gateway y XenMobile usan este DN para enviar consultas a Active Directory.	XenMobile y Citrix Gateway	

Conexiones entre XenMobile y Citrix Gateway

Requisito previo	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.	Citrix Gateway	
Escriba la dirección URL de respuesta.	XenMobile	

Conexiones de usuario: Acceso a Citrix Virtual Apps and Desktops y Citrix Secure Hub

Citrix recomienda usar el asistente de configuración rápida de Citrix ADC para configurar los parámetros de conexión entre XenMobile y Citrix 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. Esas conexiones se realizan a escritorios virtuales y aplicaciones Windows que están en Virtual Apps and Desktops. Citrix recomienda usar también el asistente de configuración rápida en Citrix ADC Gateway para configurar estos parámetros.

Requisito previo	Componente	Escriba el parámetro
Escriba el nombre de host y la URL externa de Citrix Gateway. La URL externa es la dirección web a la que se conectan los usuarios.	XenMobile	
Escriba la dirección URL de respuesta de Citrix Gateway.	XenMobile	
Escriba las direcciones IP y las máscaras de subredes para el servidor virtual.	Citrix Gateway	

Requisito previo	Componente	Escriba el parámetro
Anote la ruta para el Agente de Program Neighborhood o un sitio de Virtual Apps and Desktops.	Citrix Gateway y XenMobile	
Escriba el nombre FQDN o la dirección IP del servidor de Citrix Virtual Apps and Desktops que ejecuta Secure Ticket Authority (STA) (solo para conexiones ICA).	Citrix Gateway	
Escriba el nombre FQDN público de XenMobile.	Citrix Gateway	
Escriba el nombre FQDN público de Secure Hub.	Citrix Gateway	

Diagrama de flujo para la implementación de XenMobile

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

1: Requisitos del sistema y compatibilidad

2: Instalar y configurar

3 y 4: Lista de verificación previa a la instalación (este artículo)

5: Configurar XenMobile en la ventana del símbolo del sistema (este artículo)

6: Configurar XenMobile en un explorador web (este artículo)

7: Configurar parámetros para el entorno de XenMobile

8: Requisitos de puertos

Instalar 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. Para evitar problemas de zona horaria al sincronizar el tiempo de XenMobile con un hipervisor, apunte XenMobile a un servidor NTP. Para ello, utilice la interfaz CLI de XenMobile como se describe en Opciones de la interfaz de línea de comandos.

Requisitos previos de XenServer o VMware ESXi. Antes de instalar XenMobile en XenServer o en VMware ESXi, debe llevar a cabo lo siguiente. Para obtener más información, consulte la documentación de XenServer o VMware.

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

Requisitos previos de Hyper-V. Antes de instalar XenMobile en Hyper-V, debe llevar a cabo lo siguiente. Para obtener más información, consulte la documentación de Hyper-V.

- Instale Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2 con Hyper-V y sus roles habilitados en un equipo que disponga de los recursos de sistema adecuados. Cuando instale el rol Hyper-V, debe especificar las tarjetas de interfaz de red (NIC) en el servidor que Hyper-V usa 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 XenMobile Server en el modo FIPS, complete una serie de requisitos previos como se describe en Configurar FIPS con XenMobile.

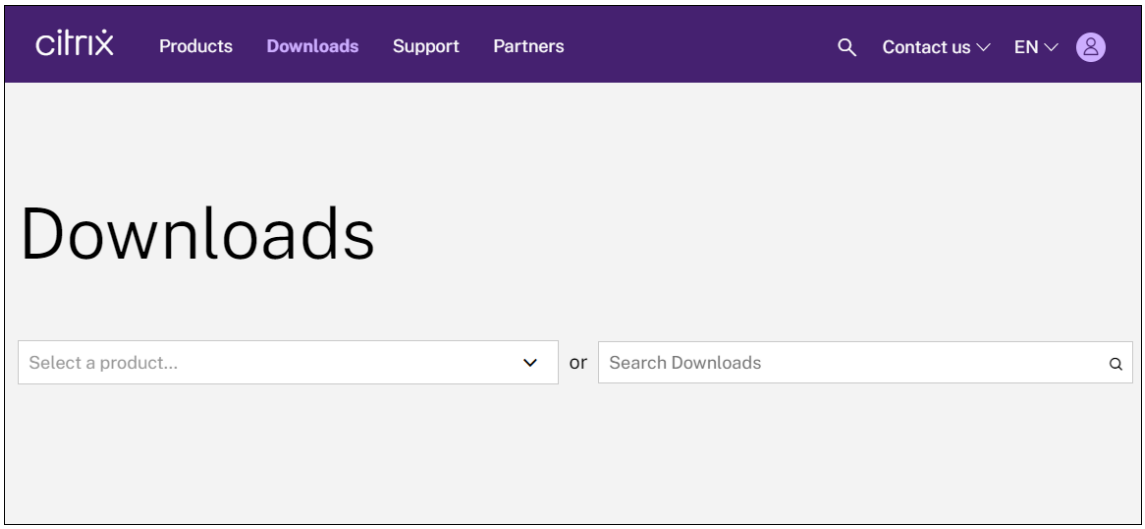
Descarga del software del producto XenMobile

Puede descargar el software del producto desde el sitio Web de Citrix. Inicie sesión en el sitio y use el enlace de descargas para ir a la página que contiene el software a descargar.

Para descargar el software de XenMobile

1. Vaya al sitio Web de Citrix.
2. Junto al cuadro de búsqueda, haga clic en **Iniciar sesión** e inicie sesión en su cuenta.
3. Haga clic en la ficha **Descargas**.

4. En la página Descargas, en la lista de **selección de productos**, haga clic en **Citrix Endpoint Management (y Citrix XenMobile Server)**. La página Citrix Endpoint Management (y Citrix XenMobile Server) aparece automáticamente.



5. Expanda **XenMobile Server (local)**.
6. Expanda **Software de producto**.
7. Haga clic en **XenMobile Server 10**.
8. Haga clic en el menú **Ir a descargas** y elija la imagen virtual que se usará para instalar XenMobile. También puede desplazarse hacia abajo hasta el botón **Descargar archivo** de la imagen que quiere instalar.
9. Siga las instrucciones en pantalla para descargar el software.

Para descargar el software de Citrix Gateway

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

1. Vaya al sitio Web de Citrix.
2. Si todavía no ha iniciado sesión en el sitio web de Citrix, haga clic en **Iniciar sesión** junto al cuadro de búsqueda e inicie una sesión con su cuenta.
3. Haga clic en la ficha **Descargas**.
4. En la página Descargas, en la lista de selección de productos, haga clic en **Citrix Gateway**.
5. Haga clic en **Ir**. Aparecerá la página Citrix Gateway.
6. En la página de Citrix Gateway, expanda la versión de Citrix Gateway que se está ejecutando.
7. En **Firmware**, haga clic en la versión del software de dispositivo que quiere descargar.

> **Nota:**
>
> También puede hacer clic en **Dispositivos virtuales** para descargar Citrix ADC 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 del software de dispositivo que quiere descargar.
9. En la página de software del dispositivo referente a la versión que quiere descargar, haga clic en **Descargar** junto al dispositivo virtual apropiado.
10. Siga las instrucciones en pantalla para descargar el software.

Configurar XenMobile para el primer uso

1. Para configurar la dirección IP y la máscara de subred, la puerta de enlace predeterminada, los servidores DNS y demás para XenMobile, use la consola de línea de comandos de XenCenter o vSphere.

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

2. Acceda a la consola de administración de XenMobile solamente con un nombre de dominio completo de XenMobile Server o las direcciones IP del nodo.
3. Inicie sesión y siga los pasos indicados en las pantallas iniciales de inicio de sesión.

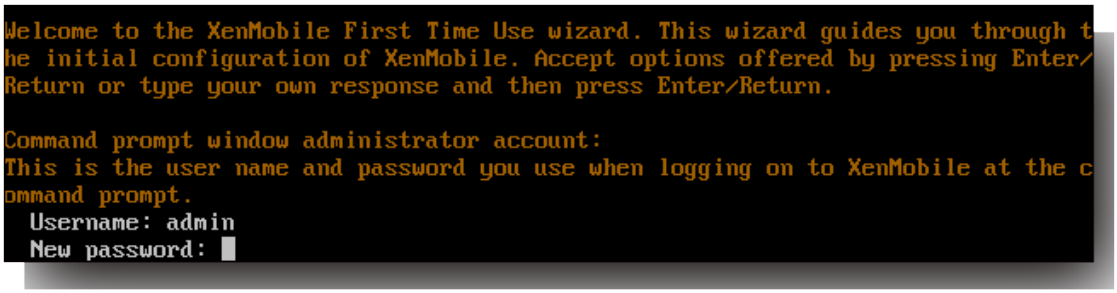
Configurar XenMobile en la ventana del símbolo del sistema

1. Importe la máquina virtual de XenMobile en Citrix XenServer, Microsoft Hyper-V o VMware ESXi. Para obtener más información, 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.

   Al crear o modificar las contraseñas de la cuenta de administrador del símbolo del sistema, de los certificados del servidor PKI y de FIPS, XenMobile impone las siguientes reglas a todos los

usuarios excepto a los usuarios de Active Directory cuyas contraseñas se administran fuera de XenMobile.

- La contraseña debe contener al menos ocho caracteres.
- La contraseña 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: ! ## $ %)



No aparecerá ningún carácter (por ejemplo, asteriscos) cuando escriba la nueva contraseña.

4. Facilite la siguiente información de red y, a continuación, escriba **y** para confirmar los parámetros:

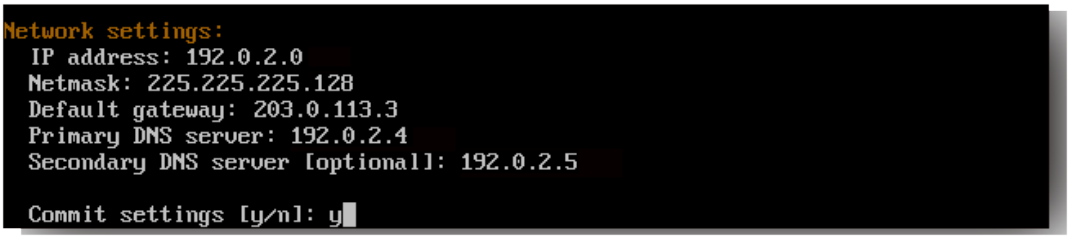
   a) Dirección IP del servidor de XenMobile Server

   b) Máscara de red

   c) Puerta de enlace predeterminada, que es la dirección IP de la puerta de enlace predeterminada en la DMZ

   d) Servidor DNS primario, que es la dirección IP del servidor DNS

   e) Servidor DNS secundario (opcional)



> **Nota:**
>
> Las direcciones que se muestran en esta imagen y las siguientes no funcionan; solo se proporcionan a modo de ejemplo.

5. Escriba **y** para aumentar la seguridad mediante la generación de una frase secreta aleatoria de cifrado, o bien, escriba **n** para proporcionar su propia frase secreta. Citrix recomienda escribir

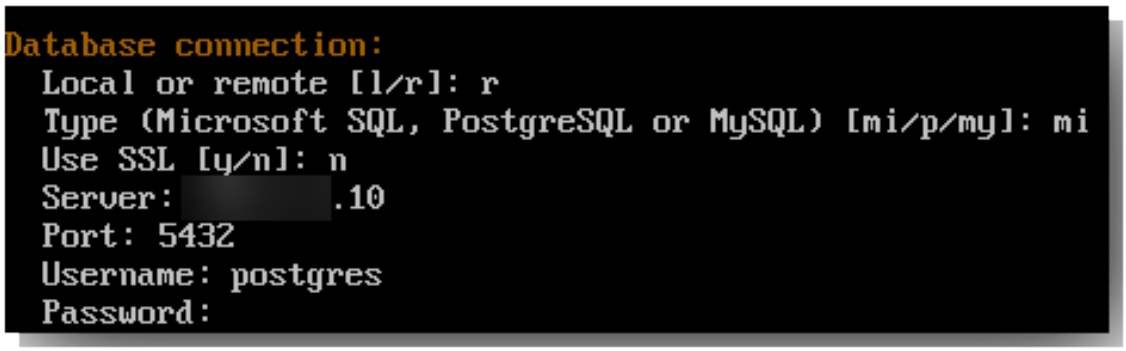
y para generar una frase secreta aleatoria.

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. Si selecciona una frase secreta aleatoria, no podrá verla.

6. También 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, según se describe en Configurar FIPS con XenMobile.

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



   - La base de datos puede ser local o remota. Escriba **l** para local o **r** para remota.
   - Seleccione el tipo de base de datos. Escriba **mi** para Microsoft SQL o **p** para PostgreSQL.

     > **Importante:**
     >
     > - Citrix recomienda usar Microsoft SQL de forma remota. PostgreSQL se incluye con XenMobile. Use PostgreSQL local o remoto *solamente* en entornos de prueba.
     > - No se admite 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.

   - Si quiere, escriba **y** para utilizar la autenticación SSL en la base de datos.

- Proporcione el nombre de dominio completo (FQDN) para el servidor que aloja XenMobile. Este servidor host proporciona servicios de administración de dispositivos y administración de aplicaciones.
- Escriba el número de puerto de la base de datos si este difiere del número de puerto predeterminado. El puerto predeterminado para Microsoft SQL es 1433 y el puerto predeterminado para PostgreSQL es 5432.
- Escriba el nombre de usuario del administrador de la base de datos.
- Escriba la contraseña del administrador de la base de datos.
- Escriba el nombre de la base de datos.
- Presione **Entrar** para confirmar los parámetros de la base de datos.

8. Si quiere, escriba **y** para habilitar instancias o la agrupación en clústeres de los nodos de XenMobile.

   > **Importante:**
   >
   > Si habilita un clúster de XenMobile, después de completarse la configuración del sistema, abra el puerto 80 para permitir la comunicación en tiempo real entre miembros del clúster. Complete esa configuración en todos los nodos de clúster.

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

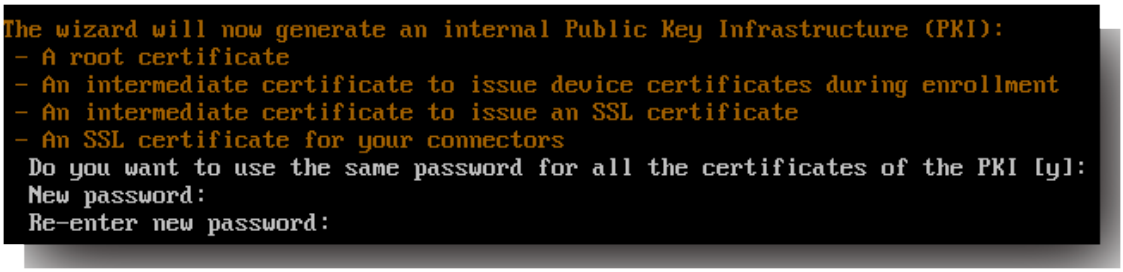
10. Presione **Entrar** para confirmar los parámetros.
11. Identifique los puertos de comunicación. Para obtener información más detallada acerca de los puertos y sus usos, consulte Requisitos de puertos.

    > **Nota:**
    >
    > Para aceptar los puertos predeterminados, presione **Entrar** (Retorno en Mac).

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

13. Escriba **y** si quiere usar la misma contraseña para cada certificado de infraestructura de clave pública (PKI). Para obtener información más detallada acerca de la función PKI de XenMobile, consulte Cargar certificados.



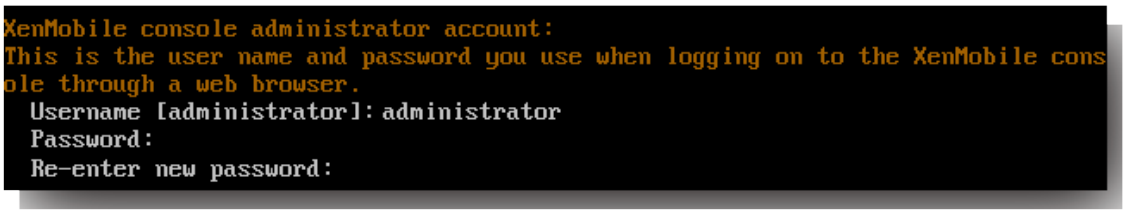
> **Importante:**
>
> Si va a agrupar instancias o nodos en clúster de XenMobile, debe proporcionar contraseñas idénticas para los nodos subsiguientes.

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

    No aparecerá ningún carácter (por ejemplo, asteriscos) cuando escriba la nueva contraseña.

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. Debe recordar o anotar estas credenciales para usarlas posteriormente.

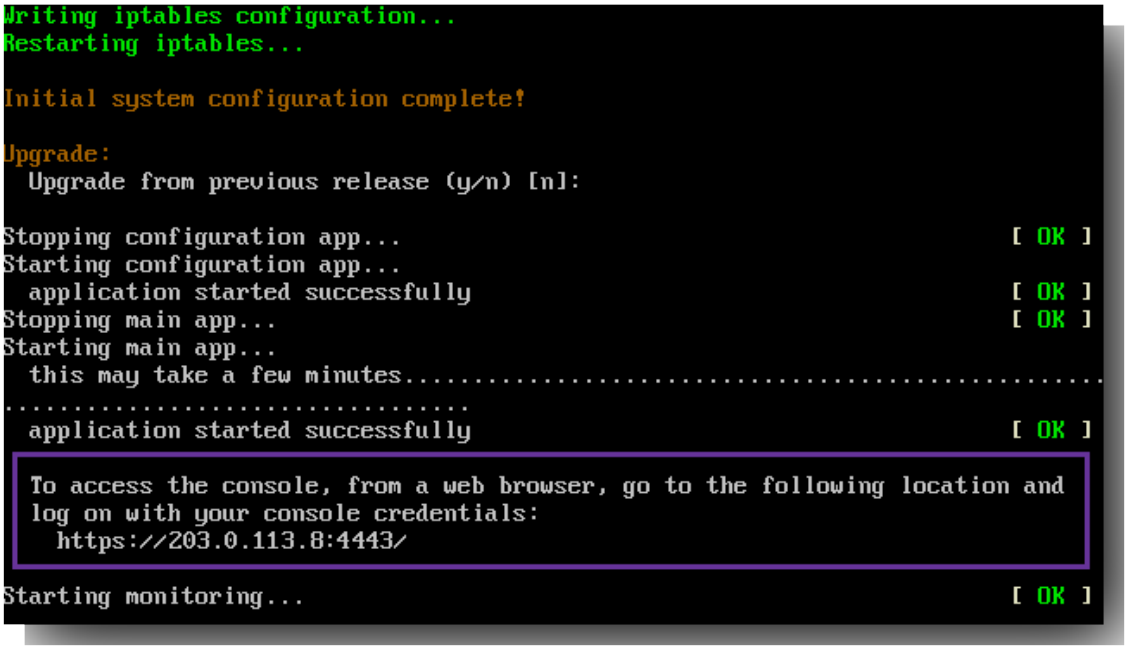


> **Nota:**
>
> No aparecerá ningún carácter (por ejemplo, asteriscos) cuando escriba la nueva contraseña.

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.

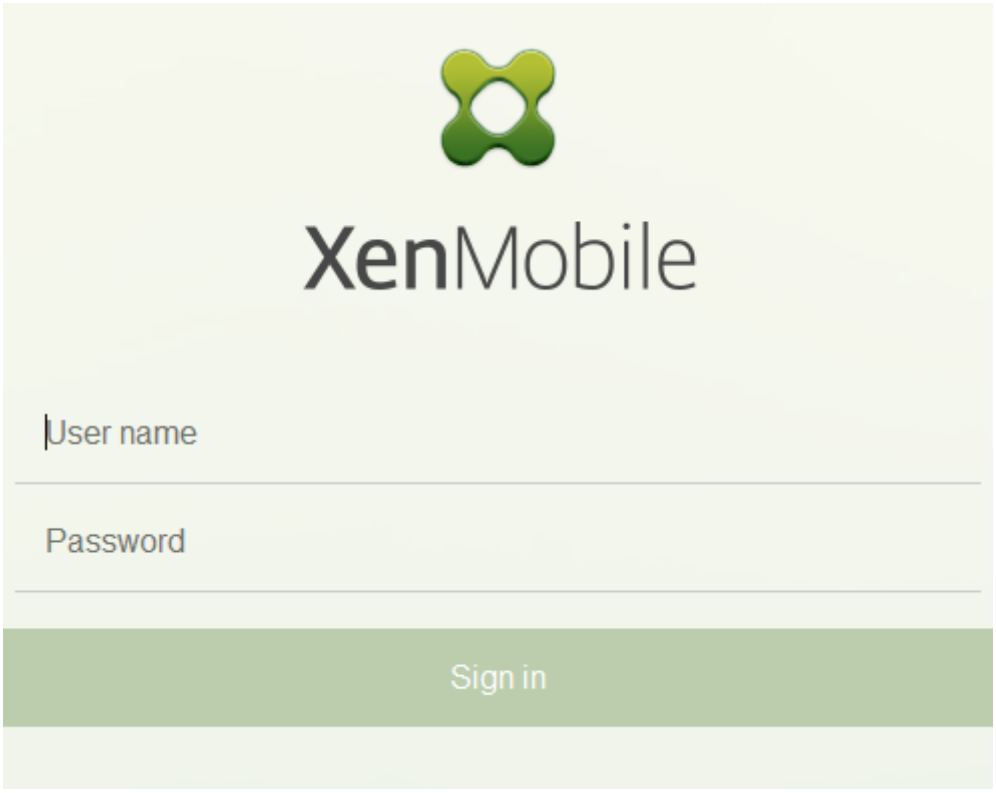
19. Copie toda la URL que aparece en pantalla, y continúe la siguiente configuración inicial de XenMobile con el explorador web.



Configurar XenMobile en un explorador web

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

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



3. En la página Get Started, haga clic en **Start**. Aparecerá la página **Licencias**.
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, debe usar Citrix Licensing en un servidor remoto.

5. En la página **Certificados**, haga clic en **Importar**. Aparecerá el cuadro de diálogo Importar.
6. Importe los certificados APNs y escucha de SSL. La administración de dispositivos iOS requiere un certificado APNs. Para obtener más información sobre cómo trabajar con certificados, consulte Certificados.

   > **Nota:**
   >
   > Este paso requiere reiniciar el servidor.

7. Si es adecuado para el entorno, configure Citrix Gateway. Para obtener información detallada sobre cómo configurar Citrix Gateway, consulte Citrix Gateway y XenMobile y Configurar parámetros para el entorno de XenMobile.

> **Nota:**
>
> - Puede implementar Citrix Gateway en el perímetro de su red interna (o intranet). Esa implementación ofrece un único punto de acceso seguro a los servidores, las aplicaciones y otros recursos de red que residan en la red interna. En esa implementación, todos los usuarios remotos deben conectarse a Citrix Gateway para poder acceder a los recursos de la red interna.
> - Aunque configurar Citrix Gateway sea optativo, después de escribir datos en la página, debe borrar o completar los campos obligatorios antes de salir de la página.

8. Complete la configuración del protocolo LDAP para acceder a usuarios y grupos de Active Directory. Para obtener detalles sobre la configuración de la conexión LDAP, consulte Configurar LDAP.
9. Configure el servidor de notificaciones para poder enviar mensajes a los usuarios. Para obtener información más detallada acerca de la configuración del servidor de notificaciones, consulte Notificaciones.

Requisito posterior. Reinicie el servidor de XenMobile Server para activar los certificados.

Configurar FIPS con XenMobile

January 4, 2022

El modo FIPS (Federal Information Processing Standards) en XenMobile admite clientes pertenecientes a organismos del gobierno federal de los Estados Unidos, ya que solo utiliza bibliotecas certificadas por FIPS 140-2 para todas las operaciones de cifrado. Si instala XenMobile Server con el modo FIPS, se asegura de que todos los datos para el cliente y para el servidor de XenMobile cumplen los estándares de FIPS 140-2. Ese cumplimiento se aplica a los datos en reposo y los datos en tránsito.

Antes de instalar un servidor de XenMobile Server en modo FIPS, complete los siguientes requisitos previos.

- Use un servidor SQL Server 2014 externo para la base de datos de XenMobile. El servidor SQL Server también debe configurarse para la comunicación SSL segura. Para obtener instrucciones sobre cómo configurar la comunicación SSL segura con SQL Server, consulte Habilitación de conexiones cifradas en el Motor de base de datos (Administrador de configuración de SQL Server).
- Para la comunicación SSL segura, se necesita instalar un certificado SSL de confianza de una entidad de certificación (CA) conocida en SQL Server. 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.

Configurar el modo FIPS

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

Dispone de la opción **Toggle FIPS mode** en la interfaz de línea de comandos de XenMobile: no es para usar en un entorno de producción. Esta opción está pensada para usarse en entornos que no son de producción, con fines de diagnóstico, y no se admite en entornos XenMobile Server de producción.

1. Durante la instalación inicial, habilite **FIPS mode**.
2. Cargue el certificado raíz de la CA del servidor SQL.
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. Aparece la frase **In FIPS Compliant Mode** en la pancarta de inicio de sesión.

Importar certificados

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

Requisitos previos de SQL

1. La conexión con la instancia SQL desde XenMobile debe ser segura y la versión debe ser SQL Server 2012 o SQL Server 2014. Para proteger la conexión, consulte Cómo habilitar el cifrado de SSL para una instancia de SQL Server con 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 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 **OK**.

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 grupo o usuario**, 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 **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 de SQL.

3. Compruebe que el servicio SQL se inicia correctamente.

Requisitos previos de Internet Information Services (IIS)

1. Descargue el certificado raíz (base 64).
2. Copie el certificado raíz al sitio web predeterminado del servidor IIS, C:\inetpub\wwwroot.
3. Marque la casilla **Autenticación** para el sitio predeterminado.
4. Establezca el parámetro **Anónimo** en **habilitado**.
5. Marque la casilla de reglas de **Seguimiento de solicitudes con error**.
6. Compruebe que CER no esté bloqueado.
7. Busque la ubicación del archivo CER en un explorador web desde el servidor local, `https://localhost/certname.cer`. El texto de certificado raíz aparecerá en el explorador web.
8. Si el certificado raíz no aparece en el explorador web, compruebe que ASP está habilitado en el servidor IIS de esta manera.

a) Abra el Administrador del servidor.

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

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

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

9. Vaya a `https://localhost/cert.cer`.

   Para obtener más información, consulte Servidor Web (IIS).

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

Importar el 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 conocer los pasos de instalación, consulte Instalar XenMobile.

- Enable FIPS: Sí
- Upload Root Certificate: Sí
- Copy(c) or Import(i): i
- Enter HTTP URL to import: `https://<FQDN of IIS server>/cert.cer`
- Server: *FQDN de SQL Server*
- Port: 1433
- User name: Cuenta del servicio con capacidad para crear la base de datos (`domain\username`).
- Password: La contraseña de la cuenta del servicio.
- Database Name: El nombre que decida.

Habilitar el modo FIPS en los dispositivos móviles

De forma predeterminada, el modo FIPS está inhabilitado en los dispositivos móviles. Para habilitar el modo FIPS, vaya a **Parámetros > Propiedades de cliente**, modifique la propiedad **Enable FIPS Mode** y establezca el valor en **verdadero**. Para obtener más información, consulte Propiedades de cliente.

Configurar la agrupación en clústeres

January 4, 2022

Para configurar la agrupación en clústeres, defina las dos siguientes direcciones IP virtuales de equilibrio de carga en Citrix ADC.

- **Dirección IP virtual de equilibrio de carga para la administración de dispositivos móviles (MDM):** Se necesita una dirección IP virtual de equilibrio de carga de 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 de MAM para que Citrix Gateway establezca conexión con los nodos de XenMobile configurados en clúster. De forma predeterminada, en XenMobile todo tráfico proveniente de Citrix Gateway se enruta a la dirección IP virtual de equilibrio de carga en el puerto 8443.

En los procedimientos de este artículo, se explica cómo crear una máquina virtual de XenMobile y unirla a una máquina virtual ya existente. Con esos pasos, se crea una configuración en clúster.

Requisitos previos

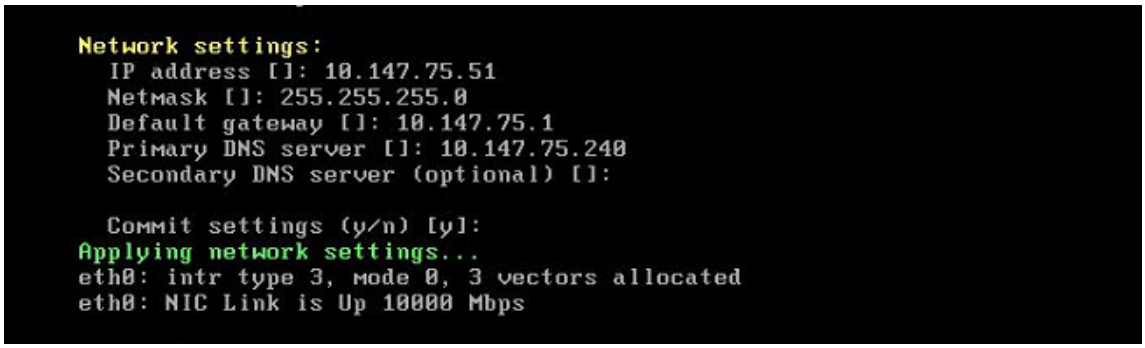
- Haber completado la configuración del nodo pertinente de XenMobile.
- Configurar NTP en todos los nodos del clúster y en la base de datos de XenMobile. Para que la agrupación en clústeres funcione correctamente, todos esos servidores deben tener la misma hora.
- Una dirección IP pública para el equilibrador de carga de MDM y una dirección IP privada para MAM.
- Certificados de servidor.
- Una dirección IP libre para la dirección IP virtual de Citrix Gateway.
- Con XenMobile implementado en una configuración de clústeres y en el modo de solo MDM o Enterprise (MDM+MAM), debe modificar la configuración del equilibrador de carga de Citrix ADC para utilizar la **persistencia de la IP de origen** en todos los equilibradores de carga MDM de Citrix ADC, es decir, los servidores virtuales definidos para los puertos 8443 y 443. Complete esa configuración antes de que los dispositivos de los usuarios se actualicen a iOS 11. Para obtener más información, consulte este artículo de Citrix Knowledge Center: https://support.citrix.com/article/CTX227406.
- Para instalar aplicaciones desde XenMobile Store en dispositivos iOS 11, debe habilitar el puerto 80 en el servidor de XenMobile Server.

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

Instalar nodos de clúster en XenMobile

Cree 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.

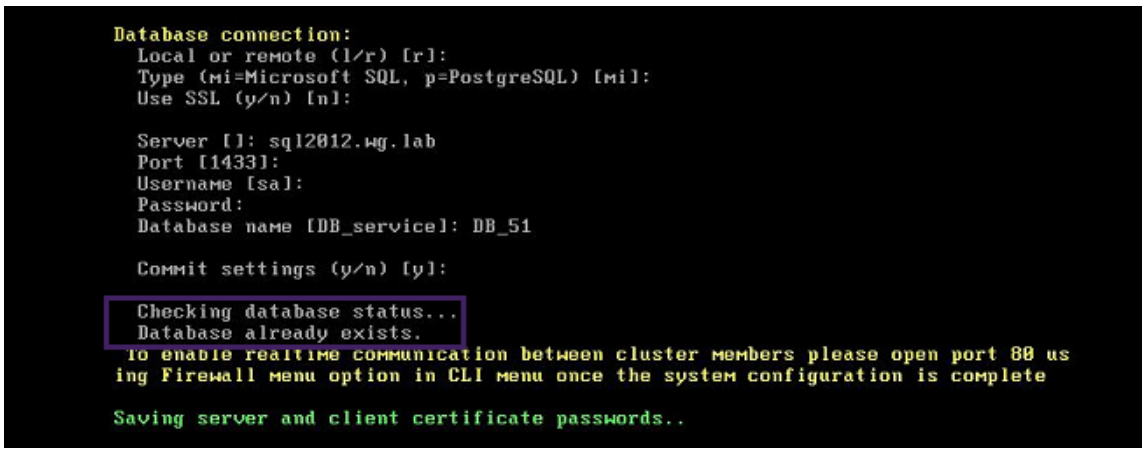
1. Abra la consola de línea de comandos de la nueva máquina virtual y escriba la contraseña nueva de la cuenta del administrador.
2. Proporcione los detalles de configuración de la red como se muestra en la siguiente imagen.



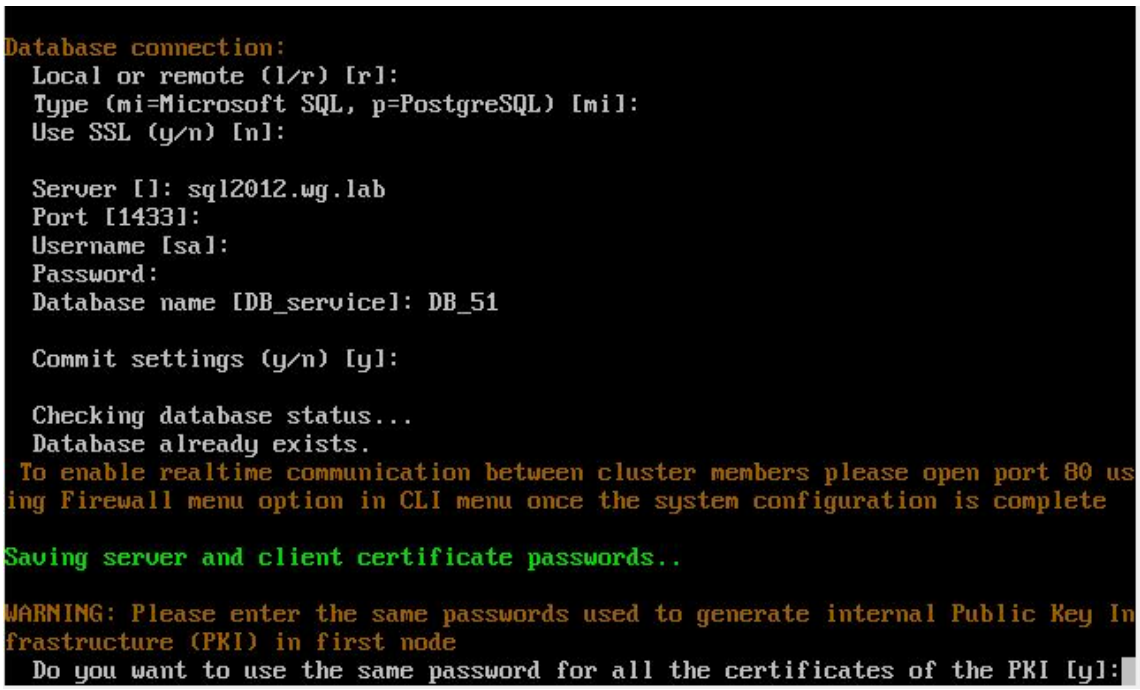
3. Si quiere usar la contraseña predeterminada para la protección de datos, escriba **y**. Si no, escriba **n** y luego introduzca una nueva contraseña.

4. Si quiere utilizar FIPS, escriba **y**; si no, escriba **n**.

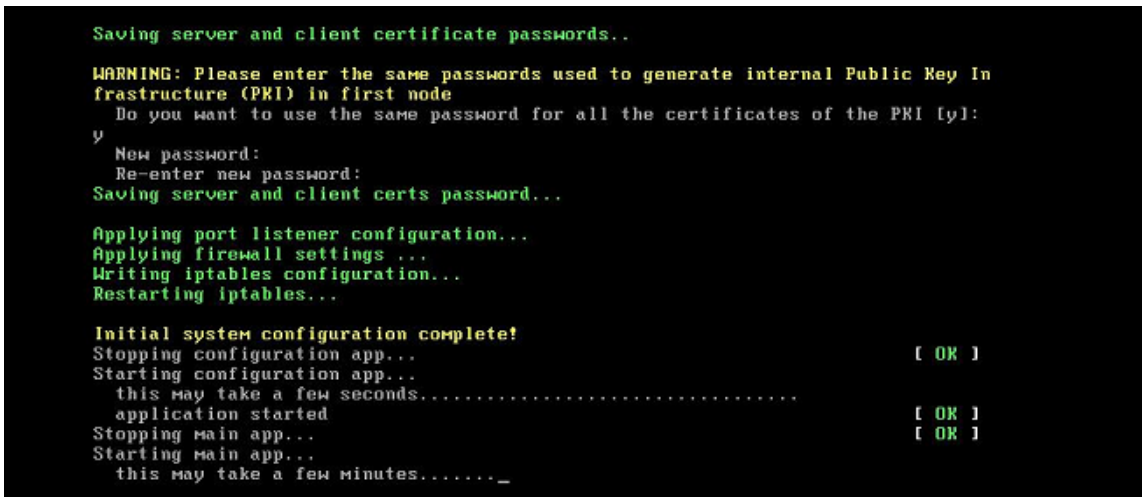
5. Configure la base de datos para que apunte a la misma base de datos que la máquina virtual anterior configurada. Verá el mensaje “Database already exists”.



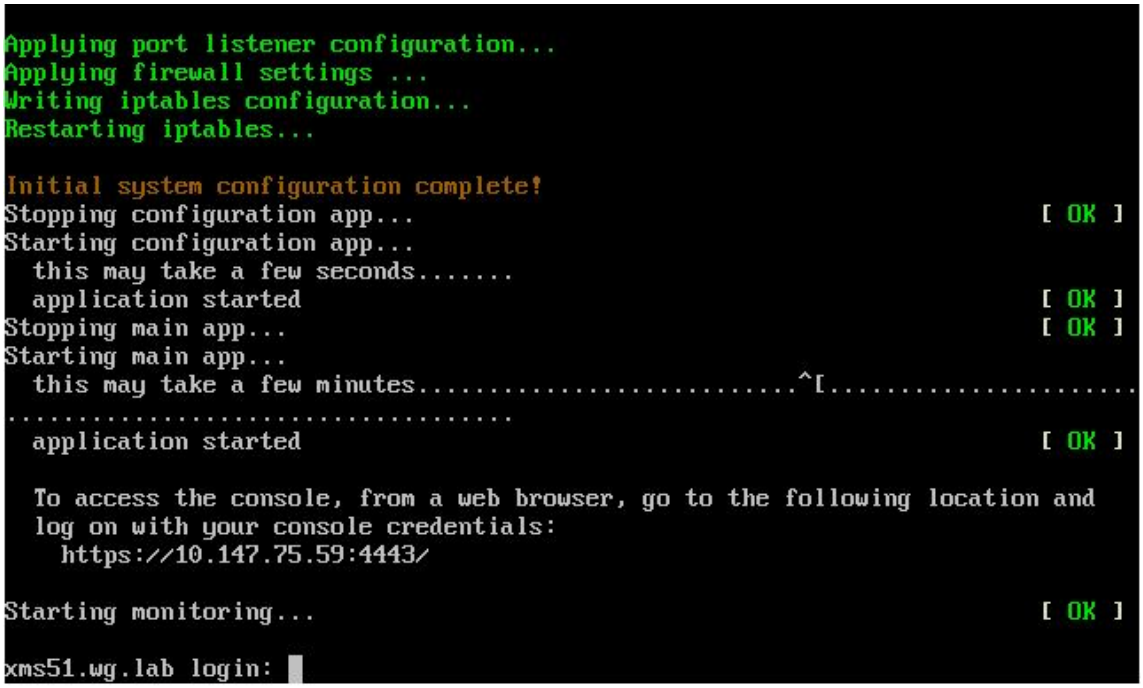
6. Escriba las mismas contraseñas de los certificados que proporcionó para la primera máquina virtual.



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



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

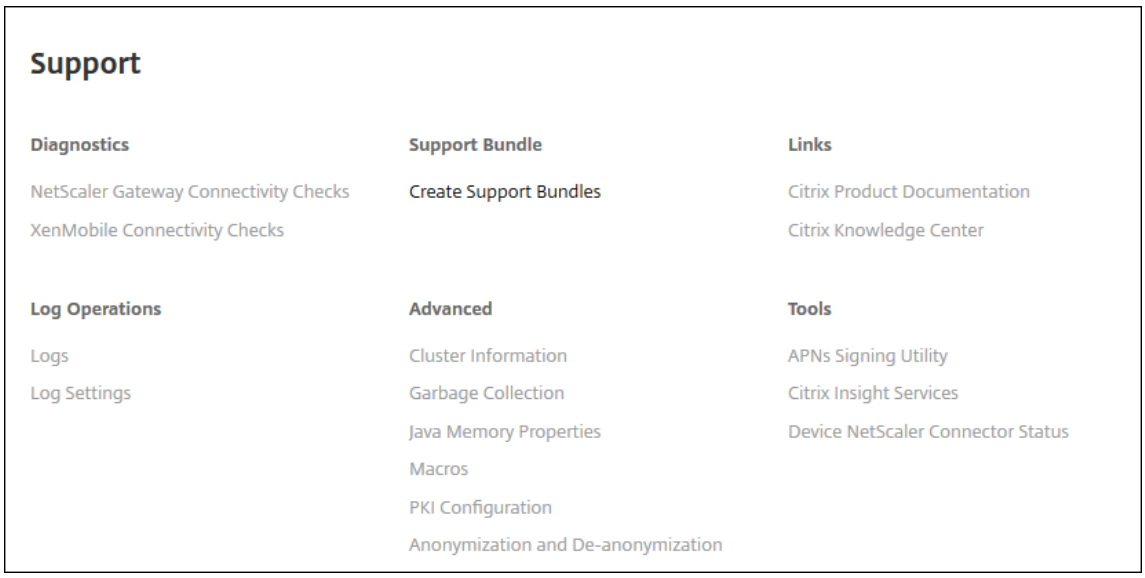


> **Nota:**
>
> Este cuadro de diálogo de inicio de sesión es idéntico al cuadro de diálogo del inicio de sesión de la primera máquina virtual. Esta coincidencia sirve para confirmar que ambas máquinas virtuales utilizan el mismo servidor de base de datos.

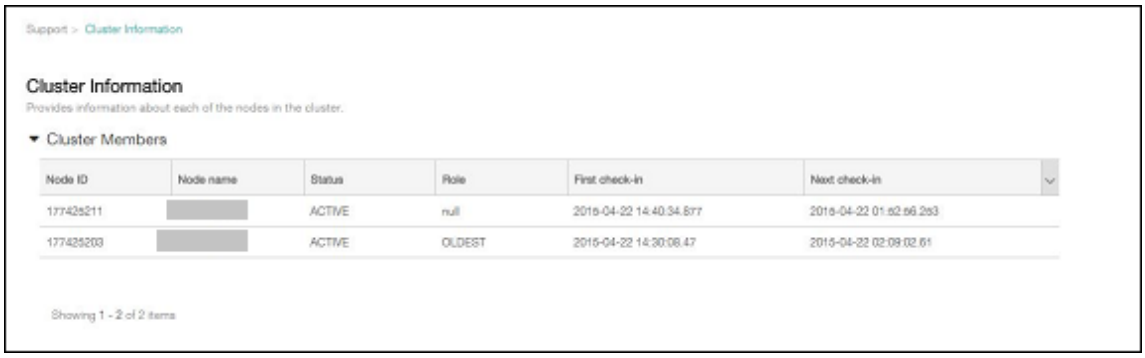
8. Utilice el nombre de dominio completo (FQDN) de XenMobile para abrir la consola de XenMobile en un explorador web.
9. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha de la consola.

Se abrirá la página **Asistencia**.

10. En **Avanzado**, haga clic en **Información del clúster**.



Aparecerá toda la información relativa al clúster, incluida la información de sus miembros, de la conexión del dispositivo y las tareas, entre otros. Ahora, el nuevo nodo es miembro del clúster.

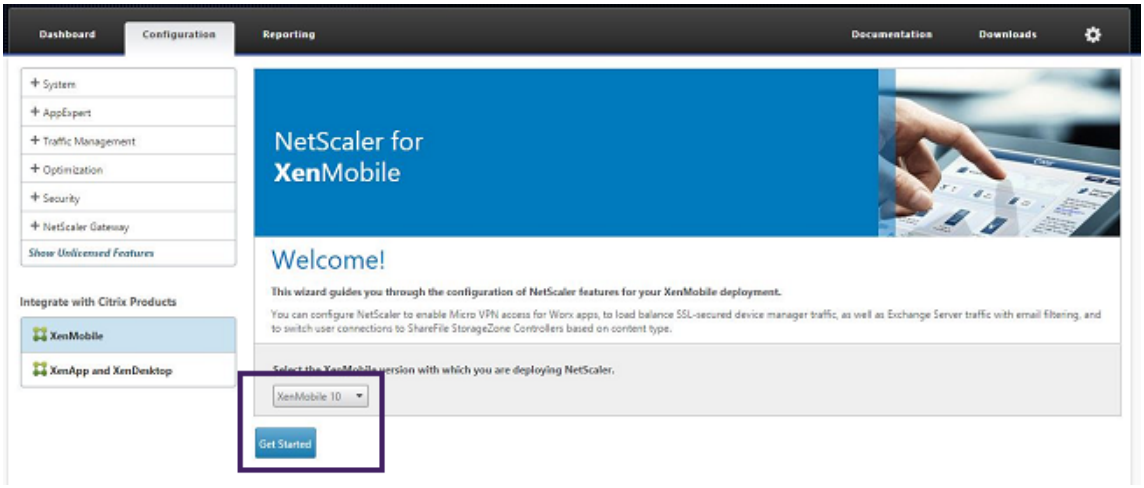


Puede agregar otros nodos siguiendo los mismos pasos. El primer nodo agregado al clúster tiene el rol **MÁS ANTIGUO**. Los nodos agregados después mostrarán el rol **NINGUNO** o **nulo**.

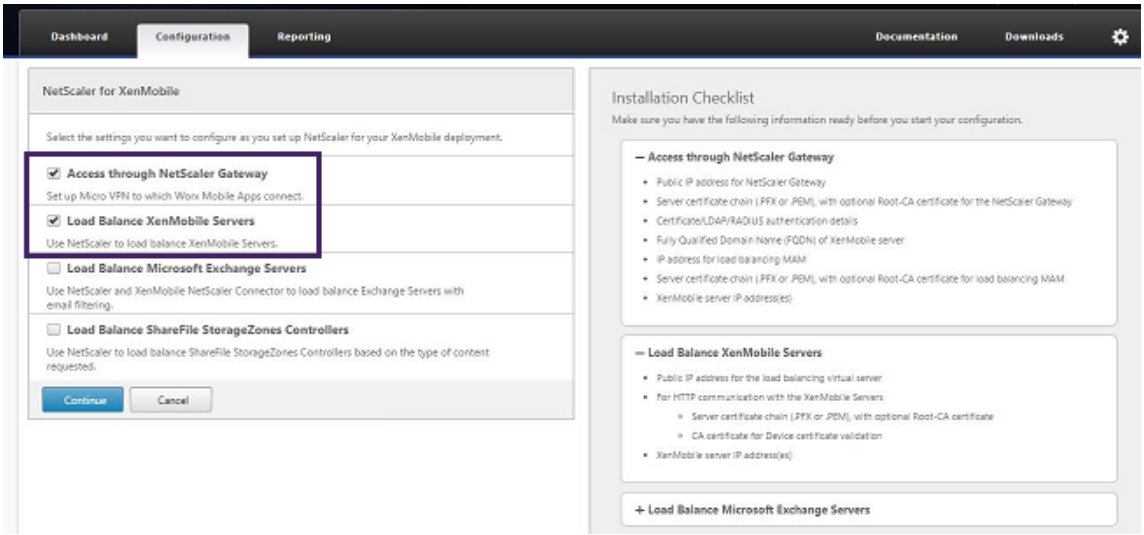
Para configurar el equilibrio de carga para el clúster de XenMobile en Citrix ADC

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 Citrix ADC. En los siguientes pasos se describe cómo equilibrar la carga de XenMobile ejecutando el asistente.

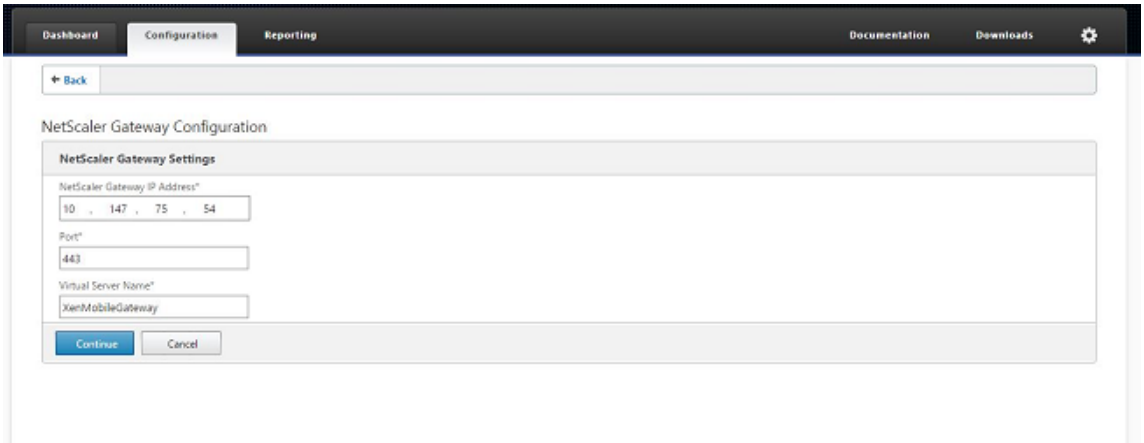
1. Inicie sesión en Citrix ADC.
2. En la ficha “Configuration”, haga clic en **XenMobile** y en **Get Started**.



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



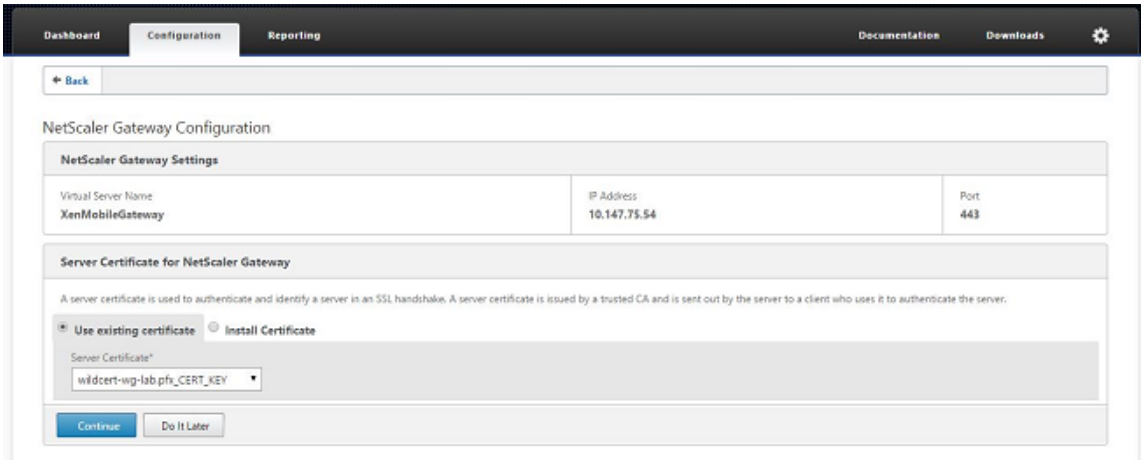
4. Escriba la dirección IP de Citrix Gateway y haga clic en **Continue**.



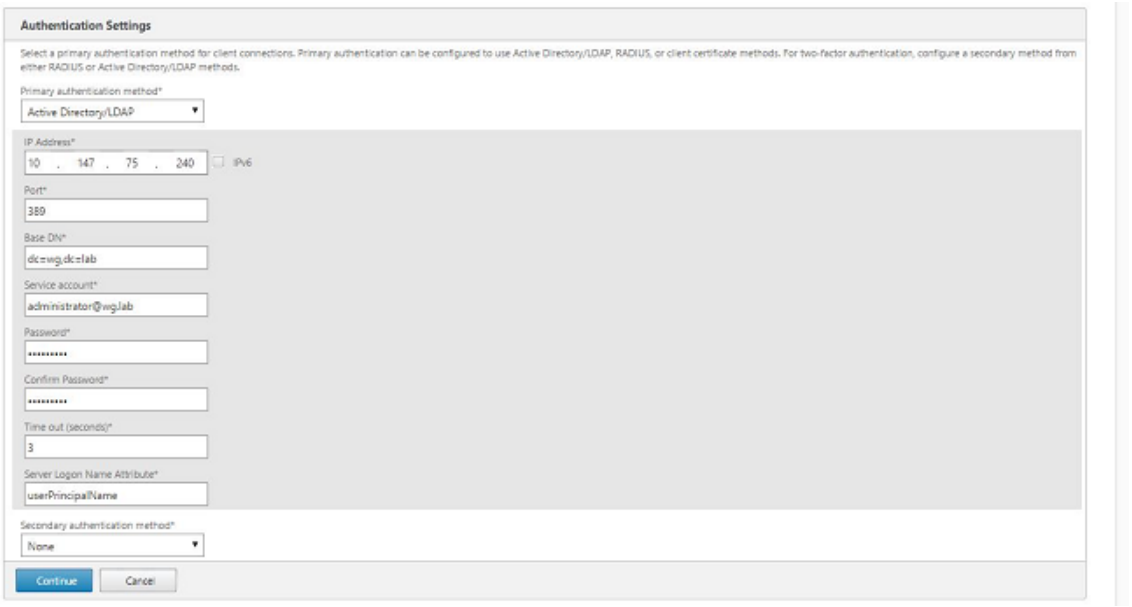
5. Vincule el certificado de servidor a la dirección IP virtual de Citrix Gateway. Para ello, lleve a

cabo una de las siguientes acciones y haga clic en **Continue**.

- En **Use existing certificate**, elija el certificado de servidor de la lista.
- Haga clic en la ficha **Install Certificate** para cargar un nuevo certificado de servidor.

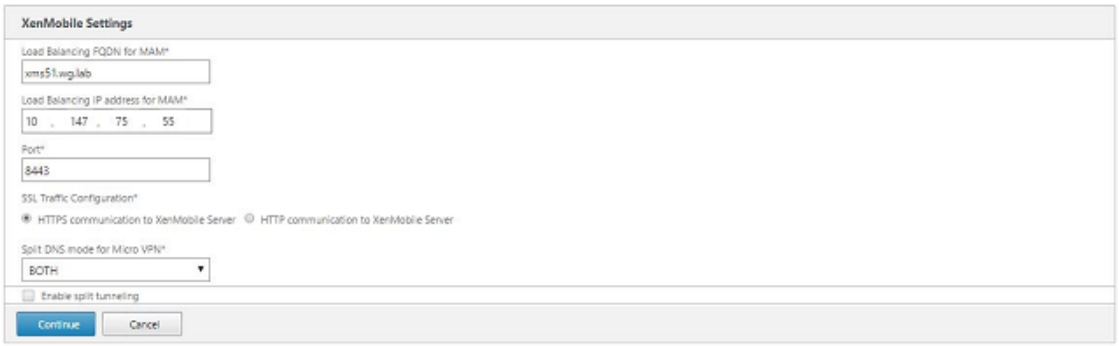


6. Escriba los detalles del servidor de autenticación y haga clic en **Continue**.



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

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

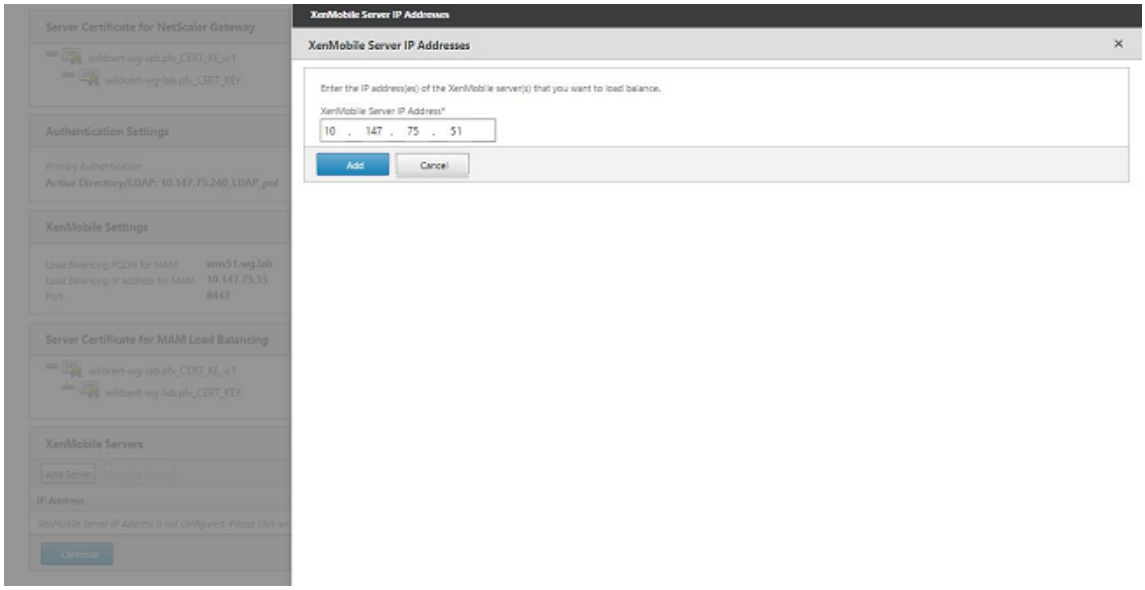


> **Nota:**
>
> Compruebe que el nombre de dominio completo perteneciente a la dirección IP virtual de equilibrio de carga para MAM y el nombre de dominio completo de XenMobile coinciden.

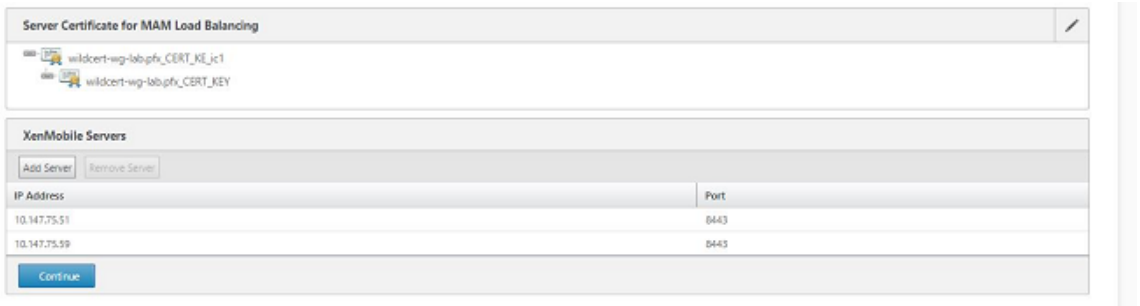
8. Si quiere utilizar el modo de puente SSL (HTTPS), seleccione **HTTPS communication to XenMobile Server**. Sin embargo, si quiere utilizar la descarga de SSL, seleccione **HTTP communication to XenMobile Server**, como se muestra en la imagen anterior. Dada la finalidad de este artículo, se opta por el modo de puente SSL (HTTPS).
9. Vincule el certificado de servidor para la dirección IP virtual de equilibrio de carga de MAM y haga clic en Continue.

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

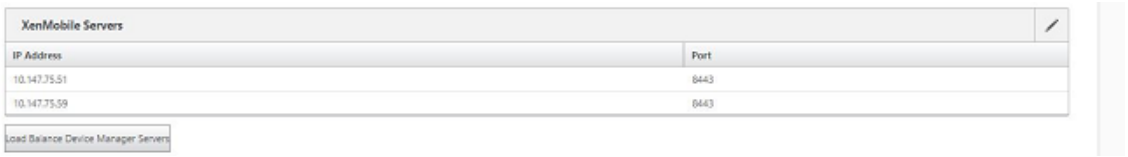
11. Escriba la dirección IP del nodo de XenMobile y haga clic en Add.



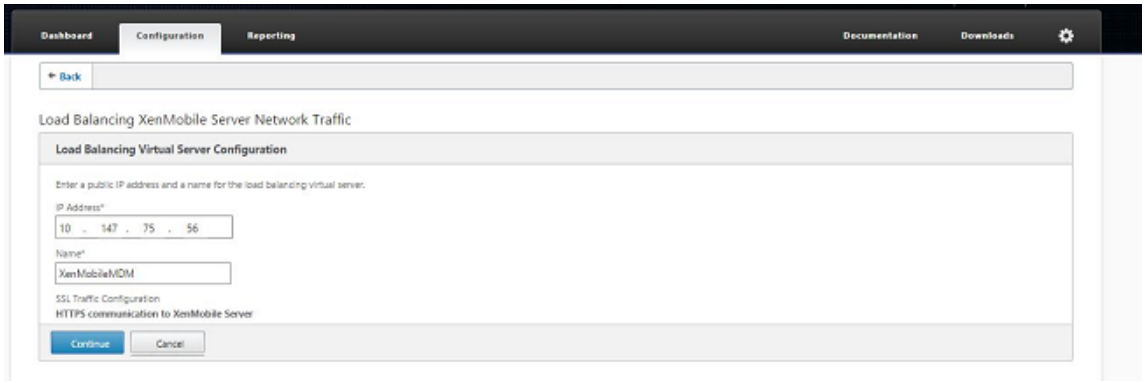
12. Repita los pasos 10 y 11 para agregar nodos de XenMobile adicionales que formen parte del clúster de XenMobile. Verá todos los nodos de XenMobile que haya agregado. Haga clic en Continue.



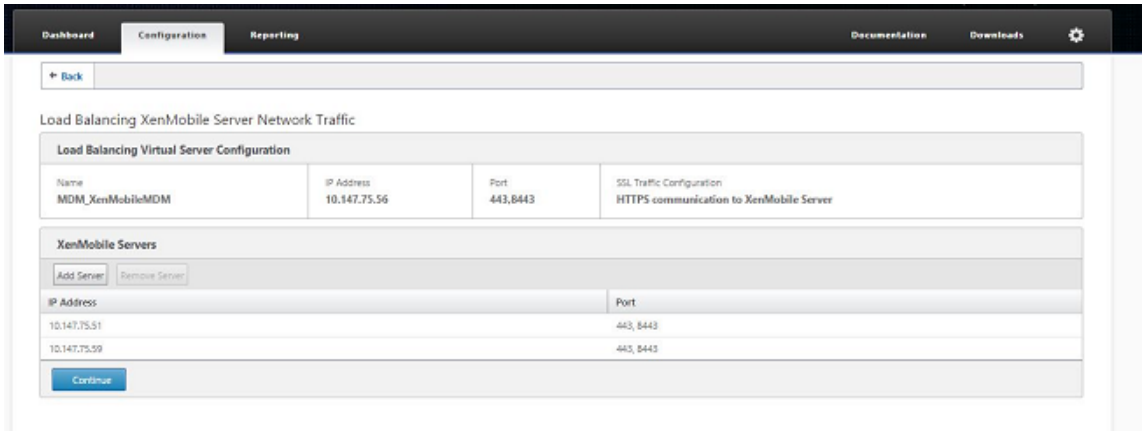
13. Haga clic en **Load Balance Device Manager Servers** para continuar con la configuración del equilibrio de carga de MDM.



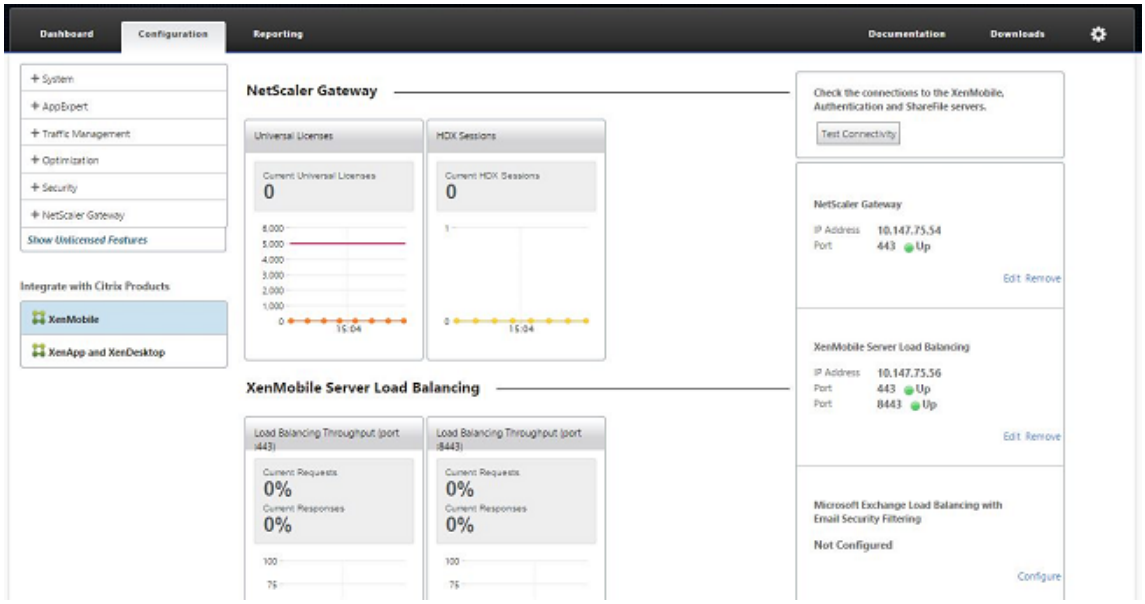
14. Indique la dirección IP que se usará como la dirección IP de equilibrio de carga de MDM y haga clic en **Continue**.



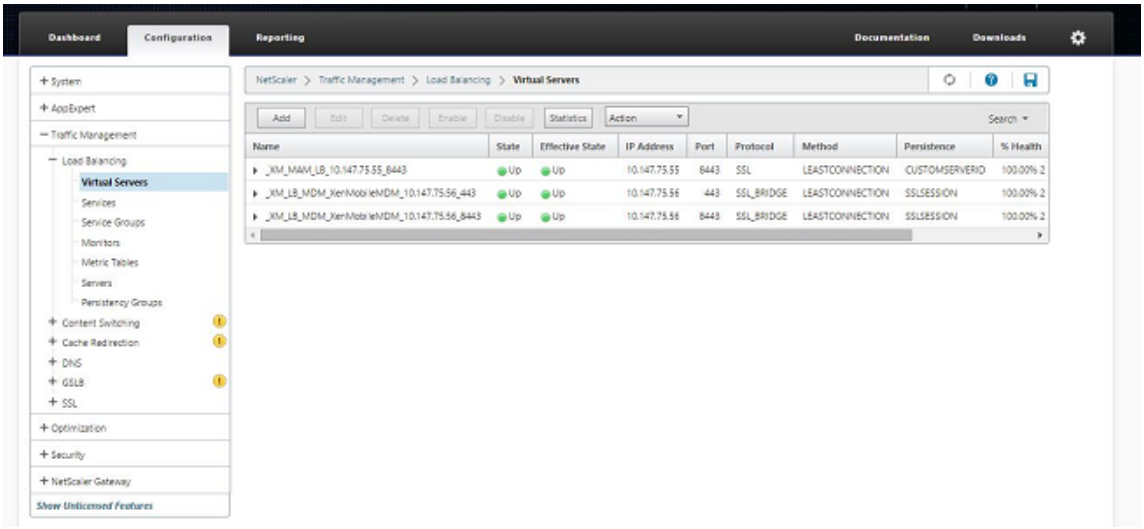
15. Cuando vea los nodos de XenMobile en la lista, haga clic en **Continue** y, a continuación, en "Done" para finalizar el proceso.



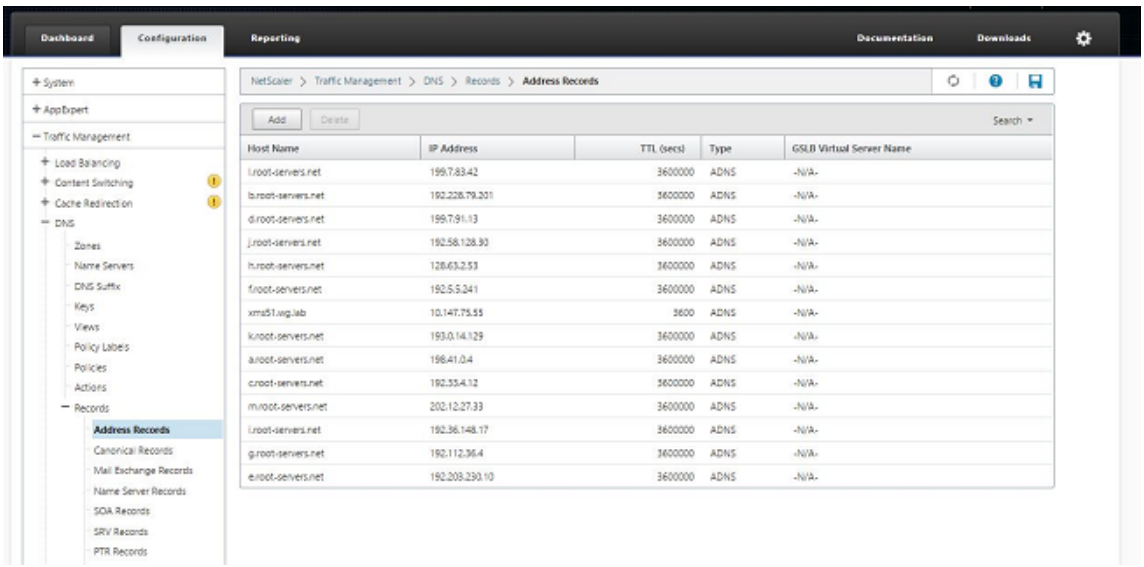
Verá el estado de la dirección IP virtual en la página de XenMobile.



16. Para confirmar que las direcciones IP virtuales funcionan, haga clic en la ficha Configuration y vaya a **Traffic Management > Load Balancing > Virtual Servers**.



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



Guía de recuperación ante desastres

January 4, 2022

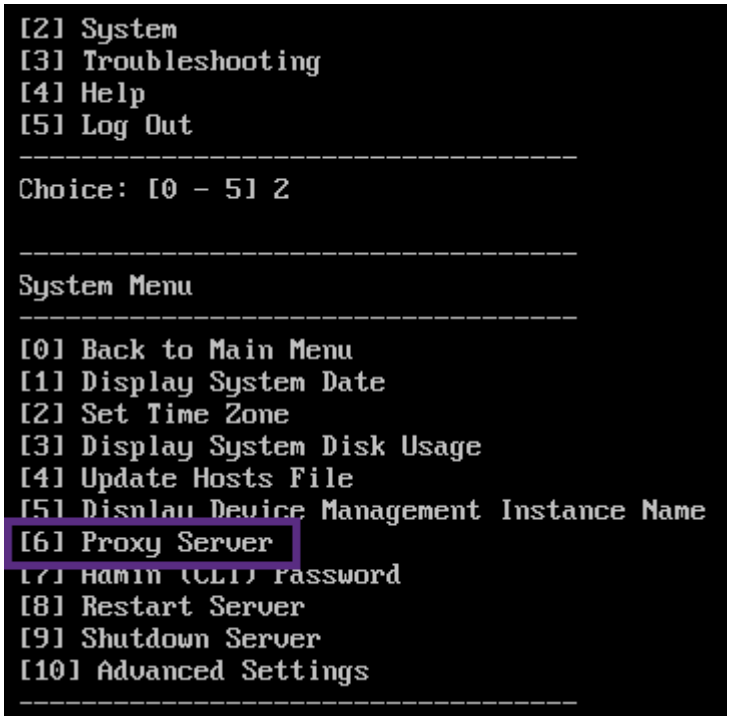
Puede planificar y configurar implementaciones de XenMobile que contengan varios sitios para la recuperación ante desastres con la ayuda de una estrategia de conmutación por error desde el sitio activo al sitio pasivo. Para obtener más información, consulte el artículo Disaster Recovery de XenMobile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

Habilitar servidores proxy

January 4, 2022

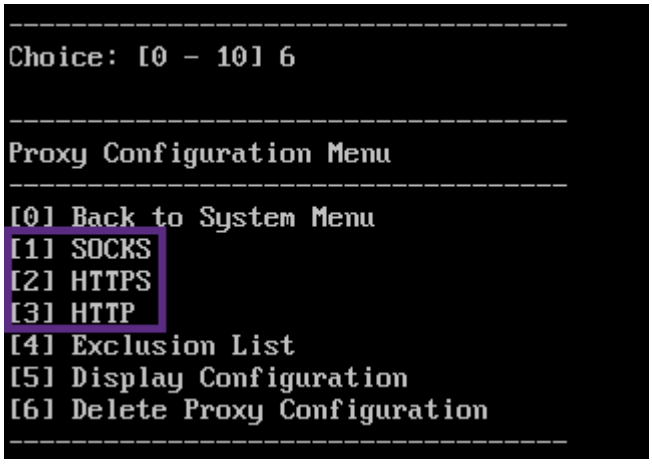
Para controlar el tráfico saliente a Internet, puede configurar un servidor proxy en XenMobile para transportar dicho tráfico. Para ello, configure el servidor proxy mediante la interfaz de línea de comandos (CLI). Tenga en cuenta que la configuración del servidor proxy requiere reiniciar el sistema.

1. En el menú principal de la interfaz de línea de comandos de XenMobile, escriba **2** para seleccionar el menú de sistema.
2. En el menú de sistema, escriba **6** para seleccionar el menú de servidor proxy.



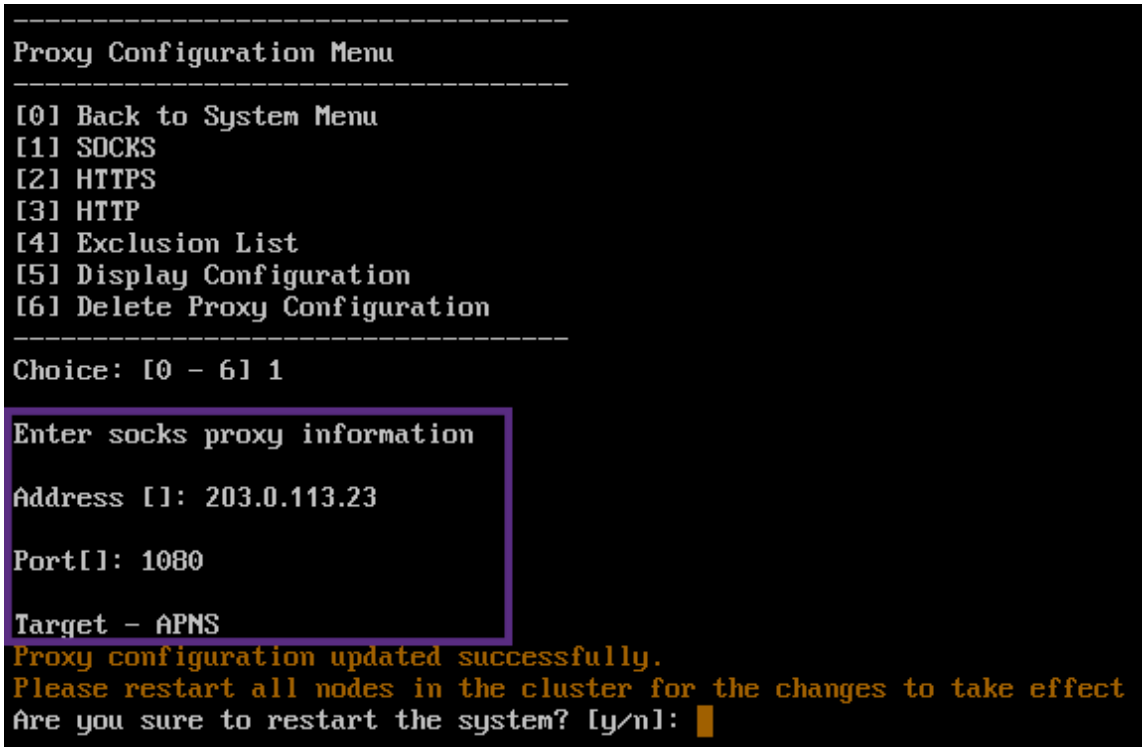
3. En el menú de configuración de proxy, escriba **1** para seleccionar SOCKS.

   Antes de guardar esta configuración, también debe configurar HTTPS. El proxy no funcionará a menos que guarde los parámetros de SOCKS y HTTPS en la misma configuración.

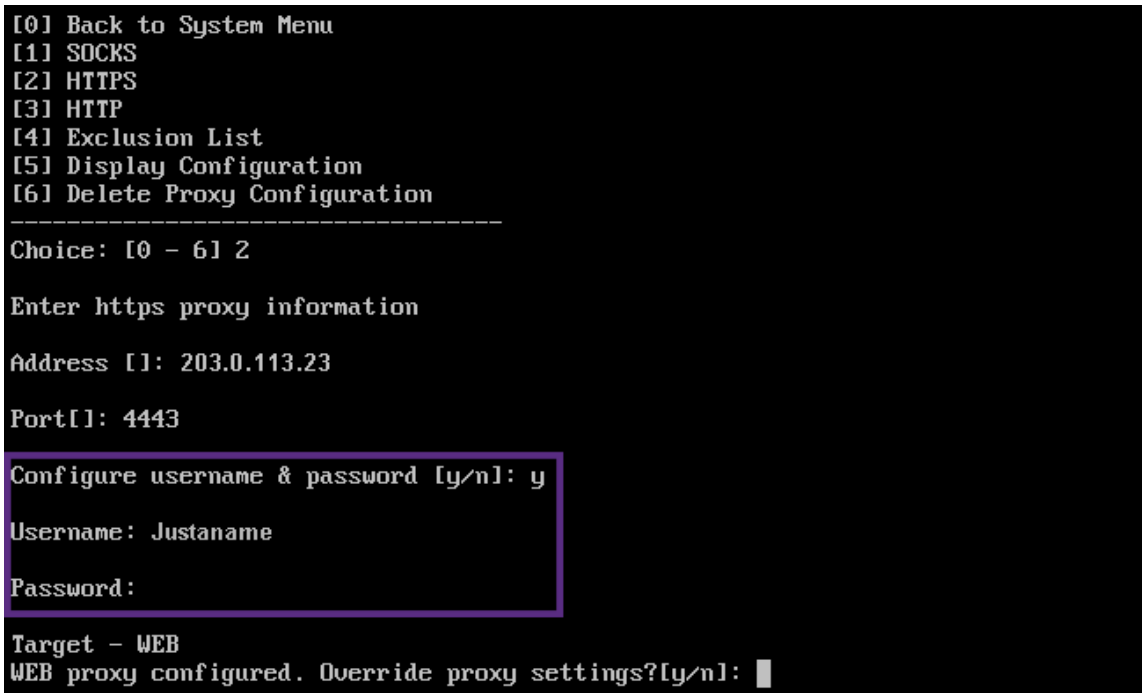


4. Introduzca la dirección IP del servidor proxy, el número de puerto y el destino. Consulte la tabla siguiente para ver los tipos de destino admitidos para cada tipo de servidor proxy.

Tipo de proxy	Destinos admitidos
SOCKS	APNs
HTTP	APNS, web, PKI
HTTPS	Web, PKI
HTTP con autenticación	Web, PKI
HTTPS con autenticación	Web, PKI



5. Escriba **n**, escriba **2** para seleccionar HTTPS y, a continuación, escriba la dirección IP, el número de puerto y el destino del servidor proxy.
6. Si elige configurar un nombre de usuario y una contraseña como método de autenticación en el servidor proxy, escriba **y**. A continuación, escriba el nombre de usuario y la contraseña.



7. Escriba **y** para guardar la configuración.

Configurar SQL Server

January 4, 2022

Para las conexiones a SQL Server desde XenMobile Server local, puede utilizar cualquiera de los controladores siguientes:

- El controlador predeterminado
- jTDS
- Controlador JDBC (Java Database Connectivity) de Microsoft

El controlador jTDS es el predeterminado cuando:

- Instala XenMobile Server local.
- Actualiza desde un servidor de XenMobile Server que está configurado para usar el controlador jTDS.

Para ambos controladores, XenMobile admite la autenticación de Windows o la autenticación de SQL Server. Para esas combinaciones de controlador y autenticación, SSL puede estar activado o desactivado.

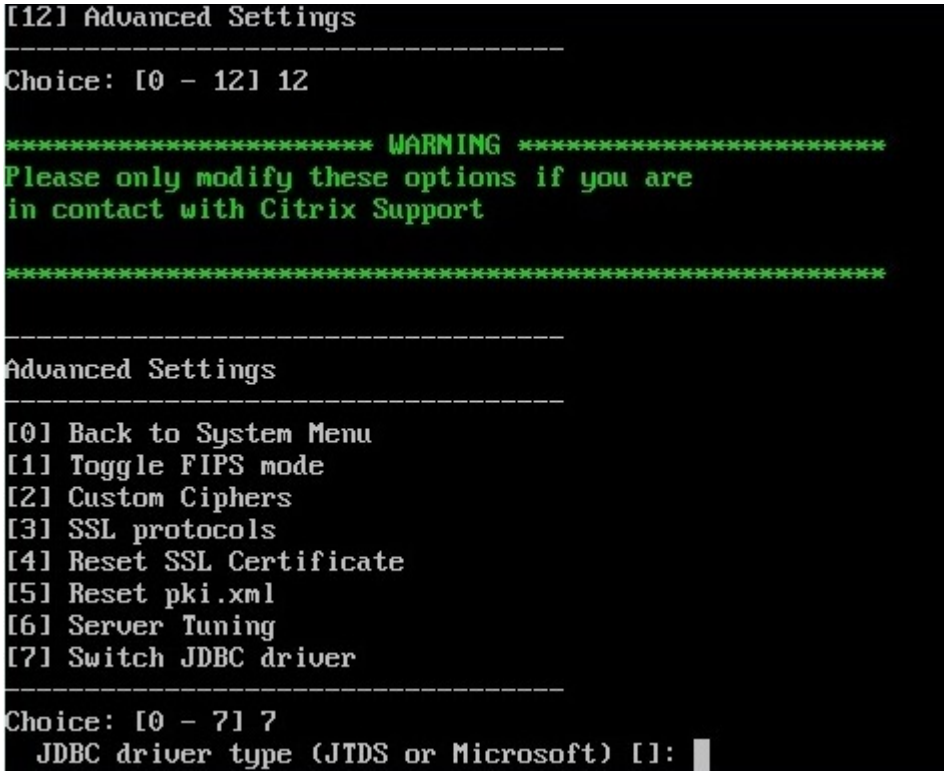
Cuando se utiliza la autenticación de Windows con el controlador JDBC de Microsoft, el controlador utiliza la autenticación integrada con Kerberos. XenMobile contacta con Kerberos para obtener los detalles del Centro de distribución de claves (KDC) de Kerberos. Si los detalles necesarios no están disponibles, la CLI de XenMobile pide la dirección IP del servidor de Active Directory.

Para pasar del controlador jTDS al controlador JDBC, utilice SSH en todos los nodos de XenMobile Server y la CLI de XenMobile para la configuración. Los pasos varían según la configuración actual del controlador jTDS, como se indica a continuación.

Cambiar a Microsoft JDBC (autenticación de SQL Server)

Para completar estos pasos, necesita el nombre de usuario y la contraseña del servidor SQL.

1. Use SSH para todos los nodos del servidor de XenMobile Server.
2. En el menú principal de la interfaz de línea de comandos de XenMobile, escriba **2** para seleccionar el **menú de sistema**.
3. Escriba **12** para seleccionar los parámetros avanzados.
4. Escriba **7** para seleccionar el cambio de controlador JDBC y, a continuación, escriba **m** para Microsoft.



5. Cuando se le pida, escriba **y** para elegir la autenticación de SQL y, a continuación, escriba el nombre de usuario y la contraseña del servidor SQL.
6. Repita los pasos para cada nodo del servidor de XenMobile Server.
7. Reinicie cada nodo del servidor de XenMobile Server.

Cambiar a Microsoft JDBC (SSL desactivado, autenticación de Windows)

Para completar estos pasos, necesita el nombre de usuario y la contraseña de Active Directory, así como el territorio del centro KDC y el nombre de usuario del centro KDC de Kerberos.

1. Use SSH para todos los nodos del servidor de XenMobile Server.
2. En el menú principal de la interfaz de línea de comandos de XenMobile, escriba **2** para seleccionar el **menú de sistema**.
3. Escriba **12** para seleccionar los parámetros avanzados.
4. Escriba **7** para seleccionar el cambio de controlador JDBC y, a continuación, escriba **m**.
5. Cuando se le pregunte si quiere utilizar la autenticación de SQL Server, escriba **n**.
6. Cuando se le pida, escriba el nombre de usuario y la contraseña de Active Directory configurados para el servidor SQL.
7. Si XenMobile no detecta automáticamente el territorio del centro KDC de Kerberos, pedirá los datos de ese centro, incluido el FQDN del servidor SQL.

8. Cuando se le pregunte si quiere utilizar SSL, escriba **n**. XenMobile guarda la configuración. Si XenMobile no puede guardar la configuración debido a errores en la operación, aparecerá un mensaje de error y los datos que escribió.
9. Repita los pasos para cada nodo del servidor de XenMobile Server.
10. Reinicie cada nodo del servidor de XenMobile Server.

Para cambiar la contraseña de la base de datos de XenMobile

Siga estas instrucciones para cambiar la contraseña de la base de datos de XenMobile; por ejemplo, cuando Citrix Support le indica que realice un cambio de contraseña.

Si su servidor SQL usa la autenticación de Windows, realice los cambios de contraseña de la base de datos en Windows Active Directory. A continuación, actualice la cuenta del administrador de la base de datos en el servidor de base de datos para sincronizar el cambio de contraseña. Ahora puede cambiar la contraseña en XenMobile de la siguiente manera.

> **Importante:**
>
> - Planifique un período de mantenimiento programado para cambiar la contraseña de la base de datos en XenMobile. El cambio de contraseña debe ocurrir durante el tiempo de inactividad del sistema.
> - Cuando cambie la contraseña, todos los nodos de XenMobile deben estar conectados a la red. Después de cambiar la contraseña, reinicie XenMobile.
>
>   If you don't restart XenMobile after a password change, XenMobile goes into recovery mode. In that case, revert to the old password in SQL server, restart XenMobile, and change the password again.

1. Verifique que todos los nodos del servidor de XenMobile Server se estén ejecutando. Para un entorno agrupado en clústeres, todos los nodos deben estar iniciados y en funcionamiento.
2. Bloquee el tráfico entrante de los dispositivos a XenMobile en el equilibrador de carga de Citrix ADC. Para ello, inhabilite el servidor virtual.
3. Para cambiar la contraseña de la base de datos en el servidor SQL, inicie sesión en la CLI de XenMobile, vaya a **Configuración > Base de datos** y escriba la contraseña modificada cuando se le solicite:

```
Server []: <ipAddress>
Port [1433]: 1433
Username [sa]: <userName>
Password: <****>
<!--NeedCopy-->
```


4. Escoja **Y** para reiniciar el servidor.
5. Repita los pasos 3 y 4 para todos los demás nodos del clúster.
6. Para desbloquear el tráfico de dispositivos entrantes, habilite el servidor virtual en el equilibrador de carga de Citrix ADC.

Propiedades de servidor

January 4, 2022

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

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

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

Definiciones de las propiedades de servidor

Agregar dispositivo siempre

- Si tiene el valor **verdadero**, XenMobile agrega un dispositivo a la consola de XenMobile, incluso aunque falle la inscripción. De esta manera, puede ver qué dispositivos intentaron inscribirse. El valor predeterminado es **false**.

Intervalo de limitación de emisión de certificados cliente de AG

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

Hora de ejecución de la limpieza de registros de auditoría

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

Intervalo de limpieza de registros de auditoría (días)

- La cantidad de días que XenMobile conserva los registros de auditoría. El valor predeterminado es **1**.

Registrador de auditoría

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

Retención de registros de auditoría (días)

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

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

- Para compensar las respuestas LDAP lentas, Citrix recomienda que agregue propiedades de servidor a las siguientes claves personalizadas.
  - Clave: **Clave personalizada**
  - Clave: **auth.ldap.connect.timeout**
  - Valor: **60000**
  - Nombre simplificado: **auth.ldap.connect.timeout**
  - Descripción: **Tiempo de espera de la conexión LDAP**
  - Clave: **Clave personalizada**
  - Clave: **auth.ldap.read.timeout**
  - Valor: **60000**
  - Nombre simplificado: **auth.ldap.read.timeout**
  - Descripción: **Tiempo de lectura de la conexión LDAP**

Renovación de certificado (en segundos)

- Especifica con cuántos segundos de antelación XenMobile empieza a renovar certificados previamente a su caducidad. Por ejemplo, si un certificado caduca el 30 de diciembre y esta propiedad está establecida en 30 días, XenMobile intenta renovar el certificado si el dispositivo se conecta entre el 1 de diciembre y el 30 de diciembre. El valor predeterminado es **2 592 000** segundos (30 días).

Tiempo de espera de la conexión

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

Tiempo de espera de conexión con Microsoft Certification Server

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

Canal de implementación predeterminado

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

Limpieza de registros de Implementación (días)

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

Inhabilitar la verificación de nombres de host

- De forma predeterminada, la verificación de nombres de host está habilitada en las conexiones salientes, excepto para el servidor PKI de Microsoft. Cuando se produce un error en la verificación de nombres de host, el registro del servidor contiene errores del tipo: "No se puede conectar con el servidor de compras por volumen: El nombre de host '192.0.2.0' no coincide con el sujeto de certificado suministrado por el servidor homólogo". Si la verificación de nombres de host deja inoperativa la implementación, cambie esta propiedad a **true**. El valor predeterminado es **false**.

Inhabilitar verificación del servidor SSL

- Si tiene el valor **true**, inhabilita la validación de certificados SSL de servidor cuando se cumplen todas las condiciones siguientes:
  - Ha habilitado la autenticación basada en certificados en XenMobile Server
  - El servidor de CA de Microsoft es el emisor del certificado
  - XenMobile Server no confía en la raíz de la CA interna que ha firmado el certificado.

El valor predeterminado es **true**.

Habilitar consola

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

Enable Crash Reporting (Habilitar informes de errores)

- Si tiene el valor **true**, Citrix recopila informes de errores y diagnósticos para ayudar a solucionar problemas con Secure Hub para iOS y Android. Si el valor es **false**, no se recopilan datos. El valor predeterminado es **true**.

Habilitar/inhabilitar la captura de registros de estadísticas de Hibernate para diagnósticos

- Si tiene el valor **true**, se habilita la captura de estadísticas de Hibernate 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 macOS OTAE (Habilitar OTAE de macOS)

- Si tiene el valor **false**, impide que se use un enlace de inscripción para dispositivos macOS, lo que significa que los usuarios de macOS solo pueden inscribirse con una invitación de inscripción. El valor predeterminado es **true**.

Habilitar desencadenante de notificaciones

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

force.server.push.required.apps

- Permite la implementación forzosa de las aplicaciones obligatorias en dispositivos iOS y Android en situaciones como, por ejemplo:
  - Se carga una nueva aplicación y se marca como obligatoria.
  - Se marca una aplicación existente como obligatoria.

  - Un usuario elimina una aplicación obligatoria.
  - Hay una actualización de Secure Hub disponible.

La implementación forzosa de las aplicaciones obligatorias tiene el valor **false** de forma predeterminada. Cree la clave personalizada y establezca el **Valor** en **true** para habilitar la implementación forzosa. Durante la implementación forzosa, las aplicaciones obligatorias habilitadas con MDX, incluidas las aplicaciones empresariales y las aplicaciones de tiendas públicas, se actualizan de inmediato. La actualización se produce incluso si configura una directiva MDX para un periodo de gracia de actualización de la aplicación y el usuario elige actualizar la aplicación más tarde.

- Clave: **Clave personalizada**
- Clave: **force.server.push.required.apps**
- Valor: **false**
- Nombre simplificado: **force.server.push.required.apps**
- Descripción: **Forzar la implementación forzosa de las aplicaciones obligatorias**

Extracción completa de usuarios permitidos y prohibidos de ActiveSync

- El intervalo (en segundos) tras el que XenMobile extrae una lista completa (referencia) de los usuarios permitidos y denegados de ActiveSync. El valor predeterminado es **28800** segundos.

hibernate.c3p0.idle_test_period

- Esta propiedad de XenMobile Server, una clave personalizada (Custom Key), determina el tiempo de inactividad, en segundos, antes de que se valide automáticamente una conexión. Configure la clave de este modo. El valor predeterminado es **30**.
- Clave: **Clave personalizada**
- Clave: **hibernate.c3p0. idle_test_period**
- Valor: **30**
- Nombre simplificado: **hibernate.c3p0. idle_test_period =*nnn***
- Descripción: **Período de prueba para el tiempo de espera antes de hibernar**

hibernate.c3p0.max_size

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

- Clave: **hibernate.c3p0.max_size**
- Valor: **1000**
- Nombre simplificado: **hibernate.c3p0.max_size**
- Descripción: **Conexiones de base de datos a SQL**

hibernate.c3p0.min_size

- Esta clave personalizada determina la cantidad mínima de conexiones a la base de datos de SQL Server que puede abrir XenMobile. Configure la clave de este modo. El valor predeterminado es **100**.
- Clave: **hibernate.c3p0.min_size**
- Valor: **100**
- Nombre simplificado: **hibernate.c3p0.min_size**
- Descripción: **Conexiones de base de datos a SQL**

hibernate.c3p0.timeout

- Esta clave personalizada determina el tiempo de espera de inactividad en segundos. El valor predeterminado es **120**.
- Clave: **Clave personalizada**
- Clave: **hibernate.c3p0.timeout**
- Valor: **120**
- Nombre simplificado: **hibernate.c3p0.timeout**
- Descripción: **Tiempo de espera de inactividad que tiene la base de datos**

Identifica si la telemetría está habilitada o no

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

Tiempo de espera de inactividad en minutos

- Si la propiedad de servidor web **Services timeout type** (Tipo de tiempo de espera de los servicios web) es **INACTIVITY_TIMEOUT**, esta propiedad define la cantidad de minutos tras los que XenMobile cierra la sesión de un administrador inactivo que haya hecho lo siguiente:

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

El valor predeterminado es **5**.

Instalación automática de inscripción de administración de dispositivos iOS habilitada

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

Inscripción en administración de dispositivos iOS: Demora de la primera etapa

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

Inscripción en administración de dispositivos iOS: Demora de la última etapa

- 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).

Administración de dispositivos iOS: Modo de entrega de identidad

- 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**.

Administración de dispositivos iOS: Tamaño de clave de identidad

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

Administración de dispositivos iOS: Días de renovación de identidad

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

Contraseña de clave privada de APNS de iOS MDM

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

Período de inactividad antes de desconectar el dispositivo

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

MAM Only Device Max (Máximo de dispositivos administrados por MAM)

- Esta clave personalizada limita la cantidad de dispositivos de solo MAM que puede inscribir un usuario. Configure la clave de este modo. Un **valor** de **0** permite inscripciones ilimitadas de dispositivos.
- Clave = **number.of.mam.devices.per.user**
- Valor = **5**
- Nombre simplificado = **MAM Only Device Max**
- Descripción = **Limita la cantidad de dispositivos MAM que cada usuario puede inscribir.**

MaxNumberOfWorker

- La cantidad de subprocesos que se utilizan cuando se importa una gran cantidad de licencias de compras por volumen. El valor predeterminado es **3**. Si necesita mayor optimización, puede aumentar la cantidad de subprocesos. No obstante, con una mayor cantidad de subprocesos (por ejemplo, 6), una importación de compras por volumen consume mucha CPU.

Single Sign-On de Citrix ADC

- Si el valor es **False**, se inhabilita la función de respuesta de XenMobile durante el inicio Single Sign-On desde Citrix ADC a XenMobile. XenMobile usa la función de respuesta para verificar el ID de sesión de Citrix Gateway si la configuración de Citrix Gateway incluye una dirección URL de respuesta. El valor predeterminado es **False**.

Cantidad de cargas fallidas consecutivas

- Muestra la cantidad de fallos consecutivos durante cargas de Customer Experience Improvement Program (CEIP). XenMobile aumenta el valor cuando falla una carga. Después de 15 fallos de carga, XenMobile inhabilita el programa CEIP, también conocido como "telemetría". Para obtener más información, consulte la propiedad de servidor **Identifica si la telemetría está habilitada o no**. XenMobile restablece el valor a **0** si una carga se realiza correctamente.

Cantidad de usuarios por dispositivo

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

Extracción de cambios incrementales de usuarios permitidos y prohibidos

- 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 **60** segundos.

Tiempo de espera de lectura de Microsoft Certification Server

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

REST Web Services (Servicios web de REST)

- Permite el servicio web de REST. El valor predeterminado es **true**.

Obtiene información de dispositivos en fragmentos de un tamaño especificado

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

Limpieza de registros de sesiones (días)

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

Modo de servidor

- Determina si XenMobile se ejecuta en modo MAM, MDM o ENT (Enterprise), que corresponden a los modos Administración de aplicaciones, Administración de dispositivos o Administración de dispositivos y aplicaciones respectivamente. Defina la propiedad Modo de servidor 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 "Propiedades de servidor". Si tiene una licencia de MDM Edition, no puede habilitar la administración de aplicaciones definiendo el modo del servidor en MAM o ENT.

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

El modo efectivo de servidor es una combinación del tipo de licencia y del modo del servidor. Para una licencia MDM, el modo efectivo del servidor es siempre MDM, independientemente de cómo esté configurado el parámetro de modo del servidor. Para licencias Enterprise y Advanced, el modo efectivo del servidor coincide con el modo del servidor si el modo de servidor es **ENT** o **MDM**. Si el modo de servidor es **MAM**, el modo efectivo de servidor es ENT.

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

Tipo de configuración de Content Collaboration

- Especifica el tipo de almacenamiento de Citrix Files. **ENTERPRISE** habilita el modo Citrix Files Enterprise. **CONNECTORS** solo ofrece acceso a los conectores de zonas de almacenamiento que

haya creado desde la consola de XenMobile. El valor predeterminado es **NONE**, lo que muestra la vista inicial de la pantalla **Configurar > ShareFile**, desde donde elige entre los conectores y Citrix Files Enterprise. El valor predeterminado es **NONE**.

Tiempo de espera estático en minutos

- Si la propiedad de servidor **Tipo de tiempo de espera de los servicios web** es **STATIC_TIMEOUT**, esta propiedad define la cantidad de minutos tras los que XenMobile cierra la sesión de un administrador que haya utilizado:
  - La API pública de XenMobile para servicios REST para acceder a la consola de XenMobile.
  - La API pública de XenMobile para servicios REST para acceder a una aplicación de terceros.

El valor predeterminado es **60**.

Desencadenar supresión de mensajes del agente

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

Desencadenar supresión de sonido del agente

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

Descarga de aplicaciones no autenticada para dispositivos Android

- Si el valor es **True**, se pueden descargar aplicaciones autoalojadas en dispositivos Android que ejecutan Android Enterprise. XenMobile necesita esta propiedad si la opción de Android Enterprise 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 **Tíquet XAM de uso único**) que tiene el token de autenticación. El valor predeterminado es **False**.

Descarga de aplicaciones no autenticada para dispositivos Windows

- 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**.

Usar ID de ActiveSync para realizar un borrado de dispositivo ActiveSync

- Si el valor es **True**, el conector de Endpoint Management para Exchange ActiveSync usa el identificador de ActiveSync como argumento para el método asWipeDevice. El valor predeterminado es **false**.

Propiedades del dispositivo definidas por el usuario N

- Se utiliza solo para dispositivos Windows CE. Esta clave personalizada permite obtener las propiedades que se crearon en el registro de los dispositivos Windows CE. Cuando esas propiedades consten en la base de datos de XenMobile, puede crear reglas de implementación según el valor de las propiedades.
- Clave: **Clave personalizada**
- Clave: **device.properties.userDefinedN**
- Valor: *administrator-defined*
- Nombre simplificado: *administrator-defined*
- Descripción: *administrator-defined*

Usuarios de Exchange solamente

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

VP baseline interval (Intervalo para el punto de referencia de VP)

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

Si tiene una gran cantidad de licencias de compras por volumen instaladas (por ejemplo, más de 50.000), Citrix recomienda aumentar el intervalo del punto de referencia para reducir la frecuencia de la importación de licencias y el consumo de recursos que eso conlleva. Si espera cambios frecuentes en las licencias de compras por volumen por parte de Apple, Citrix recomienda reducir el valor para mantener XenMobile actualizado con los cambios. El intervalo mínimo entre dos puntos de referencia es de 60 minutos. Además, XenMobile lleva a cabo una importación delta cada 60 minutos, para capturar los cambios realizados desde la última importación. Por lo tanto, si el intervalo de referencia de compras por volumen es de 60 minutos, el intervalo entre los puntos de referencia puede retrasarse hasta 119 minutos.

Tipo de tiempo de espera de los servicios web

- 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 en la propiedad de servidor **Tiempo de espera estático en minutos**.

Si es **INACTIVITY_TIMEOUT**, XenMobile considera caducado un token de autenticación si el token ha permanecido inactivo durante el tiempo especificado en la propiedad de servidor **Tiempo de espera de inactividad en minutos**. El valor predeterminado es **STATIC_TIMEOUT**.

Validez extendida de certificado MDM de Windows Phone (5 años)

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

Windows WNS Channel - Number of Days Before Renewal (Canal Windows WNS: Cantidad de días antes de la renovación)

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

Windows WNS Heartbeat Interval (Intervalo de latido de Windows WNS)

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

Tíquet XAM de uso único

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

Intervalo máximo de inactividad para la consola del portal Self-Help Portal de XenMobile MDM (en minutos)

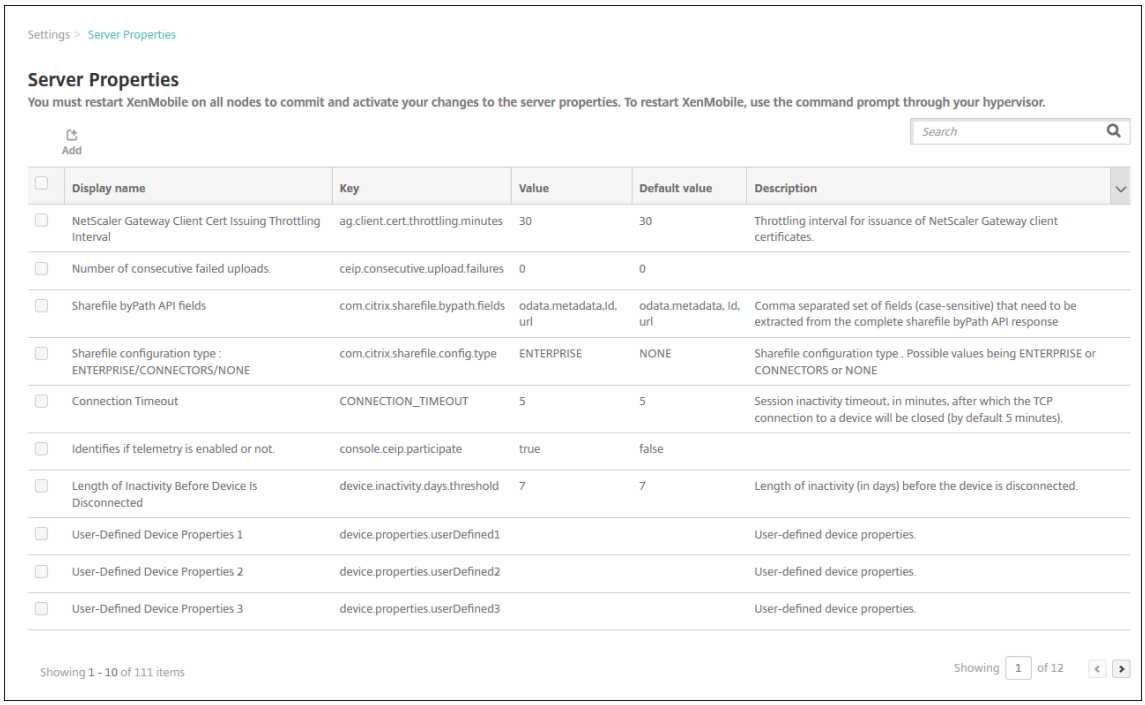
- Los minutos tras los que XenMobile cierra la sesión de un usuario inactivo en el portal Self-Help Portal de XenMobile. Un tiempo de espera de **0** significa que no se cierra la sesión del usuario inactivo. El valor predeterminado es **30**.

Agregar, modificar o eliminar propiedades de servidor

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

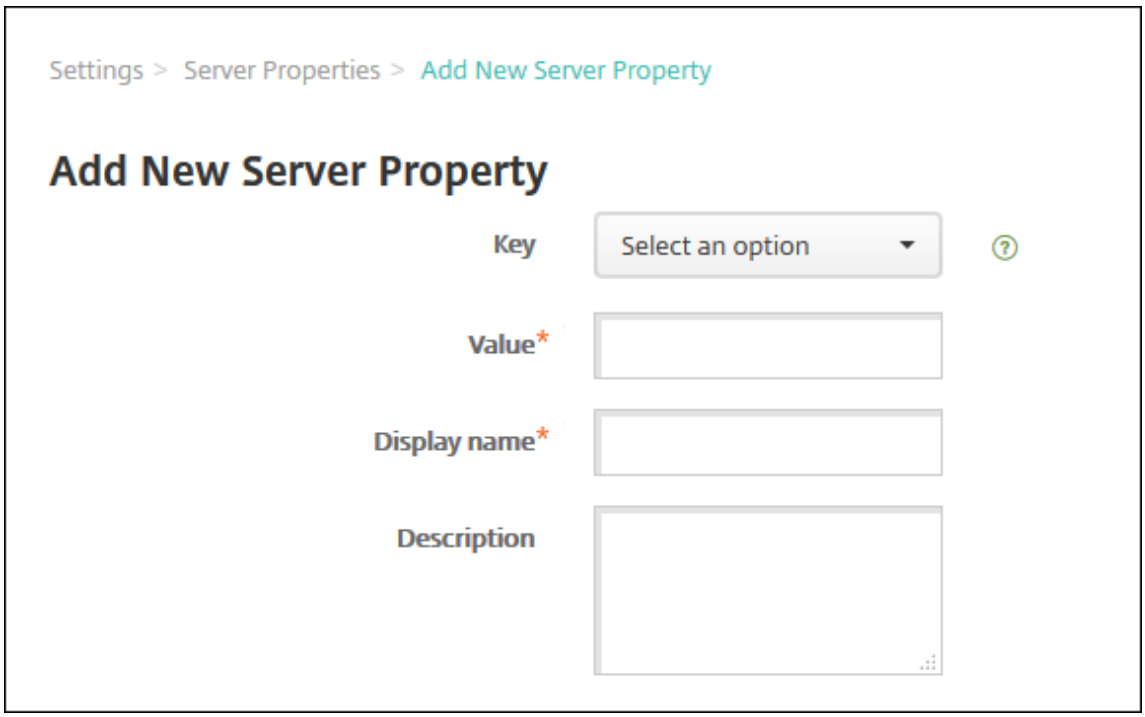
> **Nota:**
>
> Para reiniciar XenMobile, use la línea de comandos a través del hipervisor.

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



Para agregar una propiedad de servidor

1. Haga clic en **Agregar**. Aparecerá la página **Agregar nueva propiedad de servidor**.



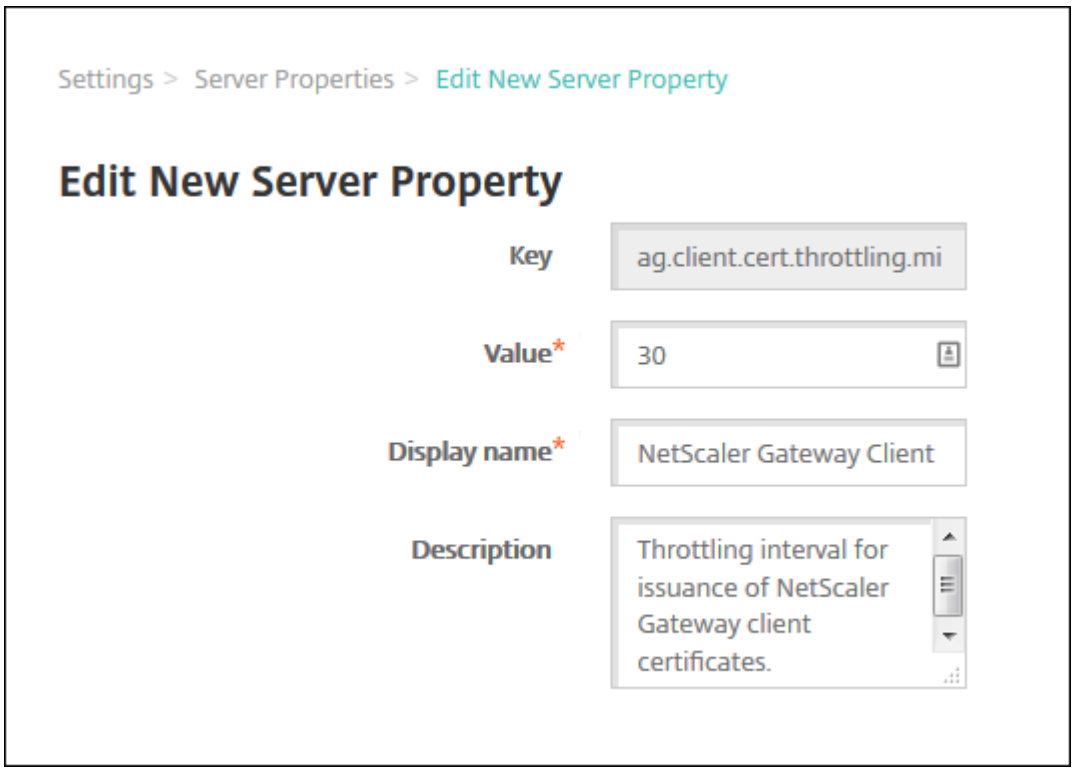
2. Configure estos parámetros:
   - Clave: En la lista, seleccione la clave apropiada. Las claves distinguen mayúsculas y minúsculas. Póngase en contacto con la asistencia de Citrix antes de modificar los valores de propiedad o para solicitar una clave especial.
   - Valor: Escriba un valor en función de la clave seleccionada.
   - Nombre simplificado: Especifique el nombre del nuevo valor de propiedad que aparece en la tabla **Propiedades de servidor**.
   - Descripción: Escriba una descripción opcional de la nueva propiedad de servidor.
3. Haga clic en **Guardar**.

Para modificar una propiedad de servidor

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

   Si marca la casilla situada junto a una propiedad de servidor, el menú de opciones aparece encima de la lista de propiedades de servidor. Haga clic en cualquier lugar de la lista para que el menú de opciones aparezca a la derecha de la lista.

2. Haga clic en **Edit**. Aparecerá la página **Modificar nueva propiedad de servidor**.



3. Cambie la siguiente información como corresponda:
   - Clave: Este campo no puede cambiarse.
   - Valor: El valor de la propiedad.
   - Nombre simplificado: El nombre de la propiedad.
   - Descripción: La descripción de la propiedad.
4. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para descartarlos.

Para eliminar una propiedad de servidor

1. En la tabla **Propiedades de servidor**, seleccione la propiedad de servidor que quiere eliminar.

   Puede eliminar más de una propiedad. Para ello, marque 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 **Eliminar**.

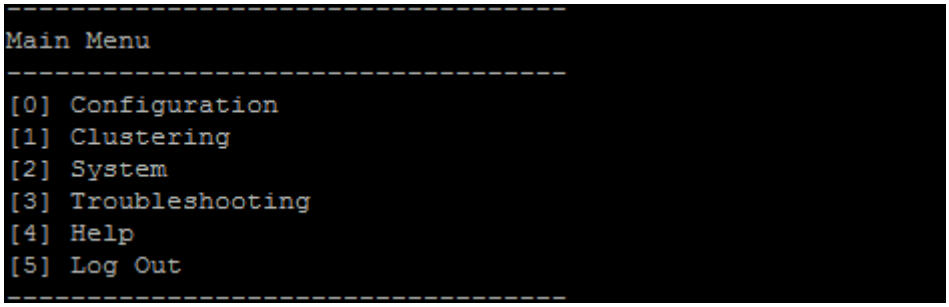
Opciones de la interfaz de línea de comandos

January 4, 2022

Para una instalación local de XenMobile Server, puede acceder a las opciones de línea de comandos de este modo:

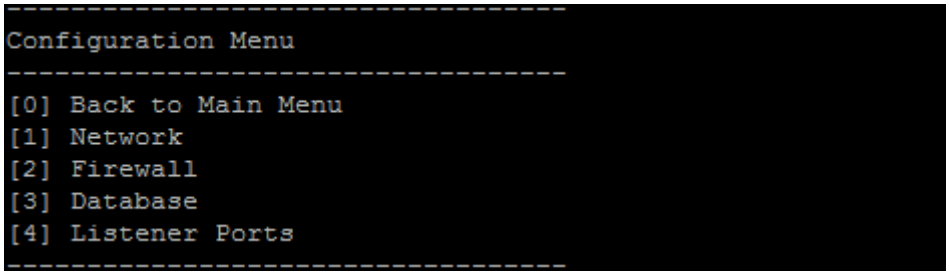
- **Desde el hipervisor donde instaló XenMobile:** En el hipervisor, seleccione la máquina virtual importada de XenMobile, inicie la vista del símbolo del sistema e inicie sesión con su cuenta de administrador de XenMobile. Para obtener información más detallada, consulte la documentación de su hipervisor.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

Puede realizar varias tareas de configuración y solución de problemas desde la línea de comandos. La siguiente imagen muestra el menú superior de la interfaz de la línea de comandos.



Opciones de Configuration

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



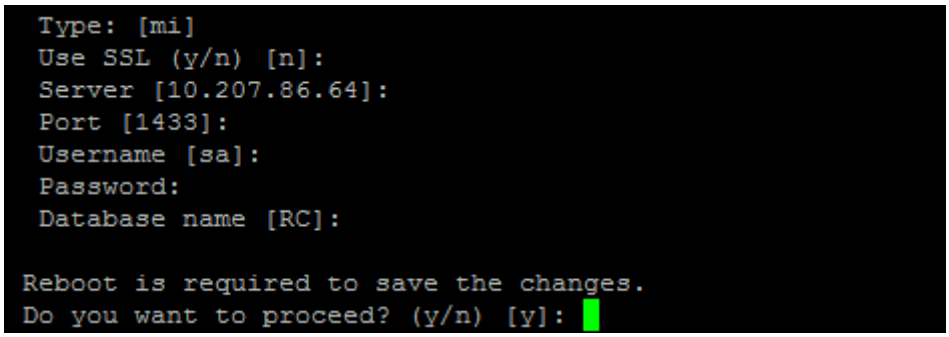
[1] Network (Red)

```
 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]:
```

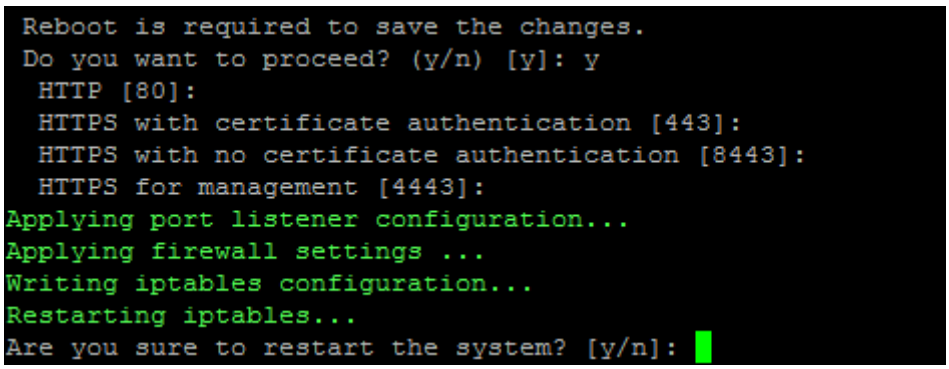
[2] Firewall

```
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)

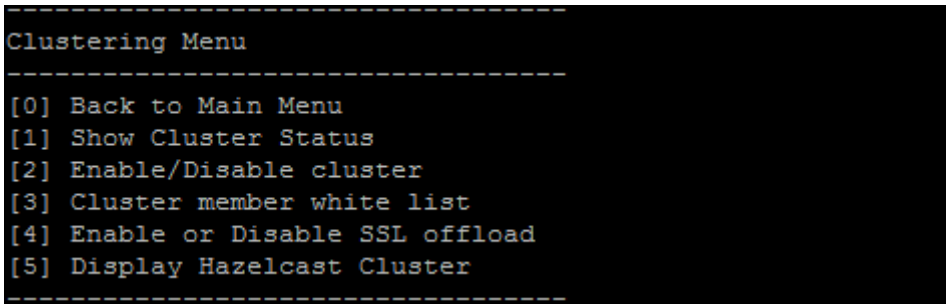


[4] Listener Ports (Puertos de escucha)

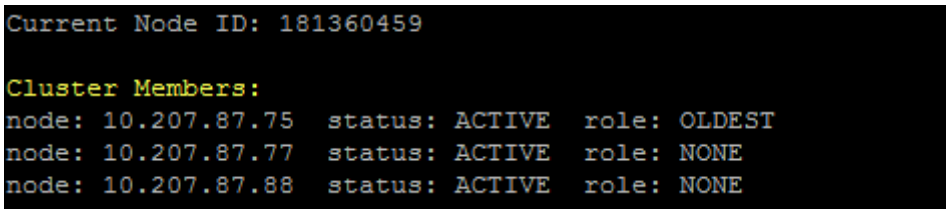


Opciones de Clustering

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



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



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

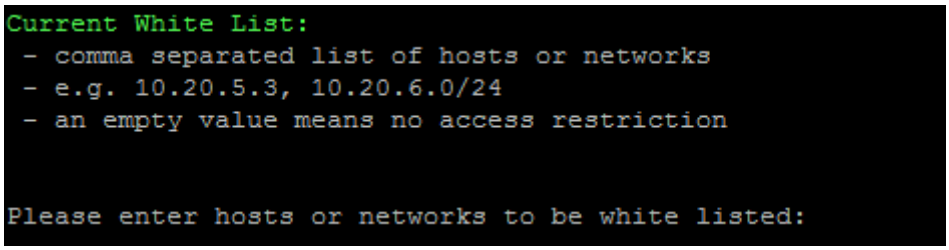
Si opta por habilitar el uso de clústeres, aparecerá el siguiente mensaje:

```
To enable real-time communication between cluster members, please open port
 80 using the Firewall menu option in CLI menu. Also configure Access white
 list under Firewall settings for restricted access.
```

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

```
You have chosen to disable clustering. Access to port 80 is not needed.
Please disable it.
```

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



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

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

```
Enabling SSL offload opens port 80 for everyone. Please configure Access
white list under Firewall settings for restricted access.
```

[5] Display Hazelcast Cluster (Mostrar clúster Hazelcast)

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

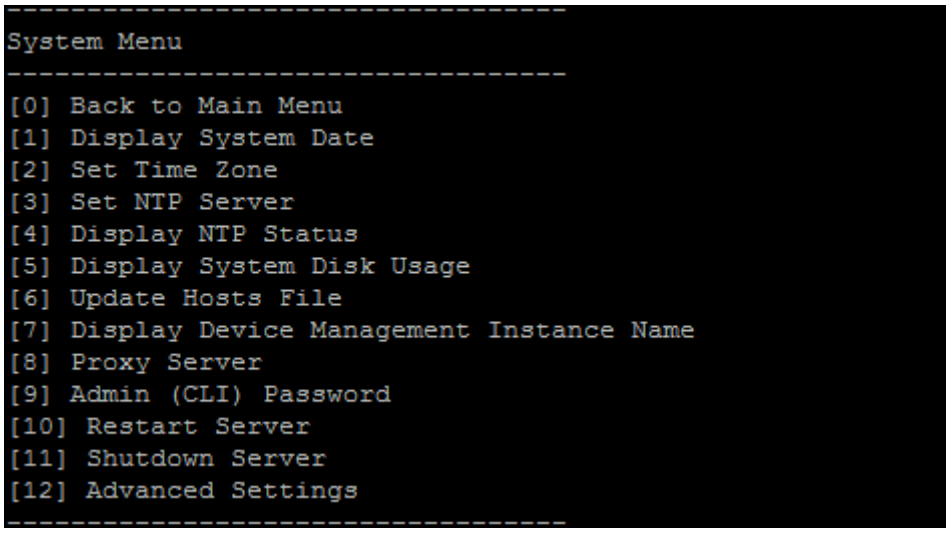
Hazelcast Cluster Members (Miembros del clúster Hazelcast):

[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 ver o configurar información a nivel del sistema, reiniciar o apagar el servidor, o bien acceder a **Advanced Settings**.



Establecer un servidor NTP permite especificar información de ese servidor. Para evitar problemas de zona horaria al sincronizar el tiempo de XenMobile con un hipervisor, apunte XenMobile a un servidor NTP. Después de cambiar esta opción, reinicie todos los servidores del clúster.

También puede comprobar el espacio en disco con el elemento de menú **[5]Mostrar uso de disco del sistema**.

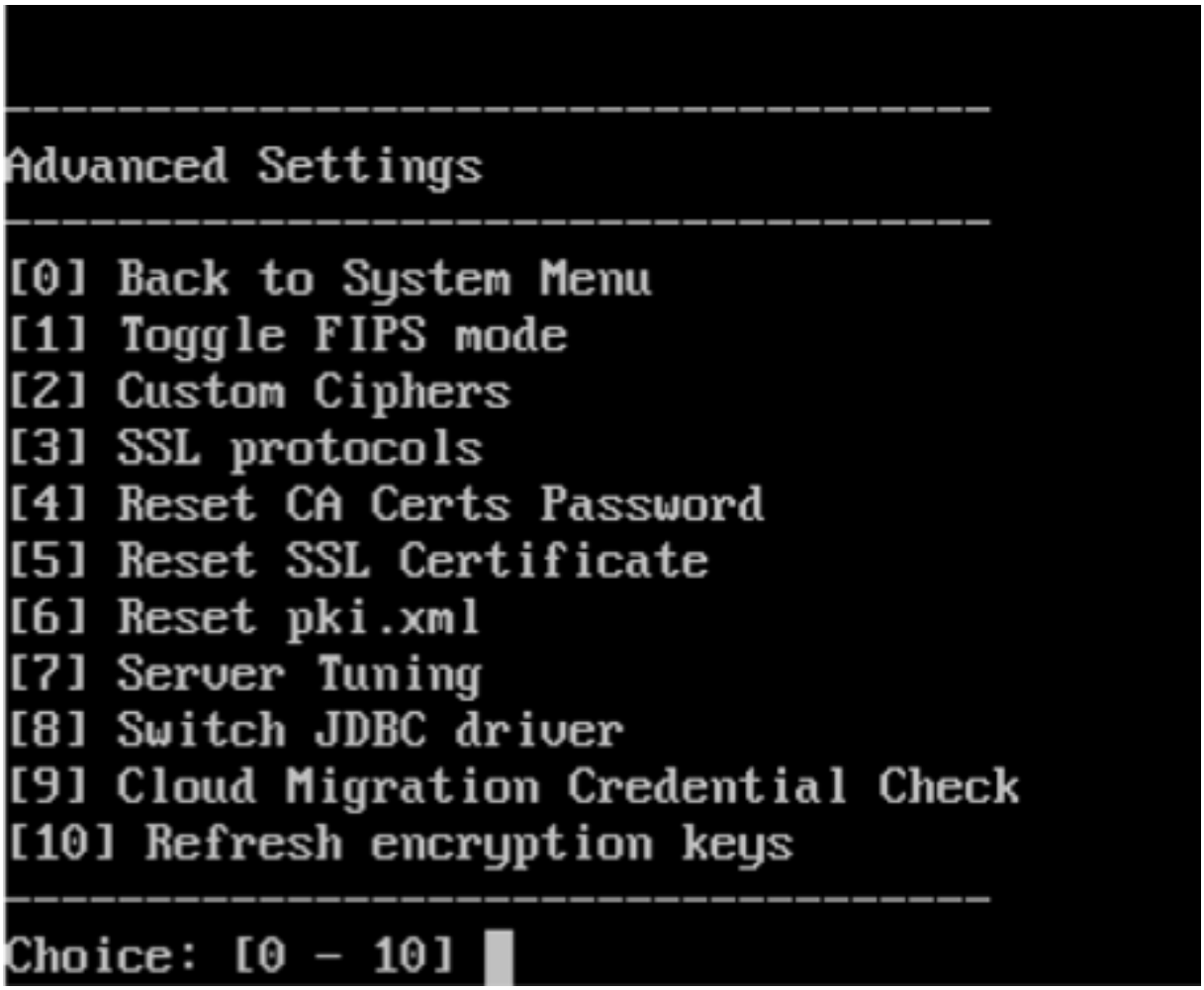
Acerca del apagado de nodos del servidor

Cuando se apaga un solo nodo de servidor en un clúster, los otros nodos generalmente pueden manejar la carga de trabajo si cumplen los requisitos que se indican en Escalabilidad y rendimiento. El impacto puede variar en función del número de nodos que estén inactivos simultáneamente, el número total de usuarios y el tiempo que los nodos estén inactivos.

- Los usuarios podrán seguir accediendo a Secure Hub y a la tienda.
- Los usuarios podrán seguir accediendo a las aplicaciones administradas implementadas e iniciarlas si uno de los nodos disponibles puede gestionar el número de usuarios. Las conexiones pueden ser más lentas, lo que resulta en comprobaciones de dispositivos más lentas.
- Las directivas de dispositivo siguen funcionando, a no ser que todos los nodos estén inactivos.

Dependiendo de los recursos y del número de dispositivos, las directivas pueden implementarse más lentamente.

[12] Advanced Settings (Parámetros avanzados)



Las opciones de **protocolos SSL** toman todos los protocolos permitidos como valor predeterminado. Después de la solicitud **New SSL protocols to enable**, escriba los protocolos que quiere habilitar. XenMobile inhabilita los protocolos que no se incluyan en la respuesta. Por ejemplo: Para inhabilitar TLSv1, escriba `TLSv1.2,TLSv1.1` y, a continuación, escriba **y** para reiniciar el servidor de XenMobile Server.

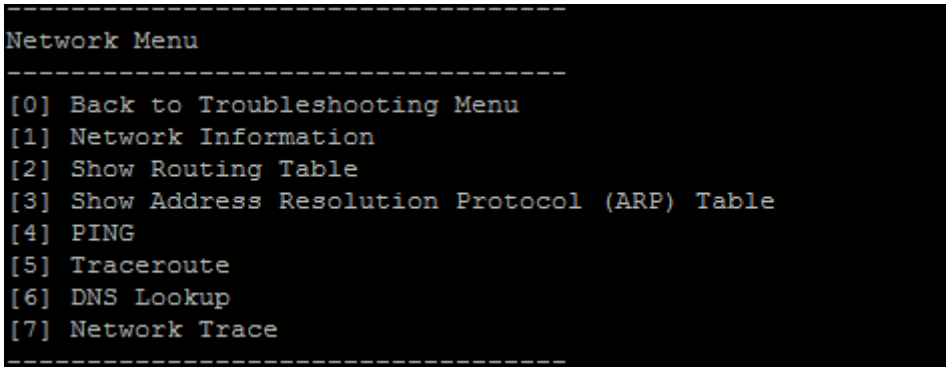
Las opciones de **Server Tuning** contienen los parámetros: tiempo de espera de la conexión al servidor, cantidad máxima de conexiones (por puerto) y cantidad máxima de subprocesos (por puerto).

Las opciones de **Switch JDBC driver** son: **jTDS** y **Microsoft JDBC**. El controlador predeterminado es jTDS. Para obtener información sobre cómo cambiar al controlador JDBC de Microsoft, consulte Controladores de SQL Server.

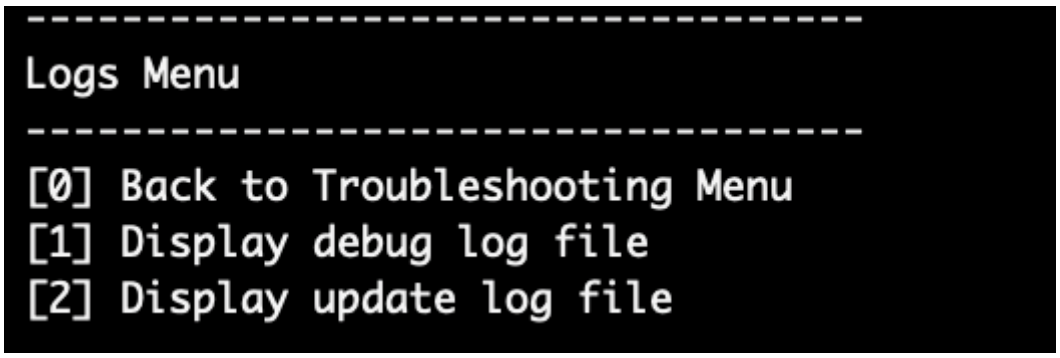
Opciones de Troubleshooting

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

[1] Network Utilities (Utilidades de red)



[2] Registros



[3] 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
---------------------------------
```

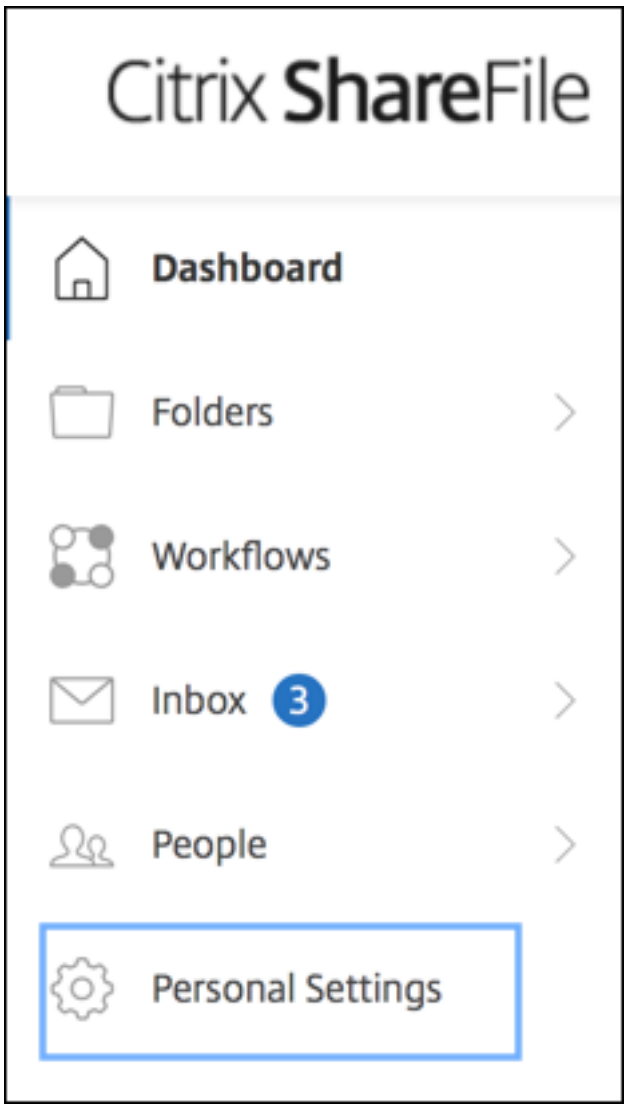
[4] Uso del disco

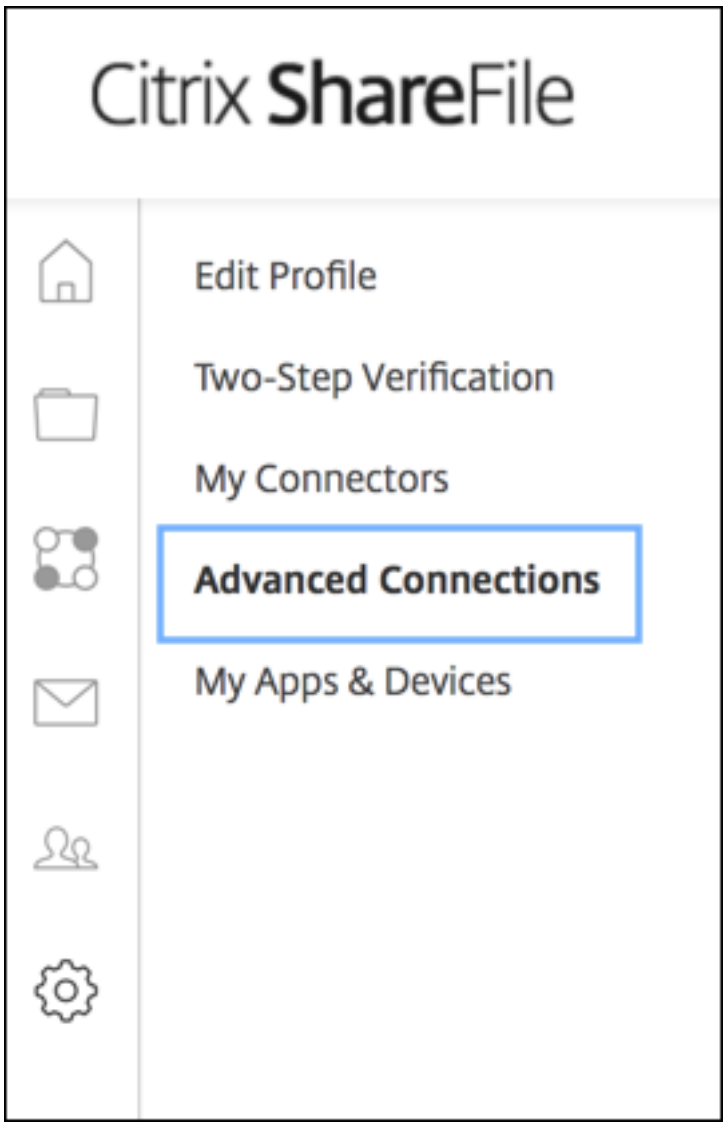
```
---------------------------------------
Troubleshooting Menu
---------------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
---------------------------------------
Choice: [0 - 4] 4
```

Para cargar un paquete de asistencia mediante Citrix Files como sitio FTP

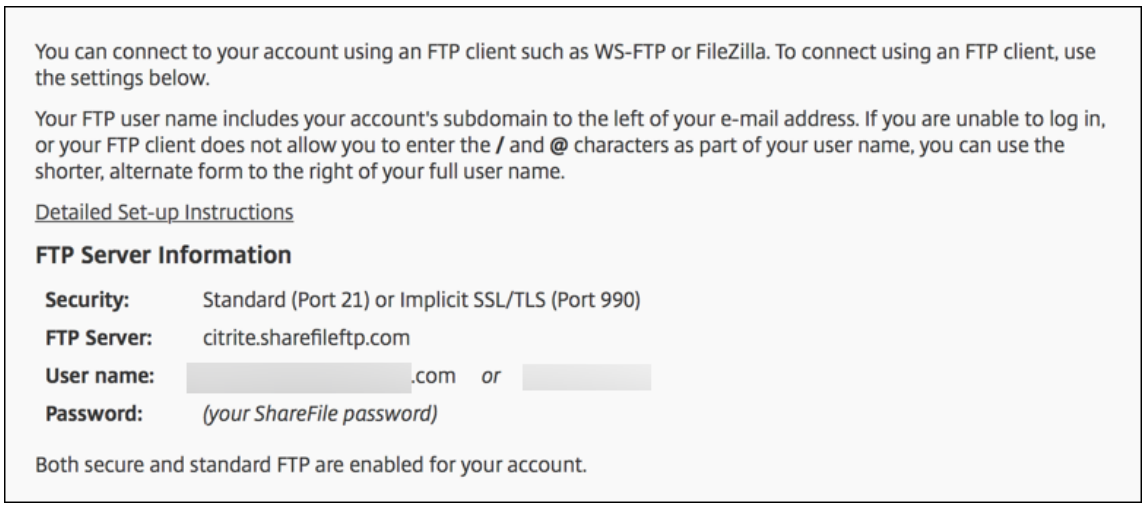
Antes de iniciar la carga de un paquete de asistencia, configure los siguientes requisitos previos en Citrix Files:

1. Verifique los detalles de inicio de sesión de FTP.
   a. En un explorador web, abra https://citrix.sharefile.com.
   b. Haga clic en **Personal Settings** y luego en **Advanced connections**.





c. En la información sobre el servidor FTP, compruebe que aparece un ID de usuario alfanumérico para el nombre de usuario, junto con los datos de subdominio/nombre de usuario predeterminados.


You can connect to your account using an FTP client such as WS-FTP or FileZilla. To connect using an FTP client, use the settings below.

Your FTP user name includes your account's subdomain to the left of your e-mail address. If you are unable to log in, or your FTP client does not allow you to enter the / and @ characters as part of your user name, you can use the shorter, alternate form to the right of your full user name.

Detailed Set-up Instructions

FTP Server Information

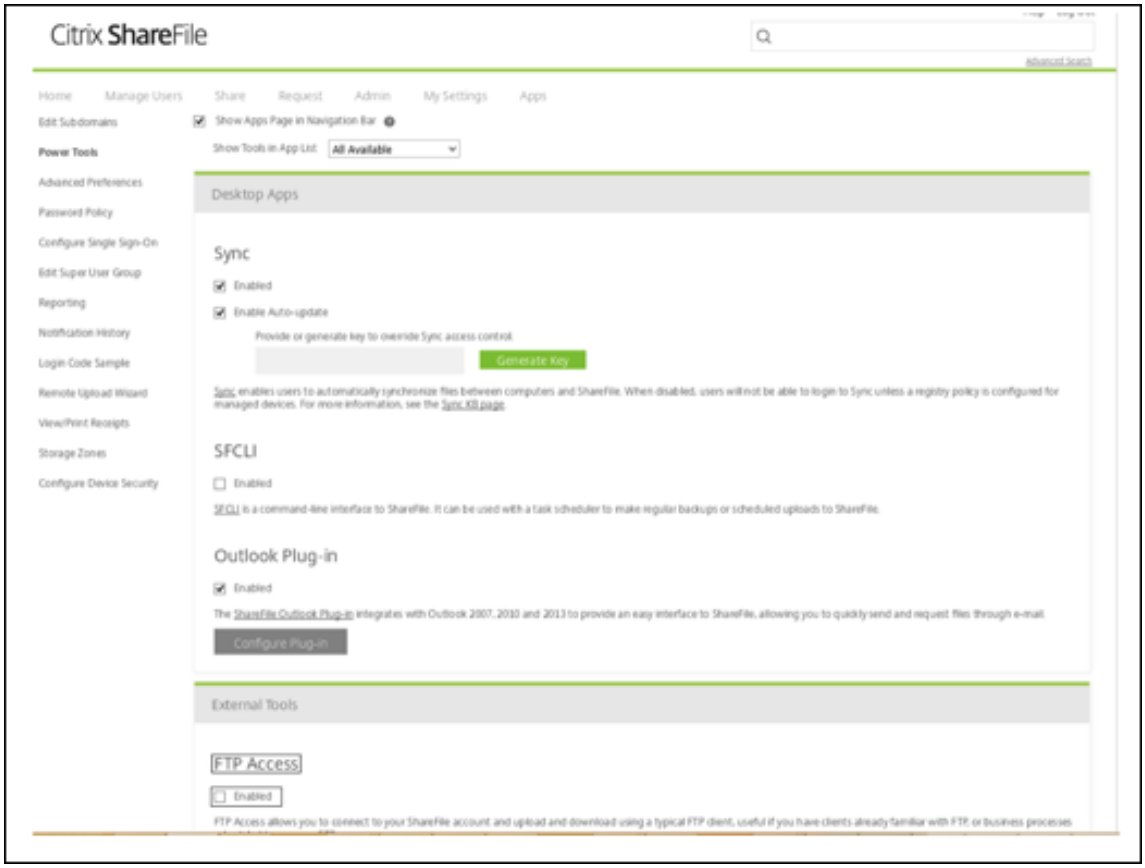
Security:	Standard (Port 21) or Implicit SSL/TLS (Port 990)
FTP Server:	citrite.sharefileftp.com
User name:	.com *or*
Password:	*(your ShareFile password)*

Both secure and standard FTP are enabled for your account.

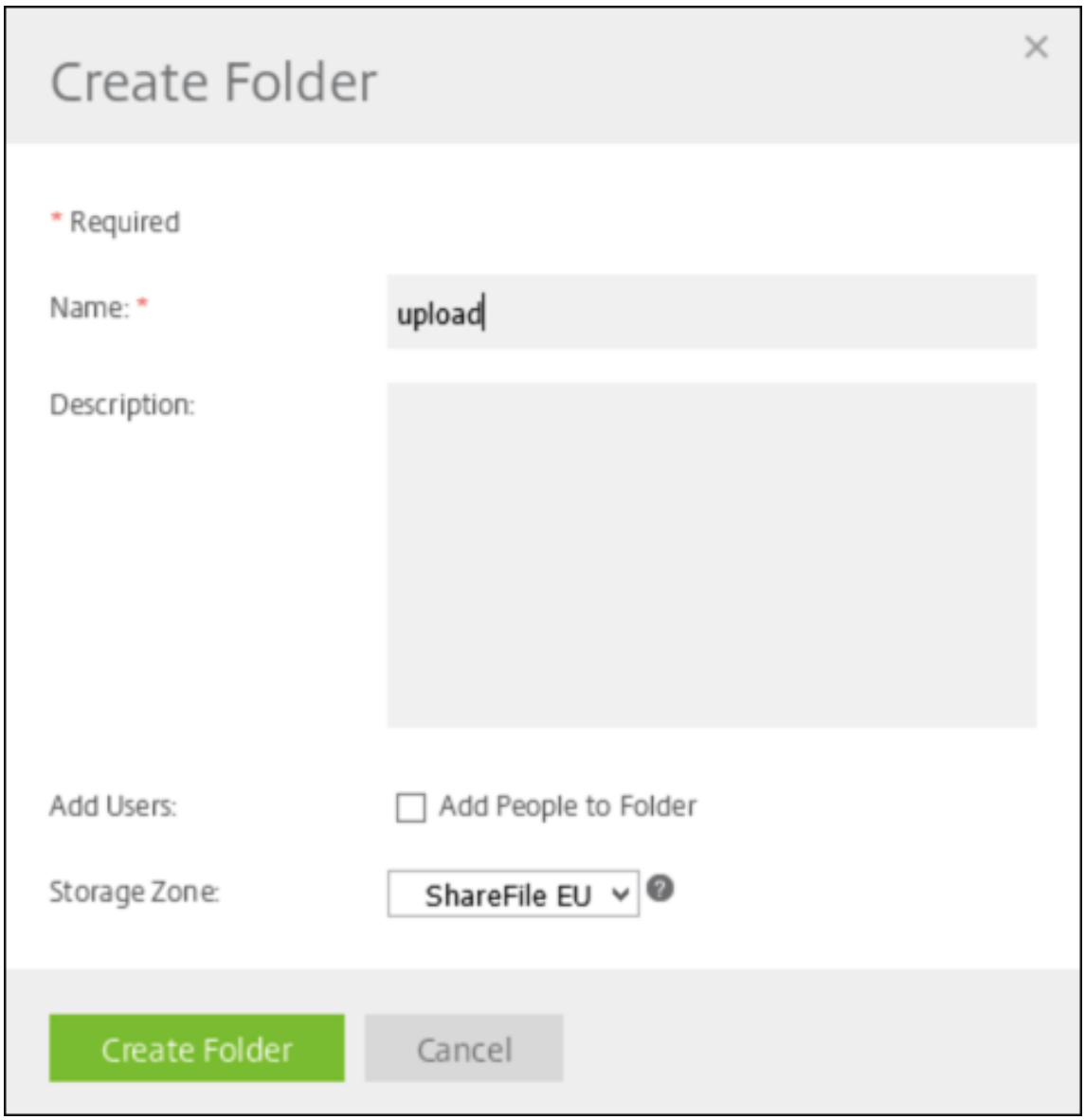
> **Notas:**
>
> - El archivo que está cargando desde XenMobile es un cliente FTP basado en CLI Linux. Como consecuencia, no se pueden introducir los caracteres de barra invertida (\) y arroba (@) como parte del nombre de usuario.
> - Si no ve el ID de usuario alfanumérico, puede solicitar este ID de usuario a su administrador de Content Collaboration o al servicio de asistencia de Content Collaboration.

2. Compruebe que el servidor de Citrix Files está habilitado para la comunicación FTP, además de la FTPS. Se recomienda que los administradores de Content Collaboration permitan la apertura de las cuentas de usuario para la comunicación FTP. No obstante, en ocasiones solo se permite la comunicación FTPS.

   Un usuario con derechos de administrador puede comprobar y habilitar esta configuración. Para ello, debe hacer clic en **Parámetros**, **Parámetros de administración**, **Preferencias avanzadas** y, por último, en **Habilitar herramientas de ShareFile**. Compruebe que la casilla de verificación **Habilitar** esté activada en **Aplicaciones externas**> **Acceso FTP**.



3. Cree una carpeta compartida para que el cliente FTP la utilice como directorio para la carga de archivos. Haga clic en **Inicio**, luego en **Carpetas** y, por último, en **Carpetas personales**.
4. En el extremo derecho, haga clic en el icono de suma (+), haga clic en **Crear carpeta** e introduzca un nombre para la carpeta.



5. En la CLI de XenMobile Server, en **Main Menu**, seleccione **Troubleshooting > Support Bundle**. A continuación, en **Support Bundle Menu**, seleccione **Generate Support Bundle**.

> **Nota:**
>
> Si existe un paquete de asistencia, escriba **y** cuando se le pregunte para anular dicho paquete.

6. Cargue el paquete de asistencia en el servidor FTP:

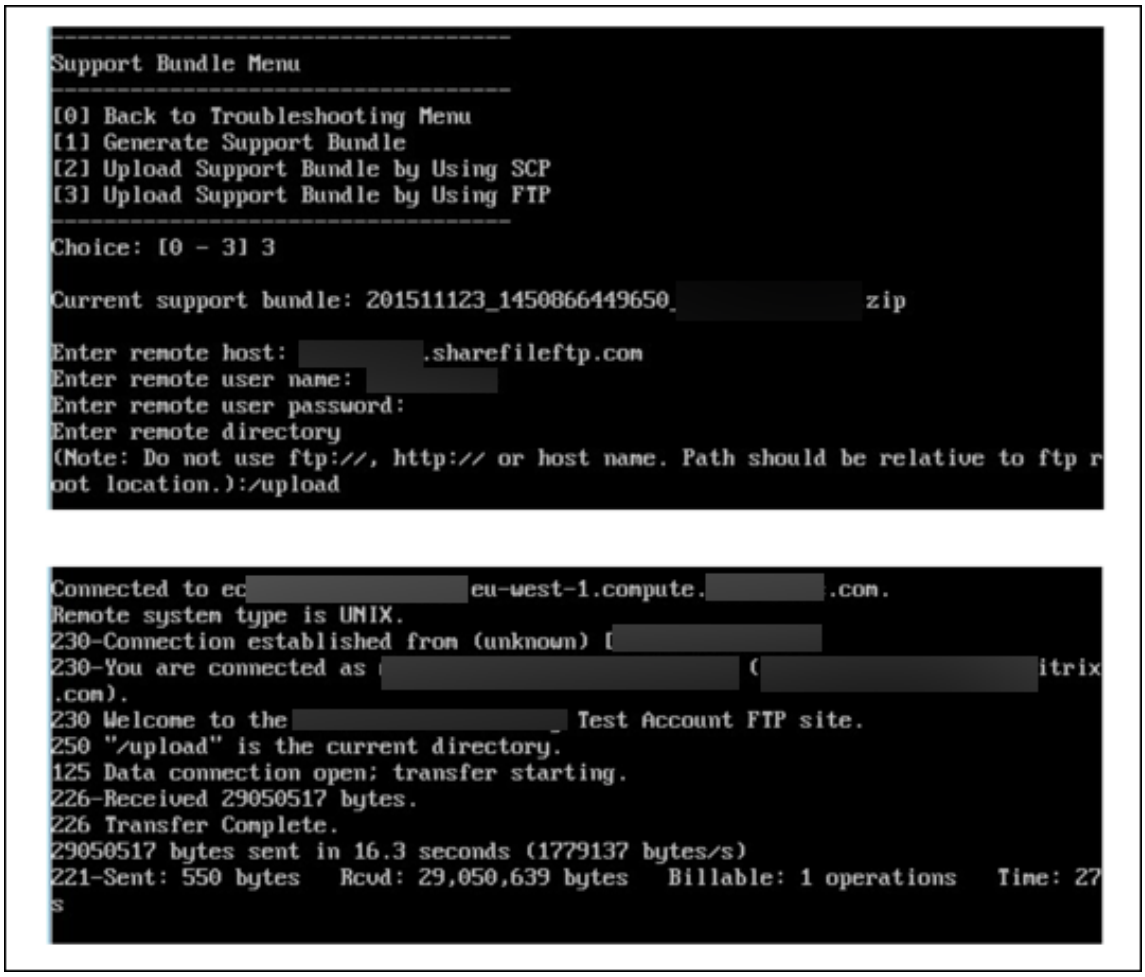
   a. Seleccione **Upload Support Bundle by using FTP**.

   b. Cuando se le indique que introduzca el host remoto (**Enter remote host**), escriba el nombre de su servidor FTP. Si se utiliza Citrix Files como servidor FTP, escriba el nombre de la empresa seguido del nombre del sitio FTP de Citrix Files. Por ejemplo, citrix.sharefileftp.com.

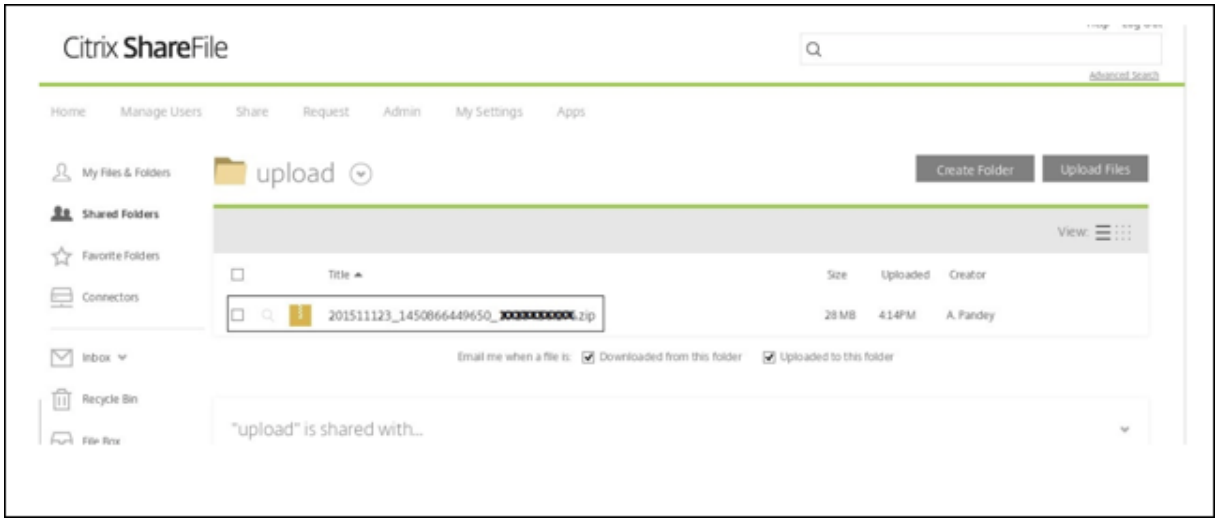
c. Cuando se le pida que introduzca el nombre de usuario remoto (**Enter remote user name**), escriba el ID de usuario alfanumérico.

d. Cuando se le pida que introduzca la contraseña de usuario remoto (**Enter remote user password**), escriba su contraseña.

e. Cuando se le solicite que introduzca el directorio remoto (**Enter remote directory**), escriba el nombre de la carpeta compartida creada en Citrix Files y, a continuación, presione **Entrar**.



Puede ver el paquete de asistencia cargado en la carpeta compartida creada en Citrix Files.



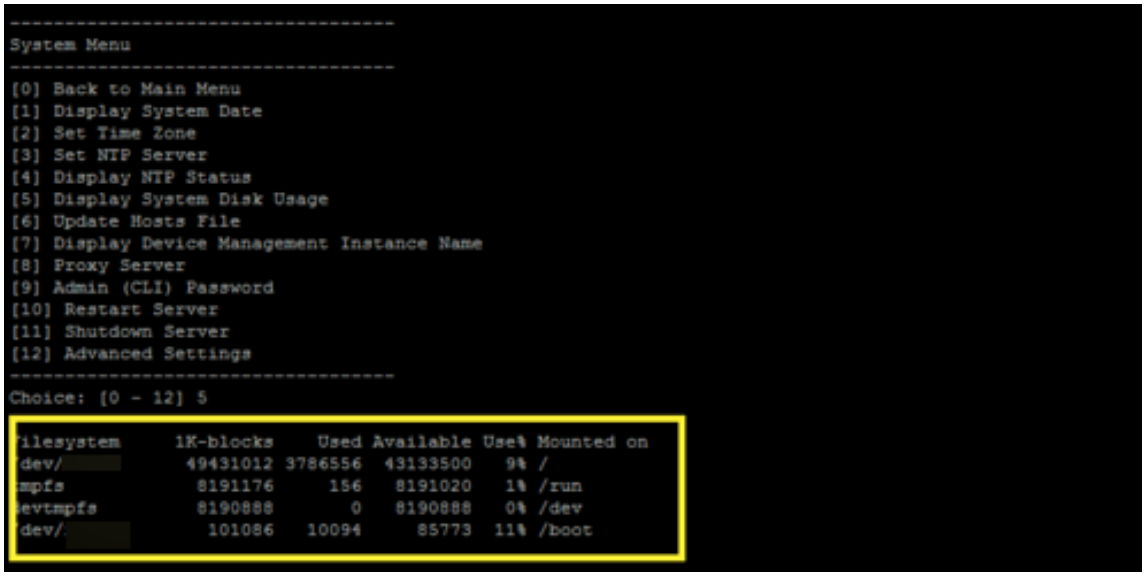
Para obtener más información sobre FTP de Citrix Files, consulte este artículo de Citrix Support Knowledge Center.

Para comprobar el espacio en disco

Puede comprobar el espacio en disco del sistema en la CLI de la siguiente manera:

1. En el menú principal, seleccione el menú **Sistema**.
2. En el menú **Sistema**, seleccione la opción **Mostrar uso de disco del sistema**.

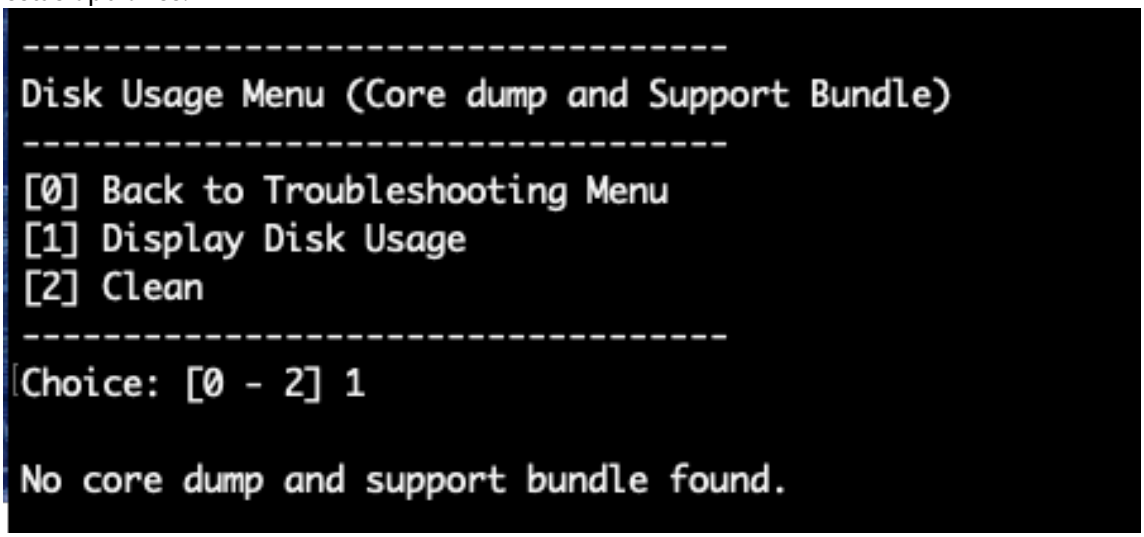
   Aparecerá la información del sistema de archivos.



Para hacer una limpieza de autoservicio del disco

Puede limpiar el disco en la CLI de la siguiente manera:

1. En el **menú Solución de problemas**, seleccione **Uso del disco**. El **menú Uso del disco** incluye estas opciones:



2. Escriba 1 para listar el archivo de volcado principal y los archivos de tipo paquetes de asistencia. Si no existen archivos, aparecerá un error que indica que **no se han encontrado archivos de volcado principal ni de paquetes de asistencia**.
3. Escriba 2 para limpiar el archivo de volcado principal y el archivo del paquete de asistencia analizados.

Flujos de trabajo iniciales en la consola de XenMobile

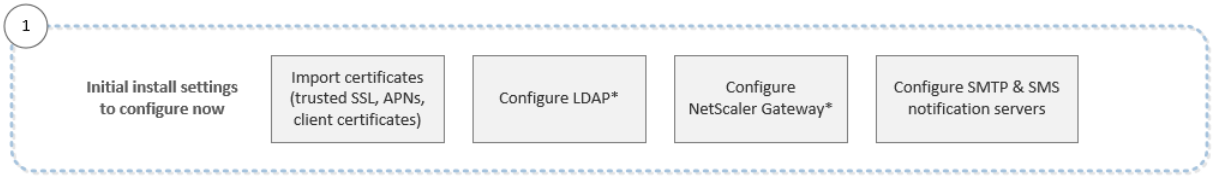
January 4, 2022

La consola de XenMobile es la herramienta de administración unificada para XenMobile. En este artículo, se da por hecho que XenMobile ya se ha instalado y está listo para su funcionamiento en la consola. Si aún tiene que instalar XenMobile, consulte Instalar XenMobile. Para obtener información acerca de los exploradores web que admiten la consola de XenMobile, consulte el artículo de "Compatibilidad de XenMobile".

Flujo de trabajo en la configuración inicial

Después de finalizar la configuración de XenMobile (primero en la consola de línea de comandos y luego en la consola de XenMobile), se abre el panel de mandos. No puede volver a las pantallas de configuración inicial. Si omitió algunas configuraciones de instalación, puede definir las siguientes configuraciones 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
- Citrix Gateway y XenMobile
- Notificaciones

Para admitir 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 Launch de Google Play.
- Crear una cuenta de administrador de Android Enterprise. Para obtener más información, consulte Android Enterprise.
- Verifique su nombre de dominio con Google. Para obtener más información, consulte Verificar un dominio para utilizar Google Workspace.
- Habilite las API y cree una cuenta de servicio para Android Enterprise. Para obtener más información, consulte Ayuda de Android Enterprise.

iOS

- Cree un ID de Apple y una cuenta de desarrollador. Para obtener más información, consulte el sitio web de Apple Developer Program.
- Cree un certificado APNs (Apple Push Notification Service). Si va a administrar dispositivos iOS con la implementación de XenMobile Server, necesitará un certificado APNs de Apple. Si usa notificaciones push para la implementación de Secure Mail, también necesita un certificado APNs de Apple. Para obtener más información sobre cómo obtener certificados APNs de Apple, vaya a Apple Push Certificates Portal. Para obtener más información acerca de XenMobile y APNs, consulte Certificados APNs y Notificaciones push en Secure Mail para iOS.
- Cree un token de empresa de compras por volumen. Para obtener más información, consulte Programa de Compras por Volumen de Apple.

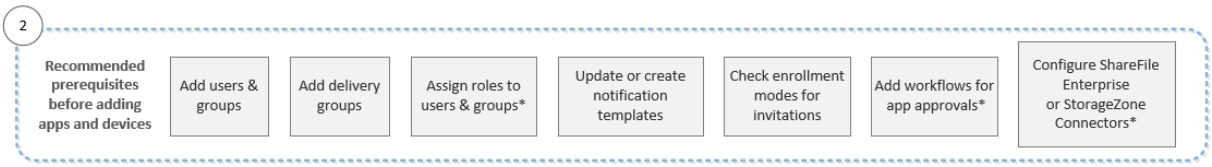
Windows

- Cree una cuenta de desarrollador para la Tienda Windows de Microsoft. Para obtener más información, consulte Tipos de cuenta, ubicaciones y precios.
- Obtenga un ID de publicador para la Tienda Windows de Microsoft. Para obtener más información, consulte Administrar los parámetros de cuenta y la información del perfil.
- Adquiera un certificado de empresa de DigiCert. Para obtener más información, consulte Company app distribution for Windows Phone.
- Si quiere utilizar la detección automática de XenMobile para la inscripción de dispositivos Windows Phone, compruebe que tiene un certificado SSL público disponible. Para obtener más información, consulte Servicio de detección automática de XenMobile.
- Cree un token de inscripción de la aplicación (AET). Para obtener más información, consulte How to generate an application enrollment token for Windows Phone.

Flujo de trabajo para los requisitos previos de consola

En esta secuencia, se muestran los requisitos previos a configurar antes de agregar aplicaciones y dispositivos.

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



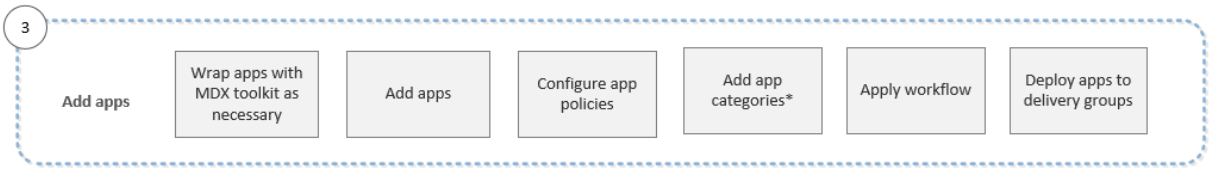
Para obtener más información acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos y apartados pertenecientes a la documentación de productos Citrix:

- Inscripción, roles y cuentas de usuario
- Implementar recursos
- Configurar roles con RBAC
- Notificaciones
- Aplicar flujos de trabajo
- Usar Citrix Content Collaboration con XenMobile

Flujos de trabajo para agregar aplicaciones

En esta secuencia 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 de MDX Toolkit
- Agregar aplicaciones
- Vista general de las directivas MDX
- Aplicar flujos de trabajo
- Implementar recursos

Flujo de trabajo para agregar dispositivos

En esta secuencia se muestra un orden recomendado a seguir en la incorporación y el registro de dispositivos en XenMobile.

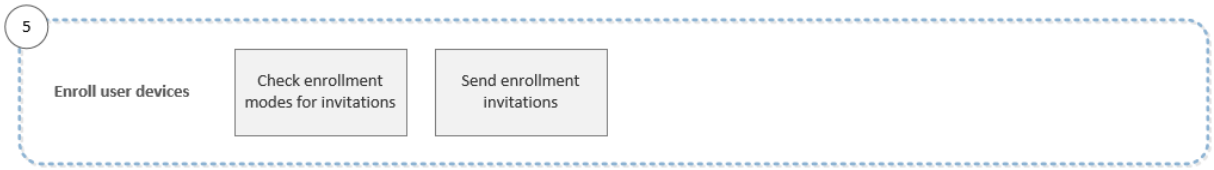
> **Nota:**
>
> Los elementos con asterisco son optativos.

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

- Dispositivos
- Sistemas operativos compatibles
- Implementar recursos
- Supervisar y ofrecer asistencia
- Acciones automatizadas

Flujos de trabajo para inscribir dispositivos de usuario

En esta secuencia se muestra un orden recomendado a seguir en la inscripción en XenMobile de dispositivos de usuario.



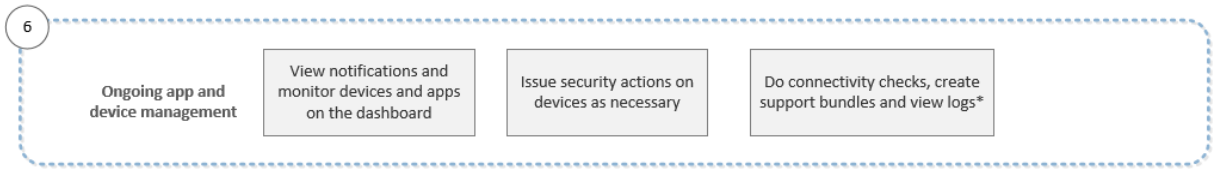
Para obtener más información acerca de cada parámetro, además de procedimientos paso a paso, consulte los siguientes artículos pertenecientes a la documentación de productos Citrix:

- Inscripción, roles y cuentas de usuario
- Notificaciones

Flujos de trabajo para la administración continua de dispositivos y aplicaciones

En esta secuencia se muestran las actividades de administración de dispositivos y aplicaciones que puede realizar en la consola.

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



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

Certificados y autenticación

January 4, 2022

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

- **XenMobile Server:** La seguridad y la experiencia de la inscripción se definen en XenMobile Server. Las opciones para incorporar usuarios son:
  - Elaborar una inscripción abierta para todos o solo por invitación.
  - 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.

- **Citrix ADC:** Con Citrix ADC, puede finalizar sesiones SSL de micro VPN. Asimismo, puede proteger la seguridad de los datos en tránsito en la red y definir la experiencia de autenticación cada vez que un usuario acceda a una aplicación.
- **Secure Hub:** Secure Hub y XenMobile Server funcionan conjuntamente en las operaciones de inscripción. Presente en el dispositivo, Secure Hub es la entidad que se comunica con Citrix ADC. Cuando una sesión caduca, Secure Hub obtiene un tíquet de autenticación de Citrix ADC y lo envía a las aplicaciones MDX. Citrix recomienda usar fijación de certificados, que impide ataques de intermediarios (ataques de tipo "Man in the middle"). Para obtener más información, consulte la sección Fijación de certificados en el artículo Secure Hub.

  Asimismo, Secure Hub favorece a la seguridad del contenedor MDX, ya que envía directivas, crea sesiones con Citrix ADC cuando se agota el tiempo de espera de las aplicaciones 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 vuelta a Citrix ADC, aplican las restricciones del modo sin conexión y las directivas de cliente (como los tiempos de espera).

Para obtener más información sobre la configuración de la autenticación, incluida una descripción general de los métodos de autenticación de uno y dos factores, consulte Authentication en el manual "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 con dominio o dominio y token de seguridad
- Autenticación con certificado de cliente o certificado y dominio
- Entidades PKI
- Proveedores de credenciales
- Certificados APNs
- SAML para Single Sign-On en Citrix Files
- Parámetros del servidor Microsoft Azure Active Directory
- Para enviar un certificado a dispositivos para autenticarse en el servidor Wi-Fi: Directiva Wi-Fi
- Para enviar un certificado único que no se utiliza para la autenticación, como un certificado raíz de CA interna, o una directiva específica: Directiva Credenciales

Certificados

XenMobile genera un certificado autofirmado de capa de sockets seguros (SSL) durante la instalación para proteger los flujos de comunicación con el servidor. Debe reemplazar ese certificado SSL por un

certificado SSL de confianza procedente de una entidad de certificación (CA) 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, los usuarios introducen su PIN de Citrix para acceder mediante 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 de certificado	Tipo de certificado requerido
Citrix Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Raíz (Citrix Gateway convierte automáticamente el formato PFX en PEM).
XenMobile Server	P12 (PFX en equipos basados en Windows)	SSL, SAML, APNs (XenMobile también genera una infraestructura de clave pública completa durante el proceso de instalación.) Importante: XenMobile Server no admite certificados con extensión .pem. Para utilizar un certificado PEM, divida el archivo .pem en un certificado y una clave e importe cada uno en XenMobile Server.
StoreFront	PFX (PKCS #12)	SSL, raíz

XenMobile admite los certificados SSL de escucha y certificados de cliente con longitudes de bits de 4096, 2048 y 1024. Los certificados de 1024 bits no son seguros.

Para Citrix Gateway y XenMobile Server, 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 Citrix 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 Citrix Gateway o XenMobile.

> **Importante: Requisitos para certificados de confianza en iOS, iPadOS y macOS**
>
> Apple tiene nuevos requisitos para los certificados de servidor TLS. Verifique que todos los certificados cumplen los nuevos requisitos de Apple. Consulte la publicación de Apple: https://support.apple.com/en-us/HT210176.
>
> Apple está reduciendo la duración máxima permitida de los certificados de servidor TLS. Este cambio solo afecta a los certificados de servidor emitidos después de septiembre de 2020. Consulte la publicación de Apple: https://support.apple.com/en-us/HT211025.

Cargar certificados en XenMobile

A cada certificado que cargue, le corresponderá una entrada en la tabla “Certificados”, con un resumen de su contenido. Cuando configure los componentes de integración con PKI que requieran un certificado, deberá elegir un certificado que cumpla los criterios de contexto. Por ejemplo, es posible que quiera configurar XenMobile para integrarlo con la entidad de certificación (CA) de Microsoft. La conexión a la entidad de certificación de Microsoft debe autenticarse con un certificado de cliente.

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

Requisitos de clave privada

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

Cargar certificados

Tiene dos opciones para cargar certificados:

- Cargue los certificados en la consola individualmente.
- Realice una carga en bloque de certificados en dispositivos iOS con la API de REST.

Para cargar certificados en la consola, tiene dos opciones:

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

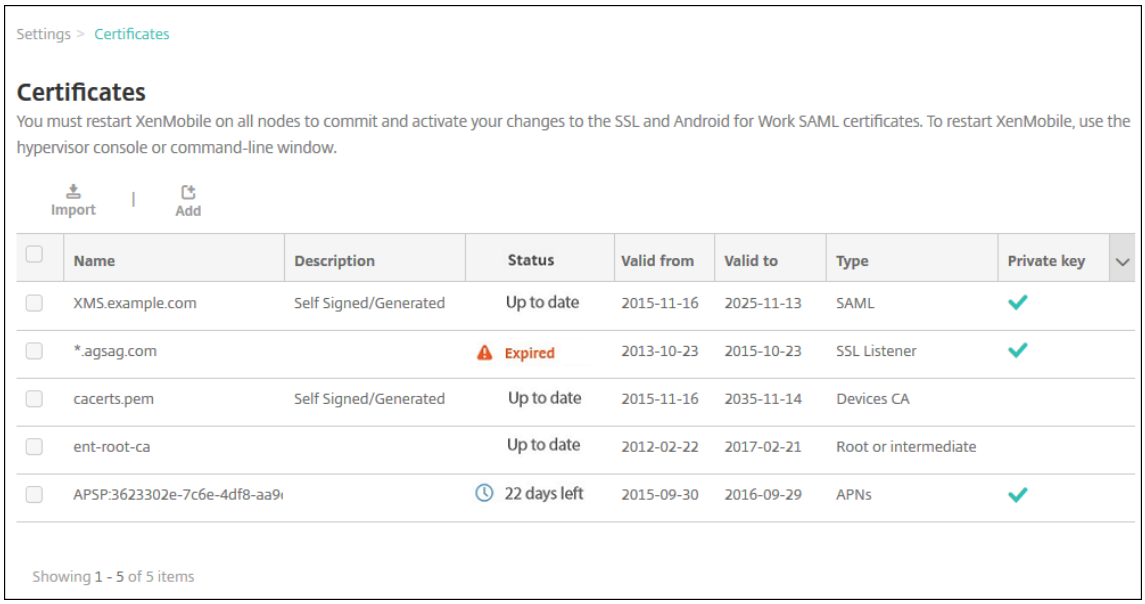
Puede cargar el certificado de CA (sin la clave privada) que usa la CA para firmar las solicitudes. También puede cargar un certificado de cliente SSL (con la clave privada) para la autenticación de clientes.

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

Para importar un almacén de claves

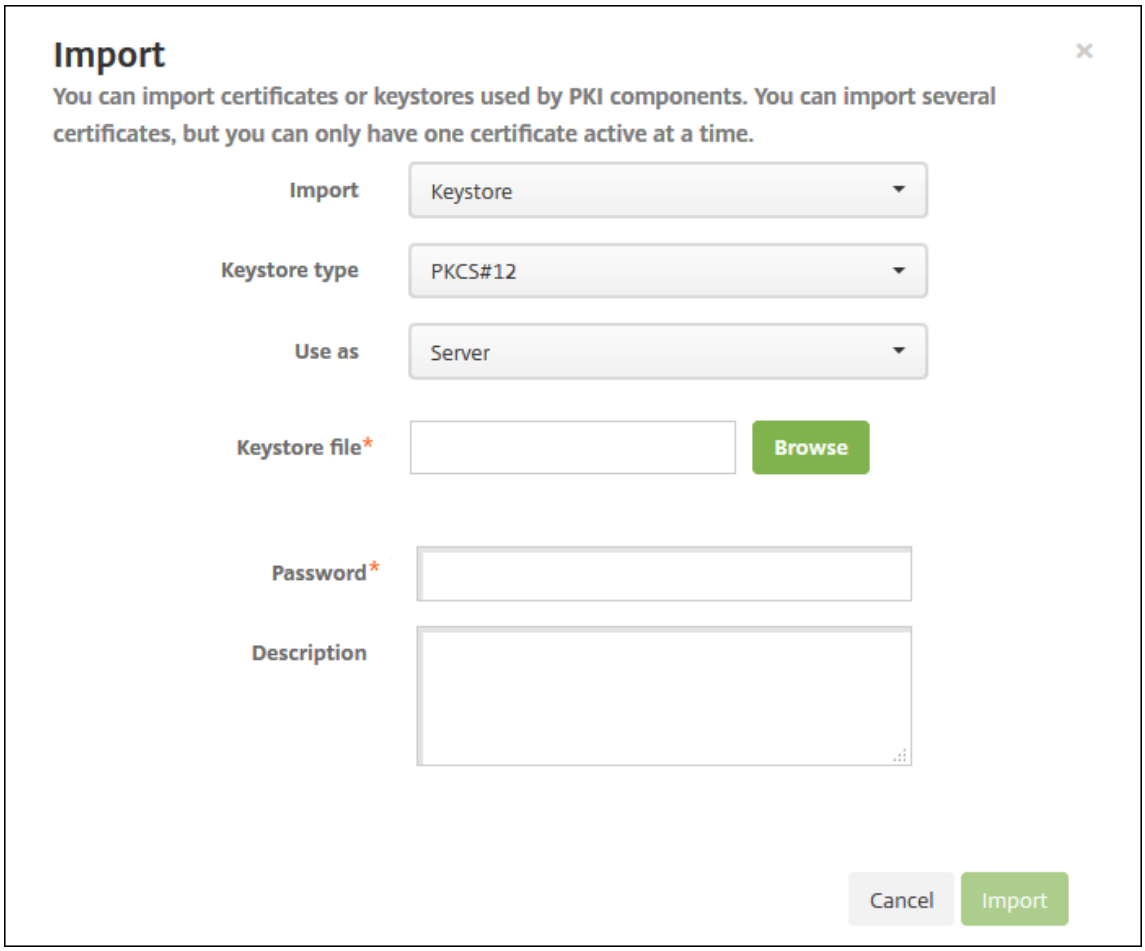
Los almacenes de claves, que son repositorios de certificados de seguridad, están diseñados para que puedan contener entradas múltiples. Al cargar entradas desde un almacén de claves, por lo tanto, se le solicitará que especifique el alias de entrada que identifica la entrada que quiera cargar. Si no se especifica ningún alias, se cargará la primera entrada del almacén. Como los archivos PKCS #12 suelen contener solo una entrada, el campo de alias no aparece cuando se selecciona PKCS #12 como tipo de almacén de claves.

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



3. Haga clic en **Importar**. Aparecerá el cuadro de diálogo **Importar**.
4. Configure estos parámetros:

- **Importar:** Seleccione **Almacén de claves** en la lista. El cuadro de diálogo **Importar** cambiará para reflejar las opciones de almacén de claves disponibles.



- **Tipo de almacén de claves:** Seleccione **PKCS #12** en la lista.
- **Usar como:** En la lista, haga clic en la forma en que usará el certificado. Las opciones disponibles son:
  - **Servidor**. Los certificados de servidor son aquellos que usa XenMobile Server, que se cargan en la consola Web de XenMobile. En este grupo se incluyen: los certificados de la entidad de certificación (CA), los certificados de la entidad de registro (RA) y los certificados para la autenticación de cliente con los demás componentes de la infraestructura. Además, puede utilizar los certificados de servidor como un almacén para los certificados que quiera implementar en los dispositivos. Este uso se aplica especialmente a certificados de entidades de certificación utilizados para establecer una relación de confianza en el dispositivo.
  - **SAML**. La certificación de SAML (Security Assertion Markup Language) permite ofrecer acceso Single Sign-On a los servidores, los sitios web y las aplicaciones.
  - **APNs**. Los certificados APNs de Apple permiten la administración de dispositivos móviles a través de Apple Push Network.

  - **Escucha SSL**. La escucha de Secure Sockets Layer (SSL) notifica a XenMobile acerca de la actividad de cifrado SSL.
- **Archivo de almacén de claves:** Busque el almacén de claves que quiere importar del tipo de archivo P12 (o PFX en equipos Windows).
- **Contraseña:** Escriba la contraseña asignada al certificado.
- **Descripción:** Escriba una descripción opcional del almacén de claves que le ayude a distinguirlo de otros almacenes.

5. Haga clic en **Importar**. El almacén de claves se agrega a la tabla "Certificados".

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. XenMobile importa todos los certificados de esa cadena (con lo que crea una entrada de certificado de servidor para cada certificado). Esta operación solo funciona si los certificados del archivo o del almacén de claves forman una cadena. Por ejemplo, si cada certificado de la cadena es el emisor del certificado anterior.

Si lo prefiere, puede agregar una descripción opcional 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 **Certificados**.
2. En la página **Certificados**, haga clic en **Importar**. Aparecerá el cuadro de diálogo **Importar**.
3. En el cuadro de diálogo **Importar**, en **Importar**, si no se ha seleccionado ya, haga clic en **Certificado**.
4. El cuadro de diálogo **Importar** cambiará para reflejar las opciones de certificado disponibles. En **Usar como**, seleccione cómo usará el almacén de claves. Las opciones disponibles son:
   - **Servidor**. Los certificados de servidor son aquellos que usa XenMobile Server, 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.
   - **Escucha SSL**. La escucha de Secure Sockets Layer (SSL) notifica a XenMobile acerca de la actividad de cifrado SSL.

5. Busque el almacén de claves que quiere importar del tipo de archivo P12 (o PFX en equipos Windows).
6. Busque el archivo de clave privada optativa del certificado. Junto con el certificado, la clave privada se usa para el cifrado y el descifrado.
7. Si quiere, escriba una descripción del certificado que le ayude a distinguirlo de otros certificados.
8. Haga clic en **Importar**. El certificado se agrega a la tabla "Certificados".

Cargar en bloque certificados en dispositivos iOS con la API de REST

Si no es práctico cargar los certificados de uno en uno, puede cargar en bloque los dispositivos iOS con la API de REST. Este método admite certificados en el formato P12. Para obtener más información acerca de la API de REST, consulte API de REST.

1. Cambie el nombre de cada uno de los archivos de certificado en el formato `device_identity_value.p12`. `device_identity_value` puede ser el IMEI, el número de serie o el MEID de cada dispositivo.

   A modo de ejemplo, elija utilizar números de serie como método de identificación. Hay un dispositivo con el número de serie `A12BC3D4EFGH`, así que el nombre del archivo de certificado que espera instalar en ese dispositivo deberá ser `A12BC3D4EFGH.p12`.

2. Cree un archivo de texto para almacenar las contraseñas de los certificados P12. En ese archivo, escriba el identificador de dispositivo y la contraseña de cada dispositivo en una línea nueva. Utilice el formato `device_identity_value=password`. Observe a continuación:

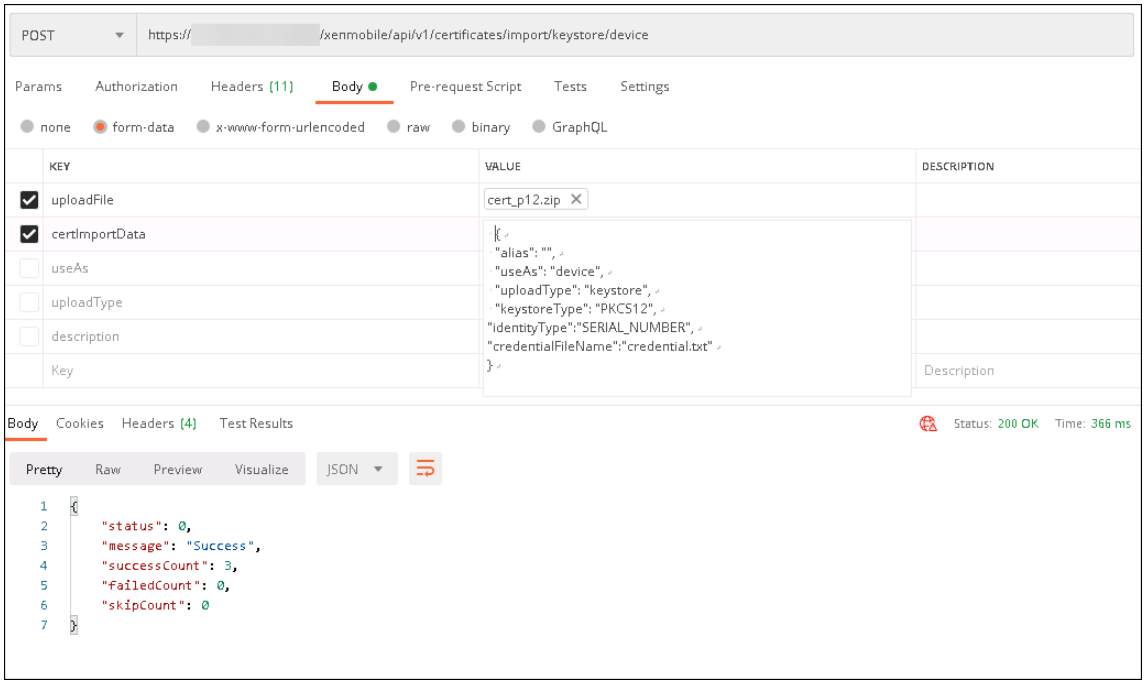
```
A12BC3D4EFGH.p12=password1!
A12BC3D4EFIJ.p12=password2@
A12BC3D4EFKL.p12=password3#
<!--NeedCopy-->
```

3. Empaquete todos los certificados y el archivo de texto que ha creado en un archivo ZIP.
4. Inicie su cliente con API de REST, inicie sesión en XenMobile y obtenga un token de autenticación.
5. Importe los certificados, poniendo lo siguiente en el cuerpo del mensaje:

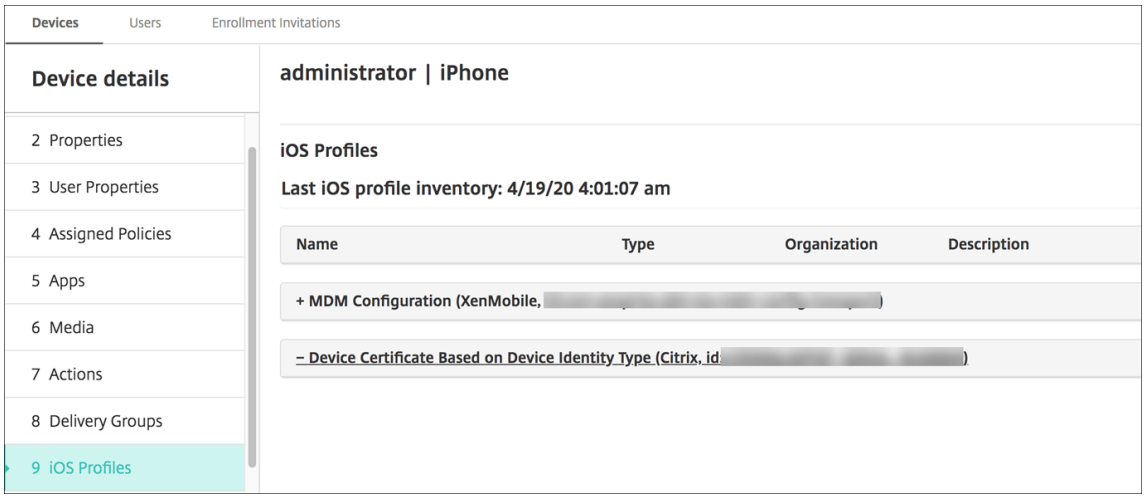
```
{

    "alias": "",
    "useAs": "device",
    "uploadType": "keystore",
    "keystoreType": "PKCS12",
```



```
    "identityType":"SERIAL_NUMBER",          # identity type can be
        "SERIAL_NUMBER","IMEI","MEID"
    "credentialFileName":"credential.txt"    # The credential file
        name in .zip
}

<!--NeedCopy-->
```

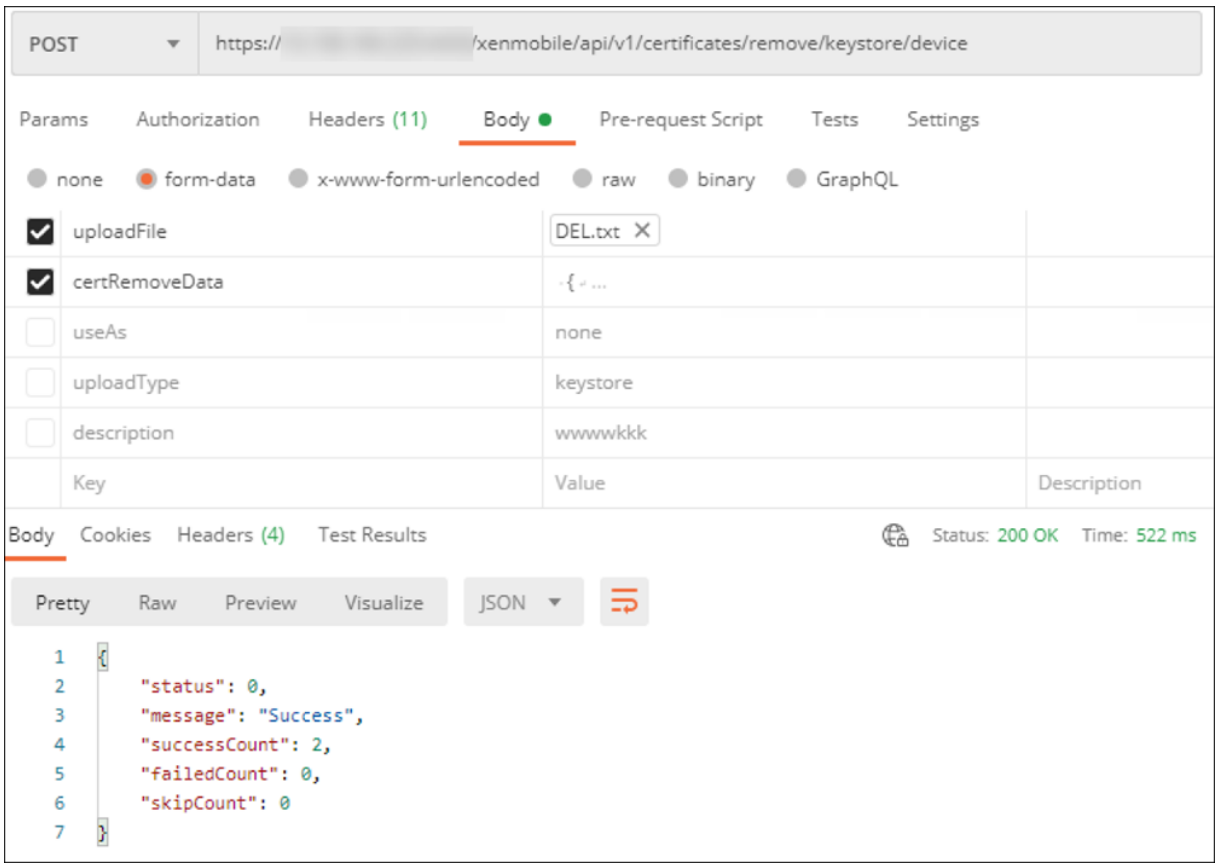


6. Cree una directiva de VPN con el tipo de credencial **Always on IKEv2** y el método de autenticación de dispositivo **Certificado de dispositivo basado en la identidad del dispositivo**. Seleccione el **tipo de identidad de dispositivo** que utilizó en los nombres de los archivos de certificado. Consulte Directiva de VPN.
7. Inscriba un dispositivo iOS y espere a que se implemente la directiva de VPN. Para confirmar la instalación del certificado, compruebe la configuración de MDM en el dispositivo. También puede comprobar los detalles del dispositivo en la consola de XenMobile.



También puede eliminar certificados en bloque mediante la creación de un archivo de texto con el valor `device_identity_value` listado para cada certificado que quiere eliminar. En la API de REST, llame a la API de eliminación y use esta solicitud, y sustituya `device_identity_value` por el identificador correspondiente:

```
1 ```
2 {
3
4     "identityType"="device_identity_value"
5  }
6
7 <!--NeedCopy--> ```
```

Actualizar un certificado

XenMobile solo permite un certificado por clave pública en el sistema a la vez. Si intenta importar un certificado del mismo par de claves que un certificado ya importado, podrá reemplazar la entrada existente o eliminarla.

En la consola de XenMobile, la forma más eficaz de actualizar los certificados es: Haga clic en el icono con forma de engranaje ubicado en la esquina superior derecha de la consola para abrir la página **Parámetros** y, a continuación, haga clic en **Certificados**. En el cuadro de diálogo **Importar**, 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.

Renovar un certificado

XenMobile Server utiliza internamente las siguientes entidades de certificación (CA) para PKI: CA raíz, CA del dispositivo y CA del servidor. Esas CA se clasifican como un grupo lógico y se les proporciona

un nombre de grupo. Cuando se aprovisiona una nueva instancia de XenMobile Server, se generan las tres CA y se les asigna el nombre de grupo “predeterminado”.

Puede renovar las CA para los dispositivos iOS, macOS y Android compatibles desde la consola de XenMobile Server o la API pública de REST. En caso de dispositivos Windows inscritos, los usuarios deben volver a inscribir sus dispositivos para recibir una nueva CA de dispositivo.

Están disponibles las siguientes API para renovar o regenerar las CA de PKI internas en XenMobile Server y renovar los certificados de dispositivo emitidos por estas entidades de certificación.

- Crear entidades de certificación (CA) de grupo.
- Activar nuevas CA y desactivar las antiguas.
- Renovar el certificado de dispositivo en una lista configurada de dispositivos. Los dispositivos ya inscritos continúan funcionando sin interrupciones. Se emite un certificado de dispositivo cuando este se conecta de nuevo al servidor.
- Devolver una lista de dispositivos que todavía usan la CA antigua.
- Eliminar la CA antigua cuando todos los dispositivos tengan la CA nueva.

Para obtener información, consulte las siguientes secciones en el documento PDF denominado Public API for REST Services:

- Sección 3.16.58: Renew Device Certificate (Renovar certificado de dispositivo)
- Sección 3.23: Internal PKI CA Groups (Grupos internos de CA de PKI)

La consola **Administrar dispositivos** incluye la acción de seguridad **Renovación de certificado**, que sirve para renovar el certificado de inscripción en un dispositivo.

Requisitos previos

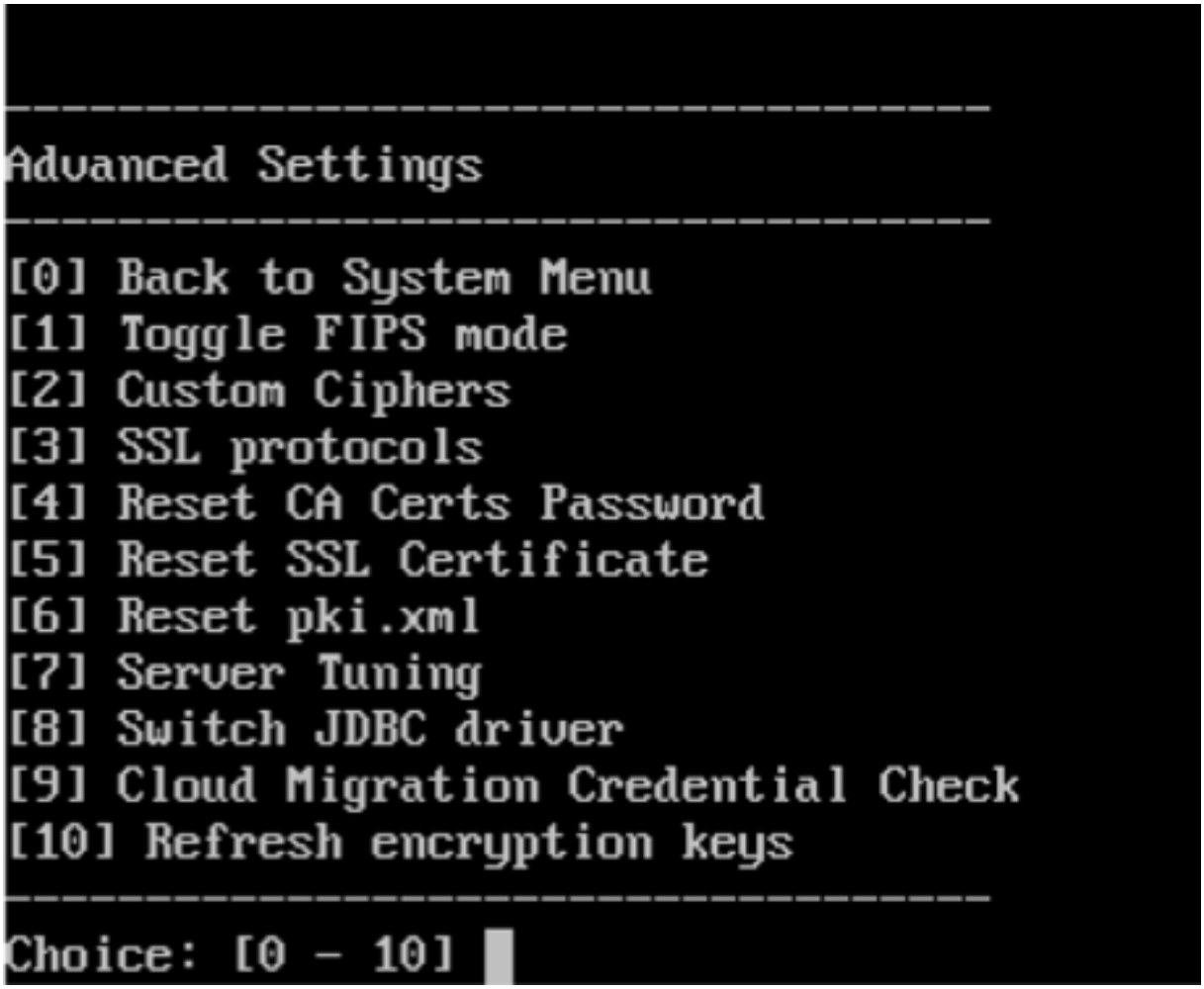
- De forma predeterminada, la función de actualización de certificado está inhabilitada. Para activar la función de actualización de certificado, establezca la propiedad de servidor **refresh.internal.ca** en el valor **verdadero**.

> **Importante:**
>
> Si Citrix ADC se ha configurado para la descarga de SSL, tras generar un certificado, debe actualizar el equilibrador de carga con el nuevo cacert.perm. Para obtener más información sobre la configuración de Citrix Gateway, consulte Para usar el modo de descarga SSL con direcciones IP virtuales de Citrix ADC.

Opción de CLI para restablecer la contraseña del certificado de CA del servidor para nodos de clúster

Después de generar un certificado de CA del servidor en un nodo de XenMobile Server, use la CLI de XenMobile para restablecer la contraseña del certificado en otros nodos del clúster. Desde el menú

principal de la CLI, seleccione **System > Advanced Settings > Reset CA certs password**. Si intenta restablecer la contraseña cuando no hay ningún certificado de CA nuevo, XenMobile no restablece la contraseña.



Administrar certificados en XenMobile

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

Su entorno puede contener alguno o todos los certificados siguientes:

- XenMobile Server
  - Certificado SSL para FQDN de MDM
  - Certificado SAML (para Citrix Files)
  - 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 XenMobile Server
  - Certificado de usuario PKI para la conectividad con PKI
- MDX Toolkit
  - Certificado de desarrollador de Apple
  - Perfil de datos de Apple (por aplicación)
  - Certificado APNs de Apple (para usar con Citrix Secure Mail)
  - Archivo JKS de Android
  - Windows Phone: Certificado DigiCert

  El SDK de MAM no empaqueta aplicaciones, por lo que no requiere un certificado.
- Citrix ADC
  - 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. No podrá seguir ejecutando operaciones seguras en su entorno ni acceder a los recursos de XenMobile.

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

Certificado APNs para Citrix Secure Mail

Los certificados Apple Push Notification Service (APNs) caducan cada año. Debe crear un certificado SSL de APNs y actualizarlo 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 Certificates Portal. Debe iniciar sesión con el mismo usuario con que creó el certificado.

Asimismo, Apple le enviará una notificación por correo electrónico entre 30 y 10 días antes de la fecha de caducidad. Esa notificación contendrá la siguiente información:

```
The following Apple Push Notification Service certificate, created for
    Apple ID CustomerID will expire on Date. Revoking or allowing this
    certificate to expire will require existing devices to be re-
    enrolled with a new push certificate.

Please contact your vendor to generate a new request (a signed CSR),
    then visit https://identity.apple.com/pushcert to renew your Apple
    Push Notification Service certificate.

Thank You,

Apple Push Notification Service
<!--NeedCopy-->
```

MDX Toolkit (certificado de distribución iOS)

Una aplicación que se ejecute en un dispositivo iOS físico (aparte de las aplicaciones del App Store de Apple) presenta estos requisitos de firma:

- Debe firmar la aplicación con un perfil de datos.
- Debe firmar la aplicación con un certificado de distribución correspondiente.

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

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

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

1. En la consola de XenMobile, haga clic en **Parámetros > Certificados**.
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 una clave caduca, los usuarios ya no pueden actualizar fácilmente la aplicación a una nueva versión.

Certificado de empresa de DigiCert para Windows Phone

DigiCert 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 detallada, consulte DigiCert Code Signing Certificates for Windows Phone en la documentación de DigiCert.

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

Citrix ADC

Para obtener información detallada sobre cómo gestionar la caducidad de los certificados en Citrix ADC, consulte How to handle certificate expiry on NetScaler en Knowledge Center de Citrix Support.

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

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

- 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

Citrix Gateway y XenMobile

January 4, 2022

Al configurar Citrix 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. Porque XenMobile crea una micro VPN que se extiende desde las aplicaciones presentes en el dispositivo hasta Citrix Gateway.

Si quiere configurar Citrix Gateway para usarlo con XenMobile¡, debe exportar, desde XenMobile, un script que deberá ejecutar en Citrix Gateway.

Requisitos previos para utilizar el script de configuración de Citrix Gateway

Requisitos de Citrix ADC:

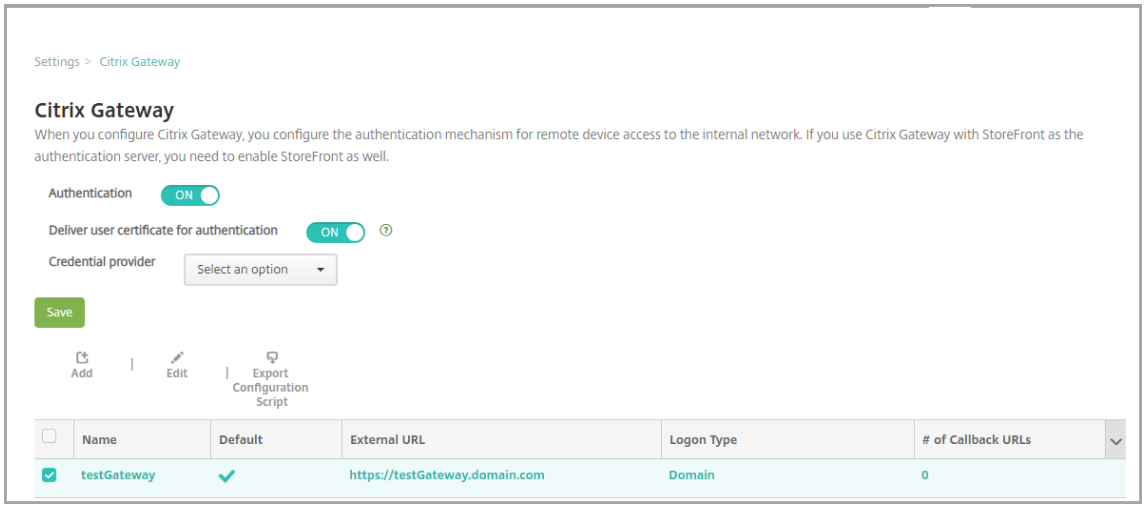
- Citrix ADC (versión mínima 11.0, compilación 70.12)
- La dirección IP de Citrix ADC está configurada y tiene conectividad con el servidor LDAP, a menos que LDAP tenga la carga equilibrada.
- La dirección IP de subred (SNIP) de Citrix ADC está configurada, tiene conectividad con los servidores back-end necesarios y tiene acceso a la red pública por el puerto 8443/TCP.
- DNS puede resolver dominios públicos.
- Citrix ADC tiene las licencias Platform, Universal o Trial. Para obtener información, consulte https://support.citrix.com/article/CTX126049.
- Un certificado SSL de Citrix Gateway está cargado e instalado en el dispositivo Citrix ADC. Para obtener más información, consulte https://support.citrix.com/article/CTX136023.

Requisitos de XenMobile

- XenMobile Server 10.6 (versión mínima)
- El servidor LDAP está configurado.

Configurar la autenticación para el acceso de dispositivos remotos a la red interna

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 **Parámetros**.
2. En **Servidor**, haga clic en **Citrix Gateway**. Aparecerá la página **Citrix Gateway**. En el siguiente ejemplo, existe una instancia de Citrix Gateway.

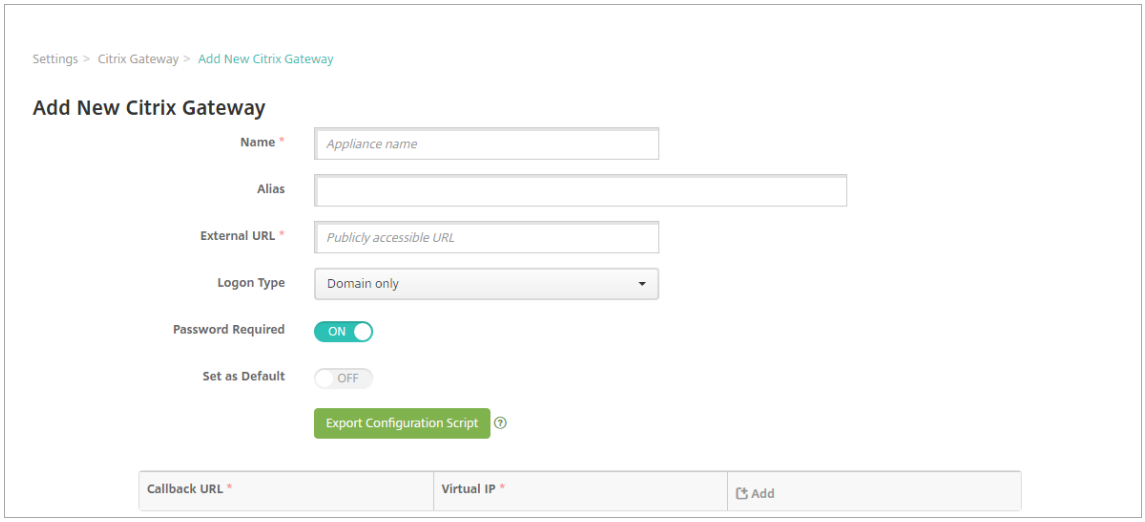


3. Configure estos parámetros:
   - **Autenticación:** Seleccione si quiere habilitar la autenticación. De forma predeterminada, está **activado**.
   - **Entregar certificado de usuario para autenticación:** Seleccione si quiere que XenMobile comparta el certificado de autenticación con Secure Hub para que Citrix Gateway gestione la autenticación de certificados de cliente. Está **desactivado** de forma predeterminada.
   - **Proveedor de credenciales:** En la lista, haga clic en el proveedor de credenciales que se va a utilizar. Para obtener más información, consulte Proveedores de credenciales.
4. Haga clic en **Guardar**.

Agregar una instancia de Citrix Gateway

Después de guardar los parámetros de autenticación, puede agregar una instancia de Citrix Gateway 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. Se abrirá la página **Parámetros**.
2. En **Servidor**, haga clic en **Citrix Gateway**. Aparecerá la página **Citrix Gateway**.
3. Haga clic en **Agregar**. Aparecerá la página **Agregar nuevo Citrix Gateway**.



4. Configure estos parámetros:

   - **Nombre:** Escriba un nombre para la instancia de Citrix Gateway.
   - **Alias:** Puede incluir un nombre como alias de Citrix Gateway.
   - **URL externa:** Escriba la URL de acceso público de Citrix Gateway. Por ejemplo, `https://receiver.com`.
   - **Tipo de inicio de sesión:** Haga clic en un tipo de inicio de sesión. Los tipos pueden ser: **Solo dominio**, **Solo token de seguridad**, **Dominio y token de seguridad**, **Certificado**, **Certificado y dominio** y **Certificado y token de seguridad**. Además, los valores predeterminados del campo **Requerir código de acceso** cambian en función del **Tipo de inicio de sesión** seleccionado. El valor predeterminado es **Solo dominio**.

   Si dispone de varios dominios, use **Certificado y dominio**. Para obtener más información sobre la configuración de la autenticación de varios dominios con XenMobile y Citrix Gateway, consulte Configurar la autenticación para varios dominios.

   Si utiliza la opción **Certificado y token de seguridad**, se necesita configuración adicional en Citrix Gateway para que admita Secure Hub. Para obtener más información, consulte Configuración de XenMobile para la autenticación con certificado y token de seguridad.

   Para obtener más información, consulte Authentication en Deployment Handbook.

   - **Requerir código de acceso:** Seleccione si quiere que se solicite la contraseña para la autenticación. El valor predeterminado varía según el **Tipo de inicio de sesión** seleccionado.
   - **Definir como predeterminado:** Seleccione si quiere usar esta instancia de Citrix Gateway como predeterminada. Está **desactivado** de forma predeterminada.
   - **Exportar script de configuración:** Haga clic en el botón para exportar un paquete de configuración que se puede cargar en Citrix Gateway para configurarlo con XenMobile. Para obtener información, consulte “Configurar un Citrix Gateway local para usarlo con XenMobile Server” más adelante en este artículo.

- **URL de respuesta** e **IP virtual:** Guarde la configuración antes de agregar estos campos. Para obtener información, consulte Agregar una URL de respuesta y una IP virtual de VPN de Citrix Gateway en este artículo.

5. Haga clic en **Guardar**.

   La nueva instancia de Citrix Gateway se agrega y aparece en la tabla. Para modificar o eliminar una instancia, haga clic en el nombre de esta en la lista.

Configurar Citrix Gateway para usarlo con XenMobile Server

Para configurar un dispositivo Citrix Gateway local y usarlo con XenMobile, realice los siguientes pasos generales, descritos en este artículo:

1. Descargue un script y los archivos relacionados desde XenMobile Server. Consulte el archivo Léame suministrado con el script para ver instrucciones detalladas actualizadas.
2. Compruebe que su entorno cumple los requisitos previos.
3. Actualice el script para su entorno.
4. Ejecute el script en Citrix ADC.
5. Pruebe la configuración.

El script configura los parámetros de Citrix Gateway requeridos por XenMobile:

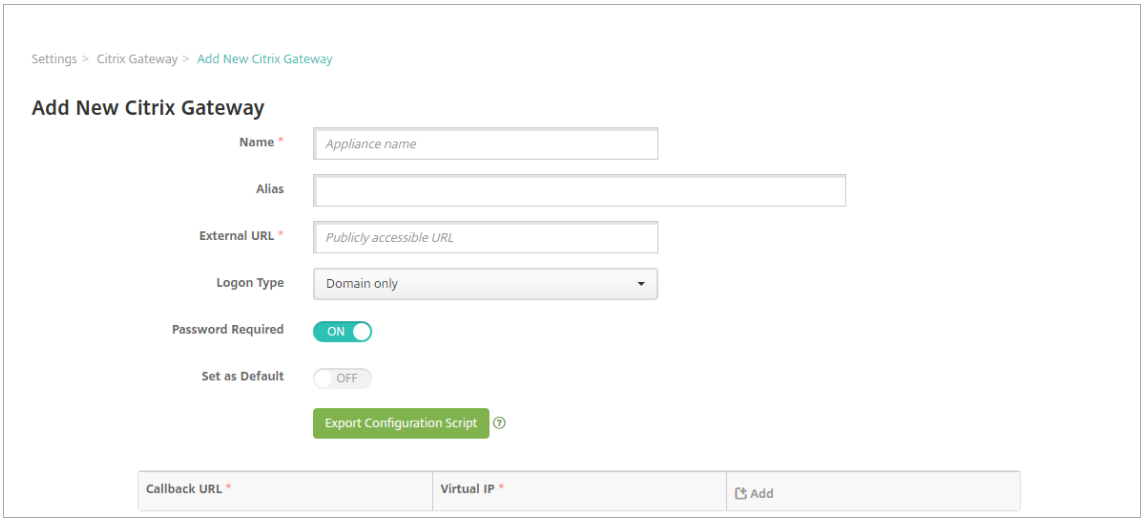
- Servidores virtuales de Citrix Gateway necesarios para MAM y MDM
- Directivas de sesión para los servidores virtuales de Citrix Gateway
- Datos de XenMobile Server
- Acciones y directivas de autenticación para el servidor virtual Citrix Gateway.
  El script describe los parámetros de configuración de LDAP.
- Directivas y acciones de tráfico de red para el servidor proxy
- Perfil de acceso sin cliente
- Registro de DNS local estático en Citrix ADC
- Otros enlaces: directiva de servicio, certificado de CA

El script no se ocupa de la siguiente configuración:

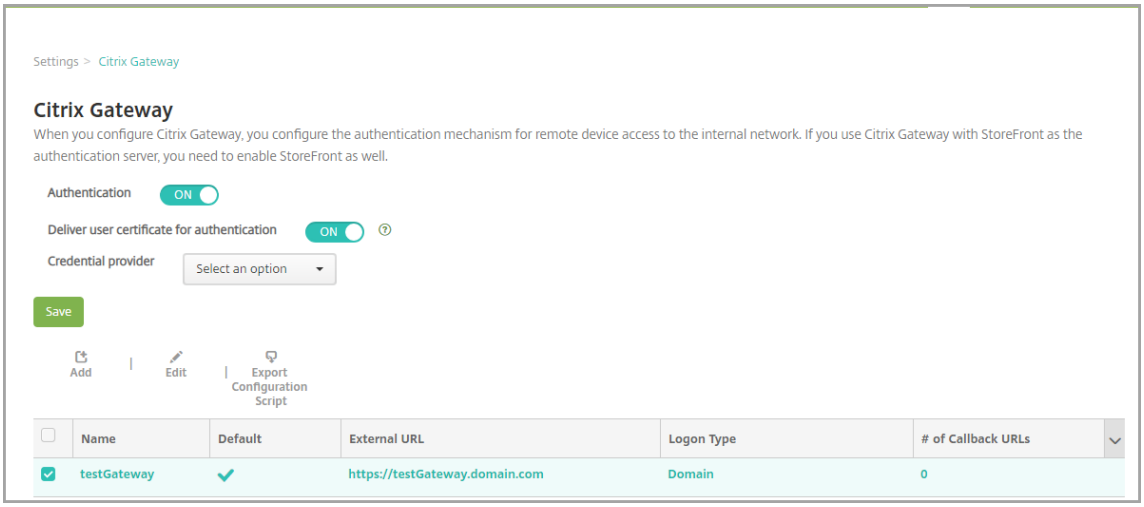
- Equilibrio de carga de Exchange
- Equilibrio de carga de Citrix Files
- Configuración del proxy ICA
- Descarga de SSL

Para descargar, actualizar y ejecutar el script

1. Si va a agregar un dispositivo Citrix Gateway, haga clic en **Exportar script de configuración** en la página **Agregar nuevo dispositivo Citrix Gateway**.



O bien, si agrega una instancia de Citrix Gateway y hace clic en **Guardar** antes de exportar el script, vuelva a **Parámetros > Citrix Gateway**, seleccione el dispositivo Citrix ADC, haga clic en **Exportar script de configuración** y, a continuación, haga clic en **Descargar**.

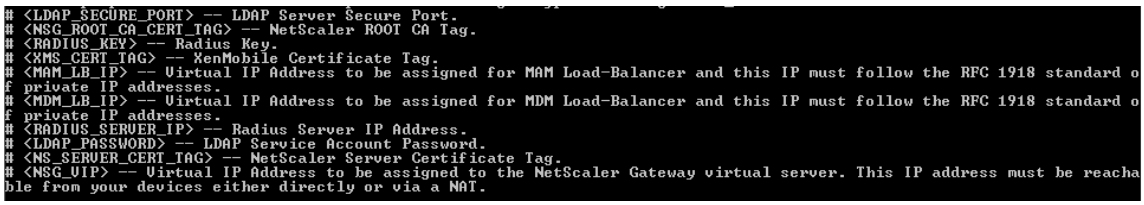


Después de hacer clic en **Exportar script de configuración**, XenMobile crea un paquete de script .tar.gz. El paquete de script incluye:

- Un archivo Léame con instrucciones detalladas
- Un script que contiene los comandos de interfaz de línea de comandos de Citrix ADC que se usan para configurar los componentes necesarios en Citrix ADC
- Un certificado de CA raíz público y el certificado de CA intermedio de XenMobile Server (no se requieren estos certificados para la descarga de SSL en la versión actual)

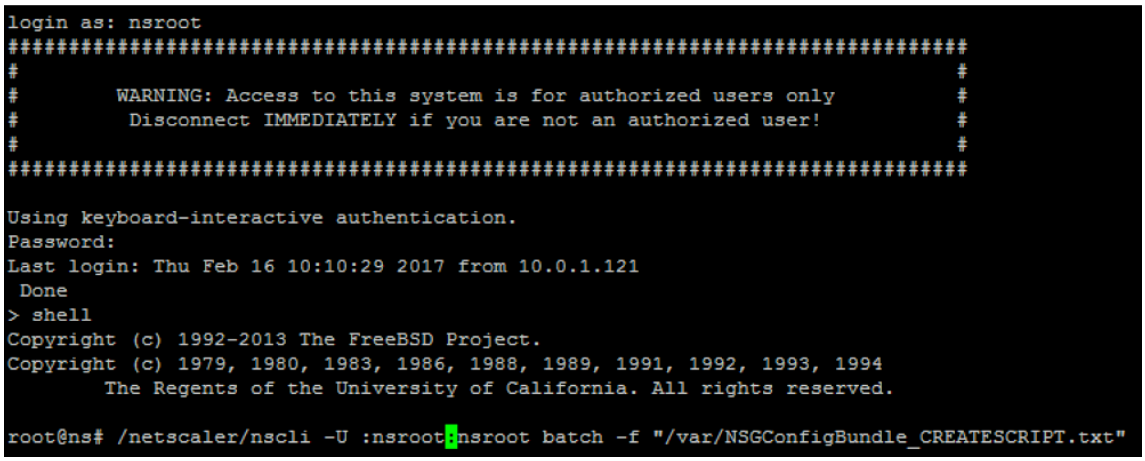
- Un script que contiene los comandos de interfaz de línea de comandos de Citrix ADC necesarios para quitar la configuración de Citrix ADC

2. Modifique el script (NSGConfigBundle_CREATESCRIPT.txt) para reemplazar todos los marcadores de posición por los valores correspondientes a su implementación.

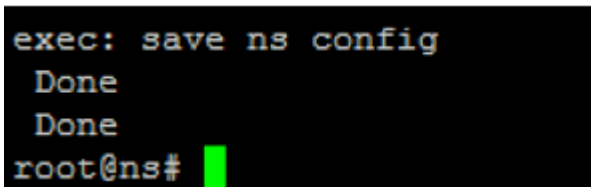


3. Ejecute el script modificado en el bash shell de Citrix ADC, como se describe en el archivo Léame incluido en el paquete del script. Por ejemplo:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management
 Password> batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

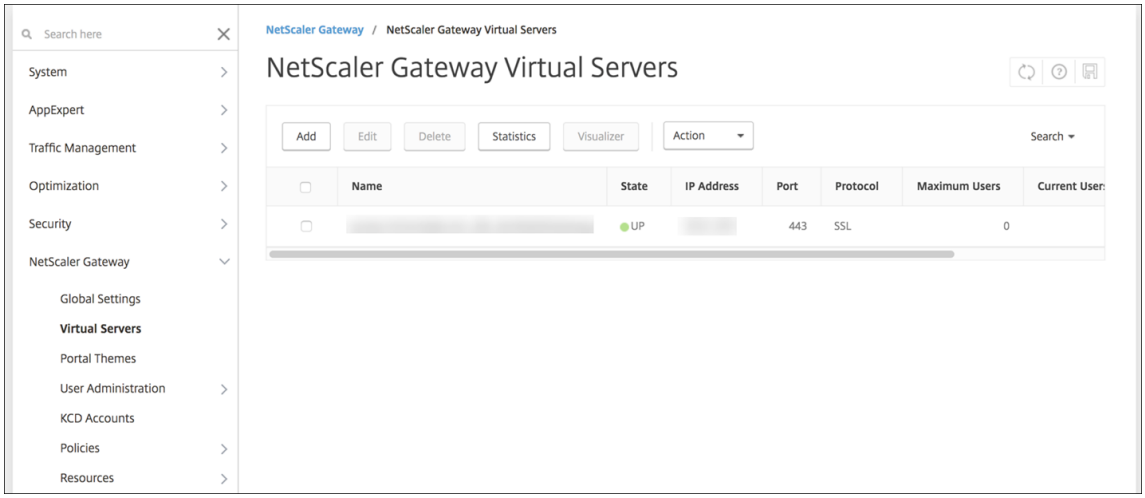


Cuando el script se complete, aparecerán las siguientes líneas.

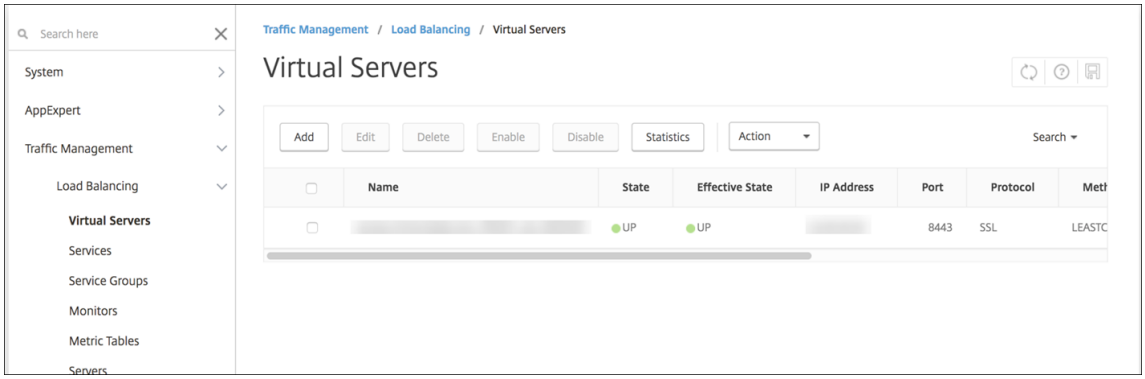


Probar la configuración

1. Compruebe que el servidor virtual Citrix Gateway muestra el estado operativo (**UP**).



2. Compruebe que el servidor virtual de equilibrio de carga proxy muestra el estado operativo (**UP**).



3. Abra un explorador web, conéctese a la URL de Citrix Gateway e intente autenticarse. Si la autenticación falla, aparece este mensaje: HTTP Status 404 - Not Found
4. Inscriba un dispositivo y compruebe que obtiene la inscripción en MDM y MAM.

Agregar una URL de respuesta y una IP virtual de VPN de Citrix Gateway

Después de agregar la instancia de Citrix Gateway, puede agregar una dirección URL de respuesta y especificar una dirección IP virtual de Citrix Gateway. Esta configuración es opcional, pero se puede definir para obtener seguridad adicional, especialmente cuando XenMobile Server está en la zona desmilitarizada (DMZ).

1. En **Parámetros > Citrix Gateway**, seleccione el dispositivo Citrix Gateway y, a continuación, haga clic en **Modificar**.
2. En la tabla, haga clic en **Agregar**.
3. Para **URL de respuesta**, escriba el nombre de dominio completo (FQDN). La URL de respuesta verifica que la solicitud proviene de Citrix Gateway.

Compruebe que la URL de respuesta derive en una dirección IP a la que se pueda acceder desde XenMobile Server. La URL de respuesta puede ser una URL externa de Citrix Gateway u otra URL.

4. Introduzca la dirección **IP virtual** de Citrix Gateway y haga clic en **Guardar**.

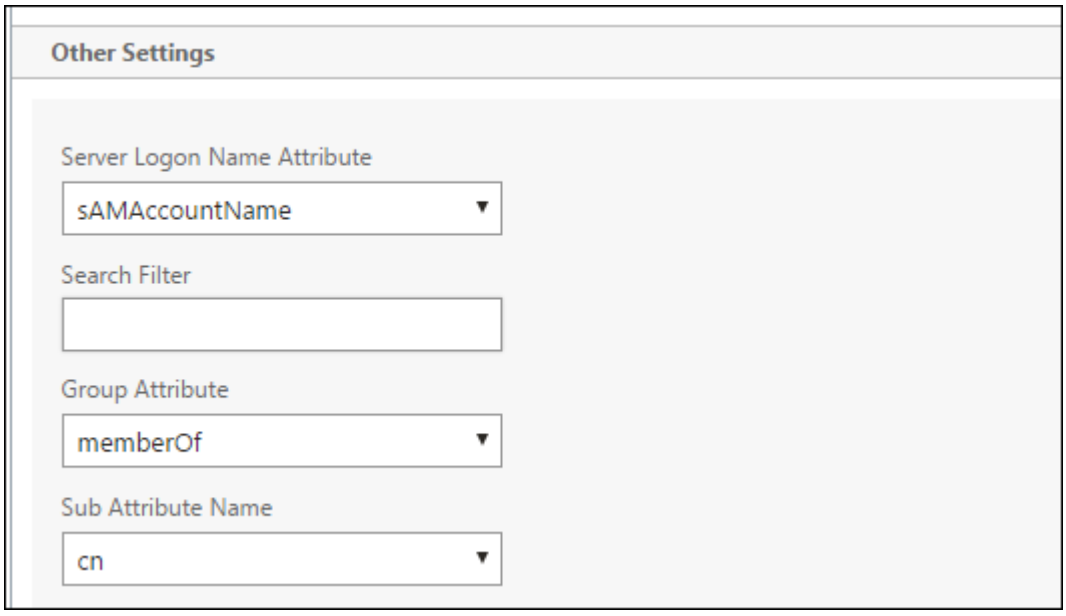
Configurar la autenticación para varios dominios

Si tiene varias instancias de XenMobile Server (por ejemplo, para entornos de prueba, desarrollo y producción), debe configurar Citrix Gateway manualmente para los entornos adicionales (puede usar el asistente de Citrix ADC para XenMobile solamente una vez).

Configurar Citrix Gateway

Para configurar las directivas de autenticación de Citrix Gateway y una directiva de sesión para un entorno de varios dominios:

1. En la herramienta de configuración de Citrix Gateway, en la ficha **Configuración**, expanda **Citrix Gateway > Directivas > Autenticación**.
2. En el panel de navegación, haga clic en **LDAP**.
3. Haga clic para modificar el perfil de LDAP. Cambie el **Atributo de nombre de inicio de sesión del servidor** a **userPrincipalName** o al atributo que quiera utilizar para las búsquedas. Anote el atributo que especifique, de manera que lo tenga disponible al configurar los parámetros de LDAP en la consola de XenMobile.



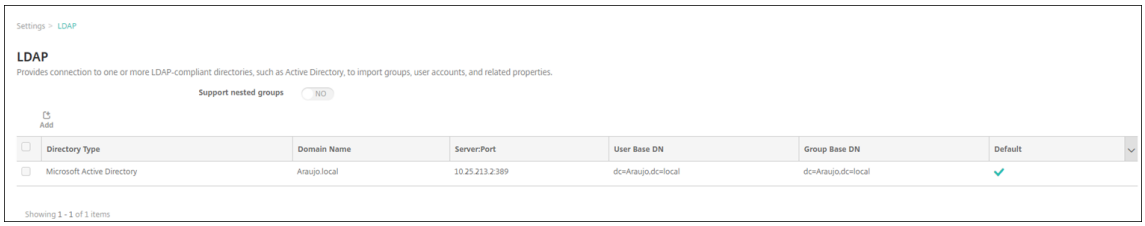
4. Repita estos pasos para cada directiva de LDAP. Se requiere una directiva de LDAP diferente para cada dominio.

5. En la directiva de sesión vinculada al servidor virtual de Citrix Gateway, vaya a **Modificar perfil de sesiones > Aplicaciones publicadas**. Compruebe que la opción **Single Sign-On Domain** está en blanco.

Configuración de XenMobile Server

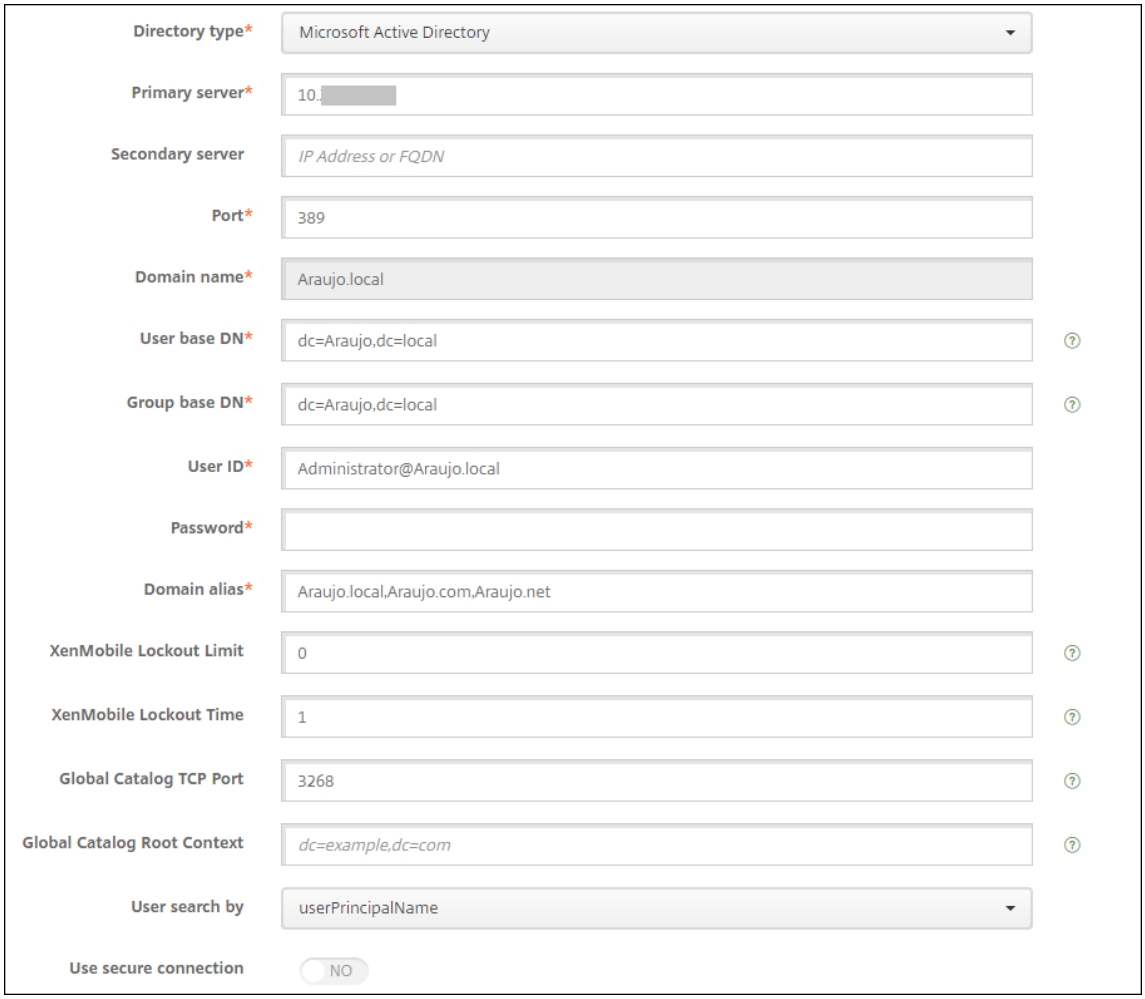
Para configurar LDAP para un entorno de XenMobile de varios dominios:

1. En la consola de XenMobile, vaya a **Parámetros > LDAP** y agregue o modifique un directorio.



2. Proporcione la información correspondiente.

   - En **Alias de dominio**, especifique los dominios que se utilizarán para la autenticación de usuarios. Separe los dominios con una coma y no introduzca espacios entre ellos. Por ejemplo: `domain1.com,domain2.com,domain3.com`
   - Compruebe que el campo **Buscar usuarios por** coincide con el valor de **Atributo de nombre de inicio de sesión del servidor** especificado en la directiva de LDAP de Citrix Gateway.



Descartar solicitudes de conexión entrantes a direcciones URL específicas

Si Citrix Gateway en su entorno está configurado para la descarga de SSL, puede que prefiera que la puerta de enlace descarte las solicitudes de conexión entrantes para direcciones URL específicas.

Si prefiere esa seguridad adicional, configure los dos servidores virtuales del equilibrador de carga para MDM (uno para el puerto 443 y otro para el puerto 8443) en Citrix Gateway. Utilice la siguiente información como plantilla para los parámetros.

> **Importante:**
>
> Las siguientes actualizaciones son solo para dispositivos Citrix Gateway configurados para la descarga de SSL.

1. Cree un conjunto de patrones con el nombre `XMS_DropURLs`.

```
1 add policy patset XMS_DropURLs
2 <!--NeedCopy-->
```


2. Agregue las siguientes URL al nuevo conjunto de patrones. Personalice esta lista según sea necesario.

```
bind policy patset XMS_DropURLs /zdm/shp/console -index 6

bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5

bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4

bind policy patset XMS_DropURLs /zdm/log.jsp -index 3

bind policy patset XMS_DropURLs /zdm/login.jsp -index 2

bind policy patset XMS_DropURLs /zdm/console -index 1
<!--NeedCopy-->
```

3. Cree una directiva para eliminar todo el tráfico dirigido a estas direcciones URL, a menos que la solicitud de conexión se origine en la subred especificada.

```
add responder policy XMS_DROP_pol  “CLIENT.IP.SRC.IN_SUBNET
    (192.168.0.0/24).NOT &&
HTTP.REQ.URL.CONTAINS_ANY(” XMS_DropURLs” )”  DROP -comment "Allow
     only subnet 192.168.0.0/24 to access these URLs. All other
    connections are DROPed"
<!--NeedCopy-->
```

4. Enlace la nueva directiva a los servidores virtuales del equilibrador de carga para MDM (puertos 443 y 8443).

```
bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName
    XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
    REQUEST

bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName
    XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
    REQUEST
<!--NeedCopy-->
```

Autenticación con dominio o dominio y token de seguridad

January 4, 2022

XenMobile admite la autenticación basada en dominios en uno o varios directorios, 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.

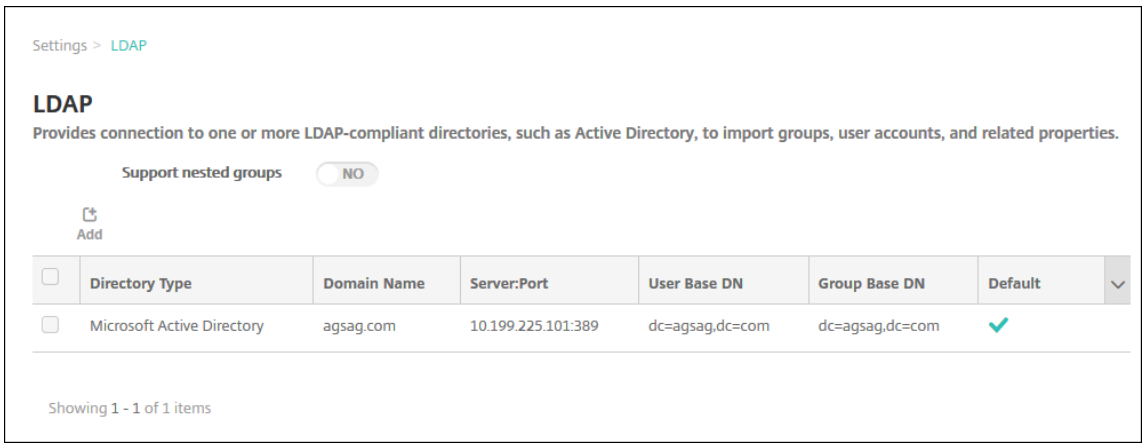
Un uso común de LDAP es proporcionar Single Sign-On a los usuarios, donde varios servicios comparten una sola contraseña (por usuario). Single Sign-On permite a los usuarios iniciar sesión una vez en el sitio web de la empresa para obtener acceso autenticado a la intranet corporativa.

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

> **Importante:**
>
> Una vez que los usuarios hayan inscrito sus dispositivos en XenMobile, XenMobile no admite que se cambie el modo de autenticación de dominio a otro modo de autenticación.

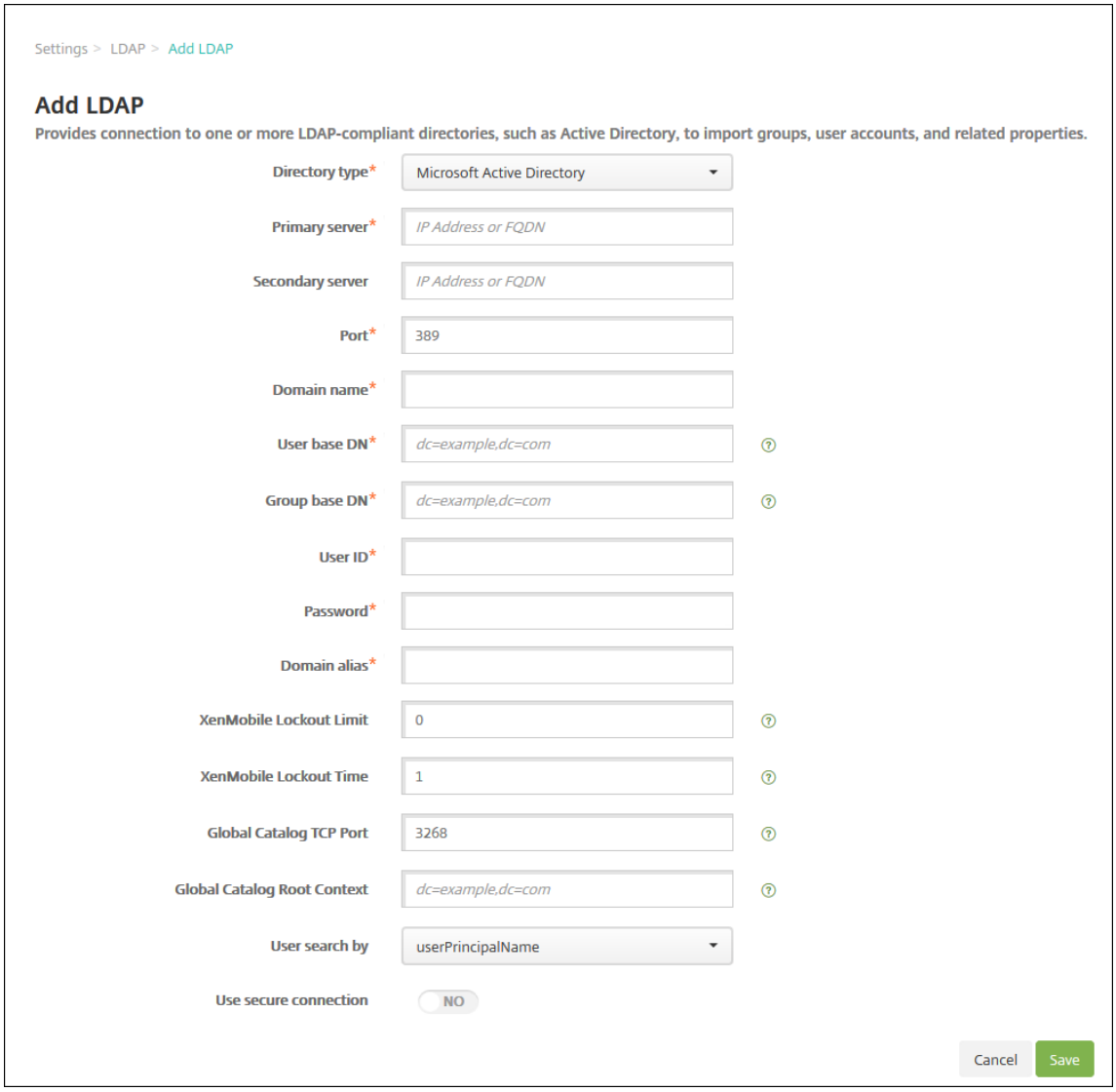
Para agregar conexiones LDAP a XenMobile

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 **Parámetros**.
2. En **Servidor**, haga clic en **LDAP**. Aparecerá la página **LDAP**. Puede agregar, modificar o eliminar directorios compatibles con el protocolo LDAP como se describe en este artículo.



Para agregar un directorio compatible con LDAP

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



2. Configure estos parámetros:

   - **Tipo de directorio:** En la lista, haga clic en el tipo de directorio correspondiente. El valor predeterminado es **Microsoft Active Directory**.
   - **Servidor principal:** Escriba el servidor principal usado para el protocolo LDAP; puede escribir la dirección IP o el nombre de dominio completo (FQDN).
   - **Servidor secundario:** 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.
   - **Puerto:** Escriba el número de puerto que utiliza el servidor LDAP. De forma predetermi-

nada, 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.

- **Nombre de dominio:** Introduzca el nombre de dominio.
- **DN base de usuarios:** Mediante un identificador único, escriba la ubicación de los usuarios en Active Directory. Los ejemplos de sintaxis son: `ou=users`, `dc=example` o `dc=com`.
- **DN base de grupos:** Escriba la ubicación de los grupos de Active Directory. Por ejemplo, `cn=users, dc=domain, dc=net`, donde `cn=users` representa el nombre del contenedor de los grupos y `dc` representa el componente de dominio de Active Directory.
- **ID de usuario:** Escriba el ID de usuario asociado a la cuenta de Active Directory.
- **Contraseña:** Escriba la contraseña asociada al usuario.
- **Alias de dominio:** Escriba un alias del nombre de dominio. Si cambia el parámetro **Alias del dominio** después de la inscripción, los usuarios deben volver a inscribirse.
- **Límite de bloqueo de XenMobile:** 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.
- **Duración de bloqueo de XenMobile:** 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. Un valor de **0** significa que no se obliga al usuario a esperar después de un bloqueo.
- **Puerto TCP del catálogo global:** 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**.
- **Contexto raíz del catálogo global:** Si quiere, puede escribir el valor del contexto raíz del catálogo global utilizado para habilitar una búsqueda en el catálogo global de Active Directory. Esta búsqueda se agrega a la búsqueda estándar LDAP en cualquier dominio y sin necesidad de especificar el nombre de dominio real.
- **Buscar usuarios por:** En la lista, haga clic en **userPrincipalName** o en **sAMAccountName**. El valor predeterminado es **userPrincipalName**. Si cambia el parámetro **Buscar usuarios por** después de la inscripción, los usuarios deben volver a inscribirse.
- **Usar conexión segura:** Seleccione si utilizar conexiones protegidas. De forma predeterminada, está **desactivado**.

3. Haga clic en **Guardar**.

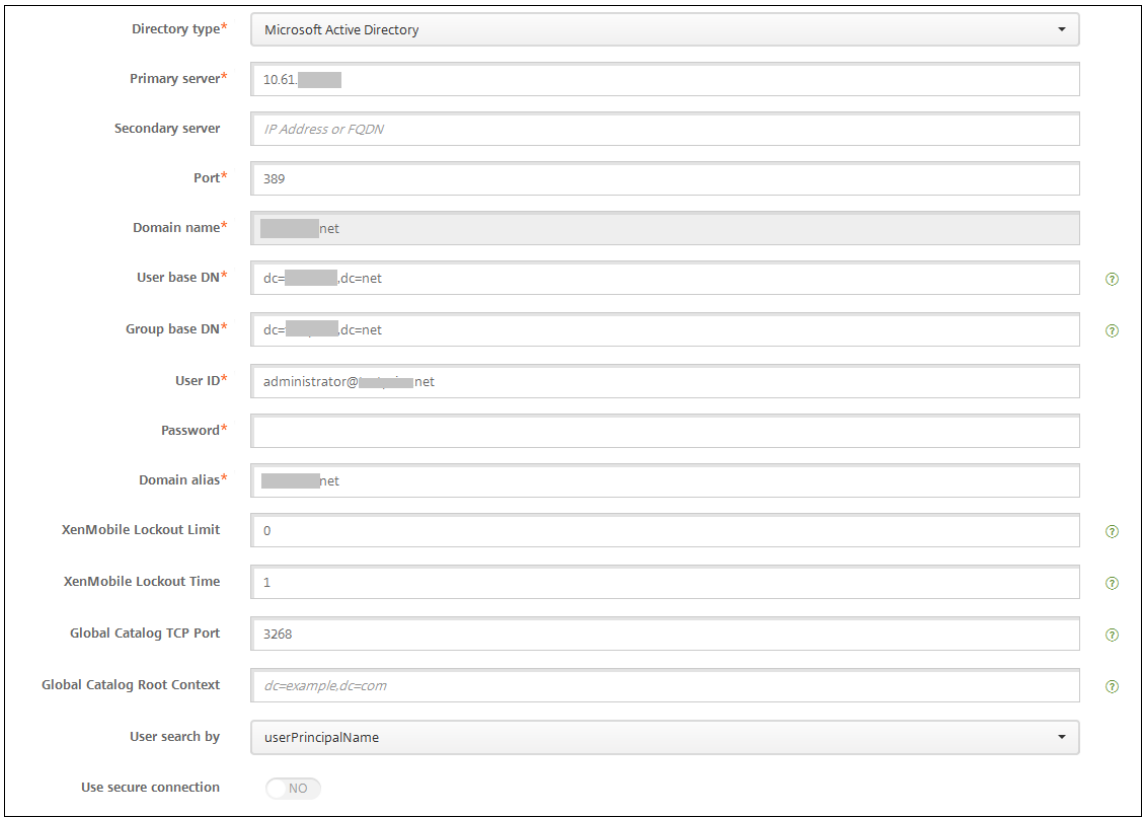
Para modificar un directorio compatible con LDAP

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

   Cuando se marca la casilla situada junto a un directorio, el menú de opciones aparece encima

de la lista de LDAP. Si hace clic en cualquier lugar de la lista, el menú de opciones aparece a la derecha de la lista.

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



3. Cambie la siguiente información como corresponda:

   - **Tipo de directorio:** En la lista, haga clic en el tipo de directorio correspondiente.
   - **Servidor principal:** Escriba el servidor principal usado para el protocolo LDAP; puede escribir la dirección IP o el nombre de dominio completo (FQDN).
   - **Servidor secundario:** Puede introducir la dirección IP o el nombre de dominio completo (FQDN) del servidor secundario (si se ha configurado).
   - **Puerto:** 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.
   - **Nombre de dominio:** No puede modificar este campo.
   - **DN base de usuarios:** Mediante un identificador único, escriba la ubicación de los usuarios en Active Directory. Los ejemplos de sintaxis son: `ou=users`, `dc=example` o `dc=com`.
   - **DN base de grupos:** Escriba el nombre del grupo de DN base especificado como `cn=groupname`. Por ejemplo, `cn=users`, `dc=servername`, `dc=net`, donde `cn=users` es el nombre del grupo. `DN` y `servername` representan el nombre del servidor que ejecuta

Active Directory.

- **ID de usuario:** Escriba el ID de usuario asociado a la cuenta de Active Directory.
- **Contraseña:** Escriba la contraseña asociada al usuario.
- **Alias de dominio:** Escriba un alias del nombre de dominio. Si cambia el parámetro **Alias del dominio** después de la inscripción, los usuarios deben volver a inscribirse.
- **Límite de bloqueo de XenMobile:** 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.
- **Duración de bloqueo de XenMobile:** 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. Un valor de **0** significa que no se obliga al usuario a esperar después de un bloqueo.
- **Puerto TCP del catálogo global:** 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**.
- **Contexto raíz del catálogo global:** Si quiere, puede escribir el valor del contexto raíz del catálogo global utilizado para habilitar una búsqueda en el catálogo global de Active Directory. Esta búsqueda se agrega a la búsqueda estándar LDAP en cualquier dominio y sin necesidad de especificar el nombre de dominio real.
- **Buscar usuarios por:** En la lista, haga clic en **userPrincipalName** o en **sAMAccountName**. Si cambia el parámetro **Buscar usuarios por** después de la inscripción, los usuarios deben volver a inscribirse.
- **Usar conexión segura:** Seleccione si utilizar conexiones protegidas.

4. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para descartarlos.

Para eliminar un directorio compatible con LDAP

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

   Puede eliminar más de una propiedad. Para ello, marque 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 **Eliminar**.

Configurar la autenticación para varios dominios

Si quiere configurar XenMobile Server para que utilice varios sufijos de dominio en una configuración LDAP, consulte el procedimiento Configurar la autenticación para varios dominios en la

documentación de Citrix Endpoint Management. Los pasos en la versión local de XenMobile Server y en la versión en la nube de Endpoint Management son los mismos.

Configurar la autenticación de dominio y token de seguridad

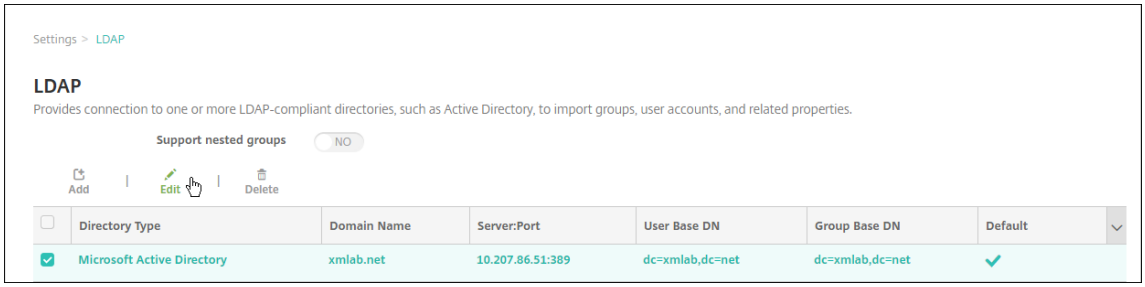
Puede configurar XenMobile para exigir a los usuarios que se autentiquen mediante el protocolo RADIUS con sus credenciales de LDAP más una contraseña de un solo uso.

Para una experiencia de uso óptima, puede combinar esta configuración con el PIN de Citrix y el almacenamiento en caché de contraseñas de Active Directory. Con esa configuración, los usuarios no tienen que escribir repetidamente sus nombres de usuario ni contraseñas LDAP. Los usuarios escriben su nombre de usuario y contraseña para la inscripción, la caducidad de contraseñas y el bloqueo de cuentas.

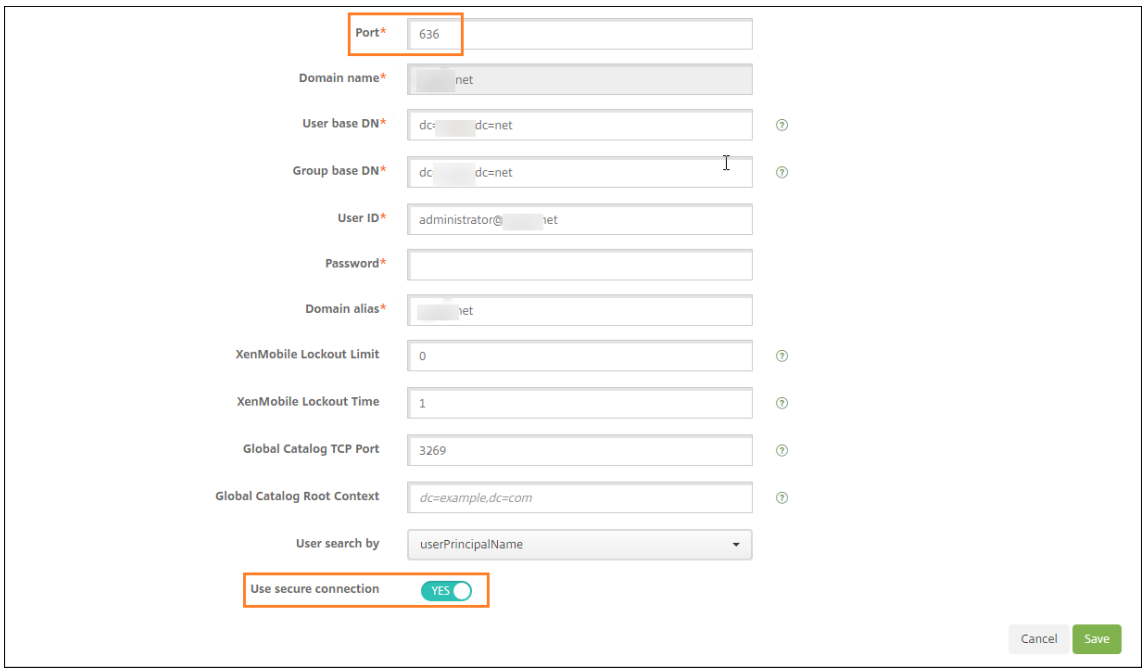
Configurar parámetros de LDAP

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 **Parámetros**, haga clic en **LDAP**.
2. Seleccione **Microsoft Active Directory** y, a continuación, haga clic en **Modificar**.



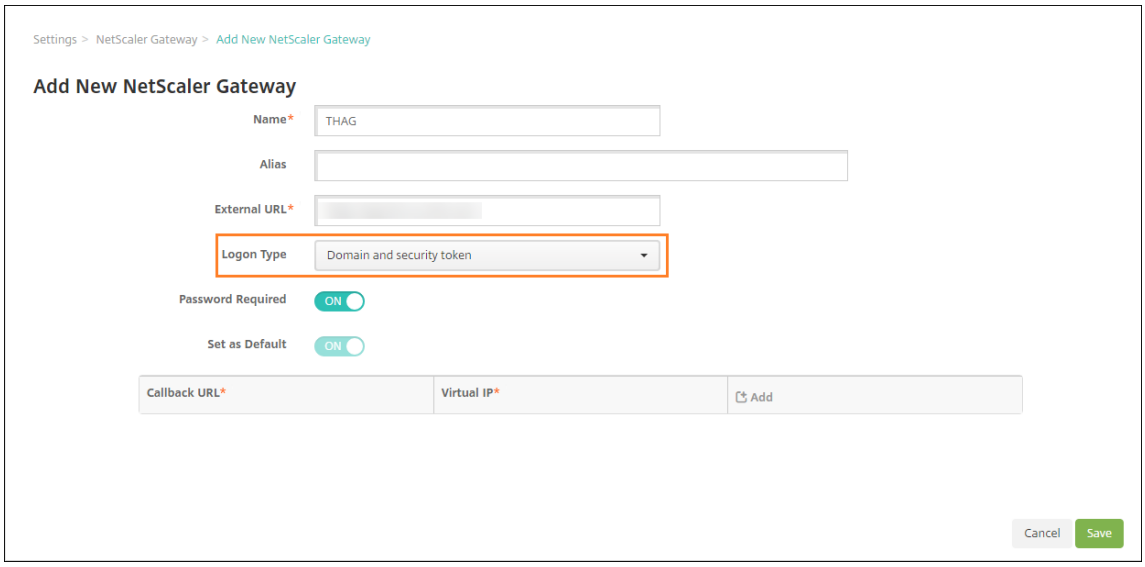
3. Verifique que el campo “Puerto” tiene el valor **636** para conexiones LDAP seguras, o bien **3269** para conexiones LDAP seguras de Microsoft.
4. Cambie **Usar conexión segura** a **Sí**.



Configurar parámetros de Citrix Gateway

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

1. En **Parámetros**, haga clic en **Citrix Gateway**.
2. Seleccione **Citrix Gateway** y, a continuación, haga clic en **Modificar**.
3. En **Tipo de inicio de sesión**, seleccione **Dominio y token de seguridad**.



Habilitar el PIN de Citrix y el almacenamiento en caché de contraseñas de usuario

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

Configurar Citrix Gateway para la autenticación con dominio y token de seguridad

Configure directivas y perfiles de sesión de Citrix Gateway para los servidores virtuales que utilice con XenMobile. Para obtener información, consulte la documentación de Citrix Gateway.

Autenticación con certificado de cliente o certificado y dominio

January 4, 2022

En XenMobile, la autenticación predeterminada 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 del usuario. La autenticación con certificado y dominio tiene las mejores posibilidades de SSO junto con la seguridad que proporciona la autenticación de dos factores en Citrix ADC.

Para una experiencia de uso óptima, puede combinar la autenticación por certificado y dominio junto con el PIN de Citrix y el almacenamiento en caché de contraseñas de Active Directory. Con resultado, los usuarios no tienen que escribir repetidamente sus nombres de usuario ni contraseñas LDAP. Los usuarios escriben su nombre de usuario y contraseña para la inscripción, la caducidad de contraseñas y el bloqueo de cuentas.

> **Importante:**
>
> Una vez que los usuarios hayan inscrito sus dispositivos en XenMobile, XenMobile no admite que se cambie el modo de autenticación de dominio a otro modo de autenticación.

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. Cuando 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 de Citrix ADC para XenMobile para llevar a cabo la configuración necesaria para XenMobile cuando se usa la autenticación con solo certificado o la autenticación con certificado y dominio en Citrix ADC. Puede ejecutar el asistente de Citrix ADC 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. Para entornos altamente seguros, la autenticación de dos factores mediante un certificado del cliente y un token de seguridad es una posibilidad. Para obtener más información, consulte Configuración de XenMobile para la autenticación con certificado y token de seguridad.

La autenticación con 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 con 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 con certificado del cliente en los modos ENT y MAM de XenMobile, debe configurar el servidor Microsoft, XenMobile Server y, a continuación, Citrix 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 XenMobile Server:

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

Para obtener información sobre la configuración de Citrix Gateway, consulte los siguientes artículos de la documentación de Citrix ADC:

- Autenticación del cliente
- Infraestructura de los perfiles SSL
- Configuring and Binding a Client Certificate Authentication Policy

Requisitos previos

- Cuando cree plantillas de entidad para Servicios de certificado de Microsoft, no use caracteres especiales para evitar posibles problemas de autenticación en los dispositivos inscritos. Por ejemplo, no use estos caracteres en el nombre de la plantilla: `: ! $ ()## % + * ~ ? | { } []`
- Para dispositivos Windows Phone 8.1 que usan autenticación con certificados y descarga SSL, debe inhabilitar la reutilización de sesiones SSL para el puerto 443 en los dos servidores virtuales de equilibrio de carga en Citrix ADC. Para ello, ejecute el siguiente comando para el puerto 443 en el servidor virtual:

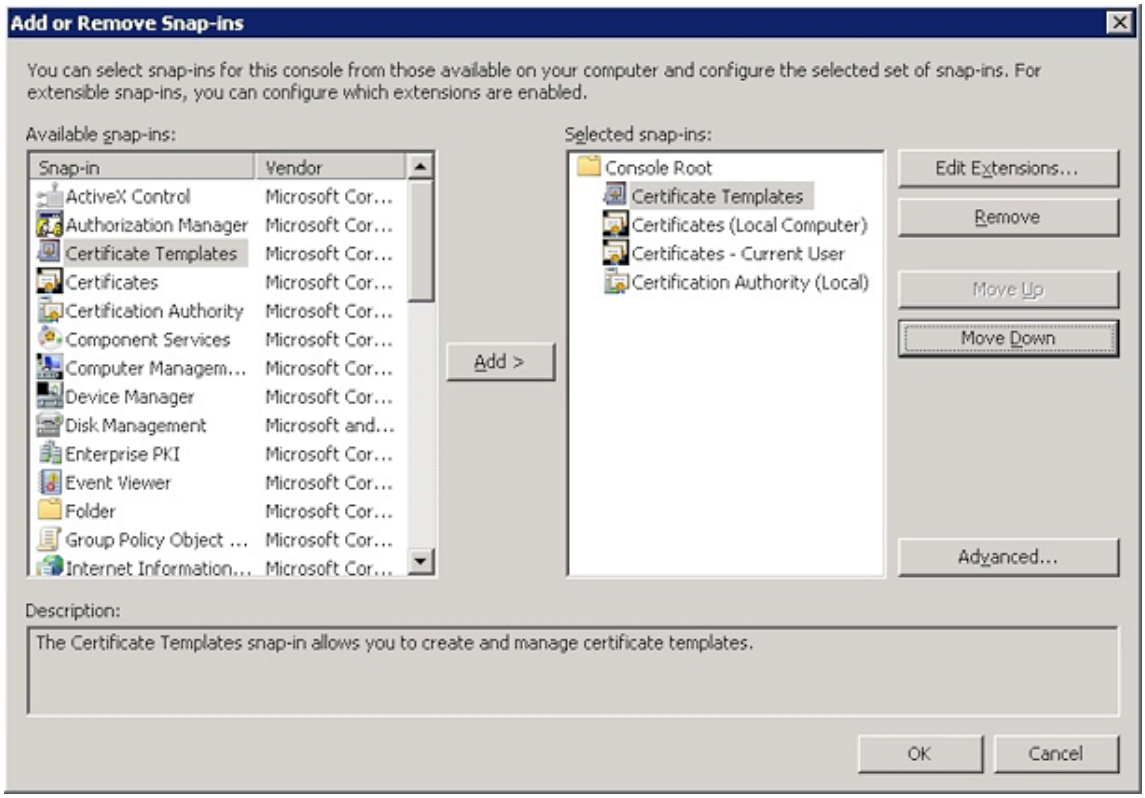
  ```
  set ssl vserver <ssl lb vserver> sessReuse DISABLE
  ```


Si inhabilita la reutilización de sesiones SSL, se inhabilitan algunas de las optimizaciones que Citrix ADC ofrece, lo que puede degradar el rendimiento en Citrix ADC.

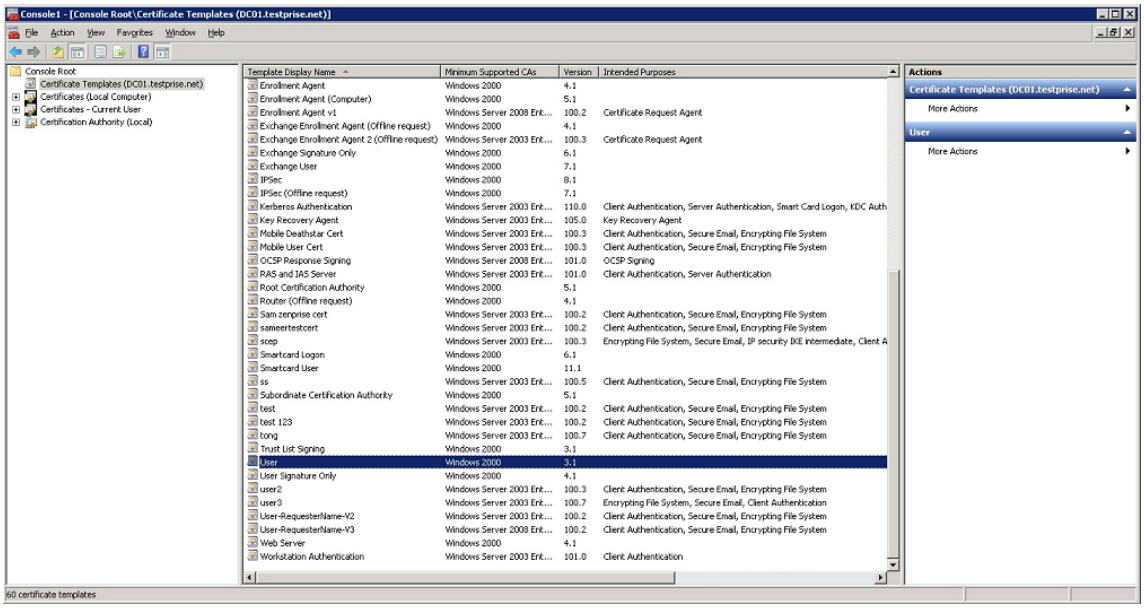
- Para configurar la autenticación basada en certificados para Exchange ActiveSync, consulte este blog de Microsoft. Configure el sitio del servidor de la entidad de certificación (CA) para que Exchange ActiveSync requiera certificados de cliente.
- Si utiliza certificados de servidor privados para proteger el tráfico de ActiveSync hacia el servidor Exchange Server, compruebe que los dispositivos móviles tienen todos los certificados raíz e intermedios necesarios. De lo contrario, la autenticación basada en certificados falla durante la configuración de buzones de correo en Secure Mail. En la consola IIS de Exchange, debe:
  - Agregar un sitio web para que XenMobile lo use con Exchange y enlazar el certificado de servidor web.
  - Usar el puerto 9443.
  - Para ese sitio web, debe agregar dos aplicaciones, una para "Microsoft-Server-ActiveSync" y otra para "EWS". En ambas aplicaciones, en **Configuración de SSL**, habilite **Requerir SSL**.

Agregar el complemento de Certificados a Microsoft Management Console

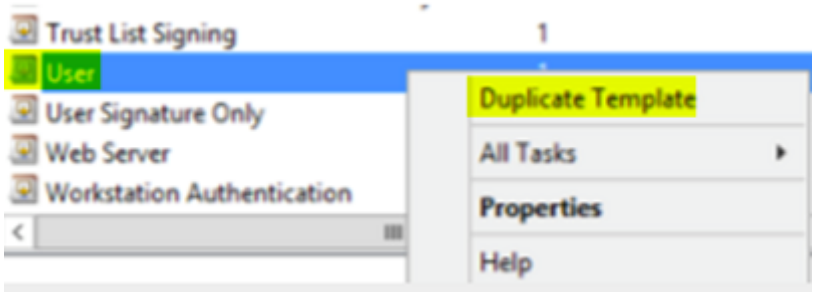
1. Abra la consola y haga clic en **Agregar o quitar complemento**.
2. Agregue los complementos siguientes:
   - Plantillas de certificado
   - Certificados (Equipo local)
   - Certificados (Usuario local)
   - Entidad de certificación (Local)



3. Expanda **Plantillas de certificado**.



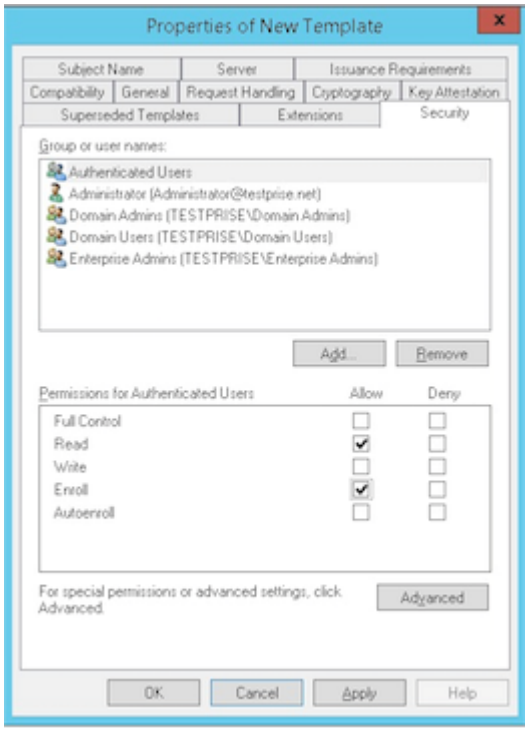
4. Seleccione la plantilla **Usuario** y **Duplicar plantilla**.



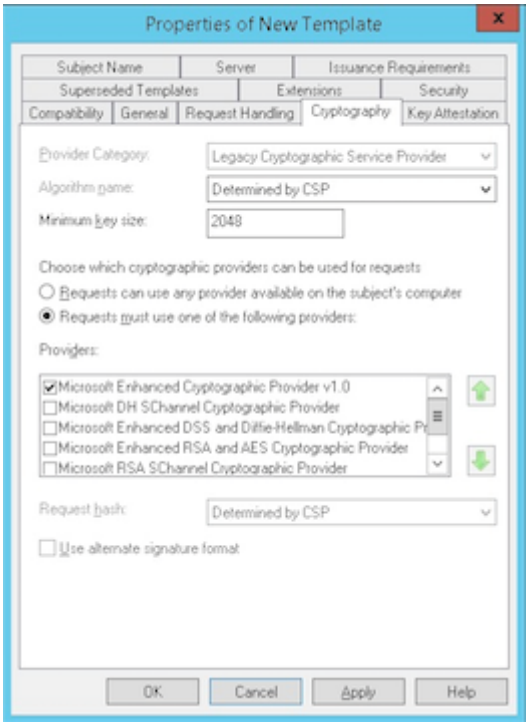
5. Suministre el nombre para mostrar de la plantilla.

> **Importante:**
>
> Marque la casilla **Publicar certificado en Active Directory** solo si es necesario. Si selecciona esta opción, todos los certificados de cliente de los usuarios se crearán en Active Directory, lo que podría desorganizar su base de datos de Active Directory.

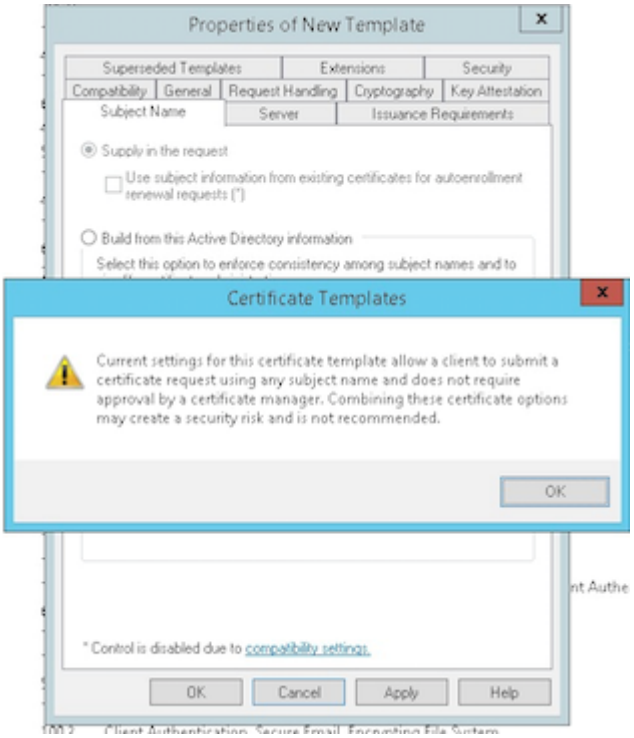
6. Seleccione **Windows 2003 Server** como tipo de plantilla. En Windows 2012 R2 Server, en **Compatibilidad**, seleccione **Entidad de certificación** y defina **Windows 2003** como destinatario.
7. En **Seguridad**, seleccione la opción **Inscribir** en la columna **Permitir** para los usuarios autenticados.



8. En **Criptografía**, compruebe que indica el tamaño de la clave. Más adelante, al configurar XenMobile, introduzca el tamaño de esa clave.

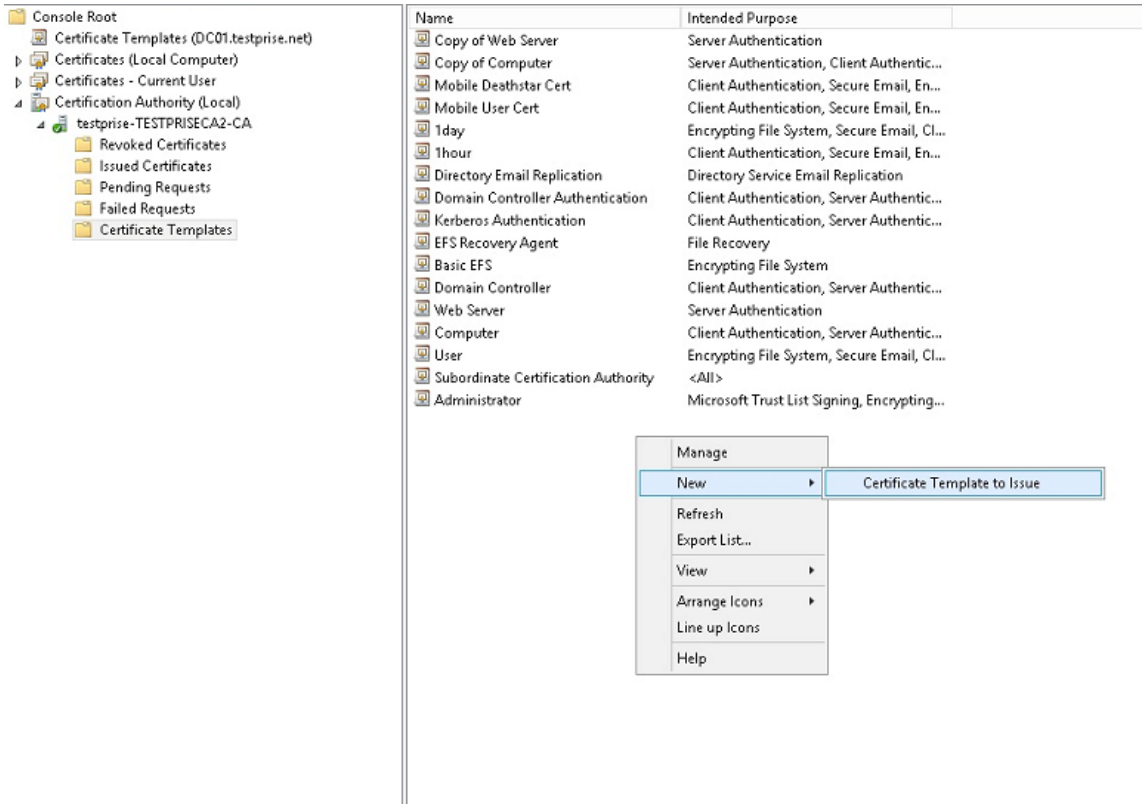


9. En **Nombre del sujeto**, seleccione **Proporcionado por el solicitante**. Aplique y guarde los cambios.

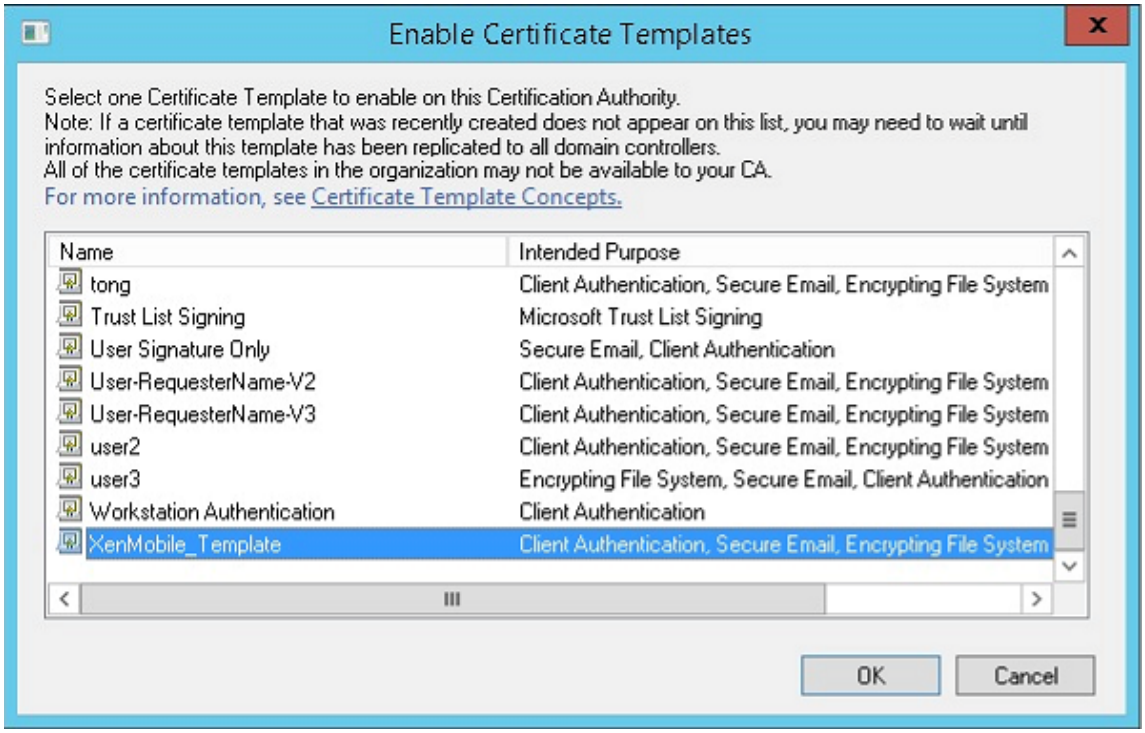


Agregar la plantilla a la entidad de certificación

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

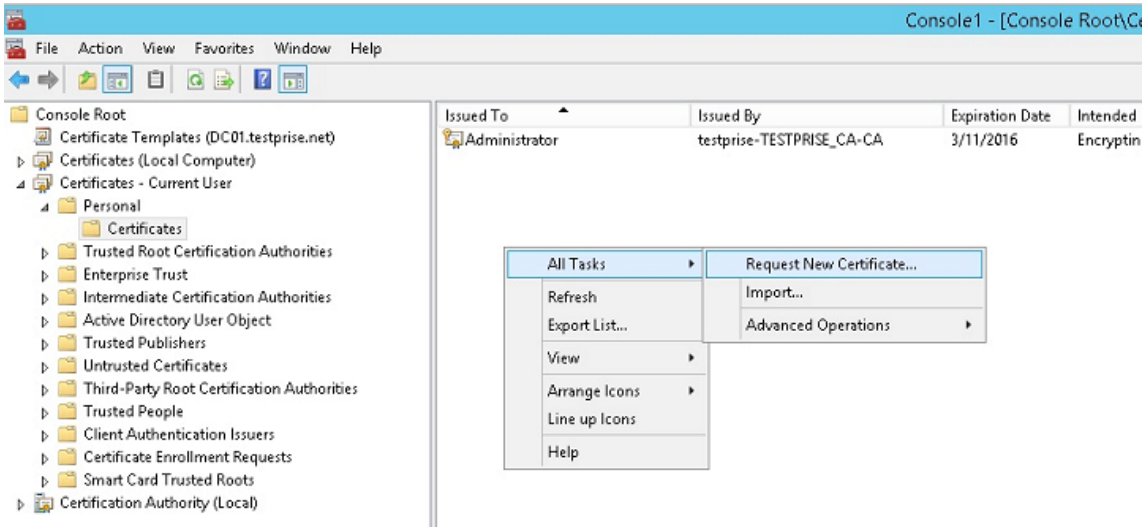


3. Seleccione la plantilla que creó en el paso anterior y haga clic en **Aceptar** para agregarla a la **Entidad de certificación**.

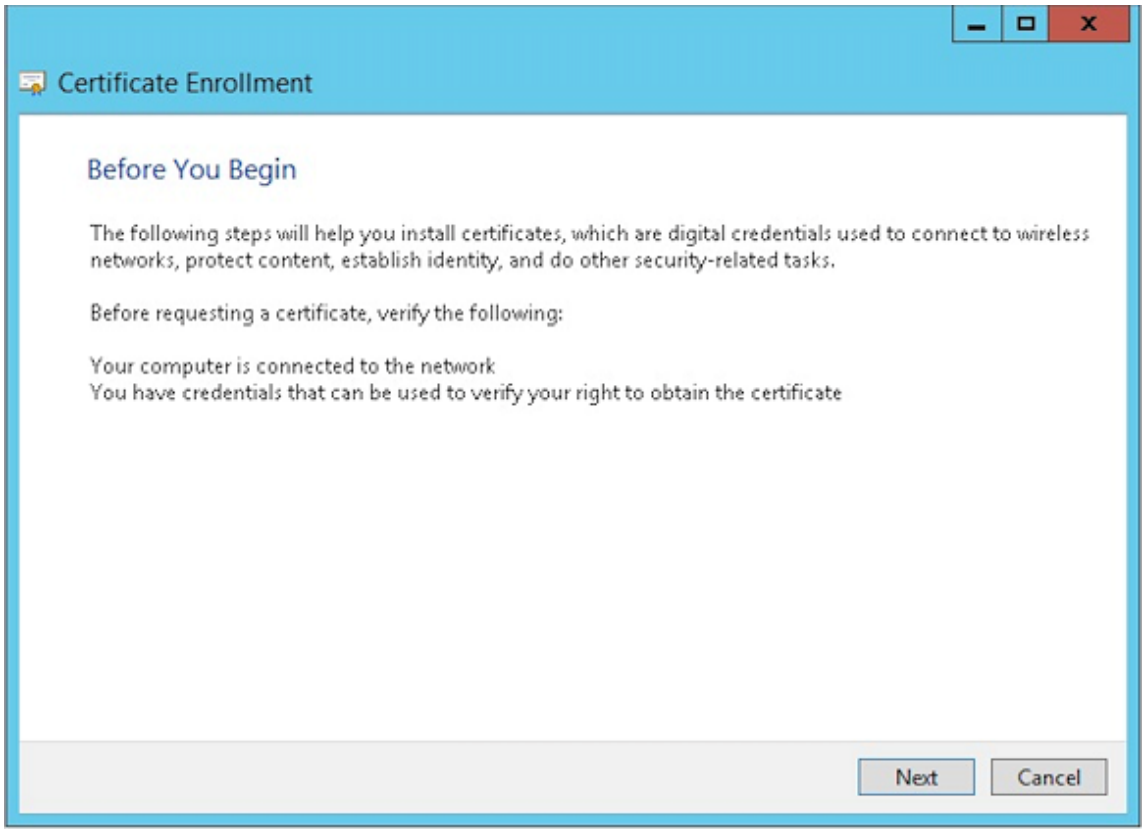


Crear un certificado PFX desde el servidor de CA

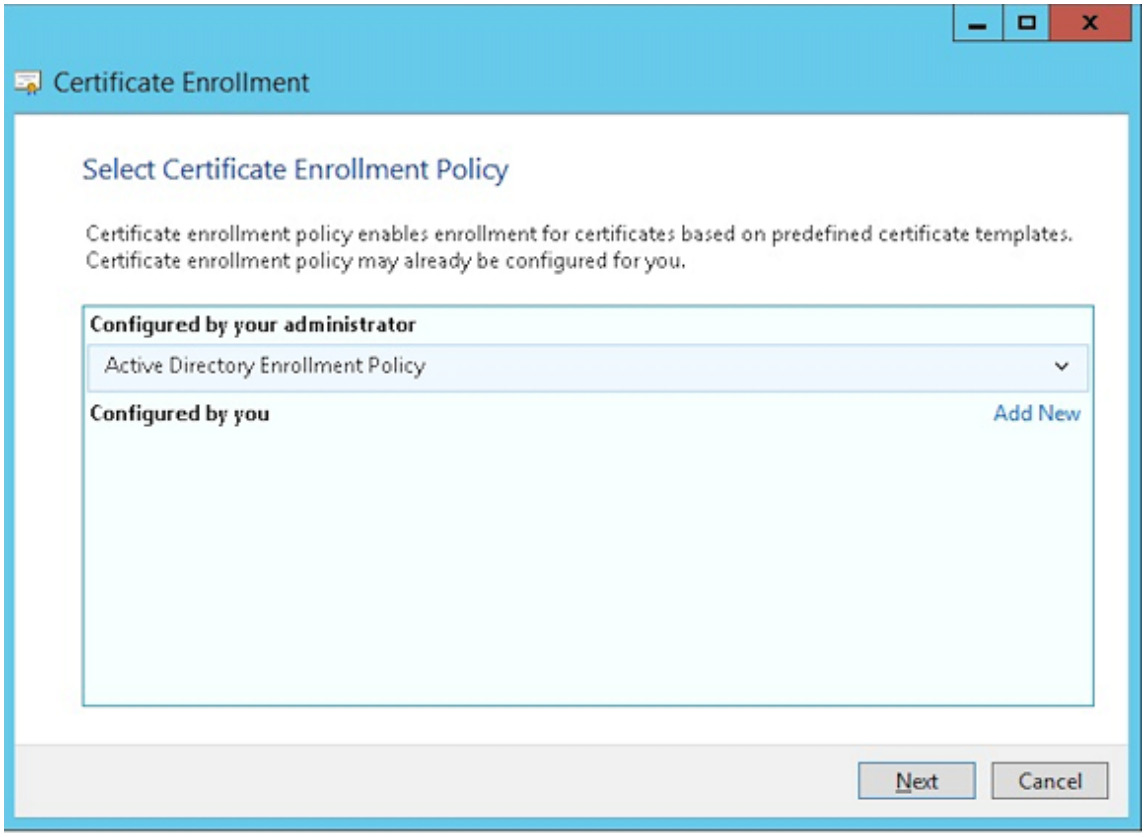
1. Cree un certificado .pfx de usuario con la cuenta de servicio con la que inició sesión. Este PFX se carga en XenMobile, con lo que se solicita un certificado de usuario de parte de los usuarios que inscriban sus dispositivos.
2. En **Usuario actual**, expanda **Certificados**.
3. Haga clic con el botón secundario en el panel derecho y después haga clic en **Solicitar un nuevo certificado**.



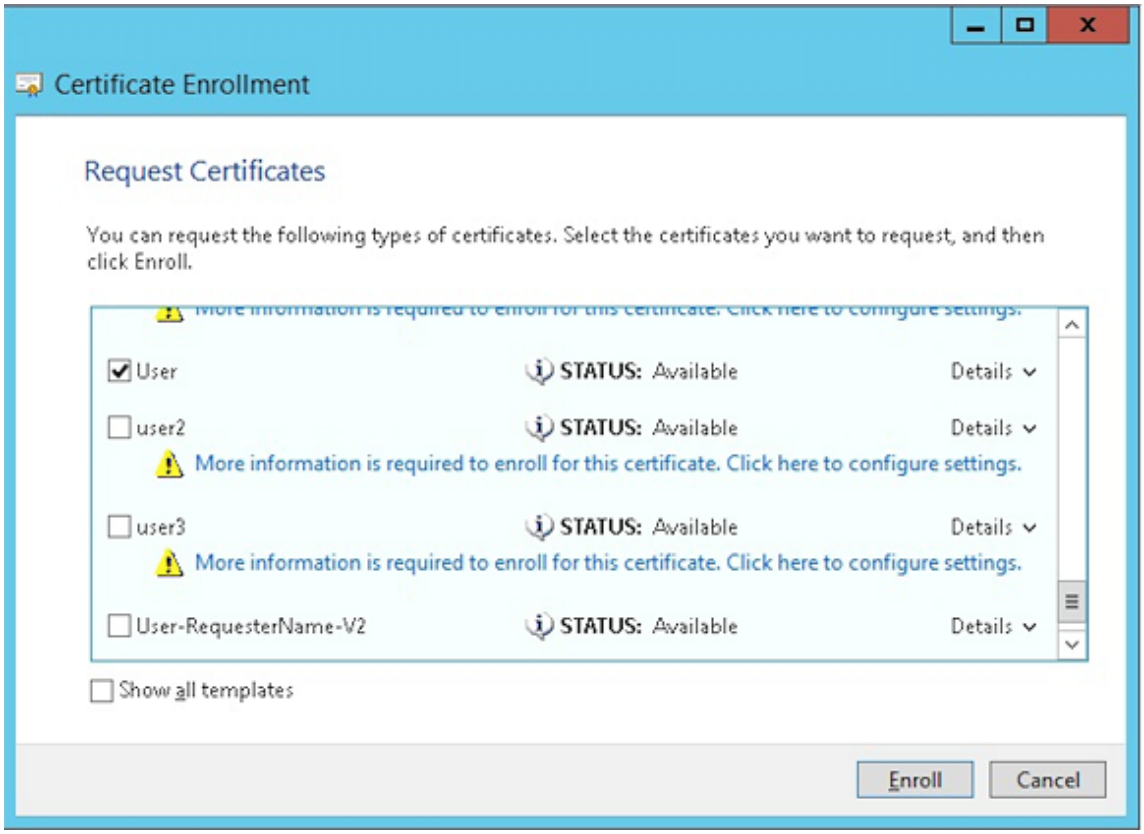
4. Aparecerá la pantalla **Inscripción de certificados**. Haga clic en **Siguiente**.



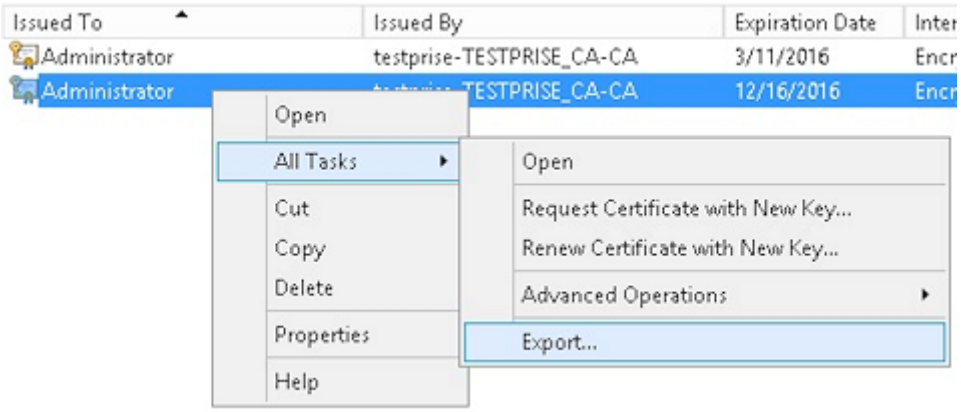
5. Seleccione **Directiva de inscripción de Active Directory** y haga clic en **Siguiente**.



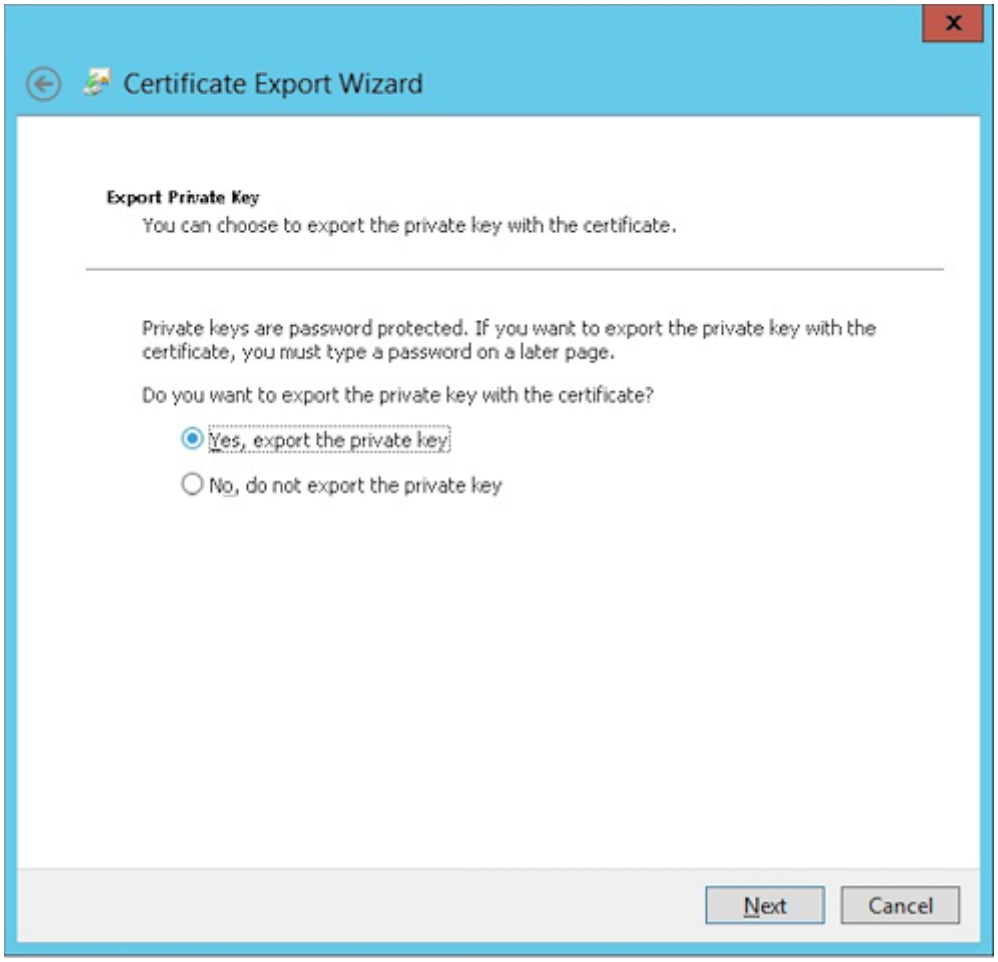
6. Seleccione la plantilla **Usuario** y haga clic en **Inscribir**.



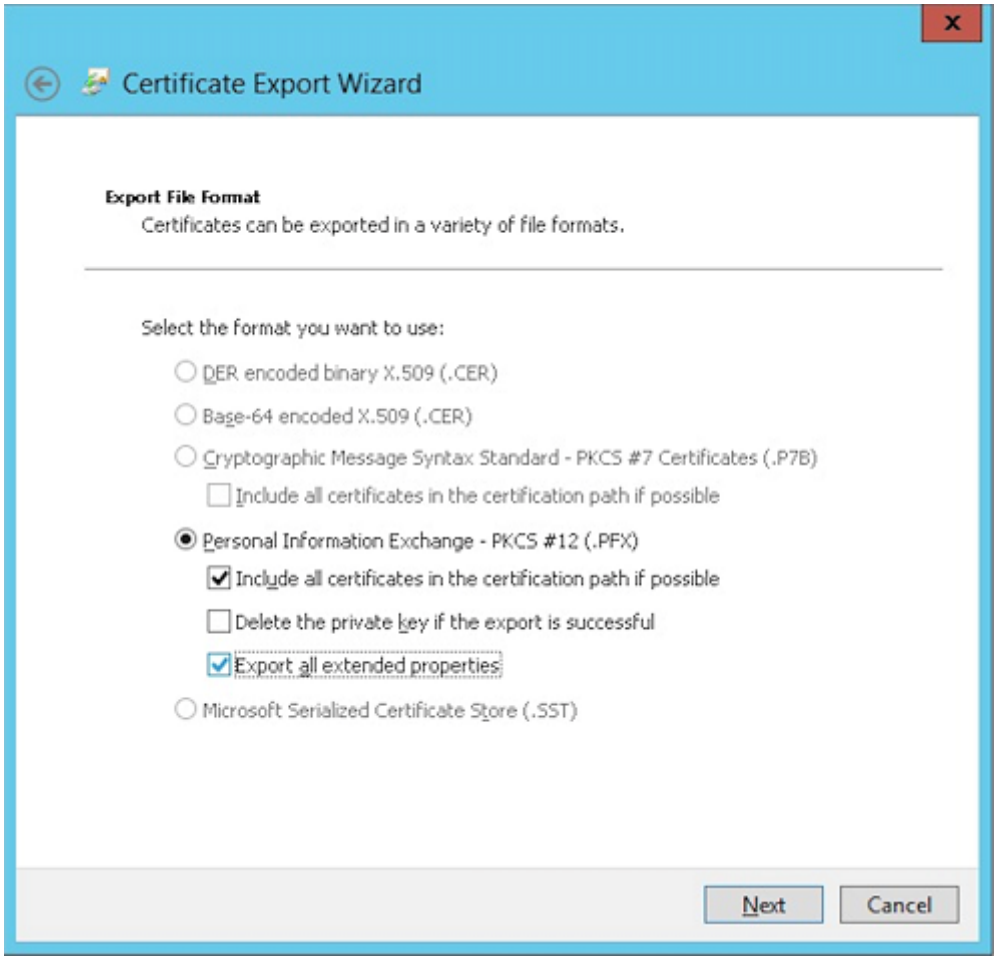
7. Exporte el archivo .pfx que creó en el paso anterior.



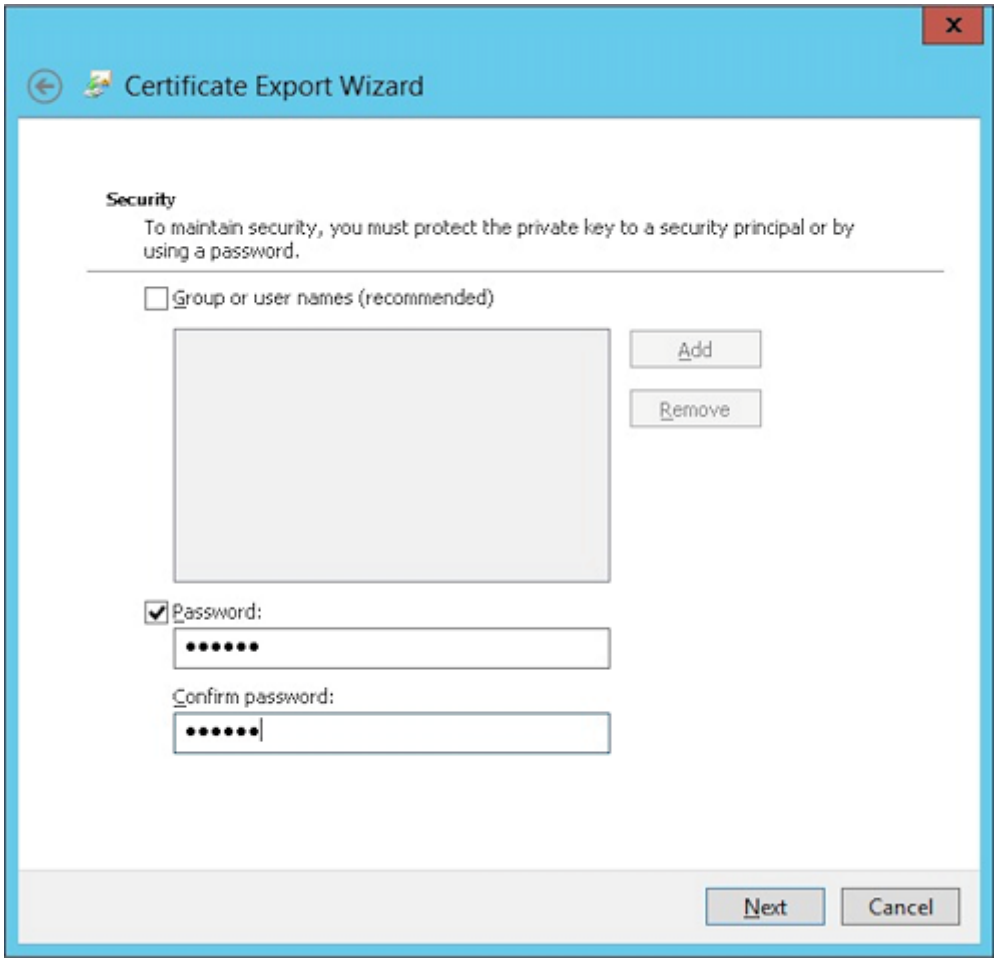
8. Haga clic en **Exportar la clave privada**.



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



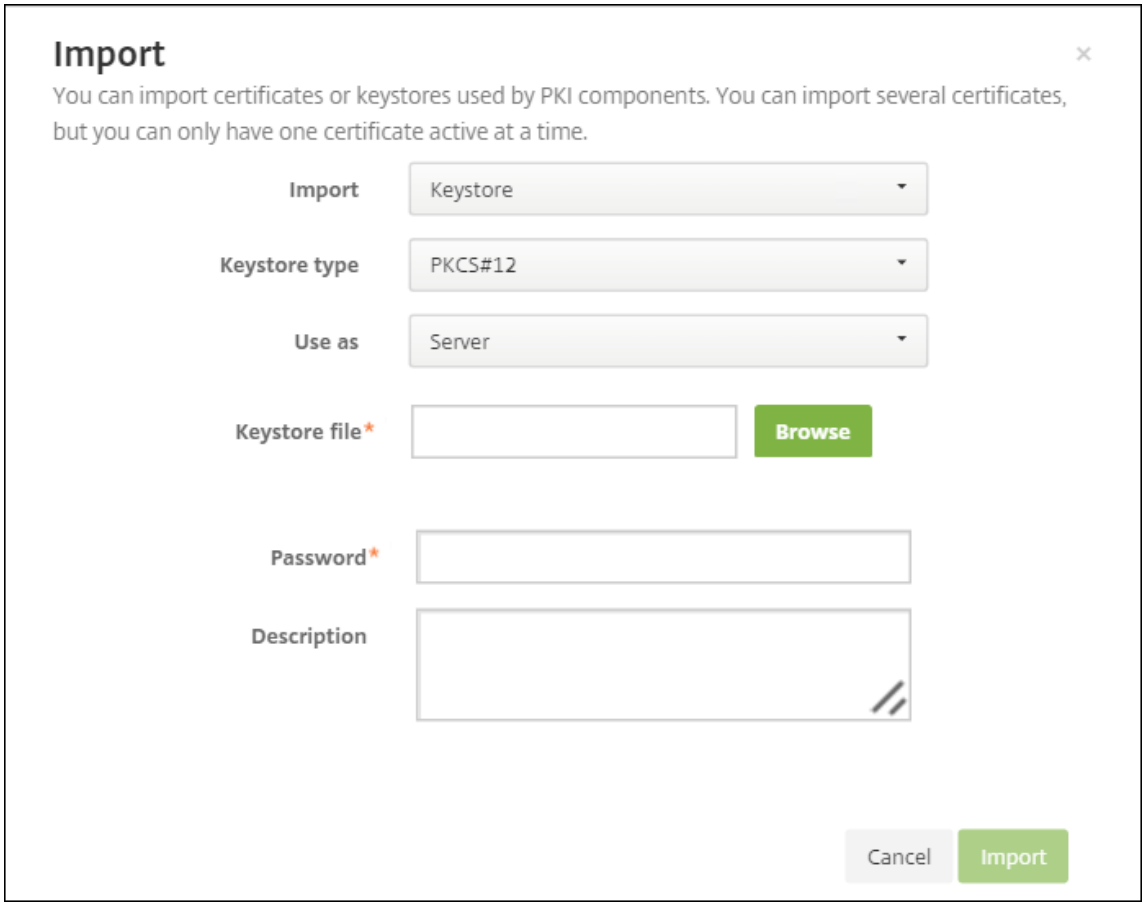
10. Defina la contraseña que va a usar para cargar este certificado en XenMobile.



11. Guarde el certificado en su disco duro.

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 **Parámetros**.
2. Haga clic en **Certificados** y, a continuación, en **Importar**.
3. Introduzca los parámetros siguientes:
   - **Importar:** Almacén de claves.
   - **Tipo de almacén de claves:** PKCS#12.
   - **Usar como:** Servidor.
   - **Archivo de almacén de claves:** Haga clic en **Examinar** para seleccionar el certificado `.pfx` que ha creado.
   - **Contraseña:** Introduzca la contraseña que creó para este certificado.

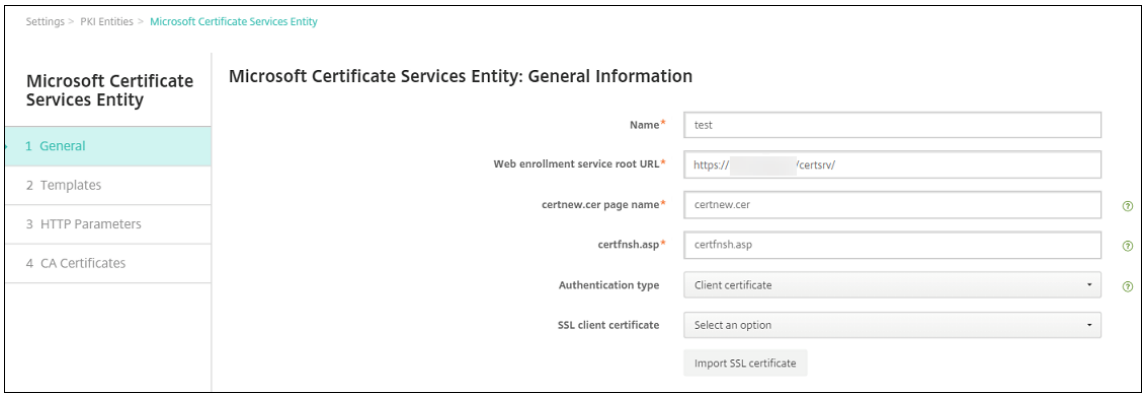


4. Haga clic en **Importar**.
5. Verifique que el certificado se ha instalado correctamente. Un certificado correctamente instalado se muestra como un certificado de usuario.

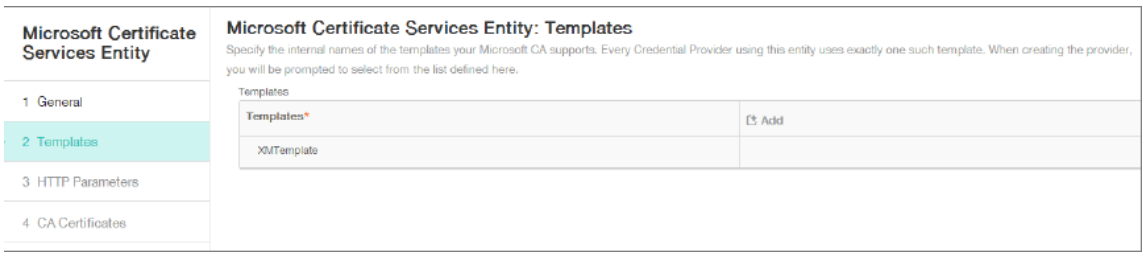
Crear la entidad PKI para la autenticación con certificados

1. En **Parámetros**, vaya a **Más > Administración de certificados > Entidades PKI**.
2. Haga clic en **Agregar** y, a continuación, haga clic en **Entidad de Servicios de certificados de Microsoft**. Aparecerá la pantalla **Entidad de Servicios de certificados de Microsoft: Información general**.
3. Introduzca los parámetros siguientes:
   - **Nombre:** Introduzca un nombre.
   - **URL raíz del servicio de inscripción web:** `https://RootCA-URL/certsrv/` Debe agregar la última barra diagonal (/) a la ruta de URL.
   - **certnew.cer page name:** certnew.cer (valor predeterminado)
   - **certfnsh.asp:** certfnsh.asp (valor predeterminado)
   - **Tipo de autenticación:** Certificado de cliente.

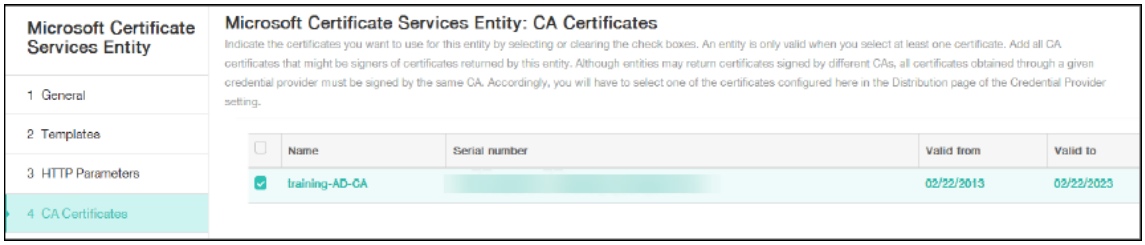
- **Certificado de cliente SSL:** Seleccione el certificado de usuario que se va a usar para emitir el certificado de cliente XenMobile.



4. En **Plantillas**, agregue la plantilla que creó cuando configuró el certificado de Microsoft. No agregue espacios.



5. Omita el paso “Parámetros HTTP” y haga clic en **Certificados de CA**.
6. Seleccione el nombre de la CA raíz que le corresponda a su entorno. Esta CA raíz es parte de la cadena importada desde el certificado cliente de XenMobile.

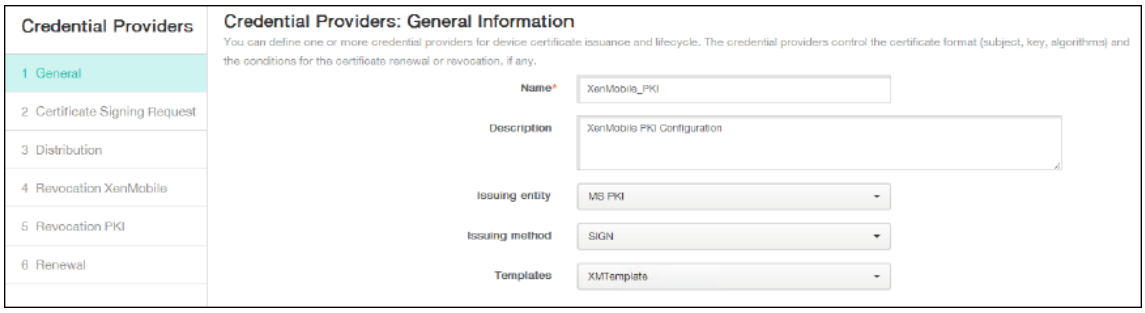


7. Haga clic en **Guardar**.

Configurar proveedores de credenciales

1. En **Parámetros**, vaya a **Más > Administración de certificados > Proveedores de credenciales**.
2. Haga clic en **Agregar**.
3. En **General**, introduzca los parámetros siguientes:
   - **Nombre:** Introduzca un nombre.
   - **Descripción:** Introduzca una descripción.

- **Entidad de emisión:** Seleccione la entidad PKI creada anteriormente.
- **Método de emisión:** SIGN.
- **Plantillas:** Seleccione la plantilla agregada en el apartado de la entidad PKI.

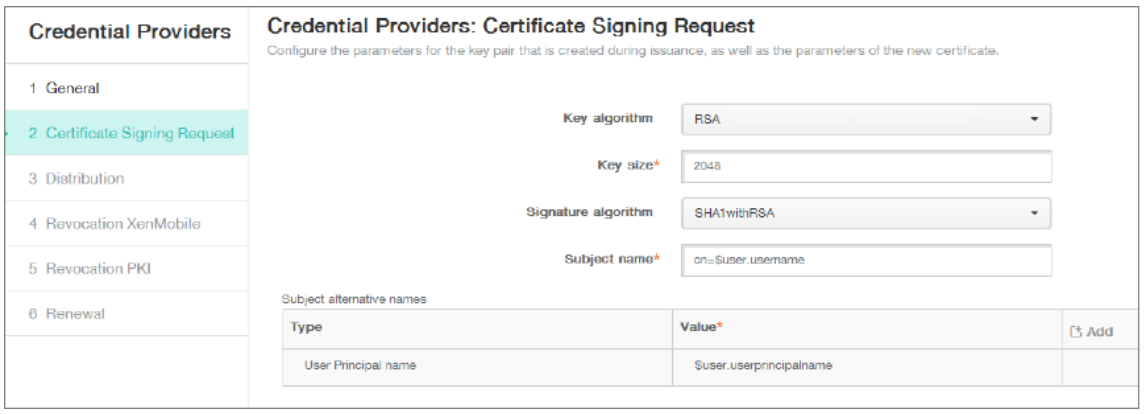


4. Haga clic en **Solicitud de firma de certificado** e introduzca los parámetros siguientes:

   - **Algoritmo de clave:** RSA
   - **Tamaño de clave:** 2048
   - **Algoritmo de firma:** SHA256withRSA
   - **Nombre del sujeto:** `cn=$user.username`

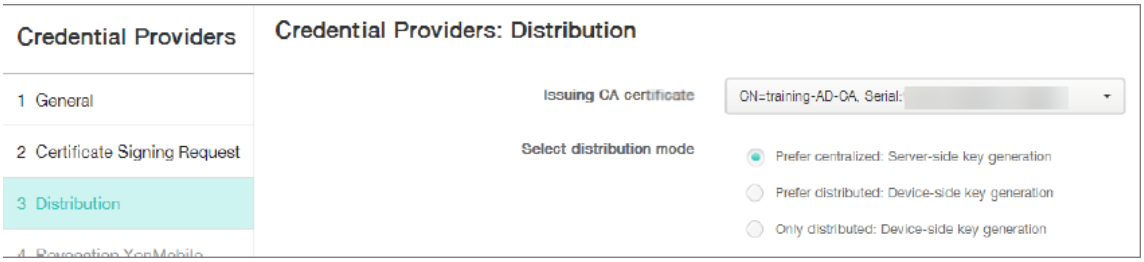
   Para **Nombre alternativo del sujeto**, haga clic en **Agregar** e introduzca los parámetros siguientes:

   - **Tipo:** Nombre principal del usuario.
   - **Valor:** `$user.userprincipalname`

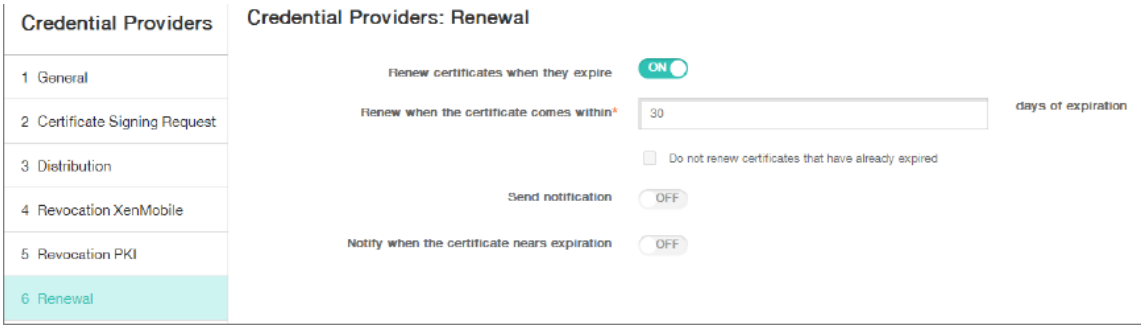


5. Haga clic en **Distribución** e introduzca los parámetros siguientes:

   - **CA emisora de certificados:** Seleccione la CA emisora que firmó el certificado del cliente XenMobile.
   - **Seleccionar modo de distribución:** Marque **Preferir modo centralizado: Generación de clave en el lado del servidor**.



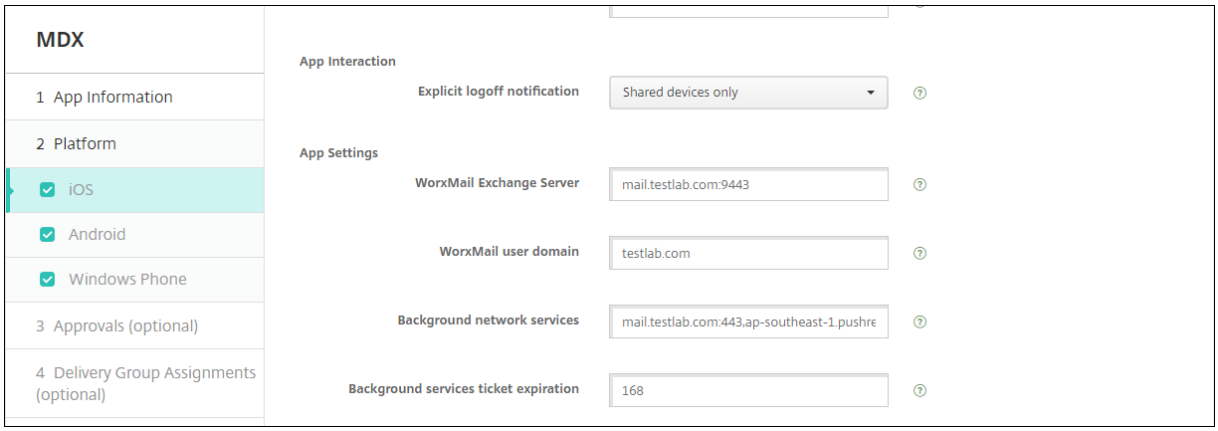
6. Para las dos secciones siguientes (**Revocación XenMobile** y **Revocación PKI**), defina los parámetros, si es necesario. En este ejemplo, ambas opciones se omiten.
7. Haga clic en **Renovación**.
8. En **Renovar certificados cuando caduquen**, seleccione **Sí**.
9. Deje todos los demás parámetros con los valores predeterminados o cámbielos si es necesario.



10. Haga clic en **Guardar**.

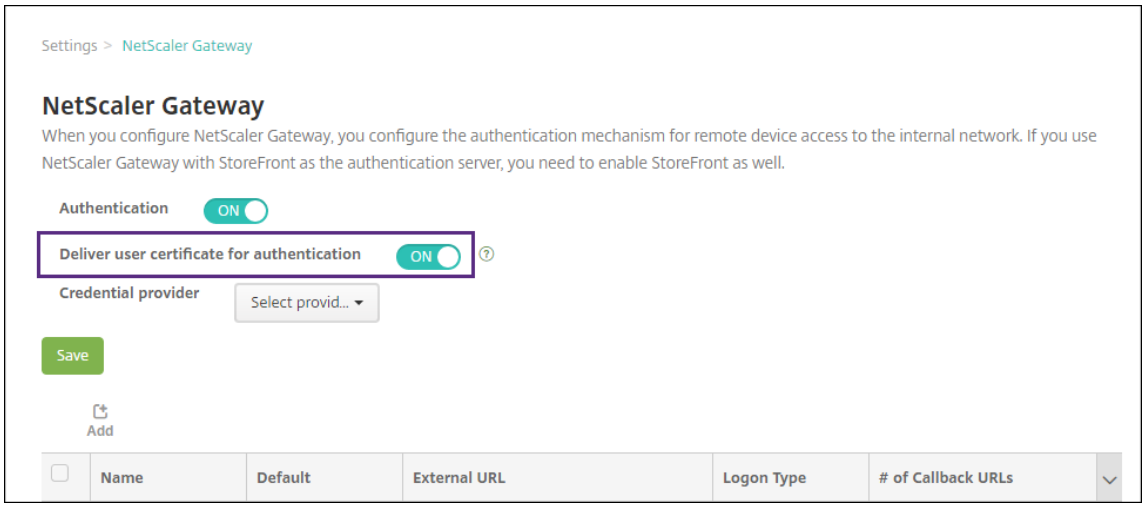
Configurar Secure Mail para la autenticación con certificados

Cuando agregue Secure Mail a XenMobile, configure los parámetros de Exchange en **Parámetros de aplicación**.

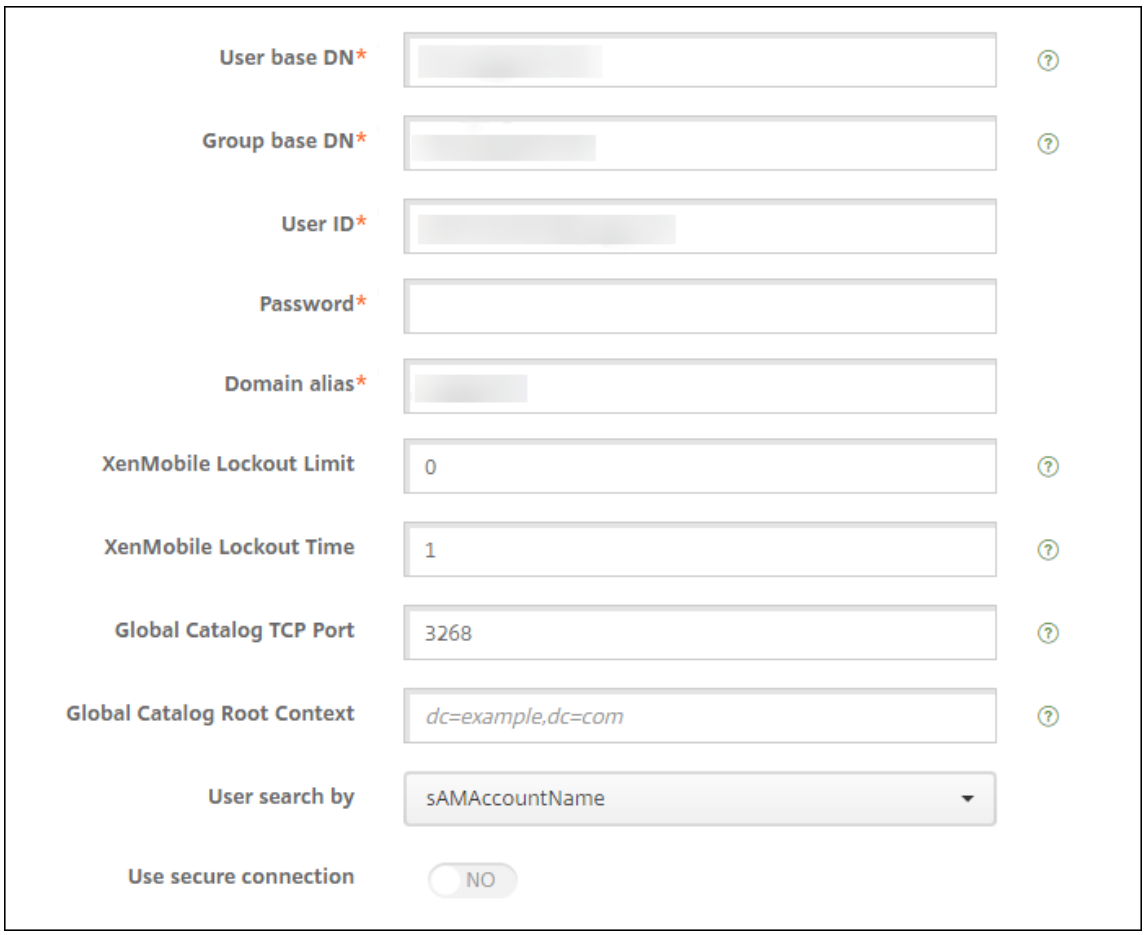


Configurar la entrega de certificados de Citrix ADC en XenMobile

1. Inicie sesión en la consola de XenMobile y haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la pantalla **Parámetros**.
2. En **Servidor**, haga clic en **Citrix Gateway**.
3. Si Citrix Gateway aún no está agregado, haga clic en **Agregar** y especifique los parámetros:
   - **URL externa:** `https://YourCitrixGatewayURL`
   - **Tipo de inicio de sesión:** Certificado y dominio.
   - **Se requiere contraseña:** No.
   - **Establecer como predeterminado:** Sí.
4. En **Entregar certificado de usuario para autenticación**, seleccione **Sí**.



5. En **Proveedor de credenciales**, seleccione un proveedor y haga clic en **Guardar**.
6. Si va a usar atributos de sAMAccount en los certificados de usuario como alternativa al nombre principal de usuario (UPN), configure el conector de LDAP en XenMobile de este modo: vaya a **Parámetros > LDAP**, seleccione el directorio, haga clic en **Modificar**, y seleccione **sAMAccount-Name** en **Buscar usuarios por**.



Habilitar el PIN de Citrix y el almacenamiento en caché de contraseñas de usuario

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

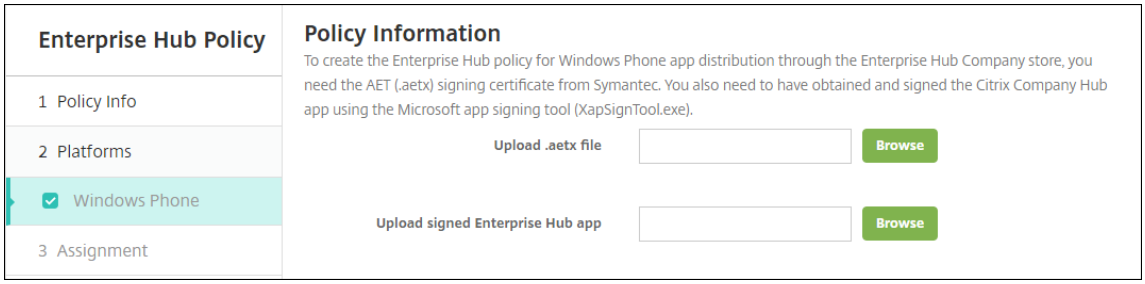
Crear una directiva de hub empresarial para Windows Phone

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

> **Nota:**
>
> Compruebe que los archivos AETX y Secure Hub utilizan:
>
> - El mismo certificado de empresa del proveedor de certificado.
> - El mismo ID de publicador en el perfil de cuenta de desarrollador de la Tienda Windows.

1. En la consola de XenMobile, haga clic en **Configurar > Directivas de dispositivo**.

2. Haga clic en **Agregar** y, a continuación, en **Más > Agente de XenMobile**, 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 Hub empresarial.



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

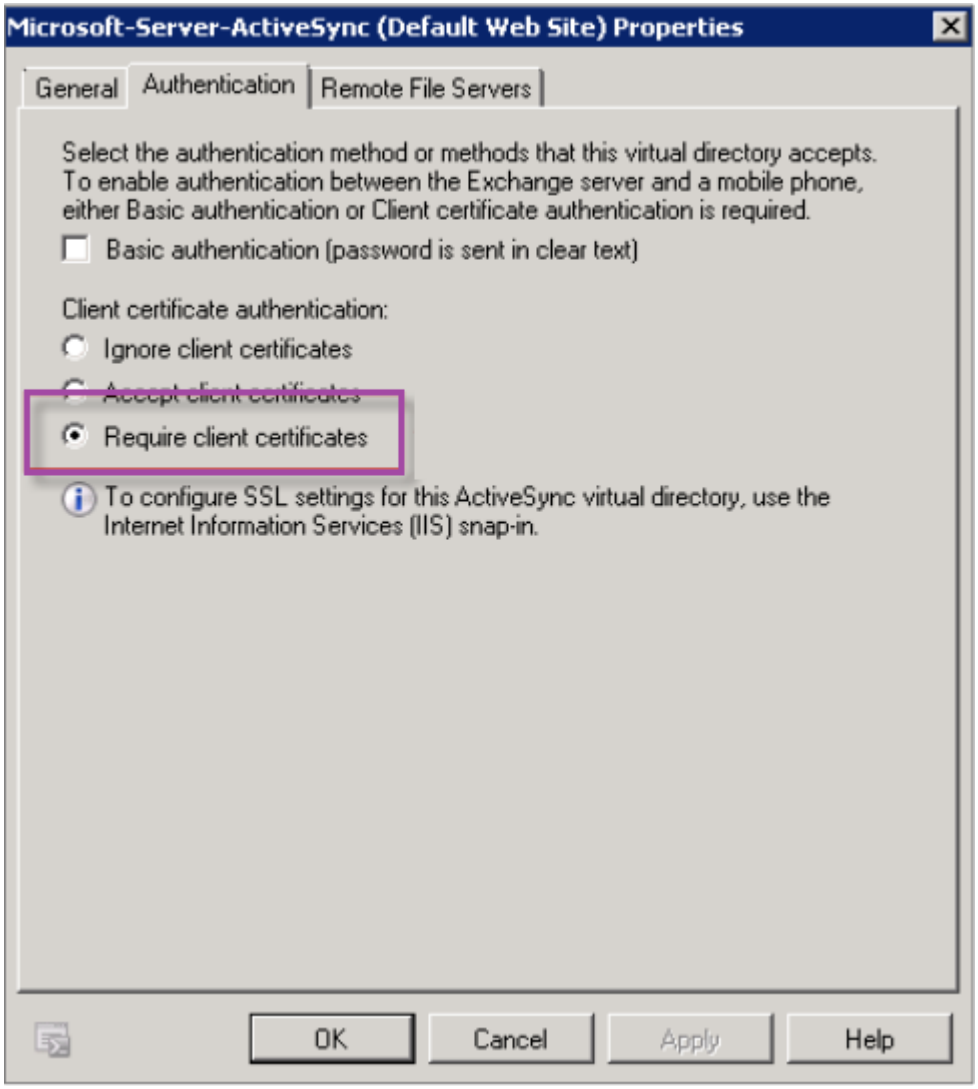
Solucionar problemas en la configuración de certificados de cliente

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

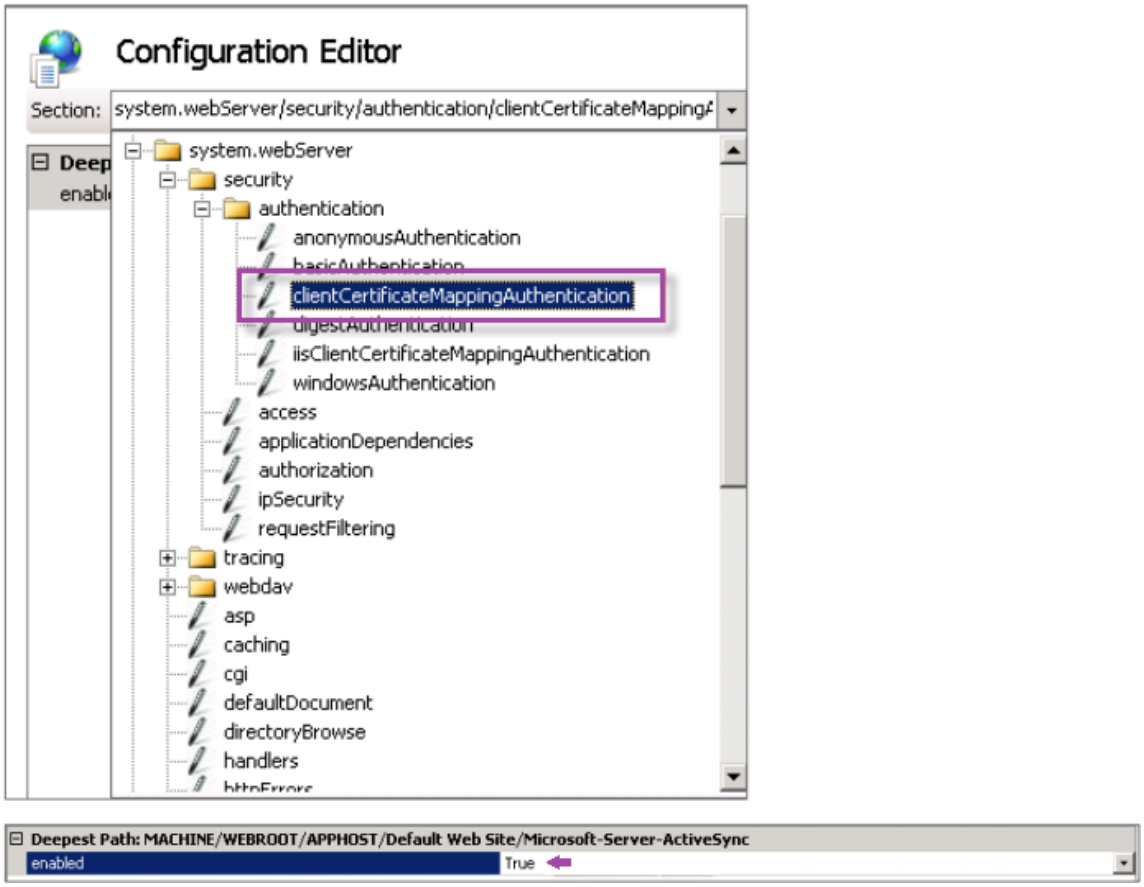
1. Los usuarios inscriben sus dispositivos móviles.
2. XenMobile solicita a los usuarios que creen un PIN de Citrix.
3. Se redirige a los usuarios a XenMobile Store.
4. Cuando los usuarios inician Secure Mail, XenMobile no les pide credenciales para configurar su buzón. En su lugar, Secure Mail solicitará el certificado del cliente de Secure Hub 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 usa 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 **Requerir certificados de cliente**.



3. En Microsoft Exchange Server, visite el sitio **Microsoft-Server-ActiveSync** para ver si tiene habilitada la autenticación con asignación de certificados del cliente. De forma predeterminada, la autenticación con asignación de certificados del cliente está inhabilitada. La opción está en **Editor de configuración > Seguridad > Autenticación**.



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

4. Revise la configuración de Citrix Gateway en la consola de XenMobile: **Entregar certificado de usuario para autenticación** debe estar **activado** y **Proveedor de credenciales** debe tener seleccionado el perfil correcto.

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

1. En la consola de XenMobile, vaya a **Administrar > Dispositivos** y seleccione el dispositivo.
2. Haga clic en **Modificar** o **Mostrar más**.
3. Vaya a la sección **Grupos de entrega** y busque esta entrada:

   Citrix Gateway Credentials: Requested credential, CertId=

Para validar si está habilitada la negociación de certificados de cliente

1. Ejecute este comando `netsh` para ver la configuración del certificado SSL que está vinculado 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=609da5df280d1f54a7deb714fb2c54
 appid={ 4dc3e181-e14b-4a21-b022-59fc669b0914 } certstorename=ExampleCertStoreNam
 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 lo siguiente:

- El token de inscripción de la aplicación (archivo AETX) se entrega a través de XenMobile mediante la directiva de dispositivo Enterprise Hub.
- 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.
- Se usa el mismo ID de publicador para firmar y empaquetar Secure Hub, Secure Mail y el token de inscripción de la aplicación.

Entidades PKI

January 4, 2022

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 son internos o externos a XenMobile. Los componentes internos se conocen como discrecionales. Los componentes externos forman parte de su infraestructura corporativa.

XenMobile admite los siguientes tipos de entidades de infraestructura PKI:

- PKI genéricas (GPKI)

La compatibilidad con GPKI de XenMobile Server incluye DigiCert Managed PKI.

- Servicios de certificados de Microsoft
- Entidades de certificación discrecionales (CA)

XenMobile admite el uso de estos servidores de CA:

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

Conceptos comunes de infraestructura de clave pública

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). Esa entidad 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 cuando configure la entidad de infraestructura PKI. Para ello, cargue los certificados en XenMobile y, a continuación, remita a ellos en la entidad de infraestructura PKI. Para las entidades de certificación discrecionales, el certificado es implícitamente el certificado de firma de CA. Para las entidades externas, debe especificar manualmente el certificado.

> **Importante:**
>
> Cuando cree plantillas de entidad para Servicios de certificados de Microsoft, para evitar posibles problemas de autenticación en los dispositivos inscritos, no use caracteres especiales en el nombre de las plantillas. Por ejemplo, no use: `! : $ ( )## % + * ~ ? | { } [ ]`

Infraestructura de clave pública genérica

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 inter-

acción con las interfaces de varias soluciones de infraestructura de clave pública. El protocolo GPKI define las siguientes tres operaciones fundamentales de infraestructura de clave pública:

- **Sign:** El adaptador puede hacerse cargo de las solicitudes de firma de certificado (CSR), transmitirlas a la infraestructura de clave pública y devolver los certificados recién firmados.
- **Fetch:** El adaptador puede recuperar certificados y pares de claves existentes (según los parámetros de entrada) desde la infraestructura de clave pública.
- **Revoke:** El adaptador puede hacer que la infraestructura de clave pública revoque un certificado determinado.

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. Por ejemplo, existen adaptadores GPKI para RSA y Entrust.

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.

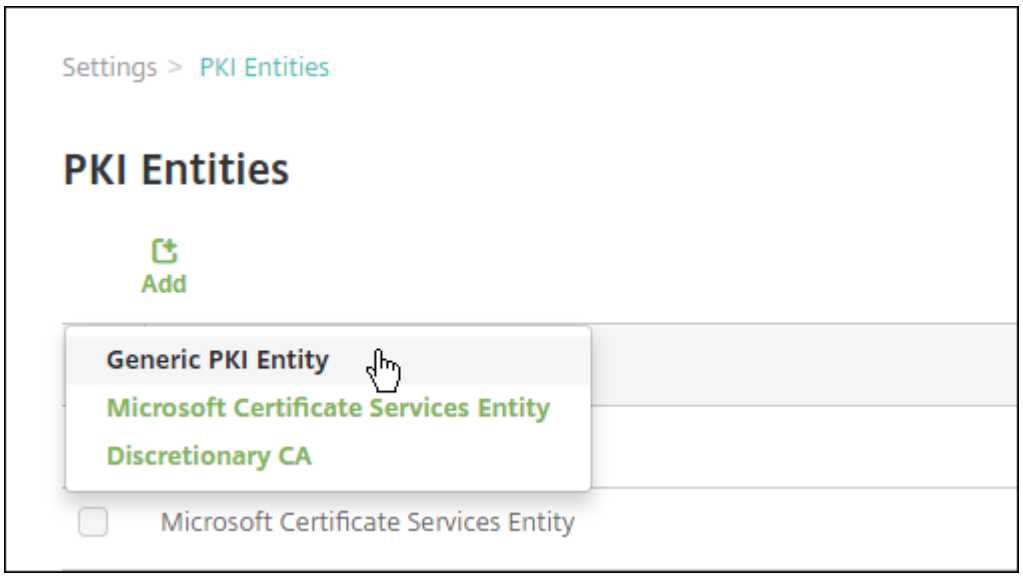
Admitir cada una de las operaciones de PKI en un adaptador es opcional. Si un adaptador admite esa operación, es que tiene la funcionalidad correspondiente (firmar, obtener o revocar). Cada una de estas capacidades se puede asociar a un conjunto de parámetros de usuario.

Los parámetros de usuario son aquellos parámetros que define el adaptador de GPKI para una operación específica, y cuyos valores debe proporcionar a XenMobile. XenMobile analiza el archivo WSDL para determinar las operaciones que puede realizar el adaptador 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.

Para agregar una infraestructura de clave pública genérica

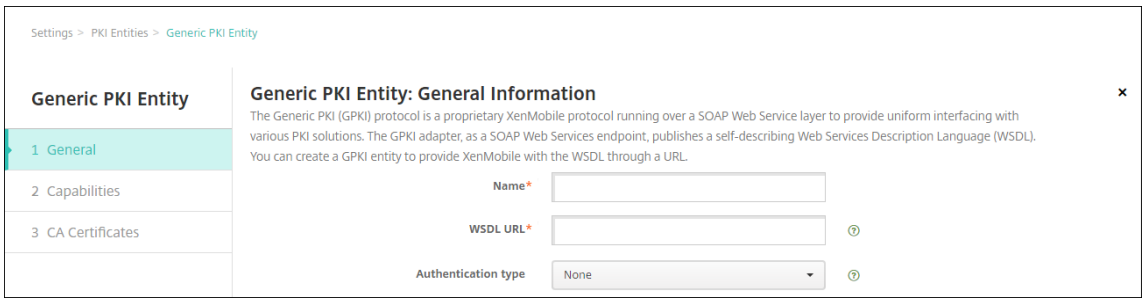
1. En la consola de XenMobile, haga clic en **Parámetros > Entidades PKI**.
2. En la página **Entidades PKI**, haga clic en **Agregar**.

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



3. Haga clic en **Entidad de PKI genérica**.

   Aparecerá la página “Entidad de PKI genérica: Información general”.



4. En la página **Entidad de PKI genérica: Información general**, lleve a cabo lo siguiente:

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

5. Haga clic en **Siguiente**.

   Aparecerá la página “Entidad de PKI genérica: Capacidades del adaptador”.

6. En la página **Entidad de PKI genérica: Capacidades del adaptador**, revise las funciones y los parámetros asociados al adaptador y, a continuación, haga clic en **Siguiente**.

   Aparecerá la página **Entidad de PKI genérica: Certificados de CA emisora**.

7. En la página “Entidad de PKI genérica: Certificados de CA emisora”, seleccione los certificados que se van a utilizar para la entidad.

   Aunque las entidades puedan devolver certificados firmados por varias entidades de certificación, 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 **Proveedor de credenciales**, en la página **Distribución**, seleccione uno de los certificados configurados aquí.

8. Haga clic en **Guardar**.

   La entidad se muestra en la tabla “Entidades PKI”.

DigiCert Managed PKI

La compatibilidad con GPKI de XenMobile Server incluye DigiCert Managed PKI, también conocida como MPKI. En esta sección se describe cómo configurar Windows Server y XenMobile Server para DigiCert Managed PKI.

Requisitos previos

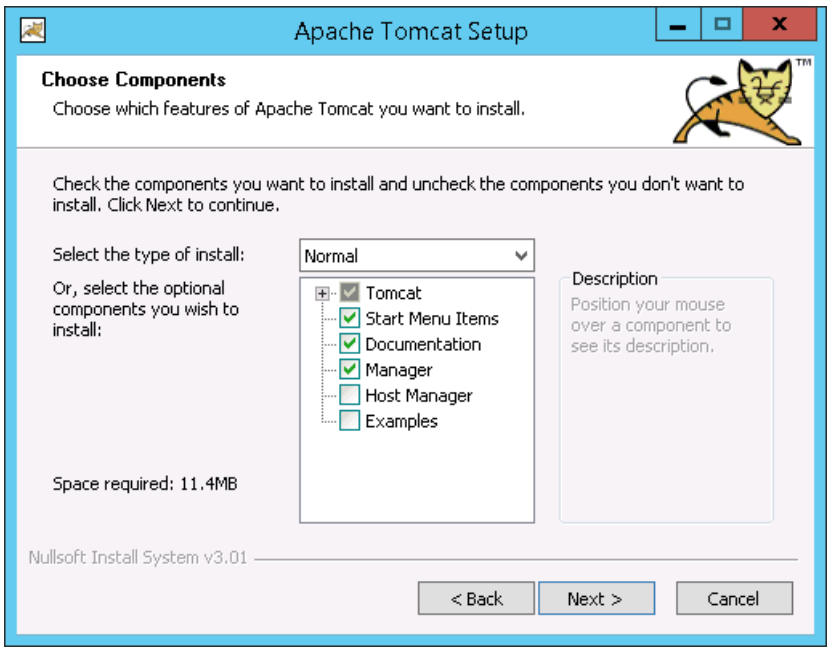
- Acceder a la infraestructura de DigiCert Managed PKI
- Windows Server 2012 R2 con los siguientes componentes instalados como se indica en este artículo:
  - Java
  - Apache Tomcat
  - Cliente de DigiCert PKI
  - Portecle
- Acceso al sitio de descargas de XenMobile

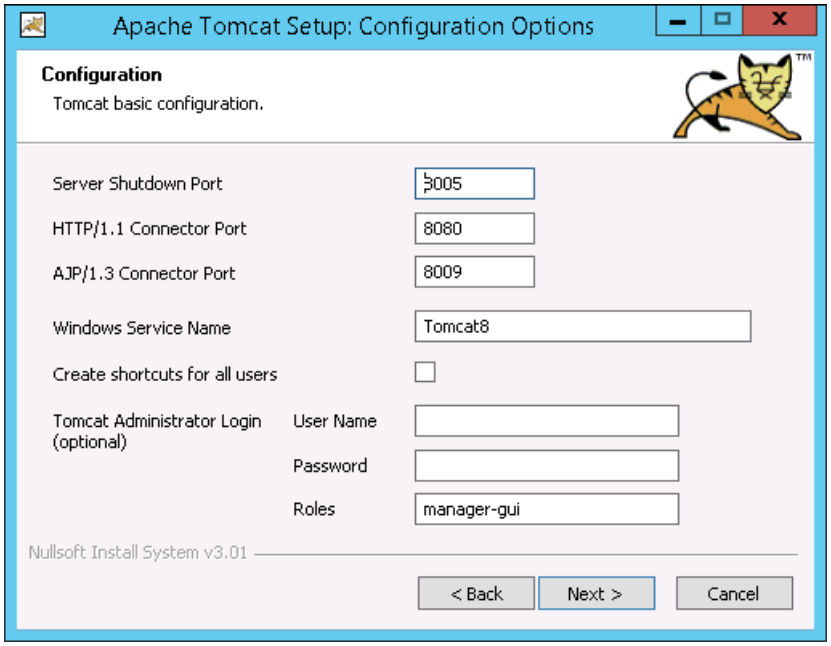
Instalar Java en Windows Server

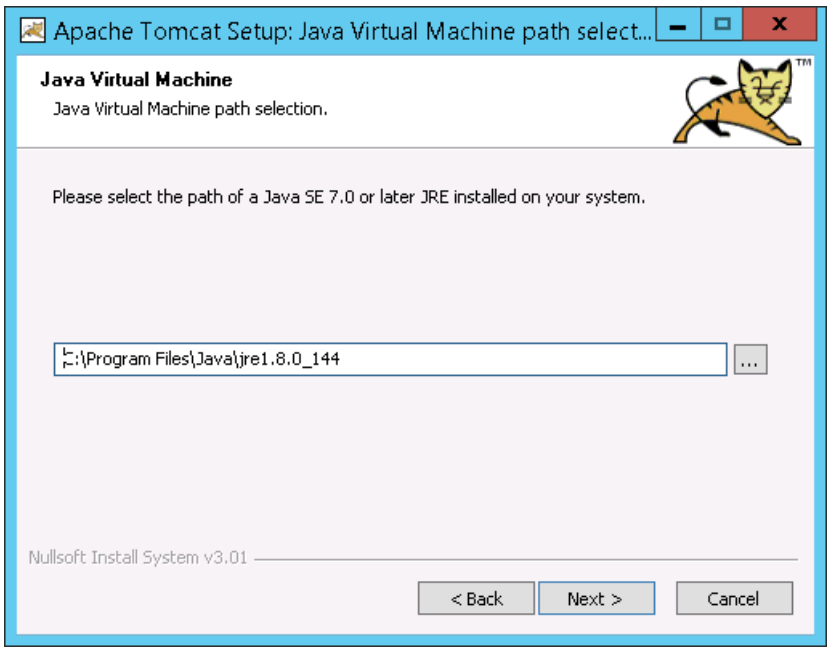
Descargue Java desde https://java.com/en/download/faq/java_win64bit.xml e instálelo. En el cuadro de diálogo Advertencia de seguridad, haga clic en **Ejecutar**.

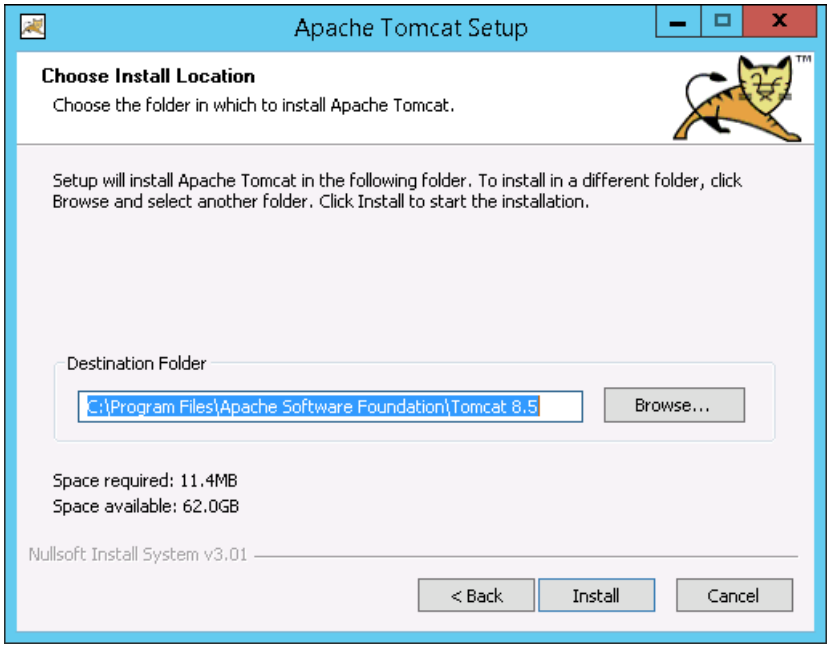
Instalar Apache Tomcat en Windows Server

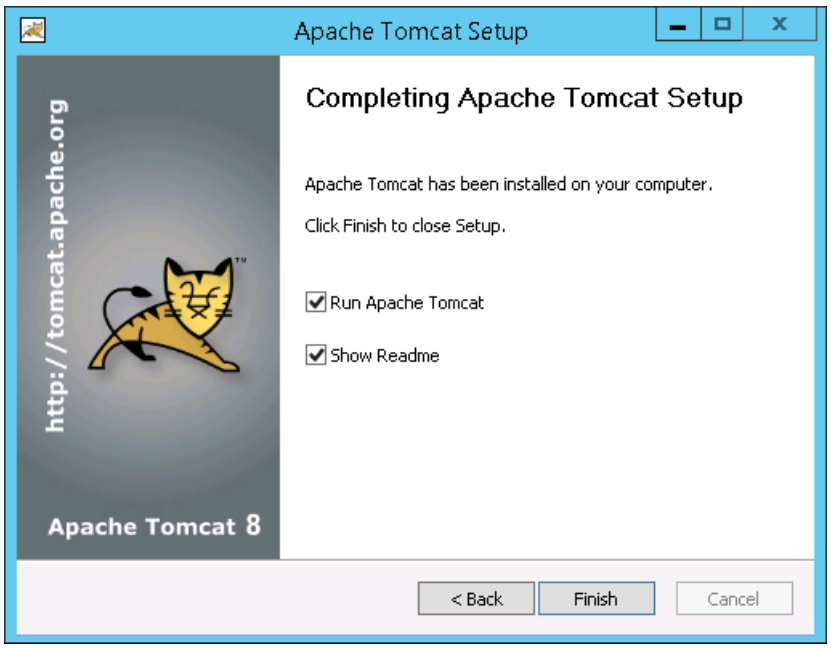
Descargue el instalador de Apache Tomcat de 32 o 64 bits para Servicios de Windows desde https://tomcat.apache.org/download-80.cgi y, a continuación, instálelo. En el cuadro de diálogo Advertencia de seguridad, haga clic en **Ejecutar**. Complete la configuración de Apache Tomcat con los ejemplos siguientes como guía.



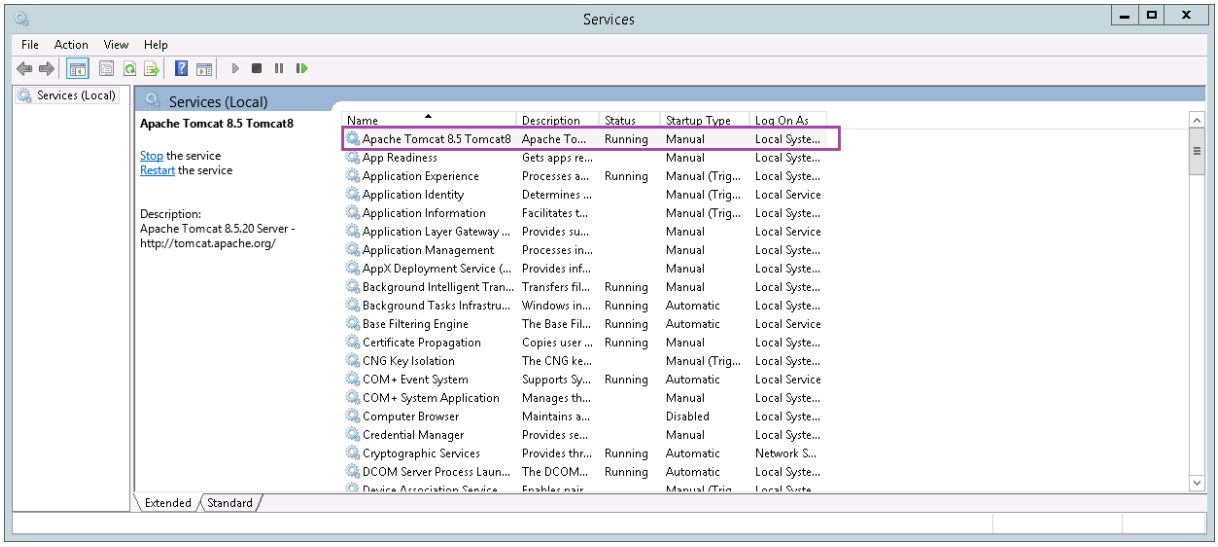


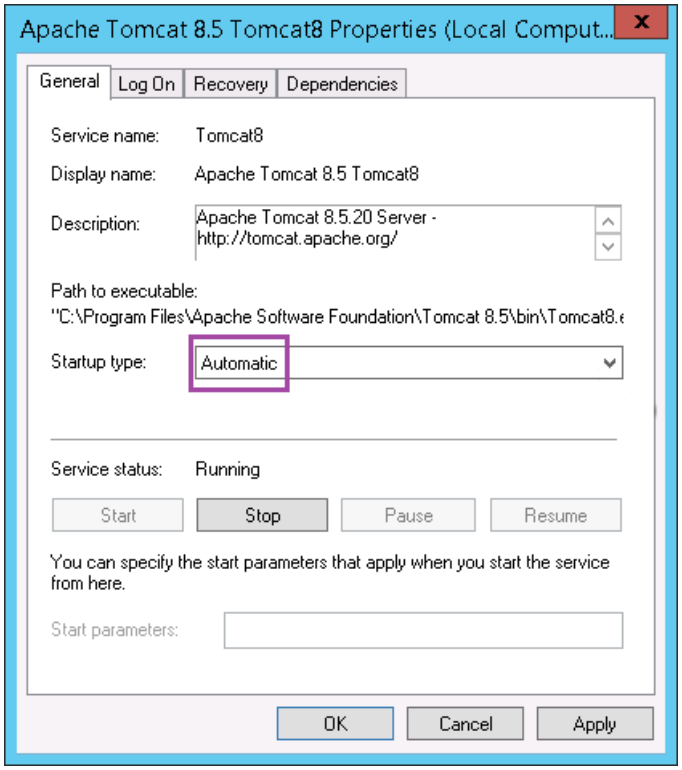






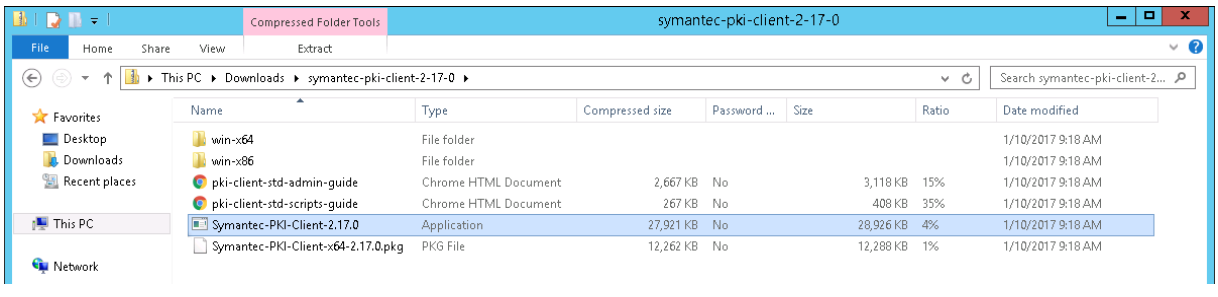
A continuación, vaya a Servicios de Windows y cambie **Tipo de inicio** de **Manual** a **Automático**.

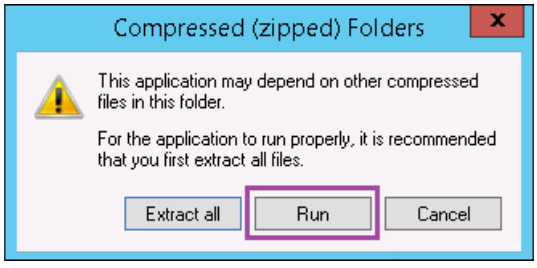




Instalar el cliente de DigiCert PKI en Windows Server

Descargue el instalador desde la consola de administrador de la infraestructura de clave pública. Si no dispone de acceso a la consola, descargue el instalador desde la página de asistencia de DigiCert How to download DigiCert PKI Client. Descomprima y ejecute el instalador.





En el cuadro de diálogo Advertencia de seguridad, debe hacer clic en **Ejecutar**. Siga las instrucciones del instalador para completar la instalación y la configuración. Cuando se completen los pasos del

instalador, se le solicitará que reinicie.

Instalar Portecle en Windows Server

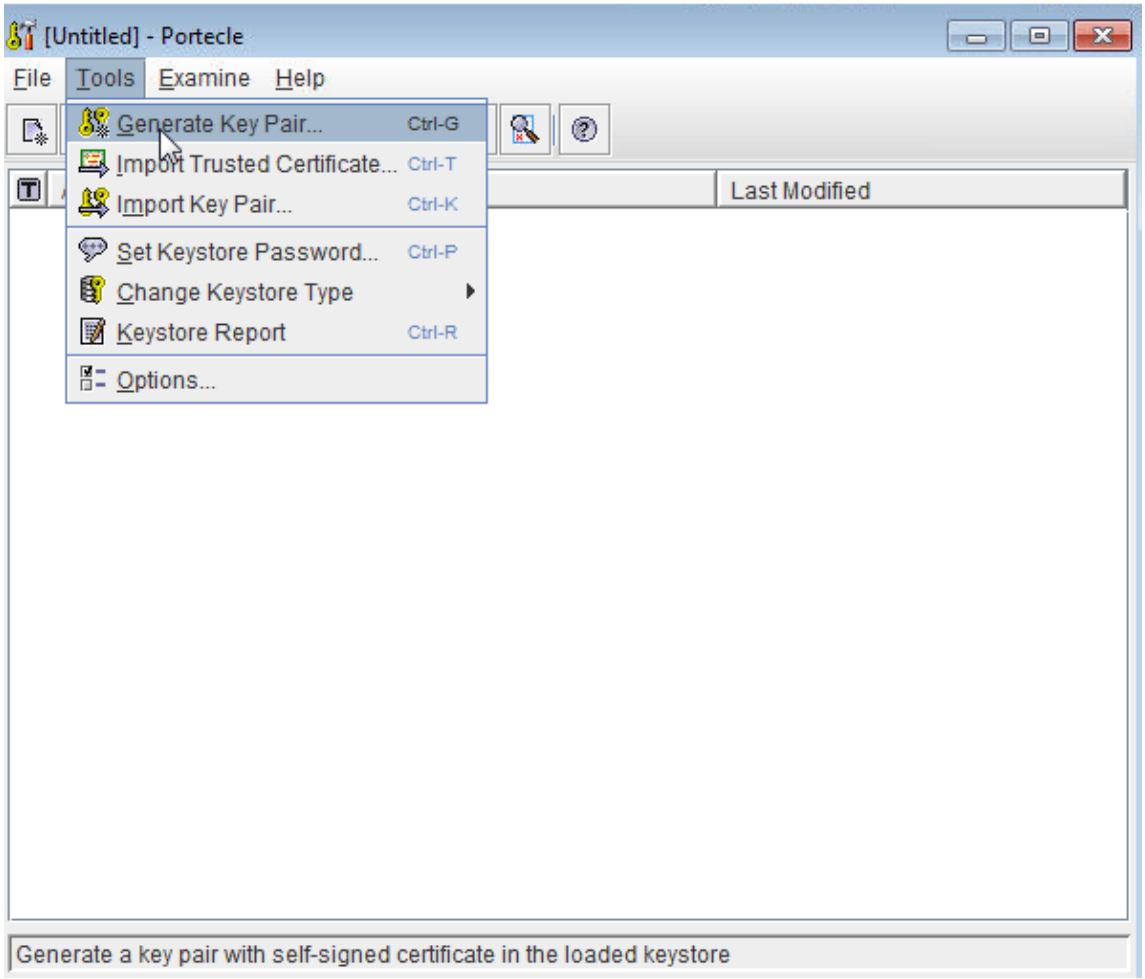
Descargue el instalador desde https://sourceforge.net/projects/portecleinstall/files/ y, a continuación, descomprímalo y ejecútelo.

Generar el certificado de la entidad de registro (RA) para DigiCert Managed PKI

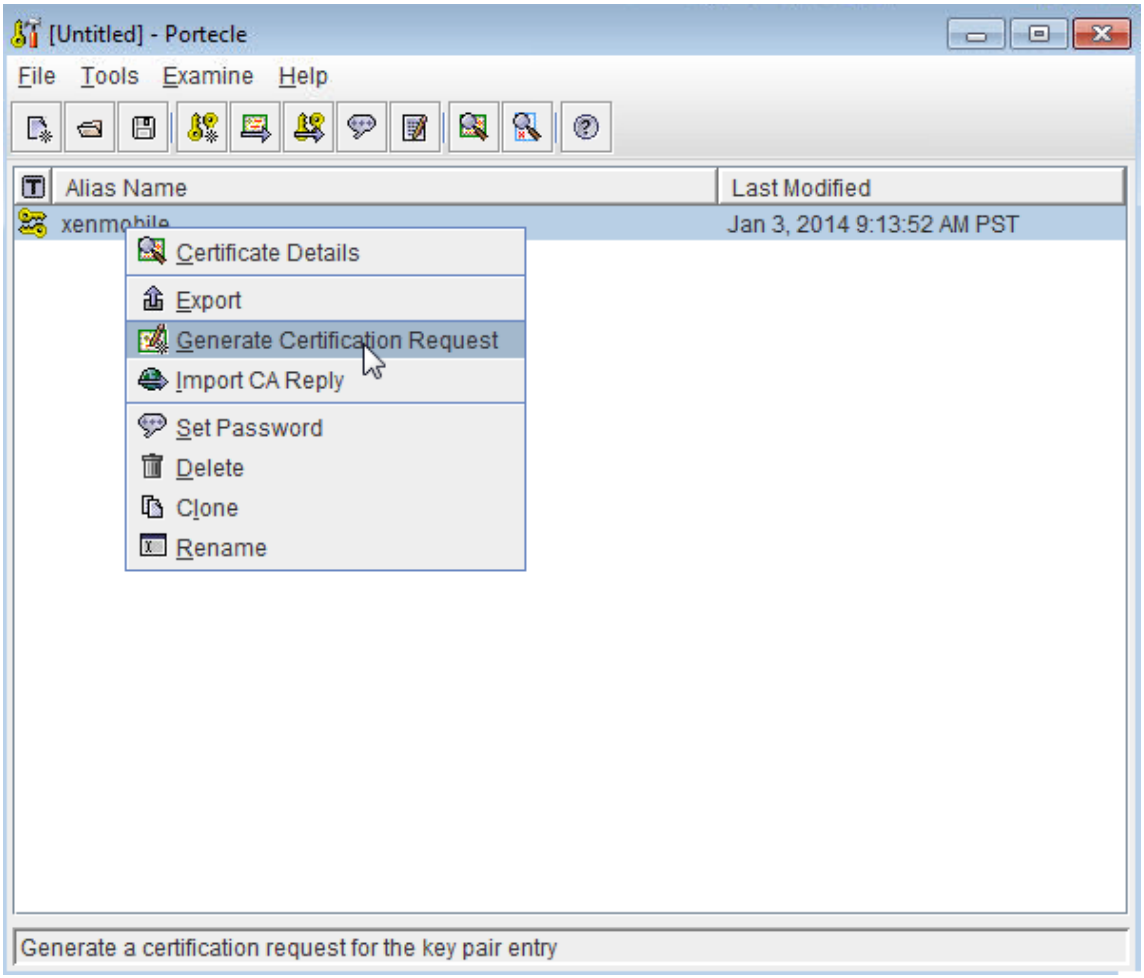
El almacén de claves relativo a la autenticación por certificados de cliente se encuentra en un certificado de entidad de registro (RA) llamado RA.jks. En los pasos siguientes se describe cómo generar ese certificado desde Portecle. También puede generar el certificado de RA desde la interfaz de línea de comandos de Java.

En este artículo también se describe cómo cargar los certificados públicos y RA.

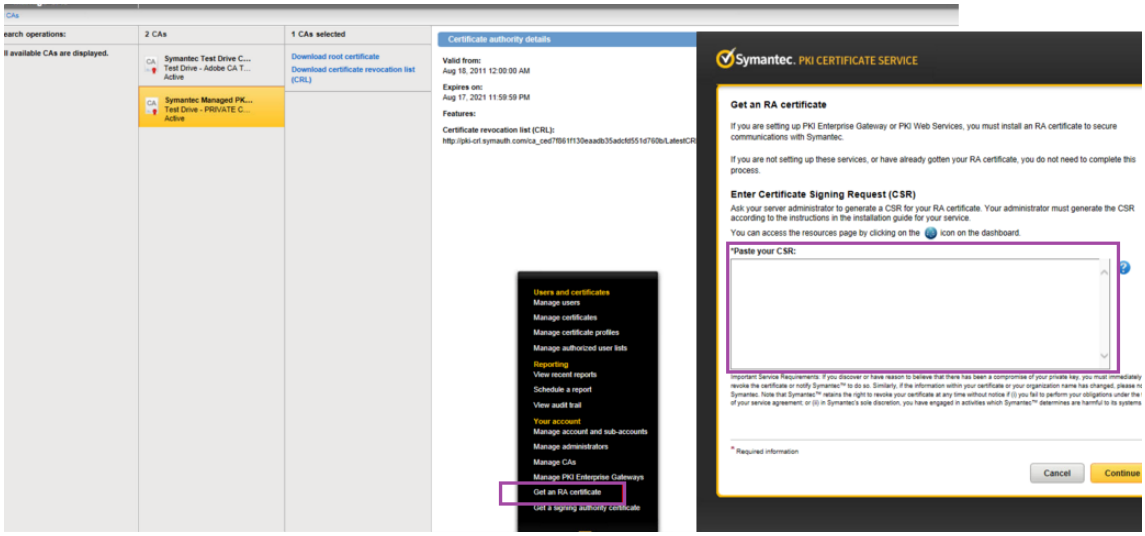
1. En Portecle, vaya a **Tools > Generate Key Pair**, proporcione la información necesaria y genere el par de claves.



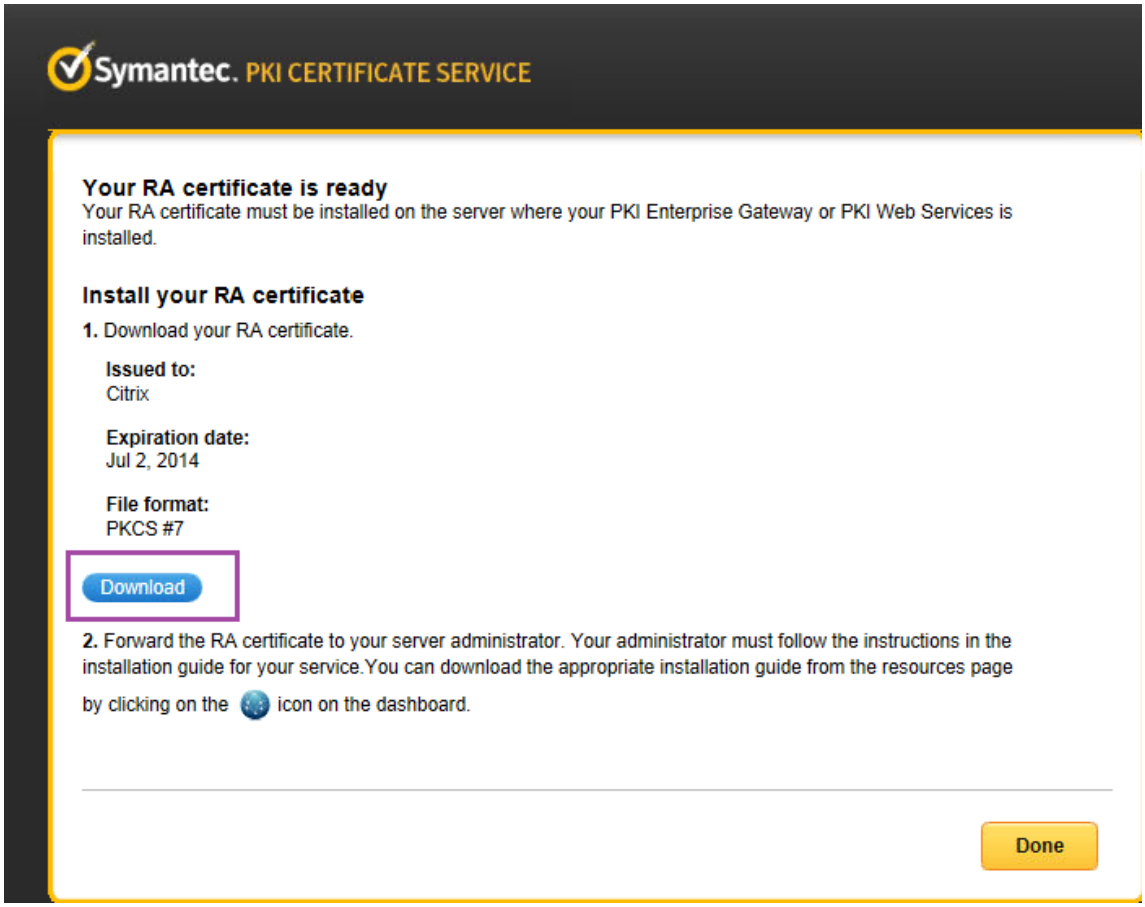
2. Haga clic con el botón secundario en el par de claves y, a continuación, haga clic en **Generate Certification Request**.



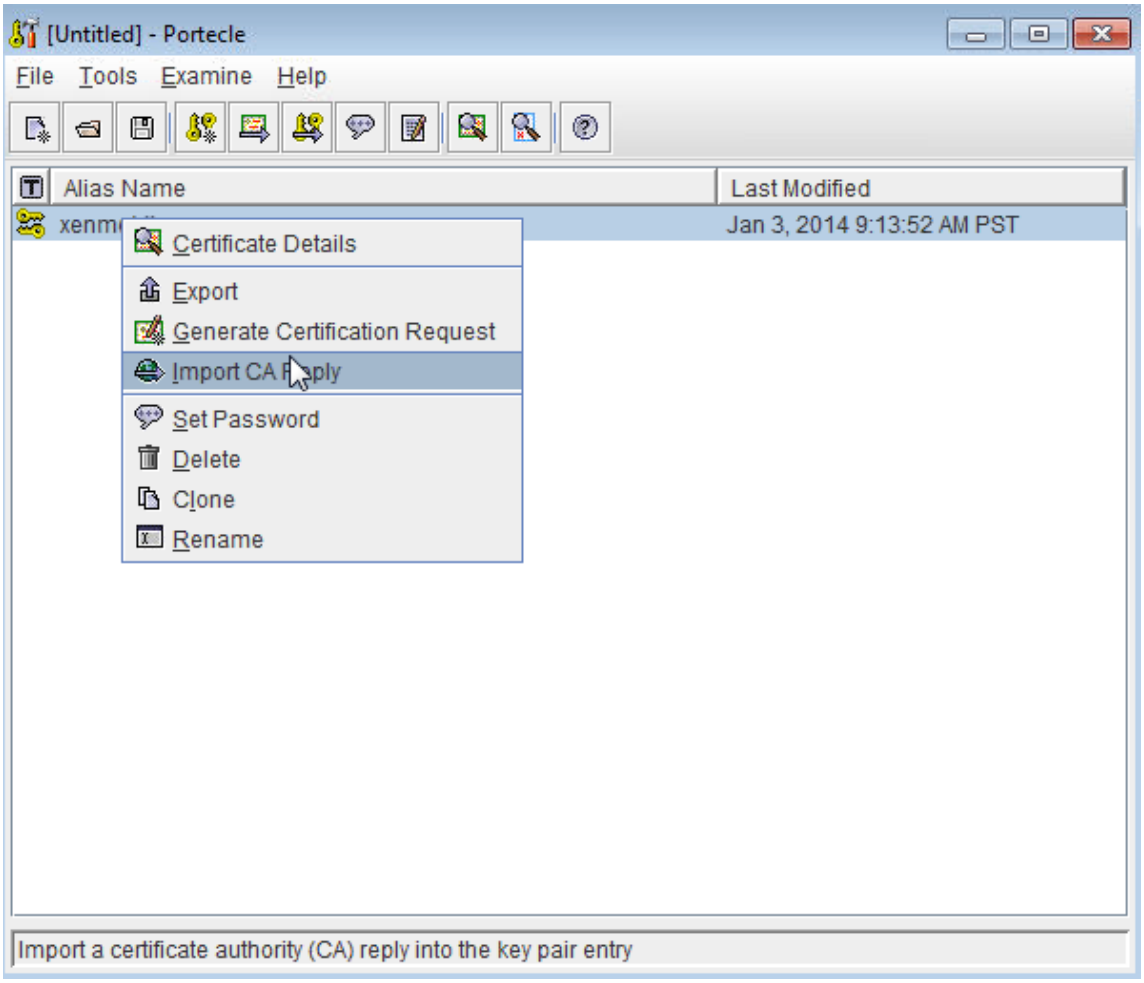
3. Copie la solicitud CSR.
4. En DigiCert PKI Manager, genere un certificado de RA: Haga clic en **Settings** > **Get a RA Certificate**, pegue la solicitud de firma de certificado y, a continuación, haga clic en **Continue**.



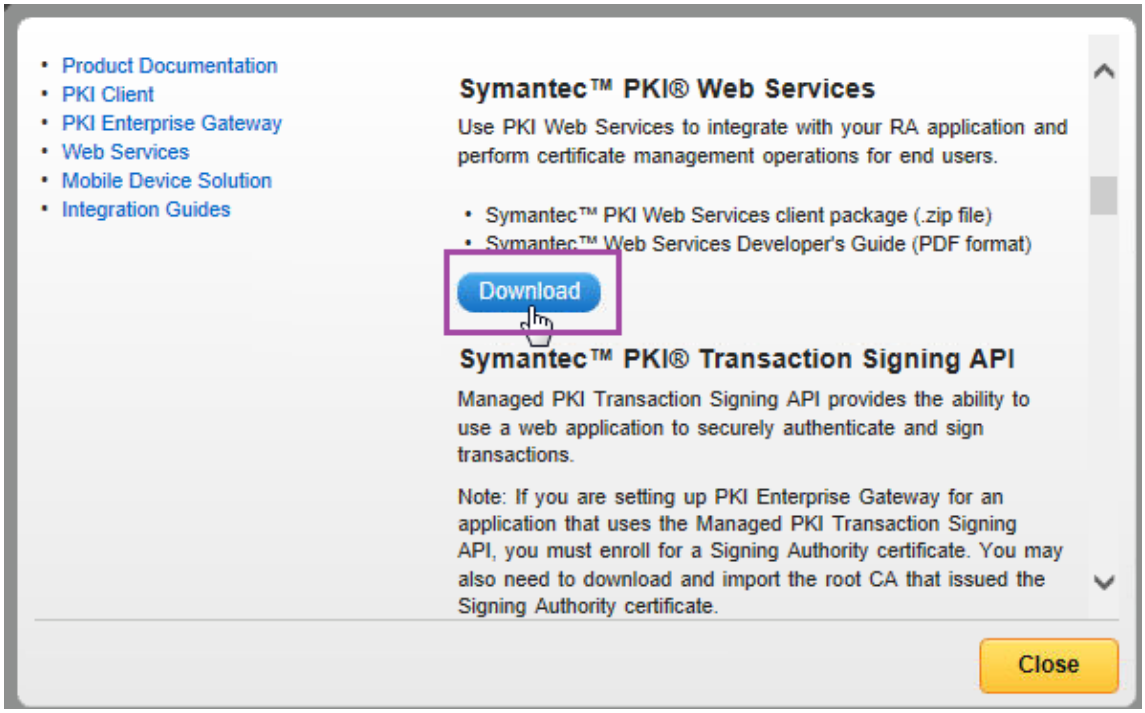
5. Haga clic en **Download** para descargar el certificado de RA generado.



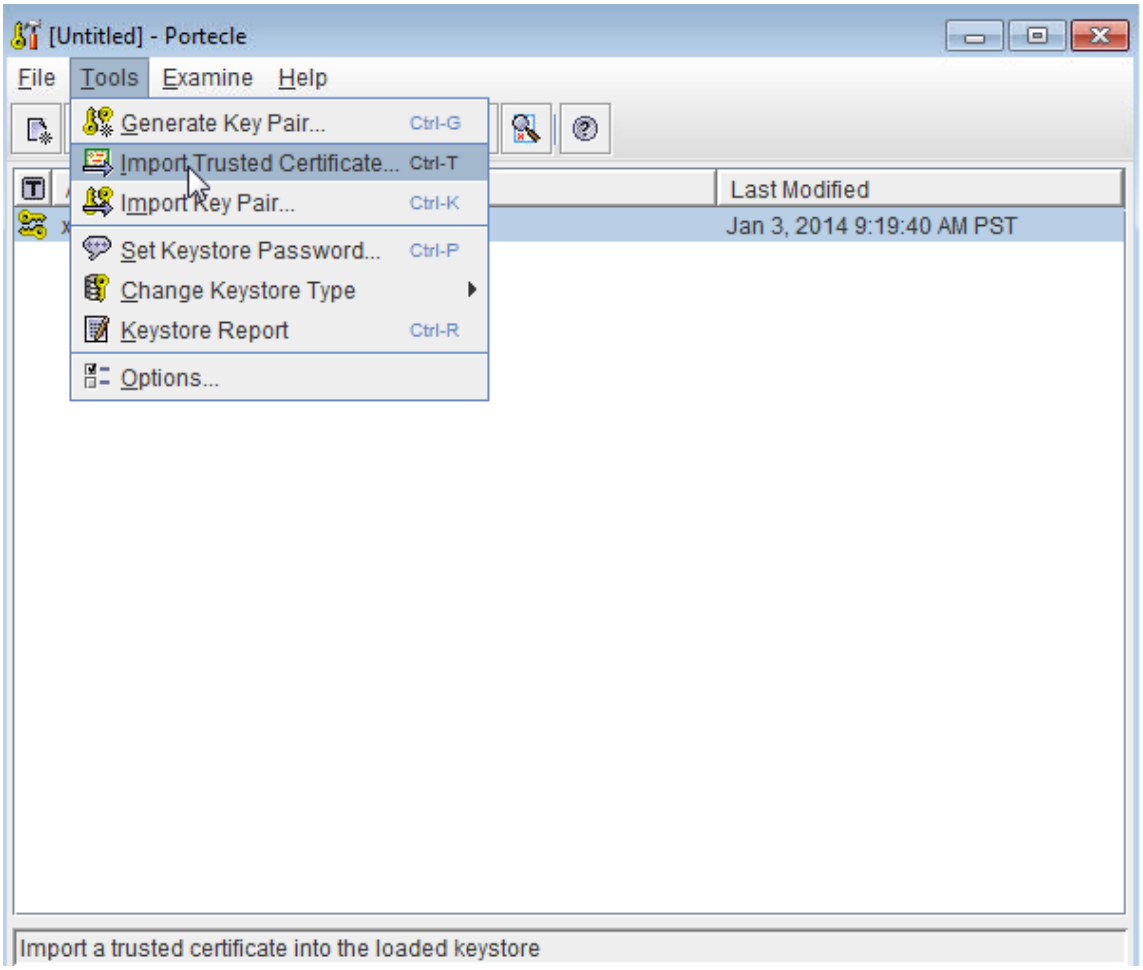
6. En Portecle, importe el certificado de RA: haga clic con el botón secundario en el par de claves y, a continuación, haga clic en **Import CA Reply**.



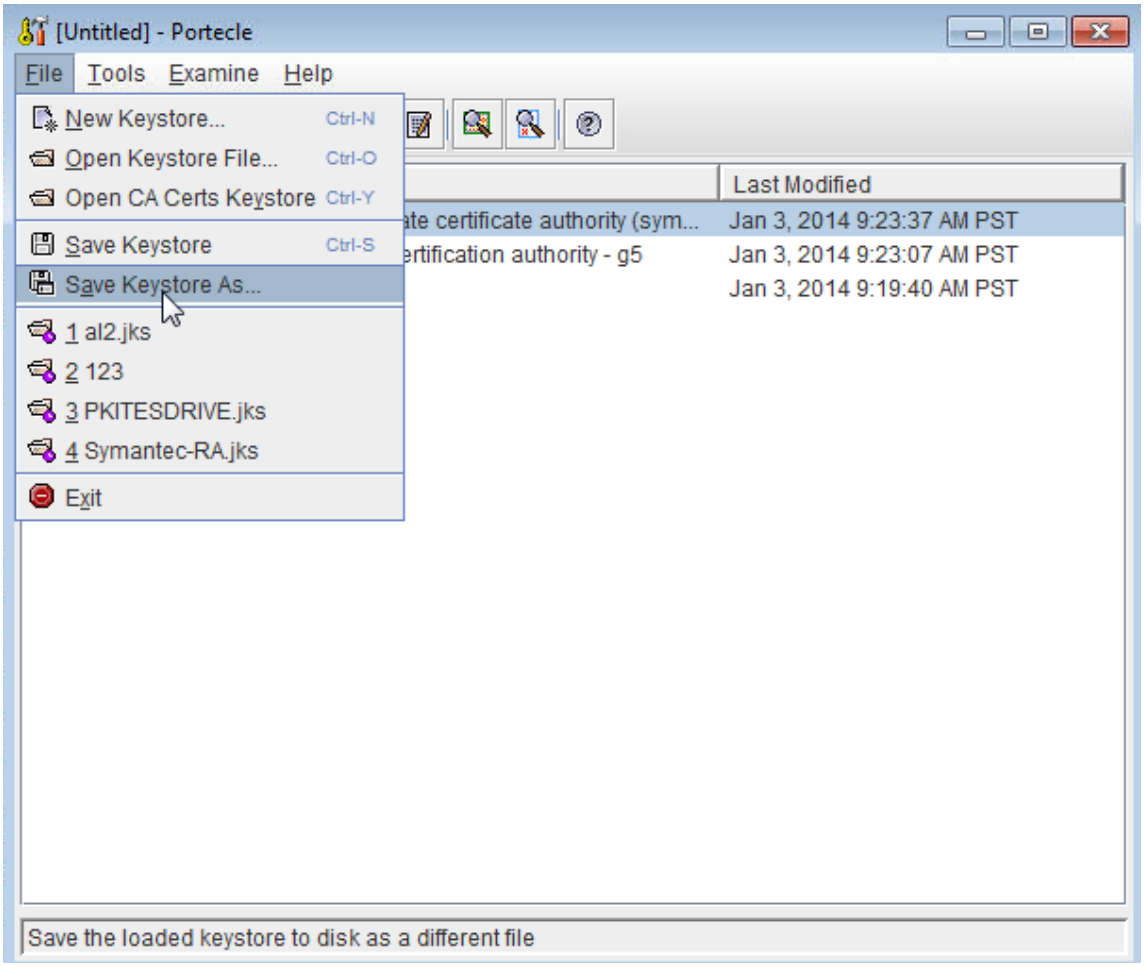
7. En DigiCert PKI Manager, vaya a **Resources > Web Services** y descargue los certificados de CA.



8. En Portecle, importe los certificados intermedios y raíz de RA en el almacén de claves: vaya a **Tools > Import Trusted Certificates**.



9. Después de importar los certificados de las entidades de certificación, guarde el almacén de claves como RA.jks en la carpeta C:\DigiCert en el servidor Windows.



Configurar DigiCert PKI Adapter en Windows Server

1. Inicie sesión en Windows Server con credenciales de administrador.
2. Cargue el archivo RA.jks generado en la sección anterior. Cargue también los certificados públicos (cacerts.jks) para su servidor Symantec MPKI.
3. Descargue el archivo del adaptador PKI de Symantec:
   a) Vaya a https://www.citrix.com/downloads.
   b) Vaya a **Citrix Endpoint Management (y Citrix XenMobile Server) > XenMobile Server (local) > Software de producto > XenMobile Server 10 > Herramientas**.
   c) En el mosaico **Symantec PKI Adapter**, haga clic en **Download File** (Descargar archivo).
   d) Descomprima y copie los archivos a la unidad C: del servidor de Windows:
      - custom_gpki_adapter.properties
      - Symantec.war

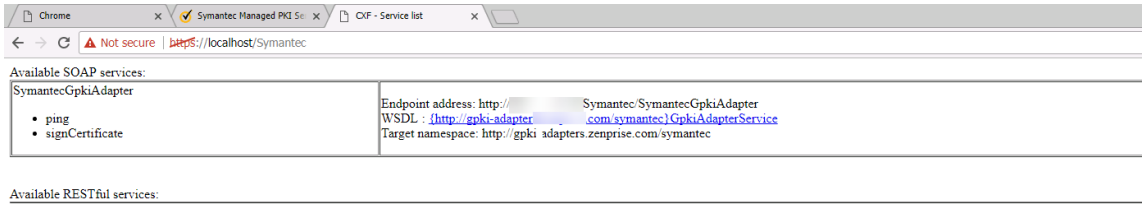
4. Abra custom_gpki_adapter.properties en el Bloc de notas y modifique los siguientes valores:

```
Gpki.CaSvc.Url=https://<managed PKI URL>

# keystore for client-cert auth

keyStore=C:\Symantec\RA.jks

# truststore for server with self-signed root CA

trustStore=C:\Symantec\cacerts.jks
<!--NeedCopy-->
```

5. Copie el archivo Symantec.war que se encuentra en la carpeta `<tomcat dir>\webapps` y, a continuación, inicie Tomcat.
6. Compruebe que la aplicación se ha implementado: abra un explorador web y vaya a `https://localhost/Symantec`.
7. Vaya a la carpeta `<tomcat dir>\webapps\Symantec\WEB-INF\classes` y modifique gpki_adapter.properties. Modifique la propiedad **CustomProperties** para que apunte al archivo custom_gpki_adapter ubicado en la carpeta C:\Symantec:

   ```
   CustomProperties=C:\\Symantec\\custom_gpki_adapter.properties
   ```

8. Reinicie Tomcat, vaya a `https://localhost/Symantec` y, a continuación, copie la dirección del dispositivo de punto final. En la sección siguiente, pegue esa dirección cuando configure el adaptador de PKI.

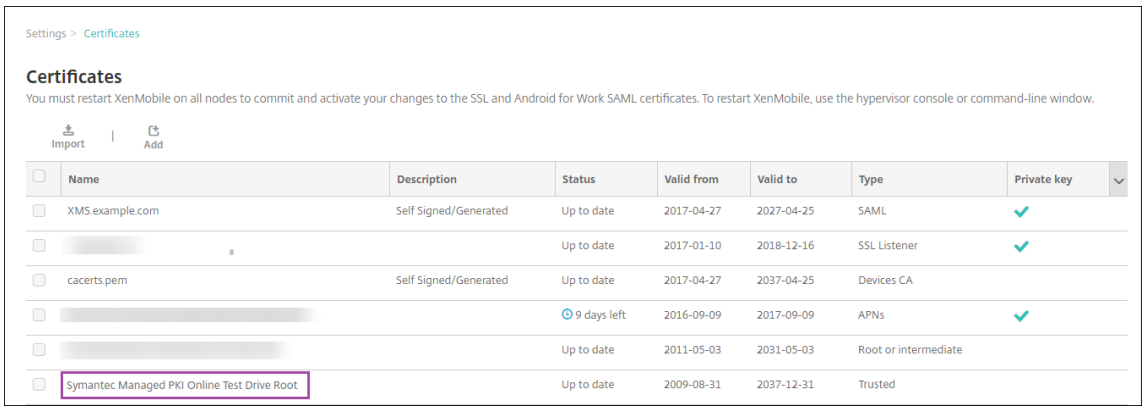


Configurar XenMobile Server para DigiCert Managed PKI

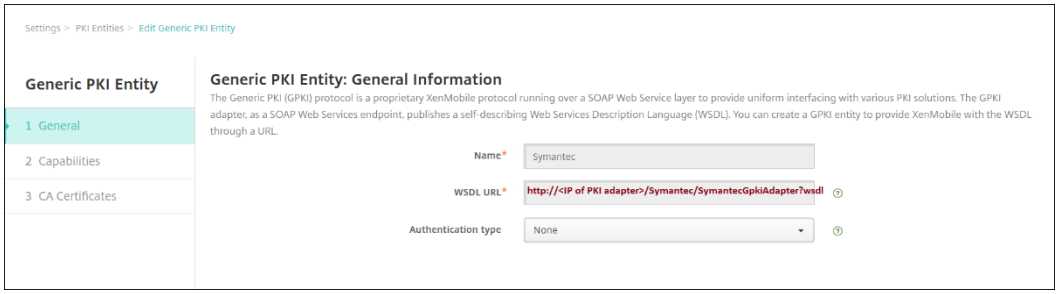
Complete la configuración de Windows Server antes de realizar la siguiente configuración de XenMobile Server.

Para importar los certificados de CA de DigiCert y configurar la entidad PKI

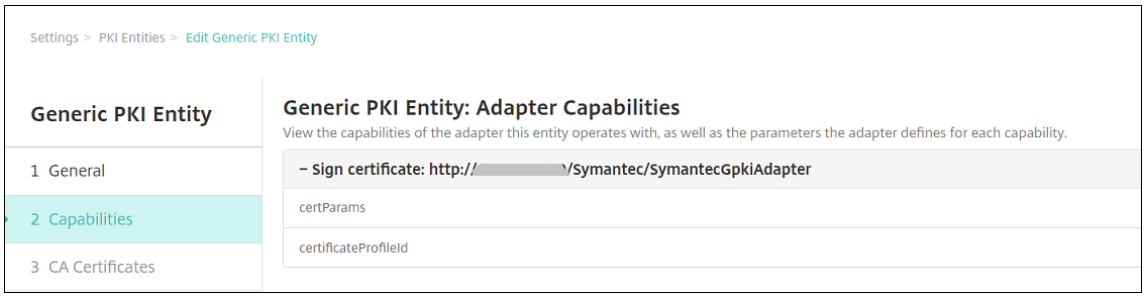
1. Importe los certificados de CA de DigiCert que emiten el certificado de usuario final. Para ello, en la consola de XenMobile Server, vaya a **Parámetros > Certificados** y haga clic en **Importar**.



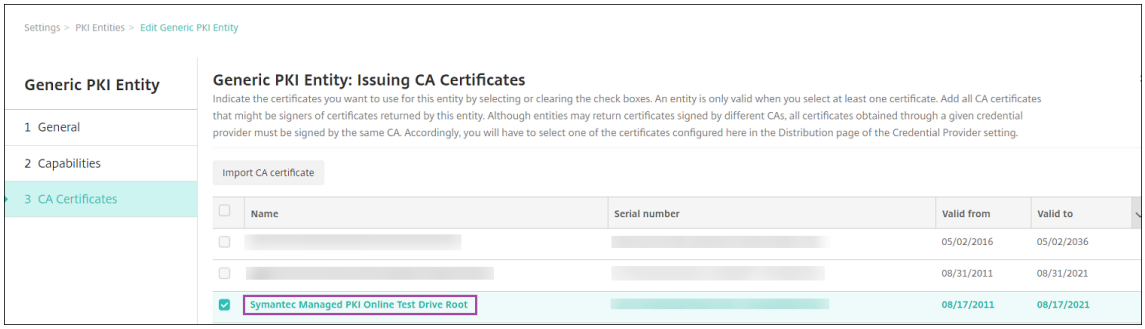
2. Agregue y configure la entidad de infraestructura de clave pública. Para ello, vaya a **Parámetros > Entidades de PKI**, haga clic en **Agregar** y, a continuación, elija **Entidad de PKI genérica**. En **URL de WSDL**, pegue la dirección del dispositivo de punto final que copió cuando configuraba el adaptador de PKI en la sección anterior y, a continuación, agregue `?wsdl` como se muestra a continuación.



3. Haga clic en **Siguiente**. XenMobile rellena los nombres de los parámetros desde el archivo WSDL.



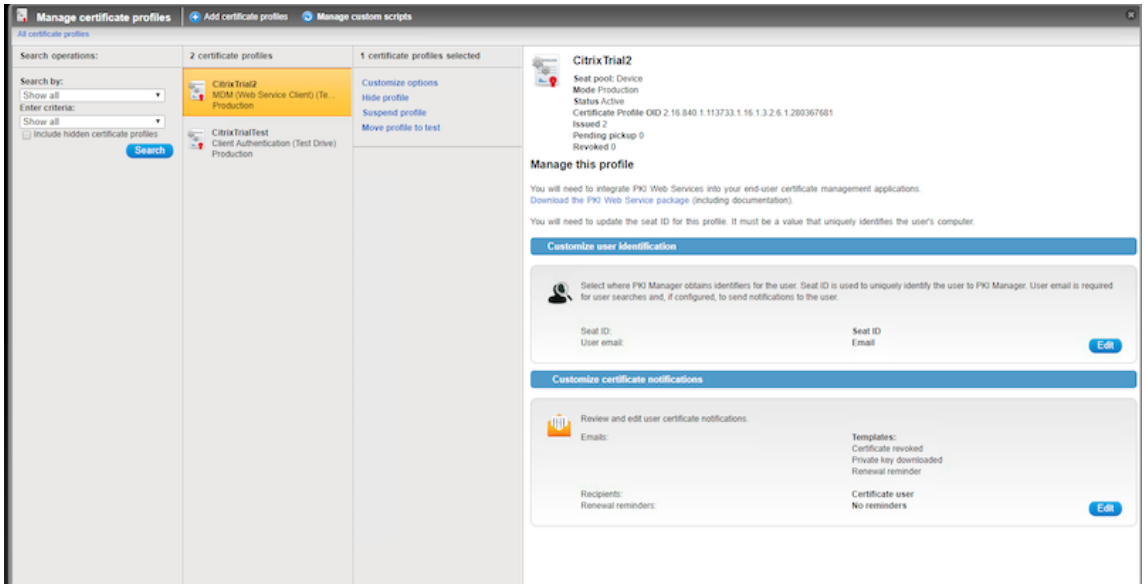
4. Haga clic en **Siguiente**, seleccione el certificado de CA correcto y, a continuación, haga clic en **Guardar**.



5. En la página **Parámetros > Entidades PKI**, verifique que el **Estado** de la entidad PKI que ha agregado es **Válido**.

Para crear el proveedor de credenciales de DigiCert Managed PKI

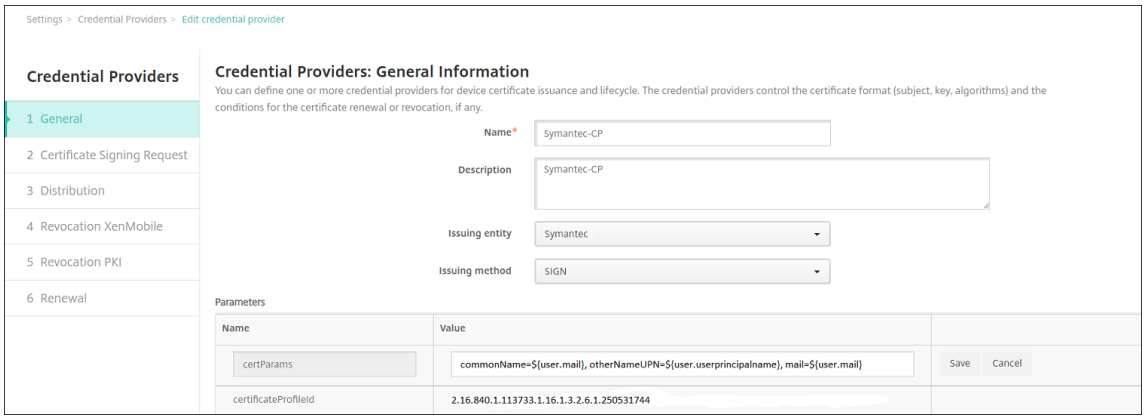
1. En la consola de DigiCert PKI Manager, copie el **OID de perfil de certificado** de la plantilla de certificados.



2. En la consola de XenMobile Server, vaya a **Parámetros > Proveedores de credenciales**, haga clic en **Agregar** y, a continuación, configure los parámetros de esta manera.

   - **Nombre:** Escriba un nombre exclusivo para la configuración del nuevo proveedor. Este nombre se usará para identificar la configuración en otras partes de la consola de XenMobile.

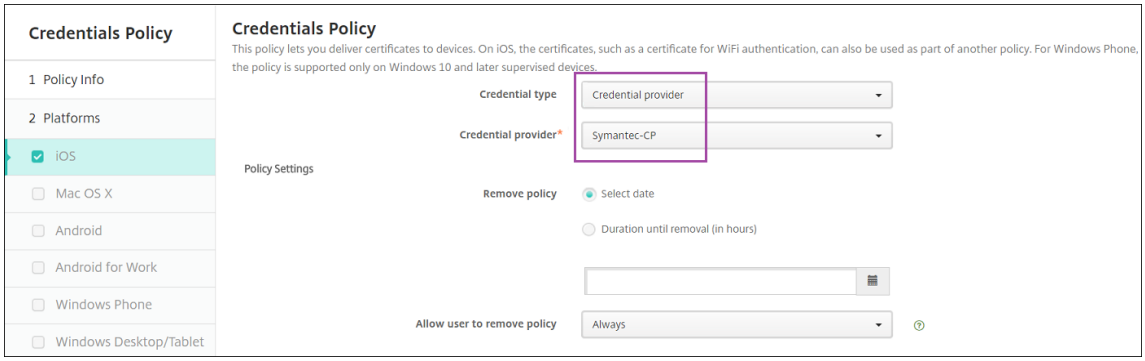
- **Descripción:** Describa el proveedor de credenciales. Aunque este campo sea optativo, una descripción puede resultar útil cuando necesite datos concretos acerca del proveedor de credenciales.
- **Entidad de emisión:** Seleccione la entidad emisora de certificados.
- **Método de emisión:** Haga clic en **Firmar** para designar el método que usará el sistema para obtener certificados de la entidad configurada.
- **certParams:** Agregue este valor: **commonName=${user.mail},otherNameUPN=${user.userprincipa**
- **certificateProfileid:** Pegue el OID de perfil de certificado que copió en el paso 1.



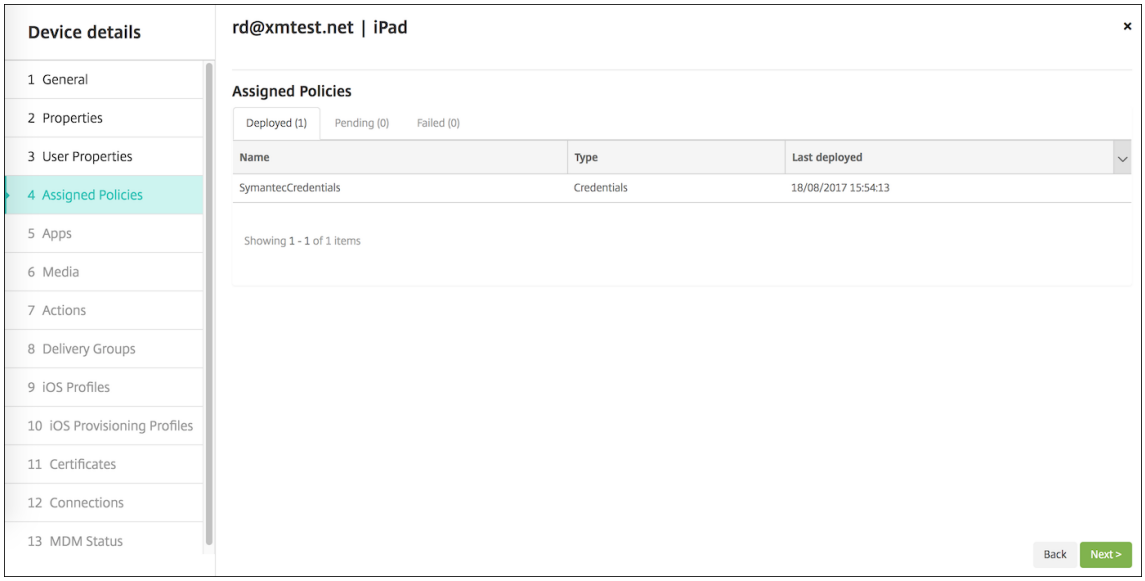
3. Haga clic en **Siguiente**. En cada una de las páginas restantes (desde “Solicitud de firma de certificado” hasta “Renovación”), acepte los parámetros predeterminados. Cuando haya terminado, haga clic en **Guardar**.

Para probar la configuración y solucionar problemas

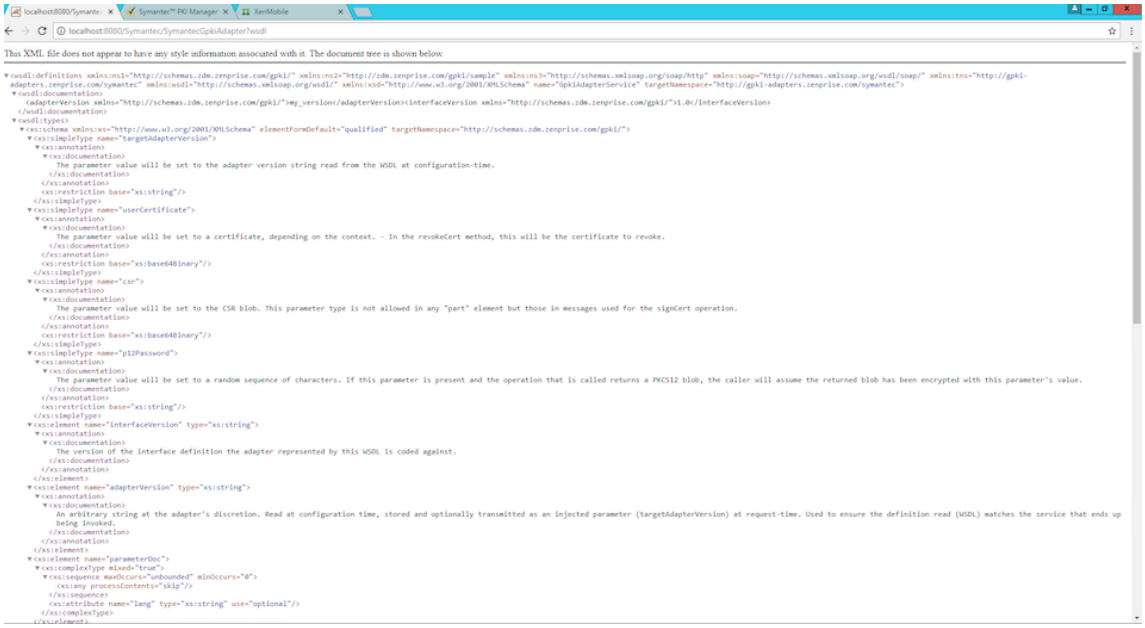
1. Cree una directiva de credenciales: Para ello, vaya a **Configurar > Directivas de dispositivo**, haga clic en **Agregar**, empiece a teclear **Credenciales** y, a continuación, haga clic en **Credenciales**.
2. Especifique el **Nombre de la directiva**.
3. Configure los parámetros de las plataformas de esta manera:
   - **Tipo de credencial:** Elija **Proveedor de credenciales**.
   - **Proveedor de credenciales:** Elija el proveedor DigiCert.



4. Después de completar la configuración de las plataformas, continúe a la página **Asignación**, asigne la directiva a grupos de entrega y haga clic en **Guardar**.
5. Para comprobar si la directiva se ha implementado en el dispositivo, vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Modificar** > **Directivas asignadas**. En el siguiente ejemplo se muestra una implementación correcta de la directiva.



Si no se ha implementado la directiva, inicie sesión en el servidor Windows y compruebe si WSDL se carga correctamente.



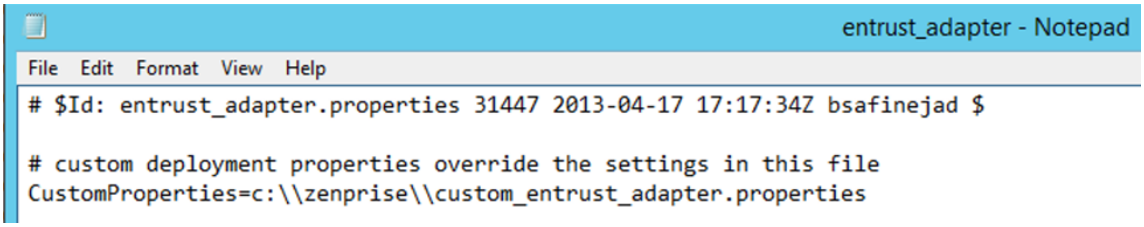
Para obtener más información sobre cómo solucionar problemas de configuración, consulte los registros de Tomcat en `<tomcat dir>\logs\catalina.<current date>`.

Adaptador de PKI de Entrust

Como alternativa a DigiCert Managed PKI, puede instalar el adaptador de PKI de Entrust. Antes de instalar el adaptador, consulte los pasos para instalar Java y Apache Tomcat en Windows Server que se indican en la sección DigiCert Managed PKI de este artículo.

Instalar el adaptador de PKI de Entrust

1. Descargue el archivo del adaptador PKI de Entrust:
   a) Vaya a https://www.citrix.com/downloads.
   b) Vaya a **Citrix Endpoint Management (y Citrix XenMobile Server) > XenMobile Server > Software de producto > XenMobile Server 10 > Herramientas**.
   c) En el mosaico **Entrust PKI Adapter**, haga clic en **Download File** (Descargar archivo).
   d) Extraiga el archivo entrust.war del archivo ZIP descargado y colóquelo en el directorio C:\Archivos de programa (x86)\Apache Software Foundation\Tomcat 8.5\webapps.
2. En C:\Archivos de programa (x86)\Apache Software Foundation\Tomcat 8.5\webapps\Entrust\WEB-INF\classes, modifique entrust_adapter.properties y establezca CustomProperties en `c:\\zenprise\\custom_entrust_adapter.properties`.



3. En su unidad C:, cree un directorio zenprise y un archivo llamado custom_entrust_adapter.properties.
4. Modifique el archivo con el siguiente contenido, con cuidado de reemplazar correctamente Entrust.MdmSvc.URL, AdminUserId y AdminPassword.

   ~

   # establezca lo siguiente en la URL que corresponda para AS/IG

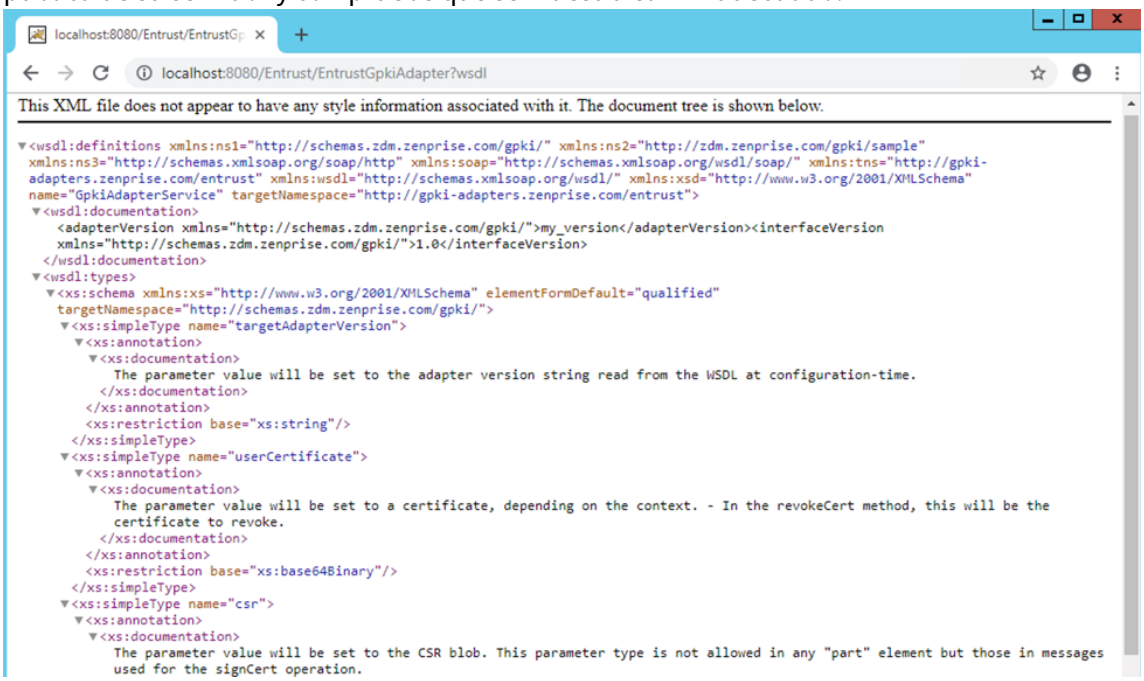
   Entrust.MdmSvc.Url=https://pki.yourcorp.com:19443/mdmws/services/AdminServiceV8

```
# set to 1 or true to force user creation from passed user and
    group parameters if using IG and user does not exist
CreateUser=

# set the credentials for the endpoint
AdminUserId=`[User ID]`
AdminPassword=`[password]`


# keystore for client-cert auth
#keyStore=
#keyStorePassword=
#keyStoreType: JKS, JCEKS and PKCS12  -- not needed for .p12 and .
    jks files

# truststore for server with self-signed root CA
#trustStore=
#trustStorePassword=
#trustStoreType: JKS, JCEKS and PKCS12  -- not needed for .p12 and
     .jks files
~
```

5. Reinicie el servicio de Tomcat. Vaya a C:\Archivos de programa (x86)\Apache Software Foundation\Tomcat 8.5\logs y abra Catalina_201x-MM-DD.log. Verifique que no haya errores y pueda ver la siguiente línea:

   13-Nov-2018 09:02:35.319 INFO [localhost-startStop-1] org.apache.cxf.endpoint.ServerImpl.initDestination Setting the server's publish address to be /EntrustGpkiAdapter

6. Vaya a `http://localhost:8080/Entrust/EntrustGpkiAdapter?wsdl` o a la URL pública de su servidor y compruebe que se muestra el XML adecuado.



Configurar XenMobile para el adaptador de PKI de Entrust

1. Inicie sesión en la consola de XenMobile y vaya a **Parámetros > Entidades PKI**. Haga clic en **Agregar > Entidad de PKI genérica**.
2. Introduzca la siguiente información:
   - **Nombre:** Introduzca un nombre para la entidad PKI.
   - **URL de WSDL:** Introduzca la URL pública del servidor.
   - **Tipo de autenticación:** Elija el método de autenticación que se va a utilizar.
     - **Ninguno**
     - **HTTP básica:** Proporcione el nombre de usuario y la contraseña necesarios para la conexión.
     - **Certificado del cliente:** Seleccione el certificado SSL de cliente correspondiente.
   - **Ubicación de recursos:** Seleccione **Mi ubicación de recursos**.
   - **Rutas relativas permitidas:** Introduzca `/Entrust/*`.
3. Una vez que haya terminado de configurar la entidad PKI, vuelva a la página **Configuración** y agregue un **proveedor de credenciales** .
4. En la ficha **General**, seleccione la entidad Entrust como **entidad emisora** y **SIGN** como **método de emisión**.
5. En la ficha **Solicitud de firma de certificados**, configure los parámetros de la siguiente manera:
   - **Algoritmo de clave: RSA**.
   - **Tamaño de clave:** 2048.

- **Algoritmo de firma: SHA256withRSA**.
- **Nombre del sujeto:** cd=$user.username
- **Nombres alternativos del sujeto:** Opcional. Recomendamos lo siguiente:
  - **Tipo: Nombre principal del usuario**.
  - **Valor:** $user.userprincipalname

    Nota:
    Si cambia algún parámetro del adaptador, siga estos pasos para volver a configurar el proveedor de credenciales.

6. Después de configurar el proveedor de credenciales, vaya a **Configurar > Directivas de dispositivo** y agregue una directiva de credenciales.
7. Configure la directiva para los sistemas operativos que piensa usar. En la página de configuración de cada sistema operativo, para **Tipo de credencial**, seleccione **Proveedor de credenciales**. En el menú **Proveedor de credenciales**, seleccione el proveedor de credenciales que configuró antes.

Servicios de certificados de Microsoft

XenMobile interactúa con Servicios de certificados de Microsoft 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). Si la CA de Microsoft genera un certificado de usuario de Citrix Gateway, Citrix Gateway admite la renovación y la revocación de esos certificados.

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.

Agregar una entidad de Servicios de certificados de Microsoft

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 **Entidades PKI**.
2. En la página **Entidades PKI**, haga clic en **Agregar**.

   Aparecerá un menú con los tipos de entidad de infraestructura de clave pública.
3. Haga clic en **Entidad de Servicios de certificados de Microsoft**.

   Aparecerá la página **Entidad de Servicios de certificados de Microsoft: Información general**.
4. En la página **Entidad de Servicios de certificados de Microsoft: Información general**, configure estos parámetros:

   - **Nombre:** Escriba un nombre para la nueva entidad; es el nombre que utilizará para hacer referencia a esa entidad. Los nombres de entidad deben ser únicos.

- **URL raíz del servicio de inscripción web:** Especifique la URL base del servicio de inscripción web de la entidad de certificación de Microsoft (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.
- **Tipo de autenticación:** Elija el método de autenticación que se va a utilizar.
  - **Ninguno**
  - **HTTP básica:** Proporcione el nombre de usuario y la contraseña necesarios para la conexión.
  - **Certificado del cliente:** Seleccione el certificado SSL de cliente correspondiente.

5. Haga clic en **Probar conexión** para comprobar que el servidor está accesible. Si no se puede establecer la conexión, aparecerá un mensaje donde se indica que falló la conexión. Compruebe los parámetros de configuración.
6. Haga clic en **Siguiente**.

   Aparece la página **Entidad de Servicios de certificados de Microsoft: Plantillas**. 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 Servicios de certificados de Microsoft, consulte la documentación de Microsoft referente a su versión de servidor Microsoft. XenMobile no presenta requisitos para los certificados que distribuye, salvo los formatos de certificado indicados en Certificados.
7. En la página **Entidad de Servicios de certificados de Microsoft: Plantillas**, haga clic en **Agregar**, escriba el nombre de la plantilla y, a continuación, haga clic en **Guardar**. Repita este paso para cada plantilla a agregar.
8. Haga clic en **Siguiente**.

   Aparece la página **Entidad de Servicios de certificados de Microsoft: Parámetros HTTP**. En esta página, puede especificar parámetros personalizados que XenMobile debe agregar a la solicitud HTTP para la interfaz de inscripción web de Microsoft. Los parámetros personalizados son útiles solo para scripts personalizados que se ejecutan en la CA.
9. En la página **Entidad de Servicios de certificados de Microsoft: Parámetros HTTP**, haga clic en **Agregar**, escriba el nombre y el valor de los parámetros HTTP a agregar. A continuación, haga clic en **Siguiente**.

Aparece la página **Entidad de Servicios de certificados de Microsoft: Certificados de CA**. 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. XenMobile aplica el cambio a la entidad de forma transparente.

10. En la página **Entidad de Servicios de certificados de Microsoft: Certificados de CA**, seleccione los certificados que se van a utilizar para la entidad.
11. Haga clic en **Guardar**.

    La entidad se muestra en la tabla "Entidades PKI".

Lista de revocación de certificados (CRL) de Citrix ADC

XenMobile solo admite la lista de revocación de certificados (CRL) cuando se trata de una entidad de certificación (CA) de terceros. Si dispone de una entidad de certificación de Microsoft configurada, XenMobile utiliza Citrix ADC para administrar la revocación.

Al configurar la autenticación por certificados de cliente, plantéese si debe configurar el parámetro de lista de revocación de certificados (CRL) de Citrix ADC, **Enable CRL Auto Refresh**. Este paso garantiza que el usuario de un dispositivo en modo solo MAM no pueda autenticarse con un certificado existente en el dispositivo.

XenMobile vuelve a emitir un certificado nuevo, porque no impide que un usuario genere otro certificado de usuario tras revocarse uno. Este parámetro aumenta la seguridad de las entidades PKI cuando la lista de revocación de certificados comprueba si hay entidades PKI caducadas.

Entidades de certificación (CA) discrecionales

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, puede activar el protocolo Online Certificate Status Protocol (OCSP) para esa entidad. Si (y solo si) habilita la compatibilidad con OCSP, la entidad de certificación agrega una extensión `id-pe-authorityInfoAccess` a los certificados que emita. La extensión apunta al respondedor OCSP interno de XenMobile que reside en la siguiente ubicación:

```
https://<server>/<instance>/ocsp
```

Al configurar el servicio OCSP, especifique 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 la extensión `id-kp-OCSPSigning extendedKeyUsage`.

El servicio de respondedor OCSP de XenMobile admite el uso de respuestas de OCSP básicas y estos 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).

Agregar entidades de certificación discrecionales

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 **Más > Entidades PKI**.
2. En la página **Entidades PKI**, haga clic en **Agregar**.

   Aparecerá un menú con los tipos de entidad de infraestructura de clave pública.
3. Haga clic en **Entidad de certificación (CA) discrecional**.

   Aparece la página **CA discrecional: Información general**.
4. En la página **CA discrecional: Información general**, lleve a cabo lo siguiente:
   - **Nombre:** Escriba un nombre descriptivo para la entidad de certificación discrecional.
   - **Certificado de CA para firmar solicitudes de certificado:** Haga clic en un certificado de la entidad de certificación discrecional que se utilizará para firmar las solicitudes de certificados.

     Esta lista de certificados se genera a partir de los certificados de CA con las claves privadas que se cargaron en XenMobile, en **Configurar > Parámetros > Certificados**.
5. Haga clic en **Siguiente**.

   Aparece la página **Discretionary CA: Parameters**.
6. En la página **Discretionary CA: Parameters**, lleve a cabo lo siguiente:
   - **Generador de números de serie:** La entidad de certificación discrecional genera números de serie para los certificados que emite. En esta lista, haga clic en **Secuencial** o en **No secuencial** para determinar el modo en que se generan los números.
   - **Siguiente número de serie:** Escriba un valor para determinar el siguiente número a emitir.

- **Certificado válido para:** Escriba la cantidad de días durante los que el certificado será válido.
- **Uso de clave:** Identifique el propósito de los certificados emitidos por la entidad de certificación discrecional. Para ello, **active** las claves apropiadas. Una vez activadas, la entidad de certificación está limitada a la emisión de certificados para esos fines.
- **Uso mejorado de clave:** Para agregar más parámetros, haga clic en **Agregar**, escriba el nombre de la clave y, a continuación, haga clic en **Guardar**.

7. Haga clic en **Siguiente**.

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

8. En la página **CA discrecional: Distribución**, seleccione un modo de distribución:

   - **Centralizado: generación de claves en el lado del servidor**. Citrix recomienda la opción centralizada. Las claves privadas se generan y se almacenan en el servidor para, luego, distribuirse a los dispositivos de usuario.
   - **Distribuido: generación de claves en el lado del dispositivo**. Las claves privadas se generan en los dispositivos de usuario. El modo distribuido utiliza SCEP y requiere un certificado de cifrado de RA con la extensión `keyUsage keyEncryption`, así como un certificado de firma de RA con la extensión `keyUsage digitalSignature`. Se puede usar el mismo certificado para el cifrado y la firma.

9. Haga clic en **Siguiente**.

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

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

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

10. Haga clic en **Guardar**.

    La entidad de certificación discrecional se muestra en la tabla “Entidades PKI”.

Proveedores de credenciales

January 4, 2022

Los proveedores de credenciales son las configuraciones de certificado en cuestión que se usarán en las distintas partes del sistema de XenMobile. Los proveedores de credenciales definen los orígenes, los parámetros y los ciclos de vida de los certificados. Esas operaciones ocurren cuando los certificados forman parte de configuraciones del dispositivo o se trata de operaciones independientes (es decir, enviadas tal cual al 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. Asimismo, los parámetros de revocación previstos para D también se aplicarán cuando C se elimine o cuando D se revoque.

De acuerdo con esas reglas, la configuración del proveedor de credenciales en XenMobile determina lo siguiente:

- El origen de los certificados.
- 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.
- 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 la clave y las extensiones del certificado.
- El modo en que los certificados se entregan al dispositivo.
- Las condiciones de revocación. Aunque todos los certificados se revocan en XenMobile cuando finaliza la relación de administración, la configuración puede especificar que la revocación ocurra antes. Por ejemplo, la configuración puede especificar revocar un certificado cuando se elimina la configuración asociada a él. 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 de certificados en XenMobile puede causar la revocación de certificados en la PKI.
- 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 PKI

y del método de emisión que seleccione para el proveedor de credenciales.

Métodos de emisión de certificados

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

- **Sign (Firmar):** Con este método, la emisión implica crear una nueva clave privada, crear una solicitud de firma de certificado y enviar esa solicitud a una entidad de certificación (CA) para su firma. XenMobile admite el método de firma para las tres entidades PKI (Servicios de certificado de Microsoft, PKI genérica y CA discrecional).
- **Fetch (Obtener):** Con este método, la emisión (en lo relativo a XenMobile) consiste en la recuperación de un par de claves que ya existe. XenMobile admite el método "fetch" solo para la PKI genérica.

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".

Entrega de certificados

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

Para que un proveedor de credenciales admita la entrega distribuida (mediante SCEP), se necesita un paso especial de configuración: se deben configurar certificados de una entidad de registro (RA). Los certificados de RA son necesarios porque, cuando se usa el protocolo SCEP, XenMobile actúa como un delegado (un registrador) para la entidad de certificación. XenMobile debe demostrar al cliente que tiene autoridad para actuar como tal. Esa autoridad se establece cargando en 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, cárguelos en XenMobile y, a continuación, vincule su implementación 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. Puede configurar cada proveedor de credenciales para que prefiera el modo centralizado o el modo distribuido, o bien para que requiera 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	No	No
Configuración de Windows Phone y Tablet	No, excepto la directiva Wi-Fi, disponible para Windows Phone 8.1, Windows 10 y Windows 11.	No

Revocación de certificados

Existen tres tipos de revocación.

- **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 eliminen del dispositivo.
- **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 Xen-

Mobile 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.

- **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 en la infraestructura de clave pública. Si el certificado está revocado, XenMobile lo revoca internamente. Este mecanismo utiliza el protocolo OCSP.

Estos tres tipos no son exclusivos, sino que se aplican juntos. Una revocación externa u otro motivo pueden causar una revocación interna. Una revocación interna afecta potencialmente a una revocación externa.

Renovación de certificados

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

XenMobile intenta obtener el nuevo certificado antes de revocar el anterior, a fin de evitar la interrupción del servicio si la emisión falla. Para la entrega distribuida (compatible con SCEP), la revocación también ocurre solamente después de que el certificado se haya instalado correctamente en el dispositivo. De lo contrario, la revocación ocurre antes de que se envíe el nuevo certificado al dispositivo. Esa revocación no depende de la instalación del certificado.

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 el certificado cumple esa condición, XenMobile intenta renovar el certificado.

Crear un proveedor de credenciales

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 los proveedores de credenciales que usan una entidad interna o una entidad externa:

- Una entidad discrecional, interna en XenMobile, es una entidad interna. El método de emisión para una entidad discrecional es siempre “sign”. Este método “sign” significa 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.

- Una entidad externa, que forma parte de la infraestructura corporativa, incluye una GPKI o CA de Microsoft.

Para obtener información detallada sobre la configuración de DigiCert Managed PKI, incluida la creación de un proveedor de credenciales, consulte "DigiCert Managed PKI" en Entidades PKI.

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 **Parámetros > Proveedores de credenciales**.
2. En la página **Proveedores de credenciales**, haga clic en **Agregar**.

   Aparecerá la página **Credential Providers: General Information**.
3. En la página **Credential Providers: General Information**, lleve a cabo lo siguiente:
   - **Nombre:** Escriba un nombre exclusivo para la configuración del nuevo proveedor. Este nombre se usará posteriormente para identificar la configuración en otras partes de la consola de XenMobile.
   - **Descripción:** Describa el proveedor de credenciales. Aunque este campo sea opcional, una descripción puede resultar útil cuando necesite datos concretos acerca del proveedor de credenciales.
   - **Entidad de emisión:** Haga clic en la entidad emisora de certificados.
   - **Método de emisión:** 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 con certificado del cliente, use **Sign**.
   - Si la lista **Plantilla** está disponible, seleccione la plantilla que agregó en el apartado de entidad PKI para el proveedor de credenciales.

     Estas plantillas pasan a estar disponibles cuando se agregan entidades de Servicios de certificado de Microsoft en **Parámetros > Entidades PKI**.
4. Haga clic en **Siguiente**.

   Aparecerá la página **Credential Providers: Certificate Signing Request**.
5. En la página **Proveedores de credenciales: Solicitud de firma de certificado**, defina lo siguiente según la configuración de su certificado:
   - **Algoritmo de clave:** Seleccione el algoritmo de clave para el nuevo par de claves. Los valores disponibles son: **RSA**, **DSA** y **ECDSA**.
   - **Tamaño de clave:** Escriba el tamaño, en bits, del par de claves. Este campo es obligatorio.

     Los valores permitidos dependen del tipo de clave. Por ejemplo, el tamaño máximo para las claves DSA es 1024 bits. Para evitar falsos negativos, los cuales dependen del hardware y software subyacentes, XenMobile no aplica tamaños de clave. Debe probar siempre las

configuraciones del proveedor de credenciales en un entorno de prueba antes de activarlas en producción.

- **Algoritmo de firma:** Haga clic en un valor para el nuevo certificado. Los valores dependen del algoritmo de clave.
- **Nombre del sujeto:** Campo obligatorio. Escriba el nombre distintivo (DN) del nuevo sujeto del certificado. Por ejemplo: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } ,C=${ user.c } \endquotation`

  Por ejemplo, para la autenticación con certificados de cliente, use los parámetros siguientes:

  - **Algoritmo de clave:** RSA
  - **Tamaño de clave:** 2048
  - **Algoritmo de firma:** SHA256withRSA
  - **Nombre del sujeto:** `cn=$user.username`
- Para agregar una nueva entrada a la tabla **Nombres alternativos del sujeto**, haga clic en **Agregar**. Seleccione el tipo de nombre alternativo y, a continuación, escriba un valor en la segunda columna.

  Para la autenticación con certificados de cliente, especifique:

  - **Tipo:** Nombre principal del usuario.
  - **Valor:** `$user.userprincipalname`

    Al igual que para Nombre del sujeto, puede usar las macros de XenMobile en el campo Valor.

6. Haga clic en **Siguiente**.

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

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

   - En la lista **Certificados de CA emisora**, 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. El certificado de CA se presenta aquí para mantener la coherencia con las configuraciones que usan entidades externas.
   - En **Seleccionar modo de distribución**, haga clic en una de las siguientes maneras de generar y distribuir claves:
     - **Preferir modo centralizado: Generación de clave en el lado del servidor:** Citrix recomienda esta opción centralizada. Admite todas las plataformas compatibles de XenMobile y es necesaria cuando se usa la autenticación de Citrix Gateway. Las claves

privadas se generan y se almacenan en el servidor para, luego, distribuirse a los dispositivos de usuario.
- **Preferir modo distribuido: Generación de clave en el lado del dispositivo:** Las claves privadas se generan y se almacenan en los dispositivos de usuario. Este modo de distribución utiliza SCEP y requiere un certificado de cifrado de RA con keyUsage keyEncryption, así como un certificado de firma de RA con KeyUsage digitalSignature. Se puede usar el mismo certificado para el cifrado y la firma.
- **Solo distribuido: Generación de clave en el lado del dispositivo:** Esta opción funciona de la misma forma que "Preferir modo distribuido: Generación de clave en el lado del dispositivo", 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 **Preferir modo distribuido: Generación de clave en el lado del dispositivo** o **Solo distribuido: Generación de clave en el lado del dispositivo**, 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.

8. Haga clic en **Siguiente**.

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

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

   - En **Revocar certificados emitidos**, seleccione una de las opciones que indican cuándo revocar los certificados.
   - Si quiere que XenMobile envíe una notificación cuando el certificado se revoque, establezca el valor de **Enviar notificación** en **Sí** 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 **Revocar certificado en PKI** en **Sí** y, en la lista **Entidad**, haga clic en una plantilla. La lista "Entidad" muestra todas las entidades de infraestructura GPKI disponibles con capacidades de revocación. Cuando el certificado se revoque XenMobile, se enviará una llamada de revocación a la infraestructura de clave pública seleccionada de la lista "Entidad".

10. Haga clic en **Siguiente**.

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

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

- **Active** el parámetro **Habilitar comprobaciones de revocación externas**. Aparecerán campos adicionales relacionados con la infraestructura de clave pública de revocación.
- En la lista **Certificado de CA de respondedor OCSP**, haga clic en el nombre distintivo (DN) del sujeto del certificado.

  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 **Cuando se revoque el certificado**, 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 **Enviar notificación** en **Sí**.

  Puede elegir entre dos opciones de notificación:
- Si selecciona **Seleccionar plantilla de notificaciones**, puede seleccionar un mensaje de notificación previamente escrito que puede personalizar. Estas plantillas se encuentran en la lista “Plantillas de notificaciones”.
- Si elige **Introducir detalles de notificación**, 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.

12. Haga clic en **Siguiente**.

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

    - Renovar el certificado. Puede enviar una notificación para la renovación y excluir los certificados ya caducados de la operación.
    - Emitir una notificación para aquellos certificados cuya fecha de caducidad se acerca (notificación antes de renovación).

13. En la página **Credential Providers: Renewal**, lleve a cabo lo siguiente si quiere renovar certificados cuando estos caduquen:

    Active la opción **Renovar certificados** cuando caduquen. Aparecen más campos.

    - En el campo **Renovar el certificado cuando queden**, escriba la antelación (la cantidad de días anteriores a la fecha de caducidad) con que debe realizarse la renovación.
    - También puede seleccionar **No renovar certificados que ya han caducado**. En este caso, “ya caducado” significa que la fecha `NotAfter` del certificado ha pasado, no que ha sido

revocado. XenMobile no renueva los certificados después de que hayan sido revocados internamente.

Si quiere que XenMobile envíe una notificación cuando el certificado se haya renovado, establezca **Enviar notificación** en **Sí**. Si quiere que XenMobile envíe una notificación cuando la fecha de caducidad se acerque, establezca **Notificar cuando se acerque la fecha de caducidad** en **Sí**.
Para cualquiera de esas opciones, puede elegir entre dos opciones de notificación:

- **Seleccionar plantilla de notificaciones:** Seleccione un mensaje de notificación previamente escrito que puede personalizar. Estas plantillas se encuentran en la lista "Plantillas de notificaciones".
- **Introducir detalles de notificación:** Escriba su propio mensaje de notificación. Proporcione la dirección de correo electrónico del destinatario, un mensaje y una frecuencia para enviar la notificación.

En el campo **Notificar cuando al certificado le queden**, escriba la antelación (la cantidad de días anteriores a la fecha de caducidad) con que debe enviarse la notificación.

14. Haga clic en **Guardar**.

    El proveedor de credenciales aparecerá en la tabla "Proveedores de credenciales".

Certificados APNs

January 4, 2022

> **Importante:**
>
> Apple dejará de desarrollar el protocolo binario heredado de APNs a partir del 31 de marzo de 2021. Apple recomienda que se utilice en su lugar la API del proveedor de APNs basada en HTTP/2. A partir de la versión 10.13.0, XenMobile Server admite la API basada en HTTP/2. Para obtener más información, consulte la actualización de noticias "Apple Push Notification Service Update" en https://developer.apple.com/. Para obtener ayuda sobre cómo comprobar la conectividad con APNs, consulte Comprobaciones de conectividad.

Para inscribir y administrar dispositivos iOS y macOS en XenMobile, debe configurar un certificado del servicio de notificaciones push de Apple (APNs) proveniente de Apple.

Resumen del flujo de trabajo:

- **Paso 1:** Cree una solicitud de firma de certificado (CSR) con uno de estos métodos:
  - Crear una solicitud de firma de certificado mediante Acceso a Llaveros en macOS (recomendado por Citrix)

  - Crear una solicitud de firma de certificado mediante Microsoft IIS
  - Crear una solicitud de firma de certificado mediante OpenSSL
- **Paso 2:** Firme la solicitud de firma de certificado en XenMobile Tools
- **Paso 3:** Envíe la solicitud de firma de certificado (CSR) firmada a Apple para obtener el certificado APNs
- **Paso 4:** Con el mismo equipo utilizado para el paso 1, complete la solicitud de firma de certificado y exporte un archivo PKCS #12:
  - Crear un archivo PKCS #12 mediante Acceso a Llaveros en macOS
  - Crear un archivo PKCS #12 mediante Microsoft IIS
  - Crear un archivo PKCS #12 mediante OpenSSL
- **Paso 5:** Importe un certificado APNs en XenMobile
- **Paso 6:** Renueve un certificado APNs

Crear una solicitud de firma de certificado

Se recomienda crear una solicitud de firma de certificado mediante Acceso a Llaveros en macOS. También puede crear una solicitud de firma de certificado mediante Microsoft IIS u OpenSSL.

> **Importante:**
>
> - Para el ID de Apple que se utiliza para crear el certificado:
>   - The Apple ID must be a corporate ID and not a personal ID.
>   - Record the Apple ID that you use to create the certificate.
>   - To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate require device reenrollment.
> - Si revoca el certificado, ya sea accidental o intencionadamente, ya no podrá administrar los dispositivos.
> - Si ha utilizado el programa iOS Developer Enterprise Program para crear un certificado push para MDM, debe gestionar las acciones correspondientes a los certificados migrados del portal Apple Push Certificates Portal.

Crear una solicitud de firma de certificado mediante Acceso a Llaveros en macOS

1. En un equipo con macOS, en **Aplicaciones > Utilidades**, inicie la aplicación Acceso a Llaveros.
2. Abra el menú **Acceso a Llaveros** y haga clic en **Asistente para Certificados > Solicitar un certificado de una entidad**.
3. El Asistente para Certificados solicitará que introduzca la información siguiente:

- **Dirección de correo electrónico:** Dirección de correo electrónico perteneciente a la cuenta de la persona o del rol responsable de administrar el certificado.
- **Nombre común:** Nombre común de la cuenta de la persona o del rol responsable de administrar el certificado.
- **Dirección de correo de la CA:** Dirección de correo electrónico de la entidad de certificación.

4. Seleccione las opciones **Se guarda en el disco** y **Permitirme especificar la información del par de llaves** y, a continuación, haga clic en **Continuar**.
5. 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**.
6. Para especificar la información del par de claves, seleccione un **Tamaño de la clave** de 2048 bits y el **Algoritmo RSA**. 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.
7. Haga clic en **Aceptar** cuando el Asistente para Certificados haya terminado el proceso de solicitud de la firma de certificado.
8. Para continuar, firme la solicitud CSR.

Crear una solicitud de firma de certificado mediante Microsoft IIS

El primer paso para generar una solicitud de certificado APNs consiste en crear una solicitud de firma de certificado (CSR). Para Windows, genere 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**.
7. Para continuar, firme la solicitud CSR.

Crear una solicitud de firma de certificado mediante OpenSSL

Si no puede usar un dispositivo macOS o Microsoft IIS para generar una solicitud de firma de certificado, use OpenSSL. Puede descargar e instalar OpenSSL desde el sitio web de OpenSSL.

1. En el equipo donde instale 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.

```
1  You are about to be asked to enter information that will be
       incorporated into your certificate request.
2  What you are about to enter is what is called a Distinguished Name
        or a DN.
3  There are quite a few fields but you can leave some blank
4  For some fields there will be a default value,
5  If you enter '.', the field will be left blank.
6  -----
7  Country Name (2 letter code) [AU]:US
8  State or Province Name (full name) [Some-State]:CA
9  Locality Name (eg, city) []:RWC
10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
       Customer
11 Organizational Unit Name (eg, section) [:Marketing
12 Common Name (eg, YOUR name) []:John Doe
13 Email Address []:john.doe@customer.com
14 <!--NeedCopy-->
```

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

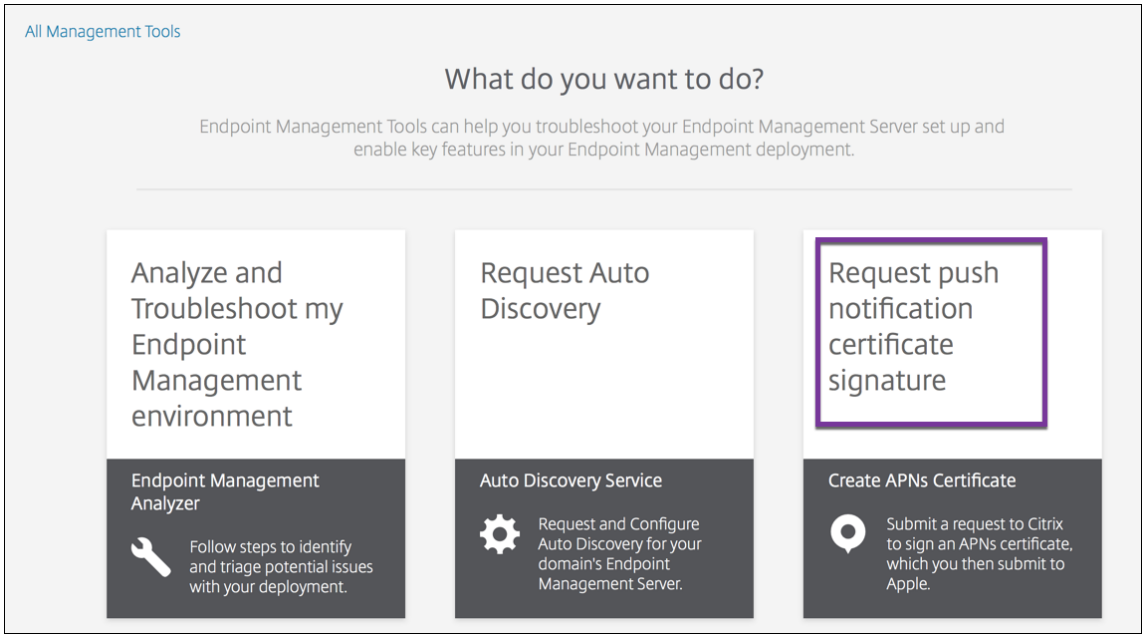
```
1  Please enter the following 'extra' attributes
2  to be sent with your certificate request
3  A challenge password []:
4  An optional company name []:
5  <!--NeedCopy-->
```

4. Para continuar, firme la solicitud de firma como se describe en la siguiente sección.

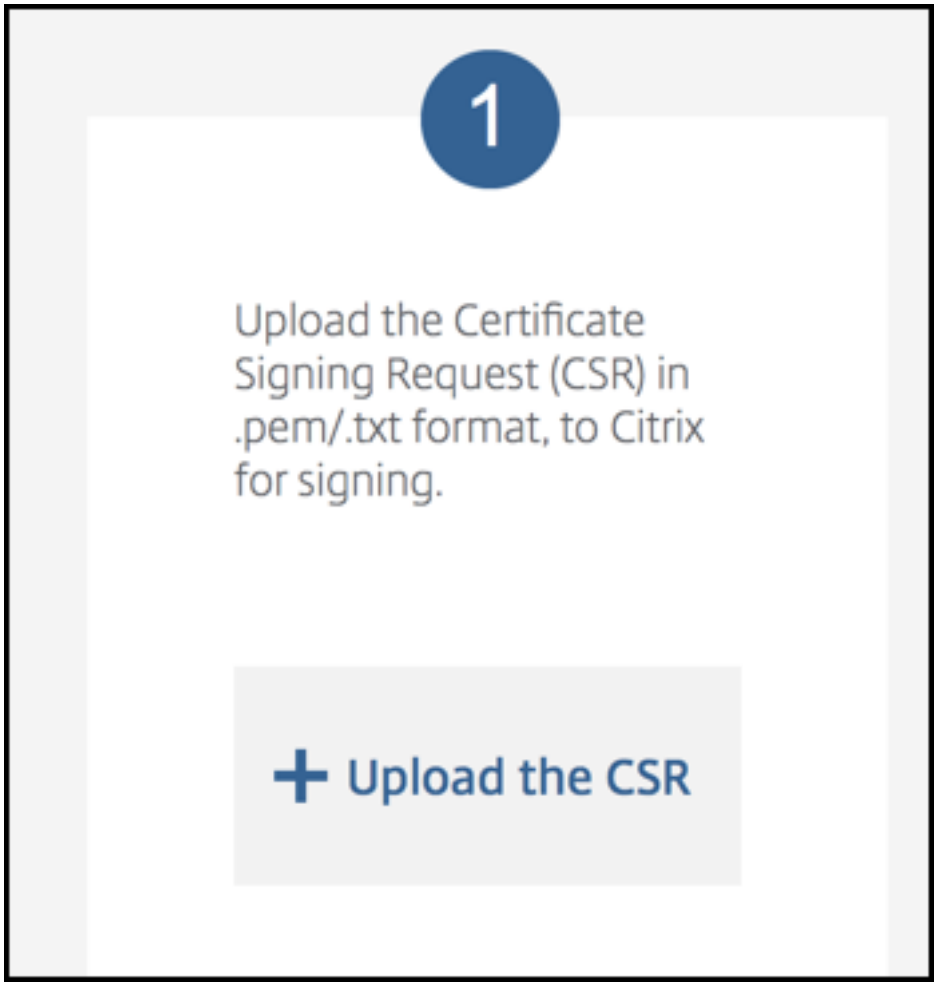
Firmar la solicitud de firma de certificado

Para utilizar un certificado con XenMobile, envíelo a Citrix para su firma. 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`.

1. En el explorador web, vaya al sitio web Endpoint Management Tools y haga clic en **Request push notification certificate signature**.



2. En la página **Creating a new certificate page**, haga clic en **Upload the CSR**.



3. Busque y seleccione el certificado.

   El certificado debe estar en el formato PEM o TXT.

4. En la página **Endpoint Management APNs CSR Signing**, haga clic en **Sign**. La solicitud se firma y se guarda automáticamente en la carpeta de descargas definida.
5. Para continuar, envíe la solicitud de firma de certificado firmada como se describe en la siguiente sección.

Enviar la solicitud de firma de certificado firmada a Apple para obtener el certificado APNs

Después de recibir la solicitud de firma de certificado (CSR) firmada de Citrix, envíela a Apple para obtener el certificado de APNs necesario para importarlo en XenMobile.

> **Nota:**
>
> Algunos usuarios han informado de problemas para iniciar sesión en el portal de certificados push de Apple. Como alternativa, inicie sesión en el Portal para desarrolladores de Apple y, a continuación, siga estos pasos.

1. En un explorador web, vaya al Portal de certificados push de Apple.
2. Haga clic en **Create a Certificate**.
3. Si es la primera vez que crea un certificado con Apple, marque la casilla **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**. Aparece un mensaje de confirmación donde se indica que la carga se ha realizado correctamente.
5. Haga clic en **Download** para obtener el certificado PEM.
6. Para continuar, rellene la solicitud de firma y exporte el archivo PKCS #12 como se describe en la siguiente sección.

Completar la solicitud de firma de certificado y exportar un archivo PKCS #12

Después de recibir el certificado APNs de Apple, vuelva a Acceso a Llaveros, Microsoft IIS u OpenSSL para exportar el certificado a un archivo PCKS #12.

Un archivo PKCS #12 contiene el archivo de certificado APNs y la clave privada. Los archivos PFX generalmente tienen la extensión PFX o P12. Puede utilizar archivos PFX o P12 indistintamente.

> **Importante:**
>
> Se recomienda guardar o exportar las claves personales y públicas del sistema local. Necesita esas claves para acceder a los certificados APNs y volver a utilizarlos. Sin las mismas claves, el certificado no es válido y debe repetir todo el proceso de solicitud CSR y APNs.

Crear un archivo PKCS #12 mediante Acceso a Llaveros en macOS

> **Importante:**
>
> Utilice el mismo dispositivo macOS para esta tarea que el que utilizó para generar la solicitud de firma de certificado.

1. En el dispositivo, busque el certificado de identidad de producción (PEM) recibido de Apple.
2. Inicie la aplicación Acceso a Llaveros y vaya a la ficha **Iniciar sesión > Mis certificados**. Arrastre y suelte el certificado de identidad del producto en la ventana abierta.
3. Haga clic en el certificado y expanda la flecha izquierda para comprobar que el certificado incluye una clave privada asociada.
4. Para comenzar a exportar el certificado a un certificado PCKS #12 (PFX), elija el certificado y la clave privada, haga clic con el botón secundario y seleccione **Exportar 2 elementos**.
5. Dé al archivo de certificado un nombre único para usarlo con XenMobile. No incluya espacios en el nombre. A continuación, elija una ubicación de carpeta para guardar el certificado, seleccione el formato de archivo PFX y haga clic en **Guardar**.
6. Escriba una contraseña para exportar el certificado. Citrix recomienda usar una contraseña única y segura. Además, compruebe que el certificado y la contraseña se encuentren en un lugar seguro para su uso y referencia posteriores.
7. La aplicación Acceso a Llaveros le solicitará la contraseña de inicio de sesión o el llavero seleccionado. Escriba la contraseña y, a continuación, haga clic en **Aceptar**. Ahora, el certificado guardado está listo para su uso con el servidor de XenMobile.
8. Para continuar, consulte Importar un certificado APNs en XenMobile.

Crear un archivo PKCS #12 mediante Microsoft IIS

> **Importante:**
>
> Use el mismo servidor IIS para esta tarea que el que utilizó para generar la solicitud de firma de certificado.

1. Abra Microsoft IIS.
2. Haga clic en el icono **Certificados de servidor**.
3. En la ventana **Certificados de servidor**, haga clic en **Completar solicitud de certificado**.

4. Busque el archivo Certificate.pem de Apple. Escriba un nombre descriptivo o el nombre del certificado y haga clic en **Aceptar**. No incluya espacios en el nombre.
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**.

   Necesita la contraseña del certificado para importarlo a XenMobile.
7. Copie el certificado PFX al servidor en el que se instalará XenMobile.
8. Para continuar, consulte Importar un certificado APNs en XenMobile.

Crear un archivo PKCS #12 mediante OpenSSL

Si utiliza OpenSSL para crear una solicitud de firma de certificado, también puede usar OpenSSL para crear un certificado APNs PFX.

1. En un símbolo del sistema o shell, ejecute el siguiente comando. `Customer.privatekey.pem` es la clave privada de su solicitud de firma de certificado. `APNs_Certificate.pem` es el certificado que acaba de recibir de Apple.

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey.pem -out apns_identity.pfx
   ```
2. Escriba una contraseña para el archivo de certificado de extensión PFX. Recuerde esta contraseña, porque necesitará volver a utilizarla cuando cargue el certificado en XenMobile.
3. Tome nota de la ubicación del archivo de certificado PFX. Copie el archivo al servidor de XenMobile para poder usar la consola de XenMobile para cargar el archivo.
4. Para continuar, importe un certificado APNs en XenMobile, como se describe en la sección siguiente.

Importar un certificado APNs en XenMobile

Después de recibir el 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 **Parámetros > Certificados**.
2. Haga clic en **Importar > Almacén de claves**.
3. En **Usar como**, elija **APNs**.
4. Busque el archivo P12 en su equipo.
5. Escriba la contraseña y, a continuación, haga clic en **Importar**.

Para obtener más información acerca de los certificados en XenMobile, consulte Certificados y autenticación.

Para renovar un certificado APNs

> **Importante:**
>
> Si usa otro ID de Apple para el proceso de renovación, deberá volver a inscribir los dispositivos de usuario.

Para renovar un certificado APNs, siga los pasos necesarios para crear un certificado y, a continuación, vaya al Portal de certificados push de Apple. Utilice ese portal para cargar el nuevo certificado. Después de iniciar sesión, aparece el certificado existente o un certificado 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. Para renovar el certificado, utilice el mismo nombre de organización y el mismo ID de Apple.

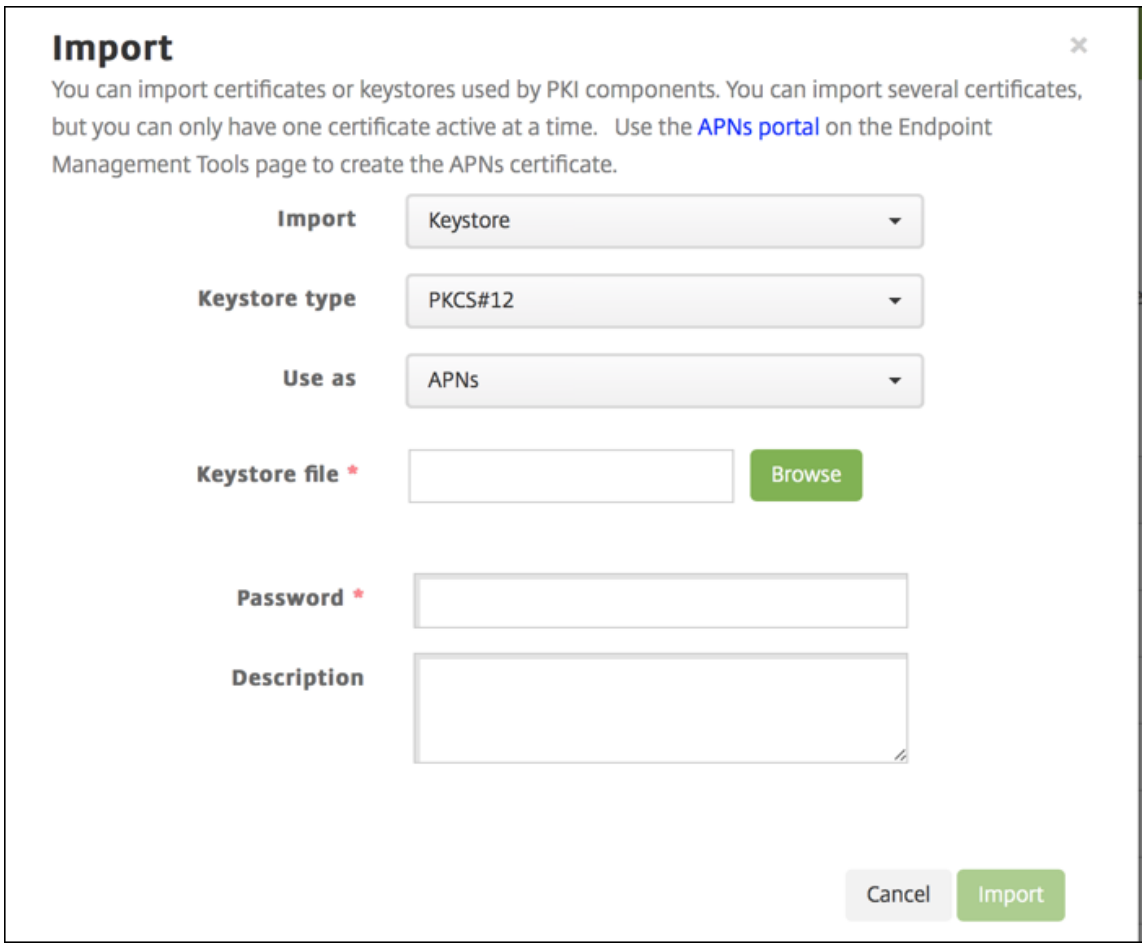
Para determinar cuándo caduca su certificado APNs, en la consola de XenMobile, vaya a **Parámetros > Certificados**. Si el certificado caduca, no lo revoque.

1. Genere una solicitud CSR mediante Microsoft IIS, Acceso a Llaveros (macOS) u OpenSSL. Para obtener más información sobre cómo generar una solicitud CSR, consulte Crear una solicitud de firma de certificado.
2. En el explorador, vaya a XenMobile Tools. A continuación, haga clic en **Request push notification certificate signature**.
3. Haga clic en **+ Upload the CSR**.
4. En el cuadro de diálogo, vaya a la solicitud CSR y haga clic en **Open** y **Sign**.
5. Cuando reciba un archivo `.plist`, guárdelo.
6. En el título del paso 3, haga clic en **Apple Push Certificates Portal** e inicie sesión.
7. Seleccione el certificado que se va a renovar y, a continuación, haga clic en **Renew**.
8. Cargue el archivo `.plist`. Recibirá un archivo PEM de salida. Guarde el archivo PEM.
9. Con ese archivo PEM, complete la solicitud CSR (de acuerdo con el método que usó para crear la CSR en el Paso 1).
10. Exporte el certificado como un archivo PFX.

En la consola de XenMobile, importe el archivo PFX y complete la configuración de este modo:

1. Vaya a **Parámetros > Certificados > Importar**.
2. En el menú **Importar**, elija **Almacén de claves**.

3. En el menú **Tipo de almacén de claves**, elija **PKCS #12**.
4. En **Usar como**, elija **APNs**.



5. Para el **Archivo de almacén de claves**, haga clic en **Examinar** y vaya al archivo.
6. En **Contraseña**, escriba la contraseña del certificado.
7. Puede escribir una **descripción** opcional.
8. Haga clic en **Importar**.

XenMobile lo redirige a la página **Certificados**. Se actualizan los campos **Nombre**, **Estado**, **Válido desde** y **Válido hasta**.

SAML para Single Sign-On en Citrix Files

January 4, 2022

Puede configurar XenMobile y Citrix Content Collaboration para que utilicen el lenguaje Security Assertion Markup Language (SAML) si quiere proporcionar el acceso Single Sign-On (SSO) a las aplicaciones

móviles de Citrix Files. Esta funcionalidad incluye:

- Aplicaciones de Citrix Files que están habilitadas para el SDK de MAM o empaquetadas con MDX Toolkit
- Clientes de Citrix Files no empaquetados, como el sitio web, Outlook Plug-in o clientes de sincronización
- **En caso de aplicaciones empaquetadas de Citrix Files**. A los usuarios que inician sesión en Citrix Files a través de la aplicación móvil de Citrix Files 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 móvil de Citrix Files envía el token SAML a Content Collaboration. Después del inicio de sesión inicial, los usuarios pueden acceder a la aplicación móvil de Citrix Files a través de SSO. También pueden adjuntar documentos desde Content Collaboration a correos de Secure Mail sin iniciar sesión cada vez.
- **En caso de clientes no empaquetados de Citrix Files**. A los usuarios que inician sesión en Citrix Files desde un explorador web u otro cliente de Citrix Files se les redirige a XenMobile. XenMobile autentica a esos usuarios, quienes adquieren un token SAML que se envía a Content Collaboration. Después del primer inicio de sesión, los usuarios pueden acceder a los clientes de Citrix Files mediante Single Sign-On, sin iniciar sesión cada vez.

Si quiere usar XenMobile como un proveedor de identidades (IdP) SAML para Content Collaboration, debe configurar XenMobile para su uso con cuentas Enterprise, como se describe en este artículo. También puede configurar XenMobile para que funcione solamente con conectores de zonas de almacenamiento. Para obtener más información, consulte Usar Citrix Content Collaboration con XenMobile.

Para obtener un diagrama detallado con una arquitectura como referencia, consulte Arquitectura.

Requisitos previos

Debe cumplir los siguientes requisitos previos antes de configurar SSO en XenMobile y las aplicaciones de Citrix Files:

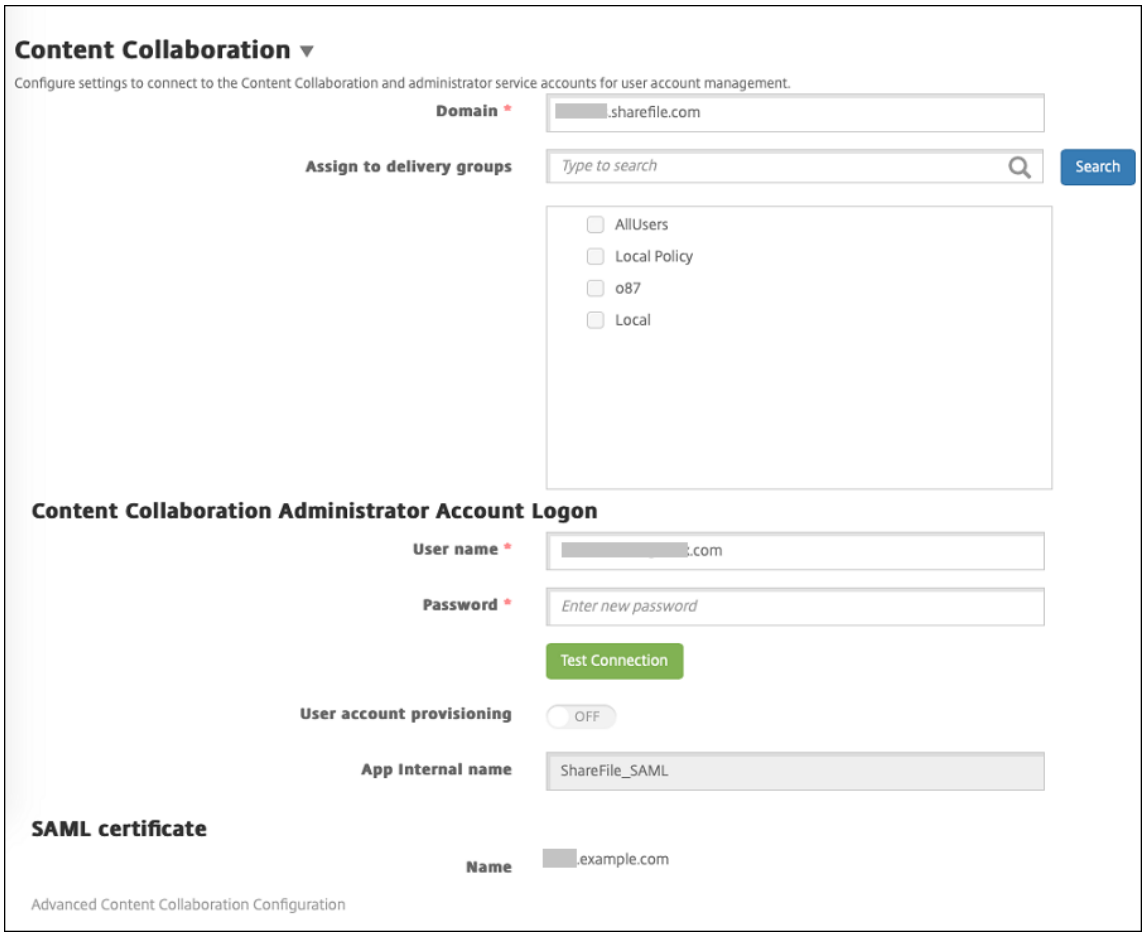
- El SDK de MAM o una versión compatible de MDX Toolkit (para aplicaciones móviles de Citrix Files).

  Para obtener más información, consulte Compatibilidad de XenMobile.
- Una versión compatible de aplicaciones móviles de Citrix Files y Secure Hub
- Cuenta de administrador de Content Collaboration.
- Conectividad verificada entre XenMobile y Content Collaboration.

Configurar el acceso a Content Collaboration

Antes de configurar SAML para Content Collaboration, proporcione la siguiente información de acceso a Content Collaboration:

1. En la consola Web de XenMobile, haga clic en **Configurar > ShareFile**. Aparecerá la página de configuración **ShareFile**. Es posible que la consola muestre el término Content Collaboration en lugar de ShareFile.



2. Configure estos parámetros:

   - **Dominio:** Escriba el nombre del subdominio de Content Collaboration. Por ejemplo: `example.sharefile.com`.
   - **Asignar a grupos de entrega:** Seleccione o busque los grupos de entrega que podrán usar SSO en Content Collaboration.
   - **Inicio de sesión de cuenta de administrador de ShareFile**
   - **Nombre de usuario:** Escriba el nombre de usuario del administrador de Content Collaboration. Este usuario debe tener privilegios de administrador.
   - **Contraseña:** Escriba la contraseña del administrador de Content Collaboration.
   - **Aprovisionamiento de cuentas de usuario:** Deje este parámetro inhabilitado. Utilice la

herramienta de administración de usuarios de Content Collaboration para el aprovisionamiento de usuarios. Consulte Aprovisionar cuentas de usuario y grupos de distribución.

3. Haga clic en **Probar conexión** para verificar que el nombre de usuario y la contraseña de la cuenta de administrador de Content Collaboration realizan la autenticación en la cuenta de Content Collaboration especificada.
4. Haga clic en **Guardar**.
   - XenMobile se sincroniza con Content Collaboration y actualiza los parámetros de Content Collaboration **ID de entidad o emisor de ShareFile** y **URL de inicio de sesión**.
   - La página **Configurar > ShareFile** muestra el **nombre interno de la aplicación**. Necesita ese nombre para completar los pasos descritos más adelante en Modificar los parámetros de Single Sign-On para Citrix Files.com.

Configurar SAML para aplicaciones MDX empaquetadas de Citrix Files

No es necesario utilizar Citrix Gateway para la configuración de Single Sign-On con aplicaciones MDX de Citrix Files empaquetadas. Para configurar el acceso de clientes de Citrix Files no empaquetados, como el sitio web, Outlook Plug-in o los clientes de sincronización, consulte Configurar Citrix Gateway para otros clientes de Citrix Files.

Los siguientes pasos se aplican a aplicaciones y dispositivos iOS y Android. Para configurar SAML en aplicaciones MDX de Citrix Files empaquetadas:

1. Con MDX Toolkit, empaquete la aplicación móvil de Citrix Files. Para obtener más información sobre cómo empaquetar aplicaciones con MDX Toolkit, consulte Empaquetar aplicaciones con MDX Toolkit.
2. En la consola de XenMobile, cargue la aplicación móvil empaquetada de Citrix Files. 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 Content Collaboration con el nombre de usuario y la contraseña de administrador que ha configurado anteriormente.
4. Compruebe que Content Collaboration y XenMobile estén configurados para la misma zona horaria. Compruebe que XenMobile muestra la hora correcta con respecto a la zona horaria configurada. Si no, Single Sign-On podría fallar.

Validar la aplicación móvil de Citrix Files

1. En el dispositivo de usuario, instale y configure Secure Hub.
2. Desde XenMobile Store, descargue e instale la aplicación móvil de Citrix Files.

3. Inicie la aplicación móvil de Citrix Files. Citrix Files se inicia sin solicitar el nombre de usuario ni la contraseña.

Validar con Secure Mail

1. En el dispositivo de usuario (si no se ha hecho aún), instale y configure Secure Hub.
2. Desde XenMobile Store, descargue, instale y configure Secure Mail.
3. Abra un nuevo correo electrónico y toque **Adjuntar desde Citrix Files**. Los archivos disponibles para adjuntar al mensaje de correo electrónico se muestran sin solicitar el nombre de usuario ni la contraseña.

Configurar el dispositivo Citrix Gateway para otros clientes de Citrix Files

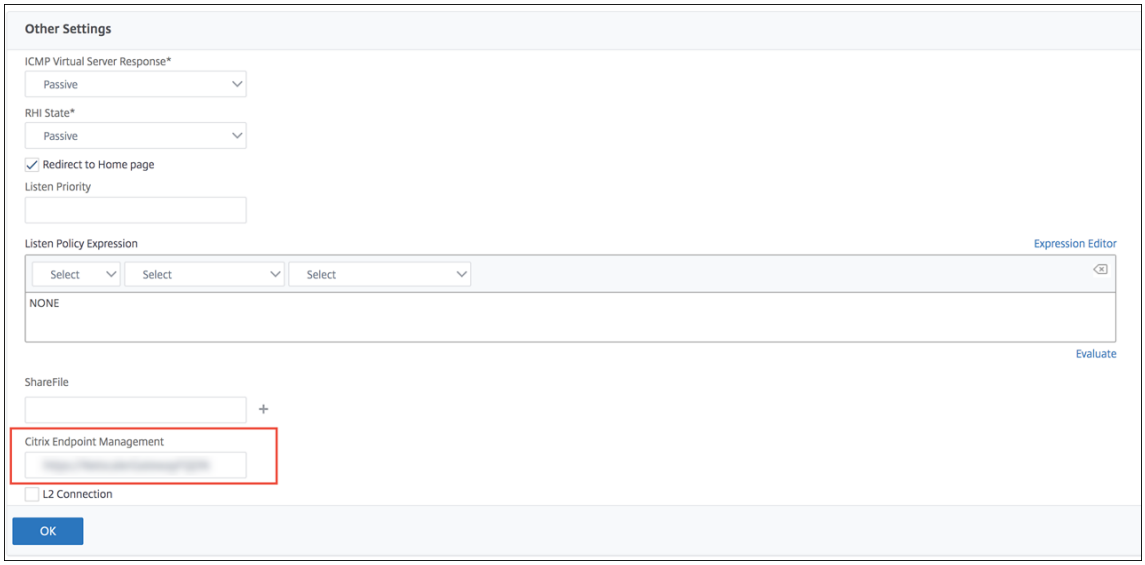
Si quiere configurar el acceso para clientes no empaquetados de Citrix Files (como el sitio web, el plugin para Outlook o los clientes de sincronización), debe configurar Citrix Gateway para que admita XenMobile como proveedor de identidades SAML de la siguiente manera.

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

Inhabilitar la redirección de la página principal

Inhabilite el comportamiento predeterminado para las solicitudes que provienen de la ruta /cginfra. Esa acción permite a los usuarios ver la URL interna solicitada original, en lugar de la página de inicio configurada.

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



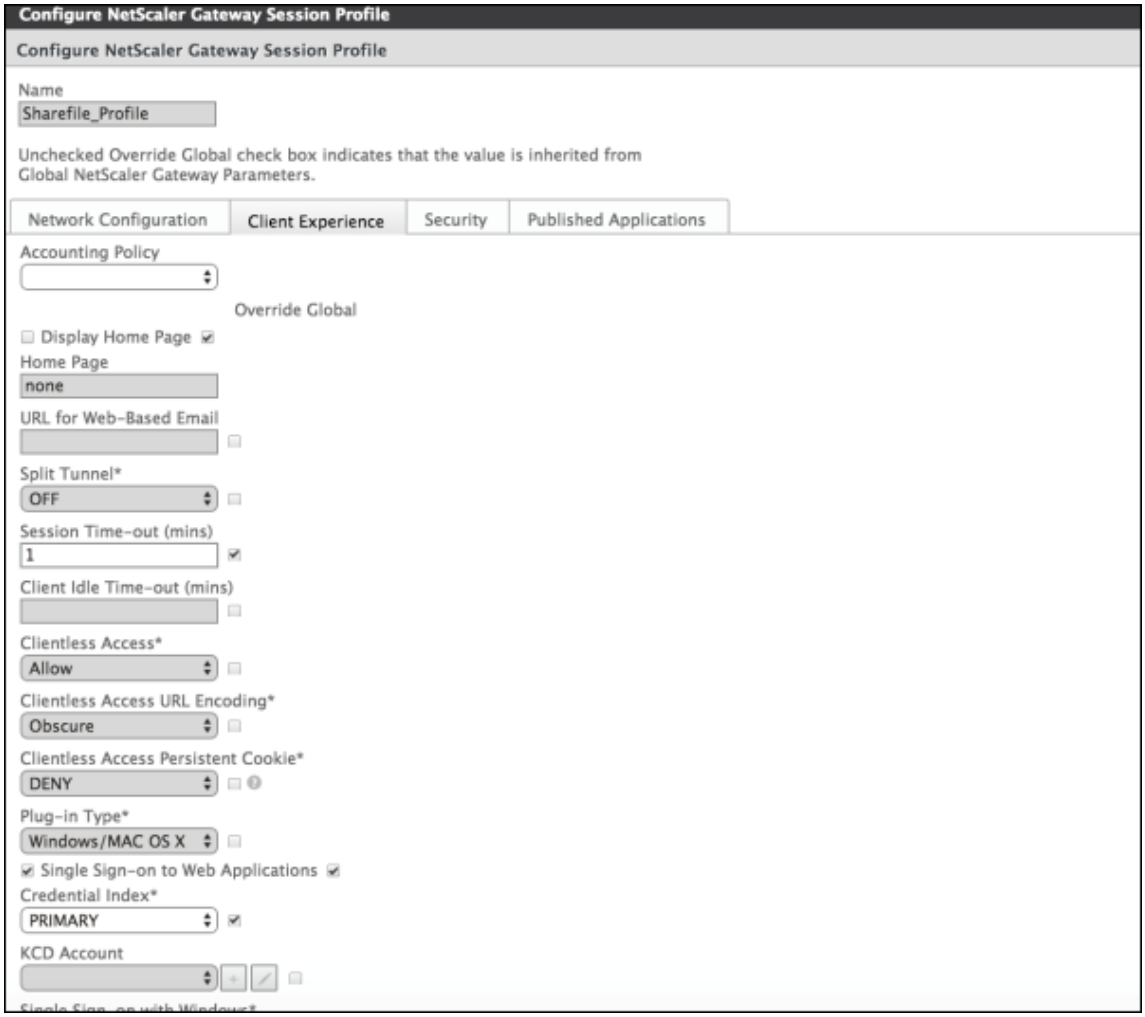
2. En **ShareFile** (ahora denominado Content Collaboration), escriba el nombre del servidor interno y el número de puerto de XenMobile.
3. En **Citrix Endpoint Management**, escriba la URL de XenMobile. Es posible que su versión de Citrix Gateway haga referencia al nombre de producto anterior **AppController**.

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

Crear un perfil de solicitudes y una directiva de sesión de Citrix Files

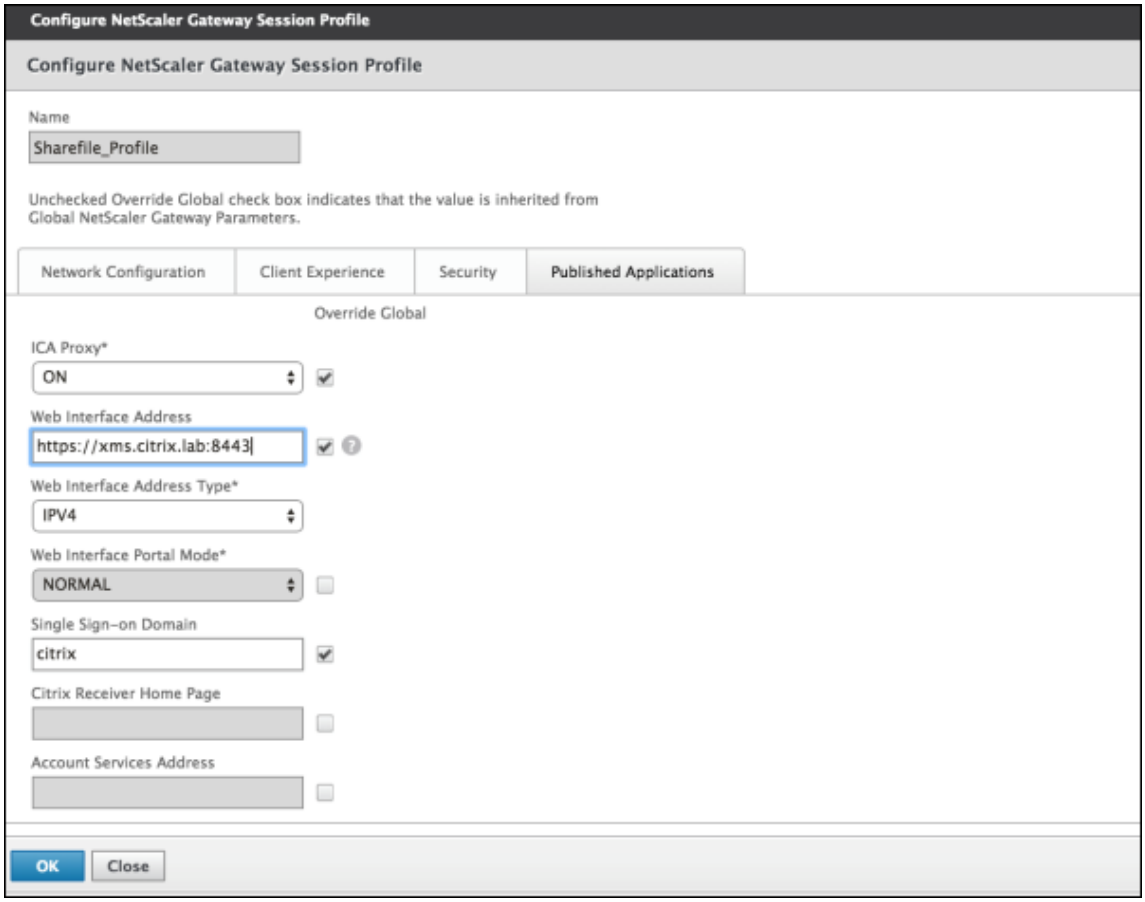
Configure los siguientes parámetros para crear un perfil de solicitudes y una directiva de sesión de Citrix Files:

1. En la herramienta de configuración de Citrix Gateway, en el panel de navegación de la izquierda, haga clic en **Citrix Gateway > Policies > Session**.
2. Cree una directiva de sesión. En la ficha **Policies**, haga clic en **Add**.
3. En el campo **Name**, escriba **ShareFile_Policy**.
4. Para crear una acción nueva, haga clic en el botón **+**. Aparecerá la página **Create Session Profile**.



Configure estos parámetros:

- **Name:** Escriba **ShareFile_Profile**.
- Haga clic en la ficha **Client Experience** y, a continuación, configure los siguientes parámetros:
  - **Home Page:** Escriba **none**.
  - **Tiempo de espera de la sesión (min):** Escriba **1**.
  - **Single Sign-On to Web Applications:** Marque este parámetro.
  - **Credential Index:** En la lista, haga clic en **PRIMARY**.
- Haga clic en la ficha **Published Applications**.

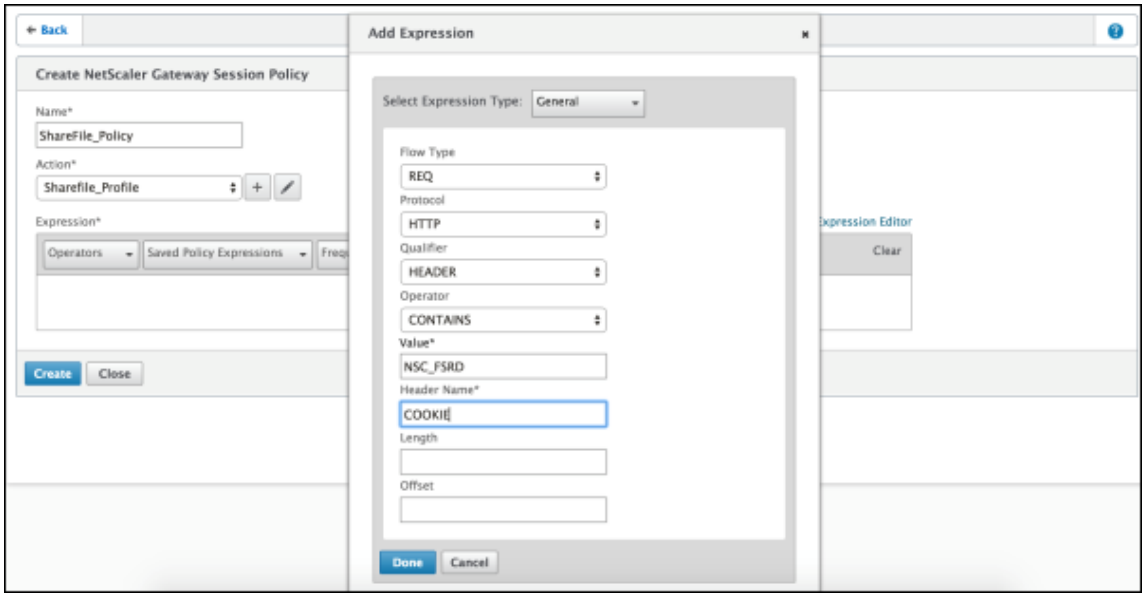


Configure estos parámetros:

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

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

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



Configure estos parámetros:

- **Value:** Escriba **NSC_FSRD**.
- **Header Name:** Escriba **COOKIE**.

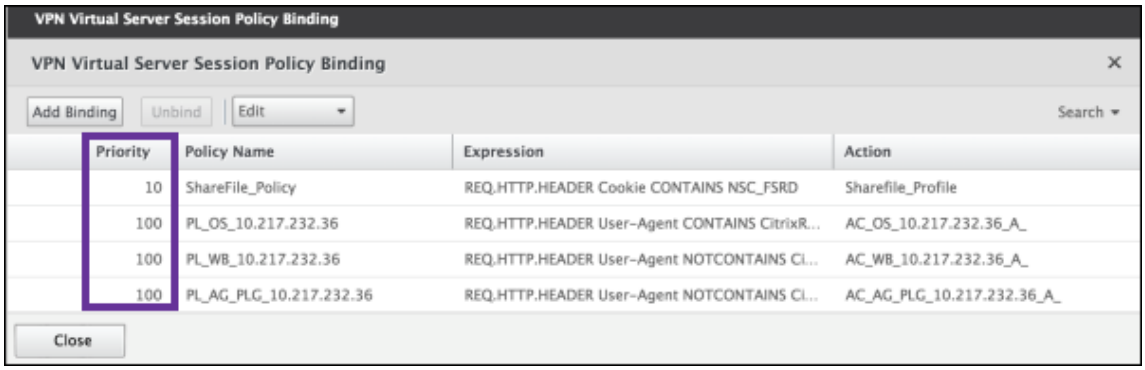
7. Haga clic en **Create** y, luego, en **Close**.

Configurar directivas en el servidor virtual de Citrix Gateway

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

1. En la herramienta de configuración de Citrix Gateway, en el panel de navegación de la izquierda, haga clic en **Citrix Gateway > Virtual Servers**.
2. En el panel **Details**, haga clic en el servidor virtual de Citrix Gateway.
3. Haga clic en **Edit**.
4. Haga clic en **Configured policies > Session policies** y, a continuación, haga clic en **Add binding**.

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



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

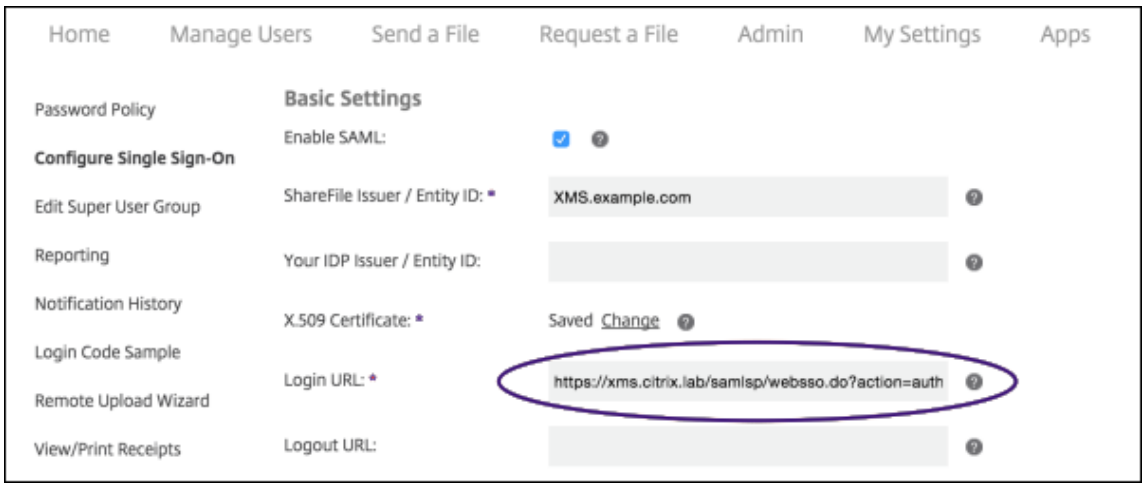
Modificar los parámetros de Single Sign-On para Citrix Files.com

Realice los siguientes cambios para aplicaciones Citrix Files que se hayan empaquetado con MDX o no.

> **Importante:**
>
> Se anexa un nuevo número al nombre interno de la aplicación:
>
> - Cada vez que modifique o vuelva a crear la aplicación Citrix Files
> - Cada vez que cambie la configuración de Content Collaboration en XenMobile
>
> Por eso, también debe actualizar la URL de inicio de sesión en el sitio web de Citrix Files, para reflejar el nombre actualizado de la aplicación.

1. Inicie sesión en su cuenta de Content Collaboration (`https://<subdomain>.sharefile.com`) como administrador de Content Collaboration.
2. En la interfaz web de Content Collaboration, 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:

   Esta es una **URL de inicio de sesión** de ejemplo antes de las modificaciones: `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 Citrix Gateway y **/cginfra/https/** delante del FQDN de XenMobile Server y, a continuación, agregue **8443** después del FQDN de XenMobile.

  Esta es una URL modificada de ejemplo: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=SHareFile_SAML_SP&reqtype=1`

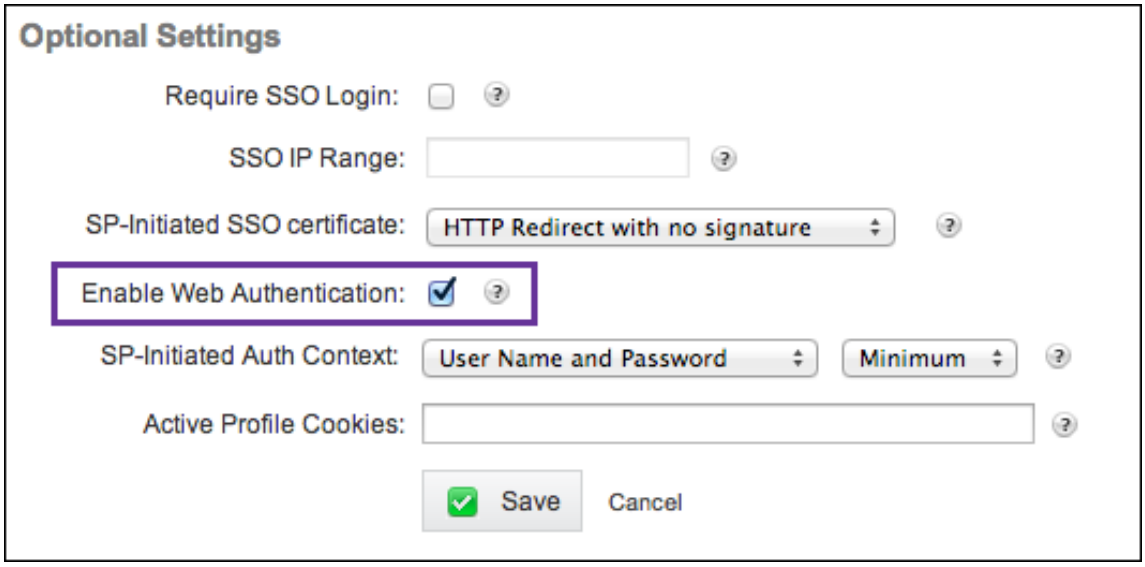
- Cambie el parámetro &app=ShareFile_SAML_SP al nombre interno de la aplicación Citrix Files. De forma predeterminada, el nombre interno es ShareFile_SAML. Sin embargo, cada vez que cambie la configuración, se agregará un número al nombre interno (ShareFile_SAML_2, ShareFile_SAML_3, etc.). Puede buscar el **nombre interno de la aplicación** en la página **Configurar > ShareFile**.

  Esta es una URL modificada de ejemplo: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

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

  Este es un ejemplo de la URL final: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`.

4. En **Parámetros optativos**, marque la casilla **Habilitar autenticación web**.



Validar la configuración

Lleve a cabo lo siguiente para validar la configuración.

1. Apunte el explorador web a `https://<subdomain>sharefile.com/saml/login`.

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

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

   Aparecerán sus carpetas de Citrix Files en `<subdomain>.sharefile.com`. Si no ve las carpetas de Citrix Files, compruebe que ha indicado correctamente las credenciales de inicio de sesión.

Azure Active Directory como proveedor de identidades

January 4, 2022

Configurar Azure Active Directory (AAD) como su proveedor de identidades (IdP) permite a los usuarios inscribirse en XenMobile con sus credenciales de Azure.

Se admiten dispositivos iOS, Android, Windows 10 y Windows 11. Los dispositivos iOS y Android se inscriben a través de Secure Hub. Este método de autenticación solo está disponible para los usuarios que se inscriben en MDM a través de Citrix Secure Hub. Los dispositivos que se inscriben en MAM no pueden autenticarse con credenciales de AAD. Para utilizar Secure Hub con MDM+MAM, configure

XenMobile de modo que se pueda usar Citrix Gateway para la inscripción de MAM. Para obtener más información, consulte Citrix Gateway y XenMobile.

Puede configurar Azure como su proveedor de identidades desde **Parámetros > Autenticación > Proveedor de identidades**. La página **Proveedor de identidades** es nueva en esta versión de XenMobile. En versiones anteriores de XenMobile, Azure se configuraba en **Parámetros > Microsoft Azure**.

Requisitos

- Versiones y licencias
  - Para inscribir dispositivos iOS o Android, se necesita Secure Hub 10.5.5.
  - Para inscribir dispositivos con Windows 10 o Windows 11, necesita licencias Premium de Microsoft Azure.
- Autenticación y servicios de directorios
  - XenMobile Server debe estar configurado para la autenticación basada en certificados.
  - Si utiliza Citrix ADC para la autenticación, este debe configurarse para la autenticación basada en certificados.
  - La autenticación de Secure Hub utiliza Azure AD y respeta el modo de autenticación que se defina en Azure AD.
  - XenMobile Server debe conectarse a Windows Active Directory (AD) mediante LDAP. Configure el servidor local de LDAP para la sincronización con Azure AD.

Flujo de autenticación

Cuando el dispositivo se inscribe a través de Secure Hub y XenMobile está configurado para usar Azure como proveedor de identidades:

1. En su dispositivo, los usuarios introducen un nombre de usuario y una contraseña de Azure Active Directory en la pantalla de inicio de sesión de Azure AD que se muestra en Secure Hub.
2. Azure AD valida el usuario y envía un token de ID.
3. Secure Hub comparte el token de ID con XenMobile Server.
4. XenMobile valida el token de ID y la información de usuario presente en el token de ID. XenMobile devuelve un ID de sesión.

Configuración de cuenta de Azure

Para usar Azure Active Directory como su proveedor de identidades, primero inicie sesión en su cuenta de Azure y haga estos cambios:

1. Registre el dominio personalizado y verifíquelo. Para ver información más detallada, consulte Guía de inicio rápido: Incorporación de un nombre de dominio personalizado a Azure.
2. Extienda el directorio local a Azure Active Directory mediante las herramientas de integración de directorios. Para obtener información más detallada, consulte Integrar directorios.

Para usar Azure Active Directory para inscribir dispositivos con Windows 10 y Windows 11, realice estos cambios en la cuenta de Azure:

1. 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**.
2. Seleccione **Agregar una aplicación** en la galería. Vaya a **ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES** y seleccione **Aplicación MDM local**. Guarde la configuración.

   Puede elegir la aplicación local incluso aunque se hubiera registrado en la nube de Citrix XenMobile. Según la terminología de Microsoft, toda aplicación no multiempresa (o multiarrendatario) es una aplicación MDM local.
3. En la aplicación, configure los términos de uso de los dispositivos de punto final, URI de ID de aplicación y la detección de XenMobile Server de la siguiente manera:
   - **URL de detección MDM:** `https://<FQDN>:8443/<instanceName>/wpe`
   - **URL de condiciones de uso MDM:** `https://<FQDN>:8443/<instanceName>/wpe/tou`
   - **URI de ID de la aplicación:** `https://<FQDN>:8443/`
4. Seleccione la aplicación MDM local que creó en el paso 2. 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.

   Para obtener más información sobre el uso de Azure Active Directory para dispositivos con Windows 10 y Windows 11, consulte el artículo Azure Active Directory integration with MDM de Microsoft.

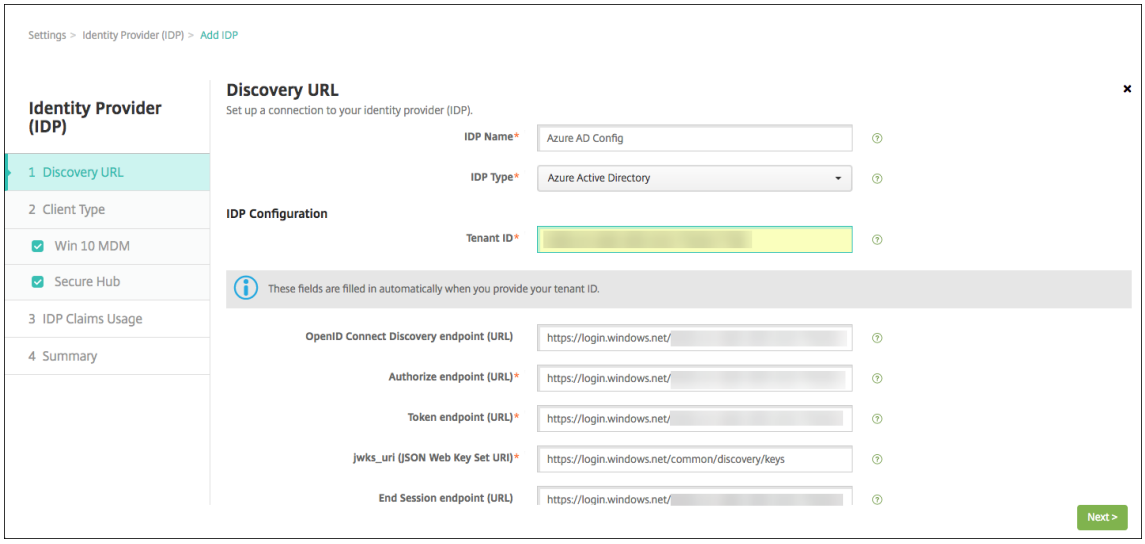
Configurar Azure Active Directory como su proveedor de identidades

1. Busque o tome nota de la información que necesaria de su cuenta de Azure:
   - "ID de arrendatario", obtenido desde la página "Configuración de la aplicación" de Azure.
   - Si quiere usar Azure AD para inscribir dispositivos con Windows 10 o Windows 11, también necesita:
     - **URI de ID de aplicación:** La dirección URL del servidor que ejecuta XenMobile.
     - **ID de cliente:** Un identificador único para la aplicación; puede obtenerlo desde la página "Configurar" de Azure.
     - **Clave:** Se obtiene desde la página "Configuración de la aplicación" de Azure.

2. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
3. En **Autenticación**, haga clic en **Proveedor de identidades (IdP)**. Aparecerá la página **Proveedor de identidades**.

4. Haga clic en **Agregar**. Aparecerá la página **Configuración de IdP**.
5. Configure la siguiente información acerca de su IdP:
   - **Nombre de IdP:** Escriba un nombre para la conexión del proveedor de identidades que está creando.
   - **Tipo de IdP:** Elija Azure Active Directory como el tipo de proveedor de identidades.
   - **ID de arrendatario:** Copie este valor de la página "Configuración de la aplicación" de Azure. En la barra de direcciones del explorador, copie la sección de números y letras.

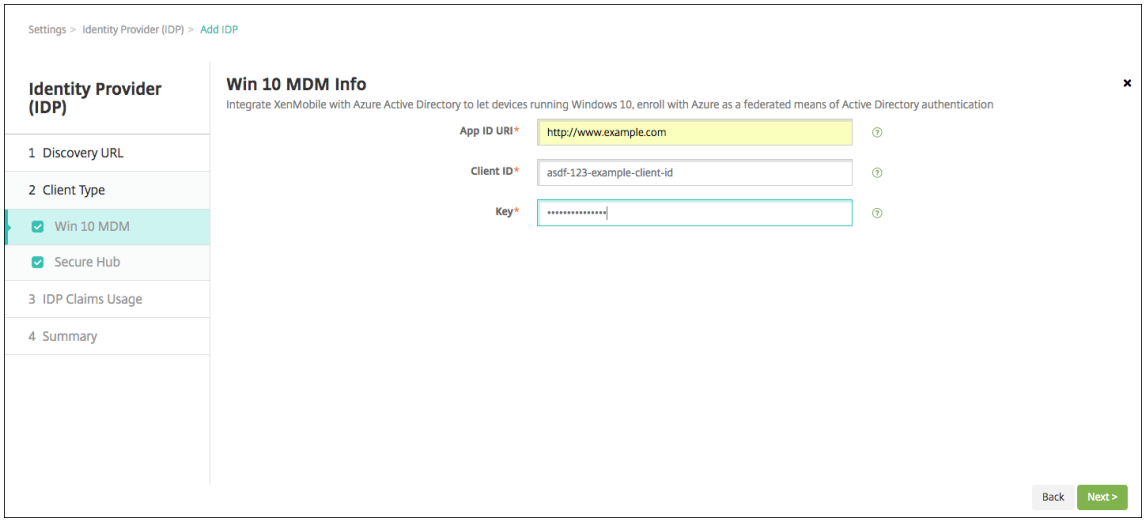
   Por ejemplo, en `https://manage.windowszaure.com/acmew.onmicrosoft.com##workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...`, el ID del arrendatario es: `abc123-abc123-abc123`.



6. El resto de los campos se rellena automáticamente. Cuando se rellenen, haga clic en **Siguiente**.

7. Para configurar XenMobile para inscribir dispositivos con Windows 10 y Windows 11 mediante Azure Active Directory para la inscripción de MDM, configure estos parámetros. Para omitir este paso opcional, desmarque **MDM Windows**.

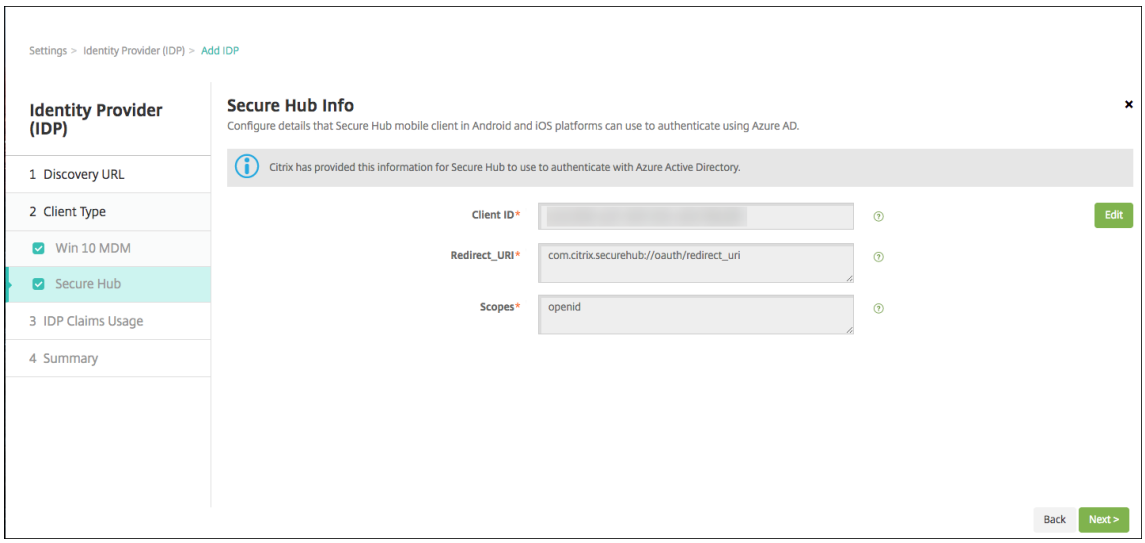
   - **URI de ID de la aplicación:** Escriba la URL del servidor de XenMobile Server que especificó cuando configuró los parámetros de Azure.
   - **ID de cliente:** Copie y pegue este valor de la página "Configuración de Azure". El ID de cliente es un identificador único de la aplicación.
   - **Clave:** Copie este valor de la página "Configuración de la aplicación" de Azure. En la sección de las claves, 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.



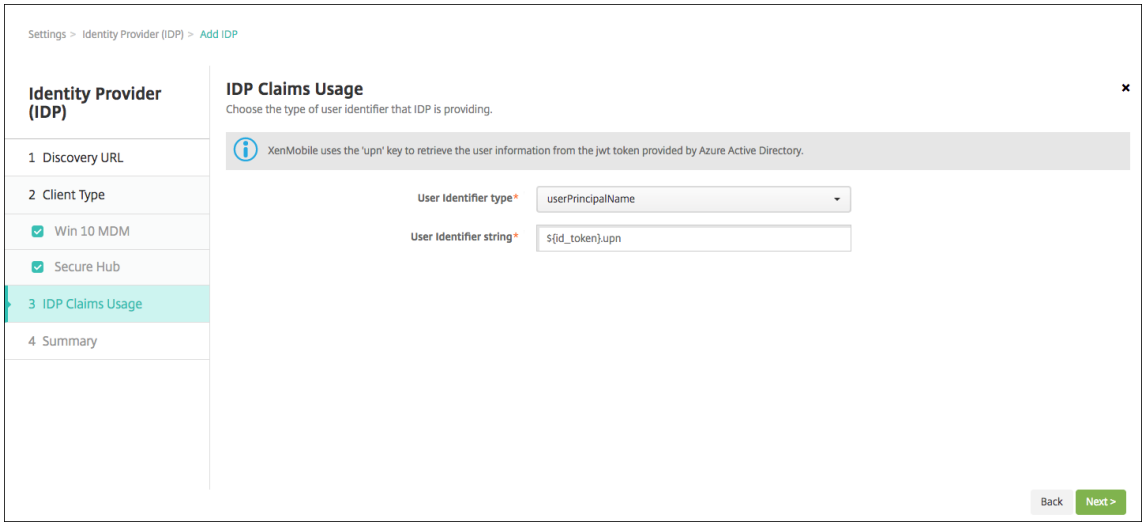
8. Haga clic en **Siguiente**.

   Citrix ha registrado Secure Hub en Microsoft Azure y se encarga de la información. En esta pantalla, se muestran los datos que utiliza Secure Hub para comunicarse con Azure Active Directory. Use esta página en el futuro si necesita cambiar alguno de estos datos. Modifique esta página solo si Citrix se lo recomienda.

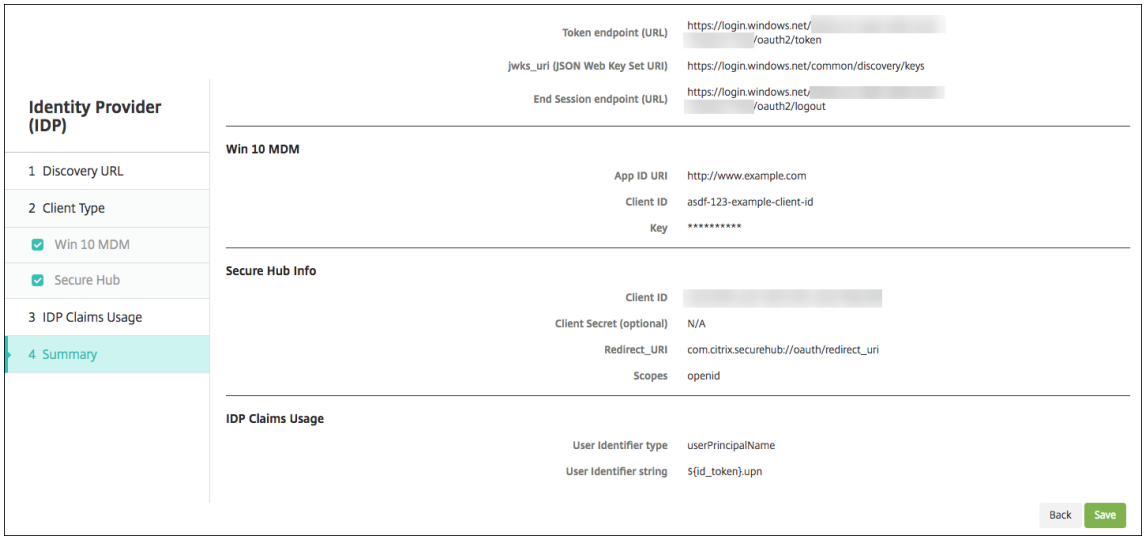
9. Haga clic en **Siguiente**.



10. Configure el tipo de identificador de usuario que proporciona el IdP:
    - **Tipo de identificador de usuario:** Elija **userPrincipalName** de la lista desplegable.
    - **Cadena de identificador del usuario:** Este campo se rellena automáticamente.
11. Haga clic en **Siguiente**.

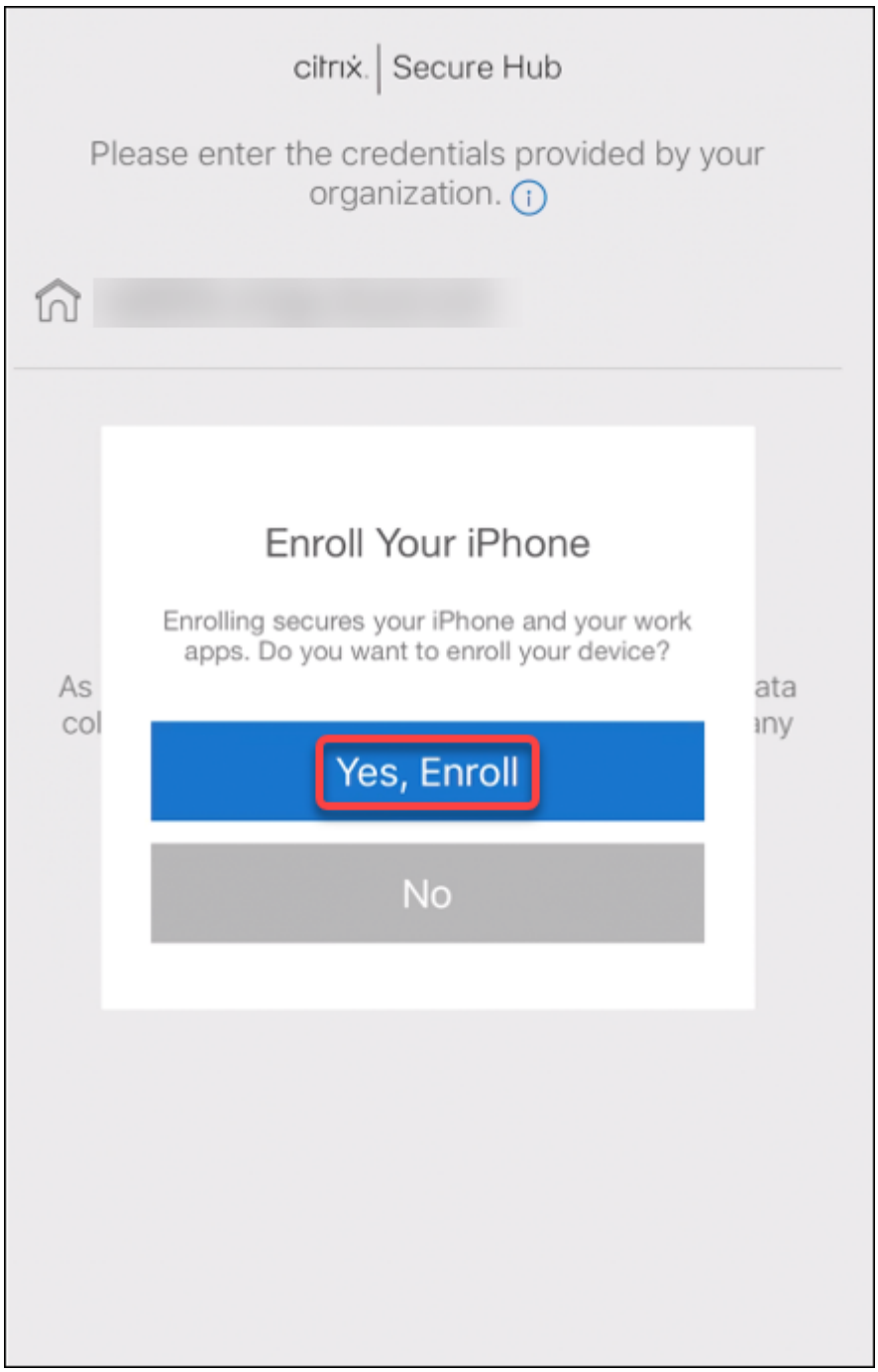


12. Revise la página **Resumen** y haga clic en **Guardar**.

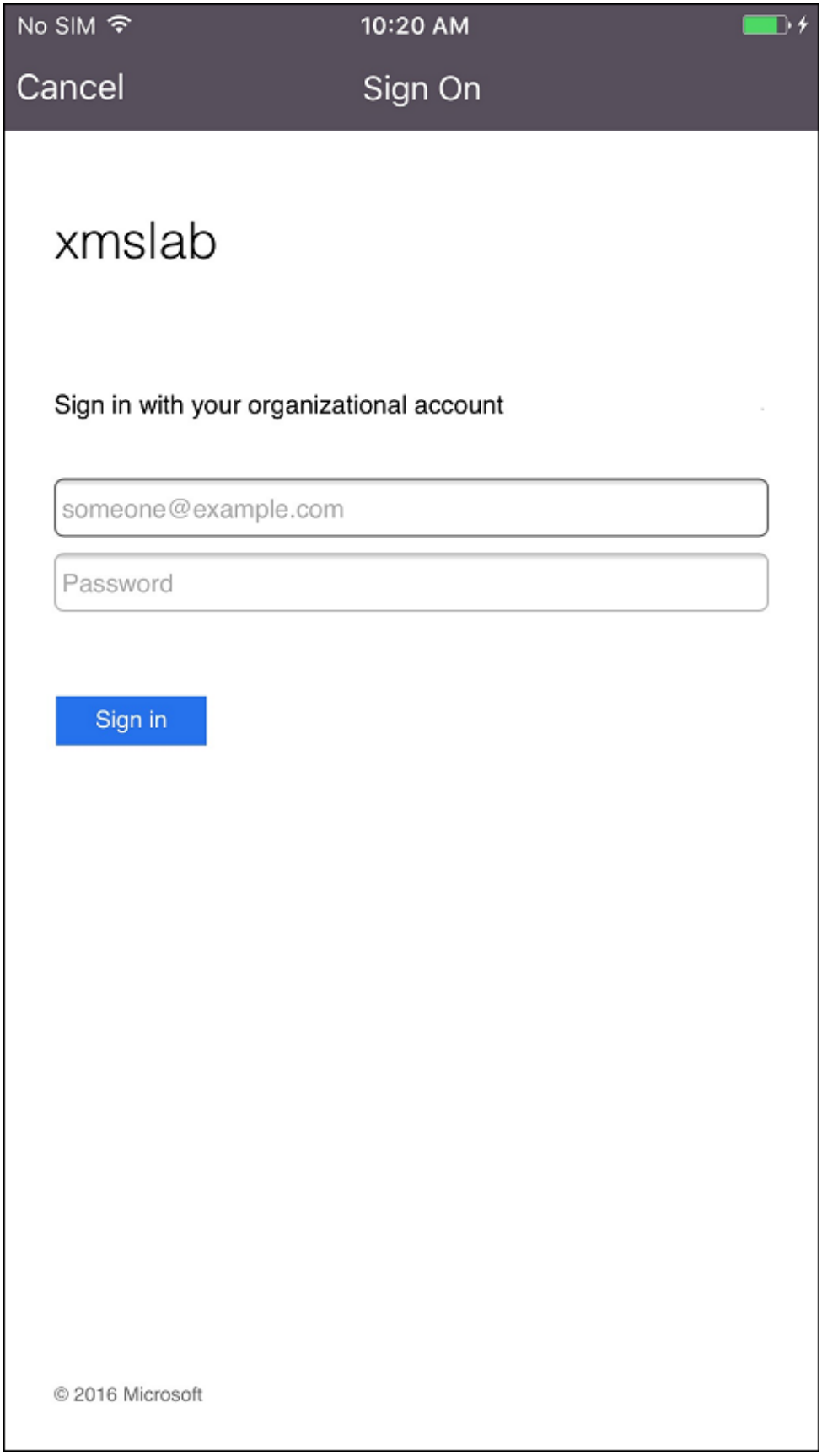


Experiencia de los usuarios

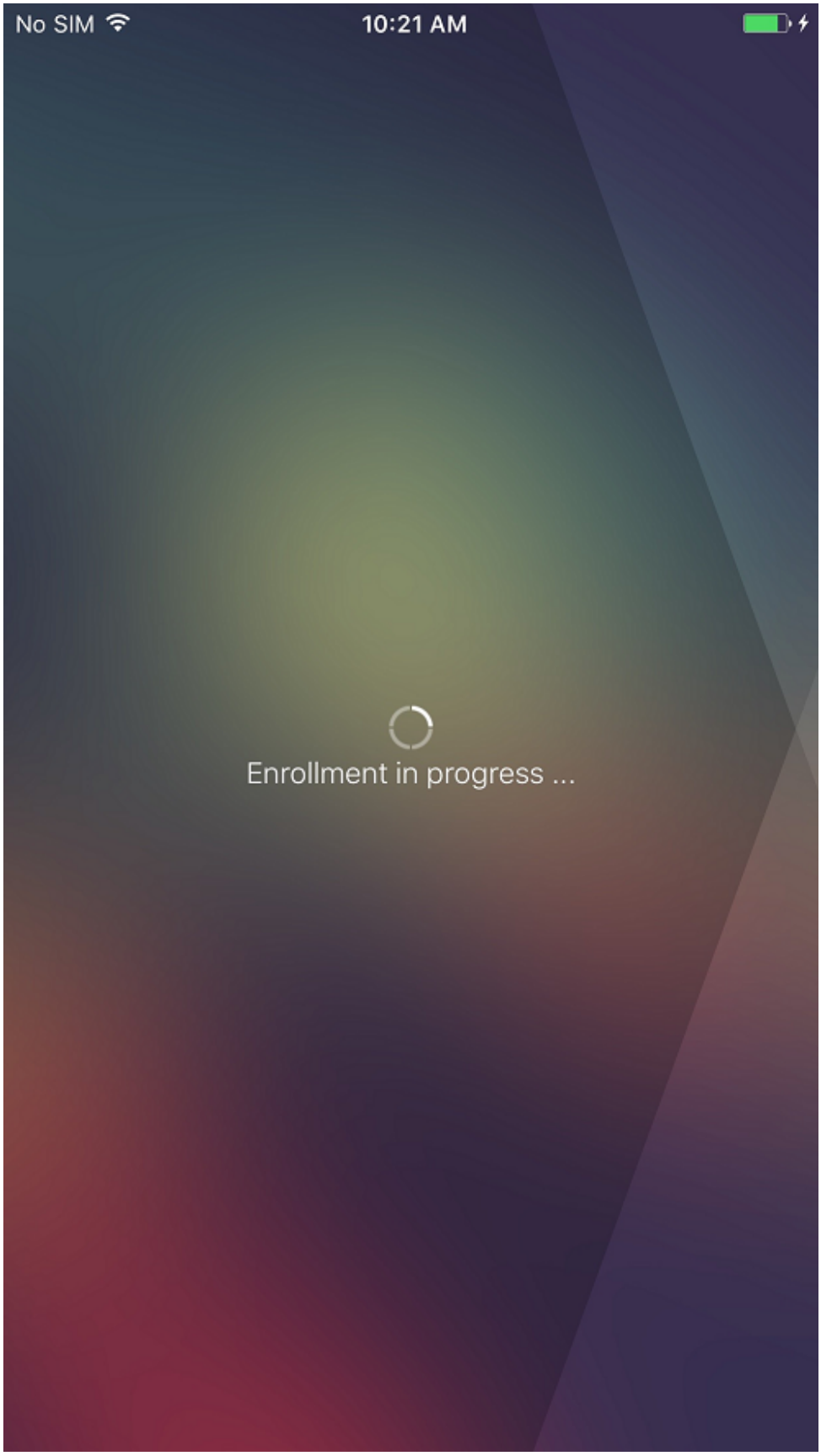
1. Los usuarios inician Secure Hub. A continuación, los usuarios introducen el nombre de dominio completo (FQDN) de XenMobile Server, un nombre de principal de usuario (UPN) o una dirección de correo electrónico.

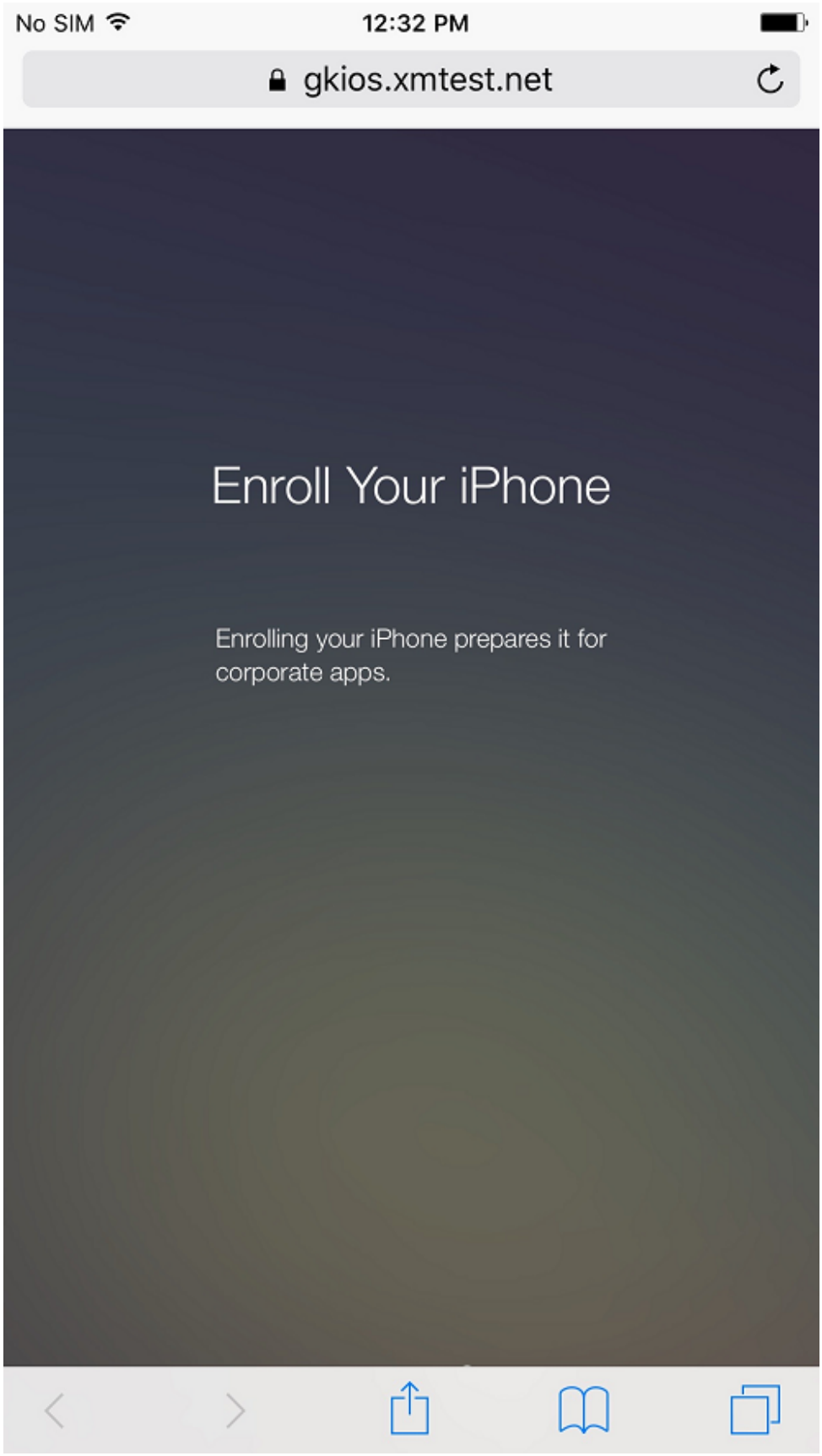


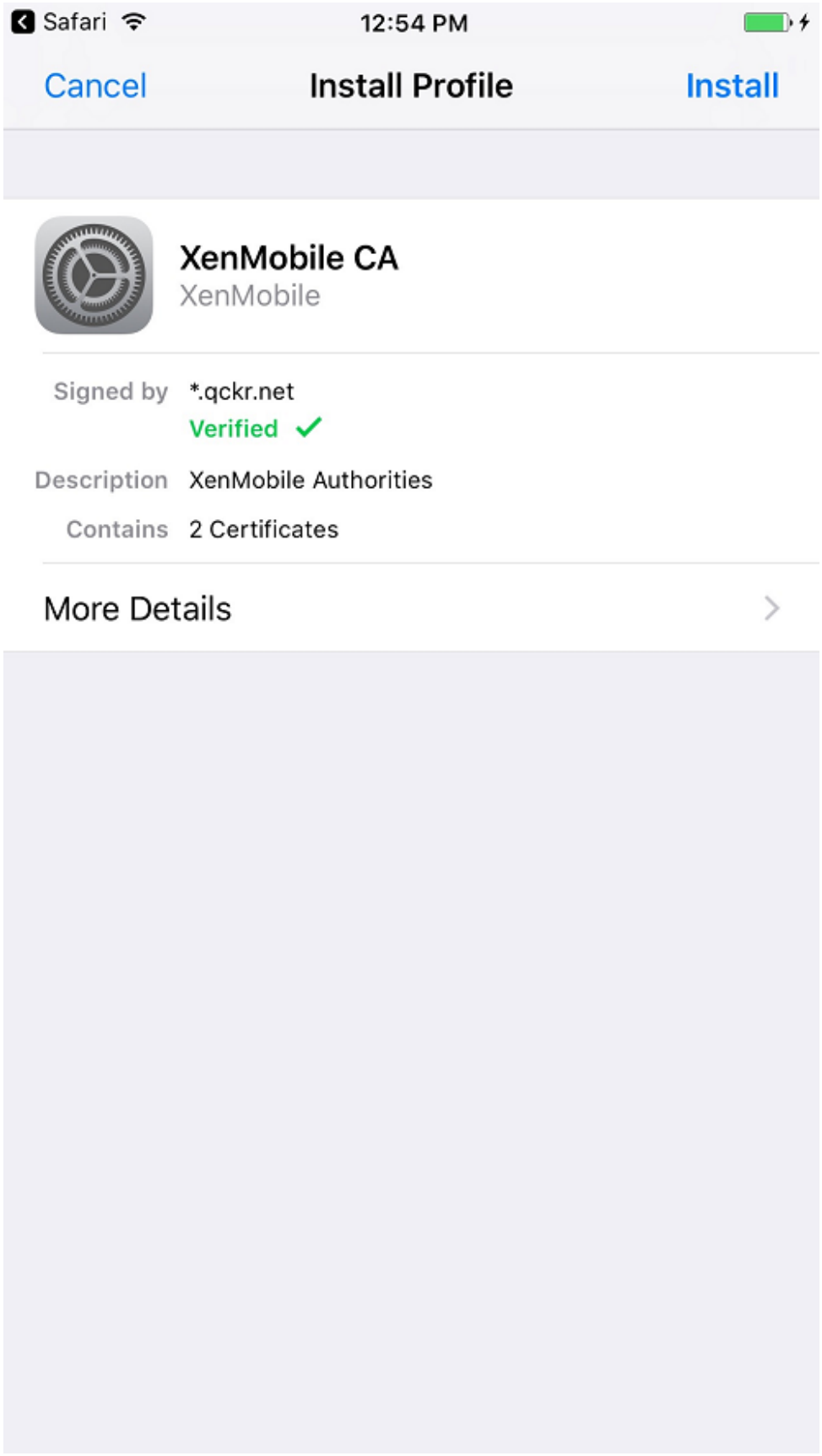
2. Luego, los usuarios hacen clic en **Sí, inscribirlo**.



3. Los usuarios inician sesión con sus credenciales de Azure AD.







4. Los usuarios completan los pasos de inscripción de la misma forma que cualquier otra inscripción a través de Secure Hub.

> **Nota:**
>
> XenMobile no admite la autenticación a través de Azure AD para invitaciones de inscripción. Si envía una invitación de inscripción a los usuarios y esa invitación contiene una URL de inscripción, los usuarios deberán autenticarse a través de LDAP en lugar de Azure AD.

Credenciales derivadas

January 4, 2022

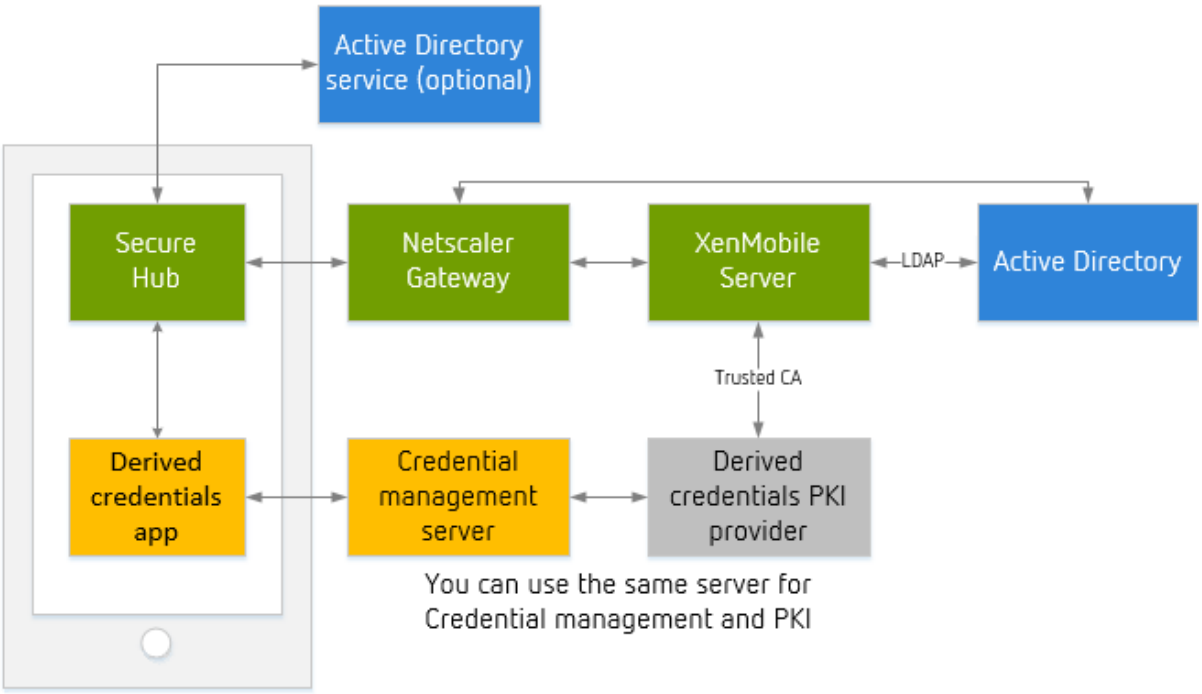
Las credenciales derivadas ofrecen una autenticación sólida para dispositivos móviles. Una tarjeta inteligente proporciona las credenciales, que residen en un dispositivo móvil, en lugar de en la tarjeta. Una tarjeta inteligente es una tarjeta Personal Identity Verification (PIV).

Las credenciales derivadas son un certificado de inscripción que contiene un identificador de usuario como, por ejemplo, su nombre principal o UPN. XenMobile almacena las credenciales obtenidas del proveedor de credenciales en un almacén seguro que tenga el dispositivo.

XenMobile puede utilizar credenciales derivadas para inscribir y autenticar dispositivos. Si se configura para las credenciales derivadas, XenMobile no admitirá invitaciones de inscripción u otros modos de seguridad de inscripción. Citrix admite el uso de una aplicación de credenciales derivadas durante la inscripción de iOS.

Arquitectura

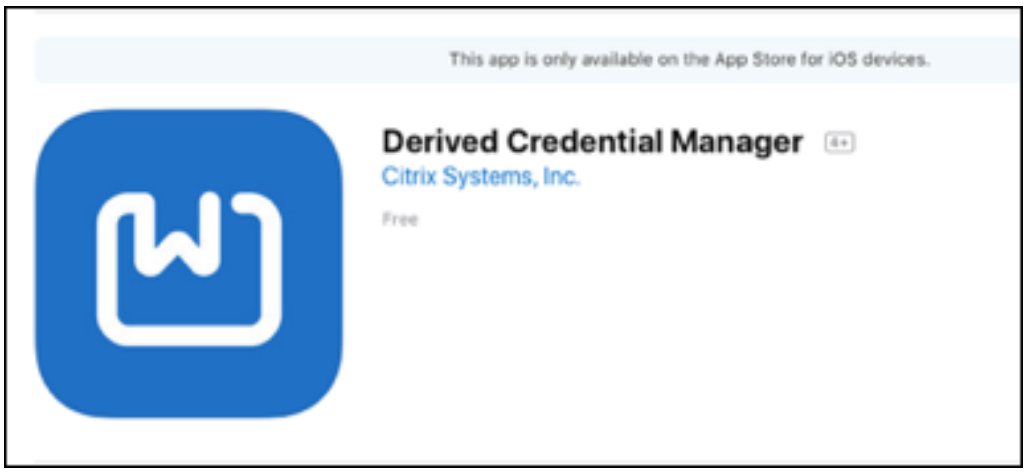
Para la inscripción, XenMobile Server se conecta a los componentes, como se muestra en el diagrama siguiente.



- Durante la inscripción del dispositivo, Secure Hub obtiene certificados de la aplicación de credenciales derivadas.
- La aplicación de credenciales derivadas se comunica con el servidor de administración de credenciales durante la inscripción.
- Puede usar el mismo servidor u otro diferente como servidor de administración de credenciales y un proveedor de PKI de terceros.
- XenMobile Server se conecta al servidor externo de PKI para obtener los certificados.

Requisitos

- Descargue e instale Citrix Secure Hub.
- En función de la solución de credenciales derivadas, descargue y configure la aplicación:
  - **Para Entrust Datacard:**
    - Descargue e instale la aplicación Citrix Derived Credential Manager en los dispositivos *antes* de inscribirse en XenMobile. Derived Credentials Manager es la aplicación del proveedor de identidades para Citrix. Este es el logotipo de esa aplicación.



    * La aplicación Citrix Derived Credentials Manager solo admite nuevas inscripciones. Los usuarios de los dispositivos deben volver a inscribirse.
        · XenMobile Server 10.8 o posterior.
        · Requiere la inscripción del dispositivo en MDM+MAM.
  - **Otros proveedores de credenciales derivadas:** Aunque es probable que la mayoría de las demás soluciones de credenciales sean compatibles con XenMobile, pruebe la integración antes de implementar una de ellas en producción.

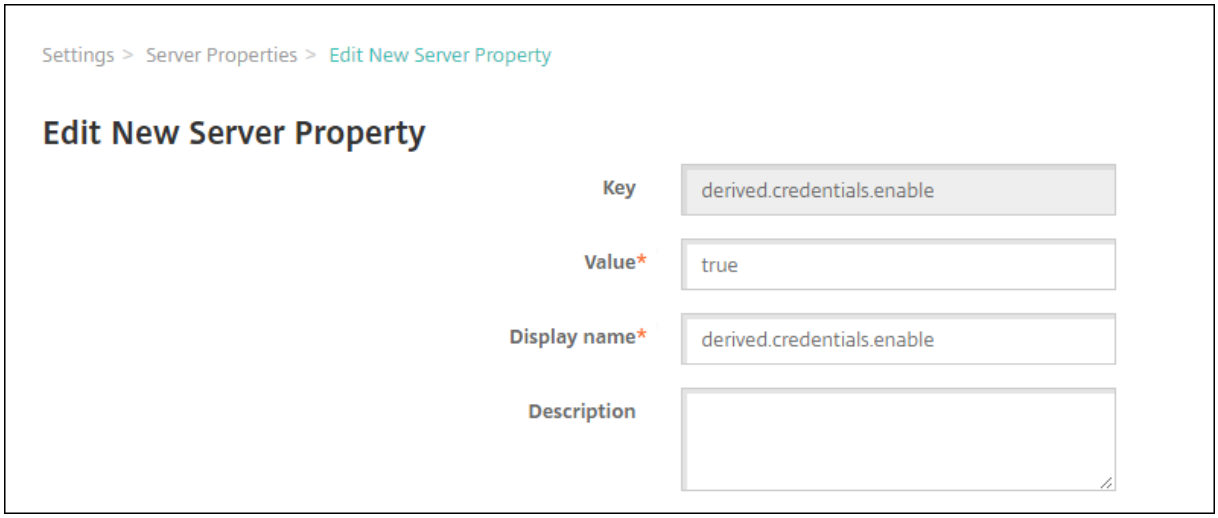
- Debe tener el certificado raíz de la entidad que emite certificados al servidor del proveedor de credenciales. Esa configuración permite a XenMobile aceptar los certificados firmados digitalmente durante la inscripción. Para obtener más información sobre cómo agregar certificados, consulte Certificados y autenticación.
  - Si el dominio de correo electrónico del usuario difiere del dominio LDAP, incluya el dominio de correo electrónico en el parámetro **Alias de dominio** en **Parámetros > LDAP**. Por ejemplo, si el dominio de las direcciones de correo electrónico es `citrix.com` y el nombre de dominio LDAP es `sample.com`, establezca **Alias de dominio** en **`sample.com , citrix.com`**.
  - XenMobile no admite el uso de credenciales derivadas con dispositivos compartidos.
- Certificados de identidad del usuario:
  - El nombre de usuario en el campo “Nombre alternativo del sujeto” debe tener el formato del campo otherName, rfc822Name o dNSName de la extensión SubjectAltName. No se admiten los demás campos. Para obtener más información sobre el nombre alternativo del sujeto, consulte el protocolo RFC en https://www.ietf.org/rfc/rfc5280.txt.
  - Actualmente, no se admite la identidad de usuario en el campo “Asunto” de correo electrónico o CN.
- Citrix Gateway configurado para la autenticación por certificado o la autenticación por certificado y token de seguridad

Habilitar credenciales derivadas

De forma predeterminada, la consola de XenMobile no contiene la página **Parámetros > Credenciales derivadas**.

Para permitir las credenciales derivadas en la interfaz:

- Vaya a **Parámetros > Propiedades de servidor**, agregue **derived.credentials.enable** como propiedad de servidor y establézcala en **true**.

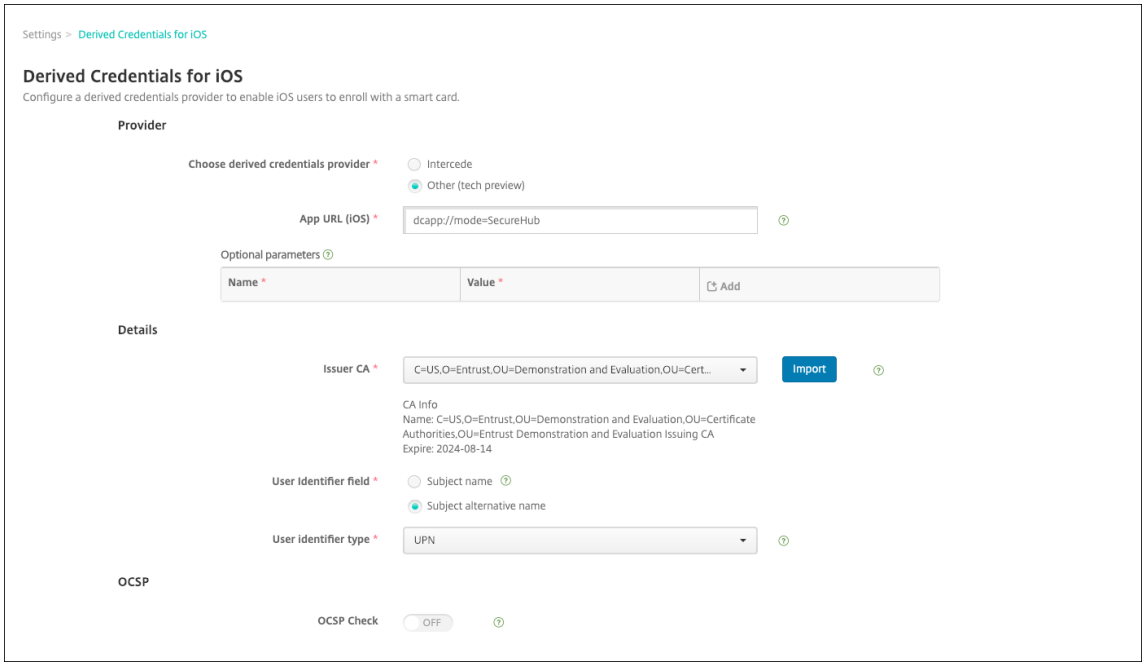


Configurar credenciales derivadas

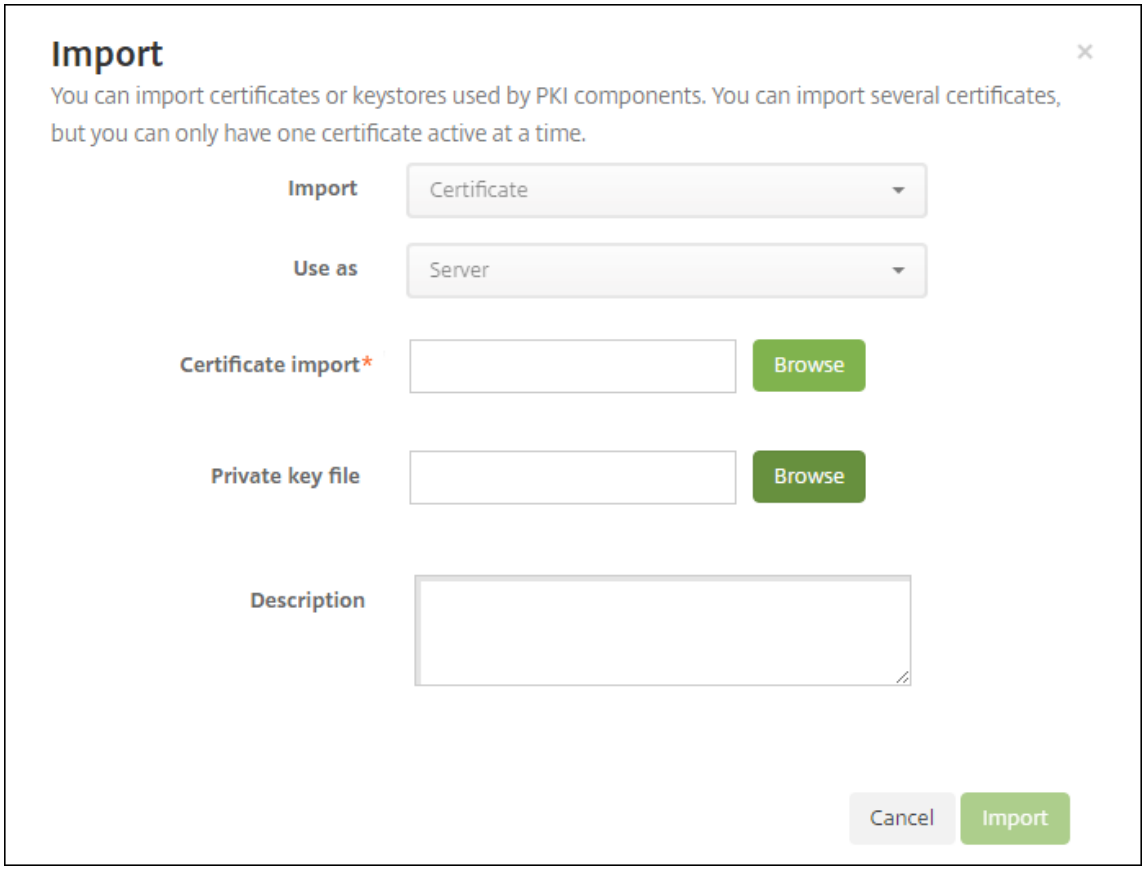
Se presupone que dispone de una configuración en funcionamiento para el proveedor de credenciales derivadas que quiere integrar en XenMobile. Puede configurar XenMobile para comunicarse con dicho servidor. También puede elegir un certificado de CA de credenciales derivadas ya agregado a XenMobile o importar el certificado.

Puede activar el soporte a Online Certificate Status Protocol (OCSP) para ese certificado de CA. Para obtener más información acerca de OCSP, consulte “Entidades de certificación discrecionales” en Entidades PKI.

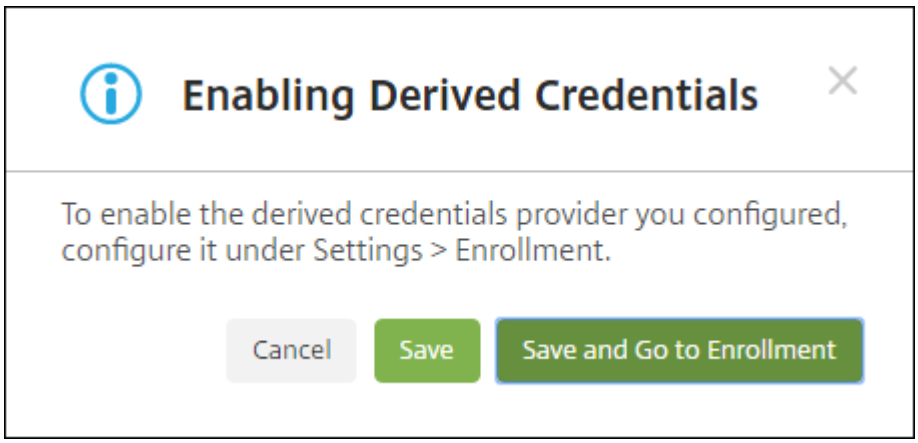
1. En la consola de XenMobile, vaya a **Parámetros > Credenciales derivadas para iOS**.
2. En **Elegir proveedor de credenciales derivadas**, elija **Otro** para Entrust Datacard. Escriba `dcapp://mode=SecureHub` en la **URL de la aplicación (iOS)**.



3. **Parámetros opcionales:** Es posible que algunos proveedores de credenciales derivadas requieran que les suministre los parámetros necesarios para la conexión. Por ejemplo, un proveedor puede requerir que especifique las direcciones URL de un servidor back-end. Haga clic en **Agregar** para proporcionar los parámetros.
4. Especificar un certificado para las credenciales derivadas: Si el certificado ya está cargado en XenMobile, seleccione ese certificado desde **CA emisora**. De lo contrario, haga clic en **Importar** para agregar un certificado. Aparecerá el cuadro de diálogo **Importar certificado**.
5. En el cuadro de diálogo **Importar certificado**, haga clic en **Examinar** para ir al certificado. A continuación, haga clic en **Examinar** para ir al archivo de clave privada.

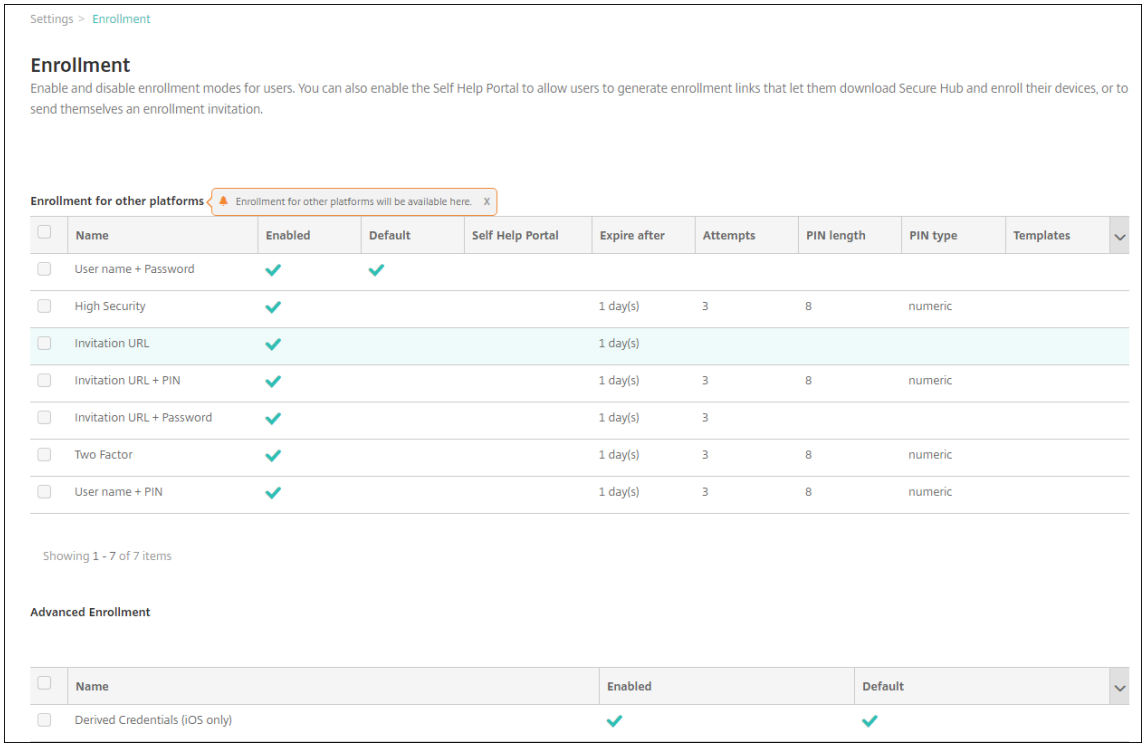


6. Configure los parámetros.
   - Para la aplicación Citrix Derived Credential Manager, el **Campo de identificador de usuario** es el **nombre alternativo del sujeto** y el **Tipo de identificador del usuario** es **userPrincipalName**.
   - Contacte con otros proveedores de credenciales derivadas para obtener la información correspondiente.
7. Puede usar un respondedor OCSP para comprobar la revocación de certificados. Citrix recomienda utilizar un respondedor OCSP por motivos de seguridad. De forma predeterminada, la comprobación de OCSP está **desactivada**.
   - Si activa la compatibilidad con OCSP para el certificado de CA, elija una opción en **Usar URL de OCSP personalizada**. De forma predeterminada, XenMobile extrae la URL de OCSP del certificado (la opción **Usar definición de certificado para la revocación**). Para especificar una dirección URL de respondedor, haga clic en **Usar personalizado** y escriba la URL.
   - **CA de respondedor:** En **CA de respondedor**, elija un certificado. O bien, haga clic en **Importar** y, a continuación, use el cuadro de diálogo **Importar certificado** para buscar el certificado.
8. Haga clic en **Guardar**. Aparecerá el cuadro de diálogo **Habilitación de credenciales derivadas**.

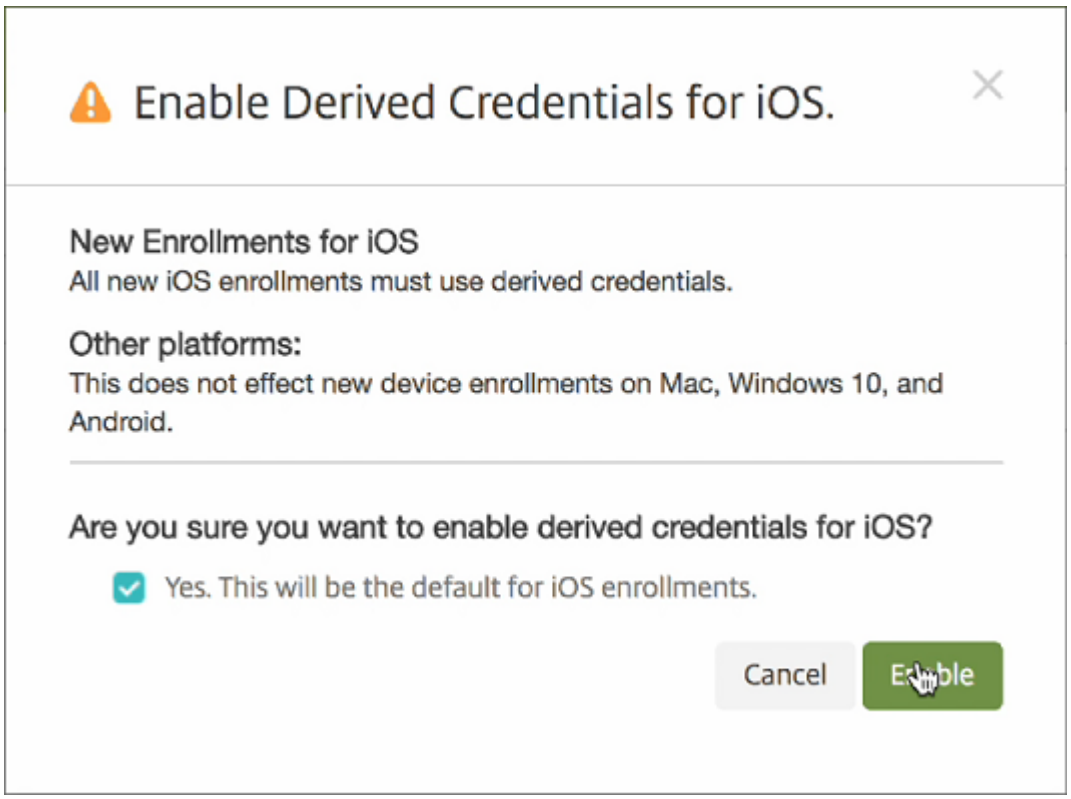


- Para habilitar la configuración de las credenciales derivadas, haga clic en **Guardar**. Para utilizar credenciales derivadas, también debe configurar los parámetros de inscripción.
- Para habilitar la configuración de las credenciales derivadas e ir inmediatamente a **Parámetros > Inscripción**, haga clic en **Guardar e ir a Inscripción**.

9. Si quiere habilitar las credenciales derivadas para la inscripción: En la página **Parámetros > Inscripción** en **Inscripción avanzada**, marque **Credenciales derivadas (solo iOS)** y, a continuación, haga clic en **Habilitar**.



10. Aparecerá un cuadro de diálogo de confirmación. Para habilitar las credenciales derivadas, marque la casilla y haga clic en **Habilitar**.



11. Si quiere modificar las opciones de las credenciales derivadas para la inscripción: En la página **Parámetros > Inscripción**, marque **Credenciales derivadas (solo iOS)** y, a continuación, haga clic en **Modificar**.

Después de habilitar las credenciales derivadas: En el informe **Inscripción de dispositivos**, la columna **Modo de inscripción** muestra **derived_credentials**.

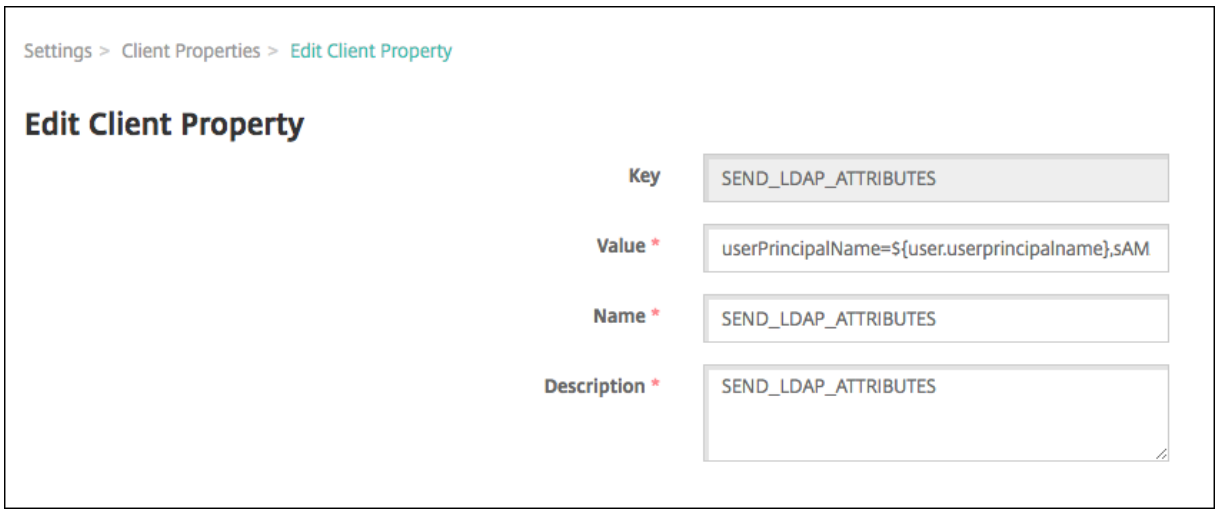
> **Importante:**
>
> Después de agregar el proveedor de credenciales derivadas, reinicie XenMobile Server.

Configurar XenMobile Server para Secure Mail

Para que Secure Mail admita credenciales derivadas, agregue la propiedad de cliente `SEND_LDAP_ATTRIBUTES`. Para obtener información sobre cómo agregar una propiedad de cliente, consulte Propiedades de cliente.

Utilice la siguiente información para la propiedad de cliente:

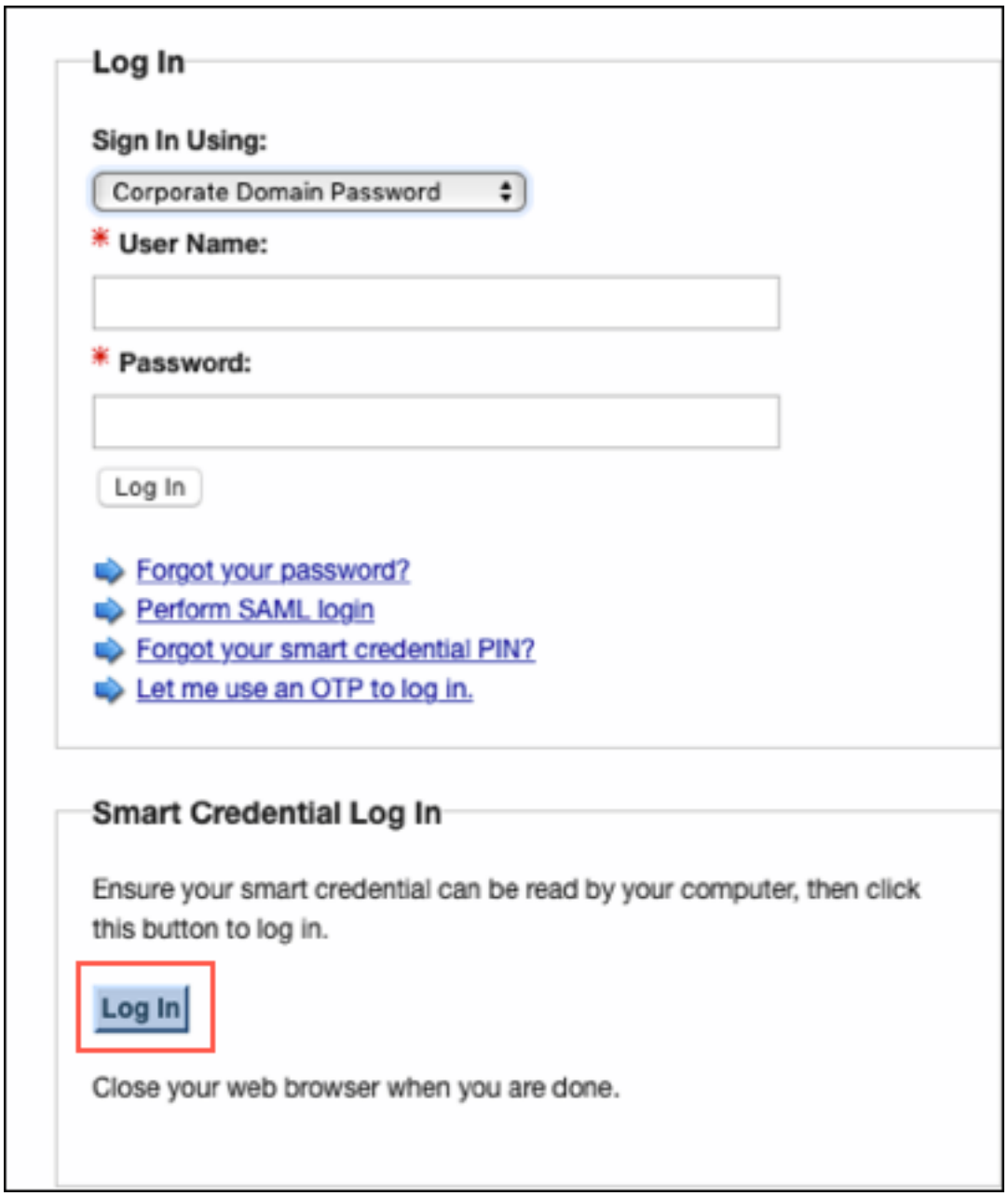
- **Clave:** `SEND_LDAP_ATTRIBUTES`
- **Valor:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`



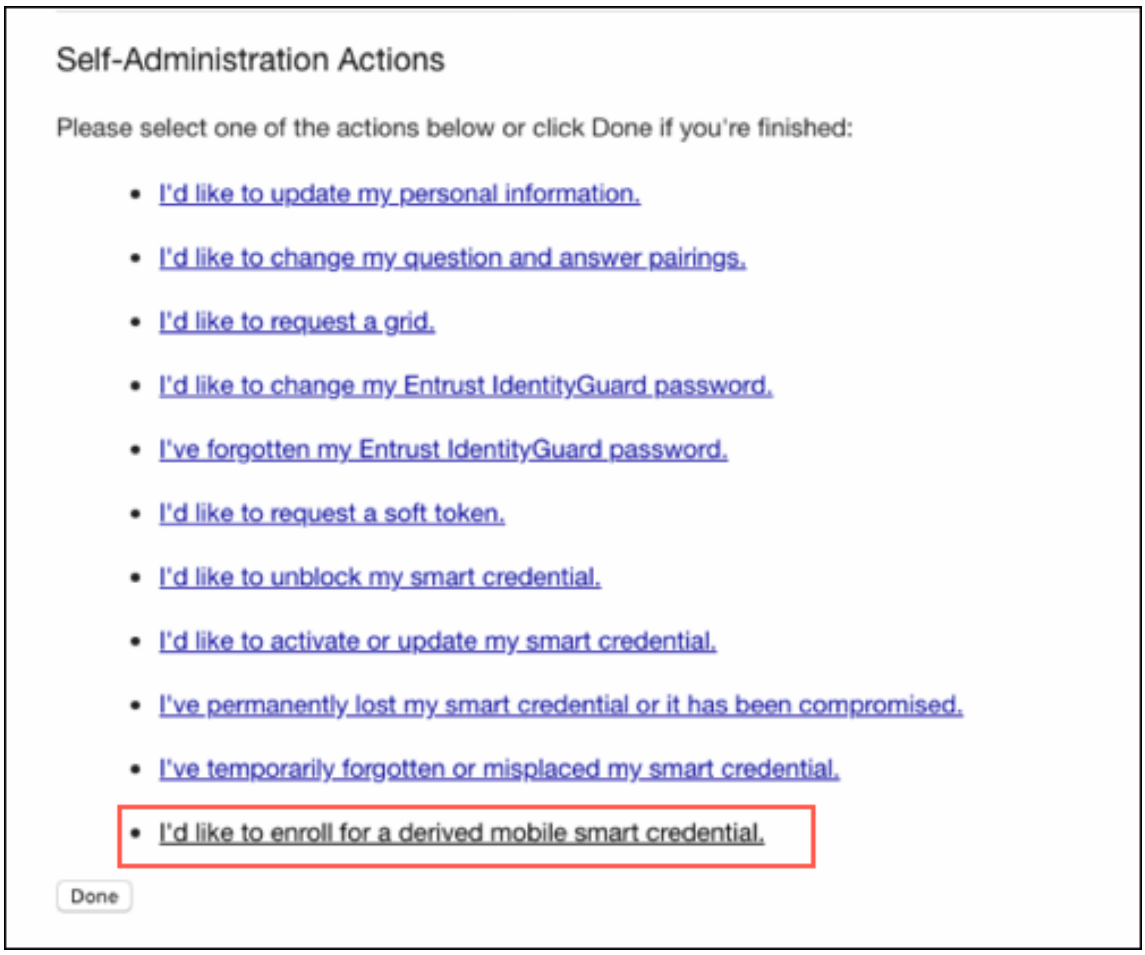
Activar credenciales derivadas de Entrust Datacard en dispositivos iOS

> **Nota:**
>
> Al utilizar el sitio web de Entrust, borre la caché del explorador web al cambiar la tarjeta PIV.

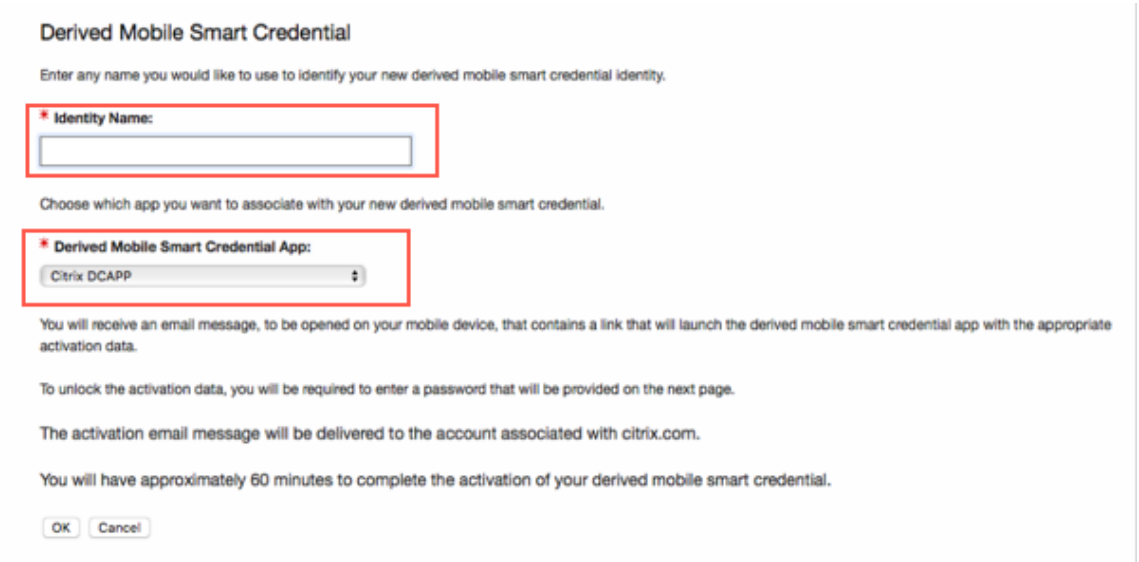
1. Para solicitar nuevas credenciales inteligentes, utilice un escritorio o cualquier dispositivo para iniciar sesión en el sitio web de Entrust. Inicie sesión con el botón **Smart Credential Log In** en la parte inferior de la página. Los usuarios deben insertar su tarjeta inteligente en un lector conectado al escritorio.



2. En **Self-Administration Actions**, marque **I'd like to enroll for a derived mobile smart credential** y haga clic en **Done**.



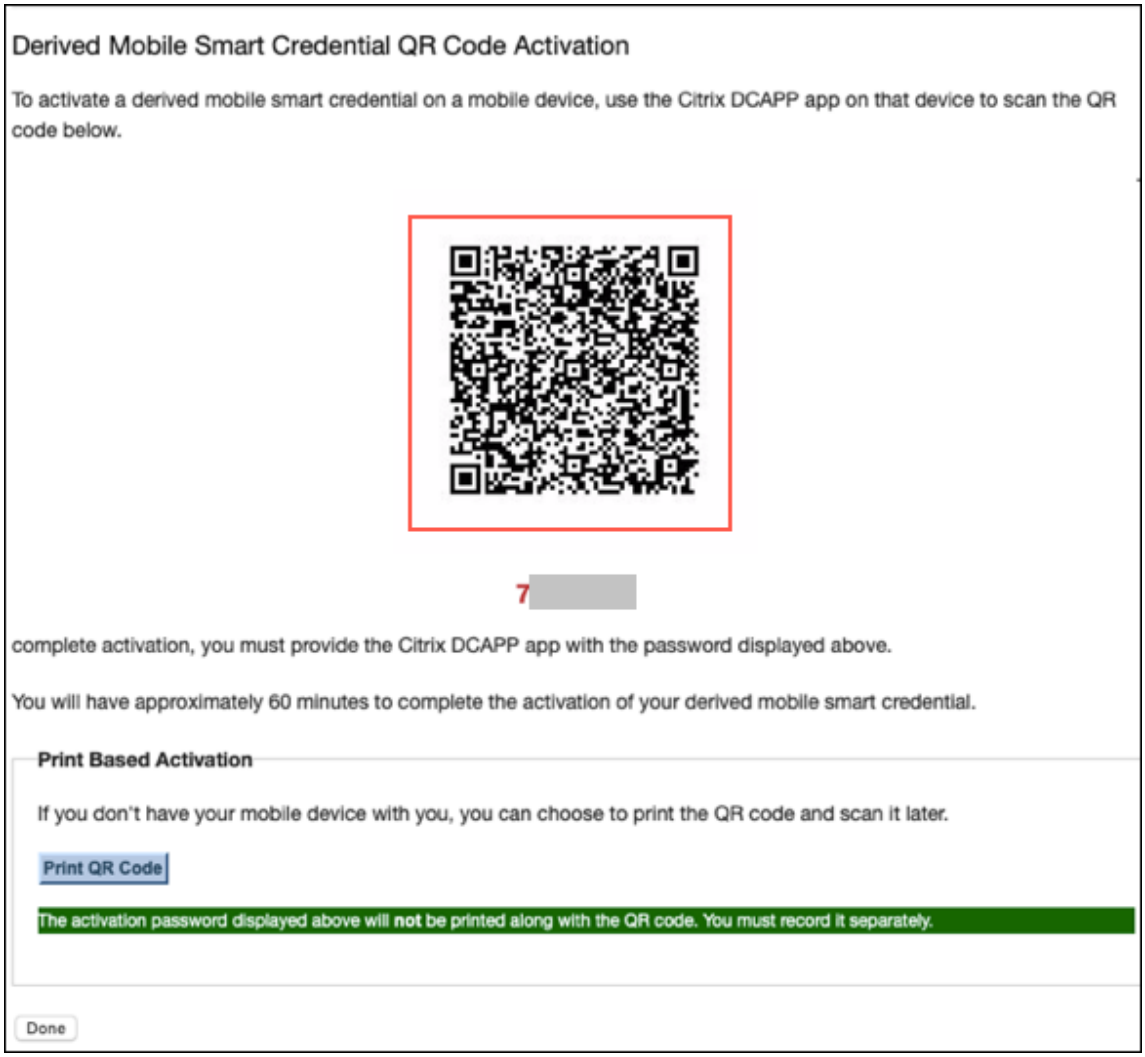
3. En la pantalla **Derived Mobile Smart Credential**, escriba el nombre en **Identity Name**. El usuario puede elegir un nombre único, como un nombre de usuario o un ID numérico.
4. Seleccione la opción **Citrix DCAPP** en el menú de la aplicación de credenciales derivadas y haga clic en **OK**.



Aparece una pantalla de activación por código QR y se solicita al usuario que escanee el código con su dispositivo móvil.

> **Nota:**
>
> De forma predeterminada, el código QR de las credenciales derivadas caduca en 3 minutos.

5. Escanee el código QR mediante la aplicación **Derived Credential Manager** presente en el dispositivo para completar la activación.

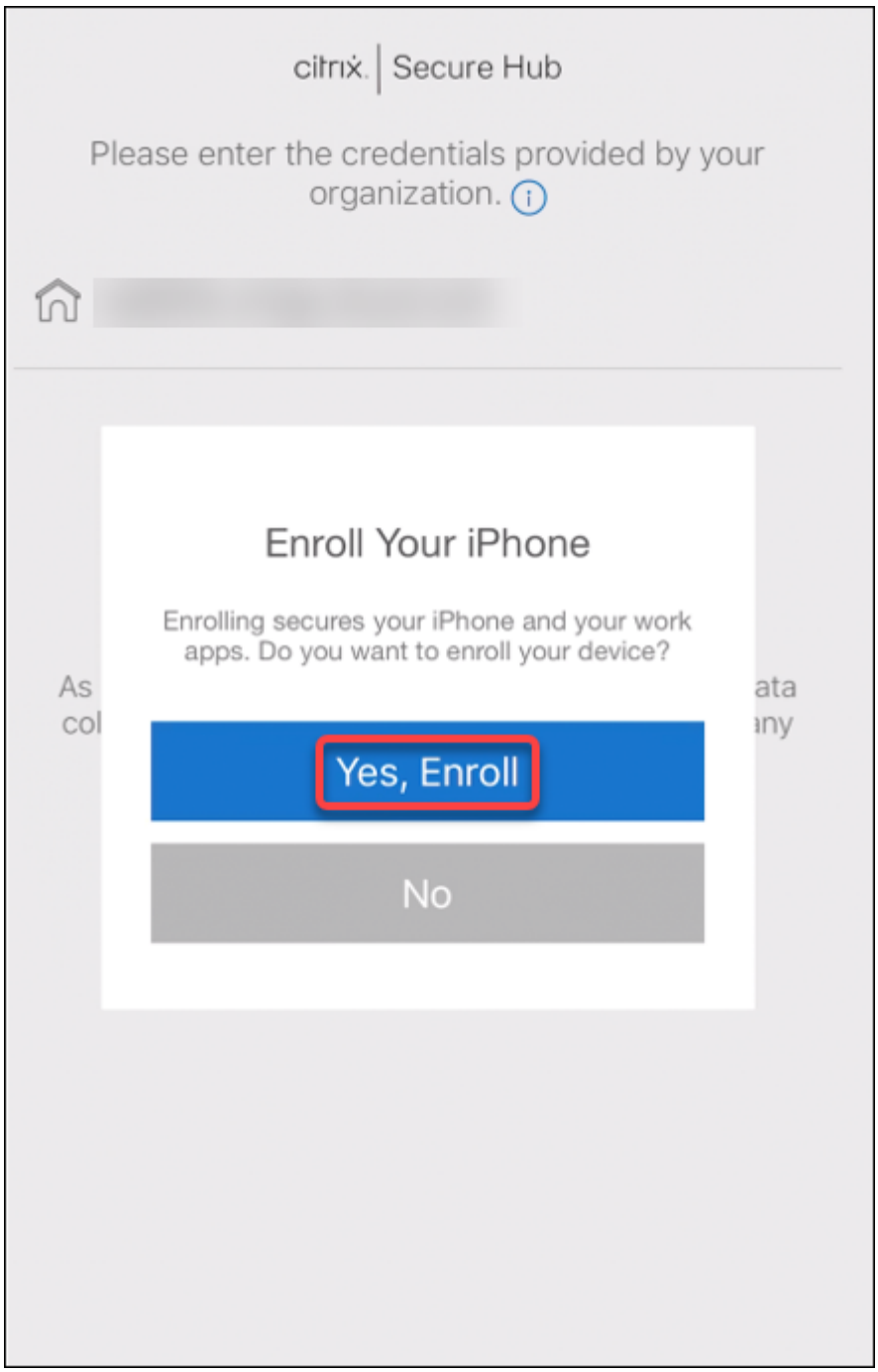


Inscripción de dispositivos

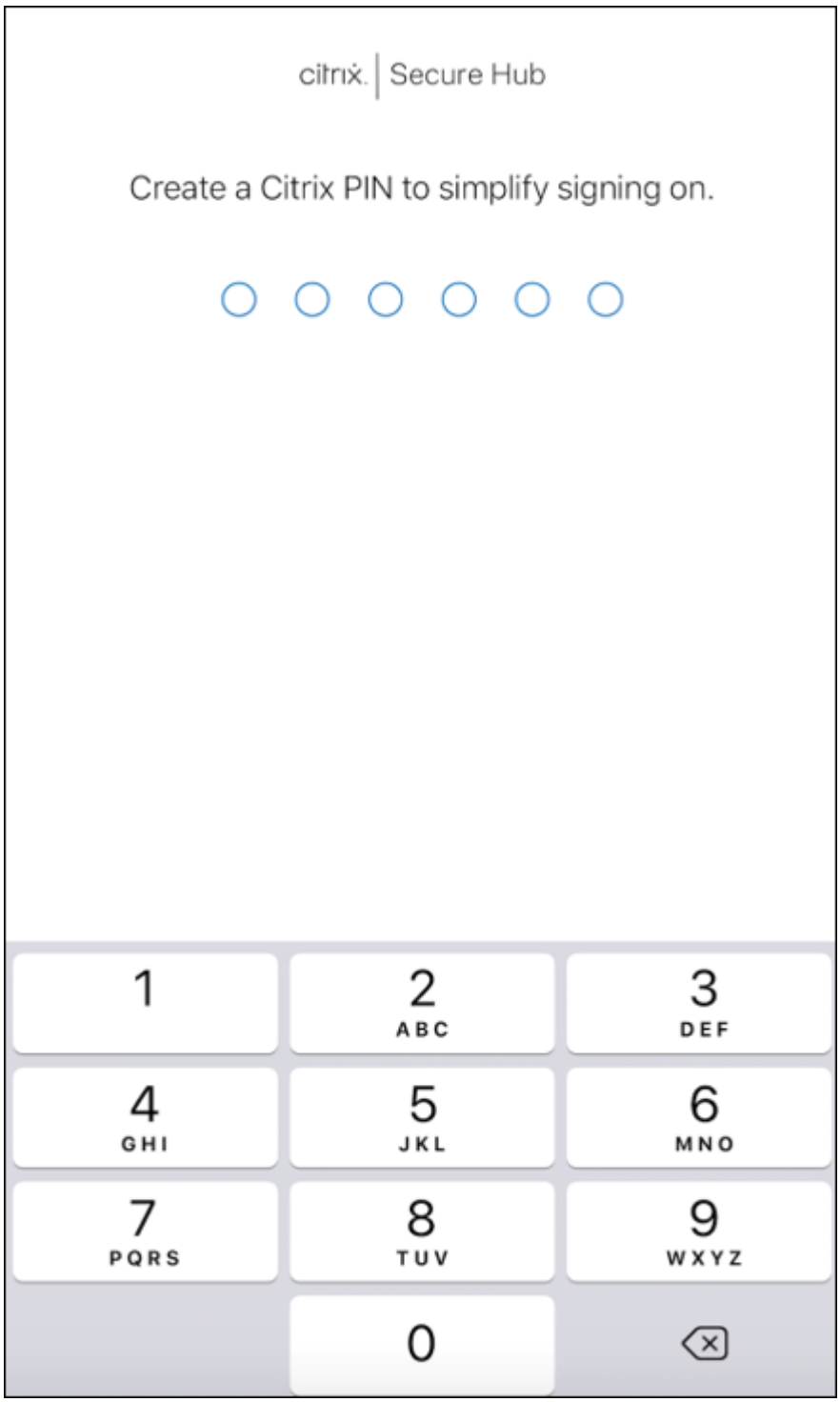
Después de completar la configuración descrita anteriormente en este artículo, los usuarios pueden inscribir los dispositivos mediante credenciales derivadas.

> **Nota:**
>
> En las capturas de pantalla de esta sección, se utiliza Entrust Datacard como ejemplo.

1. Toque **Secure Hub** para abrirlo. Cuando se le solicite, escriba el nombre de dominio completo del servidor de XenMobile Server y, a continuación, haga clic en **Siguiente**.
2. Haga clic en **Sí, inscribirlo**. Comienza la inscripción del dispositivo en Secure Hub.

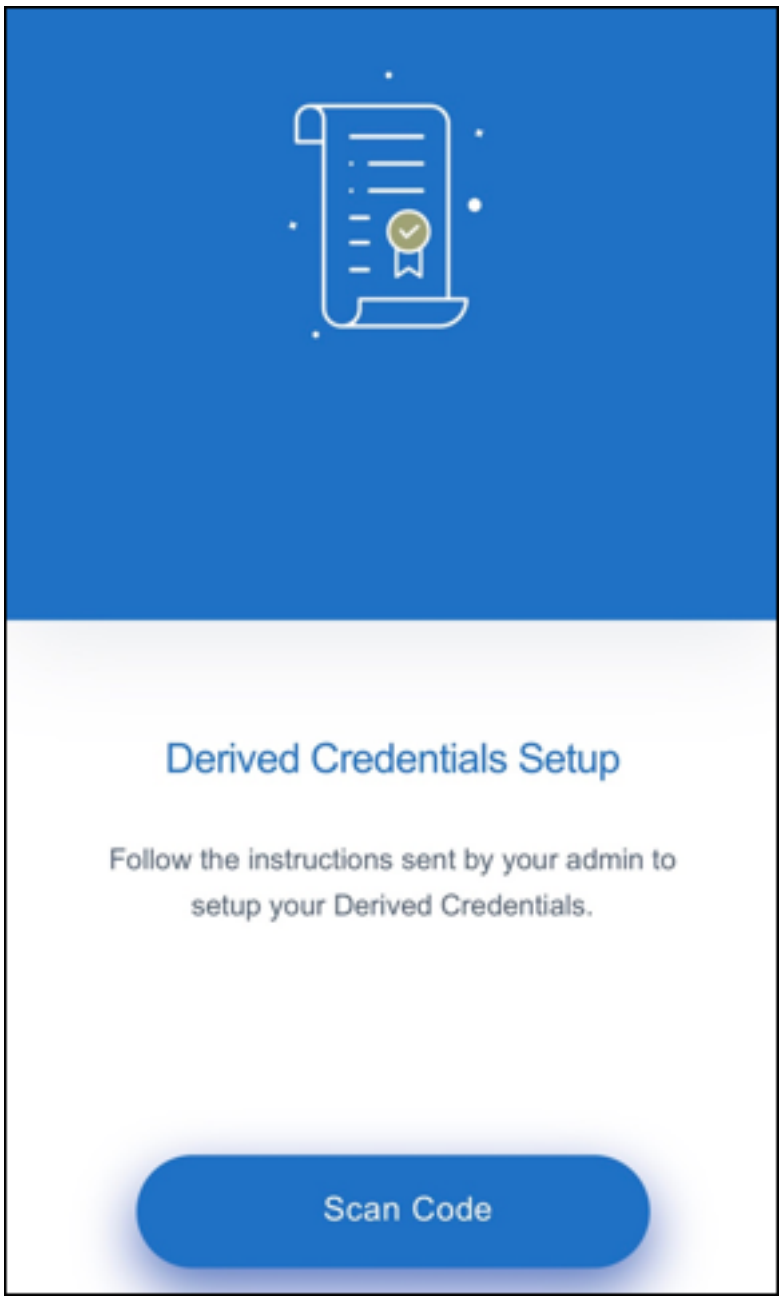


Si XenMobile Server admite credenciales derivadas, Secure Hub pide al usuario que cree un PIN de Citrix y lo confirme.



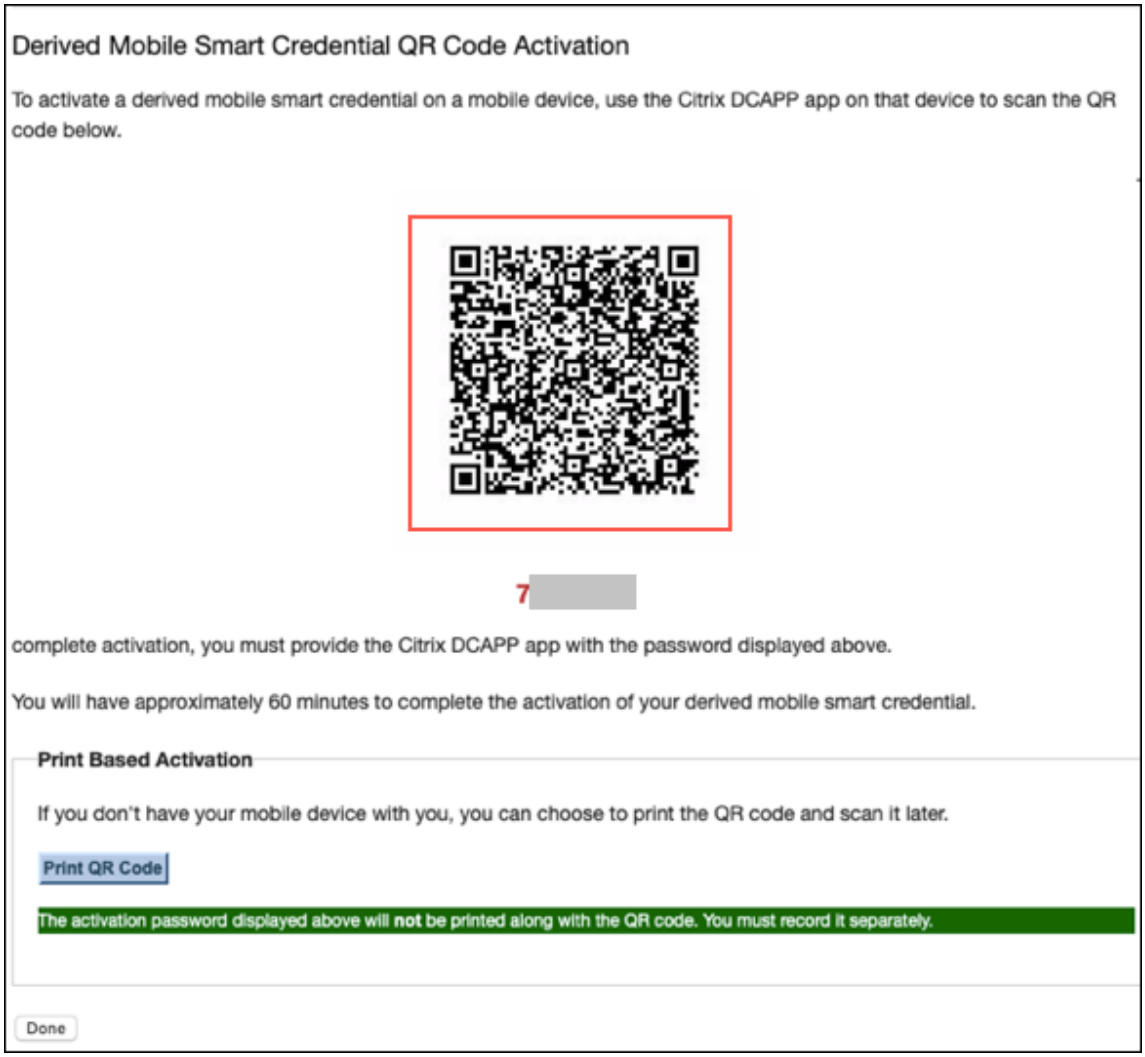
Después de confirmar el PIN de Citrix, aparece la pantalla de bienvenida a la configuración de credenciales derivadas. Siga las instrucciones para activar las credenciales inteligentes.

3. Toque la opción para **escanear el código**. Se activa la cámara del teléfono móvil.

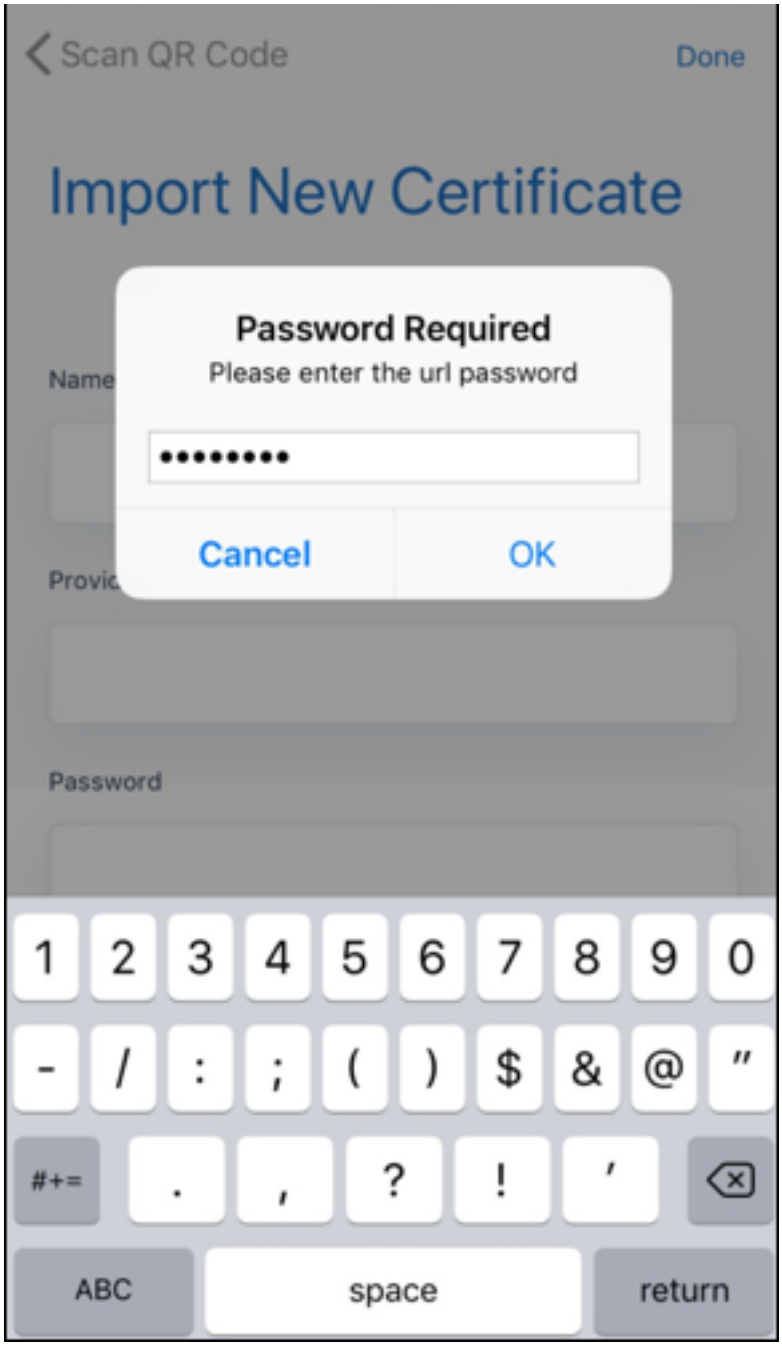


> **Nota:**
>
> Para escanear el código QR, la cámara y el micrófono deben estar habilitados y deben tener los permisos de acceso necesarios.

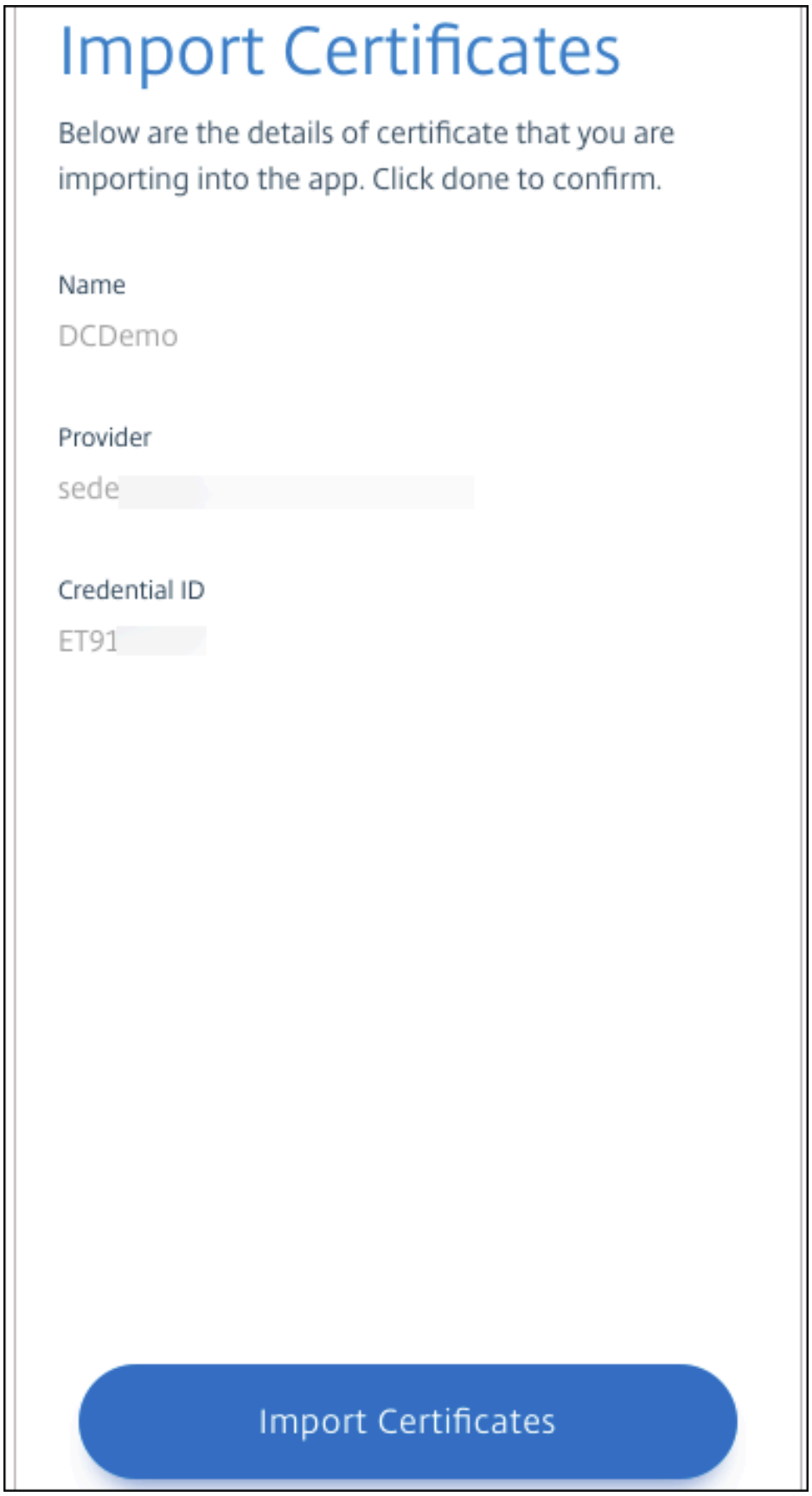
4. En la aplicación de credenciales derivadas, escanee el código QR que se creó en los pasos anteriores.



5. Después de escanear el código QR, aparece un cuadro de diálogo de contraseña en la pantalla **Importar certificado nuevo**. Escriba la contraseña y haga clic en **Aceptar**.



Aparece la pantalla **Importar certificado nuevo** con campos rellenados automáticamente.



6. Después de agregar los certificados, en la pantalla **Credenciales derivadas**, haga clic en la opción para **continuar a Secure Hub**.

7. En Secure Hub, escriba el nuevo PIN cuando se le solicite.

   Después de autenticar el PIN, Secure Hub descarga los certificados. Siga las instrucciones para completar la inscripción.

Para ver información de dispositivos en la consola de XenMobile:

- Vaya a **Administrar** > **Dispositivos** y, a continuación, seleccione un dispositivo para ver un cuadro de comandos. Haga clic en **Mostrar más**.
- Vaya a **Analizar** > **Panel de mandos**.

Actualizar

January 4, 2022

> **Sugerencia: Servicio XenMobile Migration Service**
>
> Si utiliza XenMobile Server local, nuestro servicio XenMobile Migration Service puede ayudarle a comenzar a usar el servicio Endpoint Management. La migración desde XenMobile Server a Citrix Endpoint Management no requiere que vuelva a inscribir los dispositivos.
>
> Para obtener más información, contacte con el representante de ventas, el ingeniero de sistemas o Partner de Citrix local. En estos artículos de blog, se comenta el servicio XenMobile Migration Service:
>
> New XenMobile Migration Service
>
> Making the Case for XenMobile in the Cloud

Antes de actualizar XenMobile a 10.14

1. Actualice Citrix License Server a la versión 11.16 o a una posterior antes de actualizarlo a la versión más reciente de XenMobile Server 10.14.

   La versión más reciente de XenMobile requiere Citrix License Server 11.16 (versión mínima).

   La fecha de Customer Success Services (anteriormente, fecha de Subscription Advantage) en XenMobile 10.14 es el 15 de septiembre de 2021. La fecha de Customer Success Services de su licencia de Citrix debe ser posterior a esta fecha. Puede ver la fecha junto a la licencia en el servidor de licencias. Si conecta la versión más reciente de XenMobile a un entorno de servidor de licencias anterior, la comprobación de conectividad falla y no se puede configurar el servidor de licencias.

   Para renovar la fecha que consta en la licencia, descargue el archivo de licencias más reciente

del Portal de Citrix y cárguelo en el servidor de licencias. Para obtener más información, consulte Customer Success Services.

2. Para un entorno en clúster, las implementaciones de aplicaciones y directivas iOS a dispositivos iOS 11 y posterior presentan el siguiente requisito. Si Citrix Gateway está configurado para la persistencia de SSL, debe abrir el puerto 80 en todos los nodos de XenMobile Server.
3. Si la máquina virtual con XenMobile Server que quiere actualizar tiene menos de 8 GB de RAM, se recomienda aumentarla a, por lo menos, 8 GB.
4. Recomendación: Antes de instalar una actualización de XenMobile, utilice las funcionalidades de la máquina virtual (VM) para tomar una instantánea del sistema. Asimismo, realice una copia de seguridad de la base de datos de configuración del sistema. Si tiene problemas durante la actualización, las copias de seguridad completas le permitirán recuperar los datos.

Para actualizar la versión

Puede actualizar directamente la versión 10.13.x o 10.12.x de XenMobile a 10.14. Para actualizar la versión, descargue el último binario disponible en https://www.citrix.com/downloads. Vaya a **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. En el mosaico del software XenMobile Server para su hipervisor, haga clic en **Download File** (Descargar archivo). Para cargar la actualización de la versión, utilice la página **Administración de versiones** de la consola de XenMobile.

Para actualizar desde la página "Administración de versiones"

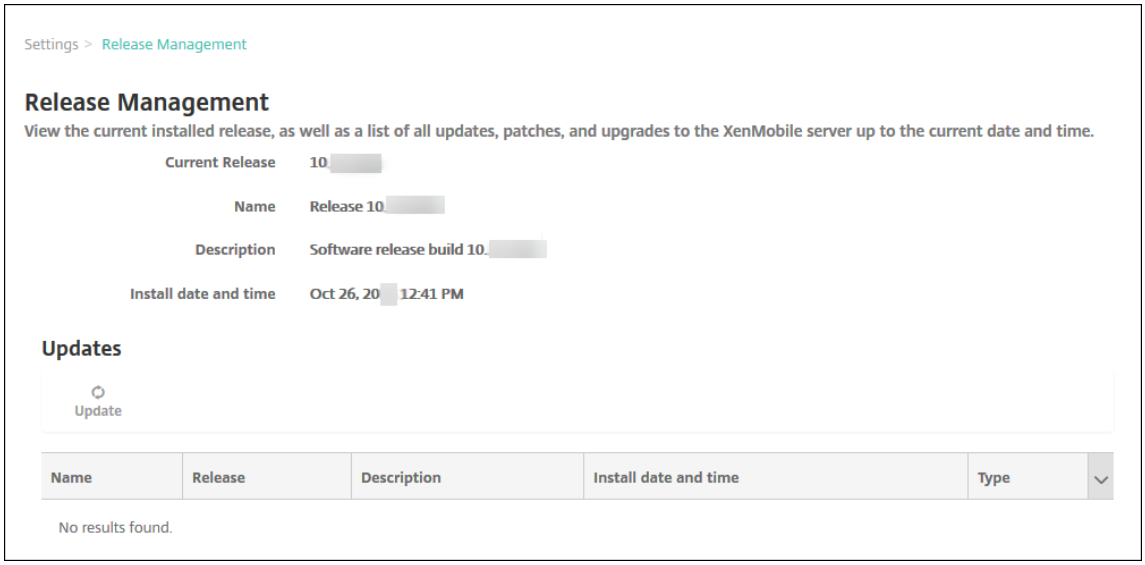
Use la página **Administración de versiones** para actualizar XenMobile Server a la versión más reciente.

Requisitos previos:

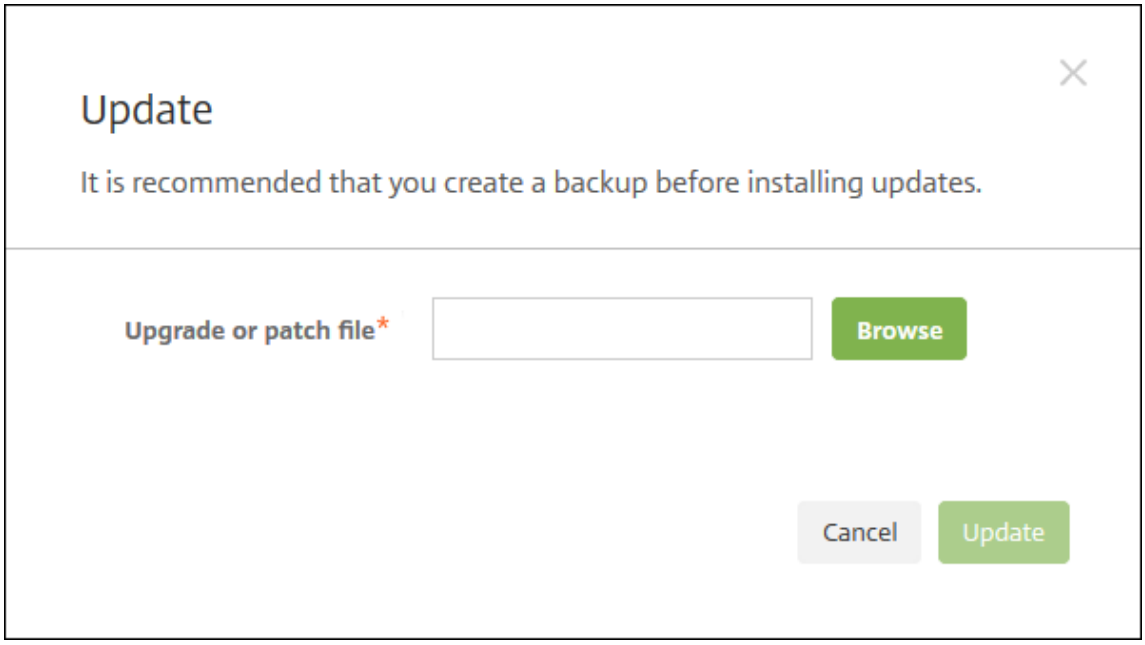
- Consulte los requisitos del sistema.

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

1. Descargue el último binario disponible en https://www.citrix.com/downloads. Vaya a **Citrix Endpoint Management (y Citrix XenMobile Server) > XenMobile Server (local) > Software de producto > XenMobile Server 10**. En el mosaico del software XenMobile Server para su hipervisor, haga clic en **Download File** (Descargar archivo).
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 **Parámetros**.
3. Haga clic en **Administración de versiones**. Aparecerá la página **Administración de versiones**.



4. En **Actualizaciones**, haga clic en **Actualizar**. Aparecerá el cuadro de diálogo **Actualizar**.



5. Seleccione el archivo de actualización de XenMobile que descargó de Citrix.com. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.
6. Haga clic en **Actualizar** y, a continuación, si el sistema se lo solicita, reinicie XenMobile.

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

Después de actualizar la versión

Después de actualizar, XenMobile requiere un reinicio. Utilice la interfaz de línea de comandos de XenMobile para reiniciar el servidor de XenMobile Server. Es importante que borre la caché del explorador web después de reiniciarse el sistema.

Si la funcionalidad relacionada con las conexiones de salida deja de funcionar y no ha cambiado la configuración de las conexiones, busque errores similares a los siguientes en el registro de XenMobile Server: "No se puede conectar con el servidor del programa VPP: El nombre de host '192.0.2.0' no coincide con el sujeto de certificado suministrado por el servidor homólogo".

Si recibe el error de validación de certificado, inhabilite la verificación de nombres de host en el XenMobile Server. De forma predeterminada, la verificación de nombres de host está habilitada en las conexiones salientes, excepto para el servidor PKI de Microsoft. Si la verificación de nombres de host deja inoperativa la implementación, cambie la propiedad de servidor **disable.hostname.verification** a **true**. El valor predeterminado de esta propiedad es **false**.

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

Para actualizar implementaciones de XenMobile en clúster

> **Importante:**
>
> Antes de instalar una actualización de XenMobile, utilice las funcionalidades de la máquina virtual (VM) para tomar una instantánea del sistema. Asimismo, realice una copia de seguridad de la base de datos de configuración del sistema. Si tiene problemas durante la actualización, las copias de seguridad completas le permitirán recuperar los datos.

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 **Parámetros > Administración de versiones**.
2. Apague todos los nodos desde el menú **System** en la interfaz de línea de comandos.
3. Desde el menú **System** en la interfaz de línea de comandos, seleccione un nodo y compruebe que el servicio se está ejecutando.
4. Inicie los demás nodos uno tras otro.

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

Actualizar una versión de XenMobile MDM Edition a Enterprise Edition

Puede actualizar XenMobile MDM Edition a XenMobile Enterprise Edition para dispositivos iOS y Android.

Requisitos previos

- La licencia Enterprise correcta.
- Citrix Gateway configurado.

Para actualizar la versión

1. Vaya a **Parámetros > Licencias** y verifique que se ha cargado el tipo de licencia Enterprise Edition correcto.
2. Vaya a **Parámetros > Propiedades de servidor** y cambie la propiedad **Modo de servidor** del valor **MDM** al valor **ENT**.
3. Vaya a **Parámetros > Citrix Gateway** y configure la información de Citrix Gateway. Establezca el mismo modo de autenticación que tiene para la edición MDM, es decir, la autenticación de dominio (Active Directory). XenMobile no admite cambiar el modo de autenticación después de haber inscrito a los usuarios.
4. Optativo: Vaya a **Parámetros > Propiedades de cliente** y habilite la autenticación con PIN de Citrix.

Después de completar estos pasos, los usuarios deben realizar los siguientes pasos para cambiar un dispositivo al modo Enterprise.

Usuarios de iOS

1. Cierre Secure Hub: Toque dos veces (rápidamente) en el botón de inicio del dispositivo y deslice hacia arriba la aplicación Secure Hub.
2. Abra Secure Hub.

Usuarios de Android

1. Abra Secure Hub.
2. Vaya a **Preferencias > Información del dispositivo**.
3. Haga clic en **Actualizar directiva**.

Si ha habilitado la autenticación con PIN de Citrix, Secure Hub pide a los usuarios que creen un PIN. Después de que el usuario crea un PIN, XenMobile configura el dispositivo en modo Enterprise. Después, en la consola de XenMobile, la página **Administrar > Dispositivos** muestra que tanto MDM como MAM están activos para el dispositivo.

Inscripción, roles y cuentas de usuario

January 4, 2022

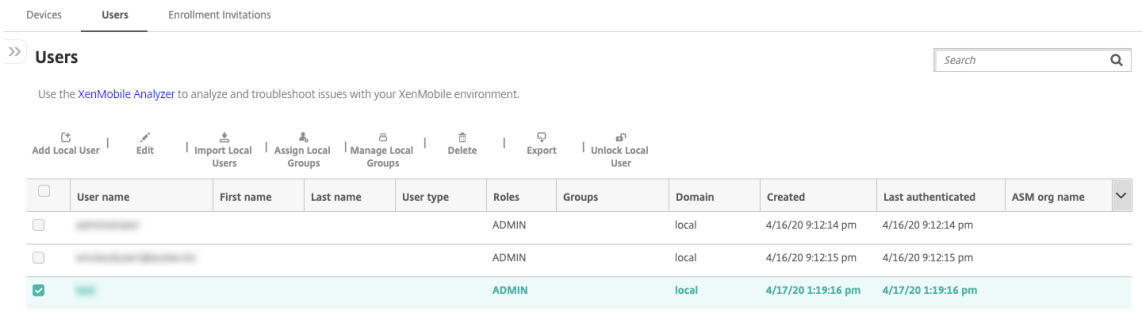
Puede configurar cuentas de usuario, roles e inscripciones en la consola de XenMobile desde la ficha **Administrar** y la página **Parámetros**: A menos que se indique lo contrario, los pasos para las siguientes tareas se proporcionan en este artículo.

- Cuentas de usuario y grupos:
  - En **Administrar > Usuarios**, puede agregar cuentas de usuario manualmente, o puede usar un archivo .csv de aprovisionamiento para importar cuentas y administrar grupos locales.
  - En **Parámetros > Flujos de trabajo**, puede utilizar flujos de trabajo para administrar la creación y la eliminación de cuentas de usuario.
- Roles para cuentas de usuario y grupos
  - En **Parámetros > Control de acceso por roles** puede 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 información, consulte Configurar roles con RBAC.
  - En **Parámetros > Plantillas de notificaciones** 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. Para obtener más información, consulte Crear y actualizar plantillas de notificaciones.
- Invitaciones y modo de seguridad de inscripción
  - Haga clic en **Parámetros > Inscripción** para configurar hasta siete modos de seguridad de inscripción y enviar invitaciones de inscripción. Cada modo de seguridad de inscripción tiene su propio nivel de seguridad y una serie de pasos que los usuarios deberán seguir para inscribir sus dispositivos.
  - Habilitar la detección automática en XenMobile para la inscripción de usuarios

Agregar, modificar, desbloquear o eliminar cuentas de usuarios locales

Puede agregar cuentas de usuario local a XenMobile de forma manual, o bien puede usar un archivo de aprovisionamiento para importar las cuentas. Para conocer los pasos para importar cuentas de usuario desde un archivo de aprovisionamiento, consulte Importar cuentas de usuario.

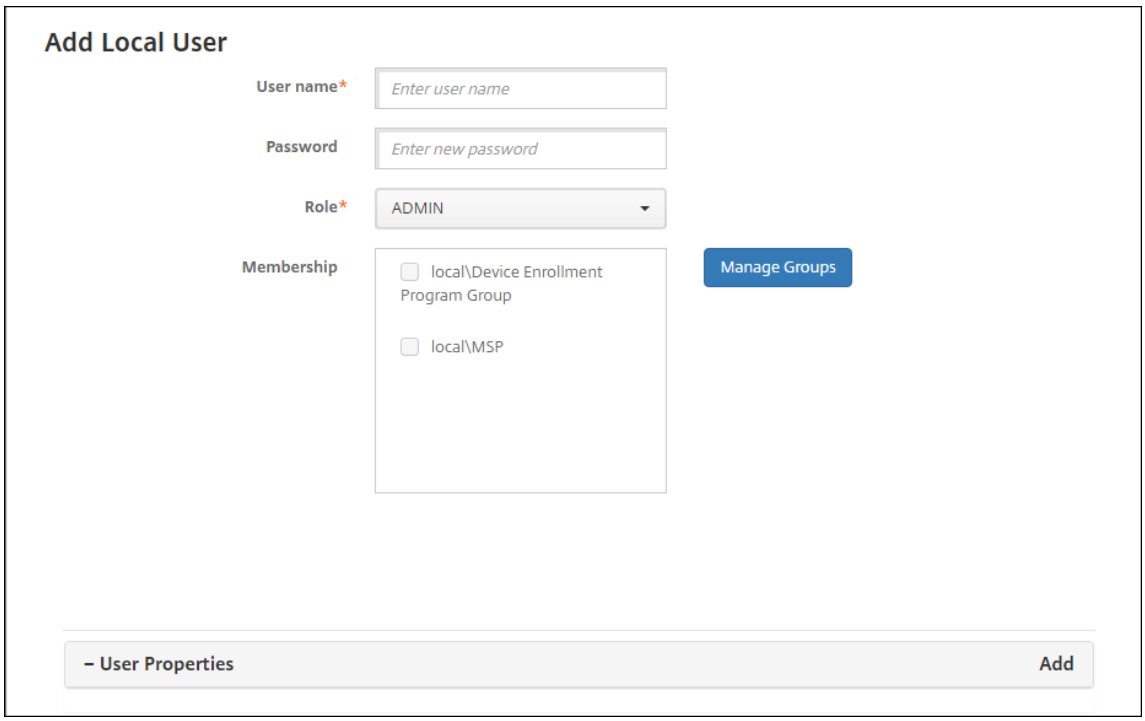
1. En la consola de XenMobile, haga clic en **Administrar > Usuarios**. Aparecerá la página **Usuarios**.



2. Haga clic en **Mostrar filtro** para filtrar la lista.

Para agregar una cuenta de usuario local

1. En la página **Usuarios**, haga clic en **Agregar usuario local**. Aparecerá la página **Agregar usuario local**.



2. Configure estos parámetros:

   - **Nombre de usuario:** Este es un campo obligatorio. Escriba el nombre. Puede incluir espacios en los nombres, además de letras mayúsculas y minúsculas.
   - **Contraseña:** Escriba una contraseña opcional de usuario. La contraseña debe tener al menos 14 caracteres y debe satisfacer todos los criterios siguientes:
     - Incluir al menos dos números
     - Incluir al menos una letra mayúscula y una minúscula
     - Incluir al menos un carácter especial

  - No incluir palabras de diccionario ni palabras restringidas, como el nombre de usuario de Citrix o la dirección de correo electrónico
  - No incluir más de tres caracteres o patrones de teclado secuenciales y repetidos, como 1111, 1234 o asdf
- **Rol:** En la lista, haga clic en el rol del usuario. Para obtener información sobre roles, consulte Configurar roles con RBAC. Las opciones posibles son:
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- **Pertenencia a grupos:** En la lista, haga clic en el grupo o en los grupos a los que agregar el usuario.
- **Propiedades de usuario:** Agregue propiedades de usuario opcionales. Para cada propiedad de usuario que quiera agregar, haga clic en **Agregar** y haga lo siguiente:
  - **Propiedades de usuario:** 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 **Listo** para guardar la propiedad de usuario o haga clic en **Cancelar**.

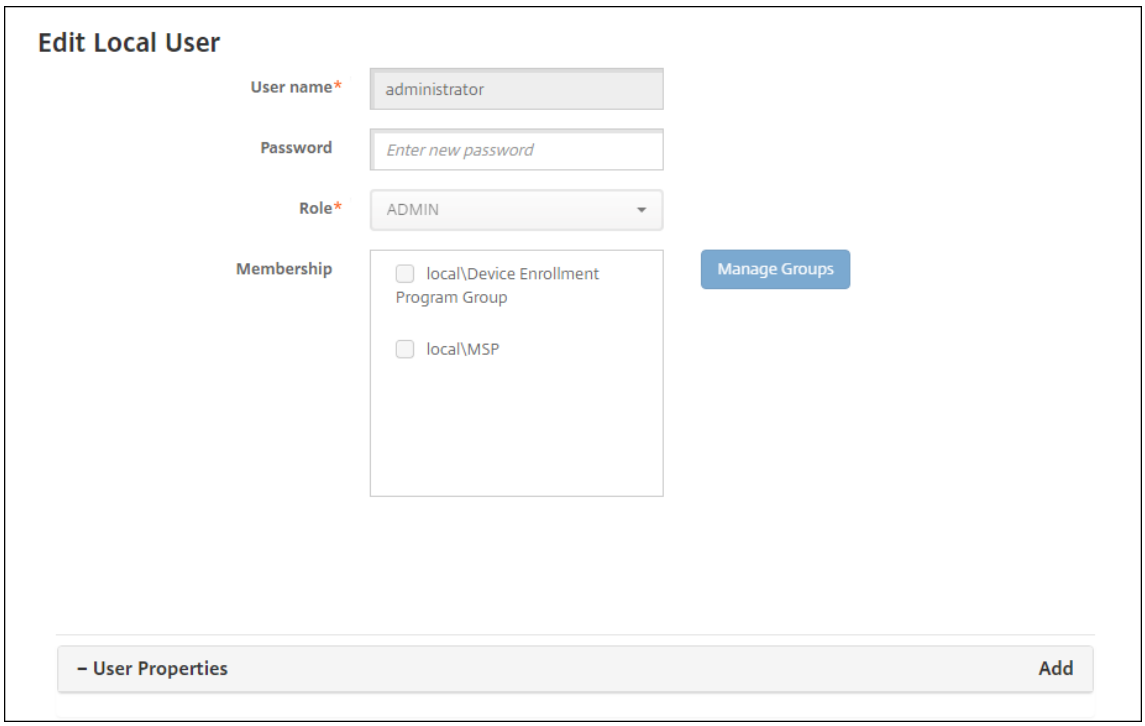
Para eliminar una propiedad de usuario, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en la X situada a la derecha. La propiedad se elimina inmediatamente.

Para modificar una propiedad de usuario, haga clic en la propiedad y realice los cambios. Haga clic en **Listo** para guardar los cambios del elemento o haga clic en **Cancelar** para no guardarlos.

3. Haga clic en **Guardar**.

Para modificar una cuenta de usuario local

1. En la página **Usuarios**, en la lista de usuarios, haga clic para seleccionar un usuario y, a continuación, haga clic en **Modificar**. Aparecerá la página **Modificar usuario local**.



2. Cambie la siguiente información como corresponda:
   - **Nombre de usuario:** No puede cambiar el nombre de usuario.
   - **Contraseña:** Cambie o agregue una contraseña de usuario.
   - **Rol:** En la lista, haga clic en el rol del usuario.
   - **Pertenencia a grupos:** 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, quite la marca de la casilla situada junto al nombre del grupo.
   - **Propiedades de usuario:** Realice una de las siguientes acciones:
     - Para cambiar cada propiedad de usuario, haga clic en ella y realice los cambios. Haga clic en **Listo** para guardar los cambios del elemento o haga clic en **Cancelar** para no guardarlos.
     - Para cada propiedad de usuario que quiera agregar, haga clic en **Agregar** y haga lo siguiente:
       * **Propiedades de usuario:** 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 **Listo** para guardar la propiedad de usuario o haga clic en **Cancelar**.
     - Para cada propiedad de usuario que quiera eliminar, 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 **Guardar** para guardar los cambios o en **Cancelar** para no guardarlos.

Para desbloquear una cuenta de usuario local

1. En la página **Usuarios**, en la lista de cuentas de usuario, seleccione una cuenta.
2. Haga clic en **Desbloquear usuario local**. Aparecerá un cuadro de diálogo de confirmación.
3. Haga clic en **Desbloquear** para desbloquear la cuenta de usuario o haga clic en **Cancelar** para no hacer ningún cambio.

Para eliminar una cuenta de usuario local

1. En la página **Usuarios**, en la lista de cuentas de usuario, seleccione una cuenta.

Puede seleccionar varias cuentas de usuario para eliminarlas. Para ello, marque la casilla situada junto a cada cuenta de usuario que quiera seleccionar.

1. Haga clic en **Delete**. Aparecerá un cuadro de diálogo de confirmación.
2. Haga clic en **Eliminar** para eliminar la cuenta de usuario o en **Cancelar** para no eliminarla.

Para eliminar usuarios de Active Directory

Para eliminar uno o varios usuarios de Active Directory a la vez, selecciónelos y haga clic en **Eliminar**.

Si un usuario eliminado tiene dispositivos inscritos y usted quiere reinscribirlos, elimine los dispositivos antes de reinscribirlos. Para eliminar un dispositivo, vaya a **Administrar > Dispositivos**, seleccione el dispositivo y, a continuación, haga clic en **Eliminar**.

Importar cuentas de usuario

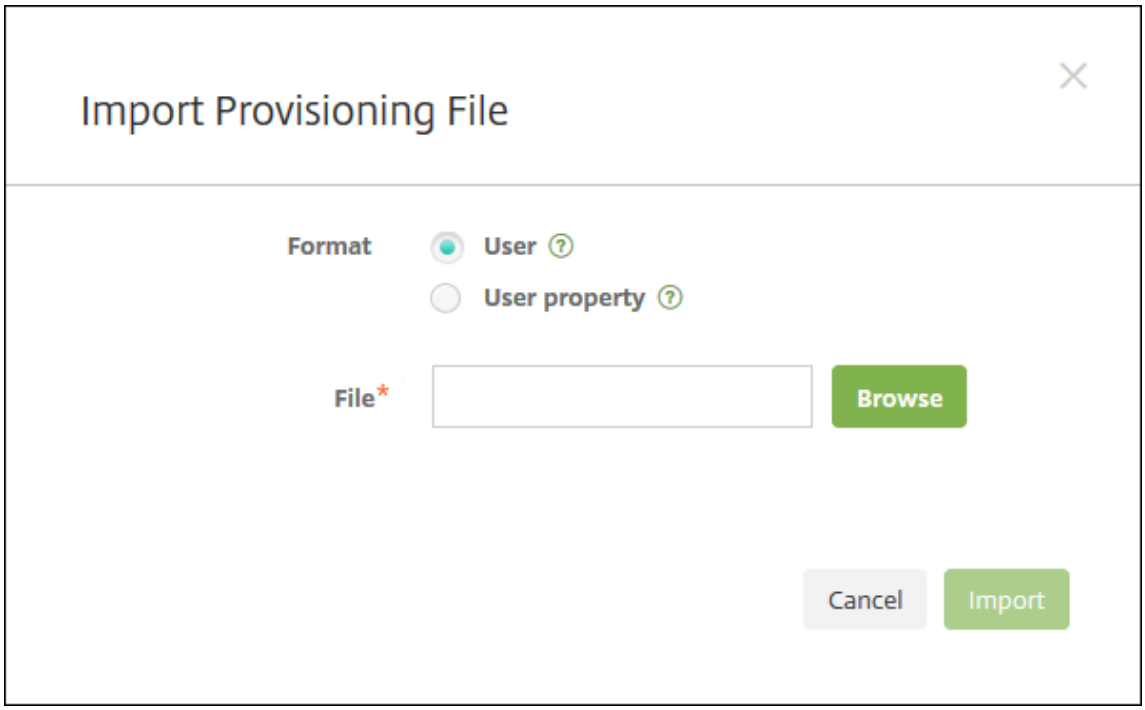
Puede importar propiedades y cuentas de usuarios locales desde un archivo de formato CSV llamado "archivo de aprovisionamiento", el cual puede crear manualmente. Para obtener información acerca de los formatos de los archivos de aprovisionamiento, consulte Formatos de archivo de aprovisionamiento.

> **Nota:**
>
> - Para usuarios locales, use el nombre de dominio junto con el nombre de usuario en el archivo de importación. Por ejemplo, especifique nombre-de-usuario@dominio. Si el usuario local que crea o importa es para un dominio administrado en XenMobile, el usuario no puede inscribirse mediante las credenciales LDAP correspondientes.
> - Si importa cuentas de usuario al directorio interno de usuarios de XenMobile, inhabilite el dominio predeterminado para acelerar el proceso de importación. Tenga en cuenta que inhabilitar el dominio afecta a las inscripciones, por lo que debe volver a habilitar el dominio predeterminado una vez completada la importación de los usuarios internos.

> - Los usuarios locales pueden tener el formato de Nombre principal del usuario (UPN). Sin embargo, Citrix recomienda no usar el dominio administrado. 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 **Administrar > Usuarios**. Aparecerá la página **Usuarios**.
2. Haga clic en **Importar usuarios locales**. Aparece el cuadro de diálogo **Importar archivo de aprovisionamiento**.



3. Seleccione **Usuario** o **Propiedad** para el formato del archivo de aprovisionamiento que va a importar.
4. Para seleccionar el archivo de aprovisionamiento que quiere usar, haga clic en **Examinar** y vaya a la ubicación de ese archivo.
5. Haga clic en **Importar**.

Formatos de archivo de aprovisionamiento

Puede crear un archivo de aprovisionamiento para importar cuentas de usuario y propiedades en XenMobile. Los formatos válidos son los siguientes:

- **Campos del archivo de aprovisionamiento de usuarios:** `user;password;role;group1;group2`

- **Campos del archivo de aprovisionamiento de atributos de usuario:** `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

> **Nota:**
>
> - 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, la propiedad `propertyV;test;1;2` debe escribirse como `propertyV\\;test\\;1\\;2` en el archivo de aprovisionamiento.
> - Los valores válidos de **Rol** son los roles predefinidos USER, ADMIN, SUPPORT y DEVICE_PROVISIONING, además de cualquier rol adicional que haya definido.
> - Use el carácter de punto (.) como separador para crear una jerarquía de grupo. No use un punto en los nombres de grupo.
> - En los archivos de aprovisionamiento de atributos, use minúsculas para los atributos de las propiedades. 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`

Como 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

La entrada `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` significa:

- **Usuario:** `user01`
- **Propiedad 1**
  - **nombre:** `propertyN`
  - **valor:** `propertyV;test;1;2`

- **Propiedad 2:**
  - **nombre:** `prop 2`
  - **valor:** `prop2 value`

Configurar modos de seguridad de inscripción

Los modos de seguridad de inscripción de dispositivos se configuran para especificar un nivel de seguridad y una plantilla de notificación para la inscripción de los dispositivos en XenMobile.

XenMobile ofrece siete modos de seguridad de inscripción, cada uno con su propio nivel de seguridad y unos pasos propios que los usuarios deberán seguir para inscribir sus dispositivos. Los modos de seguridad de inscripción se configuran en la consola de XenMobile Server, desde la página **Parámetros > Inscripción**.

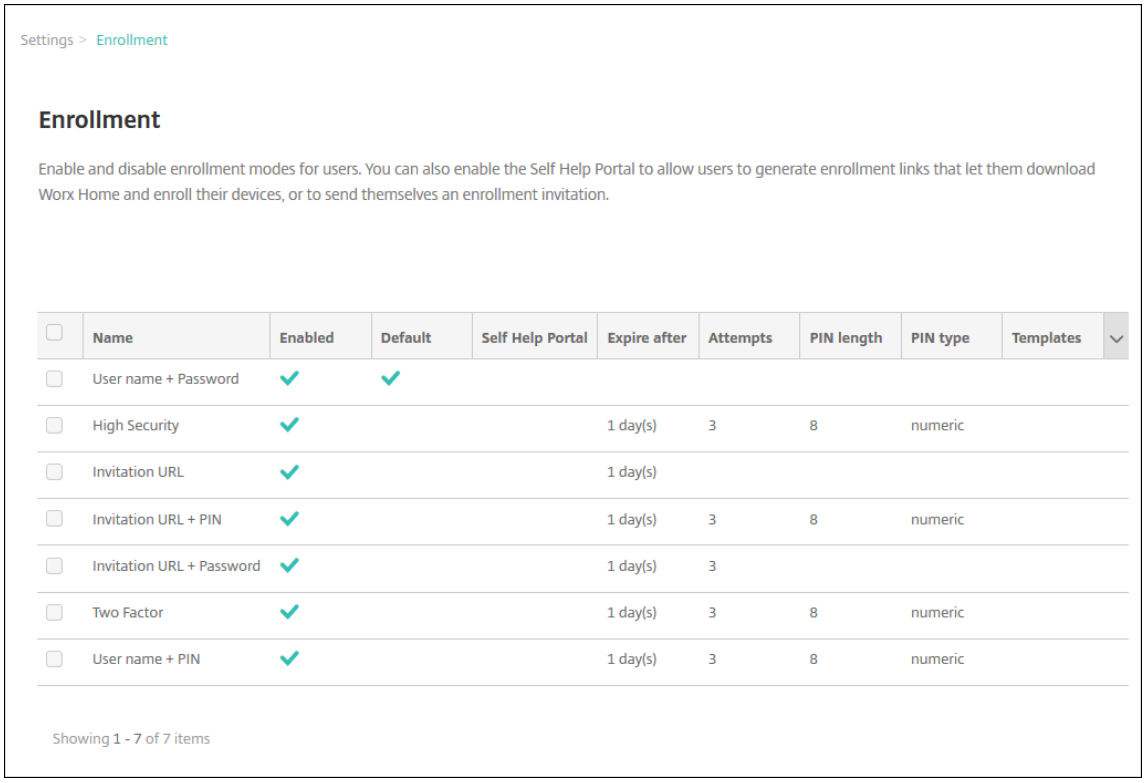
Puede hacer que algunos modos estén disponibles en Self-Help Portal. Desde el portal, los usuarios generan enlaces de inscripción que les permiten inscribir sus dispositivos. Los usuarios de iOS, iPadOS, macOS, Android Enterprise y Android heredado pueden optar por enviarse a sí mismos una invitación a la inscripción desde el portal. Las invitaciones de inscripción no están disponibles para dispositivos Windows.

Las invitaciones de inscripción se envían desde la página **Administrar > Invitaciones de inscripción**. 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 seguridad para la inscripción. Para obtener más información acerca de las plantillas de notificaciones, consulte Crear o actualizar 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 **Parámetros**.
2. Haga clic en **Inscripción**. Aparecerá la página **Enrollment**, que contiene una tabla de todos los modos de seguridad de inscripción disponibles. De manera predeterminada, están habilitados todos los modos de seguridad de inscripción.
3. Seleccione un modo de seguridad de inscripción de la lista para modificarlo. A continuación, establezca ese modo como predeterminado, inhabilítelo, o bien permita a los usuarios acceder a él a través del portal Self-Help Portal.

   > **Nota:**
   >
   > Cuando se marca la casilla situada junto a un modo de seguridad de inscripción, el menú de opciones aparece encima de la lista de los modos correspondientes. Si hace clic en cualquier lugar de la lista, el menú de opciones aparece a la derecha de la lista.



Elija uno de estos modos de seguridad de inscripción:

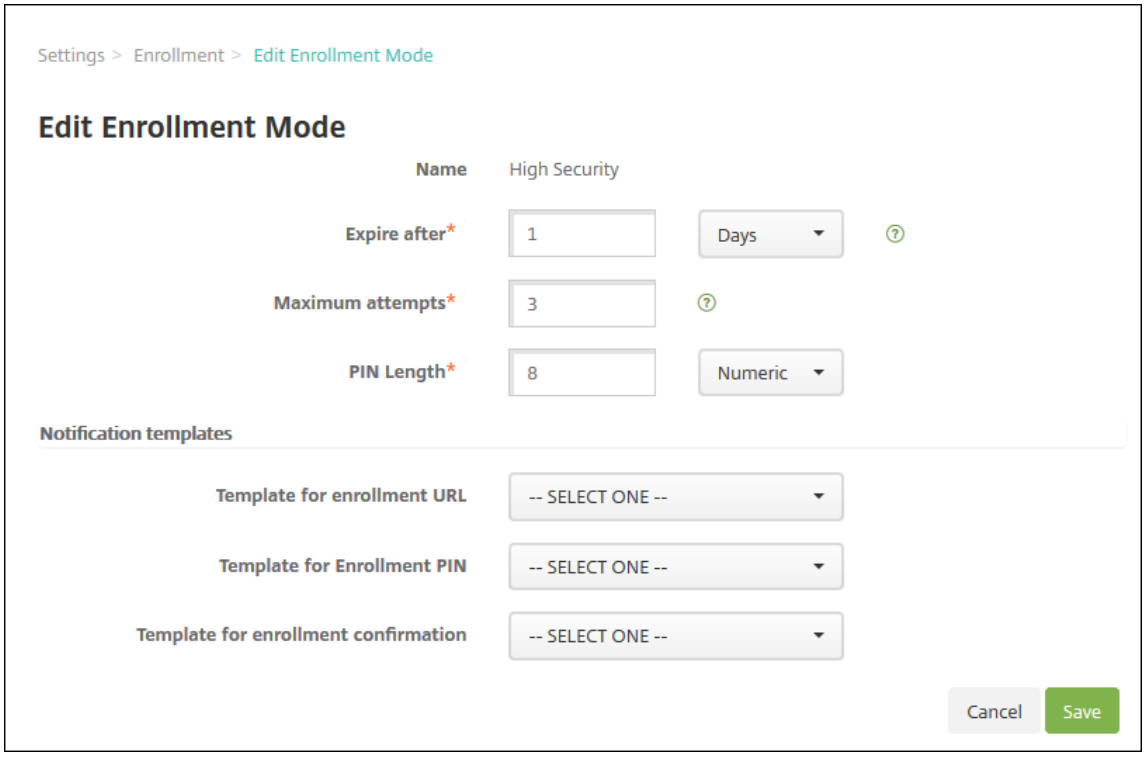
- Nombre de usuario y contraseña
- High Security (Nivel alto de seguridad)
- URL de invitación
- URL de invitación y PIN
- URL de invitación y contraseña
- Autenticación de dos factores
- Nombre de usuario + PIN

Puede utilizar las invitaciones de inscripción para restringir la inscripción a los usuarios que tengan una invitación. Para enviar invitaciones de inscripción, solo puede utilizar los modos de seguridad de inscripción **URL de invitación**, **URL de invitación + PIN** o **URL de invitación + contraseña**. Para los dispositivos que se inscriben con **Nombre de usuario + contraseña**, **Autenticación de dos factores** o **Nombre de usuario + PIN**, los usuarios deben introducir manualmente sus credenciales en Secure Hub.

Puede utilizar invitaciones de inscripción con PIN de un solo uso (OTP) como una solución de autenticación de dos factores. Las invitaciones de inscripción con OTP controlan la cantidad de dispositivos que un usuario puede inscribir. Las invitaciones de OTP no están disponibles para dispositivos Windows.

Para modificar un modo de seguridad de inscripción

1. En la lista **Inscripción**, seleccione un modo de seguridad de inscripción y, a continuación, haga clic en **Modificar**. Aparecerá la página **Modificar modo de inscripción**. El modo seleccionado determina las opciones mostradas.



2. Cambie la siguiente información como corresponda:

   - **Caduca después de:** 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.

     Introduzca **0** para impedir que la invitación caduque.

   - **Días:** En la lista, haga clic en **Días** o **Horas**, de acuerdo con la fecha límite de caducidad que ha introducido en **Caduca después de**.

   - **Máximo de intentos:** 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.

     Introduzca **0** para permitir una cantidad ilimitada de intentos.

   - **Longitud del PIN:** Escriba un número para definir la longitud del PIN generado.

   - **Numérico:** En la lista, haga clic en **Numérico** o **Alfanumérico** para el tipo de PIN.

   - **Plantillas de notificaciones:**

- **Plantilla para URL de inscripción:** En la lista, seleccione una plantilla para la URL de inscripción. Por ejemplo, la plantilla de invitaciones de inscripción envía a los usuarios un correo electrónico o un SMS. El método depende de cómo haya configurado la plantilla que les permite inscribir sus dispositivos en XenMobile. Para obtener más información acerca de las plantillas de notificaciones, consulte Crear o actualizar plantillas de notificaciones.
- **Plantilla para PIN de inscripción:** En la lista, seleccione una plantilla para el PIN de inscripción.
- **Plantilla para confirmación de la inscripción:** En la lista, seleccione la plantilla a utilizar para informar al usuario de que la inscripción se ha realizado correctamente.

3. Haga clic en **Guardar**.

Para establecer un modo de seguridad de inscripción como predeterminado

Al establecer un modo de seguridad de inscripción como predeterminado, ese modo se usará para todas las solicitudes de inscripción de dispositivos a menos que se seleccione otro modo. Si no hay ningún modo de seguridad de inscripción establecido como predeterminado, debe crear una solicitud de inscripción para cada inscripción de dispositivo.

> **Nota:**
>
> Los únicos modos de seguridad de inscripción que puede usar como predeterminados son **Nombre de usuario y contraseña**, **Dos factores** o **Nombre de usuario y PIN**.

1. Seleccione el modo de seguridad de inscripción predeterminado, ya sea **Nombre de usuario y contraseña**, **Dos factores** o **Nombre de usuario y PIN**.

   Para usar un modo como predeterminado, primero habilítelo.

2. Haga clic en **Predeterminado**. A partir de ahora, el modo seleccionado es el predeterminado. Si se había establecido otro modo de seguridad de inscripción como predeterminado, ese modo deja de serlo.

Para inhabilitar un modo de seguridad de inscripción

Al inhabilitar un modo de seguridad 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 el modo en que los usuarios pueden inscribir sus dispositivos. Para ello, deberá inhabilitar un modo de seguridad de inscripción y habilitar otro.

1. Seleccione un modo de seguridad de inscripción.

   El modo de seguridad de inscripción predeterminado no se puede inhabilitar. Si quiere inhabilitar el modo de seguridad de inscripción predeterminado, primero debe quitar su estado pre-

determinado.

2. Haga clic en **Inhabilitar**. El modo de seguridad de inscripción deja de estar habilitado.

Para habilitar un modo de seguridad de inscripción en el portal Self-Help Portal

Habilitar un modo de seguridad 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 seguridad 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 seguridad de inscripción en el portal Self-Help Portal en un momento dado.

1. Seleccione un modo de seguridad de inscripción.
2. Haga clic en **Self Help Portal**. El modo de seguridad de inscripción seleccionado ya está disponible para los usuarios en Self-Help Portal. Cualquier otro modo que ya estuviera habilitado en el portal Self-Help Portal deja de estar disponible para los usuarios.

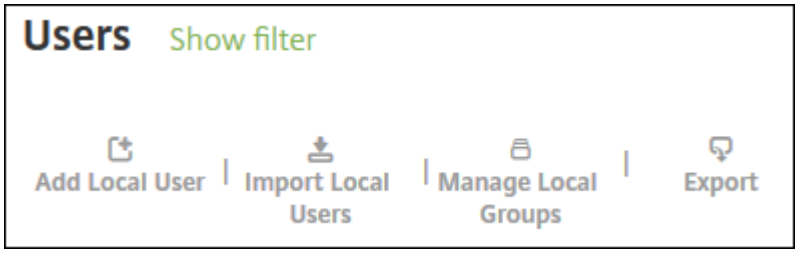
Agregar o quitar grupos

Puede administrar grupos desde el cuadro de diálogo **Administrar grupos** de la consola de XenMobile. Para ver este cuadro, vaya a las páginas **Usuarios**, **Agregar usuario local** o **Modificar usuario local**. No hay ningún comando de modificación de grupos.

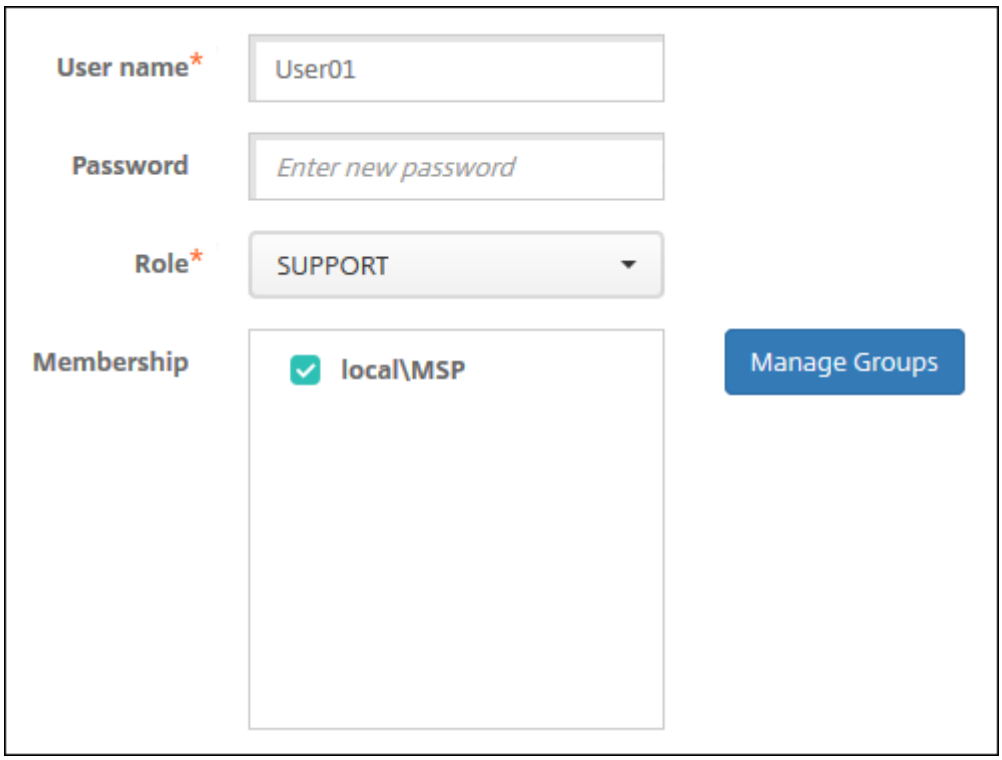
Si quita un grupo, tenga en cuenta que quitar un grupo no tiene ningún efecto sobre las cuentas de usuario. Quitar un grupo simplemente elimina la asociación de usuarios a ese grupo. Asimismo, los usuarios pierden acceso a las aplicaciones o a los perfiles proporcionados por los grupos de entrega asociados 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

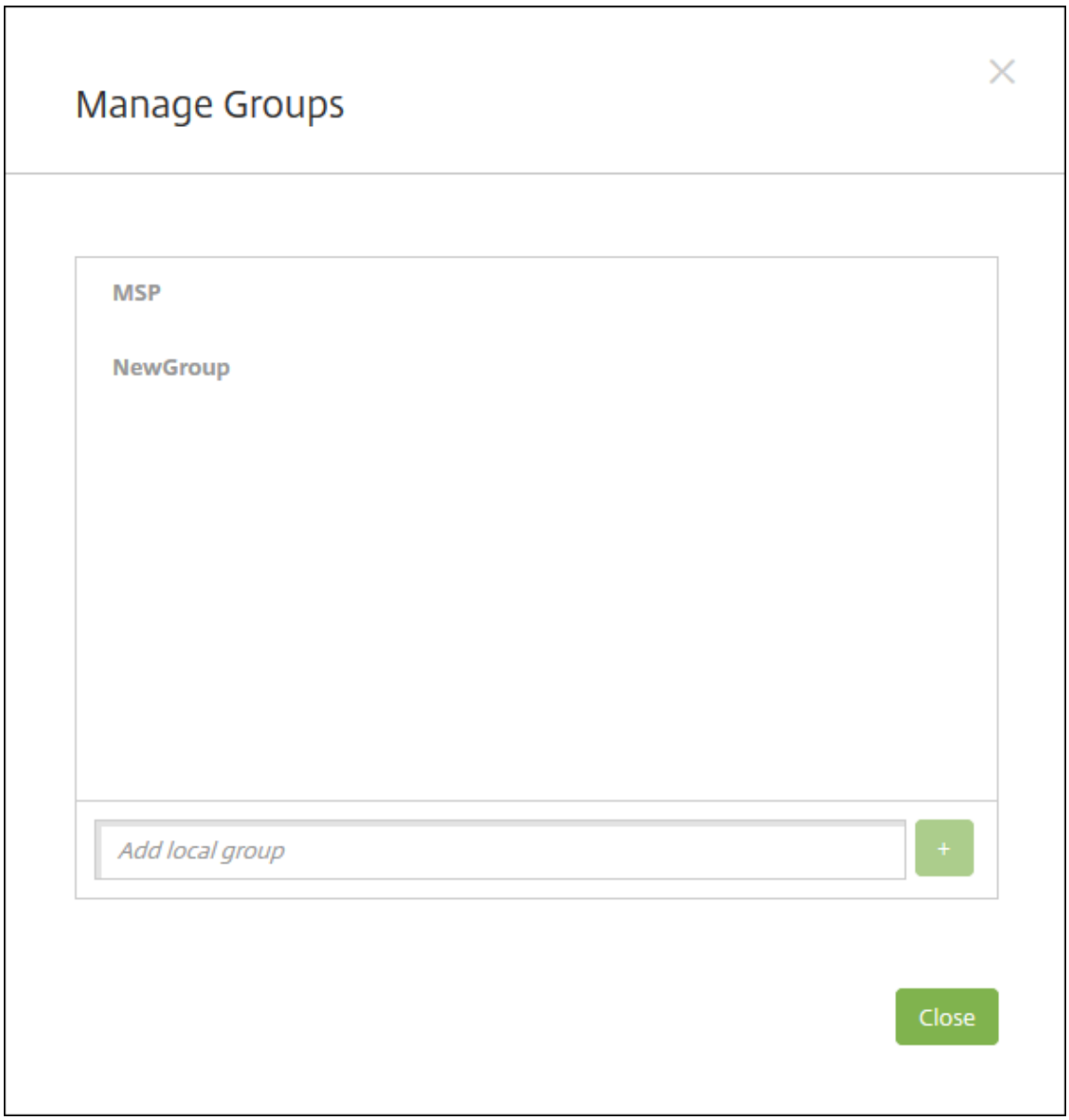
1. Lleve a cabo una de las siguientes acciones:
   - En la página **Usuarios**, haga clic en **Administrar grupos locales**.



- Ya sea en la página **Agregar usuario local** o **Modificar usuario local**, haga clic en **Administrar grupos**.



Aparecerá el cuadro de diálogo **Administrar grupos**.



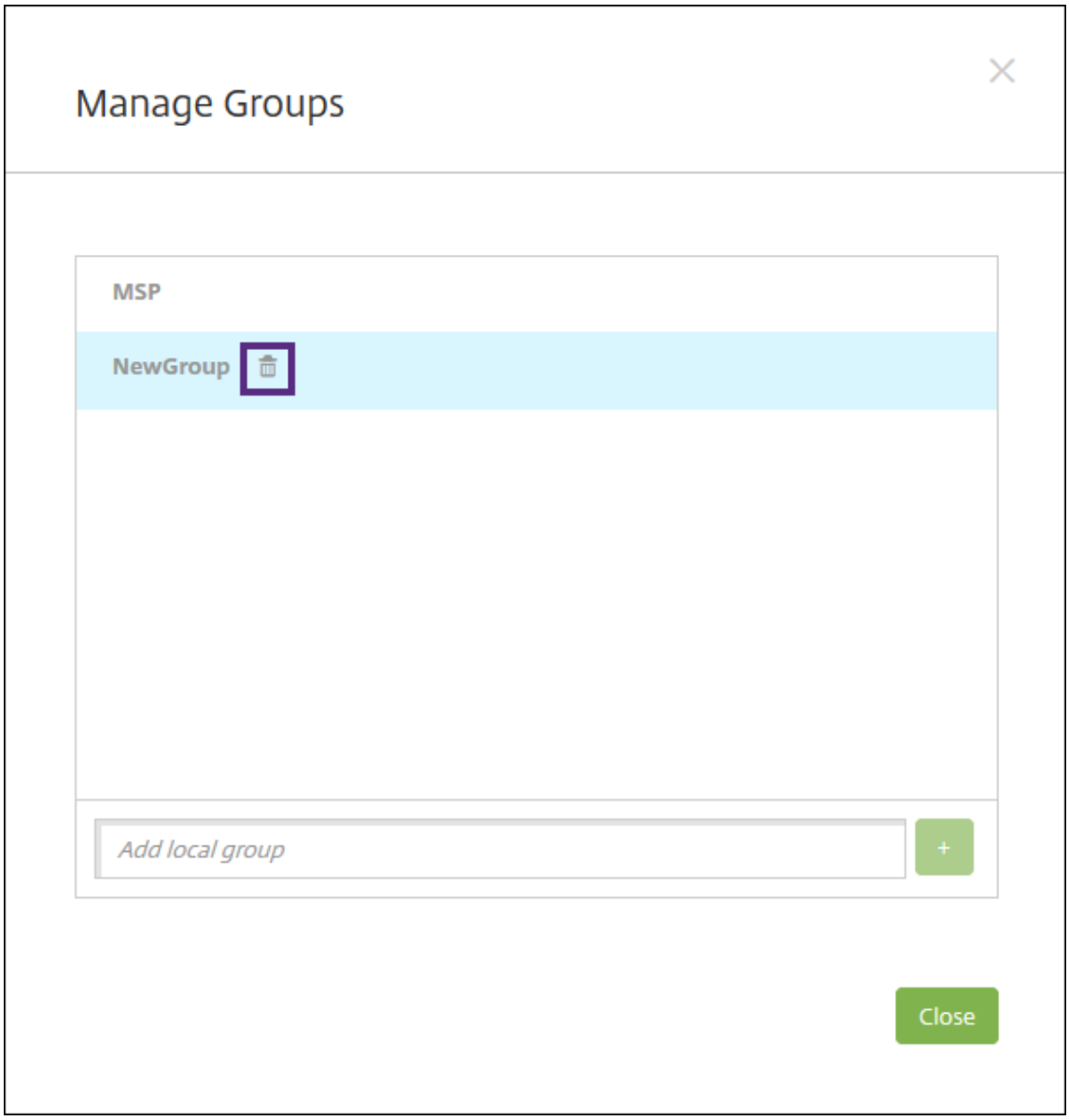
2. Bajo la lista de grupos, escriba un nuevo nombre de grupo y, a continuación, haga clic en el signo más (**+**). El grupo de usuarios se agrega a la lista.
3. Haga clic en **Cerrar**.

Para quitar un grupo

Quitar un grupo no tiene ningún efecto sobre las cuentas de usuario. Quitar un grupo simplemente elimina la asociación de usuarios con ese grupo. Los usuarios pierden acceso a las aplicaciones o a los perfiles proporcionados por los grupos de entrega asociados con ese grupo. Sin embargo, cualquier otra asociación de grupo permanece intacta. 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 **Usuarios**, haga clic en **Administrar grupos locales**.
   - Ya sea en la página **Agregar usuario local** o **Modificar usuario local**, haga clic en **Administrar grupos**.

   Aparecerá el cuadro de diálogo **Administrar grupos**.



2. En el cuadro de diálogo **Administrar grupos**, 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 **Eliminar** para confirmar la operación y eliminar el grupo.

> **Importante:**
>
> Esta operación no se puede deshacer.

5. En el cuadro de diálogo **Administrar grupos**, haga clic en **Cerrar**.

Crear y administrar 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.

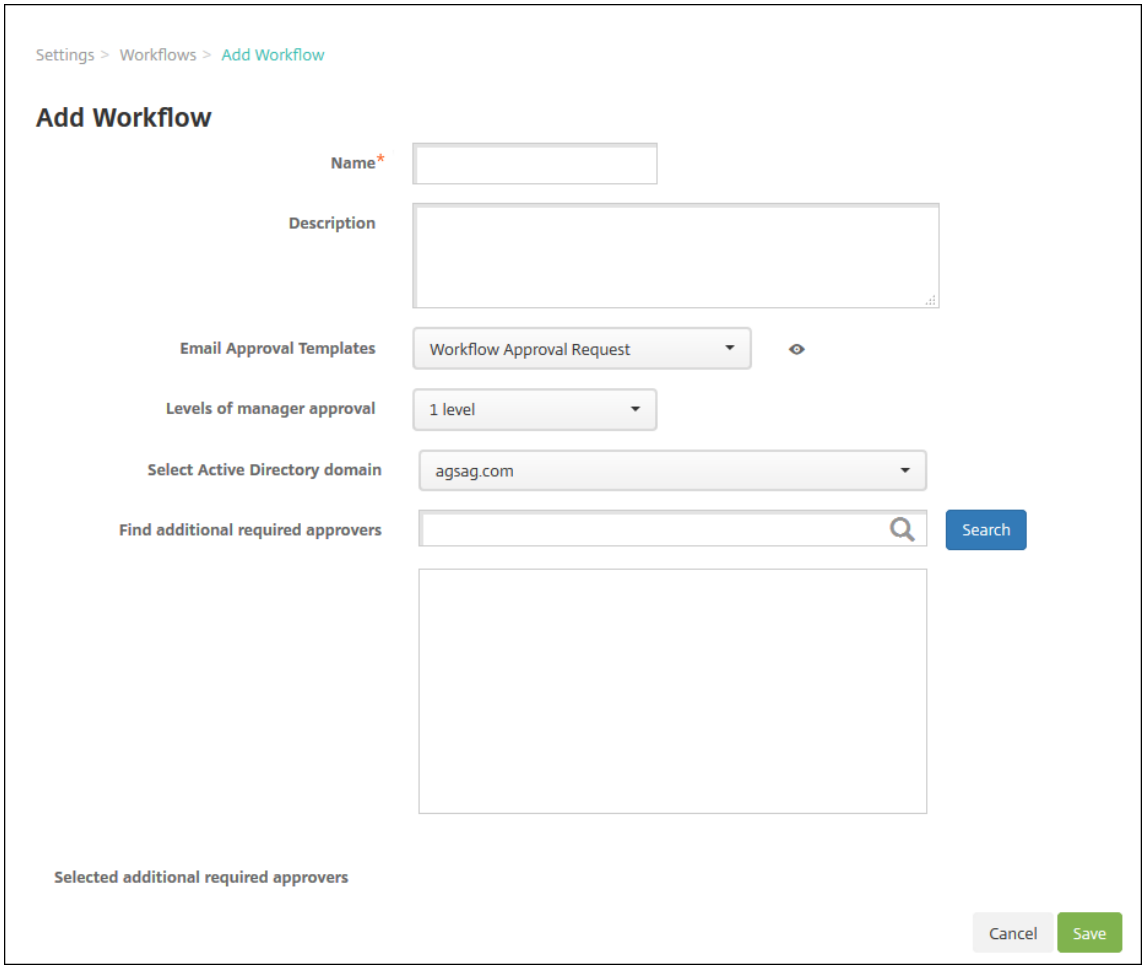
Al configurar XenMobile por primera vez, se definen los parámetros de correo electrónico referentes al flujo de trabajo; estos parámetros se deben establecer antes de utilizar los flujos de trabajo. Puede cambiar los parámetros de correo electrónico del flujo de trabajo en cualquier momento. Estos parámetros 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 **Flujos de trabajo** de la consola de XenMobile. En la página **Flujos de trabajo**, se pueden configurar varios flujos de trabajo para su uso con configuraciones de aplicaciones. Al configurar flujos de trabajo en la página “Flujos de trabajo”, 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 Agregar aplicaciones a XenMobile.

Se puede asignar hasta tres niveles de aprobación del tipo administrador para cuentas de usuario. Si necesita que otras personas aprueben la cuenta de usuario, puede buscar y seleccionar aprobadores adicionales por nombre o dirección de correo electrónico. Cuando XenMobile 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 **Parámetros**.
2. Haga clic en **Flujos de trabajo**. Aparecerá la página **Flujos de trabajo**.
3. Haga clic en **Agregar**. Aparecerá la página **Agregar flujo de trabajo**.



4. Configure estos parámetros:

   - **Nombre:** Escriba un nombre único para el flujo de trabajo.
   - **Descripción:** Si quiere, escriba una descripción del flujo de trabajo.
   - **Plantillas de correo electrónico de aprobación:** En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar al flujo de trabajo. En la consola de XenMobile, puede crear plantillas de correo electrónico en la sección **Plantillas de notificaciones** de **Parámetros**. Al hacer clic en el icono con forma de ojo situado a la derecha del campo, aparece una vista previa de la plantilla que quiere configurar.
   - **Niveles de aprobación administrativa:** En la lista, seleccione la cantidad de niveles de aprobación administrativa necesarios para este flujo de trabajo. El valor predeterminado es **1 nivel**. Las opciones posibles son:
     - No se necesita
     - 1 nivel
     - 2 niveles
     - 3 niveles
   - **Seleccionar dominio de Active Directory:** En la lista, seleccione el dominio correspondi-

ente de Active Directory que se va a usar para el flujo de trabajo.

- **Buscar aprobadores adicionales requeridos:** Escriba un nombre en el campo de búsqueda y, a continuación, haga clic en **Buscar**. Los nombres se originan en Active Directory.
- Cuando el nombre aparezca en el campo, marque la casilla situada al lado. El nombre y la dirección de correo electrónico aparecen en la lista **Aprobadores adicionales requeridos seleccionados**.
  - Para quitar un nombre de la lista, realice una de las siguientes acciones:
    * Haga clic en **Buscar** 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 **Buscar** para limitar los resultados de la búsqueda.
    * Las personas de la lista **Aprobadores adicionales requeridos seleccionados** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla situada junto a cada nombre que quiera quitar.

5. Haga clic en **Guardar**. El flujo de trabajo creado se muestra en la página **Flujos de trabajo**.

Después de crear el flujo de trabajo, puede ver sus detalles, las aplicaciones que tiene asociadas, o bien puede eliminarlo. El flujo de trabajo no se puede modificar una vez creado. Si necesita un flujo de trabajo con otros niveles de aprobación o con otros aprobadores, cree otro flujo de trabajo.

Para ver los detalles de un flujo de trabajo y cómo eliminar uno

1. En la página **Flujos de trabajo**, en la lista de los flujos de trabajo existentes, seleccione un flujo concreto. Para ello, haga clic en la fila de la tabla o marque la casilla situada junto al flujo de trabajo.
2. Para eliminar un flujo de trabajo determinado, haga clic en **Eliminar**. Aparecerá un cuadro de diálogo de confirmación. Vuelva a hacer clic en **Eliminar**.

> **Importante:**
>
> Esta operación no se puede deshacer.

Perfiles de inscripción

January 4, 2022

Un perfil de inscripción especifica lo siguiente:

- Opciones de inscripción para administración de dispositivos en dispositivos Android e iOS. En el caso de Android, las opciones de inscripción disponibles para el modo de servidor MDM+MAM (ENT) difieren de las opciones para el modo MDM.
- Opciones de inscripción para administración de aplicaciones en dispositivos Android e iOS.
- Otras opciones de inscripción:
  - Si se debe limitar el número de dispositivos que un usuario puede inscribir.
    Si se alcanza el límite de dispositivos, un mensaje de error informa al usuario que ha superado el límite de inscripción de dispositivos.
  - Si se debe permitir que un usuario rechace la administración de dispositivos.

Puede utilizar perfiles de inscripción para combinar diferentes casos de uso y rutas de migración de dispositivos en una sola consola de XenMobile Server. Entre los casos de uso, se incluyen:

- Administración de dispositivos móviles (solo MDM)
- MDM+Administración de aplicaciones móviles (MAM)
- Solo MAM
- Inscripciones de propiedad de la empresa
- Inscripciones BYOD (con la posibilidad de excluir la inscripción en MDM)
- Migración de inscripciones en Administrador de dispositivos Android a inscripciones en Android Enterprise (totalmente administrado, perfil de trabajo, dispositivo dedicado)

Al crear un grupo de entrega, puede utilizar el perfil de inscripción predeterminado denominado Global o especificar otro perfil de inscripción.

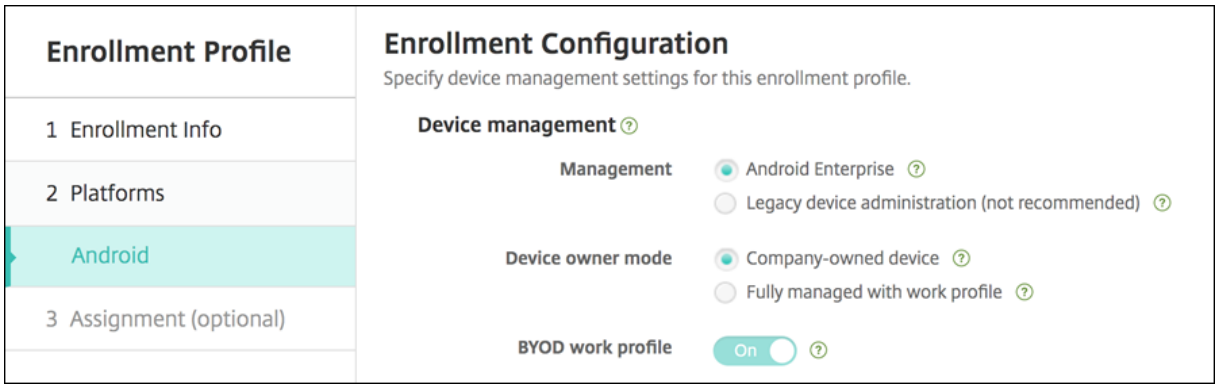
Las funciones del perfil de inscripción por plataforma incluyen lo siguiente.

- **Para dispositivos Android:** Debe especificar el modo propietario del dispositivo. Por ejemplo: Totalmente administrado, totalmente administrado con perfil de trabajo y perfil de trabajo BYOD. La opción **Dispositivo dedicado** solo aparece cuando tiene una licencia Enterprise o Advanced para XenMobile. Los nuevos dispositivos se inscriben en Android Enterprise y en la administración de aplicaciones de forma predeterminada. Los modos de seguridad de inscripción **Nombre de usuario y PIN**, **URL de invitación**, **URL de invitación y PIN**, y **URL de invitación y contraseña** no están disponibles para Android Enterprise.
- **Para dispositivos iOS:** Debe especificar el tipo de inscripción del dispositivo (inscripción de dispositivos o no administrar dispositivos). Los parámetros de iOS solo aparecen cuando tiene una licencia Enterprise o Advanced de XenMobile. Los nuevos dispositivos se inscriben en la administración de dispositivos Apple y en la administración de aplicaciones de forma predeterminada.

Si no necesita inscribir dispositivos dedicados para dispositivos Android o inscripción solo en MAM para dispositivos Android o iOS, puede desactivar la propiedad de servidor `enable.multimode.xms`. Sin embargo, mantener esta propiedad habilitada significa que solo necesita un servidor de XenMobile Server para gestionar todos los tipos de perfiles de inscripción. Consulte Propiedades de

servidor.

Cuando inhabilita `enable.multimode.xms`, solo están disponibles los parámetros de esta captura de pantalla:

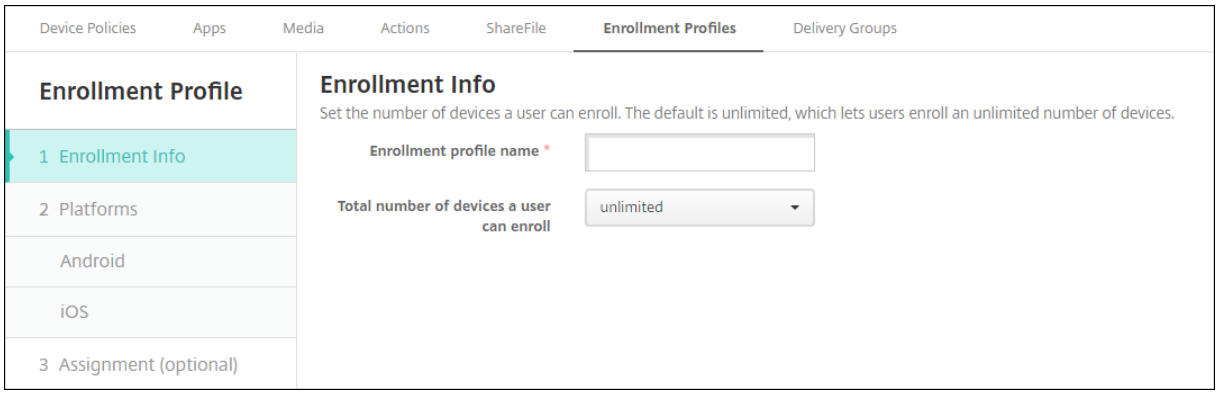


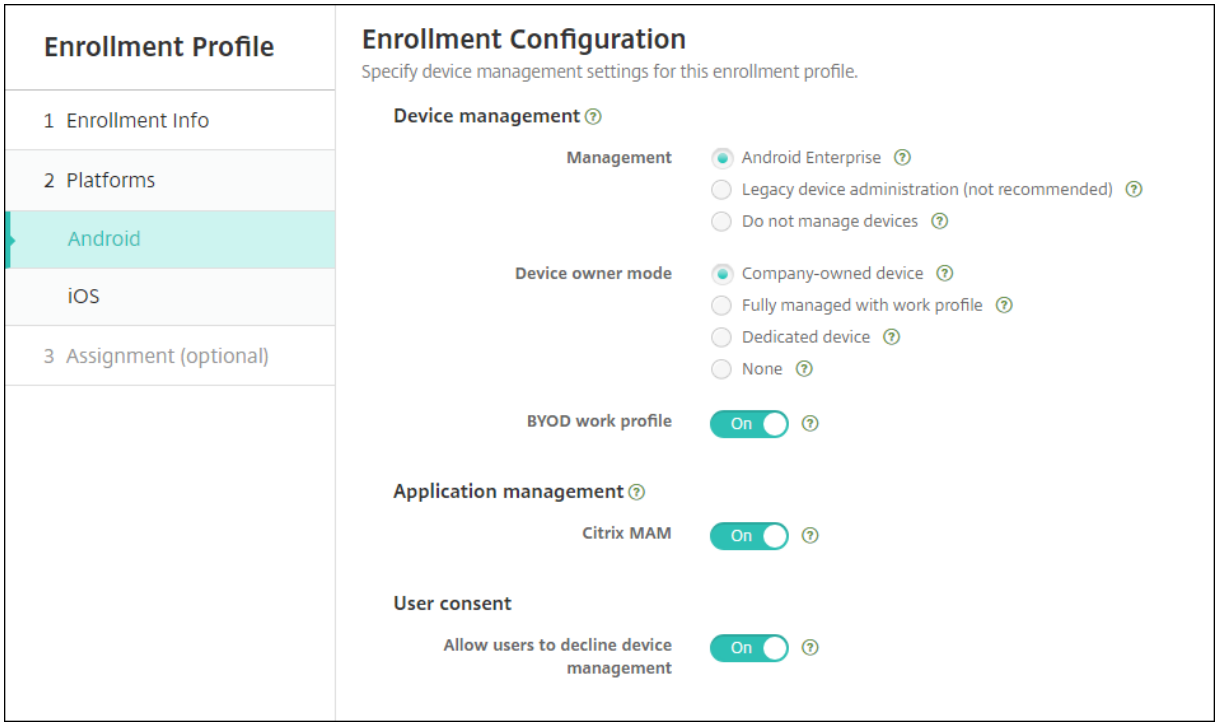
Para obtener más información sobre estos parámetros, consulte Android Enterprise.

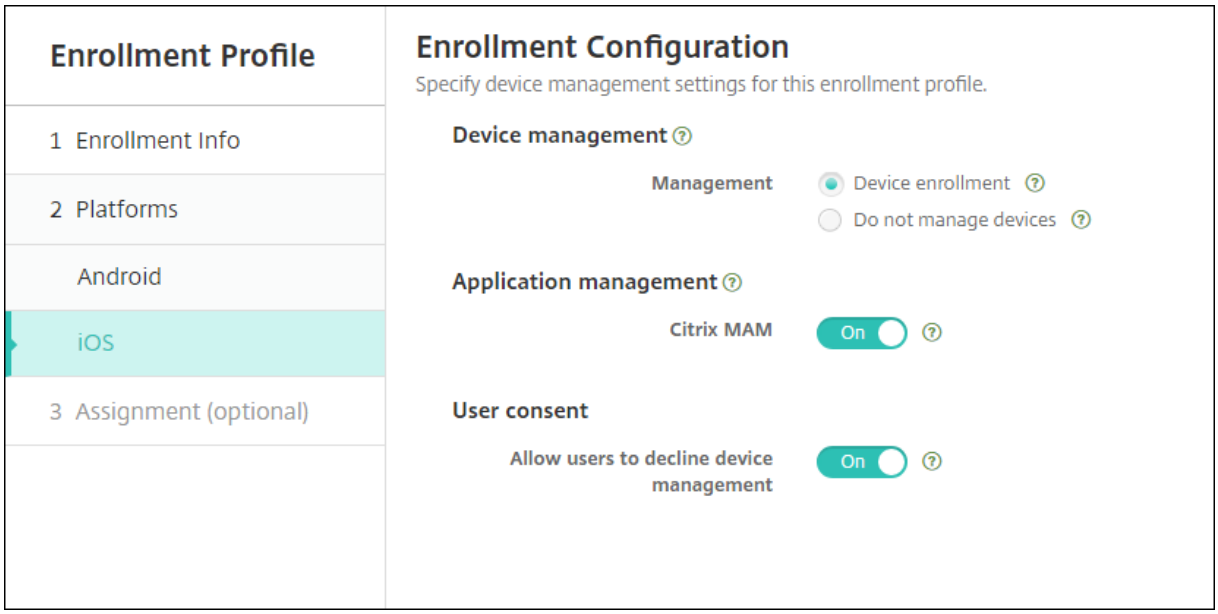
Perfil de inscripción Global

El perfil de inscripción predeterminado se llama “Global”. El perfil Global es útil para prueba hasta que tenga la oportunidad de crear perfiles de inscripción.

En las siguientes capturas de pantalla, se muestra la configuración predeterminada del perfil de inscripción Global.







Perfiles de inscripción, grupos de entrega e inscripción

Los perfiles de inscripción y los grupos de entrega interactúan de la siguiente manera:

- Puede asociar un perfil de inscripción a uno o más grupos de entrega.
- Si un usuario pertenece a varios grupos de entrega que tienen perfiles de inscripción diferentes, el nombre del grupo de entrega determina el perfil de inscripción utilizado. XenMobile Server selecciona el grupo de entrega que aparece en último lugar en una lista alfabética de grupos de

entrega. Supongamos, por ejemplo, que tiene lo siguiente:

- Dos perfiles de inscripción, llamados “EP1” y “EP2”.
- Dos grupos de entrega, llamados “DG1” y “DG2”.
- “DG1” está asociado a “EP1”.
- “DG2” está asociado a “EP2”.

Si el usuario de la inscripción está en los grupos de entrega “DG1” y “DG2”, XenMobile Server utiliza el perfil de inscripción “EP2” para determinar el tipo de inscripción del usuario.

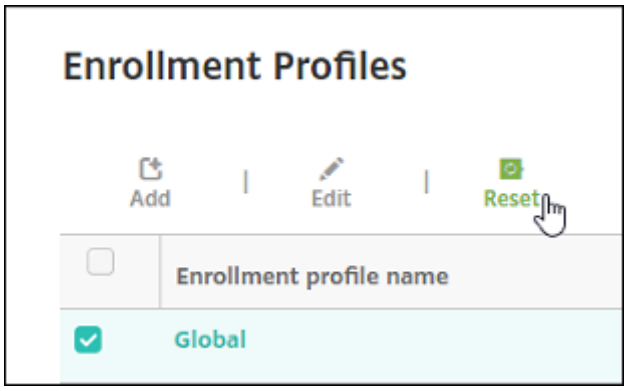
- El orden de implementación solo se aplica a los dispositivos de un grupo de entrega que tenga un perfil de inscripción configurado para MDM (administración de dispositivos).
- Después de inscribir un dispositivo, para hacer algunos cambios en un perfil de inscripción será necesario reinscribirlo:
  - Agregar MAM a un perfil de inscripción configurado para MDM.
  - Mover un dispositivo inscrito en MDM a un grupo de entrega configurado para MDM+MAM. Ese cambio afecta únicamente a las inscripciones de nuevos dispositivos. Las inscripciones de dispositivos existentes no se ven afectadas.
  - Agregar MDM a un perfil de inscripción configurado para MAM.
- Cambiar a un perfil de inscripción diferente no afecta a los dispositivos ya inscritos. Los usuarios deberán desinscribir y, a continuación, volver a inscribir esos dispositivos para que los cambios surtan efecto.

Para crear un perfil de inscripción

1. En la consola de XenMobile Server, vaya a **Configurar > Perfiles de inscripción**.
2. En la página **Información de inscripción**, escriba un nombre descriptivo para el perfil. De forma predeterminada, un usuario puede inscribir una cantidad de dispositivos ilimitada. Seleccione un valor para limitar la cantidad de dispositivos por usuario. El límite se aplica a la suma de dispositivos Android e iOS administrados con MAM o MDM que un usuario inscribe.
3. Complete las páginas de plataformas. Para obtener información acerca de los parámetros de inscripción específicos de las plataformas, consulte:
   - Android Enterprise
   - iOS: Métodos de inscripción admitidos
4. En la página **Asignación**, adjunte uno o varios grupos de entrega al perfil de inscripción.

   Un usuario puede pertenecer a varios grupos de entrega que tengan perfiles de inscripción diferentes. En ese caso, el nombre del grupo de entrega determina el perfil de inscripción utilizado. XenMobile selecciona el grupo de entrega que aparece en último lugar en una lista alfabética de grupos de entrega. Para crear grupos de entrega, vaya a **Configurar > Grupos de entrega**.

En la página **Configurar > Perfiles de inscripción**, aparecerá una lista de sus perfiles de inscripción. Para modificar el perfil Global o restablecerlo a los valores predeterminados originales, seleccione la fila del perfil Global y haga clic en **Restablecer**. El perfil Global no se puede eliminar.



Configurar roles con RBAC

January 4, 2022

Cada rol predefinido del control de acceso por roles (RBAC) tiene determinados permisos de funciones y de acceso asociados. En este artículo, se describe para qué sirve cada uno de esos permisos. Para obtener una lista completa de permisos predeterminados para cada rol integrado, descargue Role-Based Access Control Defaults.

Aplicar permisos equivale a definir los grupos de usuarios que el rol de RBAC tiene el permiso de administrar. El administrador predeterminado no puede cambiar los parámetros aplicados de los permisos. De forma predeterminada, los permisos aplicados se refieren a todos los grupos de usuarios.

Cuando hace una *asignación*, asigna el rol de RBAC a un grupo, de modo que el grupo de usuarios es propietario de los derechos de administrador de RBAC.

> **Importante:**
>
> En el permiso Parámetros, el permiso RBAC otorga acceso total a los usuarios administradores, incluida la capacidad de asignar sus propios permisos. Conceda este acceso solamente a los usuarios a los que quiere dar la capacidad de manipular todo lo que hay en el sistema de Endpoint Management.

Este artículo contiene las siguientes secciones:

- Rol de administrador
- Rol de aprovisionamiento de dispositivos
- Rol de asistencia
- Rol de usuario

- Configurar roles con RBAC

Rol de administrador

Los usuarios que tengan el rol predefinido Admin tienen o no tienen acceso a las siguientes funciones de XenMobile. De forma predeterminada, las opciones **Acceso autorizado** (excepto Self Help Portal), **Funciones de consola** y **Aplicar permisos** están habilitadas.

Acceso autorizado

Acceso de administrador a la consola	Los administradores tienen acceso a todas las funciones de la consola de XenMobile.
Acceso al portal Self Help Portal	Los administradores no tienen acceso al portal Self-Help Portal.
Inscripción de dispositivos compartidos	Los administradores no tienen acceso a la inscripción de dispositivos compartidos. Esta función está pensada para los usuarios que necesitan inscribir dispositivos compartidos.
Acceso a Remote Support	Los administradores tienen acceso a Remote Support.*
Acceso a API públicas	Los administradores tienen acceso a la API pública para llevar a cabo, previa programación, acciones disponibles en la consola de XenMobile. Esas acciones pueden ser: administración de certificados, licencias, aplicaciones, dispositivos, grupos de entrega y usuarios locales.
Inscribir dispositivos COSU	Proporciona un modo para que los administradores puedan inscribir dispositivos Android Enterprise dedicados (también conocidos como dispositivos COSU) si esta capacidad no está configurada mediante un perfil de inscripción.

* La asistencia remota (Remote Support) permite que el personal del servicio de asistencia tome el control remoto de los dispositivos móviles Windows CE y Android administrados. La transmisión de

la pantalla solo se admite en dispositivos Samsung Knox. Remote Support no está disponible para implementaciones locales en clúster de XenMobile Server. Remote Support no está disponible para nuevos clientes desde el 1 de enero de 2019. Los clientes existentes pueden seguir utilizando el producto, pero Citrix no proporciona mejoras ni correcciones.

Funciones de consola

Los administradores tienen acceso sin restricciones a todas las funciones de la consola de XenMobile.

Panel de mandos	El **panel de mandos** es la primera página que los administradores ven después de iniciar sesión en la consola de XenMobile. El **panel de pandos** muestra información básica sobre notificaciones y dispositivos.
Informes	En la página **Análisis > Informes**, se ofrecen informes predefinidos que permiten analizar las implementaciones de dispositivos y aplicaciones.
Dispositivos	La página **Administrar > Dispositivos** es donde se administran los dispositivos de los usuarios. En esta página, puede agregar dispositivos individuales o importar un archivo de aprovisionamiento de dispositivos para agregar varios dispositivos a la vez.
Grupos y usuarios locales	La página **Administrar > Usuarios** es donde se agregan, modifican o eliminan usuarios locales y grupos de usuarios locales.
Inscripción	La página **Administrar > Invitaciones de inscripción** es donde se define cómo invitar a los usuarios a inscribir sus dispositivos en XenMobile.
Directivas	La página **Configurar > Directivas de dispositivo** es donde se gestionan las directivas de los dispositivos; por ejemplo, directivas de VPN y Wi-Fi.
Aplicaciones	La página **Configurar > Aplicaciones** es donde se administran las varias aplicaciones que los usuarios pueden instalar en sus dispositivos.
Medios	La página **Configurar > Multimedia** es donde se administran los medios para contenido multimedia que los usuarios pueden instalar en sus dispositivos.
Acción	La página **Configurar > Acciones** es donde se administran las respuestas para desencadenar eventos.
Perfiles de inscripción	La página **Configurar > Perfiles de inscripción** es donde se configuran los perfiles (modos) de inscripción para permitir que los usuarios inscriban sus dispositivos.
Grupos de entrega	La página **Configurar > Grupos de entrega** es donde se administran los grupos de entrega y los recursos asociados a ellos.
Parámetros	La página **Parámetros** es donde se definen los parámetros del sistema (como propiedades de cliente y servidor, certificados y proveedores de credenciales). **Importante:** Estos parámetros incluyen el permiso RBAC. El permiso RBAC otorga acceso total a los administradores, incluida la capacidad de asignar sus propios permisos. Conceda este acceso solamente a los

usuarios a los que quiere dar la capacidad de manipular todo lo que hay en el sistema de Endpoint Management. | |
| Asistencia | La página **Solución de problemas y asistencia** es donde se realizan las actividades de solución de problemas (como ejecutar diagnósticos y generar registros). |

Dispositivos

Los administradores acceden a las funciones de los dispositivos mediante la consola. Desde ella, pueden establecer restricciones para los dispositivos, configurar y enviar notificaciones a los dispositivos y administrar las aplicaciones presentes en los dispositivos, entre otros.

Borrado completo de dispositivo	Borra todos los datos y aplicaciones de un dispositivo, incluidas las tarjetas de memoria (si el dispositivo las tuviera).
Borrar restricción	Quita una o varias restricciones de dispositivo.
Borrado selectivo de dispositivo	Borra todas las aplicaciones y datos empresariales del dispositivo, pero no afecta a las aplicaciones y datos personales.
Ver ubicaciones	Muestra la ubicación y establece restricciones geográficas en el dispositivo. Incluye: Localizar dispositivos (ver la ubicación de un dispositivo) y Seguimiento de dispositivos (realizar el seguimiento de la ubicación de un dispositivo a lo largo del tiempo).
Bloquear dispositivo	Bloquea remotamente un dispositivo de modo que los usuarios no puedan usarlo.
Desbloquear dispositivo	Desbloquea remotamente un dispositivo de modo que los usuarios puedan usarlo.
Bloquear contenedor	Bloquea remotamente el contenedor de datos empresariales de un dispositivo.
Desbloquear contenedor	Desbloquea remotamente el contenedor de datos empresariales de un dispositivo.
Restablecer contraseña de contenedor	Restablece la contraseña del contenedor de datos empresariales.

Habilitar omisión de bloqueo de activación de DEP ASM	En un dispositivo iOS supervisado, almacena un código de circunvalación cuando habilite el Bloqueo de activación. Si necesita borrar el dispositivo, use este código para quitar automáticamente el Bloqueo de activación.
Hacer sonar el dispositivo	Hace sonar remotamente un dispositivo Windows al máximo volumen durante 5 minutos.
Reiniciar el dispositivo	Reinicia los dispositivos Windows desde la consola de XenMobile.
Implementar en dispositivo	Envía aplicaciones, notificaciones y restricciones, entre otros, a un dispositivo.
Modificar dispositivo	Modifica los parámetros de un dispositivo.
Notificación a dispositivo	Envía una notificación a un dispositivo.
Agregar o quitar dispositivo	Agrega o quita dispositivos de XenMobile.
Importar dispositivos	Importa en XenMobile un grupo de dispositivos a partir de un archivo.
Exportar tabla de dispositivos	Recaba información sobre dispositivos a partir de la página “Dispositivos” y la exporta en un archivo CSV.
Revocar dispositivo	Prohíbe a un dispositivo que se conecte a XenMobile.
Bloqueo de aplicaciones	Deniega el acceso a todas las aplicaciones de un dispositivo. En Android, los usuarios no pueden iniciar sesión en XenMobile. En iOS, los usuarios pueden iniciar sesión, pero no pueden acceder a las aplicaciones.
Borrado de aplicaciones	En Android, esta operación elimina la cuenta de XenMobile del usuario. En iOS, esta operación elimina la clave de cifrado que los usuarios necesitan para acceder a las funciones de XenMobile.
Ver inventario de software	Muestra el software instalado en un dispositivo.

Solicitar duplicación AirPlay	Solicita iniciar el streaming de AirPlay.
Detener duplicación AirPlay	Detiene el streaming de AirPlay.
Habilitar el modo perdido	En **Administrar > Dispositivos**, puede colocar un dispositivo supervisado en modo perdido para bloquearlo en la pantalla de bloqueo. El modo perdido también le permite localizar el dispositivo en caso de hurto o pérdida.
Inhabilitar el modo perdido	En **Administrar > Dispositivos**, puede inhabilitar el modo perdido de un dispositivo establecido en ese modo.
Actualización de SO del dispositivo	Puede implementar una directiva para controlar las actualizaciones del SO en los dispositivos.
Apagar dispositivo	Apaga los dispositivos iOS desde la consola de XenMobile.
Reiniciar dispositivo	Reinicia los dispositivos iOS desde la consola de XenMobile.

Grupos y usuarios locales

La página **Administrar > Usuarios** es donde se administran usuarios locales y grupos de usuarios locales en XenMobile.

Agregar usuarios locales
Eliminar usuarios locales
Modificar usuarios locales
Importar usuarios locales
Exportar usuarios locales
Grupos de usuarios locales
Obtener ID de bloqueo de usuario local
Eliminar bloqueo de usuario local

Inscripción

Los administradores pueden agregar y eliminar invitaciones de inscripción, enviar notificaciones a usuarios y exportar la tabla de inscripción en un archivo CSV.

Agregar o eliminar inscripción	Agrega o quita una invitación de inscripción a usuarios o grupos de usuarios.
Notificar al usuario	Envía una invitación de inscripción a usuarios o grupos de usuarios.
Exportar la tabla de invitaciones de inscripción	Recaba información sobre inscripciones a partir de la página “Inscripción” y la exporta en un archivo CSV.

Directivas

Agregar o eliminar directiva	Agrega o quita una directiva de dispositivo o de aplicación.
Modificar directiva	Cambia una directiva de dispositivo o de aplicación.
Cargar directiva	Carga una directiva de dispositivo o de aplicación.
Clonar directiva	Copia una directiva de dispositivo o de aplicación.
Inhabilitar directiva	Inhabilita una directiva existente de aplicación.
Exportar directiva	Recaba información sobre directivas de dispositivo a partir de la página “Directivas de dispositivo” y la exporta en un archivo CSV.
Asignar directiva	Asigna una directiva de dispositivo a uno o varios grupos de entrega.

Aplicación

En XenMobile, los administradores gestionan las aplicaciones desde la página **Configurar > Aplicaciones**.

Agregar o eliminar aplicaciones empresariales o de almacenes de aplicaciones	Agrega o quita una aplicación de tienda pública de aplicaciones o una aplicación de empresa (no habilitada para MDX).
Modificar aplicaciones empresariales o de almacén de aplicaciones	Modifica una aplicación de tienda pública de aplicaciones o una aplicación de empresa (no habilitada para MDX).
Agregar/eliminar aplicación MDX, web y SaaS	Agrega/quita una aplicación habilitada para MDX, una aplicación de su red interna (aplicación web) o una aplicación de una red pública (SaaS) a/de XenMobile.
Modificar aplicaciones MDX, web y SaaS	Modifica una aplicación habilitada para MDX, una aplicación de su red interna (aplicación web) o una aplicación de una red pública (SaaS) en XenMobile.
Agregar o quitar categoría	Agrega o elimina una categoría en que pueden aparecer aplicaciones en XenMobile Store.
Asignar aplicación pública o de empresa a grupo de entrega	Asigna una aplicación de tienda pública de aplicaciones o una aplicación habilitada para MDX a un grupo de entrega para su implementación.
Asignar aplicación MDX, de enlace web o SaaS a grupo de entrega	Asigna a un grupo de entrega una aplicación habilitada para MDX, que no requiere Single Sign-On (WebLink) o proveniente de una red pública (SaaS).
Exportar tabla de aplicaciones	Recaba información sobre aplicaciones a partir de la página Apps y la exporta en un archivo CSV.

Medios

Administra el contenido multimedia obtenido de un tienda pública de aplicaciones o a través de una licencia de compras por volumen.

Agregar o eliminar libros de empresa o de almacén de aplicaciones
Asignar libros públicos/de empresa a grupo de entrega
Modificar libros de empresa o de almacén de aplicaciones

Acción

Agregar/eliminar acción	Agrega o quita una acción definida por un desencadenador (un evento, una propiedad de dispositivo o usuario, o bien el nombre de una aplicación instalada) y su respuesta asociada.
Modificar acción	Cambia una acción definida por un desencadenador (un evento, una propiedad de dispositivo o usuario, o bien el nombre de una aplicación instalada) y su respuesta asociada.
Asignar acción a grupo de entrega	Asigna una acción a un grupo de entrega para la implementación en los dispositivos de los usuarios.
Exportar acción	Recaba información sobre acciones a partir de la página “Acciones” y la exporta en un archivo CSV.

Grupo de entrega

Los administradores gestionan los grupos de entrega desde la página **Configurar > Grupos de entrega**.

Agregar o eliminar grupo de entrega	Crea o elimina un grupo de entrega, que agrega usuarios concretos y acciones, aplicaciones y directivas opcionales.
Modificar grupo de entrega	Modifica un grupo de entrega existente, lo que modifica usuarios y acciones, aplicaciones y directivas opcionales.

Implementar grupo de entrega	Pone un grupo de entrega disponible para su uso.
Exportar grupo de entrega	Recaba información sobre grupos de entrega a partir de la página “Grupo de entrega” y la exporta en un archivo CSV.

Perfil de inscripción

Administra perfiles de inscripción.

Agregar/eliminar perfil de inscripción
Modificar perfil de inscripción
Asignar perfil de inscripción a grupo de entrega

Parámetros

Los administradores configuran diferentes parámetros en la página **Parámetros**.

RBAC	Asignación RBAC, Asignar roles. **Importante:** Este permiso otorga acceso total a los administradores, incluida la capacidad de asignar sus propios permisos. Conceda este acceso solamente a los usuarios a los que quiere dar la capacidad de manipular todo lo que hay en el sistema de Endpoint Management.
LDAP	Administra uno o varios directorios que cumplen el protocolo LDAP (como Active Directory) para importar grupos, cuentas de usuario y propiedades relacionadas.
Licencia	Para XenMobile Server local. Administra licencias de Citrix.

Inscripción	Habilita el portal Self Help Portal y los modos de seguridad de inscripción para usuarios.
Administración de versiones	Muestra la versión actual instalada. Incluye: Actualización de administración de versiones
Certificados	Modificar certificado APNS, Escucha SSL de certificados
Plantillas de notificaciones	Crea plantillas de notificaciones para utilizarlas en acciones automatizadas, inscripciones y la entrega de mensajes de notificación estándar a los usuarios.
Flujos de trabajo	Administra la creación, la aprobación y la eliminación de cuentas de usuario a utilizar con configuraciones de aplicaciones.
Proveedores de credenciales	Agrega uno o varios proveedores de credenciales autorizados para emitir certificados de dispositivo. Los proveedores de credenciales controlan el formato de los certificados y las condiciones de renovación o revocación de estos.
Entidades PKI	Administra entidades de infraestructura de clave pública (genéricas, de Microsoft Certificate Services o entidades de certificación discrecional).
Probar conexión PKI	Use el botón Probar conexión, ubicado en la página **Parámetros > Entidades PKI**, para verificar que es posible acceder al servidor.
Propiedades de cliente	Administra diferentes propiedades en los dispositivos de los usuarios, como el tipo de código de acceso, su nivel de seguridad o su caducidad.
Asistencia del cliente	Establece las maneras en que los usuarios pueden ponerse en contacto con los servicios de asistencia (teléfono, correo electrónico o correo de tíquet de asistencia).

Personalización de marca de clientes	Puede crear un nombre de almacén personalizado y vistas predeterminadas de almacén para XenMobile Store. Agrega un logotipo personalizado que aparecerá en XenMobile Store o Secure Hub.
Puerta de enlace SMS del operador	Establece puertas de enlace SMS del operador para configurar notificaciones que XenMobile envía a través de ellas.
Servidor de notificaciones	Establece una puerta de enlace SMTP para enviar correos electrónicos a los usuarios.
ActiveSync Gateway	Administra el acceso de usuario a usuarios y dispositivos con ayuda de reglas y propiedades.
Programa de implementación de Apple	Agrega una cuenta del Programa de implementación de Apple a XenMobile.
Inscripción de dispositivos en Apple Configurator	Configura parámetros de Apple Configurator en XenMobile.
Configuración de compras por volumen de iOS	Agrega cuentas de compras por volumen de Apple.
Proveedor de servicios móviles	Utiliza la interfaz del proveedor de servicios móviles para emitir operaciones y consultar dispositivos BlackBerry y Exchange ActiveSync.
Citrix Gateway	Para XenMobile Server local. Agrega una instancia de Citrix Gateway. Elige si permitir la autenticación y si insertar certificados de usuario para esa autenticación. Elige un proveedor de credenciales.
Control de acceso de red	Establece las condiciones que determinan si un dispositivo no cumple las normas y, en consecuencia, se le deniega el acceso a la red.
Samsung Knox	Habilita o inhabilita XenMobile para consultar las API de REST del servidor de atestación de Samsung Knox.

Propiedades de servidor	Agrega o modifica las propiedades de servidor. Requiere reiniciar XenMobile en todos los nodos.
Syslog	Para XenMobile Server local. Envía archivos de registros a un servidor de registros del sistema (syslog) mediante el nombre de host o la dirección IP del servidor.
XenApp y XenDesktop	Permite a los usuarios agregar Virtual Apps and Desktops a través de Secure Hub.
Citrix Files	Cuando se utiliza XenMobile con cuentas Enterprise: Configura parámetros de conexión a la cuenta de Content Collaboration y a la cuenta de servicio del administrador para administrar cuentas de usuario. Requiere las credenciales existentes de administrador y el dominio de Citrix Files. Cuando se utiliza XenMobile con conectores de zonas de almacenamiento: Configure XenMobile para que apunte a los recursos compartidos de red y a las ubicaciones de SharePoint definidas en los conectores de zonas de almacenamiento.
Programa para la mejora de la experiencia	Para XenMobile Server local. Inicia o cancela el envío de estadísticas e información de uso anónimas a Citrix.
Microsoft Azure	Para XenMobile Server local. Integra XenMobile en Microsoft Azure.
Android Enterprise	Configura parámetros de servidor Android Enterprise.
Proveedor de identidades (IDP)	Configura un proveedor de identidades.
XenMobile Tools	Accede a la página XenMobile Tools.
Configuración de SNMP	Habilita SNMP para los nodos de XenMobile Server. Modifique o agregue usuarios de supervisión, configure el SNMP Manager donde aparecen las notificaciones de captura y configure los intervalos y umbrales de captura.

Asistencia

Los administradores pueden llevar a cabo varias tareas de asistencia.

Comprobaciones de conectividad de Citrix Gateway	Realiza varias comprobaciones de conectividad de Citrix Gateway mediante la dirección IP. Requiere nombre de usuario y contraseña.
Comprobaciones de conectividad de XenMobile	Realiza comprobaciones de conectividad de funciones seleccionadas de XenMobile (como la base de datos, DNS o Google Plan).
Crear paquetes de asistencia	Para XenMobile Server local. Crea un archivo a enviar a la asistencia de Citrix para solucionar problemas. Ese archivo contiene información del sistema, registros, información de base de datos, información básica, archivos de seguimiento y la información más reciente sobre la configuración de XenMobile o Citrix Gateway.
Documentación sobre los productos Citrix	Accede al sitio público de documentación de Citrix XenMobile.
Citrix Knowledge Center	Accede al sitio de asistencia de Citrix para buscar artículos de la base de conocimientos.
Registros	Accede y analiza datos de archivos de registros para la depuración, la auditoría de administradores y la auditoría de usuarios.
Información de clústeres	Para XenMobile Server local. Accede a información sobre cada uno de los nodos de un entorno en clústeres.
Recolección de elementos no utilizados	Para XenMobile Server local. Accede a información sobre objetos de la memoria que ya no se utilizan.
Propiedades de memoria de Java	Para XenMobile Server local. Accede a la instantánea del uso, los datos y los bloques de memoria de Java.

Macros	Rellena datos de dispositivo o usuario en el campo de texto de un perfil, directiva, notificación o plantilla de inscripción. Configure una sola directiva e impleméntela en una gran base de usuarios. Así, obtendrá valores específicos para cada usuario de destino.
Configuración de PKI	Importa y exporta información de la configuración de PKI.
Utilidad de firma APNS	Envía una solicitud de certificados de firma Apple Push Network (APNs) o carga un certificado APNs de Secure Mail para iOS.
Citrix Insight Services	Carga registros en Citrix Insight Services (CIS) para obtener asistencia con diferentes problemas.
Estado del dispositivo del conector de Citrix Gateway para Exchange ActiveSync	Consulta a XenMobile el estado de un dispositivo según se ha enviado al conector de Citrix Gateway para Exchange ActiveSync en función del ID de ActiveSync del dispositivo.
Anonimización y reidentificación	Para XenMobile Server local. 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 **Asistencia > Anonimización y reidentificación**, en el apartado **Avanzado**.
Parámetros de registros	Personaliza el nivel de registro o agrega un registrador personalizado.

Restringir acceso de grupos

Los usuarios administradores pueden aplicar permisos a todos los grupos de usuarios.

Rol de aprovisionamiento de dispositivos

> **Importante:**
>
> El rol de aprovisionamiento de dispositivos solo se aplica a dispositivos Windows CE.

Los usuarios con el rol predefinido de Aprovisionamiento de dispositivos tienen acceso limitado a las funciones de la consola. De forma predeterminada, su permiso está configurado para todos los grupos de usuarios y no pueden cambiar este parámetro.

Funciones de consola

Los usuarios con el rol de aprovisionamiento de dispositivos tienen restringido el acceso a las siguientes funciones de la consola de XenMobile. De forma predeterminada, cada una de las siguientes funciones está habilitada.

Dispositivos

Modificar dispositivo	Modifica los parámetros de un dispositivo.
Agregar o quitar dispositivo	Agrega o quita dispositivos de XenMobile.

Parámetros

Los usuarios con el rol de aprovisionamiento de dispositivos pueden acceder a la página **Parámetros**, pero no tienen los derechos necesarios para configurar las funciones.

Rol de asistencia

Los usuarios con el rol de asistencia tienen acceso a la asistencia remota. Sus permisos se aplican a todos los usuarios de forma predeterminada y no pueden modificar este parámetro.

Rol de usuario

Los usuarios con el rol de usuario tienen el siguiente acceso limitado a XenMobile.

Acceso autorizado

Self Help Portal	Los usuarios tienen acceso solo al portal Self-Help Portal en XenMobile.

Funciones de consola

Los usuarios tienen el siguiente acceso restringido a la consola de XenMobile.

Dispositivos

Borrado completo de dispositivo	Borra todos los datos y aplicaciones de un dispositivo, incluidas las tarjetas de memoria (si el dispositivo las tuviera).
Borrado selectivo de dispositivo	Borra todas las aplicaciones y datos empresariales del dispositivo, pero no afecta a las aplicaciones y datos personales.
Ver ubicaciones	Muestra la ubicación y establece restricciones geográficas en el dispositivo. Incluía: Localizar dispositivos (ver la ubicación de un dispositivo) y Seguimiento de dispositivos (realizar el seguimiento de la ubicación de un dispositivo a lo largo del tiempo).
Bloquear dispositivo	Bloquea remotamente un dispositivo de modo que no se pueda usar.
Desbloquear dispositivo	Desbloquea remotamente un dispositivo de modo que se pueda usar.
Bloquear contenedor	Bloquea remotamente el contenedor de datos empresariales de un dispositivo.
Desbloquear contenedor	Desbloquea remotamente el contenedor de datos empresariales de un dispositivo.
Restablecer contraseña de contenedor	Restablece la contraseña del contenedor de datos empresariales.

Habilitar omisión de bloqueo de activación de DEP ASM	En un dispositivo iOS supervisado, almacena un código de circunvalación cuando habilite el Bloqueo de activación. Si necesita borrar el dispositivo, use este código para quitar automáticamente el Bloqueo de activación.
Hacer sonar el dispositivo	Hace sonar remotamente un dispositivo Windows al máximo volumen durante 5 minutos.
Reiniciar el dispositivo	Reinicia un dispositivo Windows.
Ver inventario de software	Muestra el software instalado en un dispositivo.

Inscripción

Agregar o eliminar inscripción	Agrega o quita una invitación de inscripción a usuarios o grupos de usuarios.
Notificar al usuario	Envía una invitación de inscripción a usuarios o grupos de usuarios.

Restringir acceso de grupos

En el caso de los cuatro roles predefinidos, este permiso está configurado de forma predeterminada y puede aplicarse a todos los grupos de usuarios. No se puede modificar el rol.

Configurar roles con RBAC

En XenMobile, la función del control de acceso por roles (RBAC) permite asignar roles predefinidos o conjuntos de permisos a usuarios y grupos. Con estos permisos, se puede controlar el nivel de acceso de los usuarios a las funciones del sistema.

XenMobile implementa cuatro roles de usuario predeterminados para separar de manera lógica el acceso a las funciones del sistema:

- **Administrador:** Concede acceso completo al sistema.

- **Aprovisionamiento de dispositivos:** Concede acceso a tareas básicas de administración de dispositivos para dispositivos Windows CE.
- **Asistencia:** Concede acceso para la asistencia remota.
- **Usuario:** Rol utilizado por los usuarios que pueden inscribir dispositivos y acceder al portal Self-Help Portal.

También puede usar los roles predeterminados como plantillas base para personalizarlas y crear roles de usuario. Puede asignar permisos de roles para acceder a funciones específicas del sistema, además de las definidas para los 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. Supongamos, por ejemplo, que los usuarios del grupo A de Active Directory pueden localizar dispositivos de administradores y que los usuarios del grupo B de Active Directory pueden borrar dispositivos de empleados. En ese caso, un usuario que pertenezca a ambos grupos puede localizar y borrar dispositivos de administradores y 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:

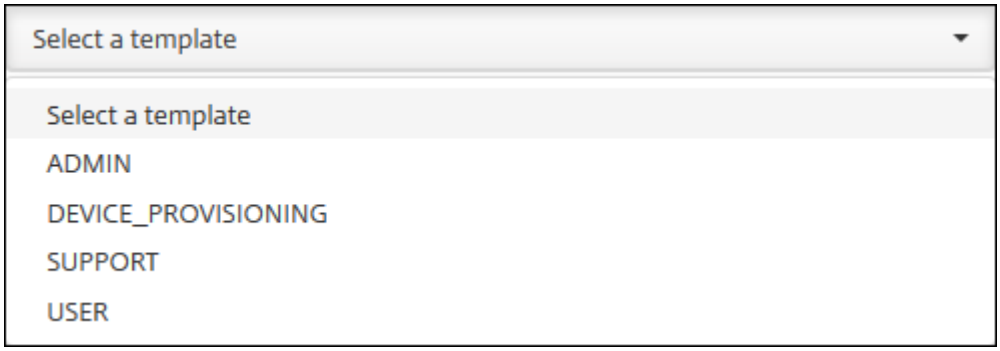
- Crear un rol.
- Agregar grupos a un rol.
- Asociar usuarios locales a roles.

1. En la consola de XenMobile, vaya a **Parámetros > Control de acceso basado en roles**. Aparecerá la página **Control de acceso basado en roles** con los cuatro roles de usuario predeterminados, además de los roles que haya agregado antes.

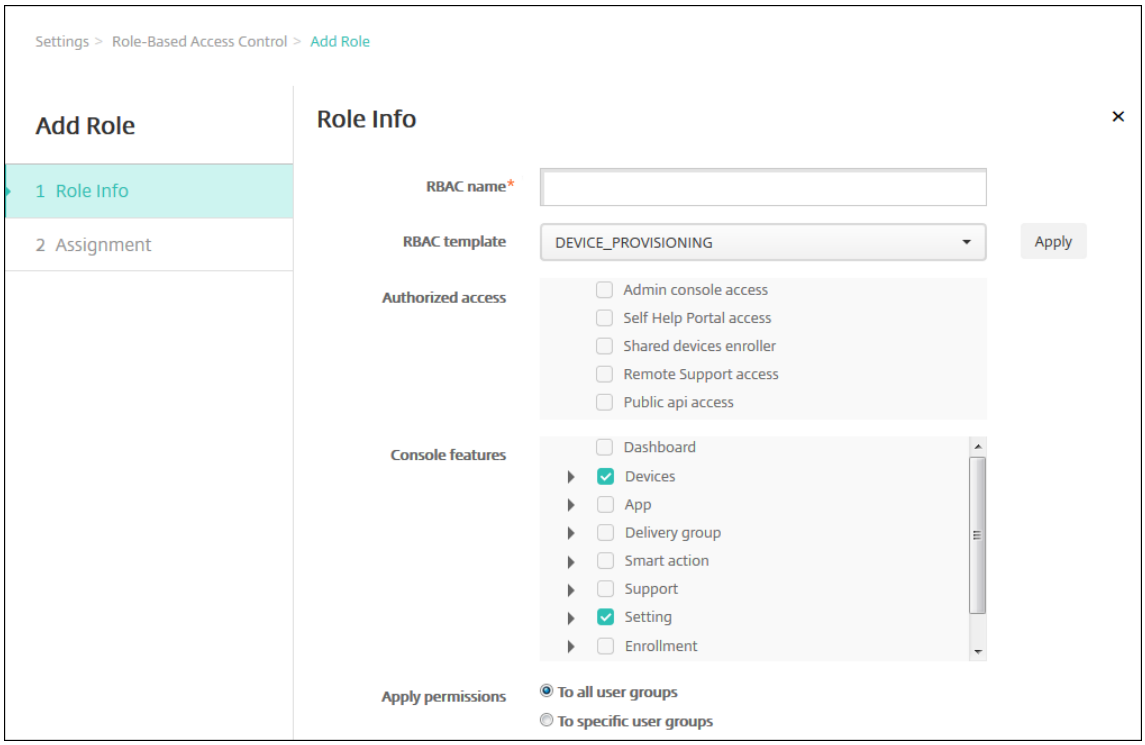
Si hace clic en el signo más (+) situado junto a un rol, ese rol se expande para mostrar todos los permisos que se le han concedido, tal y como se muestra en la siguiente ilustración.

2. Haga clic en **Agregar** para agregar un rol de usuario. Para modificar el rol, haga clic en el icono del lápiz situado a la derecha de un rol existente. Para eliminar el rol, haga clic en el icono de papelera situado a la derecha de un rol. No se pueden eliminar los roles de usuario predeterminados.
    - Si hace clic en **Agregar** o en el icono de lápiz, aparecerán la página **Agregar rol** o la página **Modificar rol**.
    - Si hace clic en el icono de papelera, aparecerá un diálogo de confirmación. Haga clic en **Eliminar** para quitar el rol seleccionado.
3. Escriba la siguiente información para crear o para modificar un rol de usuario:
    - **Nombre de RBAC:** Indique un nombre descriptivo para el nuevo rol de usuario. No se puede cambiar el nombre de un rol existente.
    - **Plantilla de RBAC:** 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 de 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 **Acceso autorizado** y **Funciones de consola**. El uso de una plantilla es opcional. Puede seleccionar directamente las opciones que quiera asignar a un rol en los campos **Acceso autorizado** y **Funciones de consola**.



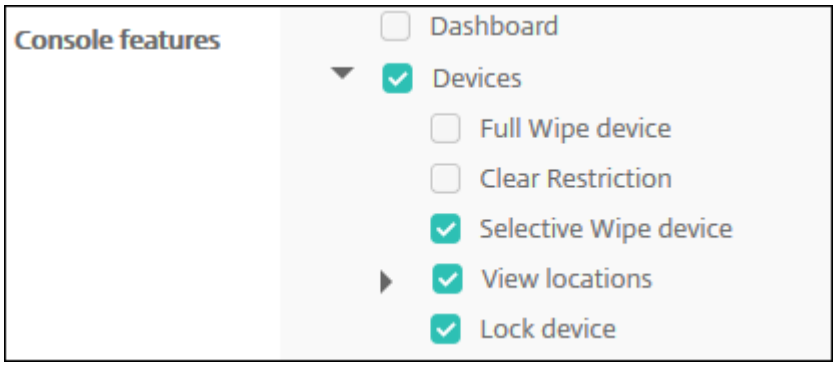
4. Haga clic en **Aplicar**, junto al campo **Plantilla de RBAC**, para rellenar las casillas **Acceso autorizado** y **Funciones de consola** con los permisos de funciones y acceso predefinidos.



5. Marque y desmarque las casillas de verificación de **Acceso autorizado** y **Funciones de consola** para personalizar el rol.

   Si hace clic en el triángulo situado junto a “Funciones de consola”, aparecerán los permisos específicos de esa función y puede marcarlos o desmarcarlos. Al hacer clic en la casilla de nivel superior, se prohíbe el acceso a esa área de la consola. Seleccione opciones individualmente bajo el nivel superior para habilitar esas opciones. Por ejemplo, en la siguiente figura, las op-

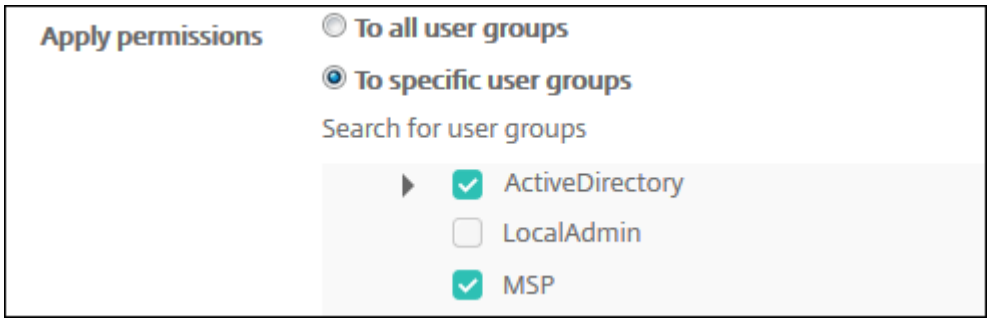
ciones de **Borrado completo del dispositivo** y **Desactivar restricciones** no aparecen para los usuarios asignados al rol. Aparecen las opciones marcadas.



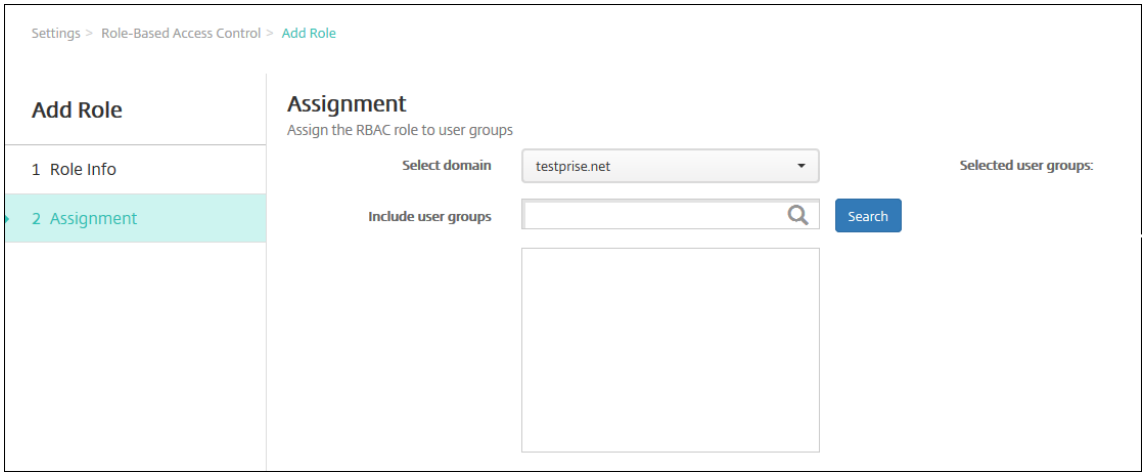
6. **Aplicar permisos:** seleccione uno o varios grupos de usuarios para limitar los grupos que puede administrar el administrador. Si hace clic en **Para grupos de usuarios específicos**, aparecerá una lista de grupos. De esa lista, puede seleccionar un grupo o varios.

   Por ejemplo, si un administrador RBAC tiene permisos para acceder a los grupos de usuarios de ActiveDirectory y MSP:

   - El administrador solo tiene acceso a la información de los usuarios que se encuentran en el grupo ActiveDirectory, el grupo MSP o ambos grupos.
   - El administrador no puede ver ningún otro usuario local o de AD. El administrador puede ver la información de los usuarios que sean miembros de grupos secundarios de cualquiera de esos grupos.
   - El administrador puede enviar invitaciones a:
     - los grupos de permisos y sus grupos secundarios
     - los usuarios que son miembros de grupos de permisos y sus grupos secundarios

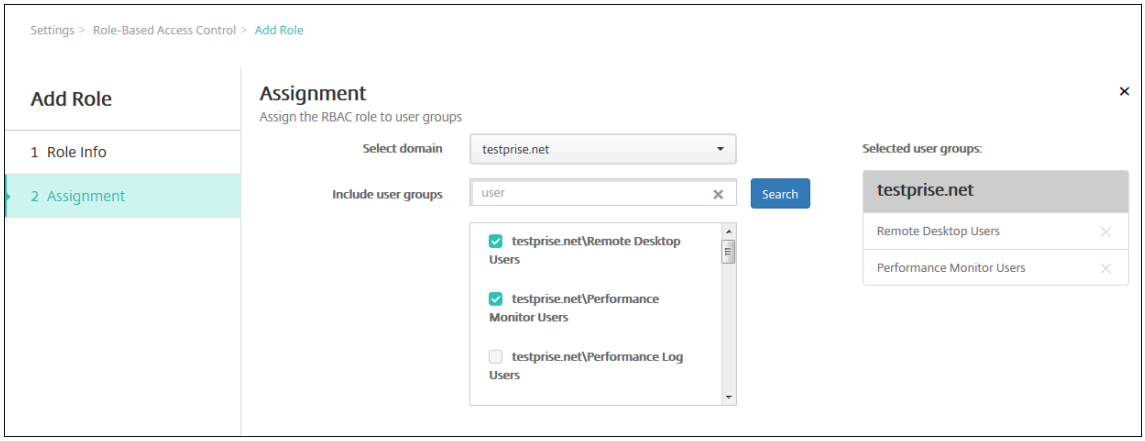


7. Haga clic en **Siguiente**. Aparecerá la página **Asignación**.



8. Escriba la siguiente información para asignar el rol a los grupos de usuarios.

   - **Seleccionar dominio:** En la lista, haga clic en un dominio.
   - **Incluir grupos de usuarios:** Haga clic en “Buscar” 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 **Grupos de usuarios seleccionados**.



> **Nota:**
>
> Para quitar un grupo de usuarios de la lista **Grupos de usuarios seleccionados**, haga clic en la “X” situada junto al nombre del grupo de usuarios.

9. Haga clic en **Guardar**.

Notificaciones

January 4, 2022

Puede utilizar notificaciones en XenMobile para los siguientes propósitos:

- Comunicarse con grupos específicos de usuarios para ciertas funciones relacionadas con el sistema. También puede destinar estas notificaciones a ciertos usuarios. Por ejemplo, usuarios con dispositivos iOS, usuarios cuyos dispositivos no cumplen los requisitos de cumplimiento o usuarios con dispositivos que son propiedad de los empleados, entre otros.
- Inscribir usuarios y sus dispositivos.
- Para notificar automáticamente a los usuarios (mediante acciones automatizadas) cuando se den ciertas condiciones. Por ejemplo:
  - Cuando un dispositivo de usuario está a punto de ser bloqueado del dominio corporativo debido a un problema de cumplimiento.
  - Cuando el dispositivo ha sido liberado por jailbreak o 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 del 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.

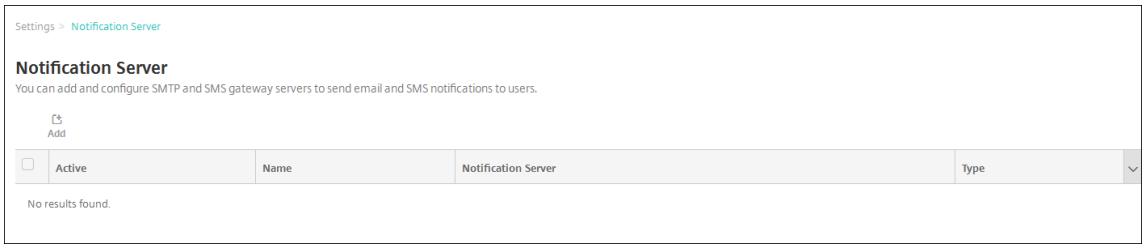
En XenMobile, también puede establecer una puerta de enlace SMS de operador y, así, configurar las notificaciones que se envían a través de la puerta de enlace SMS de un operador. Los operadores utilizan las puertas de enlace SMS para enviar transmisiones SMS a una red de telecomunicaciones o recibir 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.

Requisitos previos

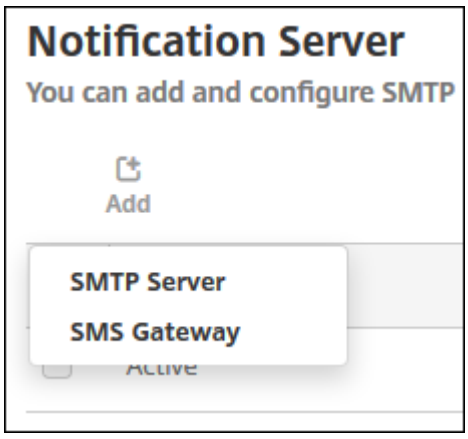
- Antes de configurar la puerta de enlace SMS, acuda al administrador del sistema para obtener la información del servidor. Es importante saber si el servidor SMS está alojado en un servidor interno de la empresa o si el servidor forma parte de un servicio de correo electrónico alojado. En ese caso, necesita información procedente del sitio web del proveedor del servicio.
- Configure 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 correspondiente en el sitio web del proveedor del servicio.
- Puede utilizar un servidor SMTP activo y un servidor SMS activo simultáneamente. Ambos canales de comunicación permiten una configuración activa.
- Debe abrir el puerto 25 desde XenMobile (ubicado en la zona DMZ de la red) para apuntarlo al servidor SMTP de la red interna. Esto permite que XenMobile envíe correctamente las notificaciones.

Configurar un servidor SMTP y una puerta de enlace SMS

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 **Parámetros**.
2. En **Notificaciones**, haga clic en **Servidor de notificaciones**. Aparecerá la página **Servidor de notificaciones**.

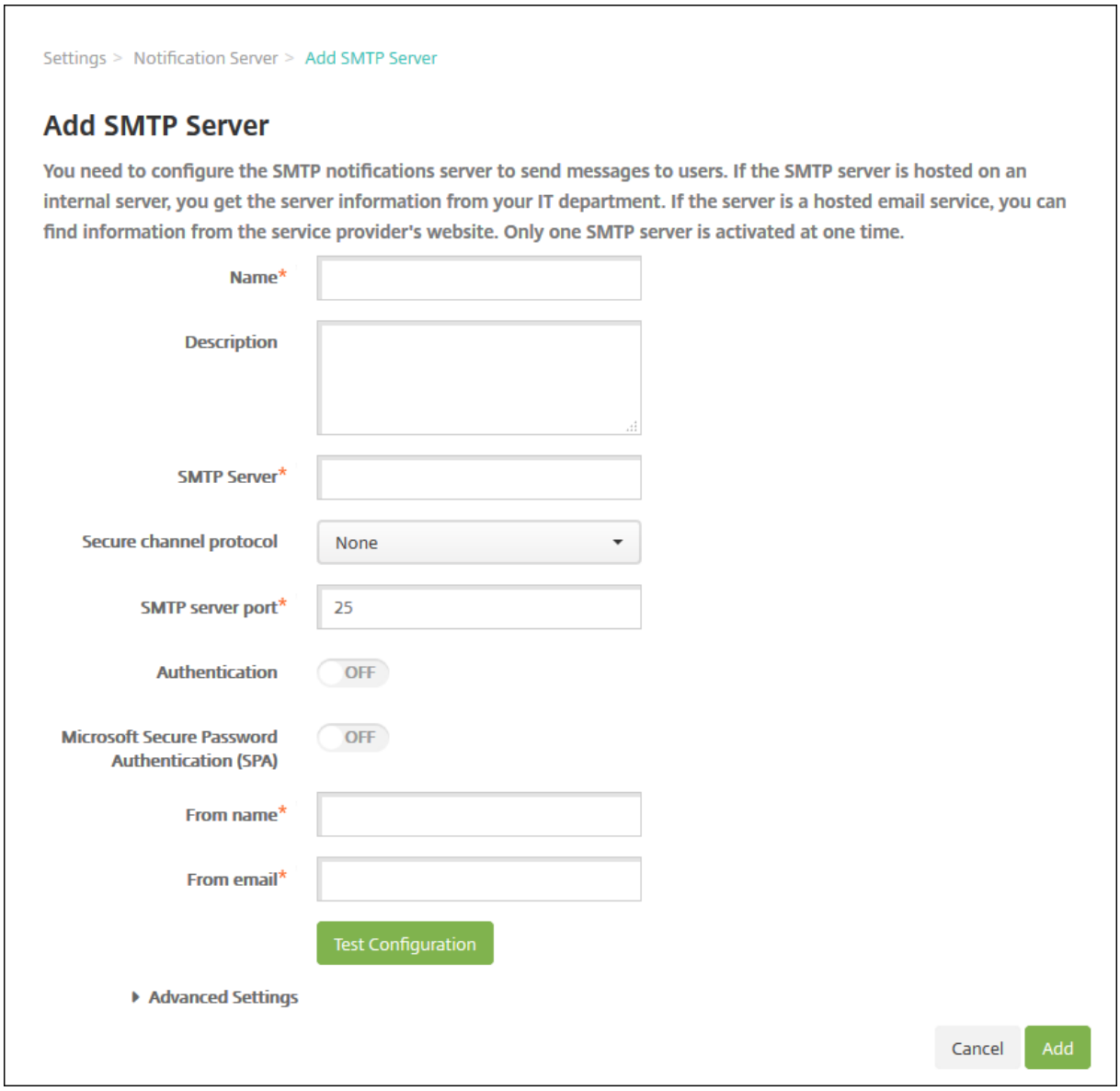


3. Haga clic en **Agregar**. Aparecerá un menú con las opciones para configurar un servidor SMTP o una puerta de enlace SMS.



- Para agregar un servidor SMTP, haga clic en **Servidor SMTP**. A continuación, consulte Agregar un servidor SMTP para ver los pasos que se deben seguir para configurar este parámetro.
- Para agregar una puerta de enlace SMS, haga clic en **Puerta de enlace SMS**. A continuación, consulte Agregar una puerta de enlace SMS para ver los pasos que se deben seguir para configurar este parámetro.

Agregar un servidor SMTP



1. Configure estos parámetros:

   - **Nombre:** Escriba el nombre asociado a esta cuenta del servidor SMTP.
   - **Descripción:** Si quiere, introduzca una descripción del servidor.
   - **Servidor SMTP:** Escriba el nombre de host del servidor. El nombre de host puede ser una dirección IP o un nombre de dominio completo (FQDN).
   - **Protocolo de canal seguro:** En la lista, haga clic en **SSL**, **TLS** o **Ninguno** 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 **Ninguno**.
   - **Puerto del servidor SMTP:** 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.

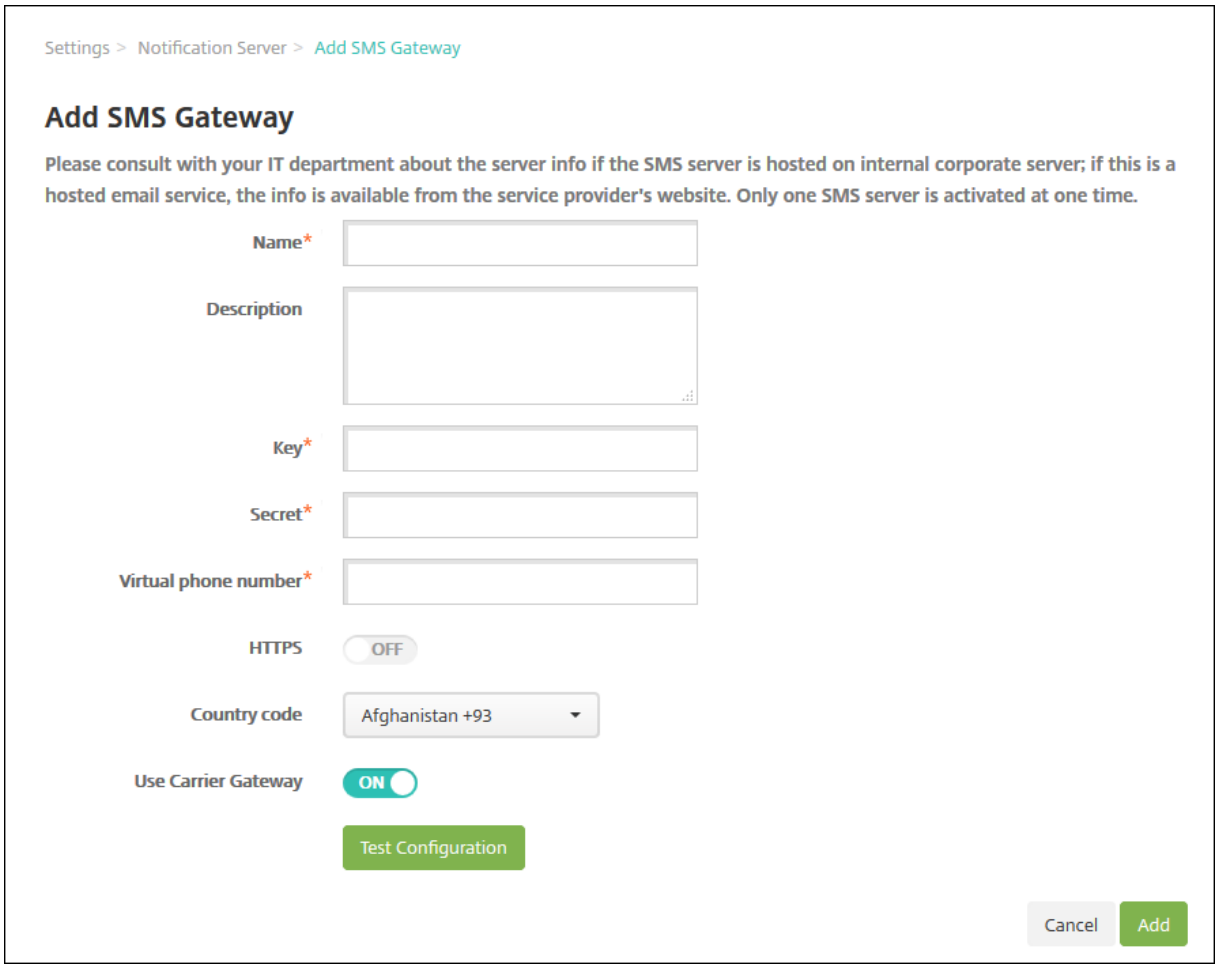
- **Autenticación:** Seleccione **Sí** o **No**. Está **desactivado** de forma predeterminada.
- Si habilita **Authentication**, configure los siguientes parámetros:
  - **Nombre de usuario:** Escriba el nombre de usuario que se usará para la autenticación.
  - **Contraseña:** Escriba la contraseña de autenticación del usuario.
- **Autenticación de contraseña segura (SPA) de Microsoft:** Si el servidor SMTP usa la autenticación SPA, haga clic en **Sí**. Está **desactivado** de forma predeterminada.
- **Nombre de remitente:** Escriba el nombre que aparece en el cuadro **De** cuando un cliente recibe un correo electrónico de notificación procedente de este servidor. Por ejemplo, Departamento de TI de la empresa.
- **Correo electrónico de remitente:** 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 **Probar configuración** para enviar una notificación de prueba por correo electrónico.
3. Expanda **Parámetros avanzados** y, a continuación, configure estos parámetros:

   - **Cantidad de reintentos de SMTP:** Escriba la cantidad de veces que se intentará volver a enviar un mensaje fallido enviado desde el servidor SMTP. El valor predeterminado es 5.
   - **Tiempo de espera de SMTP:** Escriba la duración del tiempo de espera (en segundos) al enviar una solicitud SMTP. Aumente este valor si el envío de mensajes falla continuamente debido a los tiempos de espera. Tenga cuidado al reducir este número, porque podría aumentar la cantidad de mensajes sin entregar y de mensajes cuyo tiempo de espera se ha agotado. De forma predeterminada, es de 30 segundos.
   - **Número máximo de destinatarios de SMTP:** 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 **Agregar**.

Agregar una puerta de enlace SMS



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:
   - **Nombre:** Escriba un nombre para la configuración de la puerta de enlace SMS. Este campo es obligatorio.
   - **Descripción:** Si quiere, escriba una descripción de la configuración.
   - **Clave:** Escriba el identificador numérico proporcionado por el administrador del sistema para la activación de la cuenta. Este campo es obligatorio.
   - **Secreto:** 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.
   - **Número de teléfono virtual:** 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. Está **desactivado** de forma predeterminada.

> **Importante:**
>
> Deje "HTTPS" **activado**, a menos que reciba instrucciones de Citrix Support para **desactivarlo**.

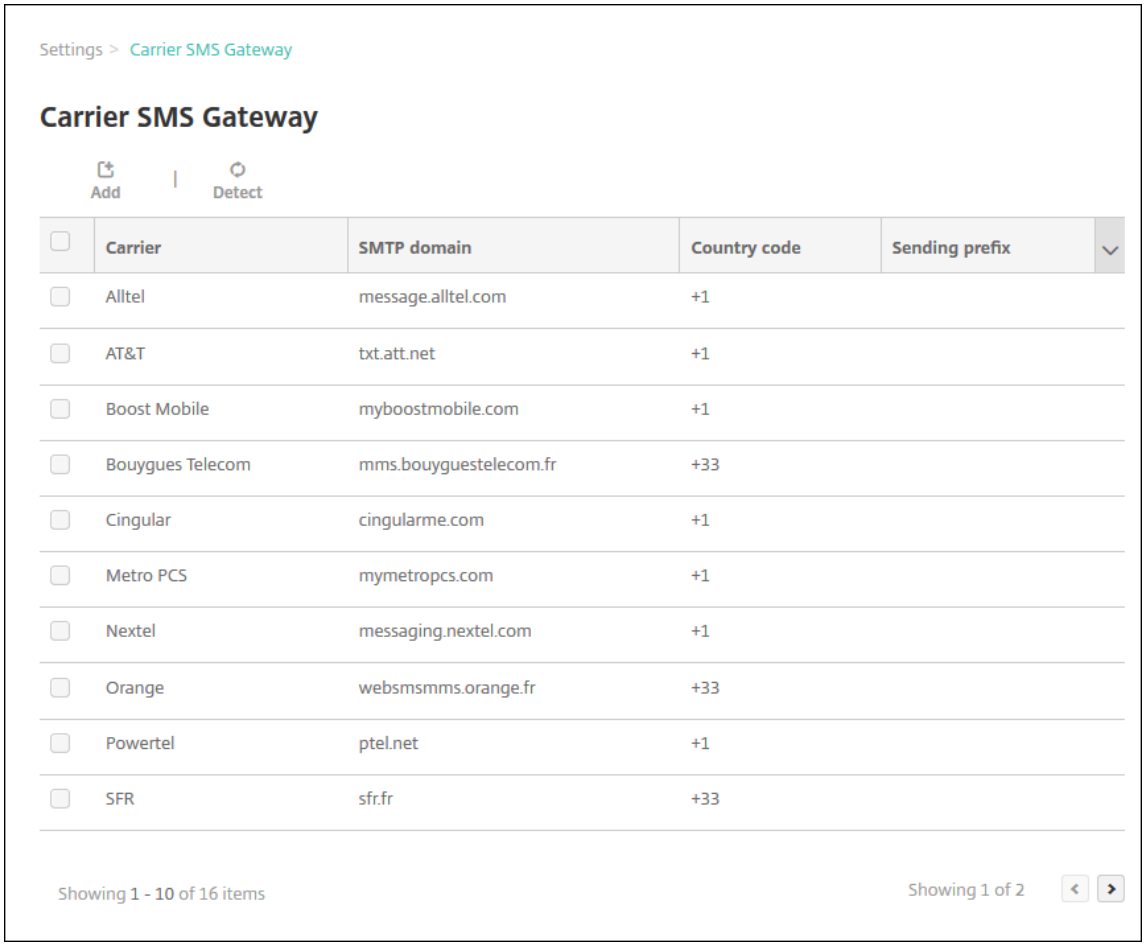
- **Código de país:** En la lista, haga clic en el prefijo predeterminado del código del país para mensajes SMS de los destinatarios de su organización. Este campo siempre comienza con un símbolo +. El valor predeterminado es **Afganistán +93**.

2. Haga clic en **Probar configuración** para enviar un mensaje de prueba mediante 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.
3. Haga clic en **Agregar**.

Agregar una puerta de enlace SMS del operador

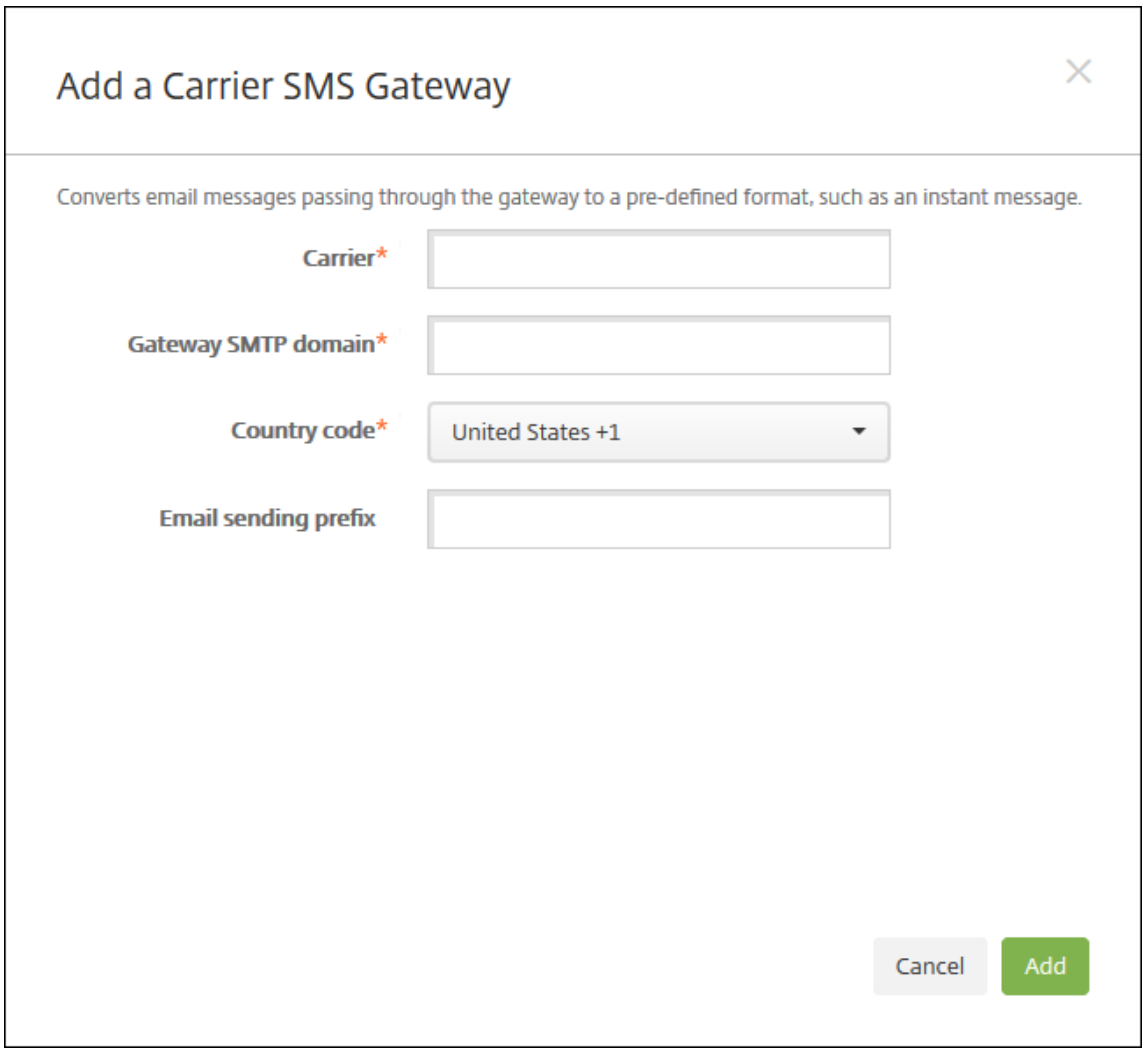
En XenMobile, puede establecer una puerta de enlace SMS de operador y, así, configurar las notificaciones que se envían a través de la puerta de enlace SMS de un operador. Los operadores utilizan las puertas de enlace Short Message Service (SMS) para enviar transmisiones SMS a una red de telecomunicaciones 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 **Parámetros**.
2. En **Notificaciones**, haga clic en **Puerta de enlace SMS del operador**. Se abrirá la página **Puerta de enlace SMS del operador**.



3. Lleve a cabo una de las siguientes acciones:

   - Haga clic en **Detectar** 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 **Agregar puerta de enlace SMS de operador**.



> **Nota:**
>
> XenMobile solo admite el envío de mensajes SMS de Nexmo. Si aún no tiene una cuenta para usar la mensajería de Nexmo, visite su sitio Web para crear una.

4. Configure estos parámetros:
   - **Operador:** Escriba el nombre del operador.
   - **Dominio SMTP de puerta de enlace:** Escriba el dominio asociado a la puerta de enlace SMTP.
   - **Código de país:** En la lista, haga clic en el código del país del operador.
   - **Prefijo de envío de correo electrónico:** Si lo prefiere, puede especificar un prefijo de envío para el correo electrónico.
5. Haga clic en **Agregar** para agregar el nuevo operador, o bien haga clic en **Cancelar** para no agregarlo.

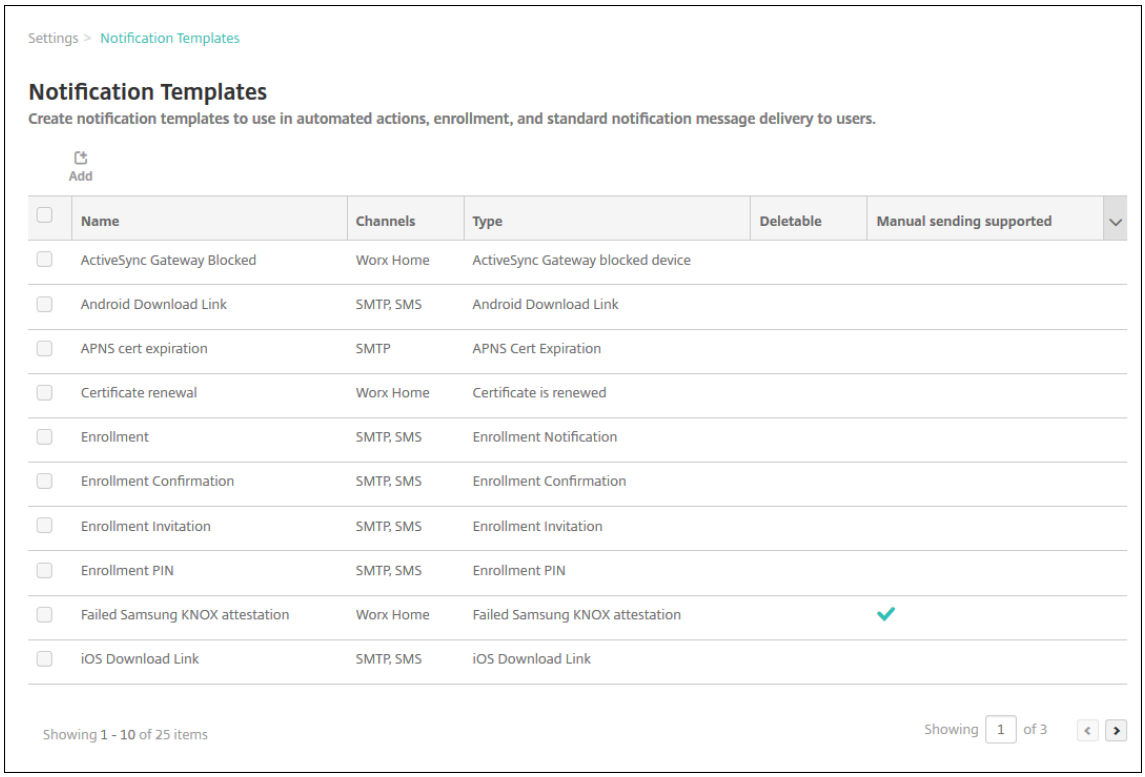
Crear y actualizar plantillas de notificaciones

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 con 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 **Parámetros**.
2. Haga clic en **Plantillas de notificaciones**. Aparecerá la página **Plantillas de notificaciones**.



Agregar una plantilla de notificaciones

1. Haga clic en **Agregar**. 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 **Servidor de notificaciones**, en la página **Parámetros**. Después de configurar los canales que se van a utilizar, puede volver a la página **Plantillas de notificaciones** para continuar agregando o modificando plantillas de notificaciones.

   > **Importante:**
   >
   > Si elige configurar el servidor SMTP o SMS más tarde, no podrá activar esos canales cuando agregue o modifique una plantilla de notificaciones, lo que significa que esos canales no estarán disponibles para el envío de notificaciones de usuario.

2. Configure estos parámetros:

   - **Nombre:** Escriba un nombre descriptivo para la plantilla.
   - **Descripción:** Escriba una descripción para la plantilla.
   - **Tipo:** 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 de certificados APNS, que es la plantilla predefinida. Esto significa que no se puede agregar una nueva plantilla de este tipo.

   > **Nota:**
   >
   > En algunos tipos de plantilla, aparece la frase “Se admite el envío manual” debajo del tipo. Lo que significa que la plantilla está disponible en la lista **Notificaciones** del **Panel de mandos** y en la página **Dispositivos** 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 “Asunto” o “Mensaje”:

   - ${outofcompliance.reason(whitelist_blacklist_apps_name)}

     > **Nota:**
     >
     > La consola de XenMobile Server contiene los términos “lista negra” y “lista blanca”. Estamos cambiando esos términos en una próxima versión a “lista de bloqueados” y “lista de permitidos”.

   - ${outofcompliance.reason(smg_block)}

3. En **Canales**, indique la información de cada canal que se va a utilizar para esta notificación. Puede elegir un canal cualquiera o todos. Los canales que seleccione dependen de la forma en que quiera enviar notificaciones:

- Si elige **Secure Hub**, solo los dispositivos iOS y Android recibirán las notificaciones, que aparecerán en la bandeja de notificaciones de los dispositivos en cuestión.
- Si elige **SMTP**, la mayoría de los usuarios deberían recibir el mensaje porque se habrán inscrito con sus direcciones de correo electrónico.
- Si elige **SMS**, solo los usuarios con dispositivos dotados de una tarjeta SIM recibirán las notificaciones.

Secure Hub:

- **Activar:** Haga clic para habilitar el canal de notificación.
- **Mensaje:** Escriba el mensaje que se enviará al usuario. Este campo es necesario si usa Secure Hub. Para obtener información sobre cómo usar las macros, consulte Macros.
- **Archivo de sonido:** Seleccione el sonido de notificación que oirá el usuario cuando reciba la notificación.

SMTP:

- **Activar:** Haga clic para habilitar el canal de notificación.

  Solo puede activar la notificación SMTP después de configurar el servidor SMTP.

- **Remitente:** Escriba un remitente optativo para la notificación, que puede consistir en un nombre, una dirección de correo electrónico o ambos.
- **Destinatario:** 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 **Administrar > Dispositivos** y enviar notificaciones desde allí. Para obtener más información, consulte Dispositivos.
- **Asunto:** Escriba un asunto descriptivo para la notificación. Este campo es obligatorio.
- **Mensaje:** Escriba el mensaje que se enviará al usuario. Para obtener información sobre cómo usar las macros, consulte Macros.

SMS:

- **Activar:** Haga clic para habilitar el canal de notificación.

  Solo puede activar la notificación SMTP después de configurar el servidor SMTP.

- **Destinatario:** 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 **Administrar > Dispositivos**.

- **Mensaje:** Escriba el mensaje que se enviará al usuario. Este campo es obligatorio. Para obtener información sobre cómo usar las macros, consulte Macros.

4. Haga clic en **Agregar**. Cuando todos los canales se hayan configurado correctamente, aparecen en este orden en la página **Plantillas de notificaciones**: SMTP, SMS y Secure Hub. Los canales configurados incorrectamente aparecen después de los canales configurados correctamente.

Modificar una plantilla de notificaciones

1. Seleccione una plantilla de notificaciones. Aparecerá la página de modificación de la plantilla en cuestión. En ella, podrá realizar cambios en todos los campos salvo en **Tipo**, además de activar o desactivar canales.
2. Haga clic en **Guardar**.

Eliminar una plantilla de notificaciones

Solo podrá eliminar las plantillas de notificación que usted haya agregado. No podrá eliminar las plantillas de notificación predefinidas.

1. Seleccione una plantilla de notificaciones existente.
2. Haga clic en **Delete**. Aparecerá un cuadro de diálogo de confirmación.
3. Haga clic en **Eliminar** para eliminar la plantilla de notificaciones o en **Cancelar** para cancelar la operación.

Dispositivos

January 4, 2022

Citrix XenMobile puede aprovisionar, proteger e inventariar una amplia gama de tipos de dispositivo desde una sola consola de administración.

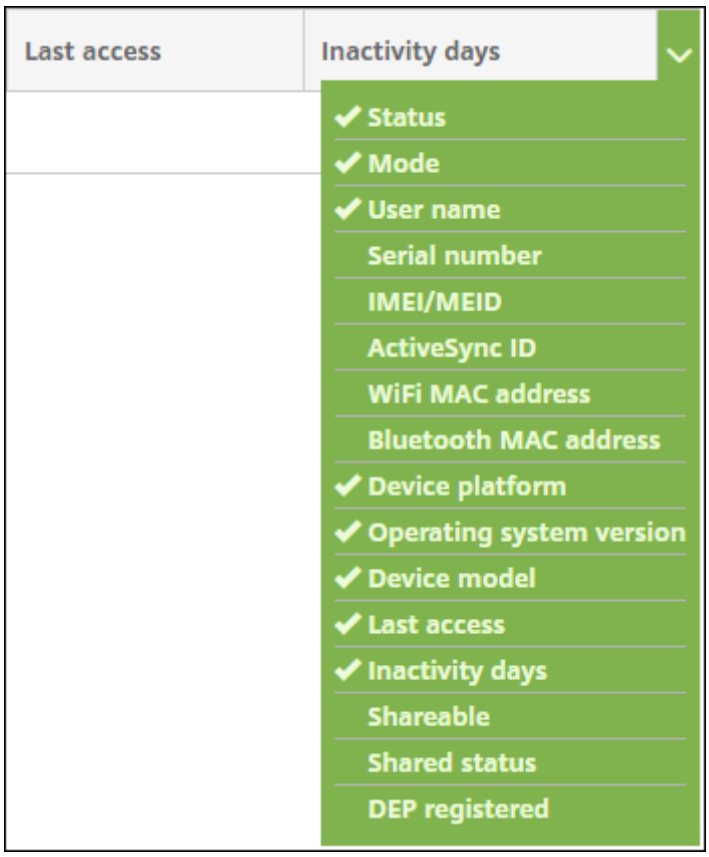
La base de datos del servidor de XenMobile almacena una lista de dispositivos móviles. Cada dispositivo móvil está definido por un número de serie exclusivo o una identificación International Mobile Station Equipment Identity (IMEI) o Mobile Equipment Identifier (MEID). Para rellenar la consola de XenMobile 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 más adelante en este artículo.

En la página **Dispositivos** de la consola de XenMobile, se ofrece una lista de cada dispositivo y la siguiente información:

- **Estado** (Los iconos indican el estado de implementación, si está administrado, si ha sido liberado por jailbreak y si ActiveSync Gateway está disponible)
- **Modo** (Si el modo del dispositivo es MDM, MAM o ambos)
- Se ofrece otra información del dispositivo, como **Nombre de usuario**, **Plataforma del dispositivo**, **Versión del sistema operativo**, **Modelo de dispositivo**, **Último acceso** y **Días de inactividad**. Estos son los encabezados predeterminados que aparecen.

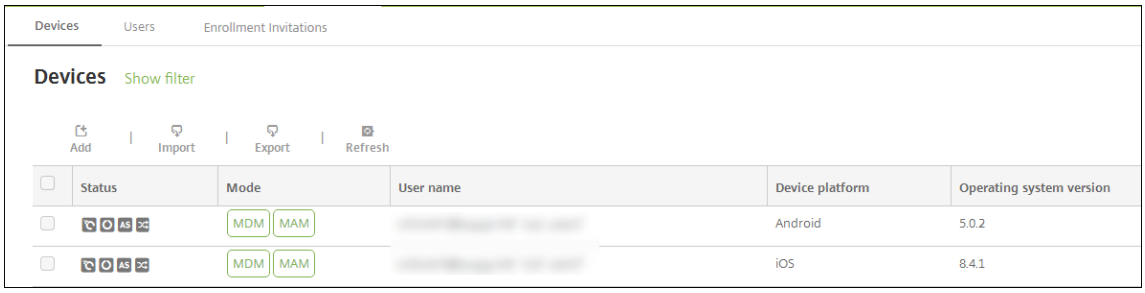
Para personalizar la tabla **Dispositivos**, haga clic en la flecha hacia abajo en el último encabezado. A continuación, seleccione los encabezados adicionales que desea mostrar en la tabla o borre los que quiera quitar.



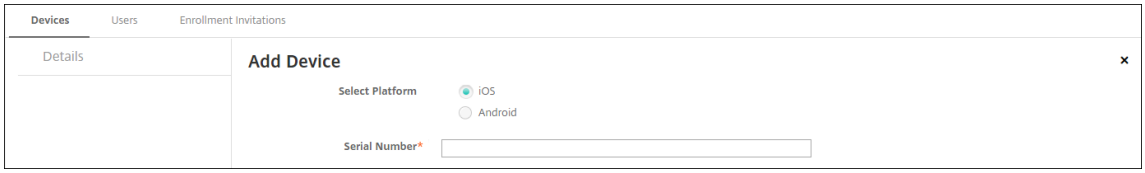
Puede agregar dispositivos manualmente, importarlos desde un archivo de aprovisionamiento, modificar los datos de los dispositivos, realizar acciones para aumentar la seguridad en ellos y enviarles notificaciones. También puede exportar todos los datos de la tabla de dispositivos a un archivo CSV para generar un informe personalizado. El servidor exporta todos los atributos de dispositivo. Si se aplican filtros, XenMobile los tendrá en cuenta al crear el archivo CSV.

Agregar manualmente un dispositivo

1. En la consola de XenMobile, haga clic en **Administrar > Dispositivos**. Aparecerá la página **Dispositivos**.



2. Haga clic en **Agregar**. Aparecerá la página **Agregar dispositivo**.



3. Configure estos parámetros:

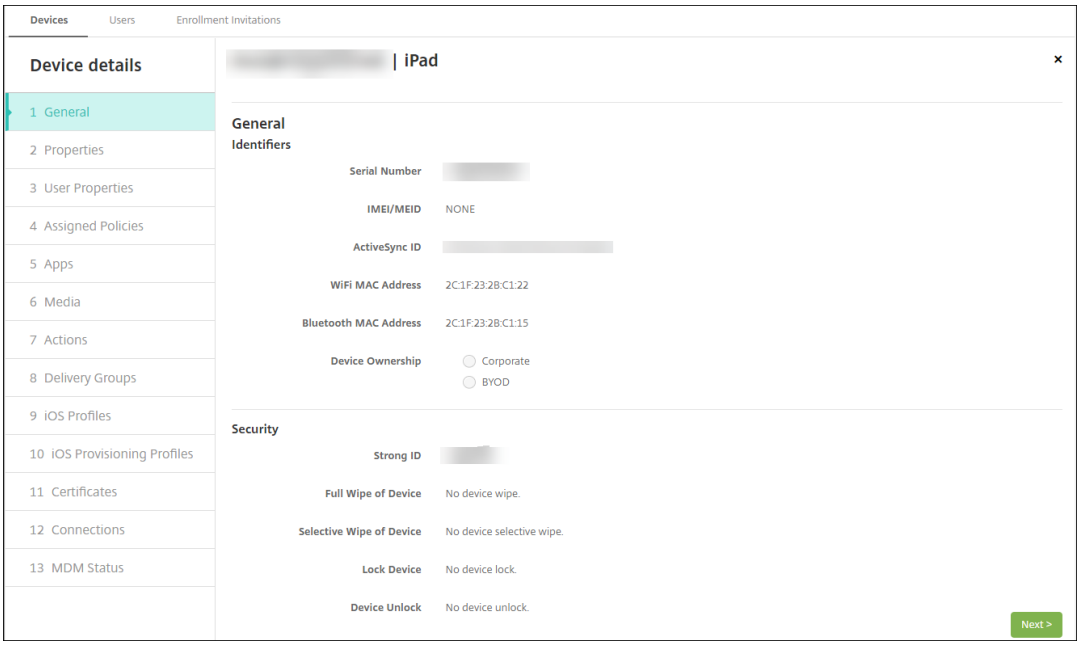
   - **Seleccionar plataforma:** Haga clic en **iOS** o **Android**.
   - **Número de serie:** Escriba el número de serie del dispositivo.
   - **IMEI/MEID:** Solo para dispositivos Android, puede escribir información referente al identificador IMEI/MEID del dispositivo.

4. Haga clic en **Agregar**. La tabla **Dispositivos** aparecerá con el dispositivo agregado al final de la lista. Seleccione el dispositivo agregado y, a continuación, en el menú que aparecerá, haga clic en **Modificar** para ver y confirmar los detalles del dispositivo.

> **Nota:**
>
> Cuando se marca la casilla de verificación situada junto a un dispositivo, el menú de opciones aparece encima de la lista de dispositivos. Si hace clic en cualquier lugar de la lista, el menú de opciones aparece a la derecha de la lista.

   - XenMobile Server configurado en modo Enterprise (XME) o MDM
   - LDAP configurado
   - Si utiliza grupos y usuarios locales:
     - Uno o varios grupos locales.
     - Usuarios locales asignados a grupos locales.
     - Los grupos de entrega se asocian con grupos locales.
   - Si usa Active Directory:

- Los grupos de entrega se asocian con grupos de Active Directory.



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 **Propietario del dispositivo**, seleccione **Empresa** 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. El campo **Borrado completo del dispositivo** contiene el código PIN del usuario. El usuario debe introducir ese código después de que se haya borrado el dispositivo. Si el usuario no consigue recordar el código, usted puede buscarlo en “Detalles del dispositivo”.

6. La página **Propiedades** muestra una lista de las propiedades de 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 **Agregar** y, a continuación, seleccione una propiedad de la lista. Para saber cuáles son los valores válidos para cada propiedad, consulte el PDF Valores y nombres de propiedades de dispositivo.

   Cuando se agrega una propiedad, esta aparece inicialmente en la categoría donde se haya agregado. Después de hacer clic en **Siguiente** y volver a la página **Propiedades**, 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 **Detalles del dispositivo** contienen información resumida acerca del

dispositivo.

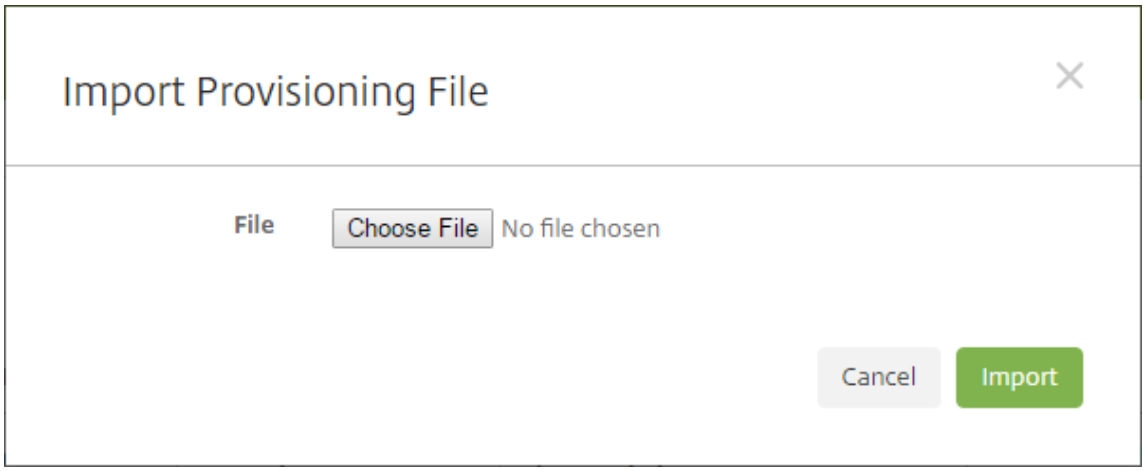
- **Propiedades de usuario:** Muestra los roles de RBAC, los miembros del grupo, las cuentas de compras por volumen y las propiedades del usuario. Puede retirar una cuenta de compras por volumen desde esta página.
- **Directivas asignadas:** Muestra la cantidad de directivas asignadas, incluidas las directivas implementadas, pendientes y fallidas. También muestra el nombre, el tipo y la última información implementada de cada directiva.
- **Aplicaciones:** Muestra la cantidad de implementaciones de aplicaciones instaladas, pendientes y erróneas según el último inventario. Indica el nombre de la aplicación, el identificador y el tipo, entre otros datos.
- **Multimedia:** Muestra la cantidad de implementaciones de archivos multimedia instalados, pendientes y erróneos según el último inventario.
- **Acciones:** Muestra la cantidad de acciones implementadas, pendientes y erróneas. Indica el nombre de la acción y la hora de la última implementación.
- **Grupos de entrega:** Muestra la cantidad de grupos de entrega en estado correcto, pendiente y fallido. 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).
- **Perfiles iOS:** Muestra el último inventario de perfiles iOS, que incluye el nombre, el tipo, la organización y la descripción.
- **Perfiles de aprovisionamiento de iOS:** 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).
- **Certificados:** 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.
- **Conexiones:** 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).
- **Estado de MDM:** Muestra información como el estado MDM, la hora del último envío push y la hora de la última respuesta del dispositivo.

Importar dispositivos desde un archivo de aprovisionamiento

Puede importar un archivo proporcionado por operadores de telefonía móvil o fabricantes de dispositivos móviles. También puede crear su propio archivo de aprovisionamiento de dispositivos. Para obtener más información, consulte Formatos del archivo de aprovisionamiento de dispositivos más adelante en este artículo.

1. Vaya a **Administrar > Dispositivos** y haga clic en **Importar**. Aparece el cuadro de diálogo **Im-**

portar archivo de aprovisionamiento.

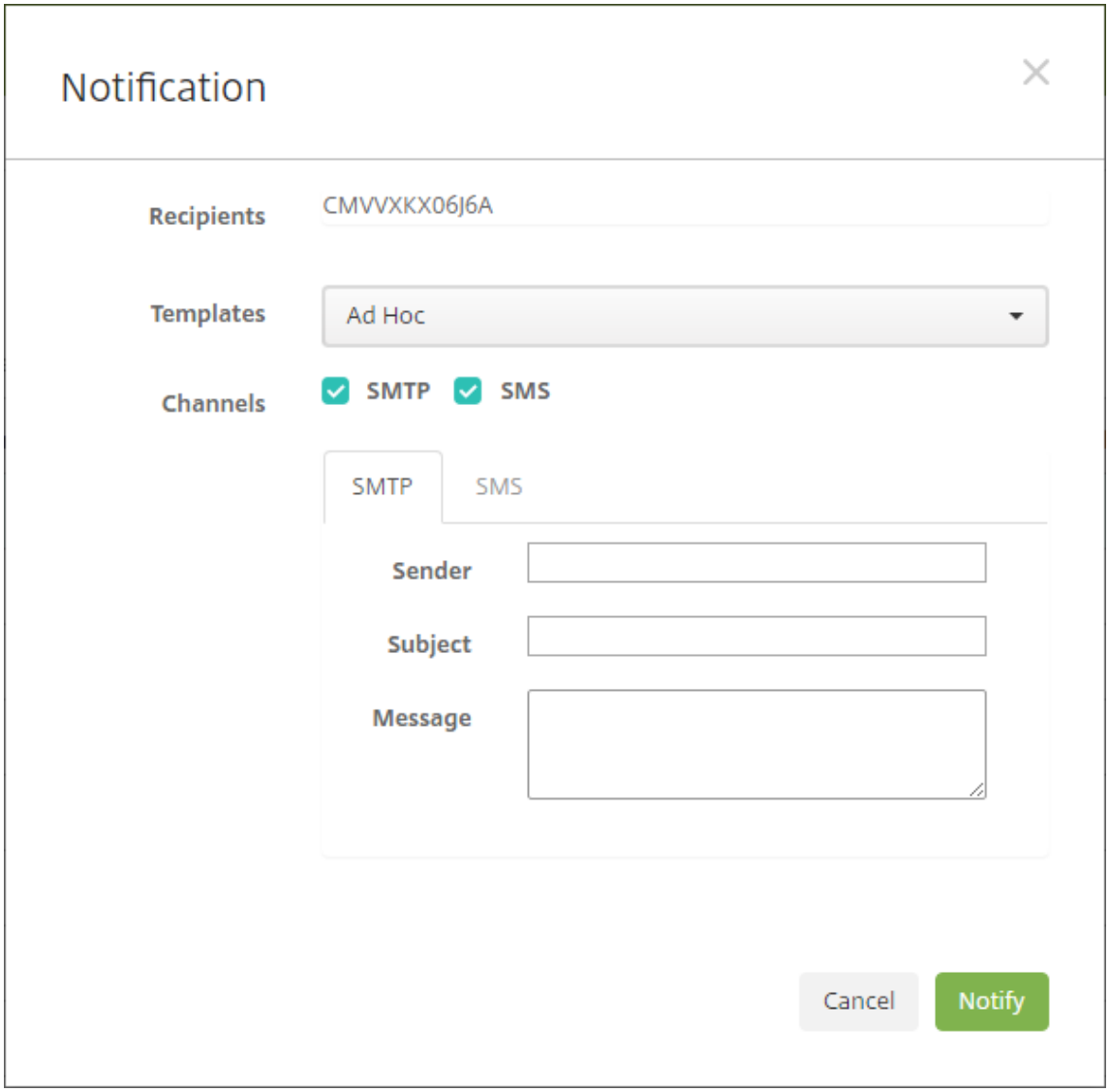


2. Haga clic en **Elegir archivo** y, a continuación, vaya al archivo que quiere importar.
3. Haga clic en **Importar**. El archivo importado aparecerá en la tabla **Dispositivos**.
4. Para modificar la información del dispositivo, selecciónelo y, a continuación, haga clic en **Modificar**. Para obtener información sobre las páginas que contiene **Detalles del dispositivo**, consulte Agregar un dispositivo manualmente.

Enviar una notificación a dispositivos

Puede enviar notificaciones a los dispositivos desde la página Dispositivos. Para obtener más información acerca de las notificaciones, consulte Notificaciones.

1. En la página **Administrar > Dispositivos**, seleccione los dispositivos a los que quiera enviar una notificación.
2. Haga clic en **Notificar**. Aparecerá el cuadro de diálogo **Notificación**. En el campo **Destinatarios**, se ofrece una lista de todos los dispositivos que van a recibir la notificación.



3. Configure estos parámetros:
    - **Plantillas:** En la lista, haga clic en el tipo de notificación que quiere enviar. Los campos **Asunto** y **Mensaje** se rellenarán con el texto configurado de la plantilla que eligió, excepto en el caso de haber elegido **Ad hoc**.
    - **Canales:** 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.
    - **Remitente:** Escriba un remitente opcional.
    - **Asunto:** Escriba el asunto para un mensaje **Ad hoc**.
    - **Mensaje:** Escriba el mensaje para un mensaje **Ad hoc**.
4. Haga clic en **Notificar**.

Exportar la tabla Dispositivos

1. Filtre la tabla **Dispositivos** según lo que quiera que aparezca en el archivo de exportación.
2. Haga clic en el botón **Exportar** situado sobre la tabla **Dispositivos**. XenMobile extrae la información de la tabla **Dispositivos** filtrada y la convierte a un archivo CSV.
3. Cuando se le solicite, abra o guarde el archivo CSV.

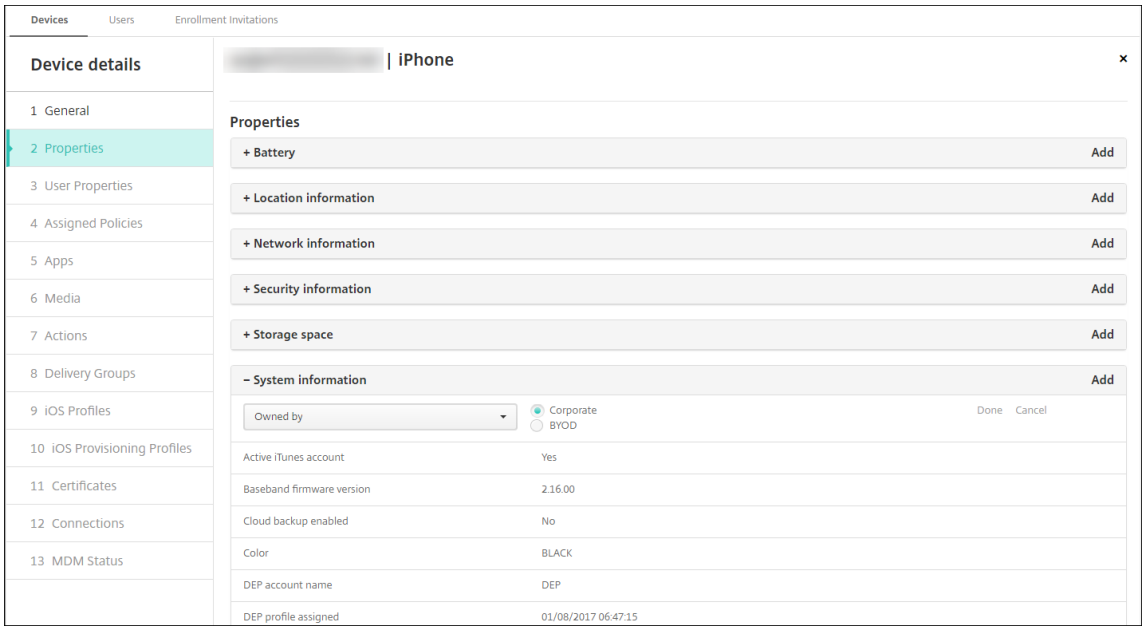
Etiquetar manualmente los dispositivos de usuario

En XenMobile, puede etiquetar manualmente un dispositivo de una de las siguientes maneras:

- Durante el proceso de inscripción por invitación.
- Durante el proceso de inscripción al portal Self Help Portal.
- Al agregar el propietario del dispositivo a las propiedades de este.

Tiene la opción de etiquetar el dispositivo como propiedad de la empresa o del empleado. Cuando se usa el portal Self-Help Portal para inscribir un dispositivo, también se puede etiquetarlo como propiedad de la empresa o propiedad del empleado. También puede etiquetar un dispositivo manualmente siguiendo este procedimiento.

1. Agregue una propiedad al dispositivo desde la ficha **Dispositivos** en la consola de XenMobile.
2. Agregue la propiedad denominada **Propietario** y elija **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 evitar tener que introducir una larga lista de dispositivos móviles manualmente. XenMobile es compatible con un formato de archivo de importación común para los tres tipos de dispositivos admitidos: 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

Tenga en cuenta lo siguiente:

- Para saber cuáles son los valores válidos para cada propiedad, consulte el PDF Valores y nombres de propiedades de dispositivo.
- 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
  ```

  Coloque una barra diagonal inversa de la siguiente manera:

  ```
  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**.

Ejemplo de un archivo de aprovisionamiento de dispositivos:

```
`1050BF3F5173010816100655105903915244201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2050BF3F5173010816100655105903925244201625379902;ANDROID;propertyN;
   propertyV$*&&éééétest
3050BF3F5173010816100655105903935244201625379903;iOS;test;
4050BF3F517301081610065510590393;;iOS;test;
;55244201625379903;ANDROID;test.testé;value;`
```

Cada línea del archivo describe un dispositivo. La primera entrada del ejemplo significa lo siguiente:

- SerialNumber: `1050BF3F5173010816100655105903 91`
- IMEI: `15244201625379901`
- OperatingSystemFamily: `WINDOWS`
- PropertyName: `propertyN`
- PropertyValue: `propertyV\;test\;1\;2;prop 2`

ActiveSync Gateway

November 6, 2020

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 (Aplicaciones obligatorias que faltan), XenMobile consulta la directiva Acceso a aplicaciones para ver cuáles son las aplicaciones obligatorias y deniega el acceso a los datos de ActiveSync si faltan esas aplicaciones. Para cada regla, puede elegir **Permitir** o **Denegar**. El valor predeterminado es **Permitir**.

Para obtener más información acerca de la directiva Acceso a aplicaciones, consulte Directiva de acceso a aplicaciones.

XenMobile admite las siguientes reglas:

Dispositivos anónimos: Comprueba si un dispositivo está en modo anónimo. Esta comprobación está disponible si XenMobile no puede volver a autenticar al usuario cuando un dispositivo intenta reconectar.

Atestación de Samsung Knox fallida: Comprueba si un dispositivo falló una consulta del servidor de atestación de Samsung Knox.

Aplicaciones prohibidas: Comprueba si un dispositivo tiene aplicaciones prohibidas, según se definen en la directiva Acceso a aplicaciones.

Permiso y denegación implícitos: Esta acción es la predeterminada de ActiveSync Gateway. La puerta de enlace crea una lista de todos los dispositivos que no cumplen ninguno de los demás criterios de regla o filtro, y permite o deniega en función de esa lista. Si no coincide ninguna regla, el valor predeterminado es Permiso implícito.

Dispositivos inactivos: Comprueba si un dispositivo está inactivo según se define en el parámetro Umbral de días de inactividad en Propiedades de servidor.

Aplicaciones obligatorias que faltan: Comprueba si en un dispositivo faltan aplicaciones obligatorias, según se definen en la directiva Acceso a aplicaciones.

Aplicaciones no sugeridas: Comprueba si un dispositivo tiene aplicaciones no sugeridas, según se definen en la directiva Acceso a aplicaciones.

Contraseña no conforme: 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 Código de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para definir una contraseña si XenMobile envía una directiva Código de acceso al dispositivo. Antes de que el usuario defina la contraseña, el código de acceso podría no cumplir los requisitos de conformidad.

Dispositivos no conformes: Comprueba si un dispositivo ya no es conforme, según lo definido en la propiedad de dispositivo No conforme. Esa propiedad es modificada normalmente por las acciones automatizadas o por las API de XenMobile de terceros.

Estado revocado: Comprueba si el certificado del dispositivo fue revocado. Un dispositivo revocado no se puede volver a inscribir hasta que se autorice de nuevo.

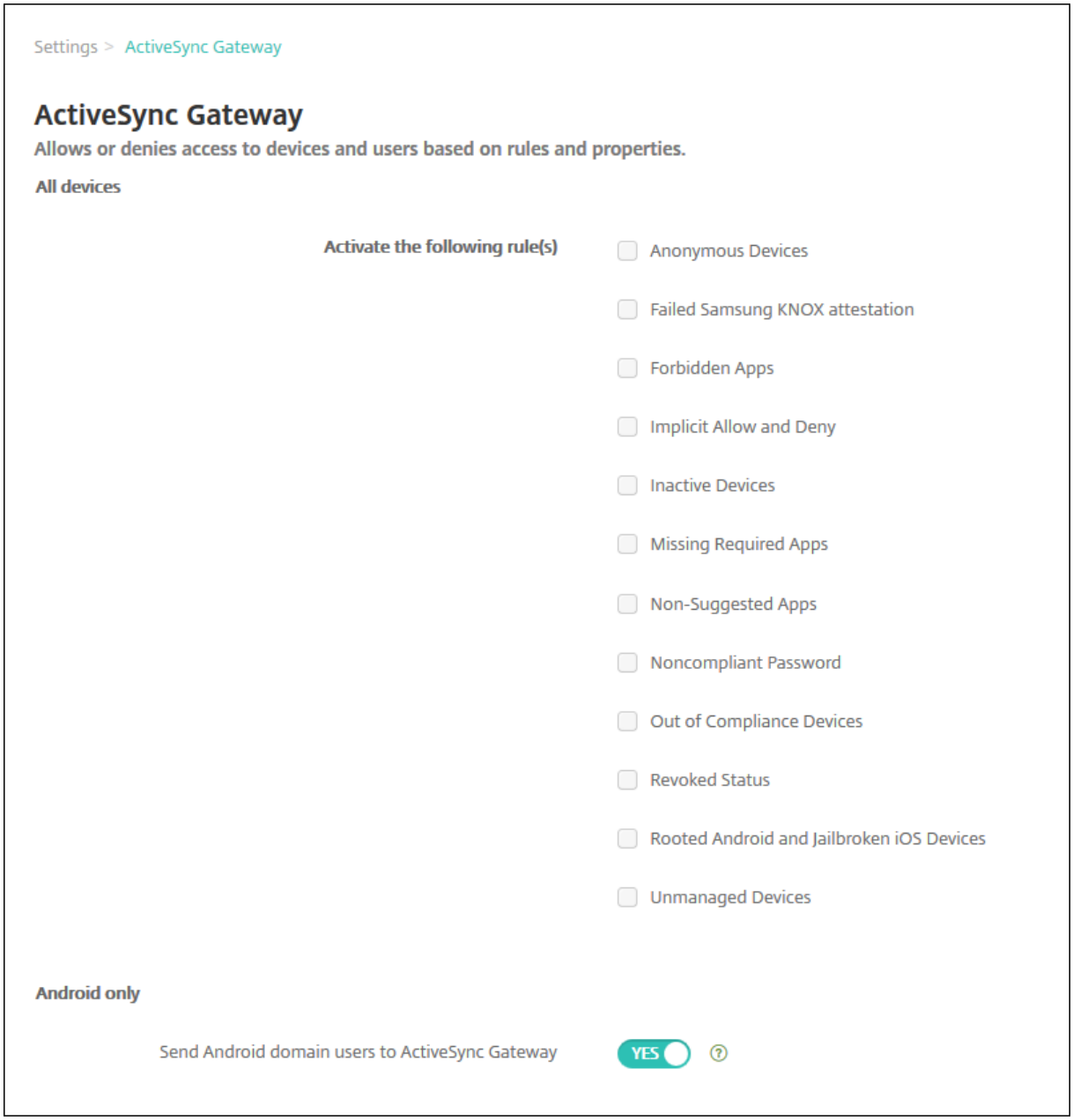
Dispositivos Android o iOS liberados por root/jailbreak: Comprueba si un dispositivo iOS está liberado por jailbreak o un dispositivo Android está liberado por rooting.

Dispositivos no administrados: Comprueba si un dispositivo aún está en estado administrado, bajo el control de XenMobile. Por ejemplo, un dispositivo inscrito en MAM o que se haya desinscrito no es un dispositivo administrado.

Enviar usuarios de dominio Android a ActiveSync Gateway: Haga clic en **SÍ** para que XenMobile envíe la información de los dispositivos Android a ActiveSync Gateway.

Para configurar los parámetros de ActiveSync Gateway

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Servidor**, haga clic en **ActiveSync Gateway**. Aparecerá la página **ActiveSync Gateway**.



1. En **Activar las reglas siguientes**, seleccione las reglas que quiera activar.
2. En **Solo Android**, en **Enviar usuarios de dominio Android a ActiveSync Gateway**, haga clic en **SÍ** para que XenMobile envíe la información de los dispositivos Android a ActiveSync Gateway.
3. Haga clic en **Guardar**.

Migrar de la administración de dispositivos a Android Enterprise

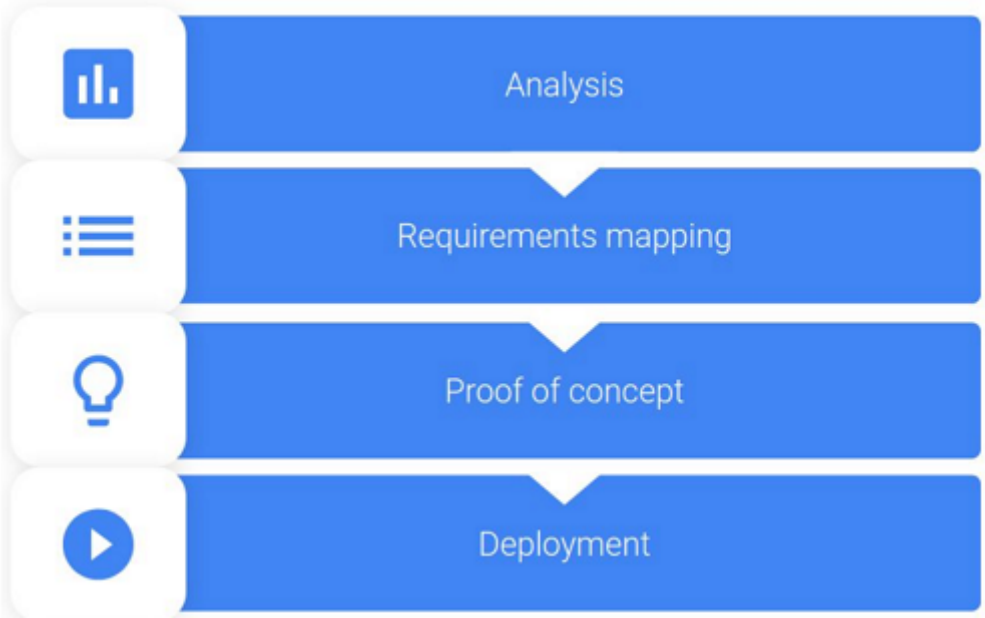
January 4, 2022

Este artículo describe consideraciones y recomendaciones para migrar desde la administración de dispositivos Android antiguos a Android Enterprise. Google va a retirar la API de administración de dispositivos Android. Esta API admitía aplicaciones de empresa en dispositivos Android. Android Enterprise es la solución moderna de administración que recomiendan Google y Citrix.

XenMobile pasará a utilizar Android Enterprise como método de inscripción predeterminado para los dispositivos Android. Una vez que Google haya retirado las API, la inscripción fallará en los dispositivos Android Q en el modo de administración de dispositivos.

Android Enterprise admite los modos de dispositivos totalmente administrados y de perfil de trabajo. La publicación de Google, Android Enterprise Migration Bluebook, detalla en qué se diferencian la administración de dispositivos antiguos y Android Enterprise. Le recomendamos que lea la información sobre migración de Google.

Esta publicación también describe las cuatro fases de la migración de la administración de dispositivos e incluye el siguiente diagrama. Este artículo contiene recomendaciones específicas sobre XenMobile para las fases de migración.



> Diagrama del libro azul
> sobre la migración a Android Enterprise.
> Publicado de nuevo con el permiso de Google.

Impacto de los elementos retirados de la administración de dispositivos

Google retirará las siguientes API de administración de dispositivos. Estas API no funcionarán en dispositivos con Android Q después de actualizar Secure Hub para que alcance el nivel de la API de Android Q:

- Disable camera: Controla el acceso a las cámaras de los dispositivos.
- Expire password: Obliga a los usuarios a cambiar su contraseña después de un período de tiempo configurable.
- Limit password: Establece requisitos restrictivos para las contraseñas.

Las API retiradas no afectan a los dispositivos inscritos en el modo solo MAM de Citrix.

Recomendaciones

Las siguientes recomendaciones son para los dispositivos que ya están inscritos en el modo de administración de dispositivos antiguos de Android, los dispositivos no inscritos y los dispositivos inscritos en el modo solo MAM de Citrix.

Estado de inscripción de los dispositivos	Acción recomendada
El dispositivo existente se inscribe en el modo de administración de dispositivos y su versión se puede actualizar a Android Q.	Antes de actualizar el dispositivo a Android Q, migre del modo de administración de dispositivos a Android Enterprise.
El dispositivo existente se inscribe en el modo de administración de dispositivos. El dispositivo no se puede actualizar a Android Q.	El dispositivo puede permanecer en el modo de administración de dispositivos. Sin embargo, piense en mover el dispositivo a Android Enterprise en la actualización del dispositivo.
El dispositivo existente se inscribe en el modo de administración de dispositivos y su versión se actualiza a Android Q.	Migre desde el modo de administración de dispositivos a Android Enterprise antes de que Google retire las API. Aparecerá un mensaje de advertencia para estos dispositivos en la consola de XenMobile.
Nuevo dispositivo entregado con Android Q e inscrito en el modo de administración de dispositivos.	Migre desde el modo de administración de dispositivos a Android Enterprise antes de que Google retire las API. Aparecerá un mensaje de advertencia para estos dispositivos en la consola de XenMobile.
Nuevo dispositivo entregado con o actualizable a Android Q. El dispositivo no está inscrito.	Use Android Enterprise para cualquier dispositivo nuevo.

Estado de inscripción de los dispositivos	Acción recomendada
El dispositivo nuevo o existente en Android Q se inscribe en el modo de administración de dispositivos después de que Google haya retirado las API.	Para evitar los efectos de las API retiradas de Google, Citrix recomienda migrar a Android Enterprise antes de que Google las retire. Después de esa fecha, la inscripción de estos dispositivos fallará.
Dispositivos nuevos o existentes inscritos en el modo solo MAM de Citrix.	No se necesita hacer nada. Las API de Google retiradas no afectan de ninguna manera a los dispositivos en el modo solo MAM.

Análisis

La fase de análisis de la migración consiste en:

- Comprender la configuración de Android heredado
- Documentar la configuración antigua para que se puedan asignar funciones antiguas a las funciones de Android Enterprise

Análisis recomendado

1. Evalúe Android Enterprise en XenMobile: totalmente administrado, totalmente administrado con perfil de trabajo, dispositivo dedicado, perfil de trabajo (BYOD).
2. Analice las funciones actuales de la administración de dispositivos y compárelas con Android Enterprise.
3. Documente los casos de uso de la administración de dispositivos.

Para documentar los casos de uso de la administración de dispositivos:

1. Cree una hoja de cálculo e indique los grupos de directivas actuales que hay en la consola de XenMobile.
2. Cree casos de uso independientes en función de los grupos de directivas existentes.
3. Para cada caso de uso, documente lo siguiente:
    - Nombre
    - Propietario de una empresa
    - Modelo de identidad de usuario
    - Requisitos de dispositivo
        - Seguridad
        - Administración

        - Usabilidad
    - Inventario de dispositivos
        - Marca y modelo
        - Versión de SO
    - Aplicaciones
4. Para cada aplicación, indique lo siguiente:
    - Nombre de la aplicación
    - Nombre del paquete
    - Método de alojamiento
    - Si la aplicación es pública o privada
    - Si la aplicación es obligatoria (verdadero/falso)

Asignación de requisitos

En función del análisis completado, determine los requisitos de las funciones de Android Enterprise.

Asignación recomendada de requisitos

1. Determine el modo de administración y el método de inscripción:
    - Perfil de trabajo (BYOD): Requiere volver a inscribirse. No es necesario restablecer los valores de fábrica.
    - Totalmente administrado: Requiere restablecer los valores de fábrica. Inscriba dispositivos mediante códigos QR, conexiones de transmisión de datos en proximidad (NFC), identificadores de controladores de directivas de dispositivo (DPC) o aprovisionamiento automático.
2. Cree una estrategia de migración de aplicaciones.
3. Asigne los requisitos de los casos de uso a las funciones de Android Enterprise. Documente la función para cada requisito de dispositivo que más se ajuste al requisito y a su correspondiente versión de Android.
4. Determine el SO de Android mínimo en función de los requisitos de las funciones (7.0, 8.0, 9.0).
5. Elija un modelo de identidad:
    - Recomendado: Cuenta de Google Play administrado.
    - Utilice cuentas de Google G Suite solamente si es cliente de Google Cloud Identity.
6. Cree una estrategia de dispositivos:
    - Sin acción: Si los dispositivos cumplen el nivel mínimo de SO.

- Actualización: Si los dispositivos son compatibles con el SO y pueden actualizarse a su versión.
- Reemplazo: Si los dispositivos no se pueden actualizar al nivel del SO compatible.

Estrategia de migración de aplicaciones recomendada

Después de completar la asignación de requisitos, mueva las aplicaciones de la plataforma Android a la plataforma Android Enterprise. Para obtener información detallada sobre la publicación de aplicaciones, consulte Agregar aplicaciones.

- Aplicaciones de la tienda pública de aplicaciones

  1. Seleccione las aplicaciones que quiere migrar y, a continuación, modifique las aplicaciones para desmarcar el parámetro de Google Play y seleccionar **Android Enterprise** como plataforma.
  2. Seleccione el grupo de entrega. Si una aplicación es obligatoria, muévala a la lista **Aplicaciones obligatorias** del grupo de entrega.

  Después de guardar una aplicación, aparecerá en la tienda de Google Play. Si tiene un perfil de trabajo, las aplicaciones aparecen en la tienda de Google Play en el perfil de trabajo.

- Aplicaciones privadas (de empresa)

  Las aplicaciones privadas se desarrollan en equipos internos o en un desarrollador externo. Le recomendamos que publique las aplicaciones privadas mediante Google Play.

  1. Seleccione las aplicaciones que quiere migrar y, a continuación, modifique las aplicaciones para seleccionar **Android Enterprise** como plataforma.
  2. Cargue el archivo APK y, a continuación, configure los parámetros de la aplicación.
  3. Publique la aplicación en el grupo de entrega requerido.

- Aplicaciones MDX

  1. Seleccione las aplicaciones que quiere migrar y, a continuación, modifique las aplicaciones para seleccionar **Android Enterprise** como plataforma.
  2. Cargue el archivo MDX. Siga el proceso de aprobación de las aplicaciones.
  3. Seleccione las directivas MDX.

  Para las aplicaciones MDX de Enterprise, recomendamos cambiarlas a aplicaciones empaquetadas en modo MDX SDK:

  – Opción 1: Aloje el archivo APK en Google Play con una cuenta de desarrollador asignada de forma privada a su organización. Publique el archivo MDX en XenMobile.

- Opción 2: Publique la aplicación desde XenMobile como una aplicación empresarial. Publique el archivo APK en XenMobile y seleccione la plataforma **Android Enterprise** para el archivo MDX.

Migración de directivas de dispositivos Citrix

En cuanto a las directivas que están disponibles para las plataformas Android y Android Enterprise, modifique la directiva correspondiente y seleccione la plataforma **Android Enterprise**.

Para Android Enterprise, tenga en cuenta el modo de inscripción. Algunas opciones de directiva solo están disponibles para dispositivos en modo de perfil de trabajo o modo totalmente administrado.

Prueba de concepto

Después de migrar aplicaciones a Android Enterprise, puede configurar una prueba de migración para comprobar que las funciones operan según lo previsto.

Configuración de la prueba de concepto recomendada

1. Configure la infraestructura de implementación:
   - Cree un grupo de entrega para sus pruebas de Android Enterprise.
   - Configure Android Enterprise en XenMobile.
2. Configure aplicaciones de usuario.
3. Configure las funciones de Android Enterprise.
4. Asigne directivas al grupo de entrega de Android Enterprise.
5. Pruebe las funciones y confírmelas.
6. Complete una guía de configuración de dispositivos para cada caso de uso.
7. Documente los pasos de configuración para los usuarios.

Implementación

Ahora puede implementar la configuración de Android Enterprise y preparar a sus usuarios para la migración.

Estrategia de implementación recomendada

La estrategia de implementación recomendada por Citrix consiste en probar todos los sistemas de producción para Android Enterprise y, más tarde, completar la migración de dispositivos.

- En este caso, los usuarios siguen utilizando dispositivos antiguos con su configuración actual. Configure nuevos dispositivos para la administración de Android Enterprise.
- Migre los dispositivos existentes solamente cuando sea necesario realizar una actualización o sustitución.
- Migre los dispositivos existentes a la administración de Android Enterprise al final de su ciclo de vida habitual. Si no, migre dichos dispositivos cuando deban reemplazarse si se pierden o se estropean.

Android Enterprise

January 4, 2022

Android Enterprise es un conjunto de herramientas y servicios proporcionados por Google como una solución de administración empresarial para dispositivos Android. Con Android Enterprise:

- Puede utilizar XenMobile para administrar dispositivos Android que sean propiedad de la empresa y dispositivos Android BYOD.
- Puede administrar todo el dispositivo o un perfil independiente en el dispositivo. Ese perfil independiente 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.
- También puede administrar dispositivos dedicados a un solo uso, como la administración de inventario. Para obtener información general sobre las prestaciones de Android Enterprise de Google, consulte Gestión con Android Enterprise.

Recursos:

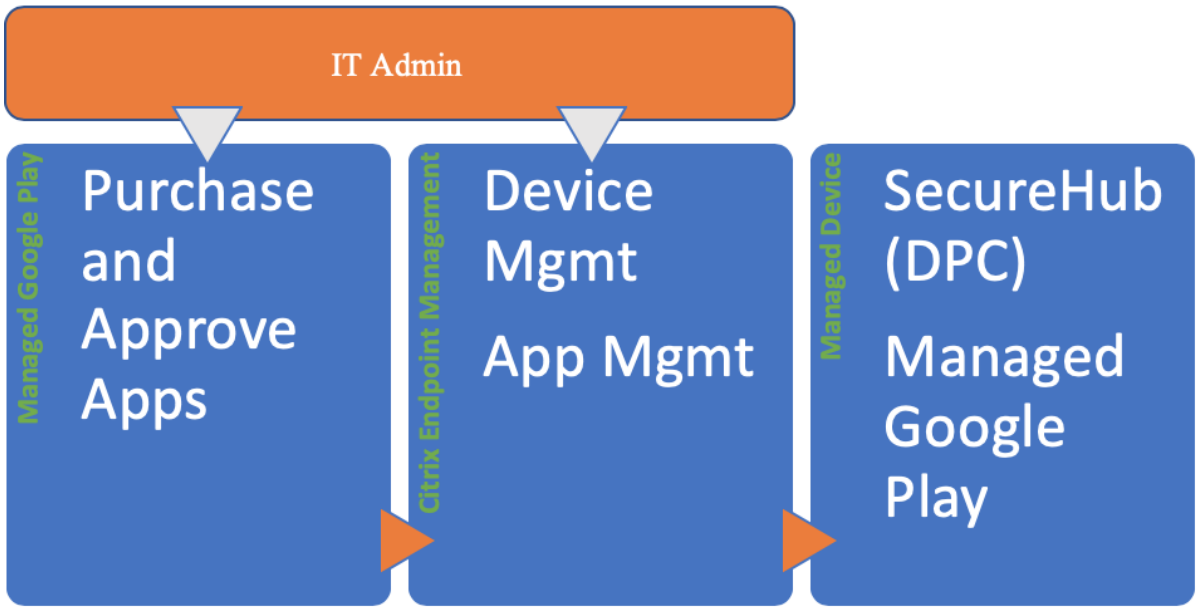
- Para obtener una lista de términos y definiciones relacionados con Android Enterprise, consulte Android Enterprise terminology en la guía para desarrolladores de Google Android Enterprise. Google actualiza estos términos con frecuencia.
- Para conocer los sistemas operativos Android compatibles con XenMobile, consulte Sistemas operativos compatibles.
- Para obtener información sobre las conexiones salientes que se deben tener en cuenta al configurar entornos de red para Android Enterprise, consulte el artículo Android Enterprise Network Requirements de la asistencia técnica de Google.

Al integrar XenMobile en Google Play administrado para utilizar Android Enterprise, se crea una empresa. Google define una empresa como un vínculo entre la organización y la solución de administración móvil empresarial (EMM). Todos los usuarios y los dispositivos que la organización administra a través de esa solución pertenecen a la empresa.

Una empresa de Android Enterprise tiene tres componentes: una solución EMM, una aplicación de controlador de directivas de dispositivos (DPC) y una plataforma de aplicaciones de empresa de Google. Al integrar XenMobile en Android Enterprise, la solución completa tiene los siguientes componentes:

- **XenMobile:** La solución EMM de Citrix. XenMobile es la solución unificada para lograr un espacio de trabajo digital seguro. XenMobile ofrece los medios para que los administradores de TI administren dispositivos y aplicaciones para sus organizaciones.
- **Citrix Secure Hub:** La aplicación DPC de Citrix. Secure Hub es el panel de inicio de XenMobile. Secure Hub aplica directivas en el dispositivo.
- **Google Play administrado:** Una plataforma de aplicaciones empresariales de Google que se integra en XenMobile. La API de EMM de Google Play establece las directivas de aplicación y distribuye las aplicaciones.

En esta ilustración se muestra cómo interactúan los administradores con estos componentes y cómo interactúan los componentes entre sí:



Usar Google Play administrado con XenMobile

> **Nota:**
>
> Puede utilizar Google Play administrado o Google Workspace para registrar Citrix como su proveedor EMM. En este artículo se analiza el uso de Android Enterprise con Google Play administrado. Si su organización usa Google Workspace para ofrecer acceso a las aplicaciones, puede utilizarlo con Android Enterprise. Consulte Android Enterprise heredado para clientes de Google Workspace (anteriormente G Suite).

Al utilizar Google Play administrado, puede aprovisionar cuentas administradas de Google Play para dispositivos y usuarios finales. Las cuentas de Google Play administrado proporcionan acceso a Google Play administrado, lo que permite a los usuarios instalar y utilizar las aplicaciones que ponga a su disposición. Si su organización utiliza un servicio de identidad de terceros, puede vincular las cuentas de Google Play administrado a las cuentas de identidad existentes.

Puesto que este tipo de empresa no está vinculada a un dominio, puede crear más de una empresa para una sola organización. Por ejemplo, cada departamento o región de una organización puede inscribirse como una empresa diferente para administrar conjuntos separados de dispositivos y aplicaciones.

Para los administradores de XenMobile, Google Play administrado combina la experiencia de usuario y las funciones de la tienda de aplicaciones de Google Play con un conjunto de capacidades de administración diseñadas para las empresas. Se utiliza Google Play administrado para agregar, comprar y aprobar aplicaciones para implementarlas en el espacio de trabajo de Android Enterprise del dispositivo. Se puede utilizar Google Play para implementar aplicaciones públicas, privadas y de terceros.

Para los usuarios de dispositivos administrados, Google Play administrado es la tienda de aplicaciones de empresa. Los usuarios pueden explorar aplicaciones, ver los detalles de la aplicación e instalarlas. A diferencia de la versión pública de Google Play, los usuarios solo podrán instalar las aplicaciones de Google Play administrado que usted haya puesto a su disposición.

Casos de implementación de dispositivos y modos de operación

El caso de implementación de dispositivos se refiere a quién pertenecen los dispositivos que usted implementa y cómo los administra usted. En cambio, los perfiles de dispositivo se distinguen en función de cómo el DPC administra y aplica las directivas en los dispositivos.

Un perfil de trabajo aísla las cuentas, las aplicaciones y los datos de empresa por un lado, y las cuentas, las aplicaciones y los datos personales por el otro. Para obtener información más detallada sobre los perfiles de trabajo, consulte el tema ¿Qué es un perfil de trabajo? en la ayuda de Google Android Enterprise.

> **Importante:**
>
> Cuando los dispositivos Android Enterprise se actualicen a la versión Android 11, Google migrará los dispositivos administrados como “totalmente administrados con un perfil de trabajo” a una nueva experiencia de perfil de trabajo con seguridad mejorada. Para obtener más información, consulte Changes ahead for Android Enterprise’s Fully Managed with Work Profile.

Administración de dispositivos	Casos de uso	Perfil de trabajo	Perfil personal	Notas
Dispositivos propiedad de la empresa (totalmente administrados)	Dispositivos propiedad de la empresa destinados únicamente al uso profesional	No	Sí. DPC puede realizar acciones en todo el dispositivo: configurar la conectividad en todo el dispositivo, establecer la configuración global y realizar un restablecimiento a los valores de fábrica.	Solo para dispositivos nuevos o de restablecimiento de fábrica.
Totalmente administrado con un perfil de trabajo	Dispositivos propiedad de la empresa destinados al uso personal y profesional	Sí	Sí. En estos dispositivos, se ejecutan dos copias del DPC: Una administra el dispositivo en modo propietario del dispositivo y la otra administra el perfil de trabajo en modo propietario del perfil. Puede aplicar directivas independientes al dispositivo y al perfil de trabajo.	Estos dispositivos se conocían anteriormente como dispositivos COPE (propiedad de la empresa con acceso privado).

Administración de dispositivos	Casos de uso	Perfil de trabajo	Perfil personal	Notas
Dispositivos dedicados*	Dispositivos propiedad de la empresa configurados para un solo caso de uso, como la señalización digital o la impresión de tíquets	No	Sí. Solo se suministran las aplicaciones obligatorias y se impide que los usuarios agreguen otras aplicaciones.	Se conocían anteriormente como dispositivos de uso único y propiedad de la empresa (COSU).
Perfil de trabajo BYOD**	Dispositivos personales inscritos en modo de perfil de trabajo (también conocido como modo propietario del perfil)	Sí	Sí. DPC administra solo el perfil de trabajo, no todo el dispositivo.	Estos dispositivos no necesitan ser nuevos ni haberse restablecido a los valores de fábrica.

* Los usuarios pueden compartir un dispositivo dedicado. Cuando un usuario inicia sesión en una aplicación en un dispositivo dedicado, el estado de su trabajo está relacionado con la aplicación, no con el dispositivo.

** XenMobile no admite dispositivos Zebra en el modo propietario de perfil. XenMobile admite dispositivos Zebra como dispositivos totalmente administrados y en modo antiguo de dispositivos (también denominado modo administrador del dispositivo).

Para obtener información sobre la migración del modo antiguo al modo de propietario del dispositivo o de propietario del perfil, consulte Migrar de la administración de dispositivos a Android Enterprise.

Métodos de autenticación

Los perfiles de inscripción determinan si los dispositivos Android se inscriben en MAM, MDM o MDM+MAM, con la posibilidad de que los usuarios se excluyan de MDM.

Para obtener información sobre la especificación del nivel de seguridad y los pasos necesarios para la inscripción, consulte Configurar modos de seguridad de inscripción.

XenMobile admite los siguientes métodos de autenticación para dispositivos Android en MDM+MAM. Para obtener más información, consulte los artículos de Certificados y autenticación.

- Dominio
- Dominio y token de seguridad
- Certificado del cliente
- Certificado de cliente y dominio
- Proveedores de identidades:
  - Azure Active Directory
  - Proveedor de identidades Citrix

Otro método de autenticación que rara vez se utiliza es el certificado de cliente junto con el token de seguridad. Para obtener información, consulte https://support.citrix.com/article/CTX215200.

Requisitos

Antes de comenzar a usar Android Enterprise, necesita:

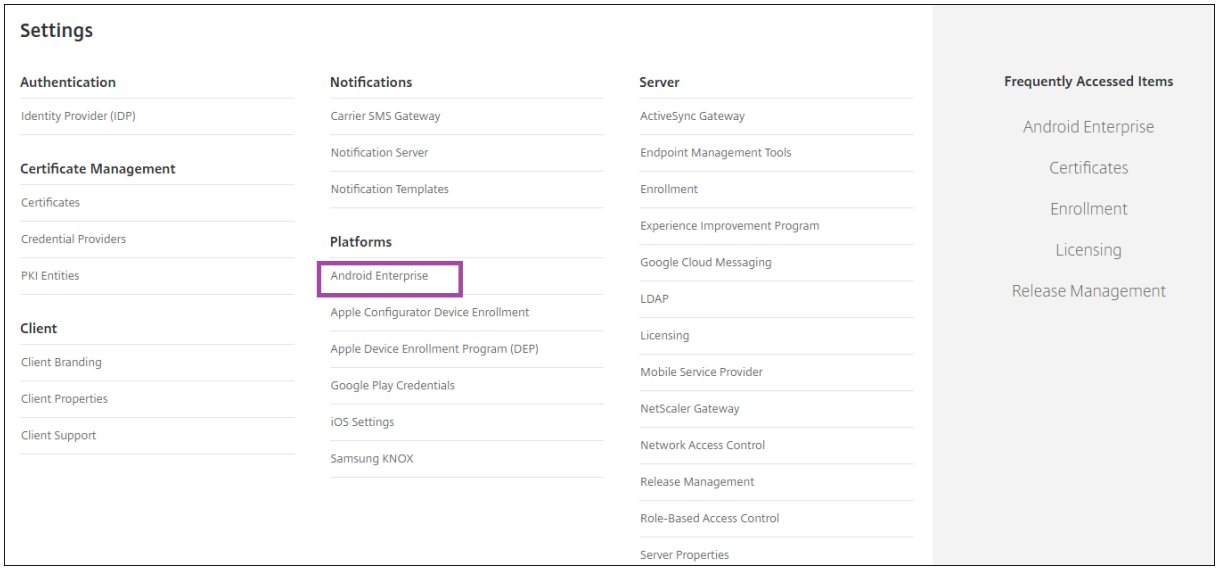
- Cuentas y credenciales:
  - Para configurar Android Enterprise con Google Play administrado, una cuenta corporativa de Google
  - Para descargar los archivos MDX más recientes, una cuenta de cliente de Citrix
  - Para implementar aplicaciones privadas (opcional), una cuenta de desarrollador de Google
- Firebase Cloud Messaging (FCM) configurado para XenMobile. Consulte Firebase Cloud Messaging para obtener instrucciones.
- Para Samsung Knox Mobile Enrollment (opcional), licencias premium de Knox.

Conectar XenMobile con Google Play

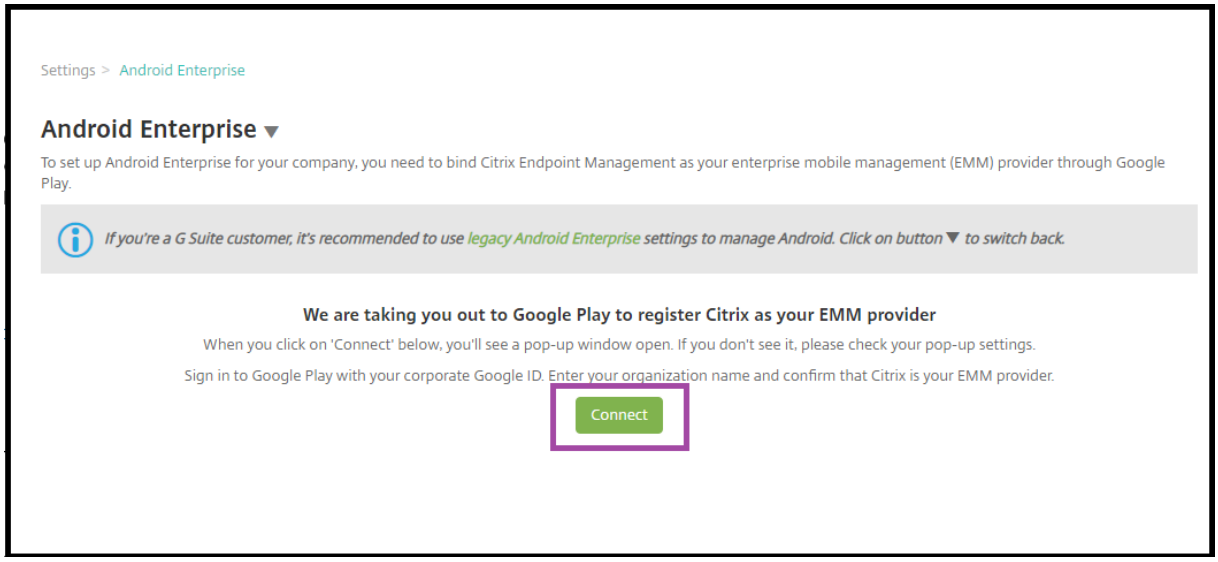
Para configurar Android Enterprise en su organización, registre Citrix como su proveedor de EMM a través de Google Play administrado. Este proceso conecta Google Play administrado con XenMobile y crea una empresa para Android Enterprise en XenMobile.

Necesita una cuenta corporativa de Google para iniciar sesión en Google Play.

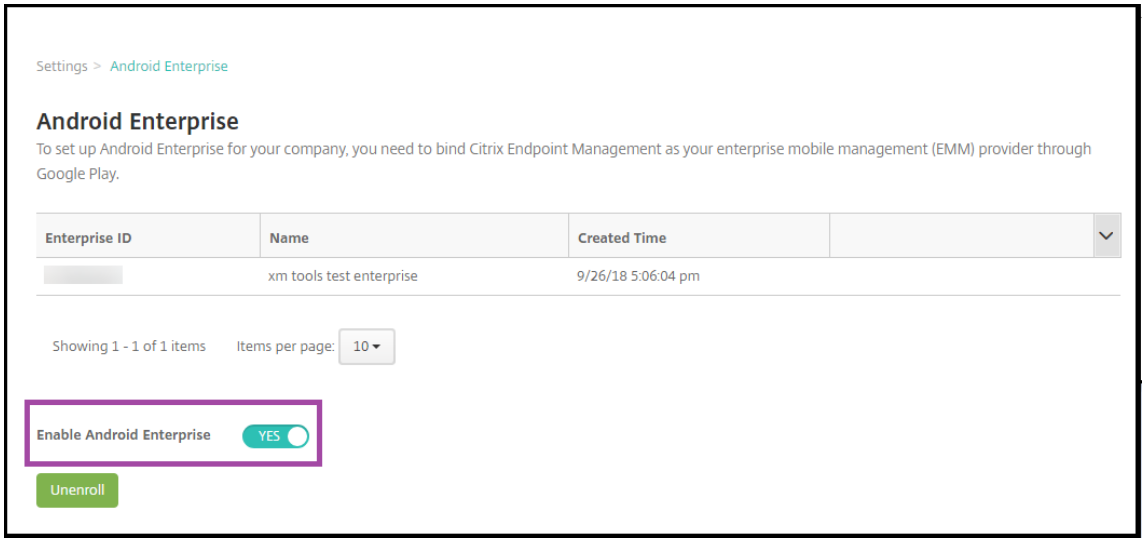
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Vaya a **Parámetros > Android Enterprise**.



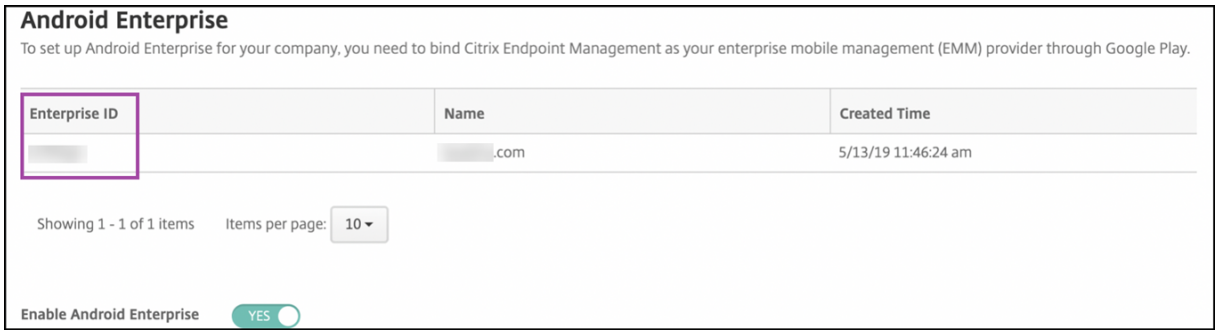
1. Haga clic en **Connect**. Se abre Google Play.



1. Inicia sesión en Google Play con las credenciales de su cuenta corporativa de Google. Introduzca el nombre de su organización y confirme que Citrix es su proveedor EMM.
2. Se agrega una ID de empresa para Android Enterprise. Para habilitar Android Enterprise, ajuste **Habilitar Android Enterprise** en **Sí**.



El ID de Enterprise aparece en la consola de XenMobile.



Su entorno está conectado a Google y está listo para administrar dispositivos. Ya puede proporcionar aplicaciones a los usuarios.

XenMobile se puede utilizar para ofrecer a los usuarios aplicaciones móviles de productividad de Citrix, aplicaciones MDX, aplicaciones de tienda pública, aplicaciones web y SaaS, aplicaciones empresariales y enlaces web. Para obtener más información sobre estos tipos de aplicaciones y sobre cómo proporcionarlas a los usuarios, consulte Agregar aplicaciones.

En esta sección se muestra cómo ofrecer aplicaciones de productividad móvil.

Proporcionar aplicaciones móviles de productividad de Citrix a usuarios de Android Enterprise

Para proporcionar aplicaciones móviles de productividad de Citrix a usuarios de Android Enterprise, debe seguir estos pasos.

1. Publique las aplicaciones como aplicaciones MDX. Consulte Configurar aplicaciones como aplicaciones MDX.

2. Configure las reglas para el desafío de seguridad que emplean los usuarios con el fin de acceder a los perfiles de trabajo de sus dispositivos. Consulte Configurar la directiva de desafío de seguridad.

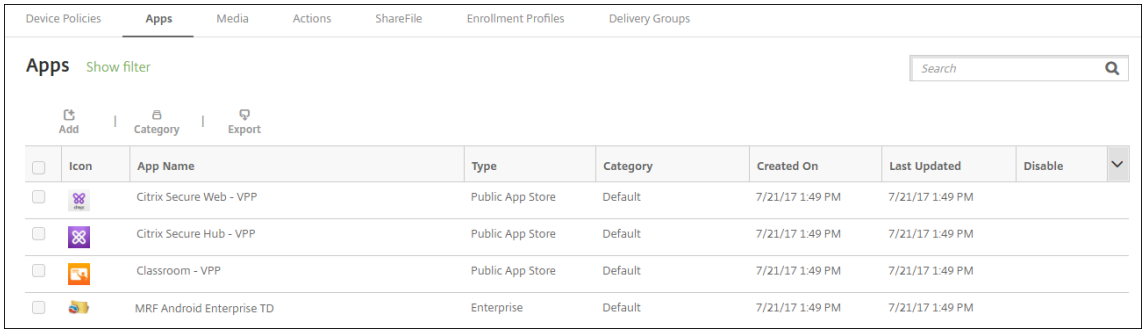
Las aplicaciones que publique están disponibles para los dispositivos inscritos de su empresa de Android Enterprise.

> **Nota:**
>
> Cuando implementa una aplicación de tienda pública de Android Enterprise en un usuario de dispositivo Android, ese usuario se inscribe automáticamente en Android Enterprise.

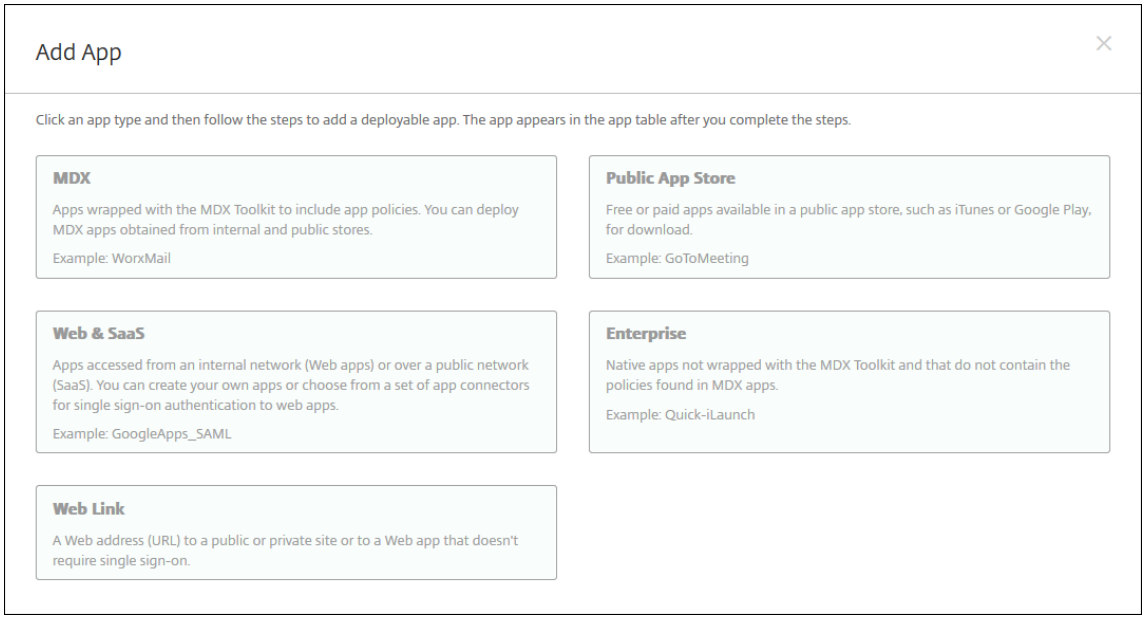
Configurar aplicaciones como aplicaciones MDX

Para configurar una aplicación de productividad de Citrix como una aplicación MDX para Android Enterprise:

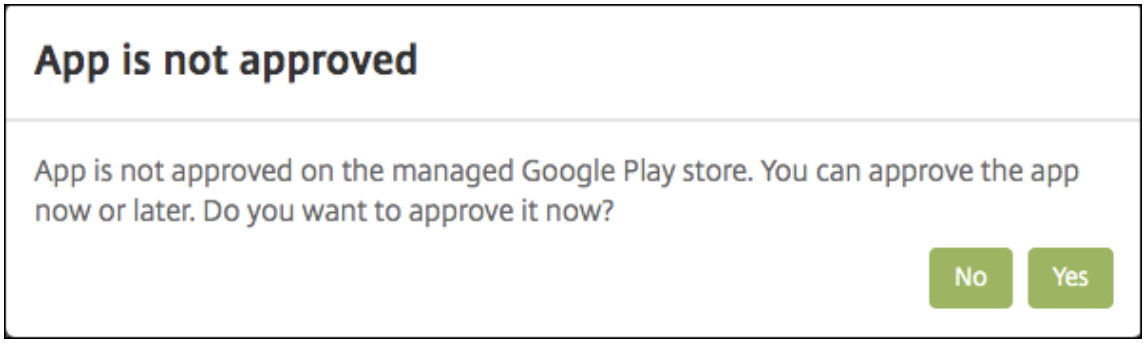
1. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones**. Aparecerá la página **Aplicaciones**.



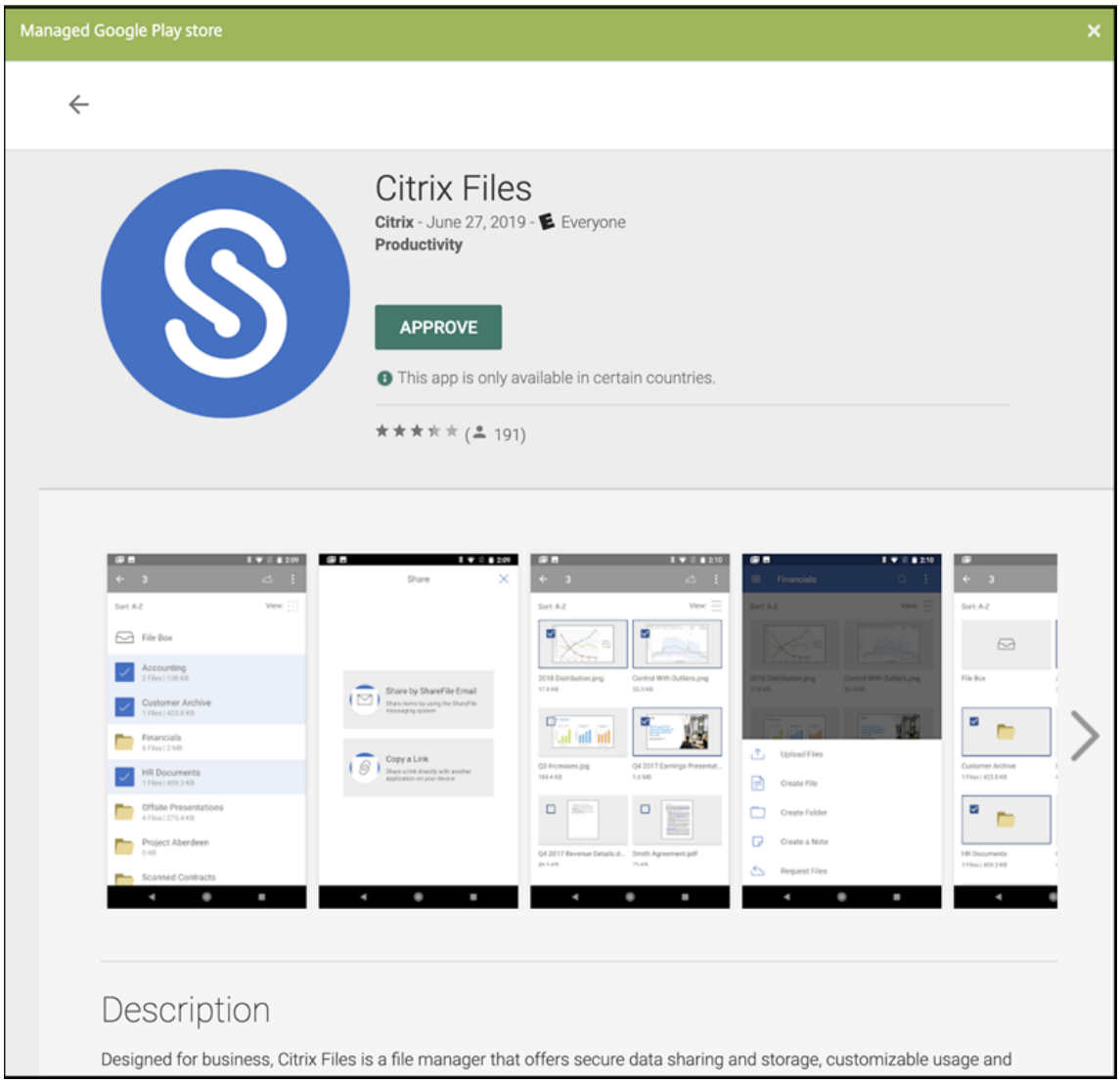
2. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



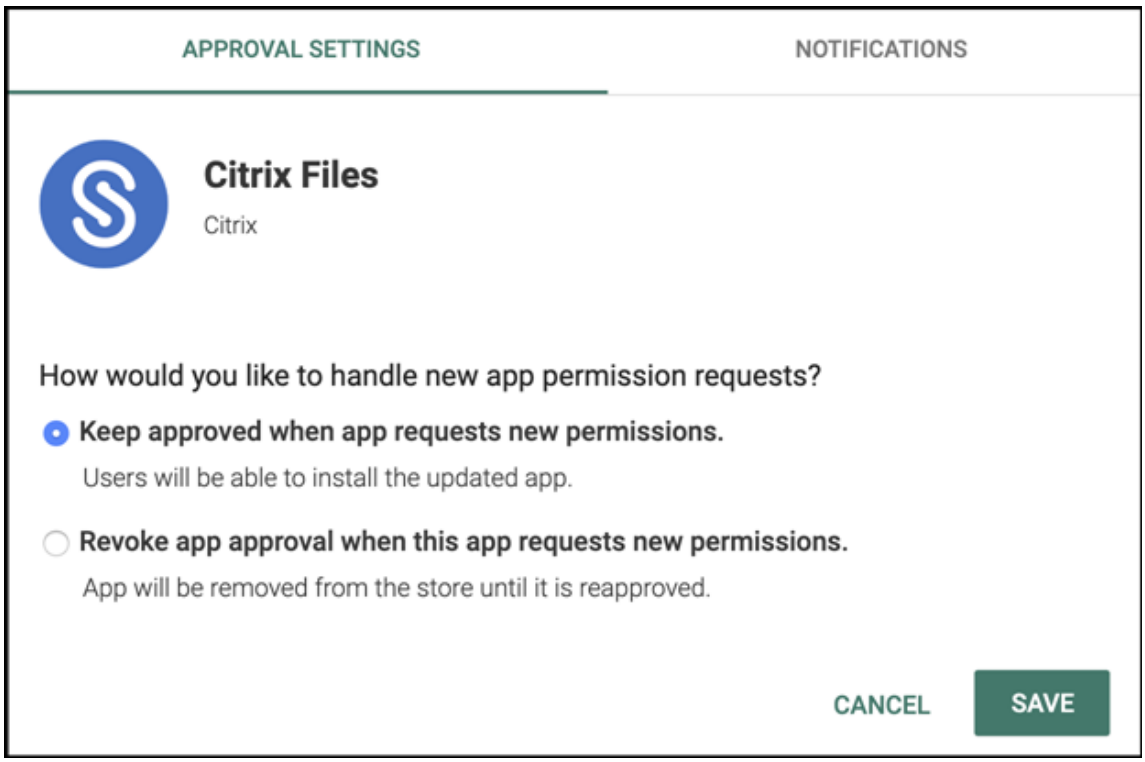
3. Haga clic en **MDX**. Aparecerá la página **Información de la aplicación**.
4. En el lado izquierdo de la página, seleccione **Android Enterprise** como plataforma.
5. En la página **Información de la aplicación**, escriba la información siguiente:
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.
   - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
   - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.
6. Haga clic en **Siguiente**. Aparecerá la página **Aplicación MDX para Android Enterprise**.
7. Haga clic en **Cargar** y vaya a la ubicación de los archivos .mdx para la aplicación. Seleccione el archivo y haga clic en **Abrir**.
8. La interfaz de usuario le notifica si la aplicación adjunta requiere la aprobación de Google Play Store administrado. Para aprobar la aplicación sin salir de la consola de XenMobile, haga clic en **Sí**.



9. Cuando se abra la página de Google Play Store administrado, haga clic en **Approve**.

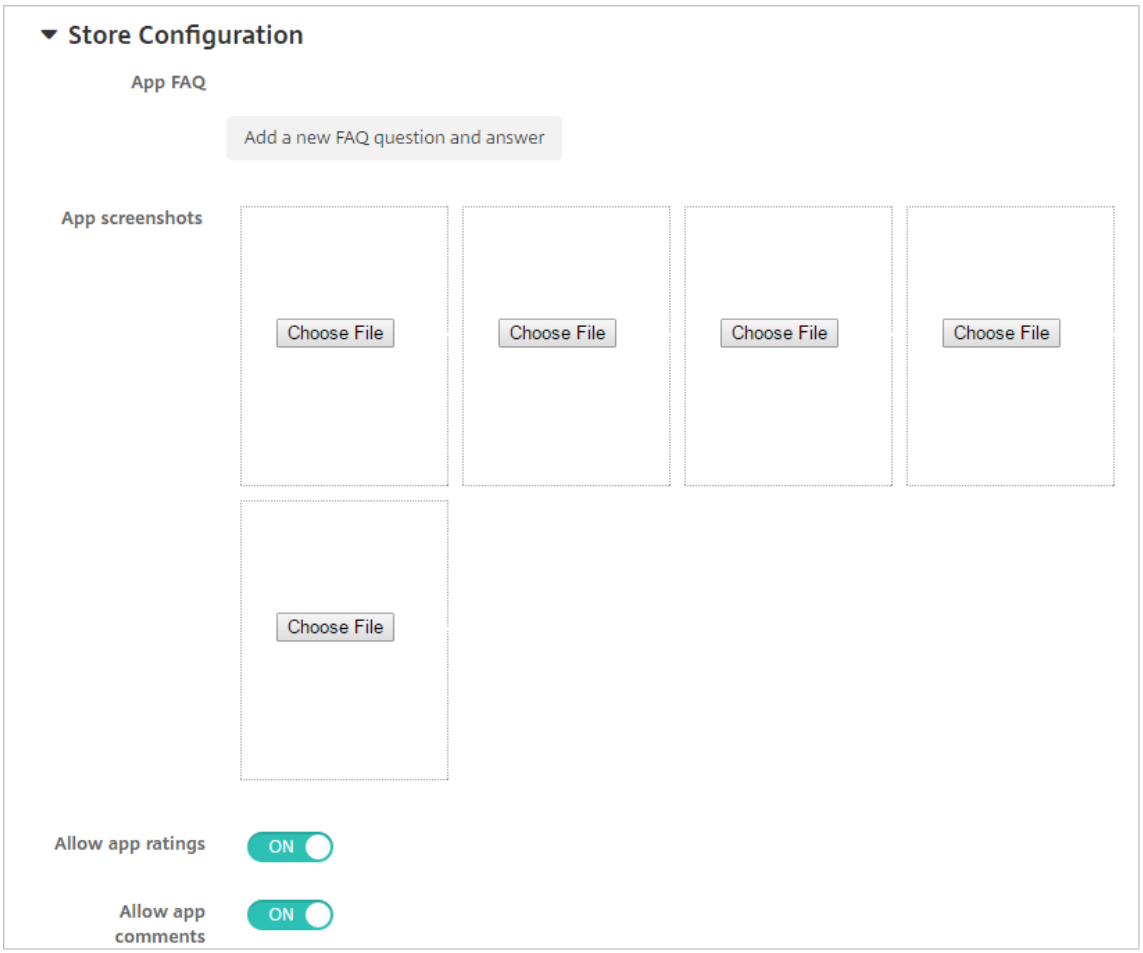


10. Vuelva a hacer clic en **Approve**.
11. Seleccione **Keep approved when app requests new permissions**. Haga clic en **Guardar**.



12. Cuando se aprueba y guarda la aplicación, aparecen más parámetros en la página. Configure estos parámetros:
    - **Nombre de archivo:** Escriba el nombre del archivo asociado a la aplicación.
    - **Descripción de la aplicación:** Escriba una descripción de la aplicación.
    - **Seguimiento del producto:** Especifique qué tipo de seguimiento de producto quiere enviar a los dispositivos de usuario. Si tiene un seguimiento diseñado para prueba, puede seleccionarlo y asignárselo a sus usuarios. El valor predeterminado es Producción.
    - **Versión de la aplicación:** Si quiere, escriba el número de versión de la aplicación.
    - **ID del paquete:** La URL de la aplicación de Google Play Store.
    - **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
    - **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
    - **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
13. Configure las **directivas MDX**. Para obtener más información sobre directivas para aplicaciones MDX, consulte Vista general de las directivas MDX e Introducción al SDK de MAM.
14. Configurar las reglas de implementación. Para obtener información, consulte Implementar recursos.
15. Expanda **Configuración del almacén**. Este parámetro no se aplica a las aplicaciones de Android

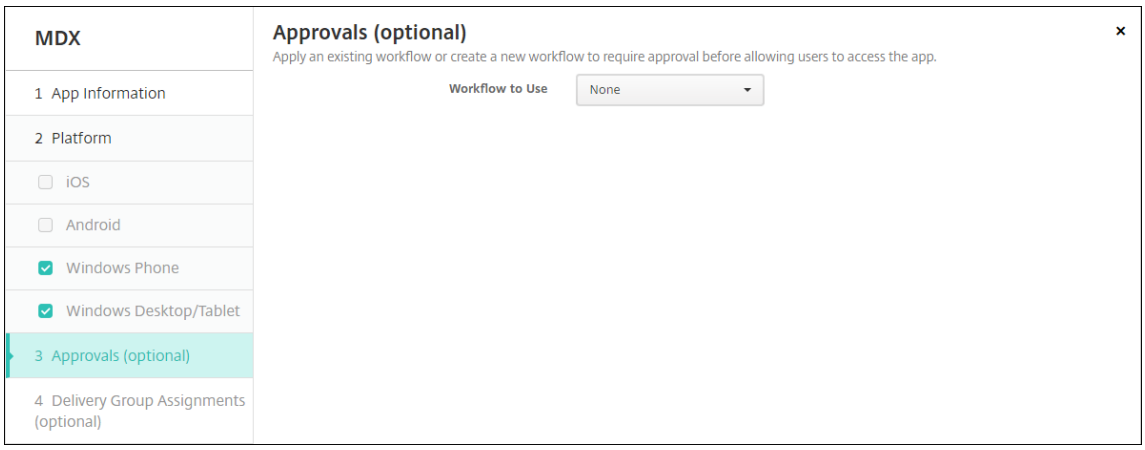
Enterprise, que solo aparecen en Google Play administrado.



Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en el almacén de aplicaciones. También puede definir si los usuarios pueden puntuar o comentar la aplicación.

- Configure estos parámetros:
  - **Preguntas frecuentes sobre aplicaciones:** Agregue una sección de preguntas frecuentes sobre la aplicación (junto con sus respuestas).
  - **Capturas de pantalla de aplicaciones:** Agregue capturas de pantalla para ayudar a clasificar la aplicación en el almacén de aplicaciones. El formato del gráfico que cargue debe ser PNG. No puede cargar imágenes en formato GIF o JPEG.
  - **Permitir puntuación de aplicaciones:** Seleccione si permitir a los usuarios puntuar la aplicación. De forma predeterminada, está **activado**.
    Permitir comentarios de aplicaciones: Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. De forma predeterminada, está **activado**.

16. Haga clic en **Siguiente**. Aparecerá la página **Aprobaciones**.



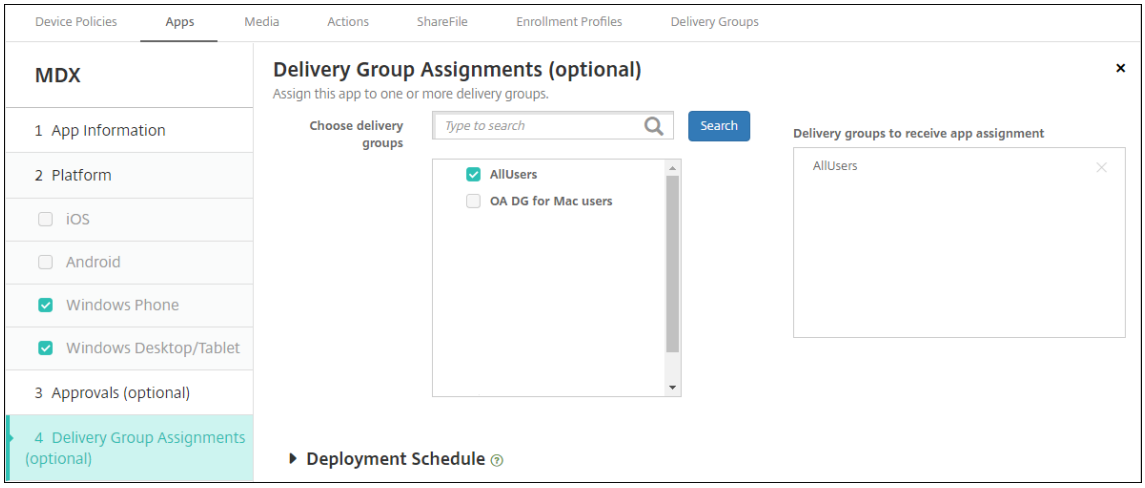
Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no quiere establecer flujos de trabajo de aprobación, puede ir directamente al paso 15.

Configure estos parámetros para asignar o crear un flujo de trabajo:

- **Flujo de trabajo para usar:** En la lista, haga clic en un flujo de trabajo existente o haga clic en **Crear un flujo de trabajo**. El valor predeterminado es **Ninguno**.
- Si selecciona **Crear un flujo de trabajo** configure los siguientes parámetros: Para obtener más información, consulte Aplicar flujos de trabajo.
- **Nombre:** Escriba un nombre único para el flujo de trabajo.
- **Descripción:** Si quiere, escriba una descripción del flujo de trabajo.
- **Plantillas de correo electrónico de aprobación:** En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar al flujo de trabajo. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
- **Niveles de aprobación administrativa:** En la lista, seleccione la cantidad de niveles de aprobación administrativa necesarios para este flujo de trabajo. El valor predeterminado es 1 nivel. Las opciones posibles son:
  - No se necesita
  - 1 nivel
  - 2 niveles
  - 3 niveles
- **Seleccionar dominio de Active Directory:** En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
- **Buscar aprobadores adicionales requeridos:** Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Buscar**. Los nombres se originan en Active Directory.
- Cuando el nombre aparezca en el campo, marque la casilla situada al lado. El nombre y la dirección de correo electrónico aparecen en la lista **Aprobadores adicionales requeridos seleccionados**.

- Para quitar a una persona de la lista **Aprobadores adicionales requeridos seleccionados**, realice una de las siguientes acciones:
  * Haga clic en **Buscar** 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 **Buscar** para limitar los resultados de la búsqueda.
  * Las personas de la lista **Aprobadores adicionales requeridos seleccionados** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla situada junto a cada nombre que quiera quitar.

17. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.



18. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione un grupo o varios de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.

19. Expanda **Programación de implementación** y, a continuación, configure estos parámetros:

    - Junto a **Implementar**, haga clic en **Sí** para programar la implementación, o bien, haga clic en **No** para cancelarla. De forma predeterminada, está **activado**.
    - Junto a Programación de implementación, haga clic en **Ahora** o en **Más tarde**. La opción predeterminada es **Ahora**.
    - Si hace clic en **Más tarde**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
    - Junto a **Condición de implementación**, puede hacer clic en **En cada conexión** o en **Solo cuando haya fallado la implementación anterior**. La opción predeterminada es **En cada conexión**.
    - Junto a **Implementar para conexiones permanentes**, asegúrese de que está selec-

cionado **No**. Está **desactivado** de forma predeterminada. Las conexiones permanentes no están disponibles para Android Enterprise si comenzó a utilizar XenMobile con la versión 10.18.19 o posterior. No recomendamos las conexiones en el caso de clientes que comenzaron a utilizar XenMobile antes de la versión 10.18.19.

Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Parámetros > Propiedades de servidor**.

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 **Implementar para conexiones permanentes**.

20. Haga clic en **Guardar**.

Repita los pasos para configurar una aplicación MDX para cada aplicación móvil de productividad.

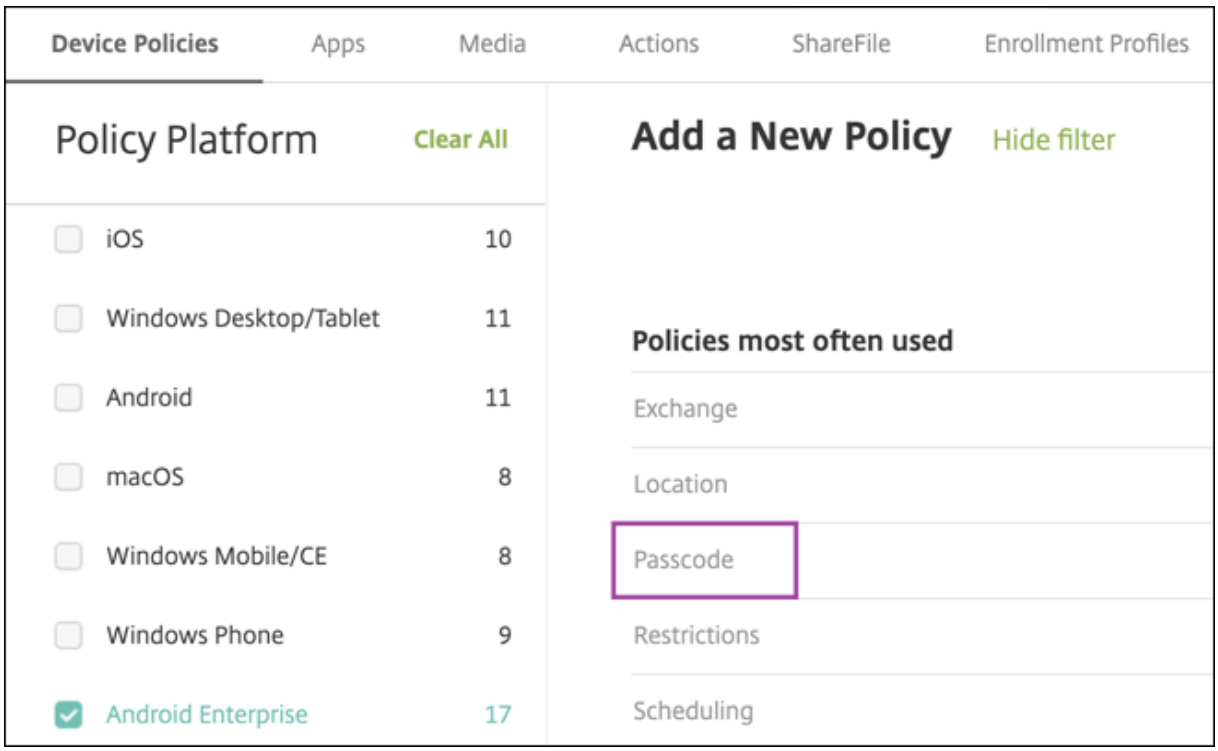
Configurar la directiva de desafío de seguridad

En XenMobile, la directiva Código de acceso configura el conjunto de reglas que los usuarios deben seguir para superar los retos de seguridad para acceder a sus dispositivos o a los perfiles de trabajo de Android Enterprise en sus dispositivos. Un desafío de seguridad puede ser un código de acceso o un reconocimiento biométrico. Para obtener más información acerca de la directiva Código de acceso, consulte Directiva de código de acceso.

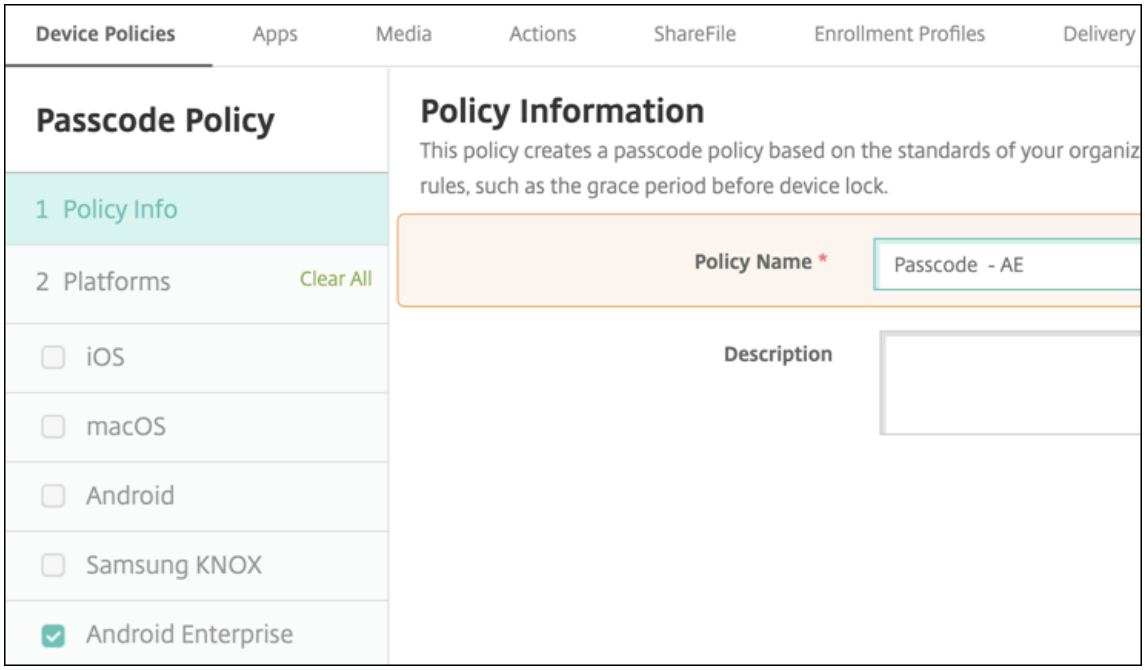
- Si la implementación de Android Enterprise incluye dispositivos BYOD, configure la directiva de código de acceso para el perfil de trabajo.
- Si la implementación incluye dispositivos totalmente administrados y propiedad de la empresa, configure la directiva de código de acceso para el propio dispositivo.
- Si la implementación incluye ambos tipos de dispositivos, configure ambos tipos de directiva de código de acceso.

Para configurar la directiva de código de acceso:

1. En la consola de XenMobile, vaya a **Configurar > Directivas de dispositivo**.
2. Haga clic en **Agregar**.
3. Haga clic en **Mostrar filtro** para ver el panel **Plataformas** de la directiva. En el panel **Plataformas** de la directiva, seleccione **Android Enterprise**.
4. Haga clic en **Código de acceso** en el panel derecho.



1. Introduzca un **nombre de directiva**. Haga clic en **Siguiente**.



2. Establezca la configuración para la directiva de código de acceso.
   - **Active** la opción **Código de acceso de dispositivo obligatorio** para ver los parámetros disponibles de los desafíos de seguridad en el propio dispositivo.
   - Establezca **Desafío de seguridad de perfil de trabajo** en **Sí** para ver los parámetros

disponibles de los desafíos de seguridad de perfil de trabajo.

3. Haga clic en **Siguiente**.
4. Asigne la directiva a uno o varios grupos de entrega.
5. Haga clic en **Guardar**.

Creación de perfiles de inscripción

Los perfiles de inscripción controlan el método de inscripción de los dispositivos Android si Android Enterprise está habilitado para su implementación de XenMobile. Cuando crea un perfil de inscripción para dispositivos Android Enterprise, puede configurarlo para inscribir los dispositivos nuevos y restablecidos a los valores de fábrica como:

- Dispositivos totalmente administrados
- Dispositivos dedicados (dispositivos COSU)
- Dispositivos totalmente administrados con un perfil de trabajo (dispositivos COPE)

También puede configurar cada uno de estos perfiles de inscripción de Android Enterprise para inscribir dispositivos Android BYOD como dispositivos de perfil de trabajo.

Si Android Enterprise está habilitado para la implementación de XenMobile, todos los dispositivos Android recién inscritos (o que se han inscrito de nuevo) se inscriben como dispositivos Android Enterprise. De forma predeterminada, el perfil de inscripción global registra los dispositivos Android nuevos y de restablecimiento de fábrica como dispositivos totalmente administrados e inscribe los dispositivos BYOD Android como dispositivos de perfil de trabajo.

Cuando crea los perfiles de inscripción, les asigna grupos de entrega. Si un usuario pertenece a varios grupos de entrega que tienen perfiles de inscripción diferentes, el nombre del grupo de entrega determina el perfil de inscripción utilizado. XenMobile selecciona el grupo de entrega que aparece en último lugar en una lista alfabética de grupos de entrega. Para obtener más información, consulte Perfiles de inscripción.

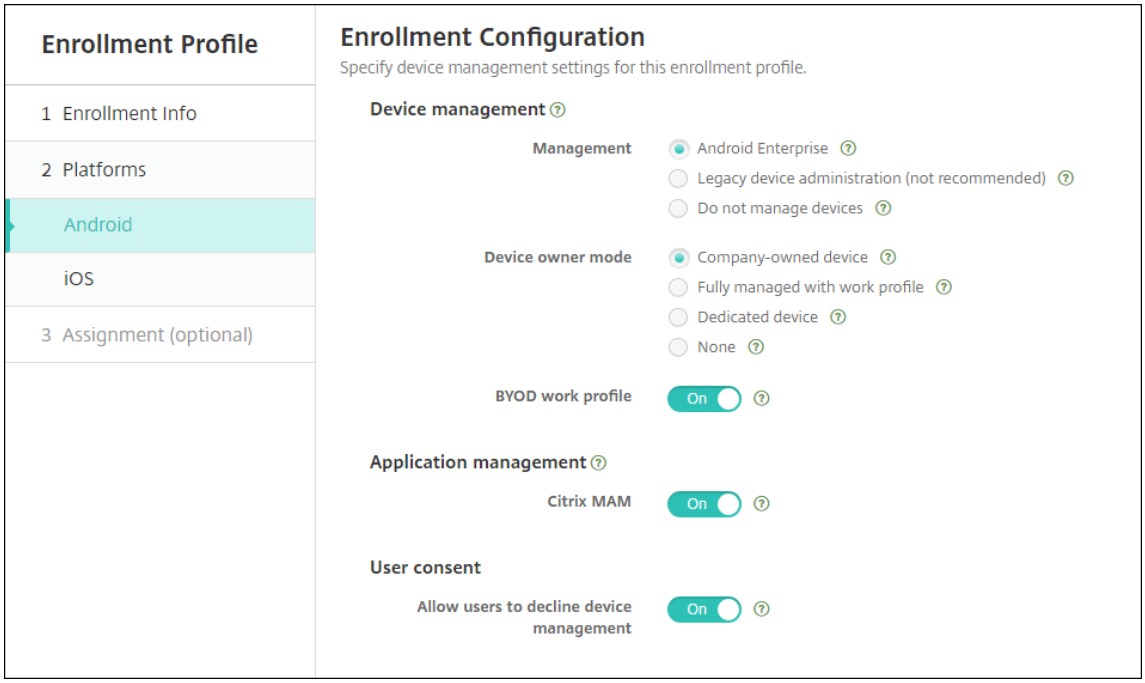
Puede utilizar perfiles de inscripción para combinar varios casos de uso, como solo MDM, MDM+MAM y solo MAM. El tipo de licencia de XenMobile Server, reflejado en la propiedad de servidor `xms.server.mode`, determina los valores disponibles en **Configurar > Perfiles de inscripción**.

Agregar un perfil de inscripción para dispositivos totalmente administrados

De forma predeterminada, los dispositivos totalmente administrados se inscriben utilizando el perfil de inscripción global, pero se pueden crear otros perfiles para inscribir dispositivos totalmente administrados.

1. En la consola de XenMobile, vaya a **Configurar > Perfiles de inscripción**.

2. Para agregar un perfil de inscripción, haga clic en **Agregar**. En la página “Información de inscripción”, escriba un nombre para el perfil de inscripción.
3. Establezca la cantidad de dispositivos que los miembros con este perfil pueden inscribir.
4. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparecerá la página Configuración de inscripción.
5. Establezca **Administración** en **Android Enterprise**.
6. Establezca **Modo propietario del dispositivo** en **Dispositivo propiedad de la empresa**.



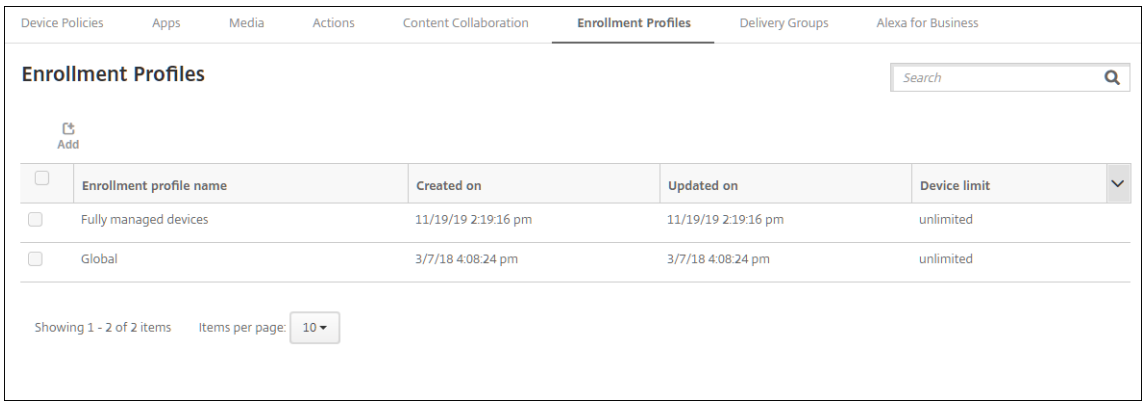
7. El **perfil de trabajo BYOD** le permite configurar el perfil de inscripción para inscribir dispositivos BYOD como dispositivos de perfil de trabajo. Los dispositivos nuevos y restablecidos a los valores de fábrica se inscriben como dispositivos totalmente administrados.
   - Establezca el **perfil de trabajo BYOD** en **Sí** para permitir la inscripción de dispositivos BYOD como dispositivos de perfil de trabajo. Está **activado** de forma predeterminada.
   - Establezca el **perfil de trabajo BYOD** en **No** para restringir la inscripción a los dispositivos totalmente administrados.
8. Elija si quiere inscribir dispositivos en Citrix MAM.
9. Si establece el **perfil de trabajo BYOD** en **Sí**, configure el consentimiento del usuario. Si quiere que los usuarios de dispositivos de perfil de trabajo BYOD puedan rechazar la administración de dispositivos al inscribirlos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Sí**.

   Si el **perfil de trabajo BYOD** está **activado**, el valor predeterminado de **Permitir a los usuarios rechazar la administración de dispositivos** es **Sí**. Si el **perfil de trabajo BYOD** está estable-

cido en **No**, la opción **Permitir a los usuarios rechazar la administración de dispositivos** está desactivada.

10. Seleccione **Asignación (opciones)**. Aparecerá la pantalla Asignación de grupos de entrega.
11. Elija un grupo o varios grupos de entrega que contengan los administradores que inscriben los dispositivos totalmente administrados. A continuación, haga clic en **Guardar**.

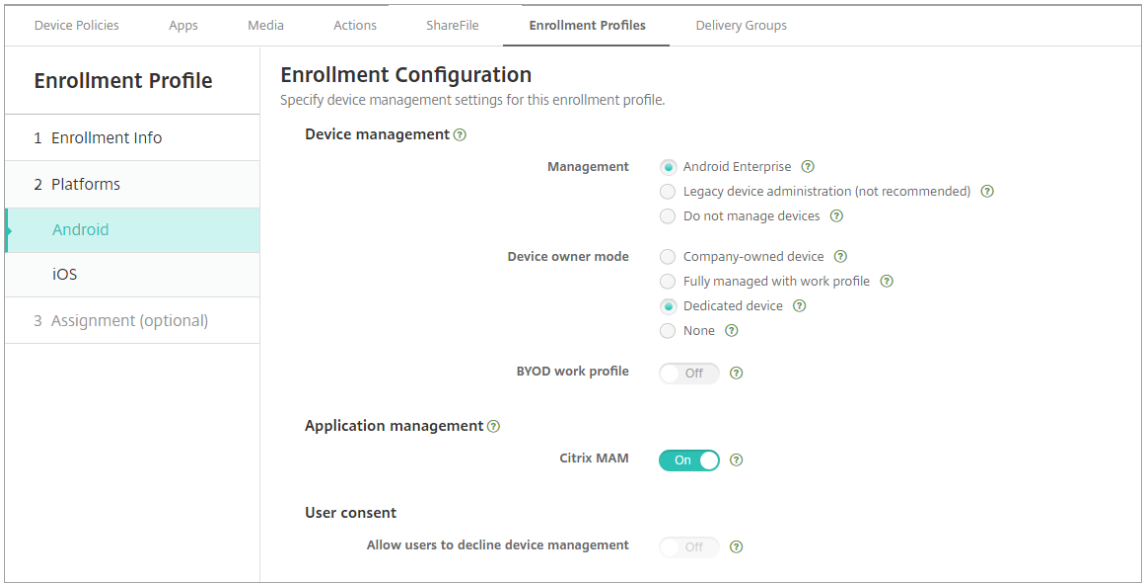
    La página "Perfil de inscripción" aparece con el perfil que agregó.



Agregar un perfil de inscripción de dispositivos dedicado

Cuando su implementación de XenMobile incluye dispositivos dedicados, un único administrador de XenMobile o un pequeño grupo de administradores inscriben muchos dispositivos dedicados. Para garantizar que estos administradores puedan inscribir todos los dispositivos necesarios, cree un perfil de inscripción para ellos con dispositivos ilimitados permitidos por usuario.

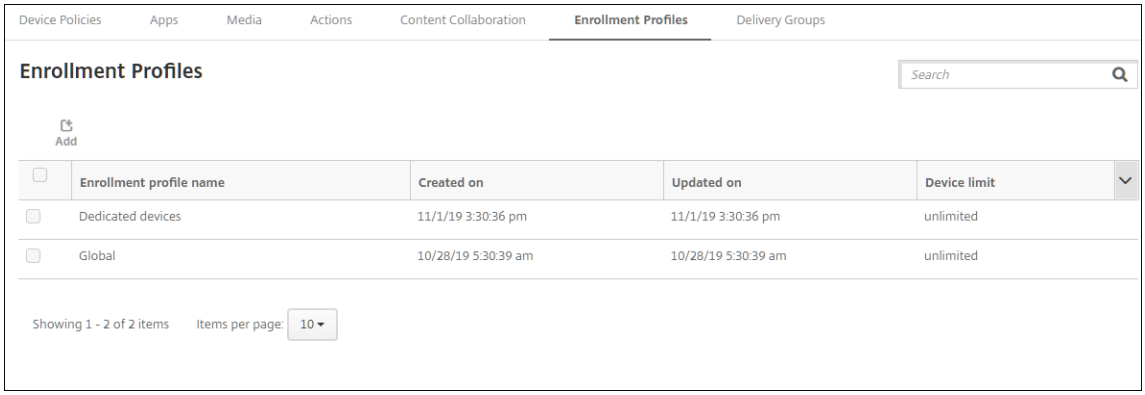
1. En la consola de XenMobile, vaya a **Configurar > Perfiles de inscripción**.
2. Para agregar un perfil de inscripción, haga clic en **Agregar**. En la página "Información de inscripción", escriba un nombre para el perfil de inscripción. Compruebe que la cantidad de dispositivos que puedan inscribir los miembros de este perfil sea ilimitada.
3. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparecerá la página Configuración de inscripción.
4. Establezca **Administración** en **Android Enterprise**.
5. Establezca **Modo propietario del dispositivo** en **Dispositivo dedicado**.



6. El **perfil de trabajo BYOD** le permite configurar el perfil de inscripción para inscribir dispositivos BYOD como dispositivos de perfil de trabajo. Los dispositivos nuevos y restablecidos a los valores de fábrica se inscriben como dispositivos dedicados. Establezca el **perfil de trabajo BYOD** en **Sí** para permitir la inscripción de dispositivos BYOD como dispositivos de perfil de trabajo. Establezca el **perfil de trabajo BYOD** en **No** para restringir la inscripción a los dispositivos propiedad de la empresa. De forma predeterminada, está **activado**.
7. Elija si quiere inscribir dispositivos en Citrix MAM.
8. Si establece el **perfil de trabajo BYOD** en **Sí**, configure el consentimiento del usuario. Si quiere que los usuarios de dispositivos de perfil de trabajo BYOD puedan rechazar la administración de dispositivos al inscribirlos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Sí**.

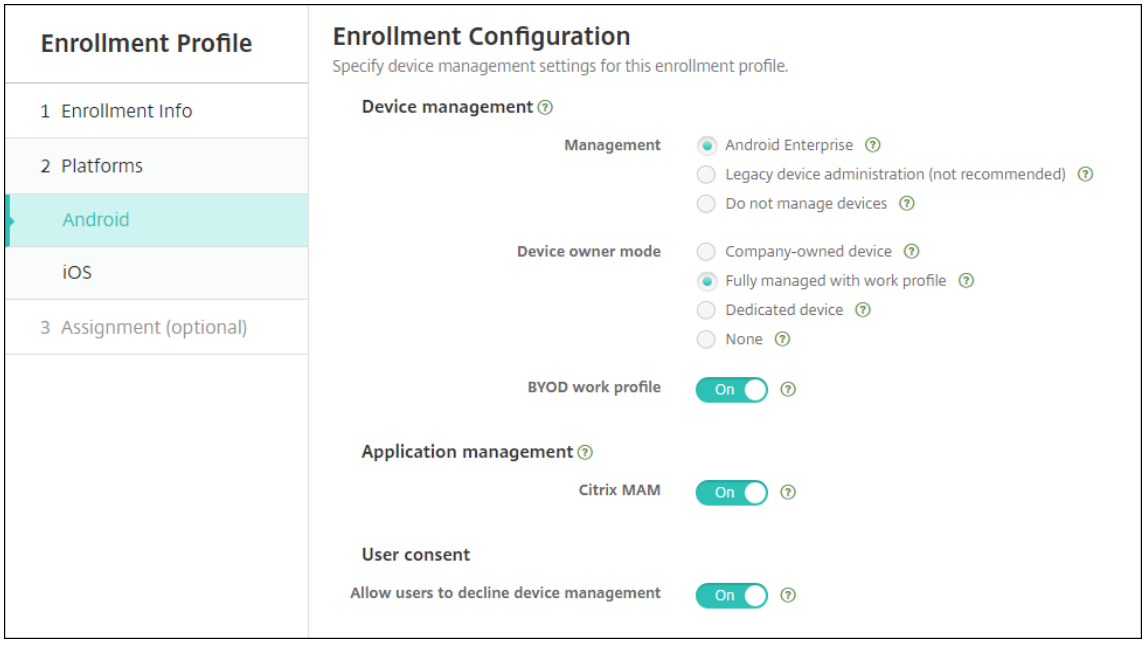
   Si el **perfil de trabajo BYOD** está **activado**, el valor predeterminado de **Permitir a los usuarios rechazar la administración de dispositivos** es **Sí**. Si el **perfil de trabajo BYOD** está establecido en **No**, la opción **Permitir a los usuarios rechazar la administración de dispositivos** está desactivada.
9. Seleccione **Asignación (opciones)**. Aparecerá la pantalla Asignación de grupos de entrega.
10. Elija un grupo o varios grupos de entrega que contengan los administradores que inscriben los dispositivos dedicados. A continuación, haga clic en **Guardar**.

    La página “Perfil de inscripción” aparece con el perfil que agregó.



Agregar un perfil de inscripción para dispositivos totalmente administrados con un perfil de trabajo

1. En la consola de XenMobile, vaya a **Configurar > Perfiles de inscripción**.
2. Para agregar un perfil de inscripción, haga clic en **Agregar**. En la página "Información de inscripción", escriba un nombre para el perfil de inscripción.
3. Establezca la cantidad de dispositivos que los miembros con este perfil pueden inscribir.
4. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparecerá la página Configuración de inscripción.
5. Establezca **Administración** en **Android Enterprise**. Establezca **Modo propietario del dispositivo** en **Totalmente administrado con perfil de trabajo**.



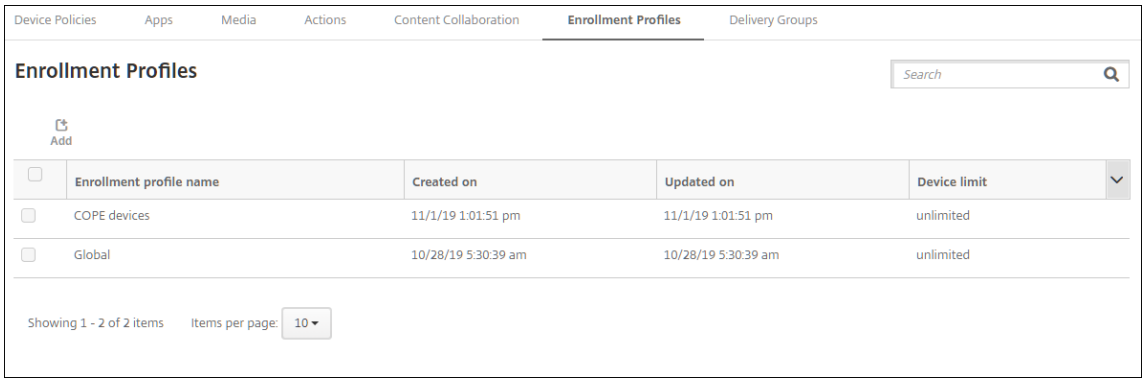
6. El **perfil de trabajo BYOD** le permite configurar el perfil de inscripción para inscribir dispositivos BYOD como dispositivos de perfil de trabajo. Los dispositivos nuevos y restablecidos a

los valores de fábrica se inscriben como dispositivos totalmente administrados con un perfil de trabajo. Establezca el **perfil de trabajo BYOD** en **Sí** para permitir la inscripción de dispositivos BYOD como dispositivos de perfil de trabajo. Establezca el **perfil de trabajo BYOD** en **No** para restringir la inscripción a los dispositivos dedicados. Está **desactivado** de forma predeterminada.

7. Elija si quiere inscribir dispositivos en Citrix MAM.
8. Si establece el **perfil de trabajo BYOD** en **Sí**, configure el consentimiento del usuario. Si quiere que los usuarios de dispositivos de perfil de trabajo BYOD puedan rechazar la administración de dispositivos al inscribirlos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Sí**.

   Si el **perfil de trabajo BYOD** está **activado**, el valor predeterminado de **Permitir a los usuarios rechazar la administración de dispositivos** es **Sí**. Si el **perfil de trabajo BYOD** está establecido en **No**, la opción **Permitir a los usuarios rechazar la administración de dispositivos** está desactivada.
9. Seleccione **Asignación (opciones)**. Aparecerá la pantalla Asignación de grupos de entrega.
10. Elija un grupo o varios grupos de entrega que contengan los administradores que inscriben los dispositivos totalmente administrados con un perfil de trabajo. A continuación, haga clic en **Guardar**.

    La página “Perfil de inscripción” aparece con el perfil que agregó.



Agregar un perfil de inscripción para dispositivos antiguos

Google va a retirar el modo de administrador de dispositivos de la administración de dispositivos. Google anima a los clientes a administrar todos los dispositivos Android en el modo propietario del dispositivo o en el modo propietario del perfil (consulte Retirada del administrador de dispositivos en las guías para desarrolladores de Google Android Enterprise).

Para habilitar este cambio:

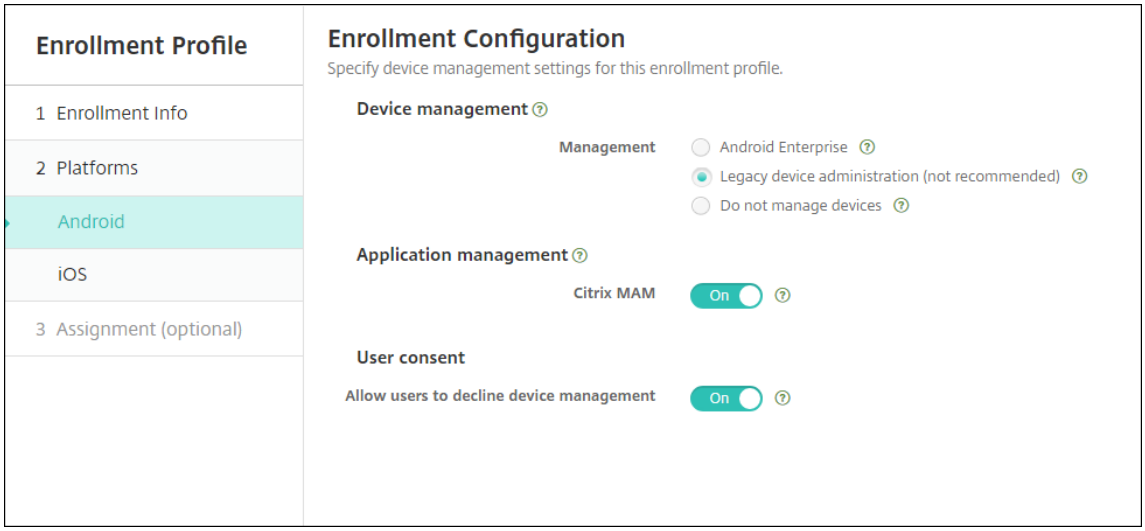
- Citrix establece Android Enterprise como opción de inscripción predeterminada para dispositivos Android.
- Si Android Enterprise está habilitado para la implementación de XenMobile, todos los dispositivos Android recién inscritos (o que se han inscrito de nuevo) se inscriben como dispositivos Android Enterprise.

Es posible que su organización no esté preparada para comenzar a administrar dispositivos Android antiguos mediante Android Enterprise. En ese caso, puede seguir administrándolos en el modo de administrador de dispositivos. En el caso de los dispositivos ya inscritos en el modo de administrador de dispositivos, XenMobile continúa administrándolos en el modo de administrador de dispositivos.

Cree un perfil de inscripción para dispositivos antiguos para permitir que las nuevas inscripciones de dispositivos Android utilicen el modo de administrador de dispositivos.

Para crear un perfil de inscripción para los dispositivos antiguos:

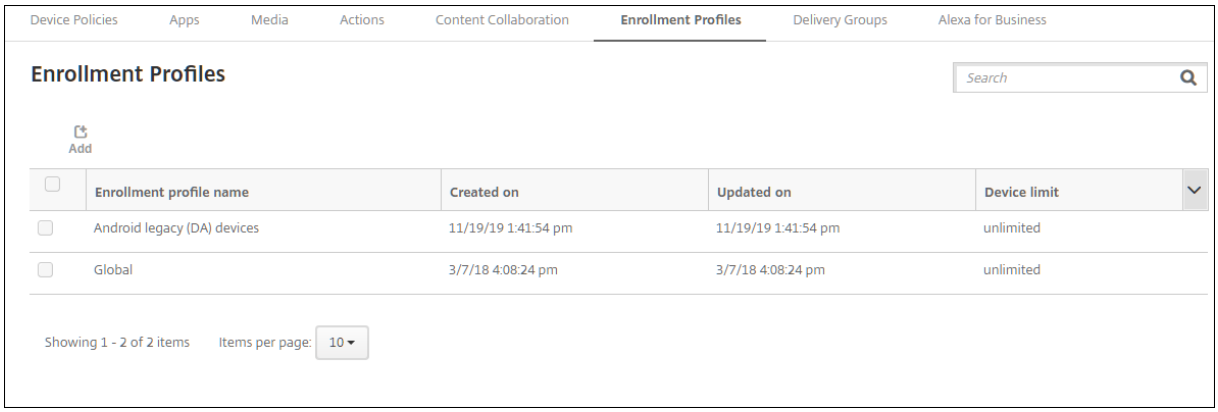
1. En la consola de XenMobile, vaya a **Configurar > Perfiles de inscripción**.
2. Para agregar un perfil de inscripción, haga clic en **Agregar**. En la página "Información de inscripción", escriba un nombre para el perfil de inscripción.
3. Establezca la cantidad de dispositivos que los miembros con este perfil pueden inscribir.
4. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparecerá la página Configuración de inscripción.
5. Establezca **Administración** en **Administración de dispositivos antigua (no se recomienda)**. Haga clic en **Siguiente**.



6. Elija si quiere inscribir dispositivos en Citrix MAM.
7. Si quiere que los usuarios puedan rechazar la administración de dispositivos al inscribirlos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Sí**. De forma predeterminada, está **activado**.

8. Seleccione **Asignación (opciones)**. Aparecerá la pantalla Asignación de grupos de entrega.
9. Elija un grupo o varios grupos de entrega que contengan los administradores que inscriben los dispositivos dedicados. A continuación, haga clic en **Guardar**.

La página “Perfil de inscripción” aparece con el perfil que agregó.



Para seguir administrando dispositivos antiguos en el modo de administrador de dispositivos, inscríbalos o vuelva a inscribirlos con este perfil. Para inscribir dispositivos de administrador de dispositivos similares a los dispositivos de perfil de trabajo, los usuarios deben descargar Secure Hub y proporcionar una URL de servidor de inscripción.

Aprovisionar dispositivos de perfil de trabajo en Android Enterprise

Los dispositivos de perfil de trabajo de Android Enterprise se inscriben en el modo propietario de perfil. Estos dispositivos no necesitan ser nuevos ni haberse restablecido a los valores de fábrica. Los dispositivos BYOD se inscriben como dispositivos de perfil de trabajo. La experiencia de inscripción es similar a la inscripción de Android en XenMobile. Los usuarios descargan Secure Hub desde Google Play e inscriben sus dispositivos.

De forma predeterminada, los parámetros de **depuración por USB y fuentes desconocidas** están inhabilitados en los dispositivos cuando estos se inscriben en Android Enterprise como dispositivos de perfil de trabajo.

Cuando inscriba dispositivos en Android Enterprise como dispositivos de perfil de trabajo, vaya siempre a Google Play. Desde allí, habilite Secure Hub para que aparezca en el perfil personal del usuario.

Aprovisionar dispositivos Android Enterprise totalmente administrados

Puede inscribir dispositivos totalmente administrados en la implementación que configuró en las secciones anteriores. Los dispositivos totalmente administrados son dispositivos propiedad de la empresa y se inscriben en el modo propietario del dispositivo. Solo los dispositivos nuevos o los restablecidos a los valores de fábrica se pueden inscribir en el modo propietario del dispositivo.

Puede inscribir dispositivos en el modo propietario del dispositivo mediante cualquiera de estos métodos de inscripción:

- **Token identificador DPC:** Con este método de inscripción, los usuarios escriben los caracteres `afw##xenmobile` al configurar el dispositivo. `afw##xenmobile` es el token identificador DPC de Citrix. Este token identifica el dispositivo como administrado por XenMobile y descarga Secure Hub de Google Play Store. Consulte Inscribir dispositivos mediante el token identificador DPC de Citrix.
- **Conexión de transmisión de datos en proximidad (NFC):** El método de inscripción de la conexión NFC transfiere datos entre dos dispositivos por transmisión de datos en proximidad. Bluetooth, Wi-Fi y otros modos de comunicación están inhabilitados en un dispositivo nuevo o que ha sido restablecido a sus valores de fábrica. NFC es el único protocolo de comunicación que el dispositivo puede utilizar en ese estado. Consulte Inscribir dispositivos con una conexión NFC.
- **Código QR:** La inscripción con códigos QR se puede utilizar para inscribir una flota distribuida de dispositivos que no admiten NFC, como las tabletas. El método de inscripción por código QR define y configura el modo de perfil del dispositivo al escanear un código QR desde el asistente de configuración. Consulte Inscribir dispositivos con un código QR.
- **Zero Touch:** La activación automática le permite configurar los dispositivos para que se inscriban automáticamente cuando se enciendan por primera vez. La activación automática se admite en algunos dispositivos Android con Android 8.0 o versiones posteriores. Consulte Activación automática.
- **Cuentas de Google:** Los usuarios introducen sus credenciales de cuenta de Google para iniciar el proceso de aprovisionamiento. Esta opción es para empresas que utilizan Google Workspace.

Inscribir dispositivos mediante el token identificador DPC de Citrix

Los usuarios escriben `afw##xenmobile` cuando se les pide que introduzcan una cuenta de Google después de encender dispositivos nuevos o restablecidos a los valores de fábrica para la configuración inicial. Esta acción descarga e instala Secure Hub. Los usuarios siguen las indicaciones de configuración de Secure Hub para completar la inscripción.

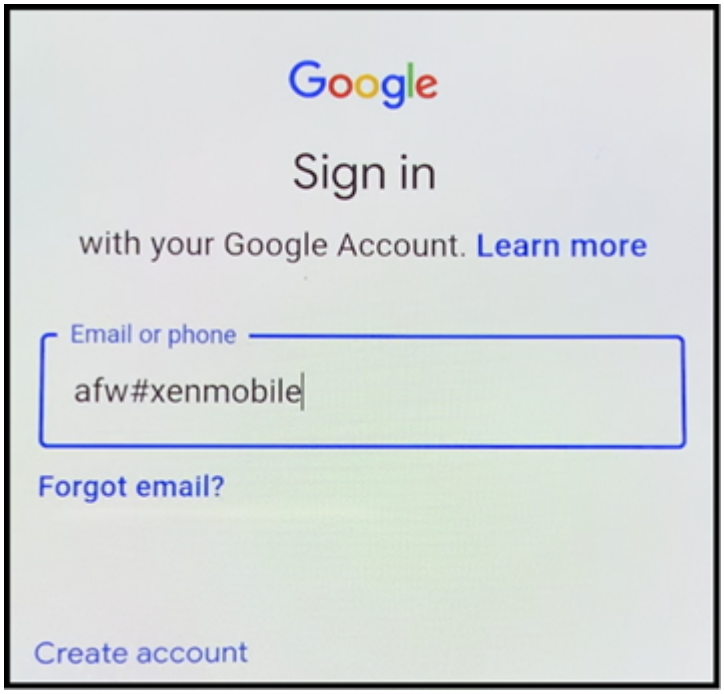
Se recomienda este método de inscripción para la mayoría de los clientes porque la versión más reciente de Secure Hub se descarga desde Google Play Store. A diferencia de otros métodos de inscripción, no es necesario proporcionar Secure Hub para descargarlo desde XenMobile Server.

Requisitos del sistema

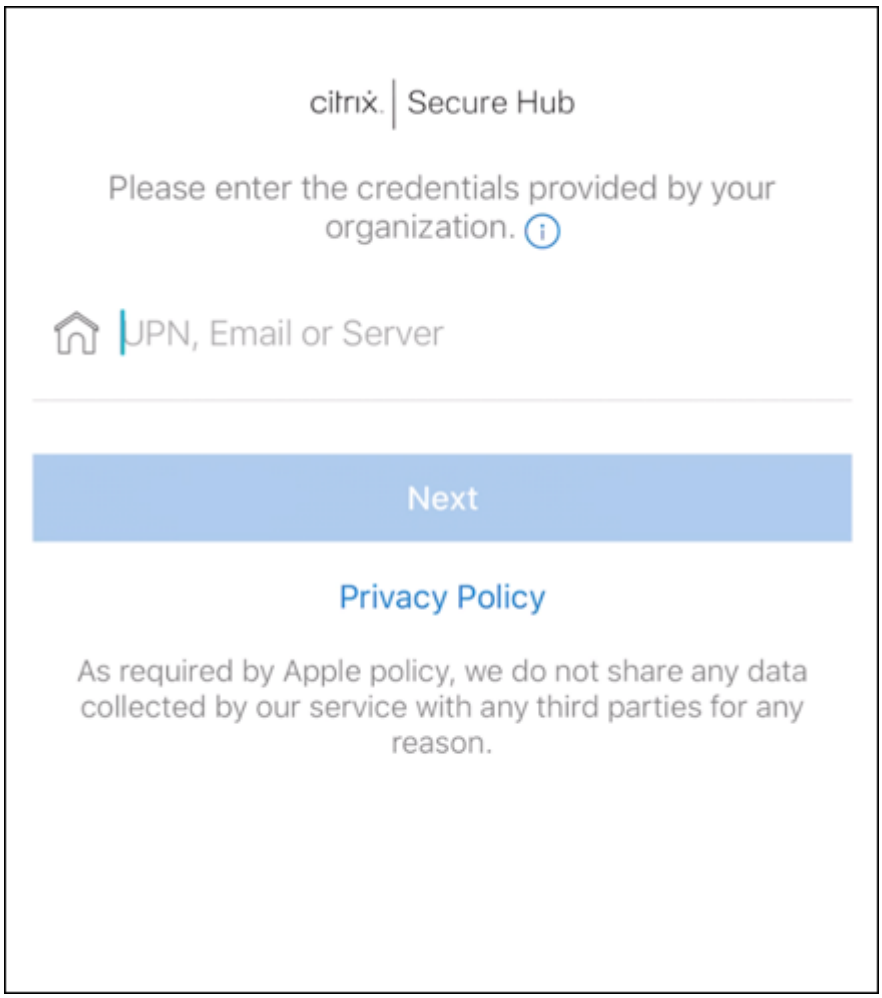
- Compatible con todos los dispositivos Android que ejecutan el sistema operativo Android.

Para inscribir el dispositivo

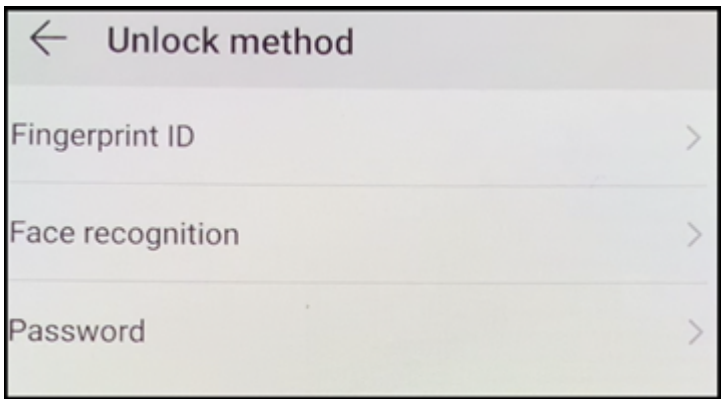
1. Encienda un dispositivo nuevo o restablecido a los valores de fábrica.
2. La configuración inicial del dispositivo se carga y solicita una cuenta de Google. Si el dispositivo carga la pantalla de inicio del dispositivo, compruebe que en la barra de notificaciones hay la notificación **Finalizar configuración**.
3. Escriba `afw##xenmobile` en el campo **Correo electrónico o Teléfono**.



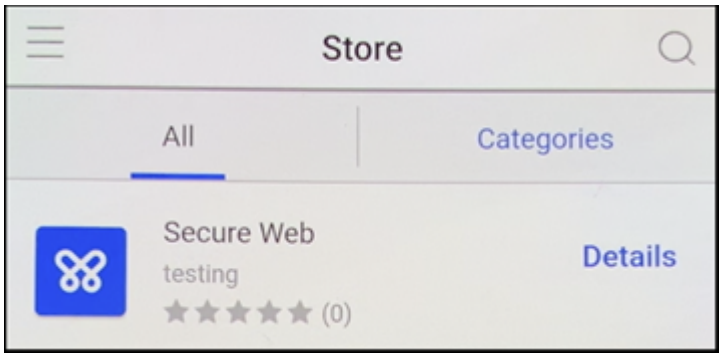
4. Toque **Instalar** en la pantalla de Android Enterprise que solicita la instalación de Secure Hub.
5. Toque **Instalar** en la pantalla del instalador de Secure Hub.
6. Toque **Permitir** para todas las solicitudes de permisos de la aplicación.
7. Toque **Aceptar y continuar** para instalar Secure Hub y permitirle que administre el dispositivo.
8. Secure Hub ya se ha instalado y se halla en la pantalla de inscripción predeterminada. En este ejemplo, la detección automática no está configurada. Si lo estuviera, el usuario puede introducir su nombre de usuario o su correo electrónico y se le encontraría un servidor. En lugar de seguir este método, introduzca la URL de inscripción del entorno y toque **Siguiente**.



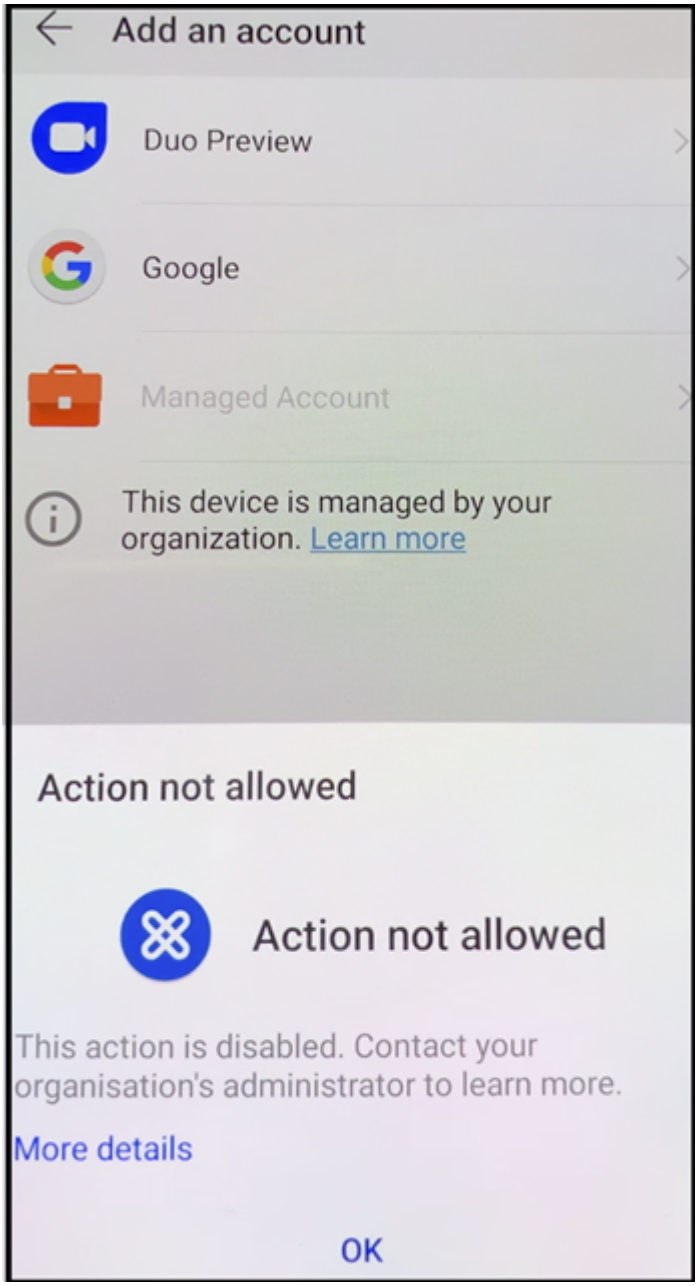
9. La configuración predeterminada de XenMobile permite a los usuarios elegir MAM o MDM+MAM. Si se le pide de esta manera, toque **Sí, inscribirlo** para elegir MDM+MAM.
10. Introduzca el nombre de usuario y la contraseña y, a continuación, toque **Siguiente**.
11. Se pide al usuario que configure un código de acceso de dispositivo. Toque **Establecer** e introduzca un código de acceso.
12. Se solicita al usuario que configure un método de desbloqueo del perfil de trabajo. En este ejemplo, toque **Contraseña** y **PIN**, e introduzca un PIN.



13. El dispositivo se encuentra ahora en la pantalla de inicio de Secure Hub **Mis aplicaciones**. Toque **Agregar aplicaciones desde la tienda**.
14. Para agregar Secure Web, toque **Secure Web**.



15. Toque **Agregar**.
16. Secure Hub dirige al usuario a Google Play Store para instalar Secure Web. Toque **Instalar**.
17. Después de que Secure Web se instale, toque **Abrir**. Introduzca una dirección URL de un sitio interno en la barra de direcciones y compruebe que se carga la página.
18. Vaya a **Parámetros > Cuentas** en el dispositivo. Observe que la **cuenta administrada** no se puede modificar. Las opciones de desarrollador para compartir la pantalla o la depuración remota también están bloqueadas.



Inscribir dispositivos con una conexión NFC

Para inscribir un dispositivo como dispositivo totalmente administrado mediante conexiones NFC, se necesitan dos dispositivos: uno que se haya restablecido a sus valores de fábrica y otro con la herramienta XenMobile Provisioning Tool.

Requisitos del sistema y requisitos previos

- Dispositivos Android compatibles.

- Un dispositivo nuevo o restablecido a los valores de fábrica, aprovisionado para Android Enterprise como un dispositivo totalmente administrado. 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 o en la página de descargas de Citrix.

Cada dispositivo solo puede tener un perfil de Android Enterprise, gestionado por Secure Hub. Solo se permite un perfil para cada dispositivo. Al intentar agregar una segunda aplicación DPC, se quita la instancia instalada de Secure Hub.

Datos transferidos a través de la conexión NFC

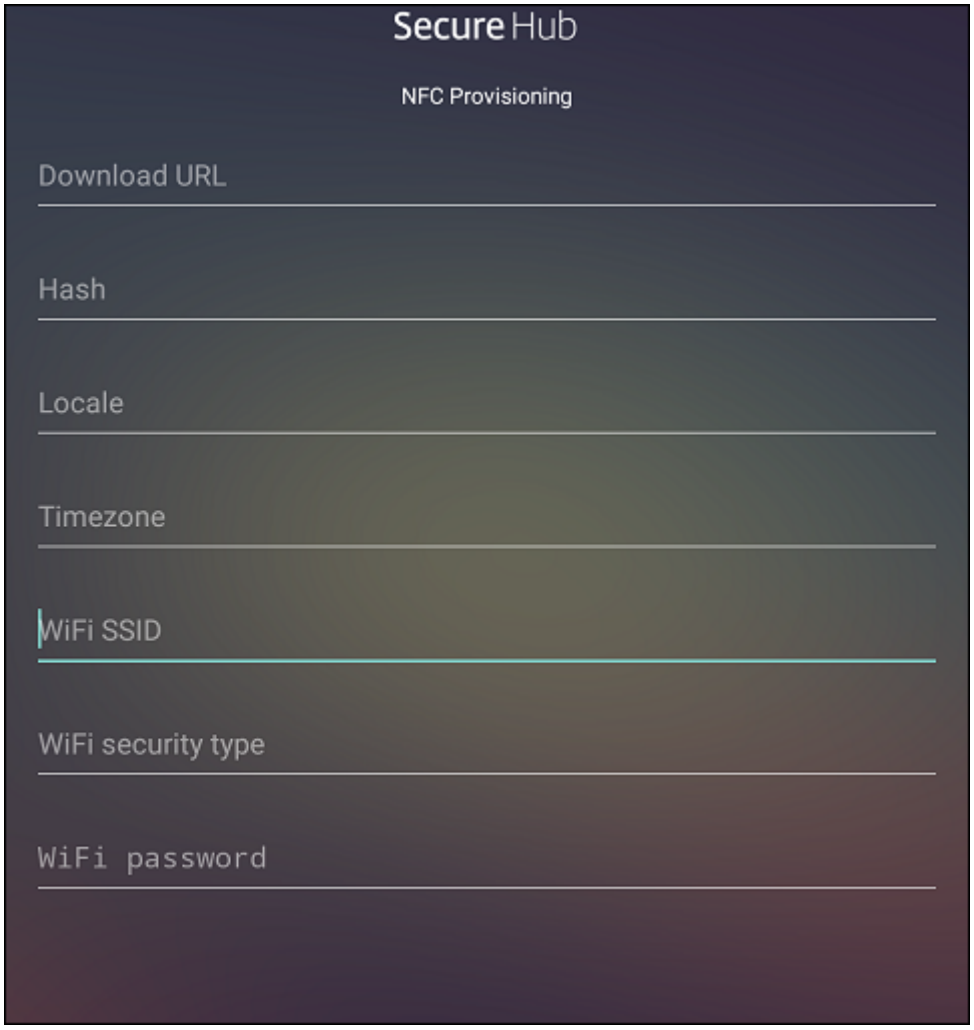
Para aprovisionar un dispositivo restablecido a sus valores de fábrica, debe enviar los siguientes datos vía una conexión NFC para inicializar Android Enterprise:

- Nombre del paquete de la aplicación DPC que actuará como propietaria del dispositivo (en este caso, Secure Hub).
- Ubicación de intranet o Internet desde donde el dispositivo puede descargar la aplicación DPC.
- Valor hash SHA1 de la aplicación DPC para verificar si la descarga se ha realizado correctamente.
- Datos de la conexión Wi-Fi para que un dispositivo restablecido a sus valores de fábrica pueda conectarse y descargar la aplicación DPC. Nota: Android no admite 802.1x Wi-Fi 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 la herramienta XenMobile Provisioning Tool

Antes de una conexión NFC, es necesario configurar la herramienta Provisioning Tool. Esta configuración se transfiere, a continuación, al dispositivo restablecido a los valores de fábrica durante la conexión NFC.



Puede introducir los datos en los campos requeridos o rellenar los campos mediante un archivo de texto. En los pasos del siguiente procedimiento, se describe cómo configurar un archivo de texto que contenga descripciones para cada campo. La aplicación no guarda información una vez introducida esta, 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 carpeta `/sdcard/` de la tarjeta SD del dispositivo. 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=<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 haya conectado a una red Wi-Fi por conexión NFC, el

dispositivo debe 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=<SHA1 hash>
```

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=<wifi ssid>
```

Esta línea es el SSID del dispositivo conectado por Wi-Fi donde se está ejecutando la herramienta Provisioning Tool.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

Los valores admitidos son WEP y WPA2. Si la red Wi-Fi no está protegida, este campo debe estar vacío.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

Si la red Wi-Fi no está protegida, este campo debe estar vacío.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

Introduzca 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=<timezone>
```

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=<package name>
```

Este dato no es necesario, porque el valor está codificado en la aplicación como “Secure Hub”. Se menciona aquí a título meramente informativo.

Si existe una red Wi-Fi protegida con WPA2, un archivo nfcprovisioning.txt completado puede tener el siguiente aspecto:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Cr
\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 Wi-Fi no protegida, un archivo nfcprovisioning.txt completado puede tener el siguiente aspecto:

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb\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 Citrix Secure Hub

La suma de comprobación de Secure Hub es un valor constante: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT-yKM. Para descargar un archivo APK destinado para Secure Hub, utilice el siguiente enlace de Google Play Store: https://play.google.com/managed/downloadManagingApp?identifier=xenmobile.

Para obtener la suma de comprobación de una aplicación

Requisitos previos:

- La herramienta **apksigner** del componente Android SDK Build-Tools
- Línea de comandos de OpenSSL

Para obtener la suma de comprobación de una aplicación, siga estos pasos:

1. Descargue el archivo APK de la aplicación desde Google Play.
2. En la línea de comandos de OpenSSL, vaya a la herramienta **apksigner**: android-sdk/build-tools/<version>/apksigner y escriba lo siguiente:

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{
 (?<=SHA-256 digest:) .* }
 '  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
<!--NeedCopy-->
```


El comando devuelve una suma de comprobación válida.

3. Para generar el código QR, introduzca la suma de comprobación en el campo `PROVISIONING_DEVICE_ADMI` . Por ejemplo:

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.
     zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"
     qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.
     PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
     play.google.com/managed/downloadManagingApp?identifier=xenmobile",
  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"
    }

 }

<!--NeedCopy-->
```

Bibliotecas utilizadas

La herramienta Provisioning Tool utiliza las bibliotecas siguientes en su código fuente:

- Biblioteca `appcompat` v7, biblioteca Design support y biblioteca Palette v7 de Google bajo la licencia de Apache 2.0

  Para obtener información, consulte Support Library Features Guide.

- Butter Knife de Jake Wharton bajo la licencia de Apache 2.0

Inscribir dispositivos con un código QR

Para inscribir dispositivos totalmente administrados mediante un código QR, debe generar un código QR. Para ello, cree un JSON y conviértalo en un código QR. La cámara del dispositivo escanea el código QR para inscribir el dispositivo.

Requisitos del sistema

- Se admite en todos los dispositivos con Android 8.0 y versiones posteriores.

Crear un código QR a partir de un JSON

Cree un JSON con los siguientes campos.

Estos campos son obligatorios:

Clave: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Valor: com.zenprise/com.zenprise.configuration.AdminFunction

Clave: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Valor: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Clave: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Valor: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

Estos campos son opcionales:

- **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.

- **android.app.extra.PROVISIONING_TIME_ZONE:** La zona horaria en que se ejecuta el dispositivo.

  Introduzca un nombre Olson con el formato área/ciudad. Por ejemplo: America/Los_Angeles para la zona horaria del Pacífico en Estados Unidos. Si no introduce ninguno, la zona horaria se rellena automáticamente.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Tiempo en milisegundos desde epoch.

  El epoch de Unix (o la hora de Unix, la hora de POSIX o la marca de hora de Unix) es la cantidad de segundos que hayan transcurridos desde el 1 de enero de 1970 (medianoche UTC/GMT). En este tiempo no se cuentan los segundos intercalares (en ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** Establézcalo en **true** para omitir el cifrado durante la creación del perfil. Establezca esta opción en **false** para forzar el cifrado durante la creación del perfil.

Un archivo JSON típico es similar al siguiente:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```


Valide el archivo JSON que se cree mediante una herramienta de validación JSON, como https://jsonlint.com. Convierta esa cadena JSON en un código QR mediante un generador de códigos QR en línea, como https://www.qr-code-generator.com.

Este código QR se escanea con un dispositivo restablecido a los valores de fábrica para inscribirlo como dispositivo totalmente administrado.

Para inscribir el dispositivo

Después de encender un dispositivo nuevo o restablecido a los valores de fábrica:

1. Toque seis veces en la pantalla de bienvenida para iniciar la inscripción por código QR.
2. Cuando se le solicite, conéctese a la Wi-Fi. Se puede acceder a la ubicación de descarga que tenga establecido Secure Hub en el código QR (codificado en JSON) a través de esta red Wi-Fi.

   Una vez que el dispositivo se haya conectado a la red Wi-Fi, descarga un lector de códigos QR desde Google e inicia la cámara.
3. Apunte la cámara al código QR para escanear el código.

   Android descarga Secure Hub desde la ubicación de descarga establecida en el código QR, valida la firma del certificado de firma, instala Secure Hub y establece el modo propietario del dispositivo.

Para obtener más información, consulte esta guía de Google para desarrolladores de Android EMM: https://developers.google.com/android/work/prov-devices#qr_code_method.

Activación automática

La activación automática le permite configurar dispositivos para que se aprovisionen como dispositivos totalmente administrados cuando al encenderse por primera vez.

Su distribuidor de dispositivos creará una cuenta para usted en el portal de activación automática de Android, una herramienta en línea que le permite aplicar configuraciones a los dispositivos. El portal de activación automática de Android le permite crear una o más configuraciones de activación automática y aplicar las configuraciones a los dispositivos asignados a su cuenta. Cuando los usuarios encienden estos dispositivos, los dispositivos se inscriben automáticamente en XenMobile. La configuración asignada al dispositivo define su proceso de inscripción automática.

Requisitos del sistema

- La activación automática se ofrece a partir de la versión Android 8.0

Información de su distribuidor sobre dispositivos y cuentas

- Los dispositivos aptos para la activación automática se compran a un distribuidor empresarial o a un socio de Google. Para obtener una lista de los socios de activación automática de Android Enterprise, consulte el sitio web de Android.
- Una cuenta de portal de activación automática de Android Enterprise, creada por su distribuidor.
- Datos de inicio de sesión de la cuenta de portal de activación automática de Android Enterprise, proporcionados por su distribuidor.

Crear una configuración de activación automática

Cuando cree una configuración de activación automática, incluya un JSON personalizado para especificar los detalles de la configuración.

Utilice este JSON para configurar el dispositivo para que se inscriba en el servidor de XenMobile Server que especifique. Sustituya la URL de su servidor por "URL" en este ejemplo.

```
1        {
2
3            "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6                "serverURL":"URL",
7            }
8
9         }
10
11 <!--NeedCopy-->
```

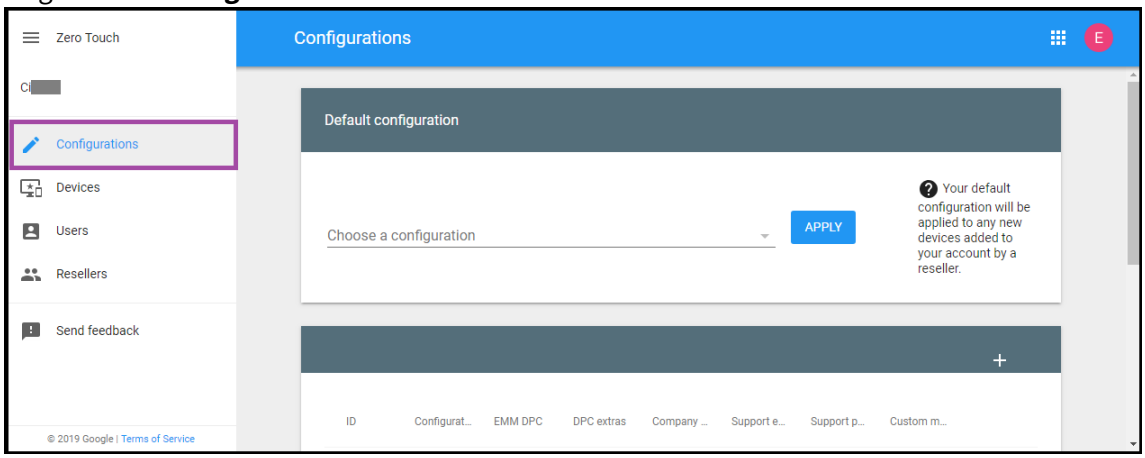
Puede utilizar un JSON opcional con más parámetros para personalizar su configuración en mayor profundidad. En este ejemplo, se especifica la instancia de XenMobile Server y el nombre de usuario y la contraseña que utilizan los dispositivos con esta configuración para iniciar sesión en el servidor.

```
1       {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4            {
5
6                "serverURL":"URL",
7                "xm_username":"username",
8                "xm_password":"password"
9             }
10
```

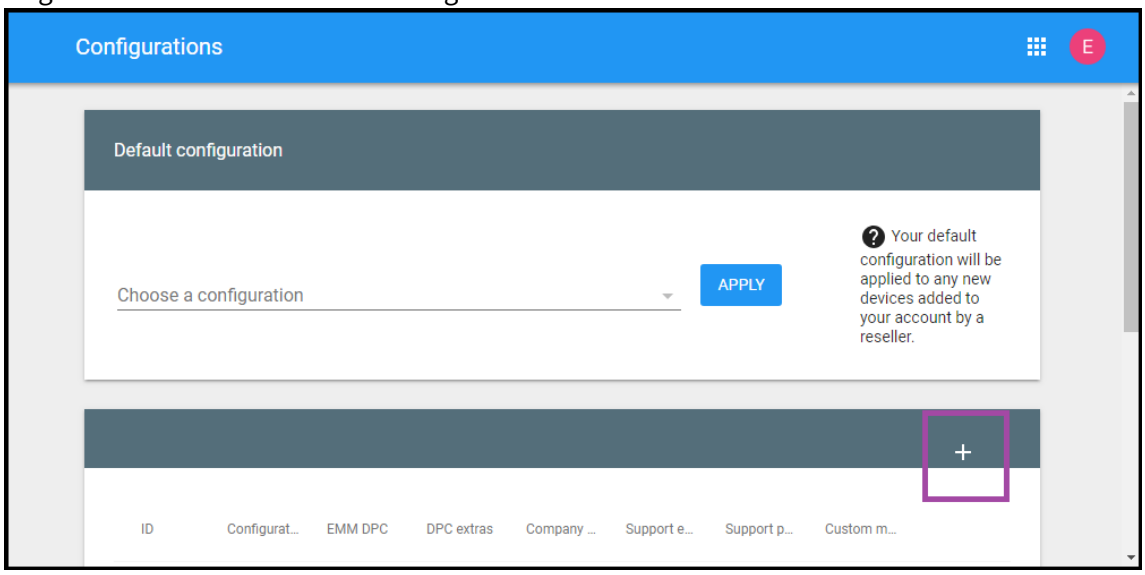


```
11                }
12
13    <!--NeedCopy-->
```

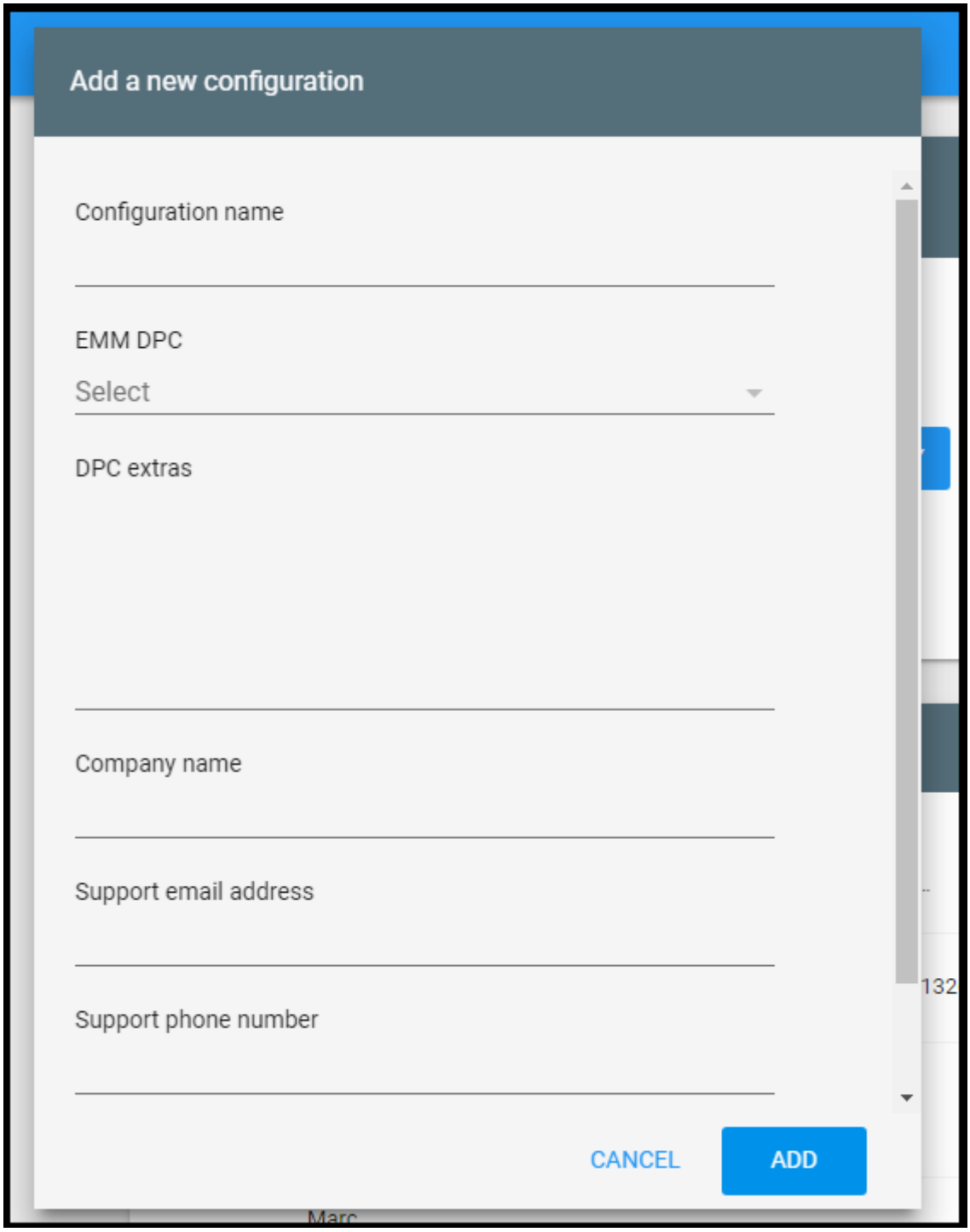
1. Vaya al portal de activación automática de Android en https://partner.android.com/zerotouch. Inicie sesión con la información de la cuenta de su distribuidor de dispositivos de activación automática.
2. Haga clic en **Configuraciones**.



3. Haga clic en **+** sobre la tabla de configuración.



4. Introduzca la información de configuración en la ventana de configuración que aparece.

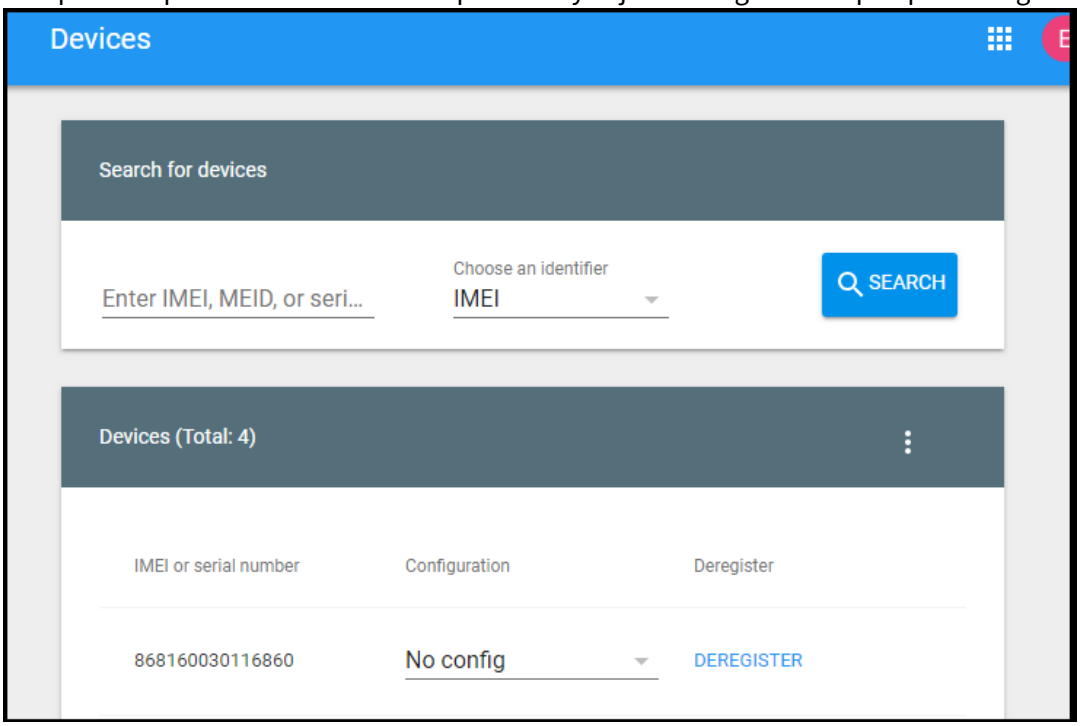


- **Nombre de configuración:** Escriba el nombre que quiera para esta configuración.
- **Controlador de políticas de dispositivo de EMM:** Elija **Citrix Secure Hub**.
- **Información adicional de DPC:** Pegue el texto JSON personalizado en este campo.
- **Nombre de empresa:** Escriba el nombre que quiera que aparezca en sus dispositivos Android Enterprise de activación automática durante el aprovisionamiento del dispositivo.
- **Dirección de correo de electrónico de asistencia:** Escriba una dirección de correo elec-

trónico con la que los usuarios puedan ponerse en contacto para obtener ayuda. Esta dirección aparece en los dispositivos Android Enterprise de activación automática antes del aprovisionamiento de dispositivos.

- **Teléfono de asistencia:** Escriba un número de teléfono con el que los usuarios puedan ponerse en contacto para obtener ayuda. Este número de teléfono aparece en los dispositivos Android Enterprise de activación automática antes del aprovisionamiento de dispositivos.
- **Mensaje personalizado:** Si quiere, agregue una o dos frases para ayudar a los usuarios a ponerse en contacto con usted o para darles más detalles sobre lo que ocurre con su dispositivo. Este mensaje personalizado aparece en los dispositivos Android Enterprise de activación automática antes del aprovisionamiento de dispositivos.

5. Haga clic en **Agregar**.
6. Para crear más configuraciones, repita los pasos 2, 3 y 4.
7. Para aplicar una configuración a un dispositivo:
   a) En el portal de activación automática de Android, haga clic en **Dispositivos**.
   b) Busque el dispositivo en la lista de dispositivos y elija la configuración que quiera asignar.



   c) Haga clic en **Update**.

Puede aplicar una configuración a muchos dispositivos mediante un archivo CSV.

Para obtener información sobre cómo aplicar una configuración a muchos dispositivos, consulte el tema de ayuda Activación automática para administradores de TI de Android Enterprise. Esta sección

de ayuda de Android Enterprise contiene más información sobre cómo administrar configuraciones y aplicarlas a los dispositivos.

Aprovisionar dispositivos Android Enterprise dedicados

Los dispositivos Android Enterprise dedicados son dispositivos totalmente administrados que se destinan a cumplir un solo caso de uso. Los dispositivos dedicados también se conocen como dispositivos de uso único y propiedad de la empresa (COSU). Así, restringe estos dispositivos a una aplicación o a un pequeño conjunto de aplicaciones que permitan realizar las tareas necesarias para este caso de uso. También impide que los usuarios habiliten otras aplicaciones o realicen otras acciones en el dispositivo.

Inscriba los dispositivos dedicados mediante cualquiera de los métodos de inscripción utilizados para otros dispositivos totalmente administrados, como se describe en Aprovisionar dispositivos Android Enterprise totalmente administrados. Aprovisionar dispositivos dedicados requiere una configuración adicional antes de inscribirlos.

Para aprovisionar dispositivos dedicados:

- Agregue un perfil de inscripción para los administradores de XenMobile a los que permite inscribir dispositivos dedicados en su implementación de XenMobile. Consulte Crear perfiles de inscripción.
- Permita las aplicaciones a las que quiera que acceda el dispositivo dedicado.
- Si quiere, configure la aplicación permitida para permitir el modo de bloqueo de tarea. Cuando una aplicación se encuentra en el modo de bloqueo de tarea, esa aplicación queda anclada a la pantalla del dispositivo cuando el usuario la abre. No aparece el botón Inicio y el botón Atrás está desactivado. El usuario sale de la aplicación mediante una acción programada en la aplicación, como cerrar sesión.
- Inscriba cada dispositivo en el perfil de inscripción que ha agregado.

Requisitos del sistema

- La inscripción de dispositivos Android dedicados comienza a ofrecerse a partir de Android 6.0.

Permitir aplicaciones y establecer el modo de bloqueo de tarea

Con la directiva Quiosco, puede permitir aplicaciones y establecer el modo de bloqueo de tarea. De forma predeterminada, se permiten los servicios Secure Hub y Google Play.

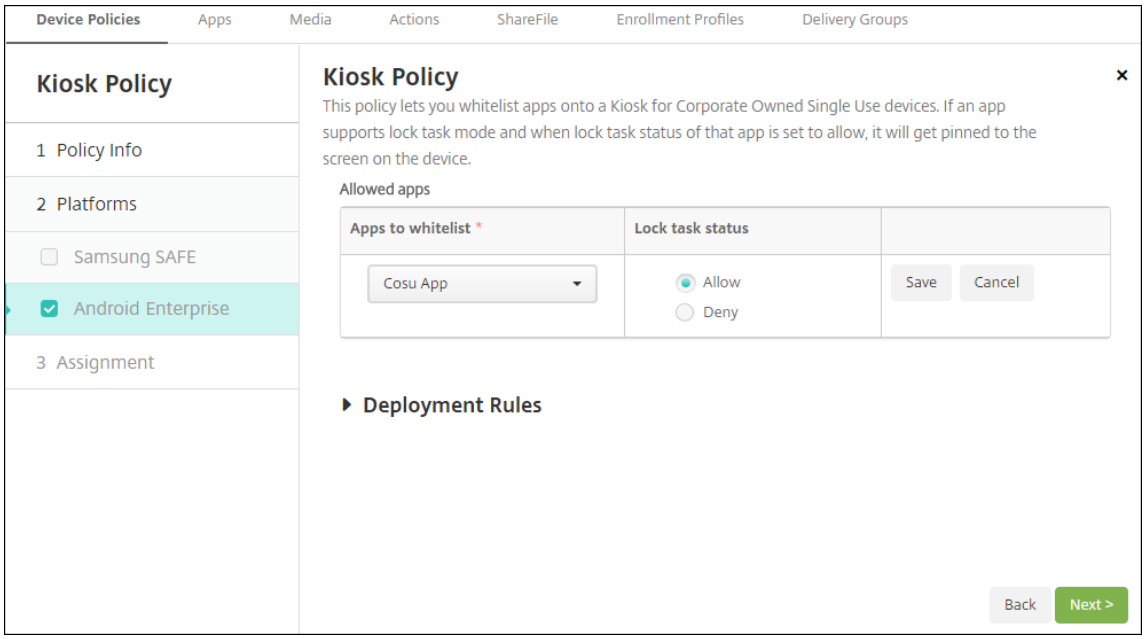
Para agregar la directiva de quiosco

1. En la consola de XenMobile, haga clic en **Configurar > Directivas de dispositivo**. Aparecerá la página **Directivas de dispositivo**.

2. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar nueva directiva**.
3. Expanda **Más** y, a continuación, en "Seguridad", haga clic en **Quiosco**. Aparecerá la página de asignación **Directiva de quiosco**.
4. En Plataformas, seleccione **Android Enterprise**. Desmarque las demás plataformas.
5. En el panel "Información de directiva", escriba el **nombre de la directiva** y una **descripción** opcional.
6. Haga clic en **Siguiente** y, a continuación, en **Agregar**.
7. Para permitir una aplicación y permitir o denegar el modo de bloqueo de tarea para esa aplicación:

   En la lista, seleccione la aplicación que quiere permitir.

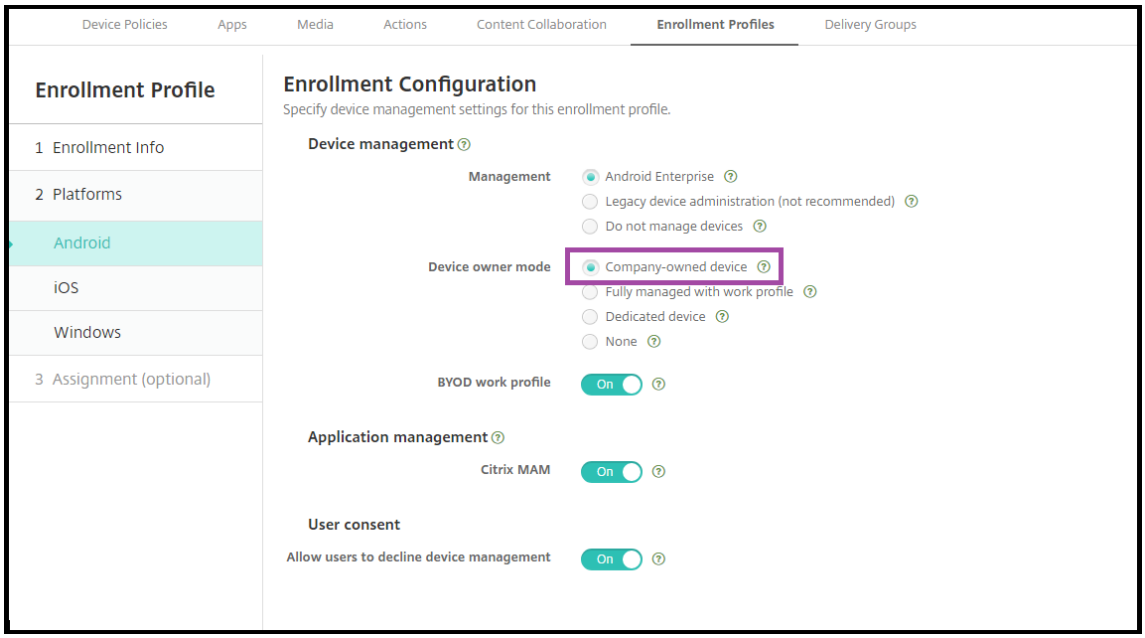
   Seleccione **Permitir** para que la aplicación quede anclada en la pantalla del dispositivo cuando el usuario la abra. Elija **Denegar** para que la aplicación no quede anclada. El valor predeterminado es **Permitir**.



8. Haga clic en **Guardar**.
9. Para permitir otra aplicación y permitir o denegar el modo de bloqueo de tarea para esa aplicación, haga clic en **Agregar**.
10. Configure las reglas de implementación y elija los grupos de entrega. Para obtener más información, consulte Directivas de dispositivo.

Para inscribir el dispositivo

1. Haga clic en **Siguiente** o seleccione **Android** en **Plataformas**. Aparecerá la página Configuración de inscripción.
2. Establezca **Administración** en **Android Enterprise**.
3. Establezca **Modo propietario del dispositivo** en **Dispositivo propiedad de la empresa**.



4. Seleccione **Asignación (opciones)**. Aparecerá la pantalla Asignación de grupos de entrega.
5. Elija un grupo o varios grupos de entrega que contengan los administradores que inscriben los dispositivos dedicados. A continuación, haga clic en **Guardar**.

Si ha habilitado el **perfil de trabajo BYOD** en el perfil de inscripción, los dispositivos que no son nuevos o restablecidos a los valores de fábrica se inscriben como dispositivos de perfil de trabajo. Consulte Aprovisionar dispositivos de perfil de trabajo en Android Enterprise.

Aprovisionar dispositivos totalmente administrados con un perfil de trabajo (dispositivos COPE) en Android Enterprise

Los dispositivos totalmente administrados con un perfil de trabajo, conocidos anteriormente como dispositivos COPE, son dispositivos propiedad de la empresa que están pensados tanto para el trabajo como para fines personales. Su organización administra estos dispositivos totalmente. Puede aplicar un conjunto de directivas al dispositivo y un conjunto de directivas diferente al perfil de trabajo.

En la consola de XenMobile, los dispositivos totalmente administrados con un perfil de trabajo aparecen con estos términos:

- El propietario del dispositivo es “Empresa”.

- El tipo de instalación del dispositivo en Android Enterprise es “COPE (propiedad de la empresa con acceso privado)”.

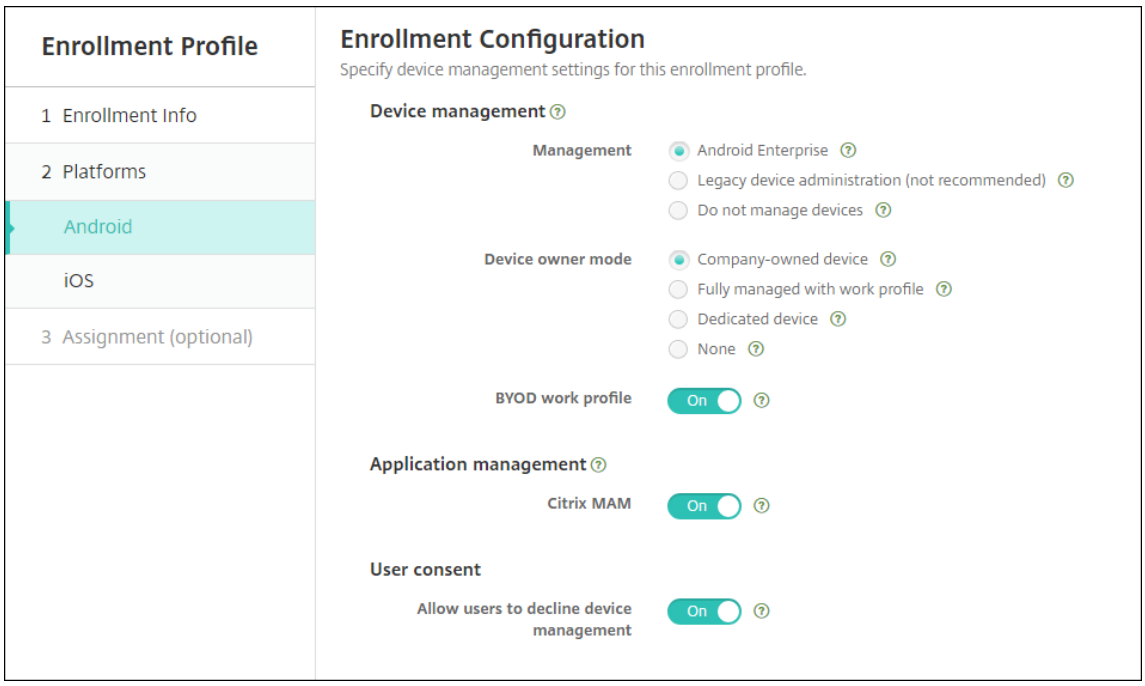
Requisitos del sistema

- La inscripción de dispositivos totalmente administrados con perfiles de trabajo se admite de Android 8.0 a Android 10.x.

Agregar un perfil de inscripción para dispositivos totalmente administrados con perfiles de trabajo

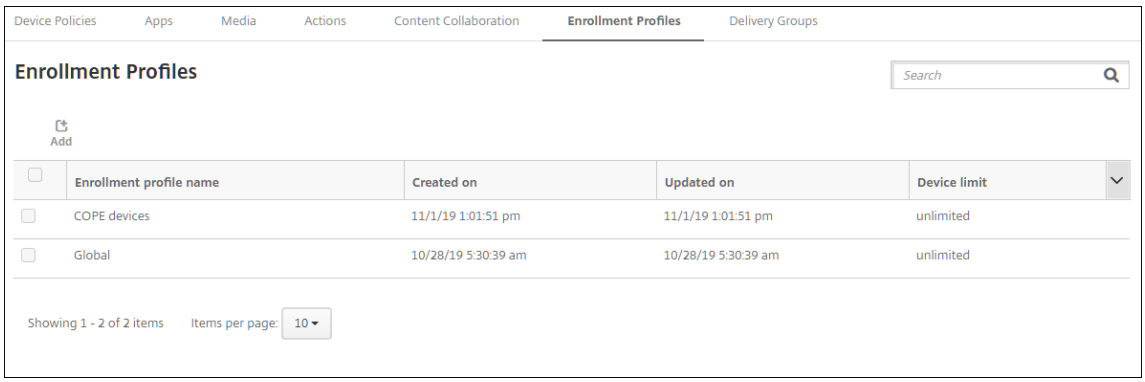
Cree un perfil de inscripción para inscribir dispositivos totalmente administrados con perfiles de trabajo. Los administradores de los grupos de entrega asignados a este perfil de inscripción pueden inscribir dispositivos totalmente administrados con perfiles de trabajo. Para garantizar que estos administradores puedan inscribir todos los dispositivos necesarios, cree un perfil de inscripción para ellos con dispositivos ilimitados permitidos por usuario. Asigne este perfil a un grupo de entrega que contenga los administradores que inscriban dispositivos totalmente administrados con perfiles de trabajo.

1. En la consola de XenMobile, vaya a **Configurar > Perfiles de inscripción**.
2. Para agregar un perfil de inscripción, haga clic en **Agregar**. En la página “Información de inscripción”, escriba un nombre para el perfil de inscripción. Compruebe que la cantidad de dispositivos que puedan inscribir los miembros de este perfil sea ilimitada.
3. Haga clic en **Siguiente** o seleccione **Android Enterprise** en **Plataformas**. Aparecerá la página Configuración de inscripción.
4. Establezca el **tipo de inscripción** en una de las siguientes opciones:
    - **Totalmente administrado/Perfil de trabajo:** Los nuevos dispositivos o los restablecidos a los valores de fábrica se inscriben totalmente administrados. Los dispositivos BYOD se inscriben únicamente con un perfil de trabajo administrado por usted.
    - **COPE/Perfil de trabajo:** Los dispositivos nuevos y restablecidos a los valores de fábrica se inscriben como dispositivos totalmente administrados con un perfil de trabajo. Los dispositivos BYOD se inscriben únicamente con un perfil de trabajo administrado por usted.



5. Seleccione **Asignación (opcional)** o haga clic en **Siguiente**. Aparecerá la pantalla Asignación de grupos de entrega.
6. Elija un grupo o varios grupos de entrega que contengan los administradores que inscriben los dispositivos dedicados. A continuación, haga clic en **Guardar**.

   La página “Perfil de inscripción” aparece con el perfil que agregó.



Si un usuario pertenece a varios grupos de entrega que tienen perfiles de inscripción diferentes, el nombre del grupo de entrega determina el perfil de inscripción utilizado. XenMobile selecciona el grupo de entrega que aparece en último lugar en una lista alfabética de grupos de entrega.

Para inscribir el dispositivo

Los dispositivos nuevos y los restablecidos a los valores de fábrica se inscriben como dispositivos totalmente administrados con un perfil de trabajo mediante el token identificador DPC, la conexión de

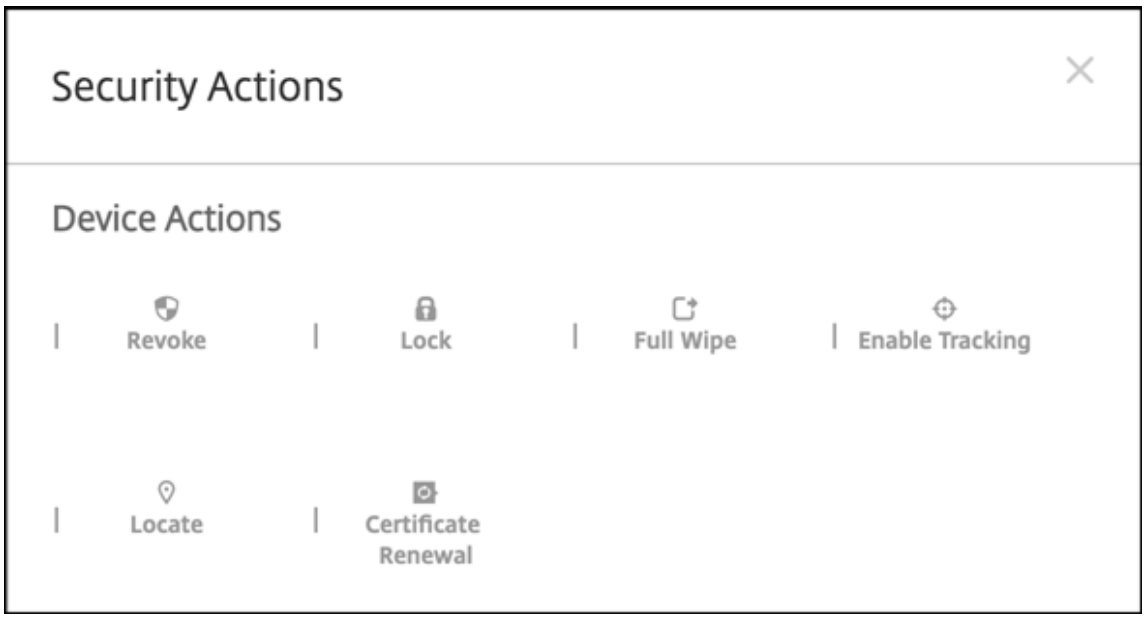
transmisión de datos en proximidad (NFC) o los métodos de código QC. Consulte Inscribir dispositivos mediante el token identificador DPC de Citrix, Inscribir dispositivos con una conexión NFC o Inscribir dispositivos con un código QR.

Los dispositivos que no son nuevos o restablecidos a los valores de fábrica se inscriben como dispositivos de perfil de trabajo como se describe en Aprovisionar dispositivos de perfil de trabajo en Android Enterprise.

Ver dispositivos Android Enterprise en la consola de XenMobile

1. En la consola de XenMobile, vaya a **Administrar > Dispositivos**.
2. Para agregar la columna **¿Dispositivo habilitado para Android Enterprise?**, haga clic en el menú situado a la derecha de la tabla de esta página.

3. Para ver las acciones de seguridad disponibles, seleccione un dispositivo totalmente administrado y haga clic en **Proteger**. Cuando el dispositivo está totalmente administrado, la acción **Borrado completo** está disponible, pero **Borrado selectivo** no. Esta diferencia se debe a que el dispositivo solo permite aplicaciones de Google Play Store administrado. No hay una opción para que el usuario instale aplicaciones desde la tienda pública. Su organización administraba todo el contenido del dispositivo.



Configurar directivas de aplicaciones y de dispositivo para Android Enterprise

Para obtener información general de las directivas controladas tanto a nivel de dispositivo como de aplicación, consulte Directivas MDX y directivas de dispositivo compatibles con Android Enterprise.

Qué debe saber sobre las directivas:

- **Protección contra la pérdida de datos:** La tecnología de contenedores MAM de XenMobile protege las aplicaciones con cifrado y otras tecnologías de prevención de pérdida de datos (DLP) móviles. Utilice el SDK de Citrix MAM o MDX Toolkit para habilitar MDX en las aplicaciones.
- **Restricciones a dispositivos:** Docenas de restricciones para los dispositivos le permiten controlar funciones como:
  - El uso de la cámara del dispositivo
  - Copiar y pegar contenido entre perfiles personales y de trabajo
- **VPN por aplicación:** Utilice la directiva Configuraciones administradas para configurar perfiles de VPN para Android Enterprise.
- **Directiva de correo electrónico:** Se recomienda utilizar la directiva Configuraciones administradas para configurar aplicaciones.

En esta tabla se indican todas las directivas de dispositivo disponibles para dispositivos Android Enterprise.

> **Importante:**
>
> Para los dispositivos que se inscriben en Android Enterprise y utilizan aplicaciones MDX, puede controlar algunos parámetros a través de MDX y Android Enterprise. Utilice la configuración de

> directiva menos restrictiva para MDX y controle la directiva a través de Android Enterprise.

Permisos de aplicación de Android Enterprise	Configuraciones administradas por Android Enterprise	Inventario de aplicaciones
Desinstalación de aplicaciones	Actualizar automáticamente aplicaciones administradas	Controlar actualización del SO
Credenciales	XML personalizado	Exchange
Archivos	Administración de Keyguard	Quiosco
Ubicación	Código de acceso	Restricciones
Clave de licencia MDM de Samsung	Programación	Wi-Fi
Opciones de XenMobile		

Directivas de dispositivo para los dispositivos totalmente administrados con un perfil de trabajo (dispositivos COPE)

En el caso de los dispositivos totalmente administrados con perfiles de trabajo (dispositivos COPE), se pueden usar algunas directivas de dispositivo para aplicar configuraciones diferentes a todo el dispositivo y al perfil de trabajo. También puede usar otras directivas de dispositivo para aplicar una configuración solo a todo el dispositivo o solo al perfil de trabajo.

Directiva	Aplicable a
Permisos de aplicación de Android Enterprise	Perfil de trabajo
Configuraciones administradas por Android Enterprise	Perfil de trabajo
Inventario de aplicaciones	Perfil de trabajo
Desinstalación de aplicaciones	Perfil de trabajo
Actualizar automáticamente aplicaciones administradas	Perfil de trabajo
Controlar actualización del SO	N/D
Credenciales	Perfil de trabajo
XML personalizado	N/D

Directiva	Aplicable a
Exchange	N/D
Archivos	Perfil de trabajo
Administración de Keyguard	Dispositivo y perfil de trabajo
Quiosco	N/D
Ubicación	Dispositivo (solo modo de ubicación)
Código de acceso	Dispositivo y perfil de trabajo
Restricciones	Dispositivo y perfil de trabajo (crear directivas separadas para el dispositivo y el perfil de trabajo)
Clave de licencia MDM de Samsung	N/D
Programación	Perfil de trabajo
Wi-Fi	Dispositivo
Opciones de XenMobile	Perfil de trabajo

Consulte también Directivas MDX y directivas de dispositivo compatibles con Android Enterprise e Introducción al SDK de MAM.

Acciones de seguridad

Android Enterprise admite las siguientes acciones de seguridad. Para ver una descripción de cada acción de seguridad, consulte Acciones de seguridad.

Acción de seguridad	Perfil de trabajo	Totalmente administrado
Renovación de certificados	Sí	Sí
Borrado completo	No	Sí
Localizar	Sí	Sí
Bloquear	Sí	Sí
Bloqueo y restablecimiento de contraseña	No	Sí
Notificar (Hacer sonar)	Sí	Sí
Revocar	Sí	Sí

Acción de seguridad	Perfil de trabajo	Totalmente administrado
Borrado selectivo	Sí	No

Notas de acciones de seguridad

- La acción de seguridad “Localizar” falla, a menos que la directiva Localización establezca el modo de ubicación para el dispositivo en **Alta precisión** o **Ahorro de batería**. Consulte Directiva de ubicación.
- En dispositivos de perfil de trabajo con versiones de Android anteriores a Android 8.0:
  - La acción de bloqueo y restablecimiento de contraseña no es compatible.
- En dispositivos de perfil de trabajo con la versión de Android 8.0 o posterior:
  - El código de acceso enviado bloquea el perfil de trabajo. El dispositivo en sí no se bloquea.
  - Si no hay un código de acceso establecido en el perfil de trabajo:
    - Si no se envía ningún código de acceso o el código enviado no cumple los requisitos de código de acceso, el dispositivo se bloquea.
  - Si hay un código de acceso establecido en el perfil de trabajo:
    - Si no se envía ningún código de acceso o el código enviado no cumple los requisitos de código de acceso, el perfil de trabajo se bloquea, pero el dispositivo no se bloquea.
- En dispositivos totalmente administrados con perfiles de trabajo (dispositivos COPE):
  - Puede aplicar la acción de seguridad Bloquear por separado al dispositivo o al perfil de trabajo.

Desinscribir una empresa de Android Enterprise

Si ya no quiere utilizar su empresa de Android Enterprise, puede desinscribirla.

> **Advertencia:**
>
> Una vez que desinscriba una empresa, las aplicaciones de Android Enterprise en dispositivos ya inscritos a través de ella se restablecen a sus estados predeterminados. Google ya no administra los dispositivos. Si se inscribe en una nueva empresa de Android Enterprise, deberá aprobar aplicaciones para la nueva organización desde Google Play administrado. A continuación, puede actualizar las aplicaciones desde la consola de XenMobile.

Después de que la empresa Android Enterprise se ha desinscrito:

- En los dispositivos y los usuarios inscritos a través de la empresa, las aplicaciones de Android Enterprise se restablecen a sus estados predeterminados. Las directivas de configuraciones administradas por Android Enterprise aplicadas ya no afectan a las operaciones.

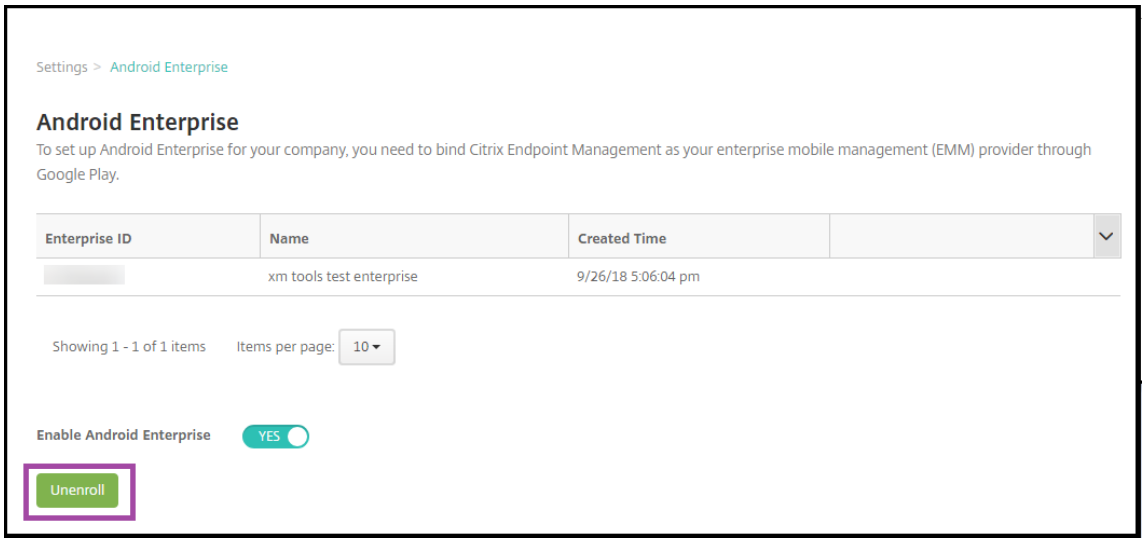
- XenMobile administra los dispositivos inscritos a través de la empresa. Desde el punto de vista de Google, esos dispositivos no están administrados. No puede agregar nuevas aplicaciones de Android Enterprise. No se pueden aplicar directivas de configuraciones administradas por Android Enterprise. Se pueden aplicar otras directivas, tales como Programación, Contraseña y Restricciones, a estos dispositivos.
- Si intenta inscribir dispositivos en Android Enterprise, se inscriben como dispositivos Android, no como dispositivos Android Enterprise.

Puede desinscribir una empresa de Android Enterprise desde la consola de XenMobile Server y con la ayuda de las herramientas de XenMobile Tools.

Cuando realiza esta tarea, XenMobile abre una ventana emergente para XenMobile Tools. Antes de comenzar, compruebe que XenMobile tenga permiso para abrir ventanas emergentes en el explorador web que esté utilizando. Algunos exploradores web, como Google Chrome, requieren que se inhabilite el bloqueo de ventanas emergentes y se agregue la dirección del sitio de XenMobile a la lista de permitidos para bloquear ventanas emergentes.

Para desinscribir una empresa de Android Enterprise

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página Parámetros.
2. En la página Parámetros, haga clic en **Android Enterprise**.
3. Haga clic en **Desinscribir**.



Distribuir aplicaciones de Android Enterprise

January 4, 2022

XenMobile administra las aplicaciones implementadas en los dispositivos. Puede organizar e implementar los siguientes tipos de aplicaciones de Android Enterprise.

- **Aplicaciones de la tienda de aplicaciones administrada:** Estas aplicaciones incluyen aplicaciones gratuitas o de pago disponibles en Google Play Store administrado. Por ejemplo, GoToMeeting.
- **MDX:** Aplicaciones preparadas con el SDK de MAM o empaquetadas con MDX Toolkit. Estas aplicaciones incluyen directivas MDX. Las aplicaciones MDX se obtienen de fuentes internas y tiendas públicas. Implemente aplicaciones móviles de productividad de Citrix como aplicaciones MDX.
- **Aplicaciones de empresa:** Aplicaciones privadas que usted desarrolla u obtiene de otra fuente. Estas aplicaciones se ofrecen a los usuarios a través de Google Play Store administrado. Google Play Store administrado es la tienda de aplicaciones de empresa de Google.
- **Aplicaciones privadas habilitadas para MDX:** Aplicaciones de empresa preparadas con el SDK de MAM o empaquetadas con MDX Toolkit.

Puede agregar aplicaciones de empresa y aplicaciones privadas habilitadas para MDX de dos formas diferentes.

- Agregue las aplicaciones a la consola de XenMobile como aplicaciones de empresa, tal y como se describe en las secciones Aplicaciones de empresa y Aplicaciones privadas habilitadas para MDX de este artículo.
- Publique las aplicaciones directamente en Google Play Store administrado con la cuenta de desarrollador de Google. A continuación, agregue las aplicaciones a la consola de XenMobile como aplicaciones administradas de la tienda de aplicaciones. Consulte Aplicaciones administradas de la tienda de aplicaciones.

Si publica aplicaciones con la cuenta de desarrollador de Google y, a continuación, pasa a utilizar la consola de XenMobile, cambiará el propietario de las aplicaciones. En este caso, deberá administrar las aplicaciones en ambas ubicaciones. Citrix recomienda agregar las aplicaciones siguiendo un método u otro, no los dos.

Si necesita quitar aplicaciones autoadministradas de Google Play Store administrado, abra un tíquet con Google. Los desarrolladores pueden inhabilitar, pero no eliminar, aplicaciones de Google Play Store administrado.

En las secciones siguientes, se ofrece información más detallada sobre la configuración de aplicaciones Android Enterprise. Para obtener información sobre cómo distribuir aplicaciones, consulte Agregar aplicaciones. Este artículo contiene:

- Flujos de trabajo generales para agregar aplicaciones web y SaaS o enlaces web
- El flujo de trabajo para aplicaciones obligatorias de empresa y de tienda pública
- Cómo entregar aplicaciones empresariales desde la red de entrega de contenido (CDN) de Citrix Content Delivery para las aplicaciones empresariales.

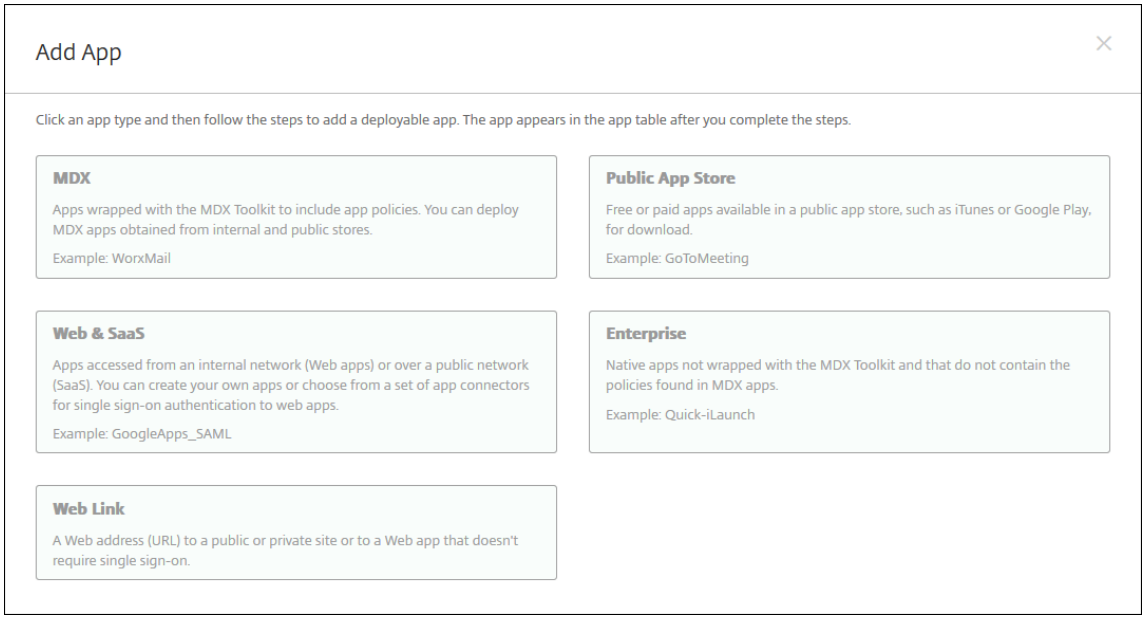
Aplicaciones administradas de la tienda de aplicaciones

Puede agregar a XenMobile aplicaciones gratuitas y de pago disponibles en Google Play Store administrado.

> **Nota:**
>
> Para que todas las aplicaciones de Google Play Store sean accesibles desde Google Play administrado, utilice la propiedad de servidor **Access all apps in the managed Google Play store**. Consulte Propiedades de servidor. Al establecer esta propiedad en **true**, todos los usuarios de Android Enterprise pueden acceder a aplicaciones de la tienda pública de Google Play. A continuación, puede usar la directiva Restricciones para controlar el acceso a estas aplicaciones.

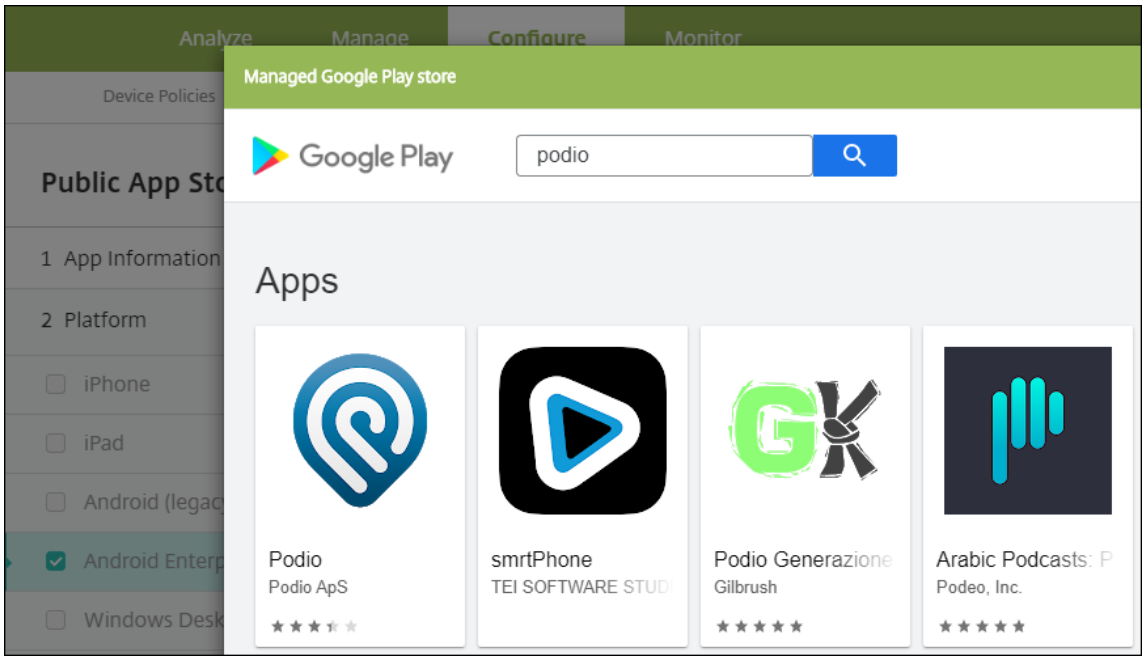
Paso 1: Agregar y configurar aplicaciones

1. En la consola de XenMobile, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.
2. Haga clic en **Tienda pública de aplicaciones**.

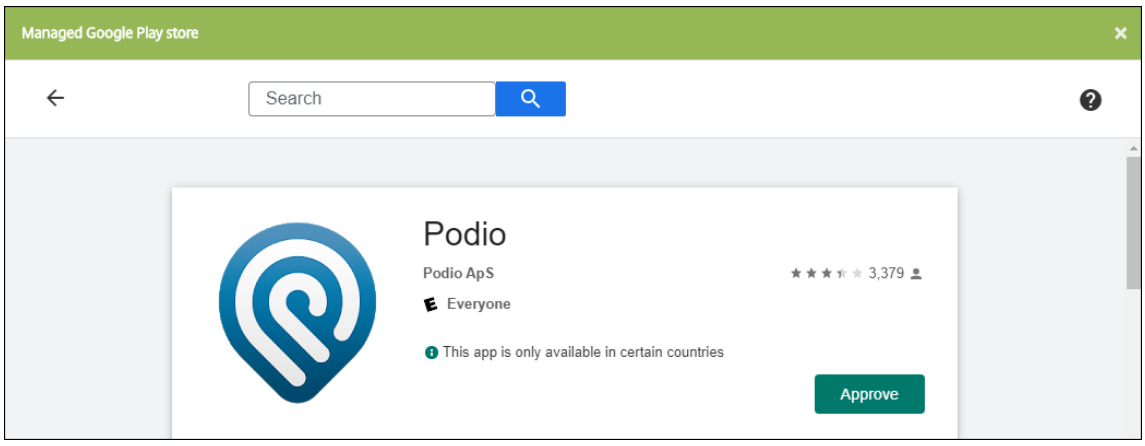


3. En el panel **Información de la aplicación**, escriba la información siguiente:
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.
   - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
   - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.
4. Seleccione **Android Enterprise** como plataforma.

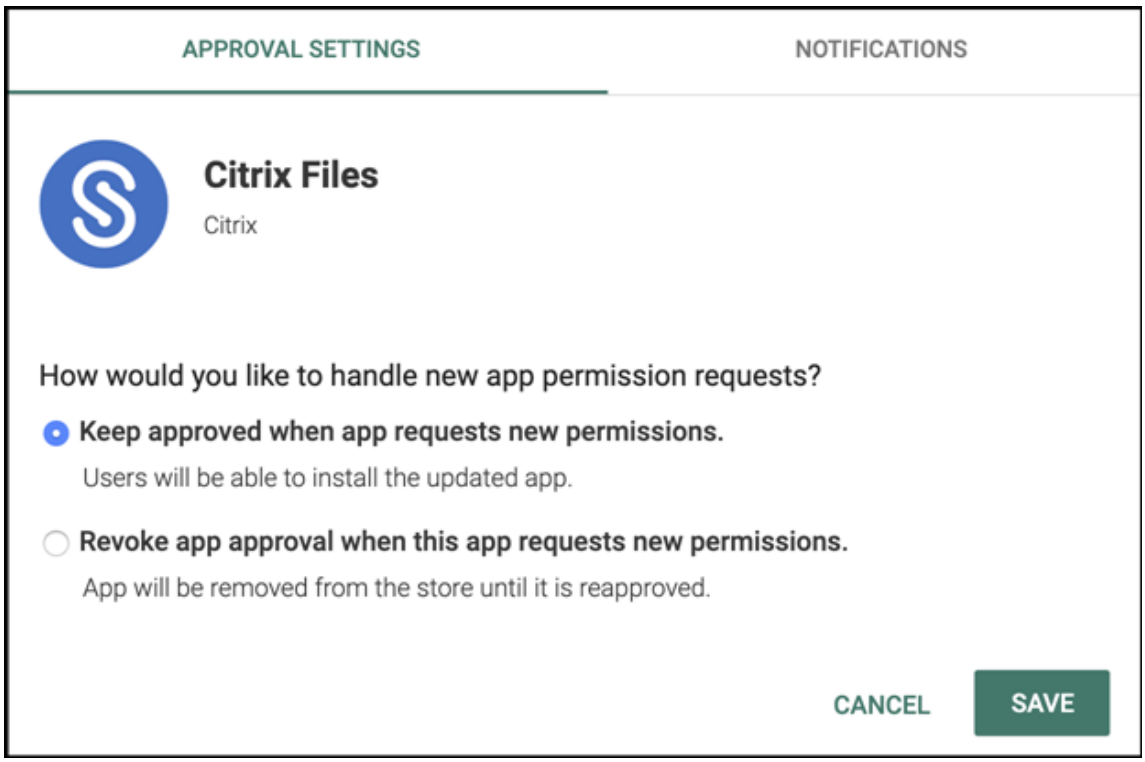
5. Escriba el nombre de la aplicación o el ID del paquete en el cuadro de búsqueda y haga clic en **Buscar**. Puede encontrar el ID de paquete en Google Play Store. El ID se encuentra en la dirección URL de la aplicación. Por ejemplo, `com.Slack` es el ID de paquete en `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`.



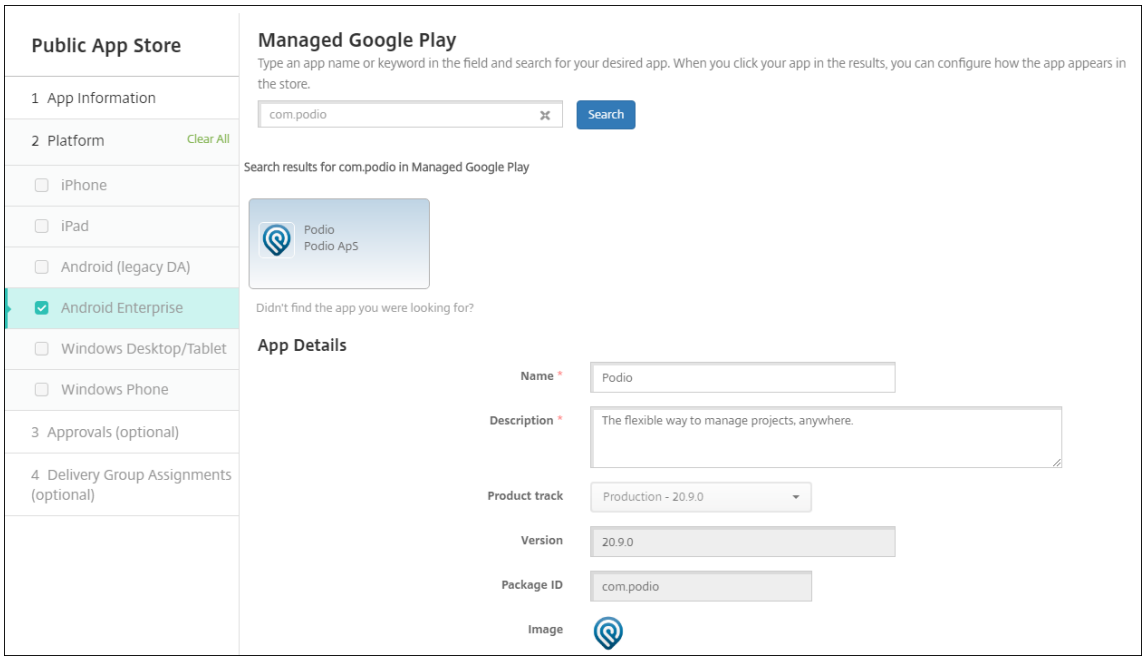
6. Aparecerán las aplicaciones que coincidan con los criterios de búsqueda. Haga clic en la aplicación pertinente y, a continuación, haga clic en **Aprobar**.



7. Vuelva a hacer clic en **Approve**.
8. Seleccione **Keep approved when app requests new permissions**. Haga clic en **Guardar**.



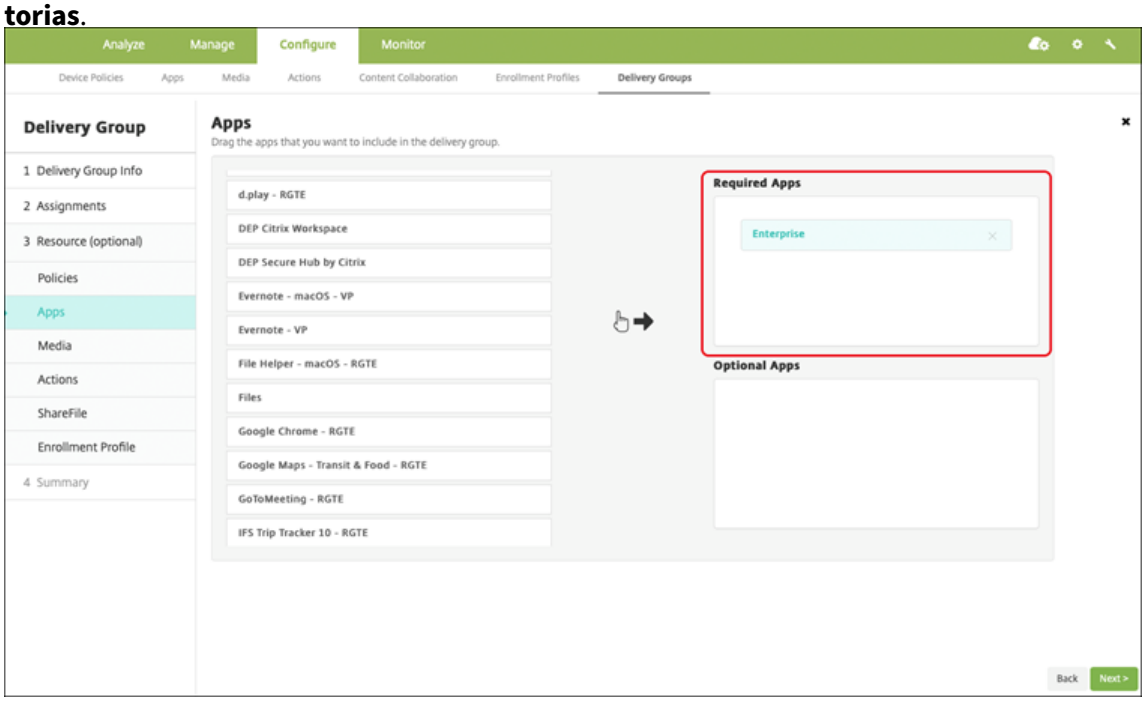
9. Haga clic en el icono de la aplicación y defina el **nombre** y la **descripción** de la aplicación.



10. Asigne los grupos de entrega que quiera a la aplicación y haga clic en **Guardar**. Para obtener información, consulte Implementar recursos.

Paso 2: Configurar la implementación de aplicaciones

1. Vaya a **Configurar > Grupos de entrega** y seleccione el grupo de entrega que configuró. Haga clic en **Edit**.
2. En la sección **Aplicaciones**, arrastre las aplicaciones deseadas al cuadro **Aplicaciones obligatorias**.



3. En la página **Resumen**, haga clic en **Guardar**.
4. En la página **Grupos de entrega**, seleccione el grupo de entrega y haga clic en **Implementar**.

Aplicaciones MDX

Agregue los archivos MDX a XenMobile y configure los detalles de la aplicación, además de las configuraciones de las directivas que se aplicarán a ella. Si quiere configurar las aplicaciones móviles de productividad de Citrix para Android Enterprise, agréguelas como aplicaciones MDX. Para obtener información sobre las directivas de aplicaciones que están disponibles para cada tipo de plataforma de dispositivos, consulte:

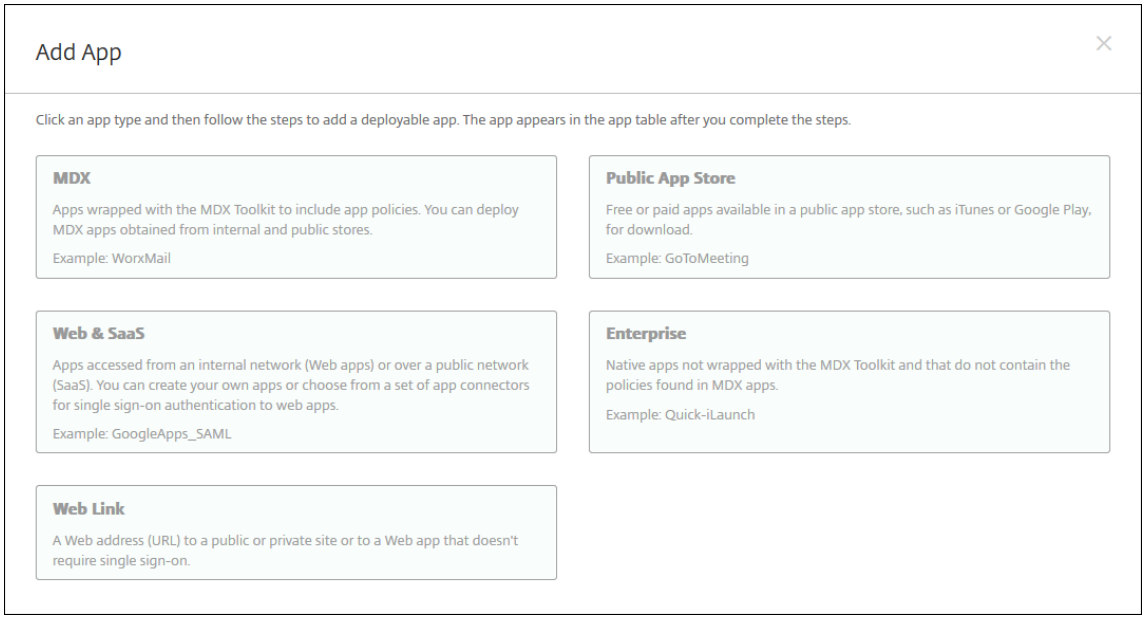
- Introducción al SDK de MAM
- Vista general de las directivas MDX

Paso 1: Agregar y configurar aplicaciones

1. Para las aplicaciones móviles de productividad de Citrix, descargue los archivos MDX de tienda pública; es decir, vaya a https://www.citrix.com/downloads. Vaya a **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.

Para otros tipos de aplicaciones MDX, debe obtener el archivo MDX.

2. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones**. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



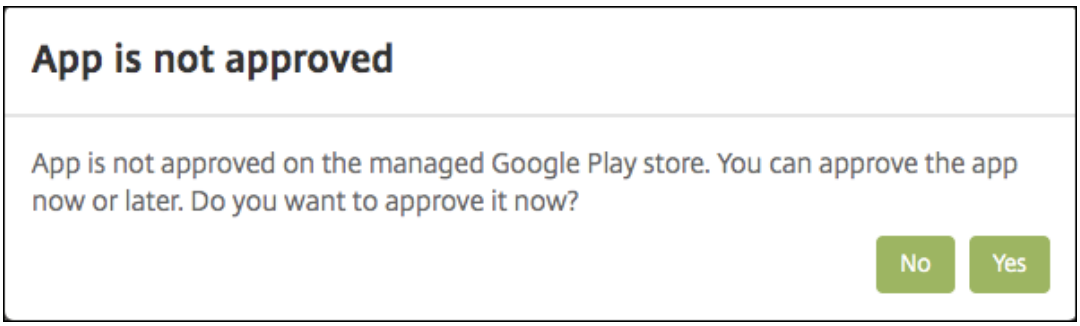
3. Haga clic en **MDX**. Aparecerá la página **Información de la aplicación** MDX. En el panel **Información de la aplicación**, escriba la información siguiente:

   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.
   - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
   - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.

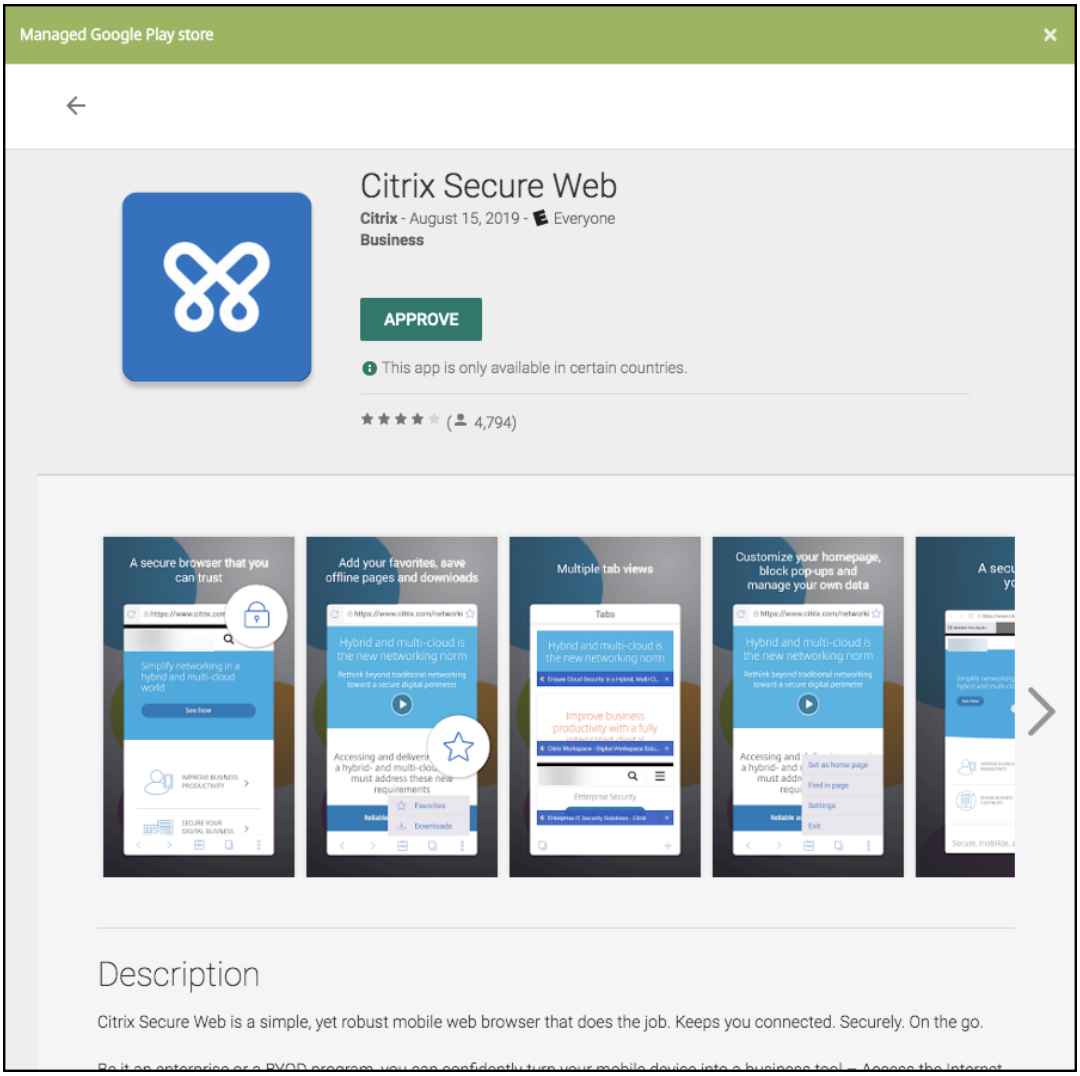
4. Seleccione **Android Enterprise** como plataforma.

5. Haga clic en **Cargar** y vaya al archivo MDX. Android Enterprise solo admite aplicaciones preparadas con el SDK de MAM o MDX Toolkit.

   - La interfaz de usuario le notifica si la aplicación adjunta requiere la aprobación de Google Play Store administrado. Para aprobar la aplicación sin salir de la consola de XenMobile, haga clic en **Sí**.



Una vez abierto Google Play Store administrado, siga las instrucciones para aprobar y guardar la aplicación.



Al agregarse correctamente la aplicación, aparece la página **Detalles de la aplicación**.

6. Configure estos parámetros:

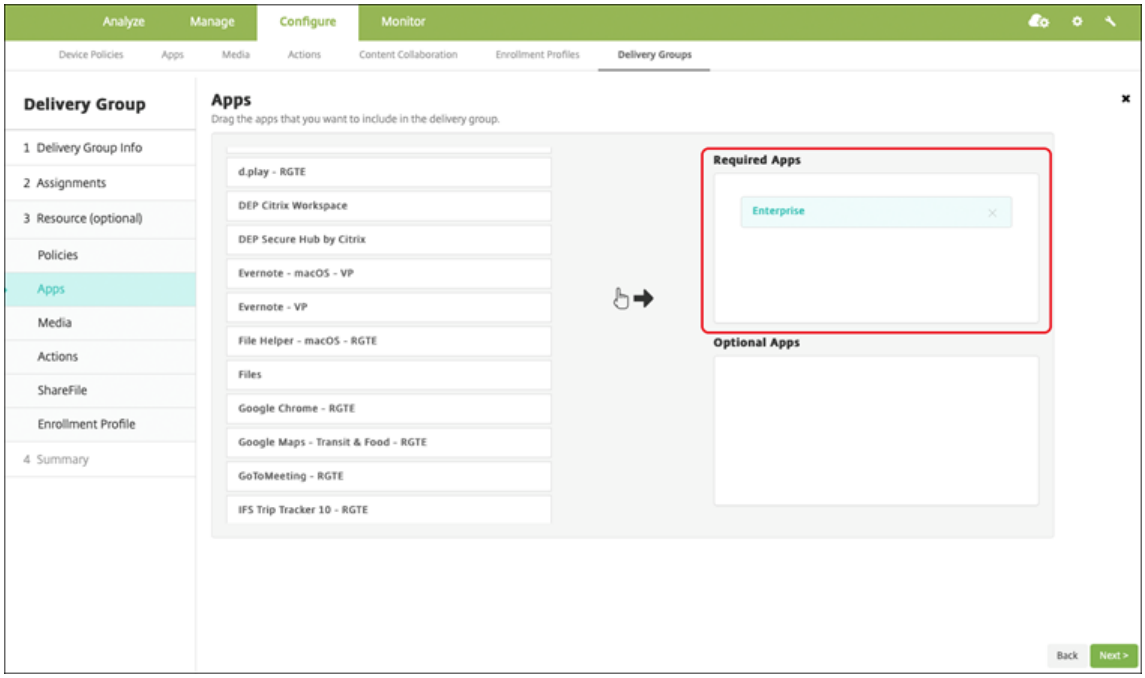
   - **Nombre de archivo:** Escriba el nombre del archivo asociado a la aplicación.

- **Descripción de la aplicación:** Escriba una descripción de la aplicación.
- **Versión de la aplicación:** Si quiere, escriba el número de versión de la aplicación.
- **ID del paquete:** Escriba el ID del paquete de la aplicación, obtenido de Google Play Store administrado.
- **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
- **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
- **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.

7. 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 y restricciones a aplicaciones. En la consola, se ofrece información descriptiva sobre cada una de las directivas. Para obtener información sobre las directivas de aplicaciones que están disponibles para cada tipo de plataforma de dispositivos, consulte:
   - Introducción al SDK de MAM
   - Vista general de las directivas MDX
8. Configure las reglas de implementación y los parámetros del almacén.
9. Asigne los grupos de entrega que quiera a la aplicación y haga clic en **Guardar**. Para obtener información, consulte Implementar recursos.

Paso 2: Configurar la implementación de aplicaciones

1. Vaya a **Configurar > Grupos de entrega** y seleccione el grupo de entrega que configuró. Haga clic en **Edit**.
2. En la sección **Aplicaciones**, arrastre las aplicaciones deseadas al cuadro **Aplicaciones obligatorias**.



3. En la página **Resumen**, haga clic en **Guardar**.
4. En la página **Grupos de entrega**, seleccione el grupo de entrega y haga clic en **Implementar**.

Aplicaciones de empresa

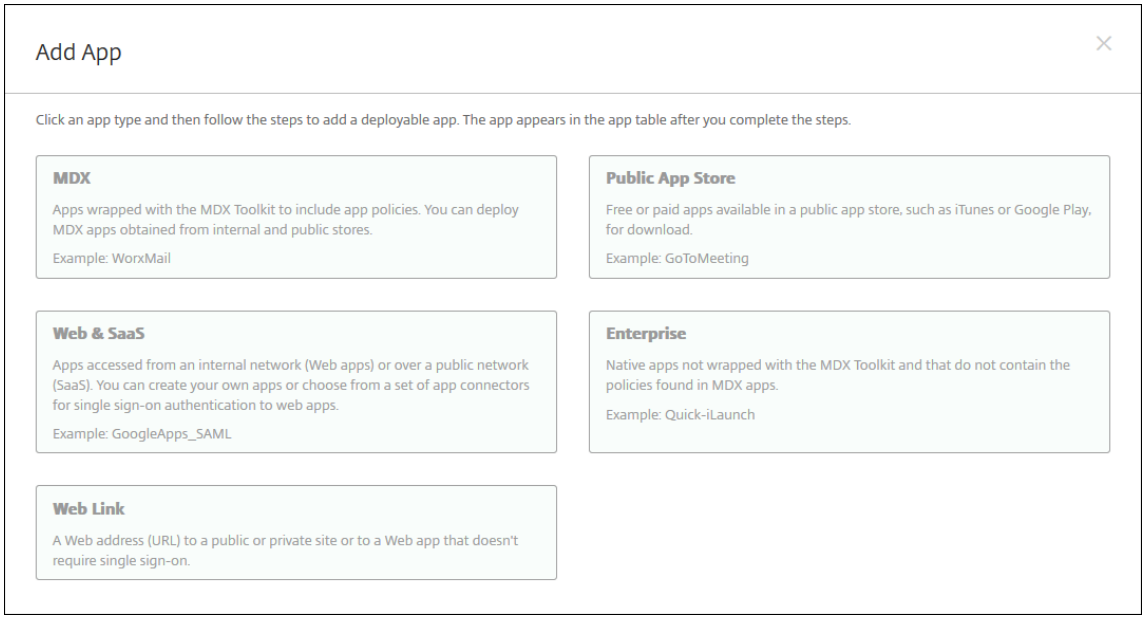
Las aplicaciones empresariales representan aplicaciones privadas que no están preparadas con el SDK de MAM o MDX Toolkit. Se trata de aplicaciones desarrolladas internamente o se han obtenido directamente de otras fuentes. Para agregar una aplicación de empresa, se necesita el archivo APK asociado a ella. Debe seguir las Prácticas recomendadas de aplicaciones privadas de Google.

Paso 1: Agregar y configurar aplicaciones

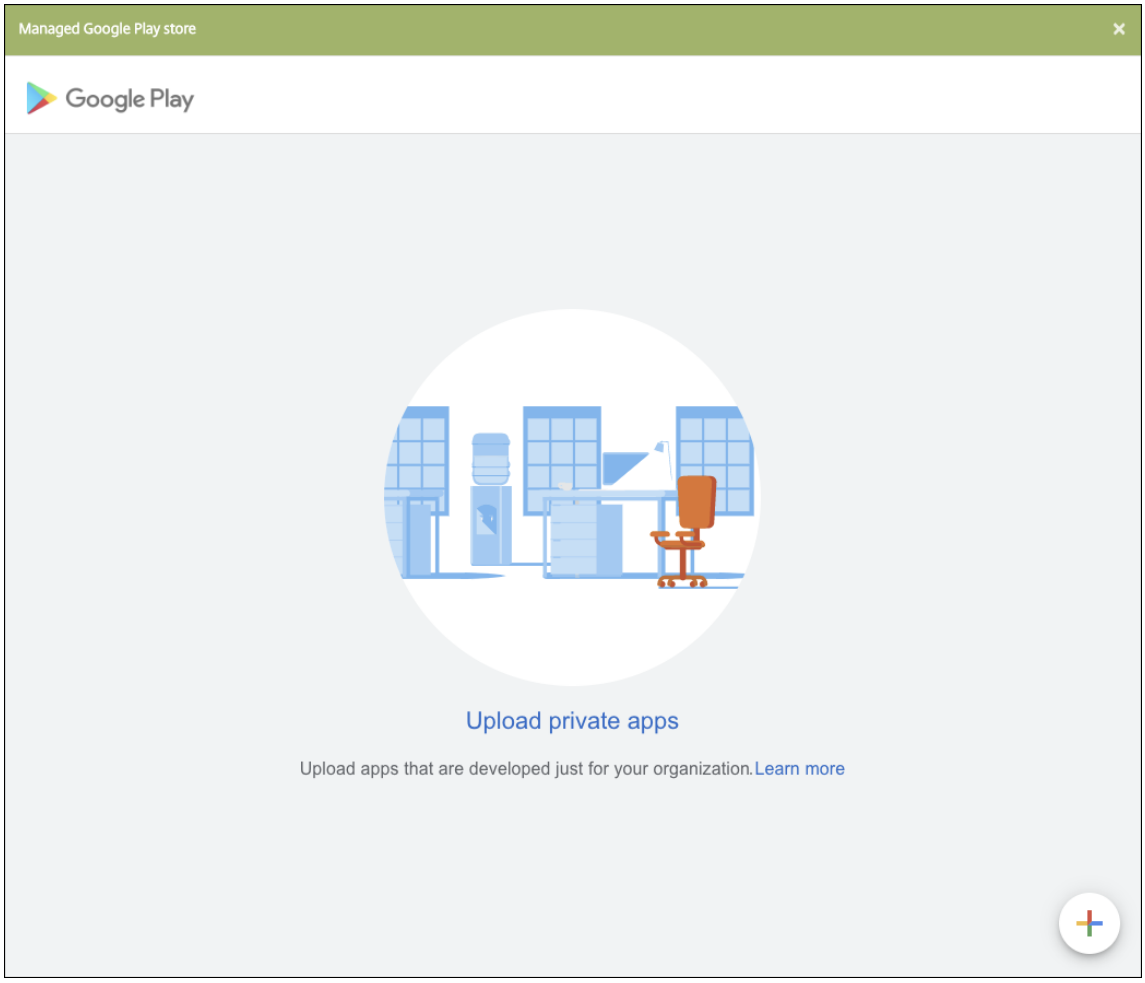
Agregue la aplicación de una de dos maneras:

- Publique la aplicación directamente en Google Play Store administrado y agréguela a la consola de XenMobile como una aplicación de Google Play Store administrado. Siga las indicaciones de la documentación de Google sobre cómo publicar aplicaciones privadas y, a continuación, siga los pasos descritos en la sección Aplicaciones administradas de la tienda de aplicaciones.
- Agregue la aplicación a la consola de XenMobile como una aplicación de empresa. Siga estos pasos:

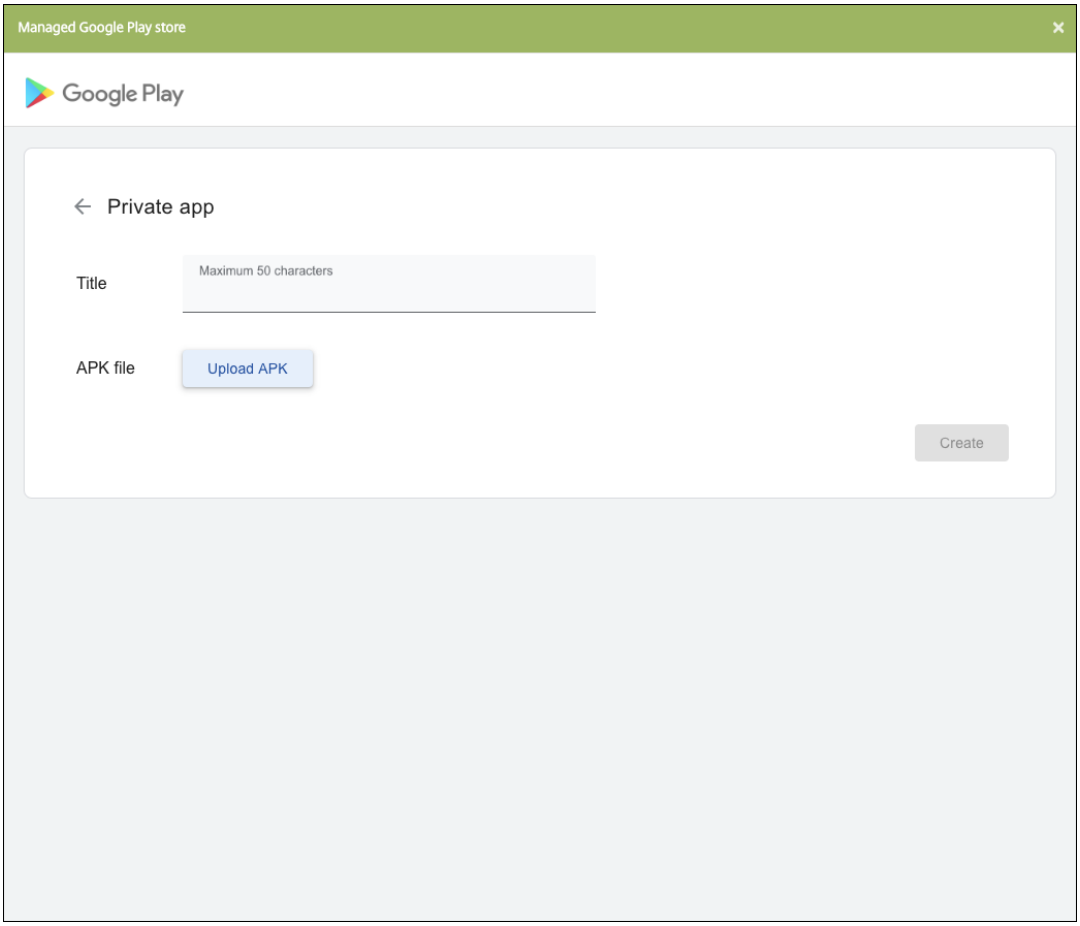
1. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones**. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



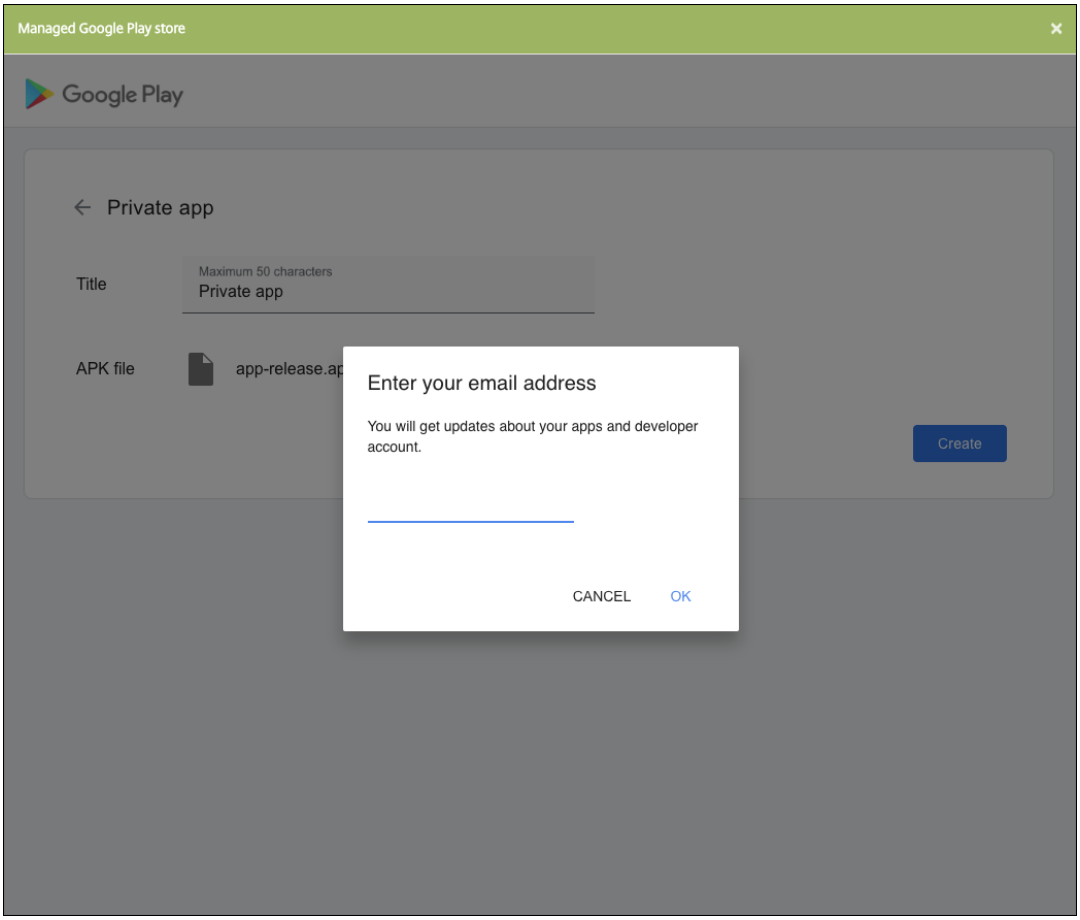
2. Haga clic en **Empresa**. En el panel **Información de la aplicación**, escriba la información siguiente:
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en "Nombre de la aplicación", en la tabla "Aplicaciones".
   - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
   - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.
3. Seleccione **Android Enterprise** como plataforma.
4. El botón **Cargar** abre Google Play Store administrado. No es necesario registrarse con una cuenta de desarrollador para publicar una aplicación privada. Haga clic en el icono **Más** situado en la esquina inferior derecha para continuar.



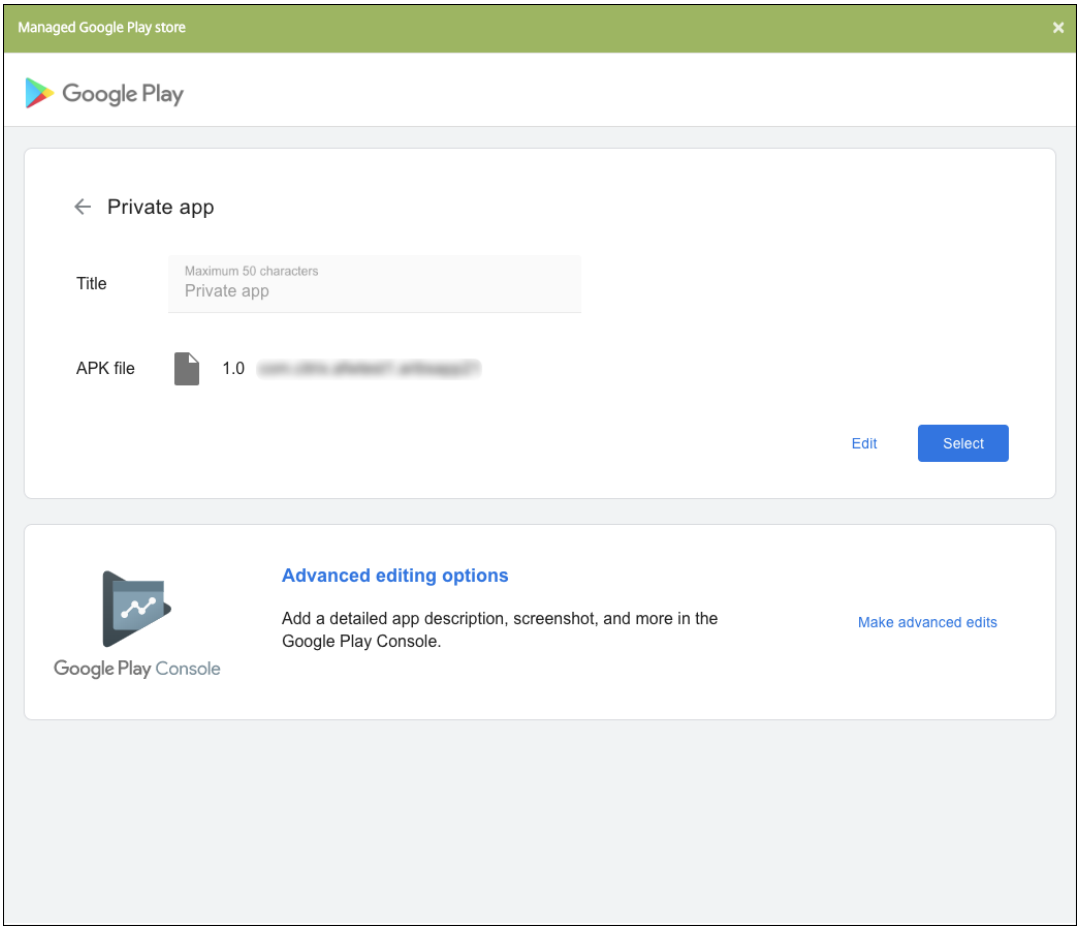
a) Introduzca el nombre de la aplicación y cargue el archivo APK. Cuando haya terminado, haga clic en **Crear**. La aplicación privada puede tardar hasta 10 minutos en publicarse.



b) Introduzca una dirección de correo electrónico para obtener actualizaciones sobre sus aplicaciones.



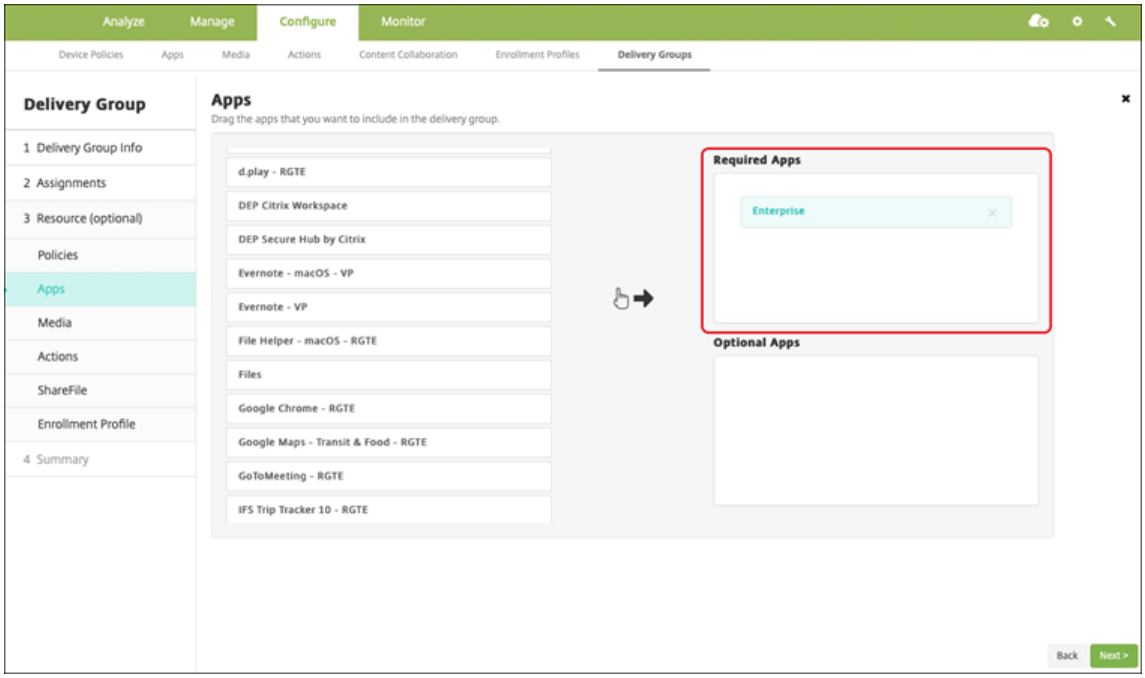
c) Después de publicar la aplicación, haga clic en el icono de la aplicación privada. Si quiere agregar una descripción de la aplicación, cambiar el icono de esta o realizar otras acciones, haga clic en la opción para **realizar modificaciones avanzadas**. De lo contrario, haga clic en **Seleccionar** para abrir la página de información de la aplicación.



5. Haga clic en **Siguiente**. Aparecerá la página de información referente a la aplicación para la plataforma pertinente.
6. Configure los parámetros para el tipo de plataforma, como:
   - **Nombre de archivo:** Si quiere, escriba un nuevo nombre para la aplicación.
   - **Descripción de la aplicación:** Si quiere, indique una nueva descripción de la aplicación.
   - **Versión de la aplicación:** Este campo no se puede cambiar.
   - **ID del paquete:** Identificador único de la aplicación.
   - **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
   - **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
   - **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
7. Configure las reglas de implementación y los parámetros del almacén.
8. Asigne los grupos de entrega que quiera a la aplicación y haga clic en **Guardar**. Para obtener información, consulte Implementar recursos.

Paso 2: Configurar la implementación de aplicaciones

1. Vaya a **Configurar > Grupos de entrega** y seleccione el grupo de entrega que configuró. Haga clic en **Edit**.
2. En la sección **Aplicaciones**, arrastre las aplicaciones deseadas al cuadro **Aplicaciones obligatorias**.



3. En la página **Resumen**, haga clic en **Guardar**.
4. En la página **Grupos de entrega**, seleccione el grupo de entrega y haga clic en **Implementar**.

Aplicaciones privadas habilitadas para MDX

Para agregar aplicaciones de Android Enterprise como aplicaciones de empresa habilitadas para MDX:

1. Cree una aplicación privada de Android Enterprise y habilítela para MDX.
2. Agregue la aplicación a la consola de XenMobile.
   - Aloje y publique la aplicación en Google Play Store administrado.
   - Agregue la aplicación a la consola de XenMobile como aplicación de empresa.
3. Agregue el archivo MDX a XenMobile.

Si decide alojar y publicar aplicaciones a través de Google Play Store, no elija la firma de certificados de Google. Firme la aplicación con el mismo certificado utilizado para habilitar la aplicación para MDX. Para obtener más información sobre la publicación de aplicaciones, consulte la documentación de Google en Cómo publicar tu app y Firma tu app. El SDK de MAM no empaqueta aplicaciones, por lo que no requiere un certificado distinto del utilizado para desarrollar la aplicación.

Para obtener más información sobre cómo publicar aplicaciones privadas a través de la consola de Google Play, consulte Publicar aplicaciones privadas desde Play Console en la documentación de Google.

Para publicar una aplicación a través de XenMobile, consulte las secciones siguientes.

Preparar una aplicación privada de Android Enterprise

Al crear una aplicación privada de Android Enterprise, debe seguir las prácticas recomendadas de aplicaciones privadas de Google.

Después de crear una aplicación privada de Android Enterprise, integre el SDK de MAM en la aplicación o empaquete la aplicación con MDX Toolkit. A continuación, agregue los archivos resultantes a XenMobile.

Puede actualizar la aplicación cargando un archivo APK actualizado. Los pasos siguientes cubren el empaquetado de aplicaciones con MDX Toolkit.

1. Cree la aplicación privada de Android Enterprise y genere un archivo APK con firma.
2. El siguiente archivo de ejemplo contiene todas las directivas conocidas. Es posible que algunas de ellas no sean aplicables a su entorno. Se ignoran todas las configuraciones que no se puedan utilizar. Cree un archivo XML con los siguientes parámetros:

```
<?xml version="1.0" encoding="UTF-8"?>
<MobileAppPolicies>
    <PolicySchemaVersion>
        1.0
    </PolicySchemaVersion>
    <Policies>
        <DevicePasscode>false</DevicePasscode>
        <AppPasscode>false</AppPasscode>
        <MaxOfflinePeriod>72</MaxOfflinePeriod>
        <StepupAuthAddress/>
        <RequireUserEntropy>false</RequireUserEntropy>
        <BlockRootedDevices>true</BlockRootedDevices>
        <BlockDebuggerAccess>false</BlockDebuggerAccess>
        <RequireDeviceLock>false</RequireDeviceLock>
        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
            NonCompliantDeviceBehavior>
        <WifiOnly>false</WifiOnly>
        <RequireInternalNetwork>false</RequireInternalNetwork>
        <InternalWifiNetworks/>
        <AllowedWifiNetworks/>
        <UpgradeGracePeriod>168</UpgradeGracePeriod>
        <WipeDataOnAppLock>false</WipeDataOnAppLock>
```



```
22          <ActivePollPeriod>60</ActivePollPeriod>
23          <PublicFileAccessLimitsList/>
24          <CutAndCopy>Unrestricted</CutAndCopy>
25          <Paste>Unrestricted</Paste>
26          <DocumentExchange>Unrestricted</DocumentExchange>
27          <OpenInExclusionList/>
28          <InboundDocumentExchange>Unrestricted</
               InboundDocumentExchange>
29          <InboundDocumentExchangeWhitelist/>
30          <connectionSecurityLevel>TLS</connectionSecurityLevel>
31          <DisableCamera>false</DisableCamera>
32          <DisableGallery>false</DisableGallery>
33          <DisableMicrophone>false</DisableMicrophone>
34          <DisableLocation>false</DisableLocation>
35          <DisableSms>false</DisableSms>
36          <DisableScreenCapture>false</DisableScreenCapture>
37          <DisableSensor>false</DisableSensor>
38          <DisableNFC>false</DisableNFC>
39          <BlockLogs>false</BlockLogs>
40          <DisablePrinting>false</DisablePrinting>
41          <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
               MvpnNetworkAccess>
42          <MvpnSessionRequired>False</MvpnSessionRequired>
43          <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
44          <DisableLocalhostConnections>false</
               DisableLocalhostConnections>
45          <CertificateLabel/>
46          <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
47          <DefaultLoggerLevel>15</DefaultLoggerLevel>
48          <MaxLogFiles>2</MaxLogFiles>
49          <MaxLogFileSize>2</MaxLogFileSize>
50          <RedirectSystemLogs>false</RedirectSystemLogs>
51          <EncryptLogs>false</EncryptLogs>
52          <GeofenceLongitude>0</GeofenceLongitude>
53          <GeofenceLatitude>0</GeofenceLatitude>
54          <GeofenceRadius>0</GeofenceRadius>
55          <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
56          <Authentication>OfflineAccessOnly</Authentication>
57          <ReauthenticationPeriod>480</ReauthenticationPeriod>
58          <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
59      </Policies>
60  </MobileAppPolicies>
61  <!--NeedCopy-->
```

3. Empaquete la aplicación con MDX Toolkit. Para obtener información sobre cómo usar MDX

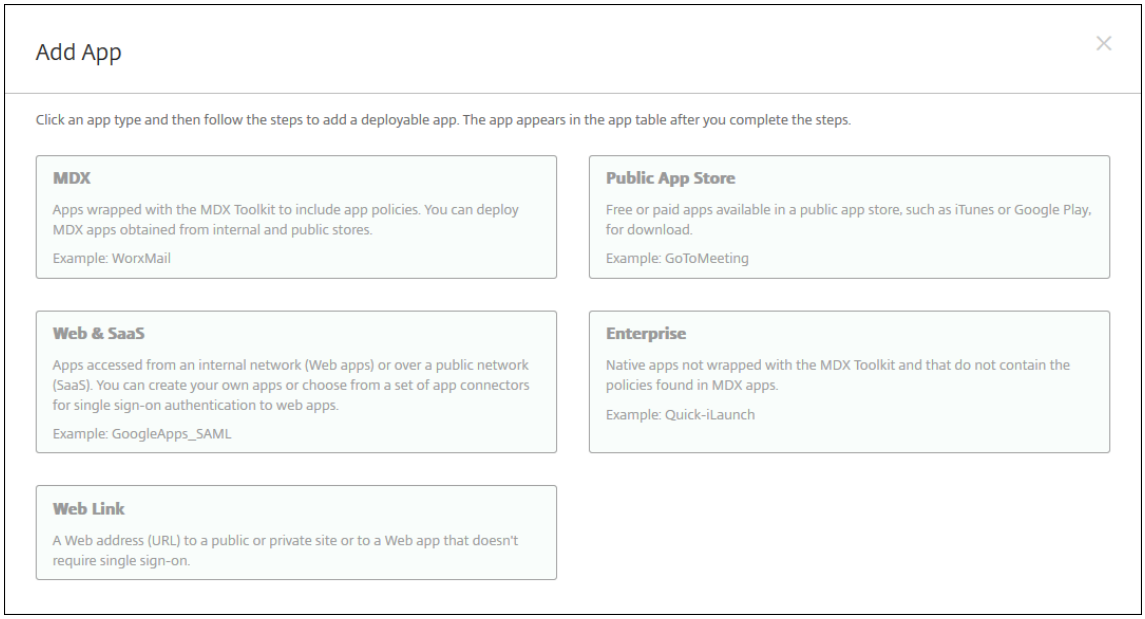
Toolkit, consulte Empaquetar aplicaciones móviles Android.

Establezca el parámetro **apptype** en **Premium**. Utilice el archivo XML del paso anterior en el comando que se describe a continuación.

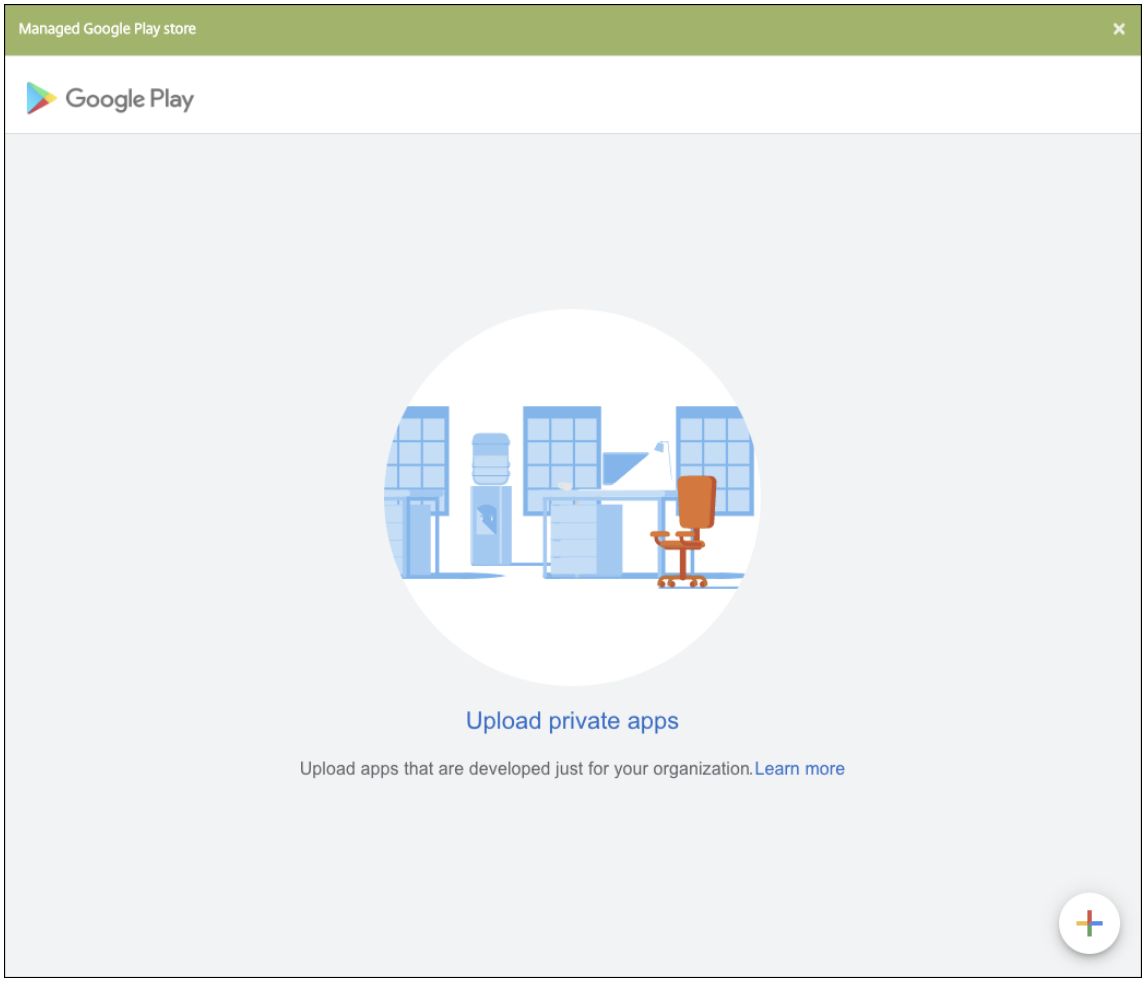
Si conoce la URL de la tienda de aplicaciones, establezca el parámetro **storeURL** en la URL de la tienda. Una vez publicada la aplicación, los usuarios pueden descargarla desde la URL de la tienda.

Aquí se muestra un ejemplo de un comando de MDX Toolkit utilizado para empaquetar una aplicación llamada SampleAEapp:

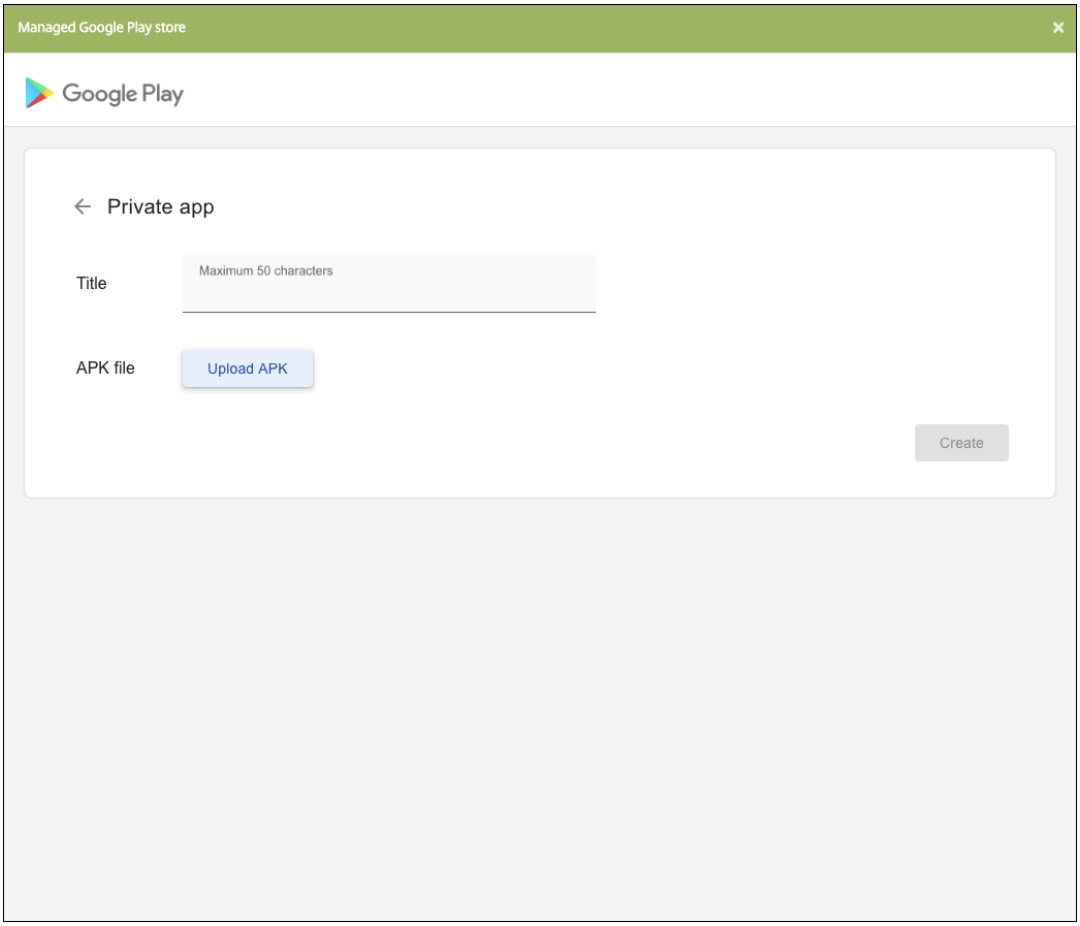
```
```
 java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -
    Duser.variant
 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
 -MinPlatform 5.0
 -keystore /MyKeystore
 -storepass mystorepwd123
 -keyalias key0
 -keypass mykeypwd123
 -storeURL "https://play.google.com/store/apps/details?id=
    SampleAEappPackage"
 -appType Premium
 -premiumMdxPolicies <Path to Premium policy XML>
<!--NeedCopy--> ```
```

Al empaquetar la aplicación, se genera un archivo APK empaquetado y un archivo MDX.

### Agregar el archivo APK empaquetado

Agregue la aplicación de una de dos maneras:

- Publique la aplicación directamente en Google Play Store administrado y agréguela a la consola de XenMobile como una aplicación de Google Play Store administrado. Siga las indicaciones de la documentación de Google sobre cómo publicar aplicaciones privadas y, a continuación, siga los pasos descritos en la sección Aplicaciones administradas de la tienda de aplicaciones.
- Agregue la aplicación a la consola de XenMobile como una aplicación de empresa. Siga estos pasos:

1. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones**. Se abrirá la página **Aplicaciones**.
2. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.

 
```



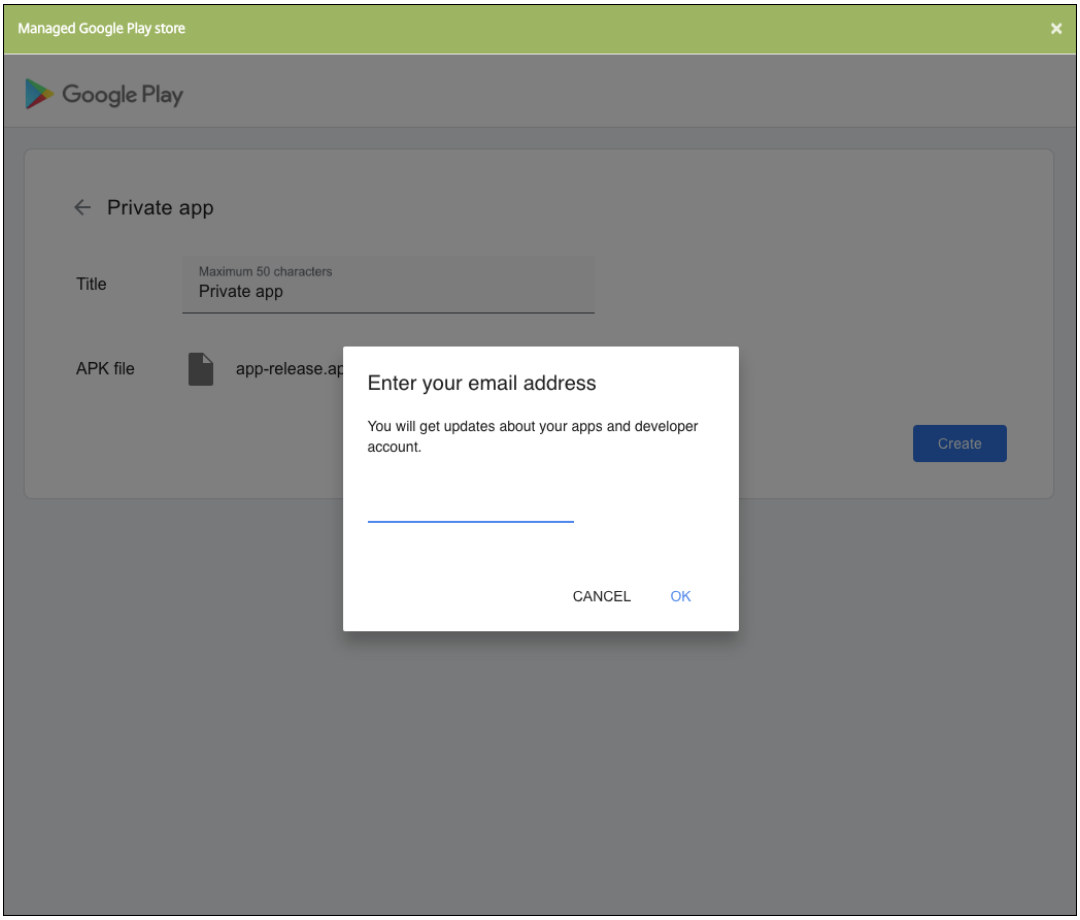
3. Haga clic en **Empresa**. En el panel **Información de la aplicación**, escriba la información siguiente:
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en "Nombre de la aplicación", en la tabla "Aplicaciones".
   - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
   - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.
4. Seleccione **Android Enterprise** como plataforma.
5. El botón **Cargar** abre Google Play Store administrado. No es necesario registrarse con una cuenta de desarrollador para publicar una aplicación privada. Haga clic en el icono **Más** situado en la esquina inferior derecha para continuar.



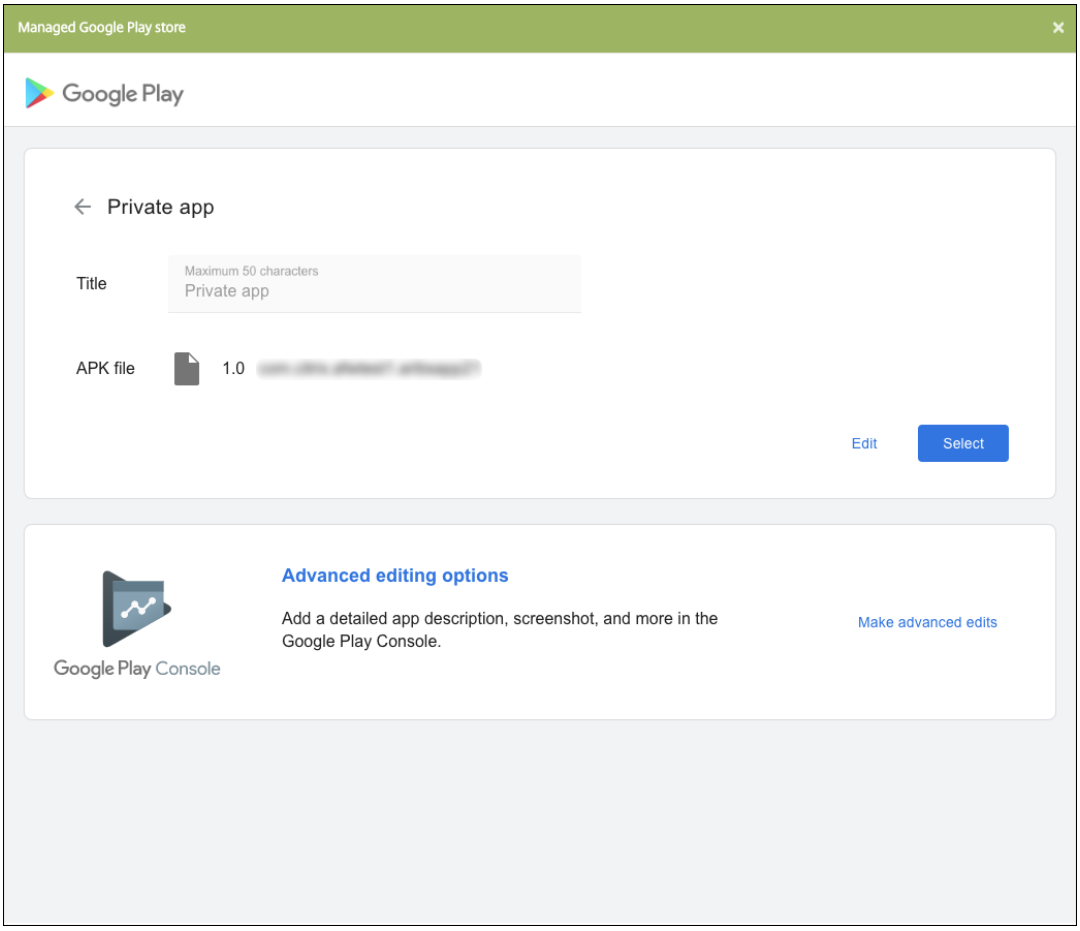
a) Introduzca el nombre de la aplicación y cargue el archivo APK. Cuando haya terminado, haga clic en **Crear**. La aplicación privada puede tardar hasta 10 minutos en publicarse.



b) Introduzca una dirección de correo electrónico para obtener actualizaciones sobre sus aplicaciones.



c) Una vez publicada la aplicación, haga clic en el icono de una aplicación privada y, a continuación, en **Seleccionar** para abrir la página de información de la aplicación.



6. Haga clic en **Siguiente**. Aparecerá la página de información referente a la aplicación para la plataforma pertinente.
7. Configure los parámetros para el tipo de plataforma, como:
   - **Nombre de archivo:** Si quiere, escriba un nuevo nombre para la aplicación.
   - **Descripción de la aplicación:** Si quiere, indique una nueva descripción de la aplicación.
   - **Versión de la aplicación:** Este campo no se puede cambiar.
   - **ID del paquete:** Identificador único de la aplicación.
   - **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
   - **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
   - **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
8. Configure las reglas de implementación y los parámetros del almacén.
9. En la página de la **aplicación de empresa para Android Enterprise**, haga clic en **Siguiente**. Aparecerá la página **Aprobaciones**.

Para utilizar flujos de trabajo que requieran aprobación antes de permitir que los usuarios accedan a la aplicación, consulte Aplicar flujos de trabajo. Si no necesita flujos de trabajo de aprobación, puede ir directamente al paso 13.

10. Haga clic en **Siguiente**.
11. Aparecerá la página **Asignación de grupos de entrega**. No es necesario realizar ninguna acción en esta página. Los grupos de entrega y la programación de implementación de esta aplicación se configuran al agregar el archivo MDX. Haga clic en **Guardar**.

Opcional: Agregar o cambiar la dirección URL de la tienda

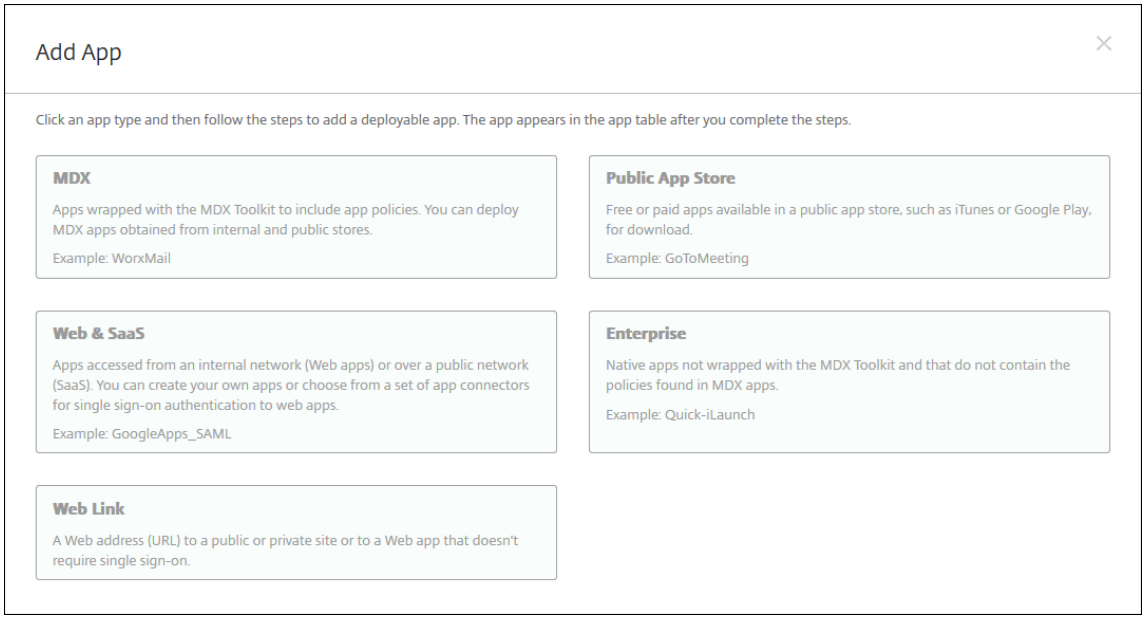
Si no sabía cuál era la dirección URL de la tienda al empaquetar la aplicación, puede agregarla ahora.

1. Seleccione la aplicación en Google Play Store administrado. Al seleccionar la aplicación, la URL de la tienda aparece en la barra de direcciones del explorador. Copie el nombre del paquete de la aplicación desde el formulario de la URL. Por ejemplo: `https://play.google.com/store/apps/details?id=SampleAEappPackage`. Puede que la URL que copie empiece por `https://play.google.com/work/`. Debe cambiar `work` a `store`.
2. Con MDX Toolkit, agregue la URL del almacén al archivo MDX:

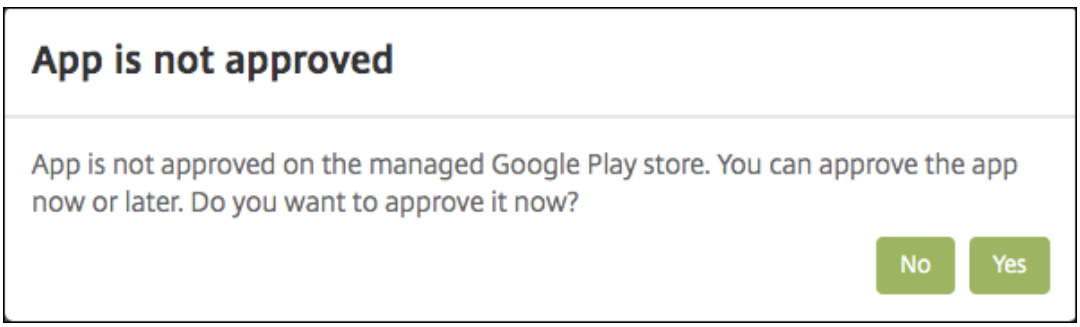
```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \
setinfo \
-in ~/Desktop/SampleApps/Sample.mdx \
-out ~/Desktop/SampleApps/wrapped/Sample.mdx \
-storeURL "https://play.google.com/store/apps/details?id=
   SampleAEappPackage"
<!--NeedCopy-->
```

Agregar el archivo MDX

1. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones**. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.

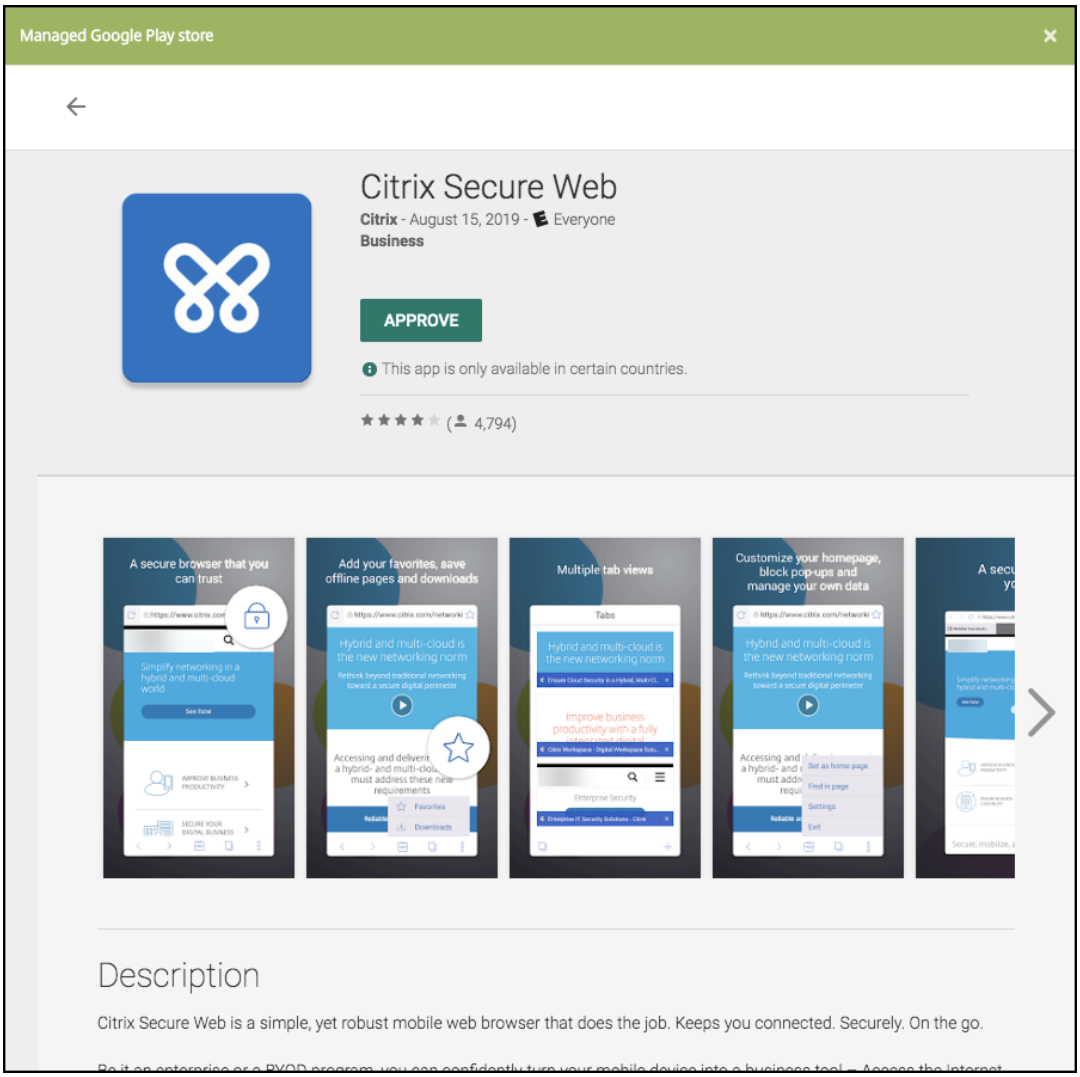


2. Haga clic en **MDX**. Aparecerá la página **Información de la aplicación** MDX. En el panel **Información de la aplicación**, escriba la información siguiente:
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.
   - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
   - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.
3. Seleccione **Android Enterprise** como plataforma.
4. Haga clic en **Cargar** y vaya al archivo MDX. Android Enterprise solo admite aplicaciones empaquetadas con MDX Toolkit.
   - La interfaz de usuario le notifica si la aplicación adjunta requiere la aprobación de Google Play Store administrado. Para aprobar la aplicación sin salir de la consola de XenMobile, haga clic en **Sí**.



Una vez abierto Google Play Store administrado, siga las instrucciones para aprobar y

guardar la aplicación.



Al agregarse correctamente la aplicación, aparece la página **Detalles de la aplicación**.

5. Configure estos parámetros:

- **Nombre de archivo:** Escriba el nombre del archivo asociado a la aplicación.
- **Descripción de la aplicación:** Escriba una descripción de la aplicación.
- **Versión de la aplicación:** Si quiere, escriba el número de versión de la aplicación.
- **ID del paquete:** Escriba el ID del paquete de la aplicación, obtenido de Google Play Store administrado.
- **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
- **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
- **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos

en los que no se puede ejecutar la aplicación.

6. 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 y restricciones a aplicaciones. En la consola, se ofrece información descriptiva sobre cada una de las directivas. Para obtener información sobre las directivas de aplicaciones que están disponibles para cada tipo de plataforma de dispositivos, consulte:

   - Introducción al SDK de MAM
   - Vista general de las directivas de aplicaciones MDX de terceros

7. Configure las reglas de implementación y los parámetros del almacén.

   La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

   La opción permanente:

   - No está disponible para Android Enterprise cuando se trata de clientes que comenzaron a usar Endpoint Management a partir de la versión 10.18.19 o una posterior
   - No se recomienda para Android Enterprise cuando se trata de clientes que comenzaron a usar Endpoint Management antes de la versión 10.18.19.

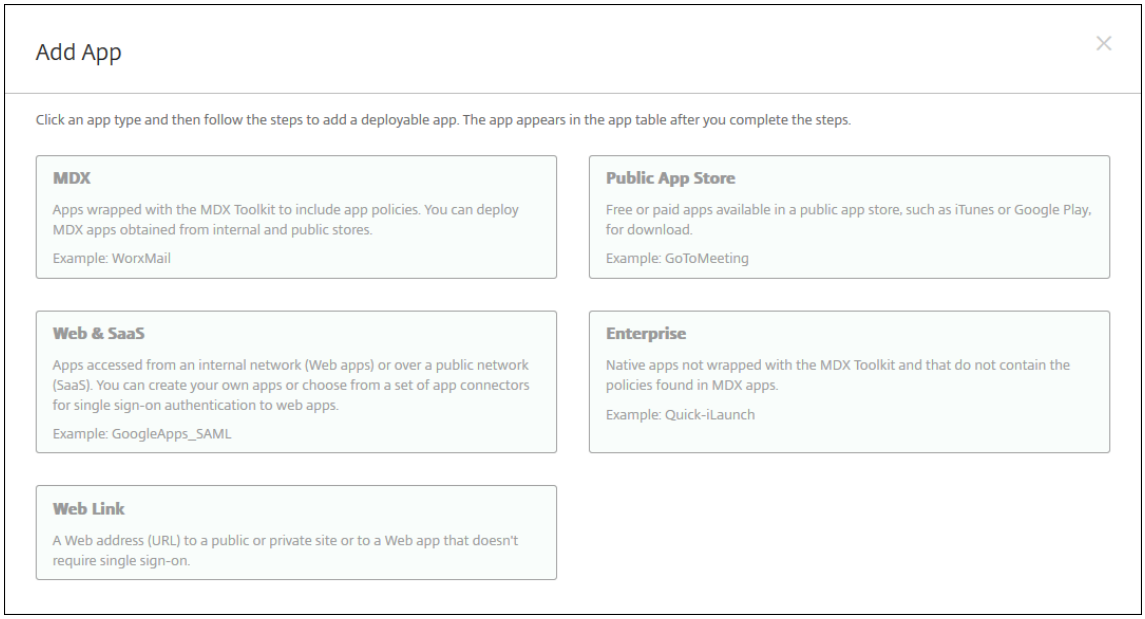
   La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Implementar para conexiones permanentes**.

8. Asigne los grupos de entrega que quiera a la aplicación y haga clic en **Guardar**. Para obtener información, consulte Implementar recursos.

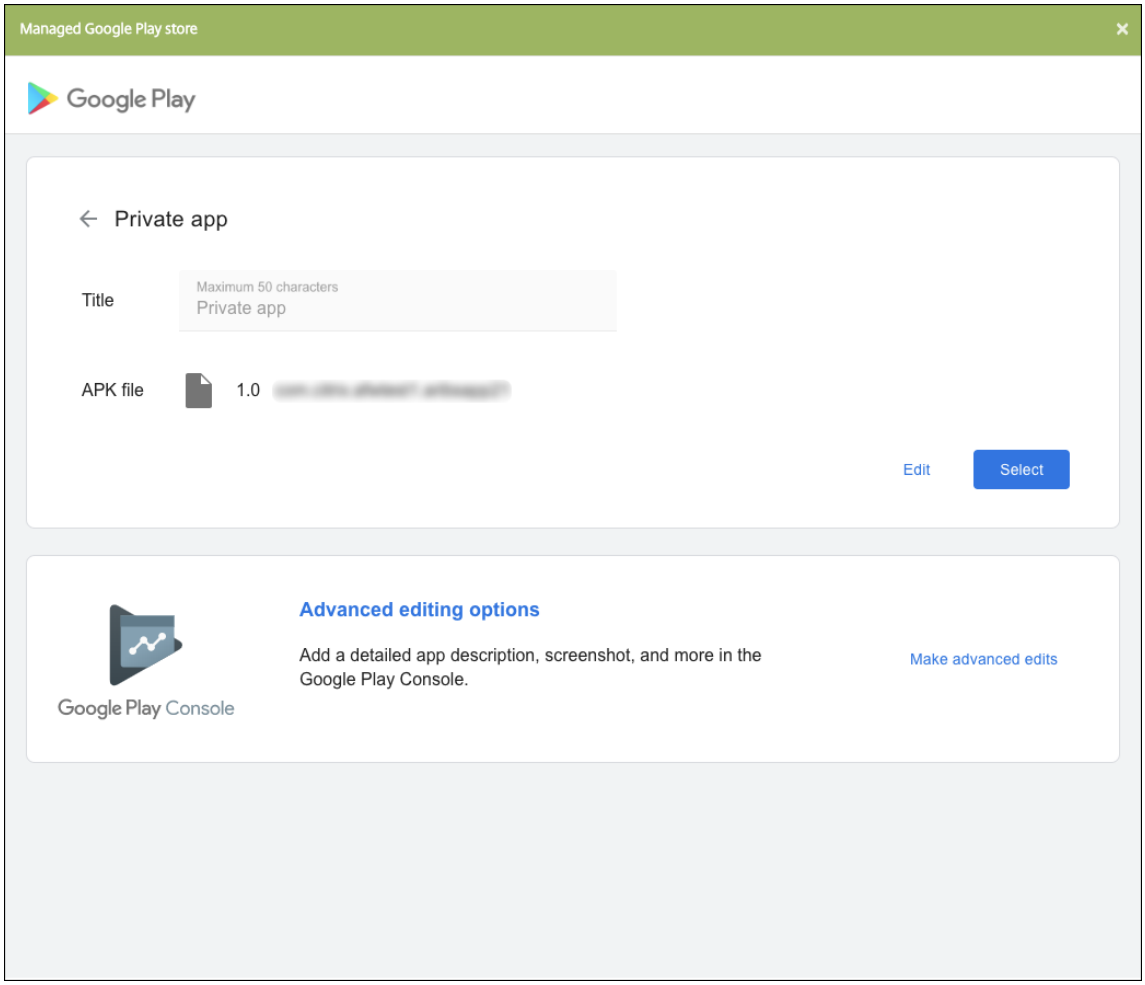
Actualizar la aplicación

Para actualizar la aplicación de Android Enterprise, empaquete y cargue un archivo APK actualizado:

1. Empaquete el archivo APK de la aplicación actualizada con el SDK de MAM o MDX Toolkit.
2. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones**. Se abrirá la página **Aplicaciones**.



3. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.
4. Haga clic en **Empresa**. En el panel **Información de la aplicación**, escriba la información siguiente:
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en "Nombre de la aplicación", en la tabla "Aplicaciones".
   - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
   - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.
5. Seleccione **Android Enterprise** como plataforma.
6. Haga clic en **Siguiente**. Aparecerá la página **Aplicación de empresa para Android Enterprise**.
7. Haga clic en **Cargar**.
8. En la página de Google Play Store administrado, seleccione la aplicación que quiera actualizar.
9. En la página de información de la aplicación, haga clic en la opción **Modificar** situada junto al nombre del archivo APK.



10. Vaya al nuevo archivo APK y cárguelo.
11. En la página de Google Play Store administrado, haga clic en **Guardar**.

Android Enterprise heredado para clientes de Google Workspace (anteriormente G Suite)

January 4, 2022

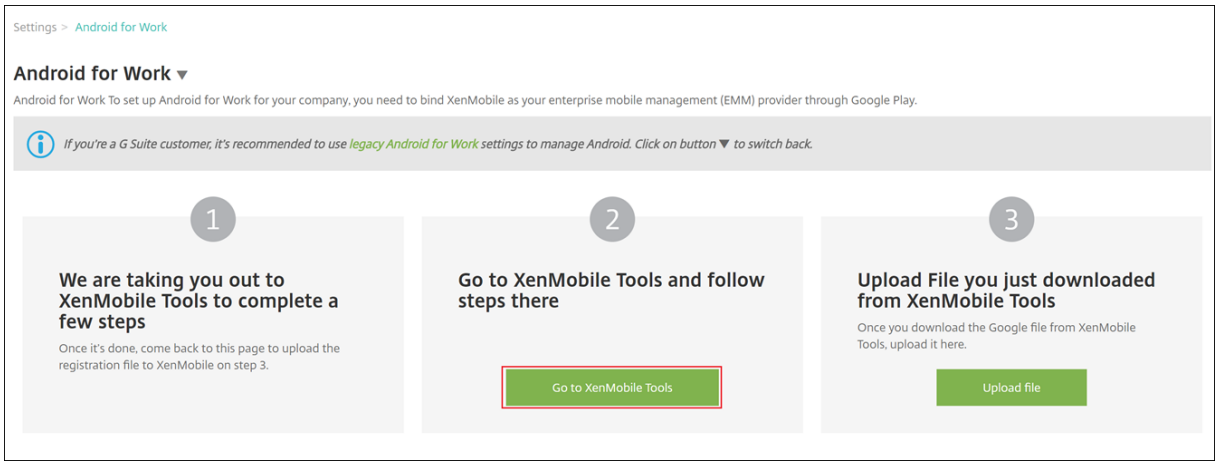
Los clientes de Google Workspace (antes denominado G Suite) deben usar los parámetros de Android Enterprise heredado para configurar Android Enterprise heredado.

Requisitos para Android Enterprise heredado:

- Un dominio accesible públicamente
- Una cuenta de administrador de Google

- Dispositivos que permitan el uso de perfiles administrados y dispongan de Android 5.0 Lollipop o versiones posteriores
- Una cuenta de Google que tenga Google Play instalado
- Un perfil de Work instalado en el dispositivo

Para empezar a configurar Android Enterprise antiguo, haga clic en **Legacy Android Enterprise**, en la página **Android Enterprise**, en los parámetros de XenMobile.



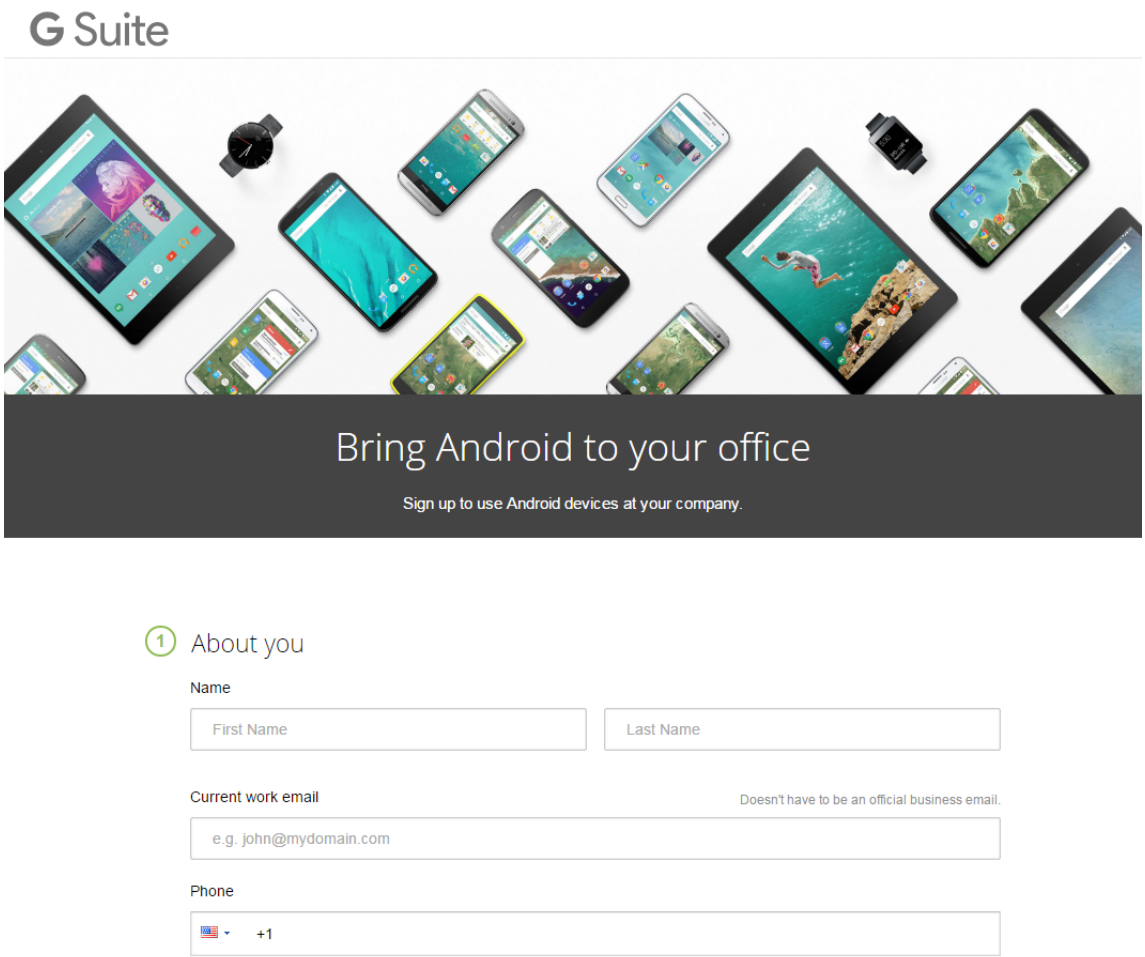
Crear una cuenta de Android Enterprise

Para poder configurar una cuenta de Android Enterprise, antes debe verificar el nombre de dominio en Google.

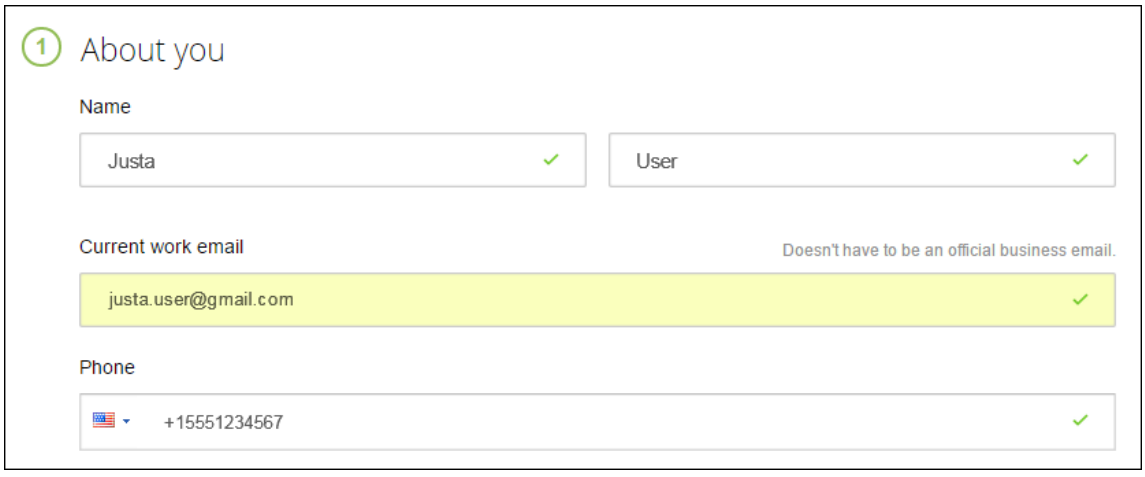
Si ya ha verificado el nombre de su dominio en Google, puede pasar a Configurar una cuenta de servicio de Android Enterprise y descargar un certificado de Android Enterprise.

1. Vaya a https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

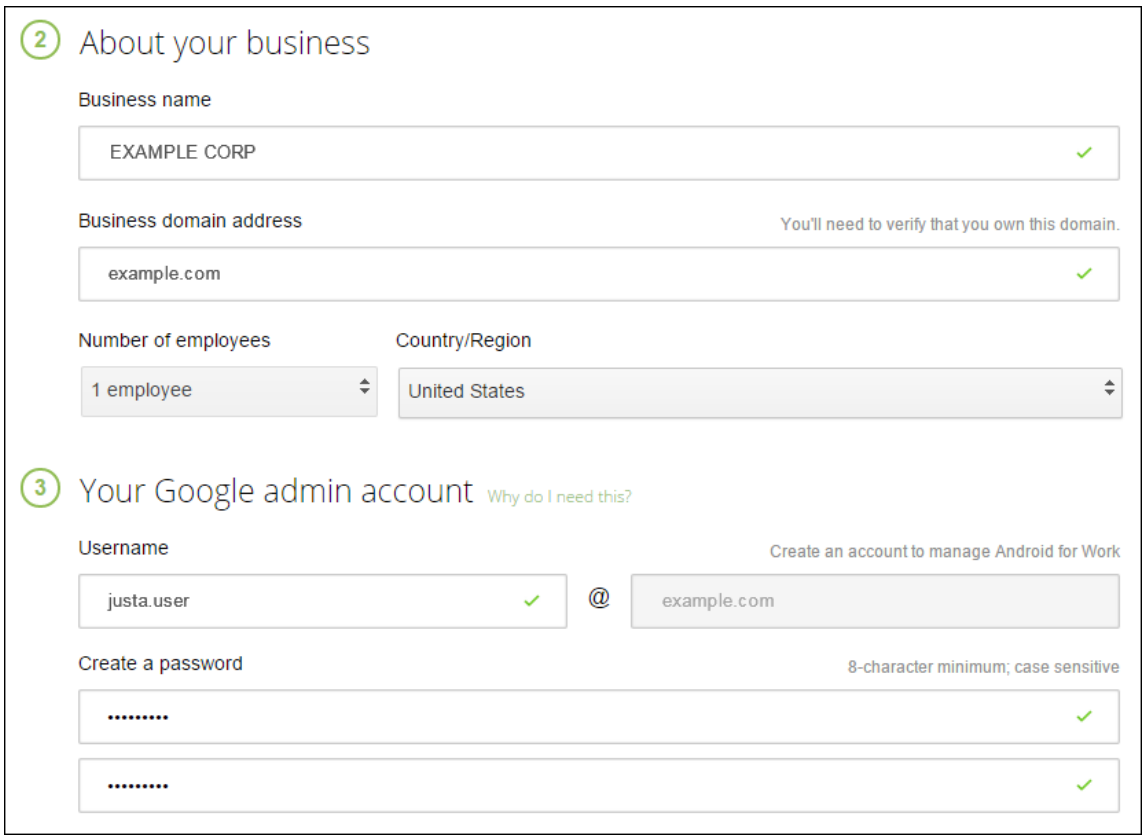
   Aparece la siguiente página, donde puede introducir información sobre el administrador y la empresa.



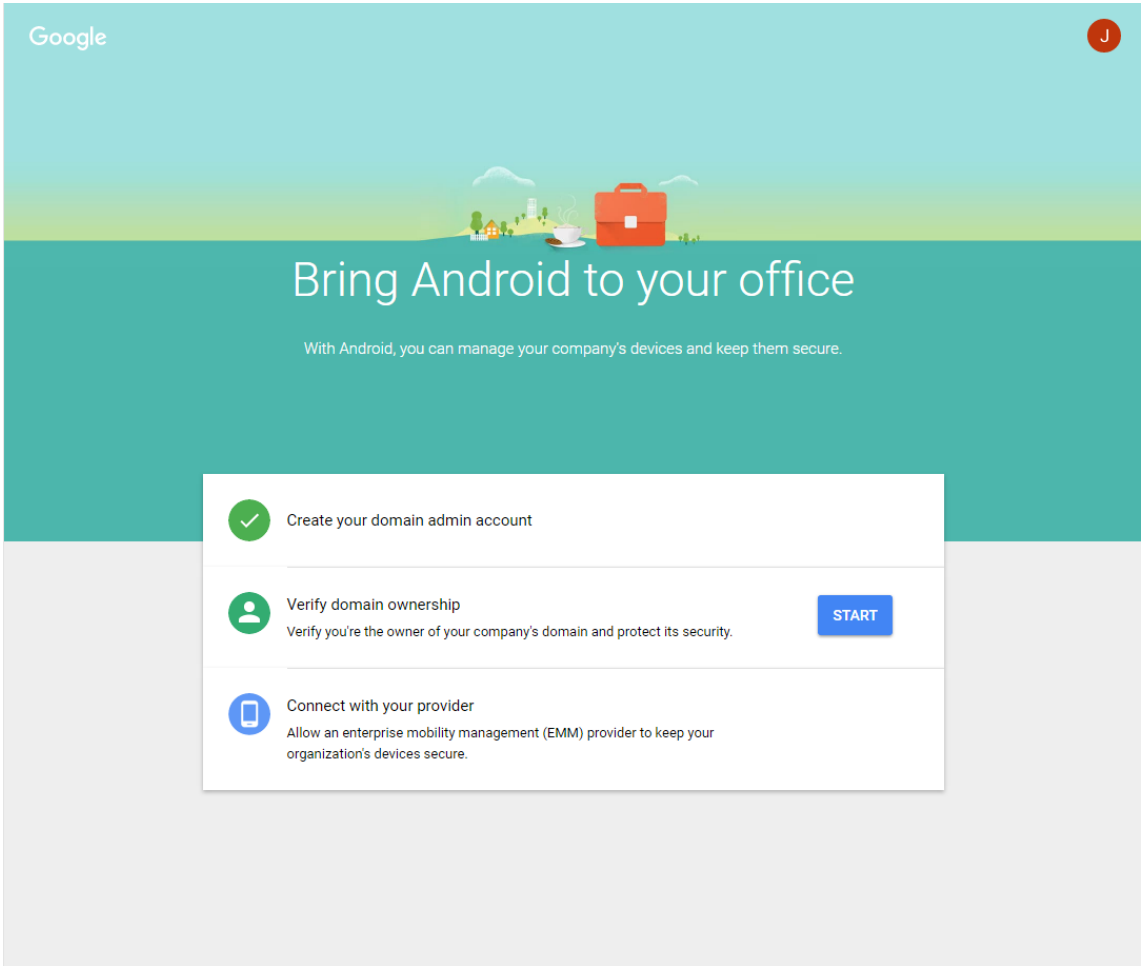
2. Introduzca la información del usuario administrador.



3. Escriba la información de la empresa, además de la información de su cuenta de administrador.



Una vez completado el primer paso, verá la página siguiente.



Verificación de la propiedad del dominio

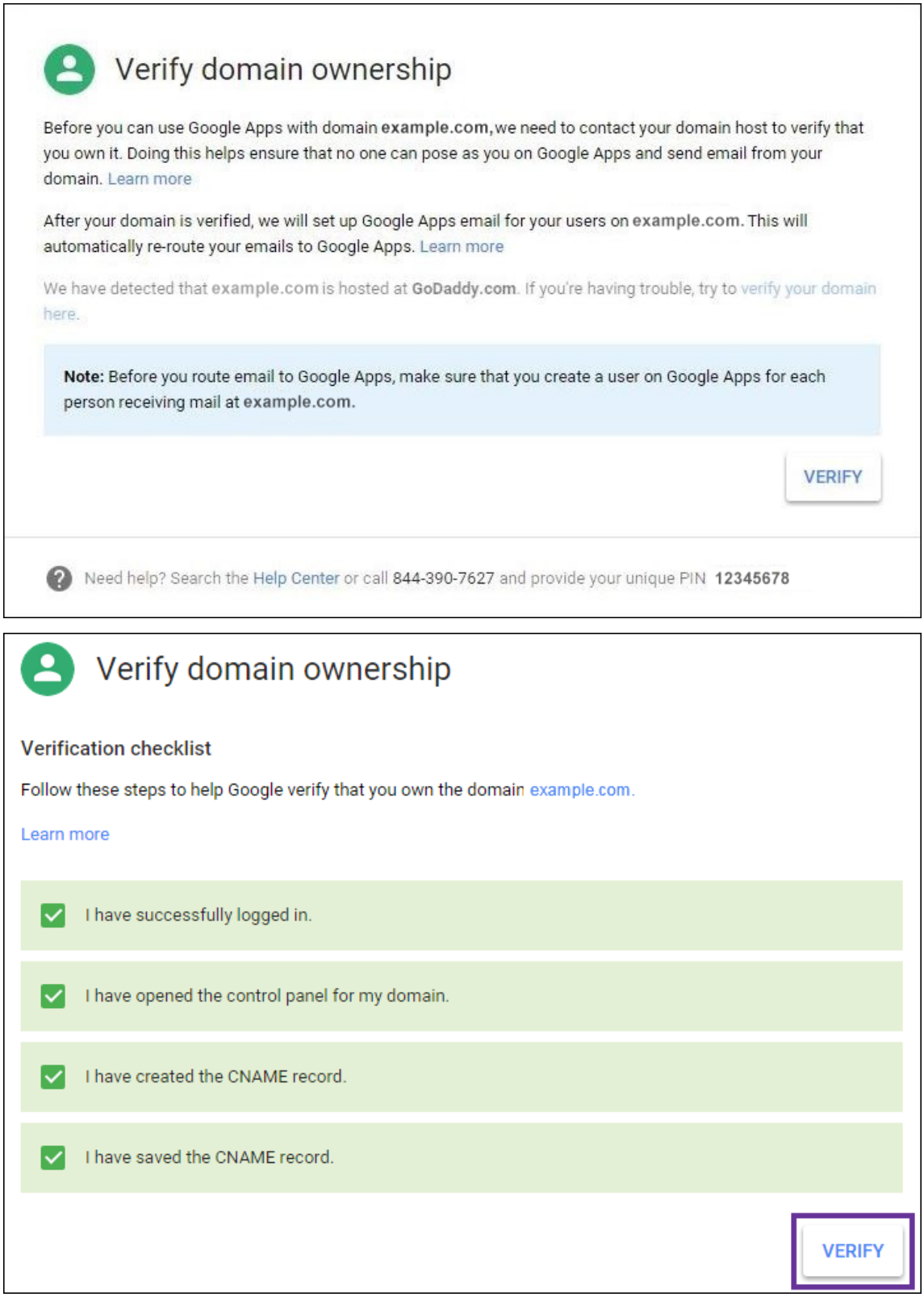
Permita a Google verificar el dominio de alguna de las siguientes maneras:

- Agregue un registro TXT o CNAME al sitio web de su host de dominio.
- Cargue un archivo HTML en el servidor web del dominio.
- Agregue una etiqueta `<meta>` a la página de inicio. Google recomienda el primer método. Los pasos para comprobar que usted es el propietario del dominio no se describen en este artículo, pero puede encontrar esta información aquí: https://support.google.com/a/answer/6248925.

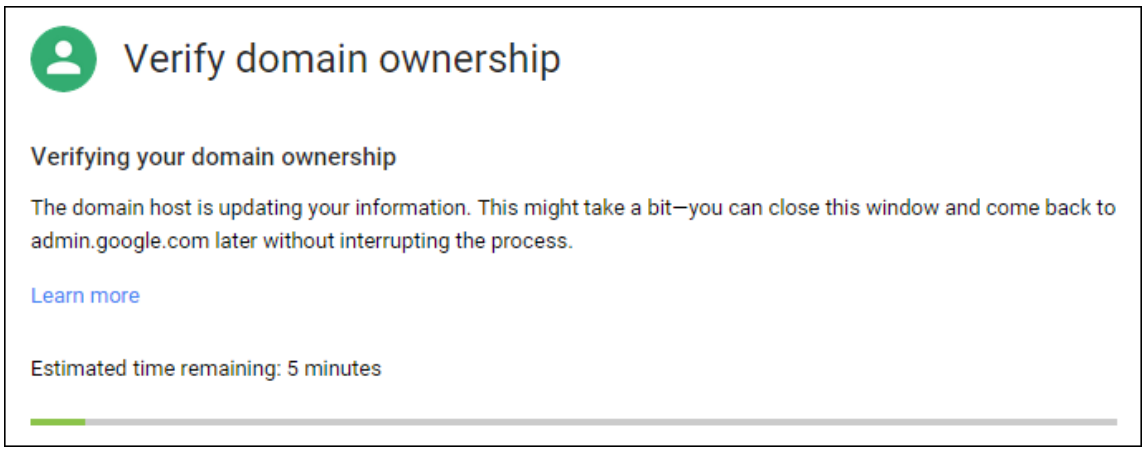
1. Haga clic en **Comenzar** para iniciar la verificación de su dominio.

   Verá la página **Verificar propiedad de dominio**. Siga las instrucciones de esta página para verificar su dominio.

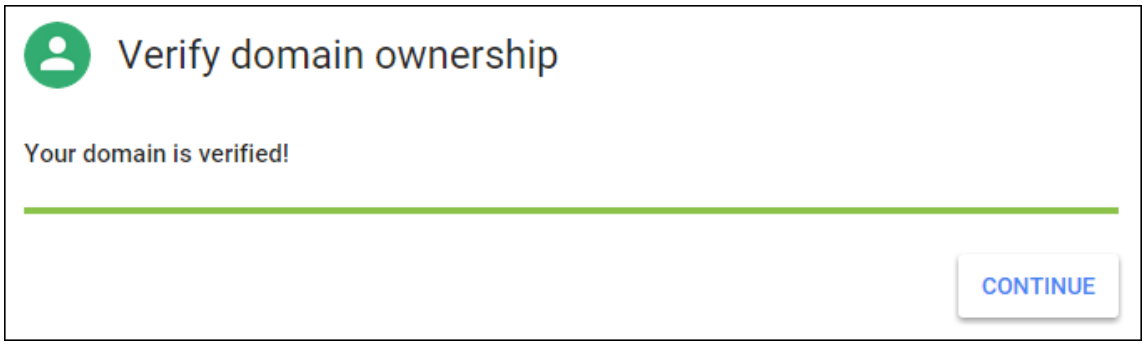
2. Haga clic en **Verificar**.



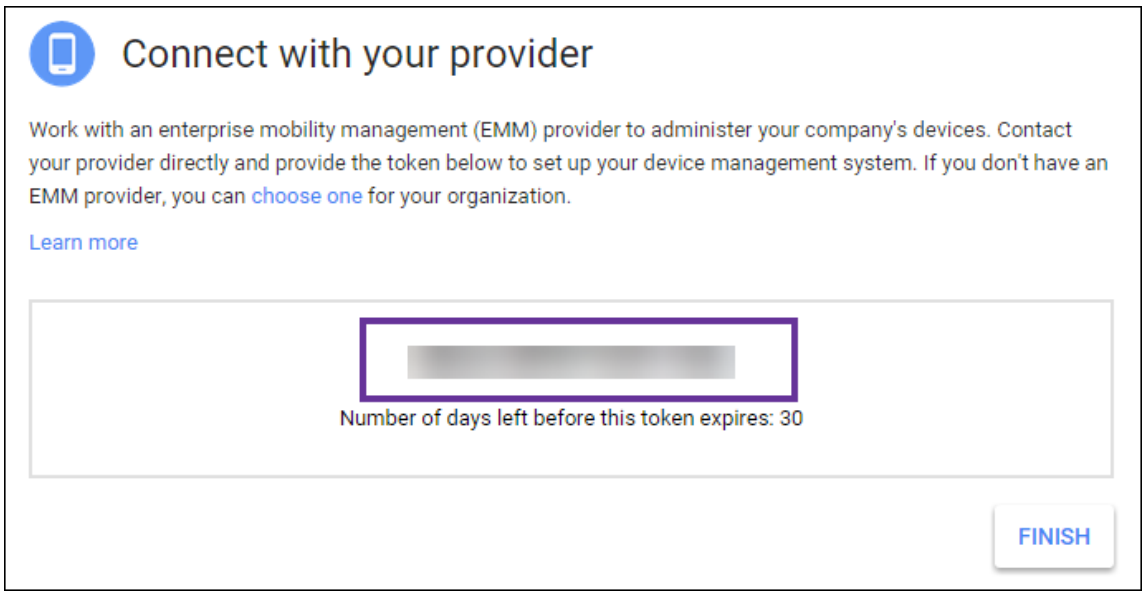
3. Google verifica que usted posee el dominio.



4. Aparecerá la siguiente página tras una verificación correcta. Haga clic en **Continue**.



5. Google crea un token de vinculación de EMM que usted debe suministrar a Citrix y usarlo para configurar los parámetros de Android Enterprise. Copie y guarde el token, porque lo necesitará más adelante durante el procedimiento de configuración.



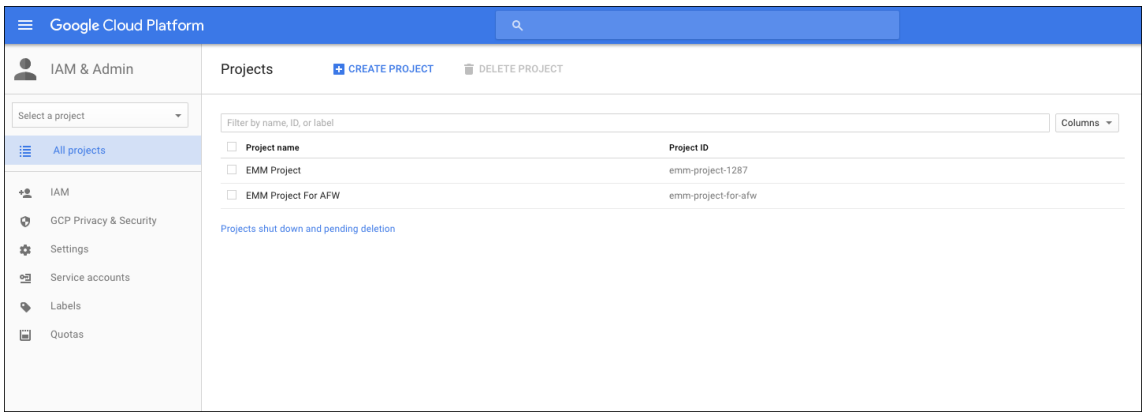
6. Haga clic en **Finalizar** para completar la configuración de Android Enterprise. Aparecerá una página que indicará que el dominio se ha verificado correctamente.

Después de crear una cuenta de servicio de Android Enterprise, puede iniciar sesión en la consola de administración de Google para administrar sus opciones de movilidad.

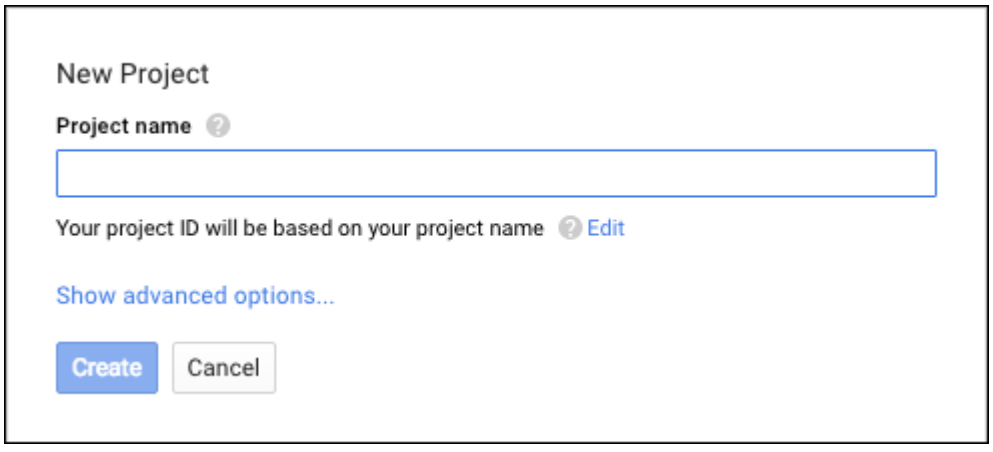
Configuración de una cuenta de servicio de Android Enterprise y descarga de un certificado de Android Enterprise

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 sobre el protocolo de autenticación que se está utilizando, vaya a https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

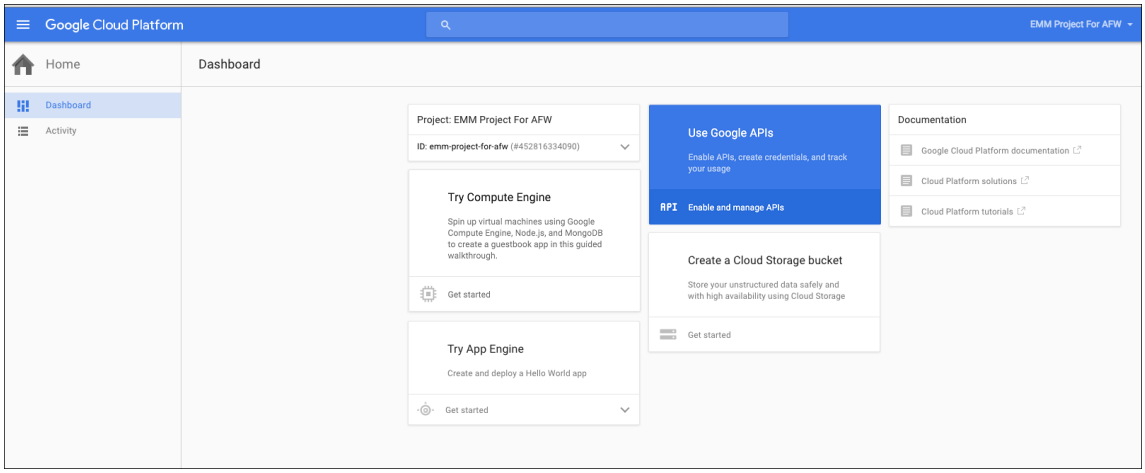
1. En un explorador web, vaya a https://console.cloud.google.com/project e inicie sesión con las credenciales de administrador de Google.
2. En la lista **Projects**, haga clic en **Create Project**.



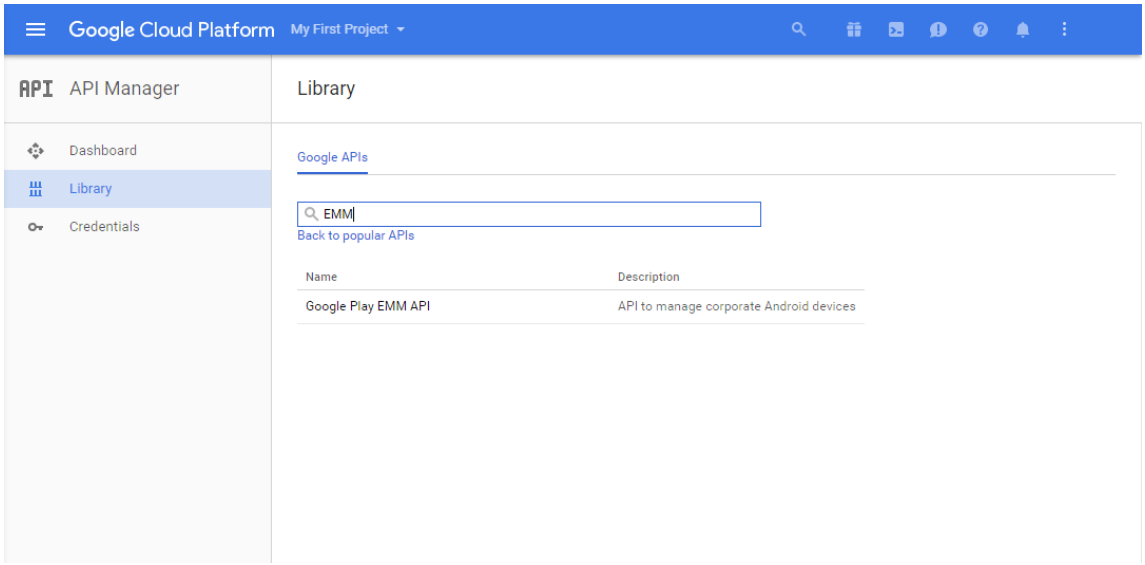
3. En **Project name**, introduzca un nombre para el proyecto.



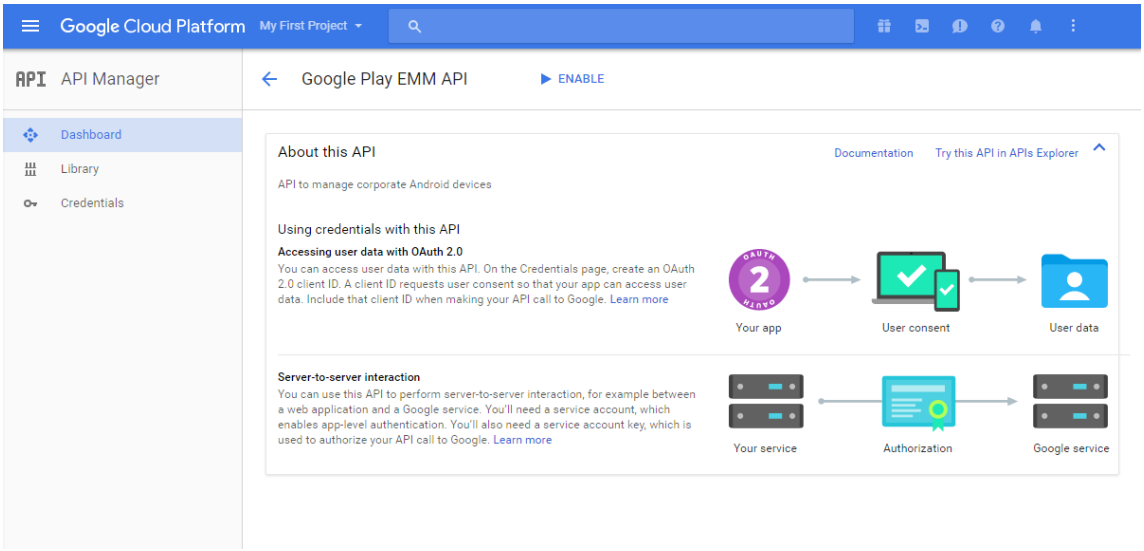
4. En el panel de mandos, haga clic en **Use Google APIs**.



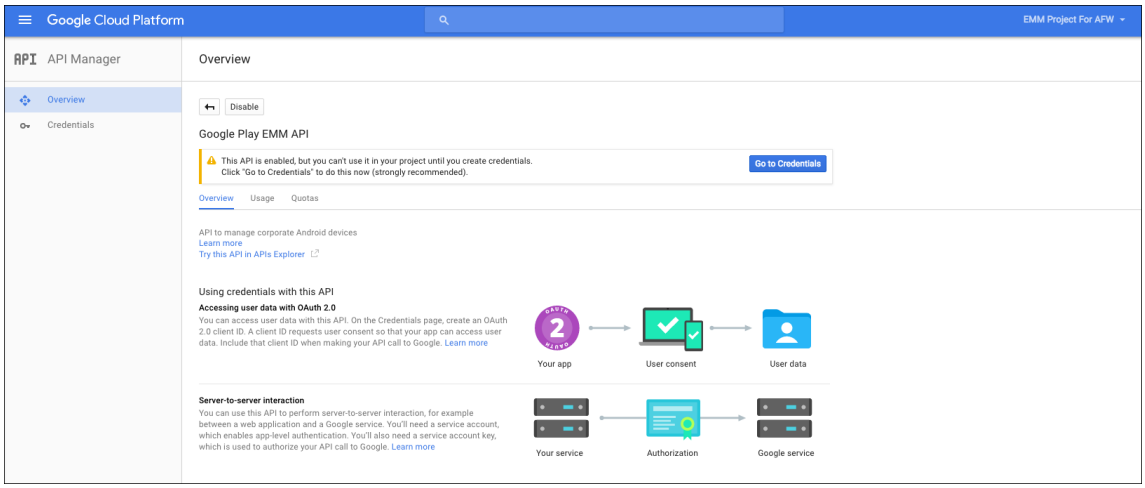
5. Haga clic en **Library** y, en **Search**, escriba **EMM**. A continuación, haga clic en el resultado de la búsqueda.



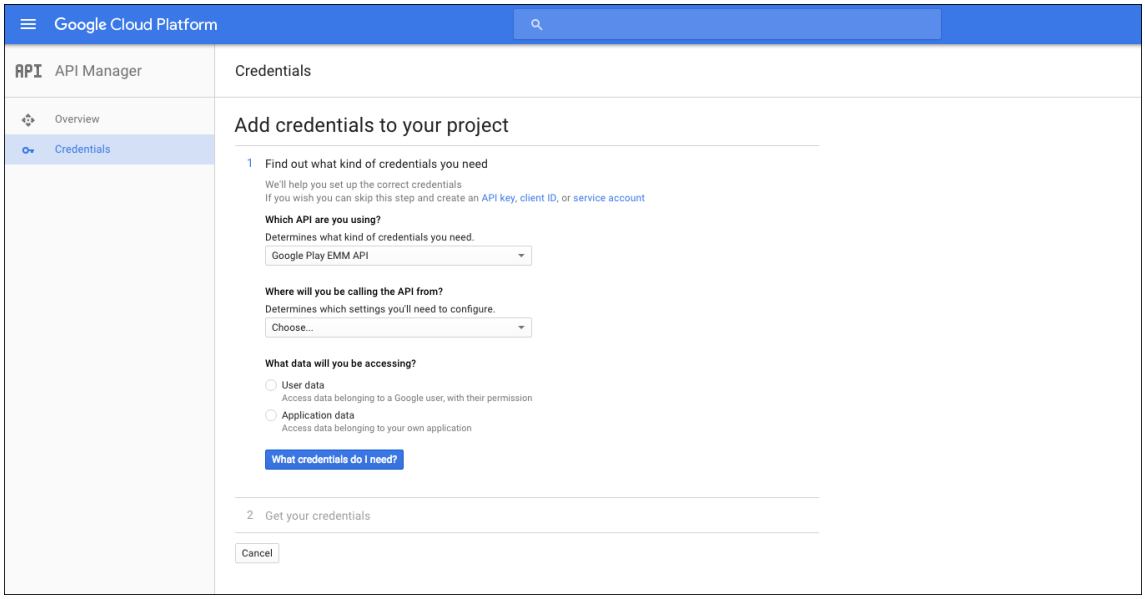
6. En la página **Overview**, haga clic en **Enable**.



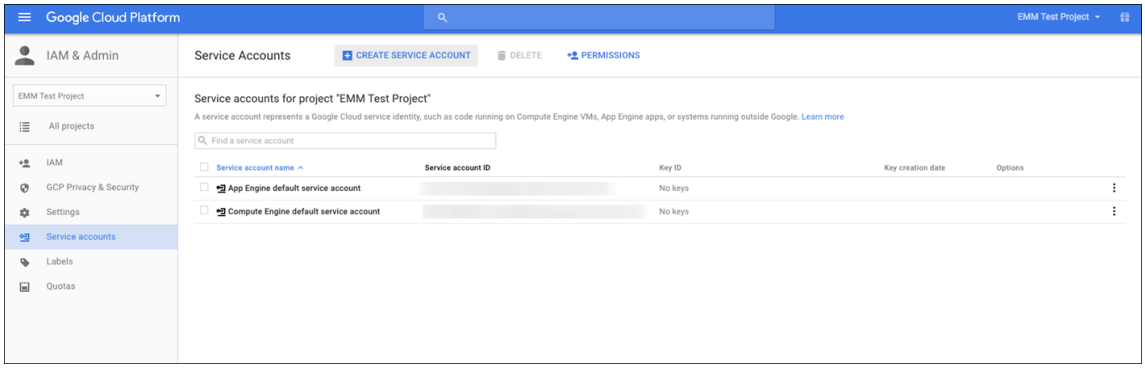
7. Junto a **Google Play EMM API**, haga clic en **Go to Credentials**.



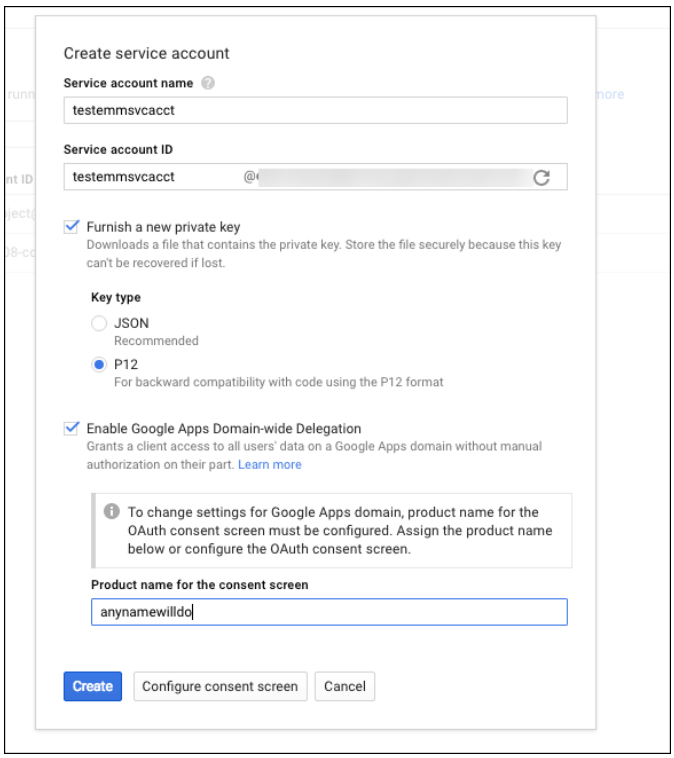
8. En la lista **Add credentials to our project**, en el paso 1, haga clic en **service account**.



9. En la página **Service Accounts**, haga clic en **Create Service Account**.

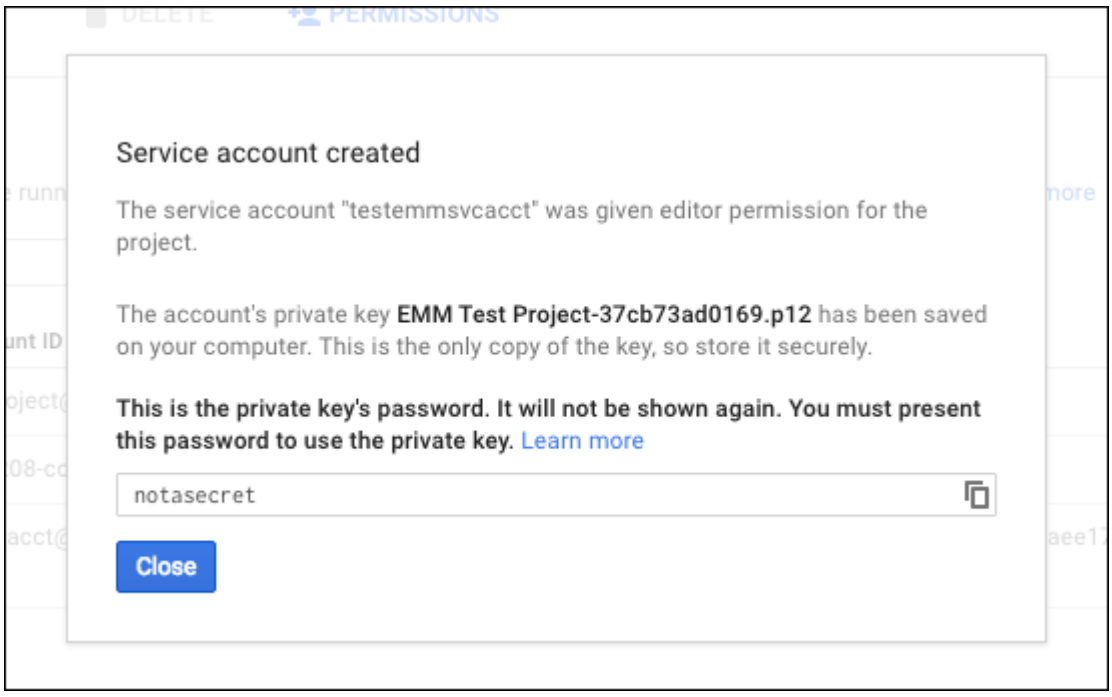


10. En **Create service account**, establezca un nombre para la cuenta y marque la casilla **Furnish a new private key**. Haga clic en **P12**, marque la casilla **Enable Google Apps Domain-wide Delegation** y haga clic en **Create**.

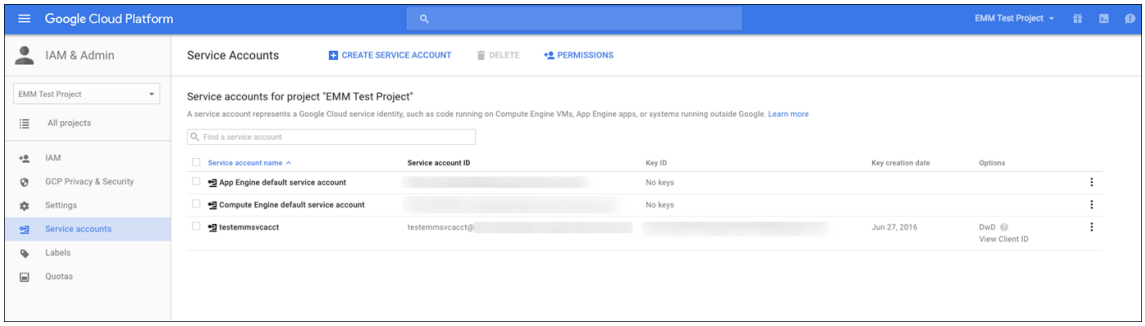


El archivo de certificado (P12) se descargará en su equipo. Guarde el certificado en una ubicación segura.

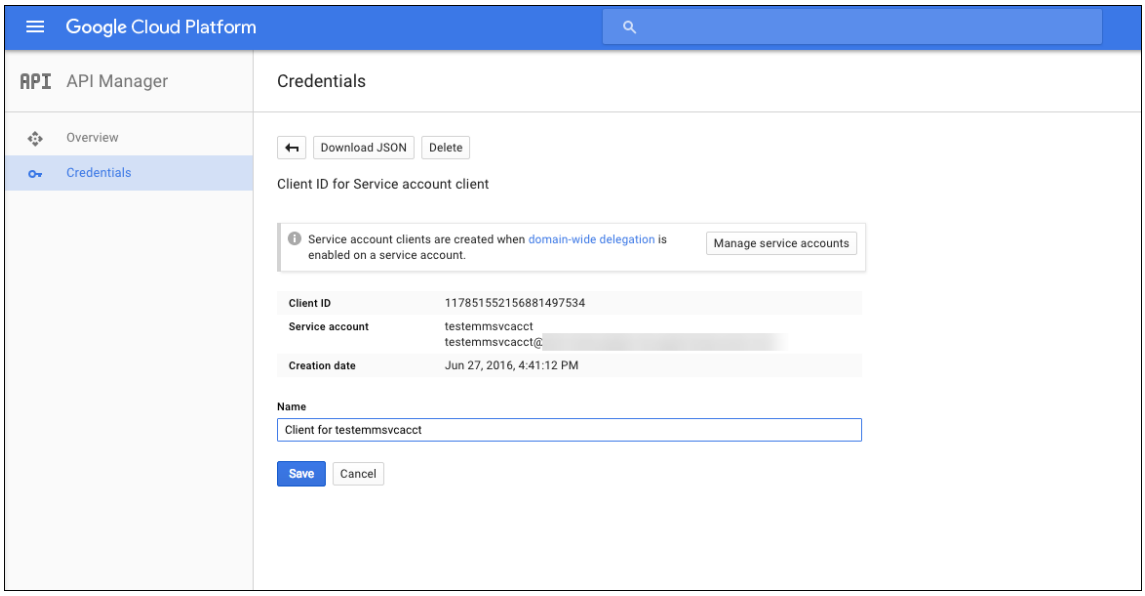
11. En la pantalla de confirmación **Service account created**, haga clic en **Close**.



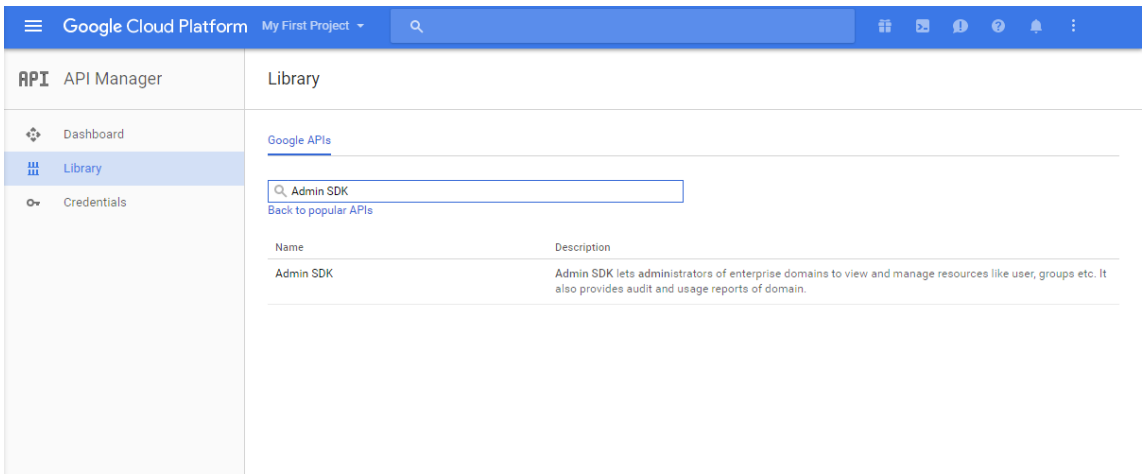
12. En **Permissions**, haga clic en **Service accounts** y, en **Options** para su cuenta de servicio, haga clic en **View Client ID**.



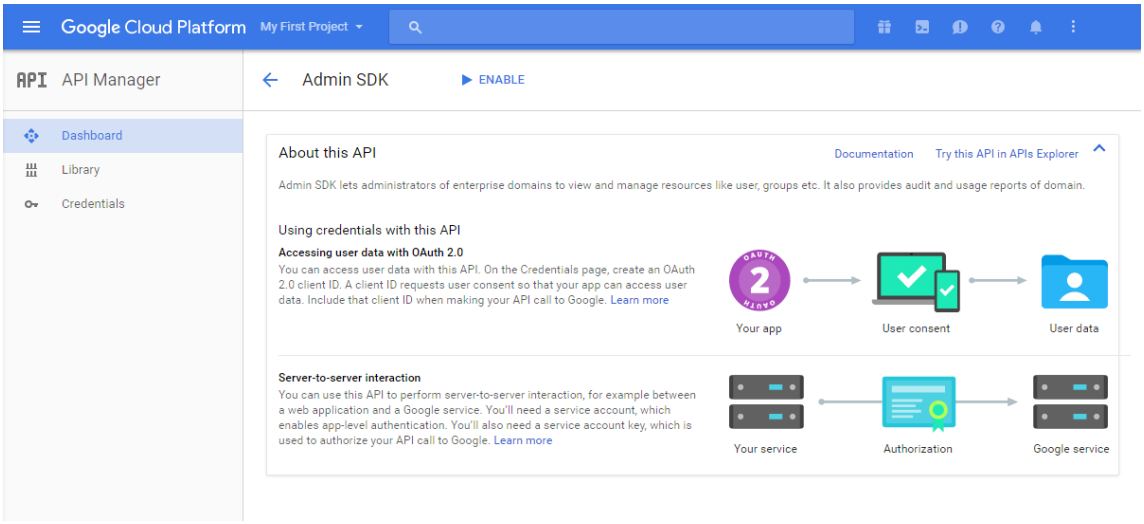
13. Aparecerán los datos requeridos para la autorización de cuentas en la consola de administración de Google. Copie el **ID del cliente** y el **ID de la cuenta de servicio** a una ubicación donde pueda recuperar la información más adelante. Necesita esta información, junto con el nombre de dominio, para enviarla a Citrix para que proceda a permitirla.



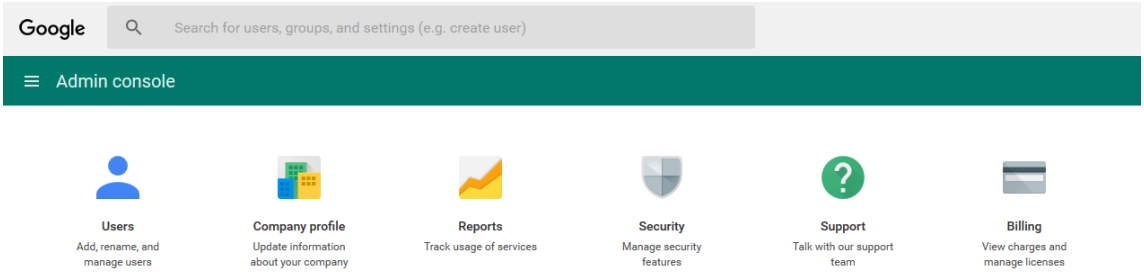
14. En la página **Library**, busque **Admin SDK** y haga clic en el resultado de búsqueda.



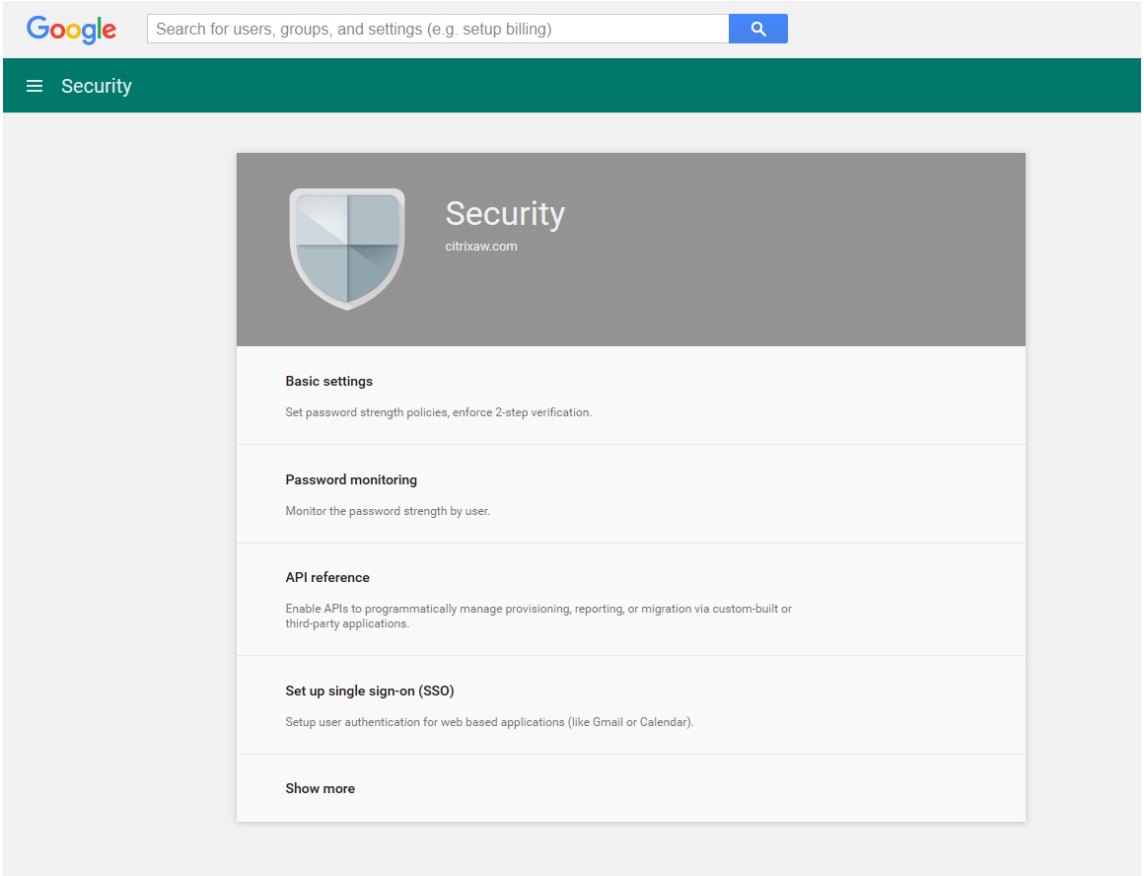
15. En la página **Overview**, haga clic en **Enable**.

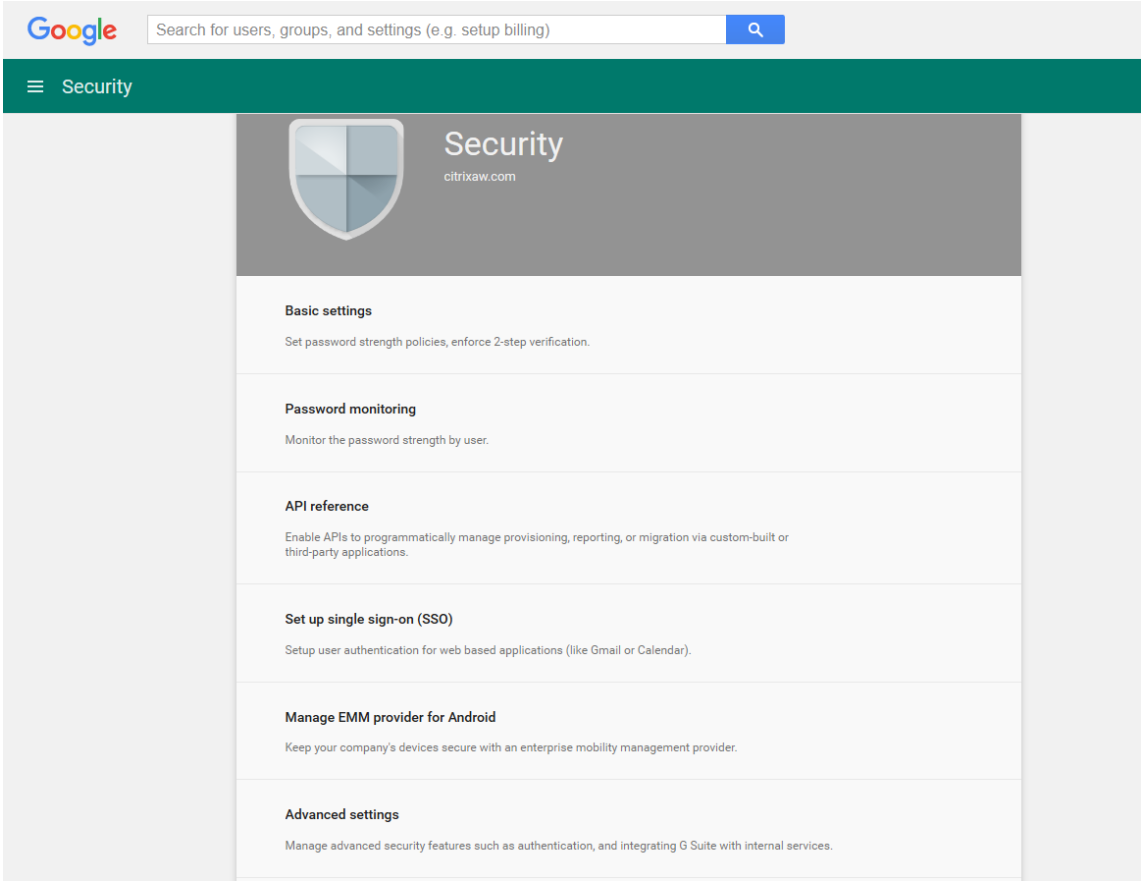


16. Abra la consola de administración de Google para su dominio y haga clic en **Seguridad**.

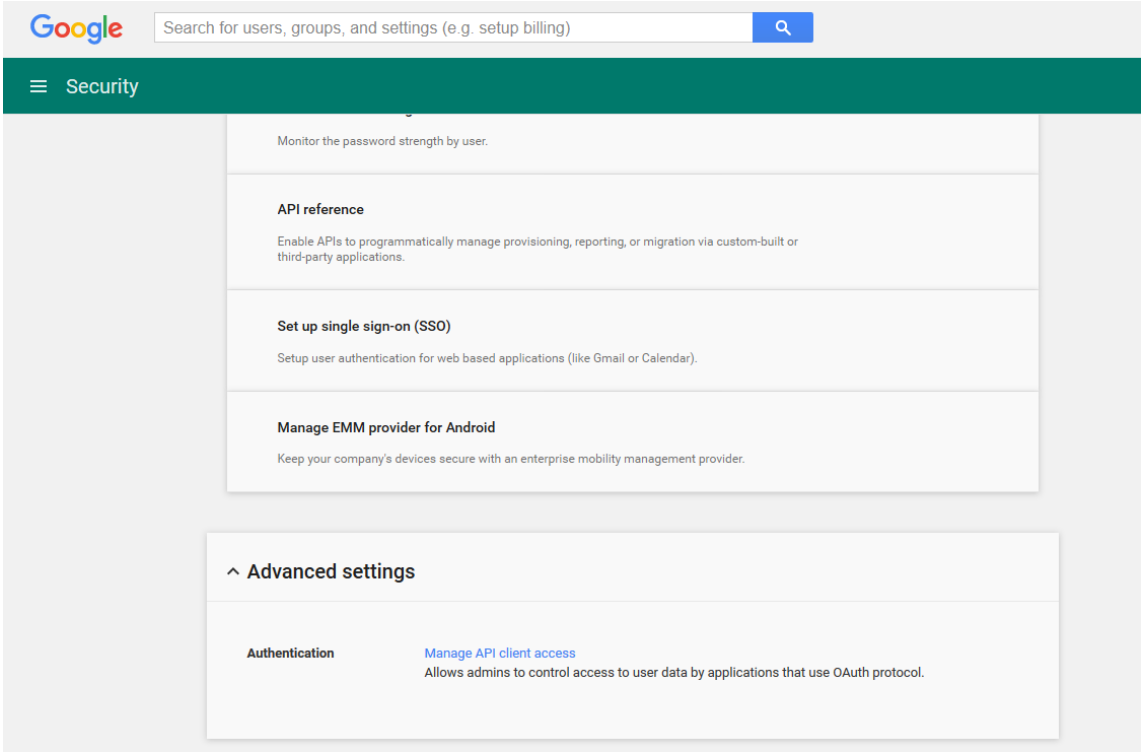


17. En la página **Ajustes**, haga clic en **Mostrar más** y en **Configuración avanzada**.

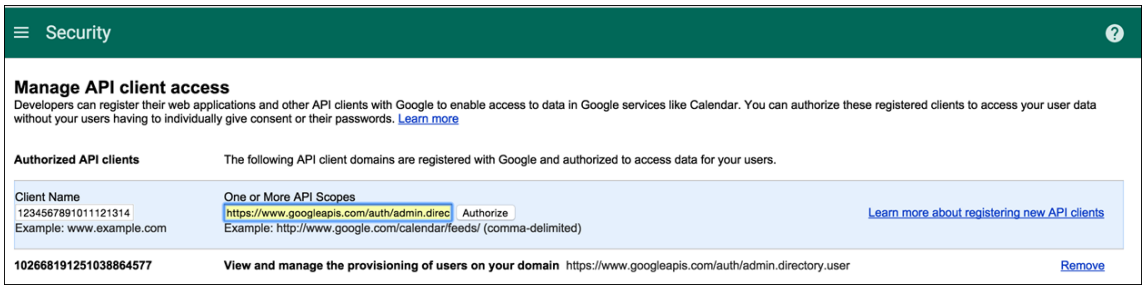




18. Haga clic en **Administrar el acceso de cliente API**.



19. En **Nombre de cliente**, introduzca el ID de cliente que guardó previamente, en **Uno o más ámbitos API**, introduzca `https://www.googleapis.com/auth/admin.directory.user` y haga clic en **Autorizar**.



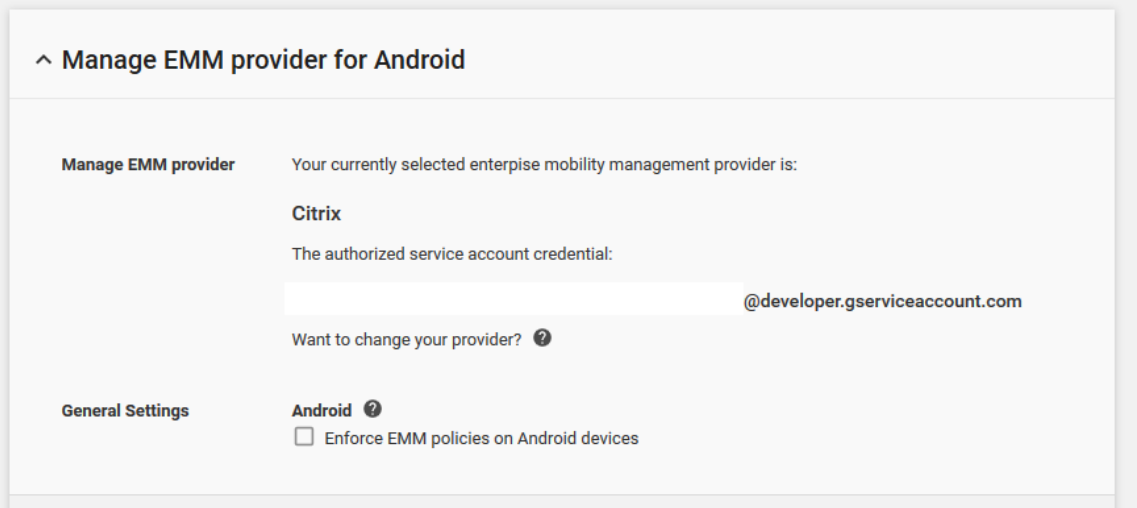
Vincular a EMM

Para poder utilizar XenMobile para administrar los dispositivos Android for Work, 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 **Seguridad**.
2. Haga clic en **Administrar proveedor de EMM de Android**.

   Verá que su cuenta de Google Android Enterprise aparece vinculada a Citrix como su proveedor EMM.

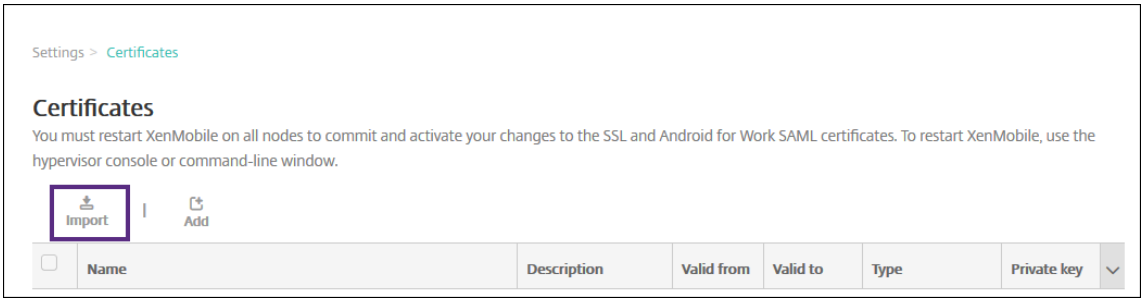
   Después de confirmar la vinculación con el token, ya puede empezar a usar la consola de XenMobile para administrar sus dispositivos Android. Importe el certificado P12 generado en el paso 14. Configure los parámetros del servidor de Android Enterprise, habilite el inicio de sesión Single Sign-On basado en SAML y defina al menos una directiva de dispositivo para Android Enterprise.



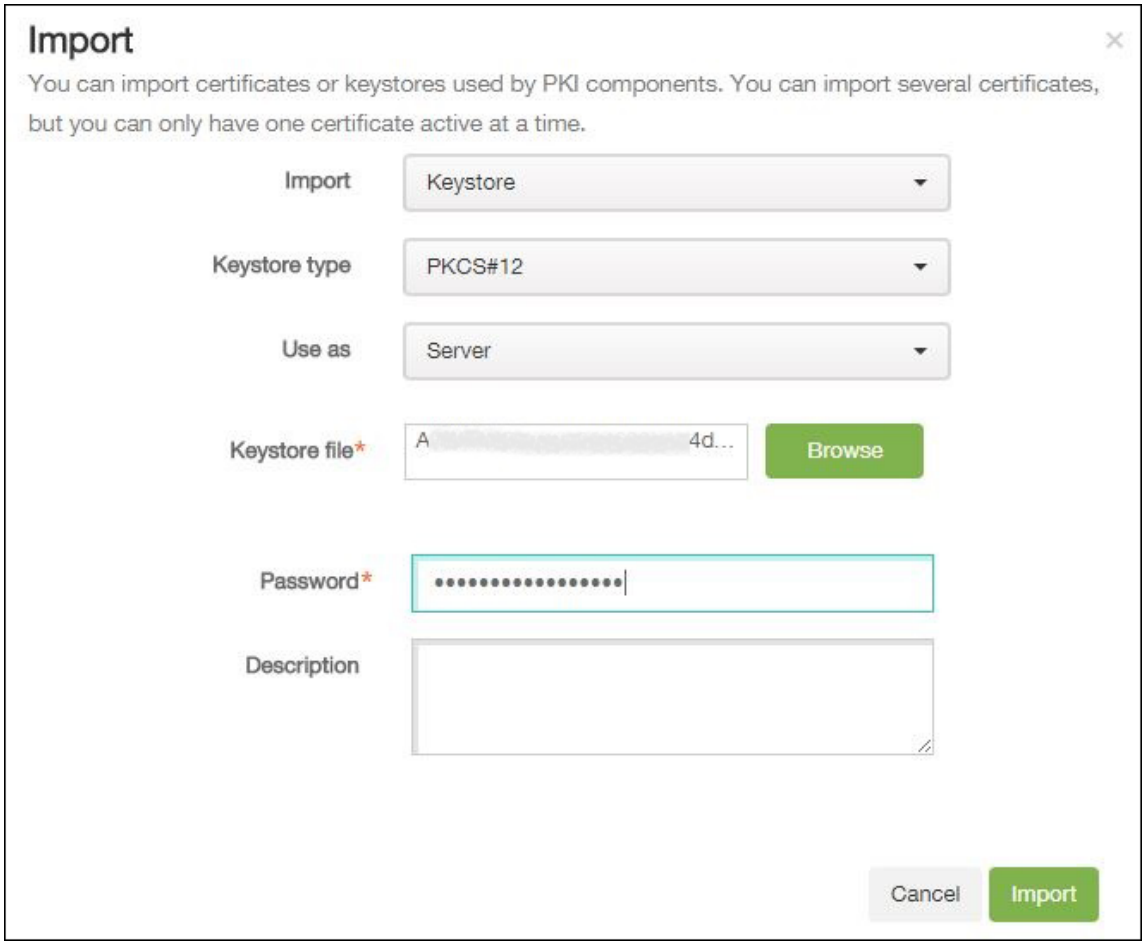
Importar el certificado P12

Siga estos pasos para importar el certificado P12 de Android Enterprise:

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 **Parámetros** y, a continuación, haga clic en **Certificados**. Aparecerá la página **Certificados**.



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



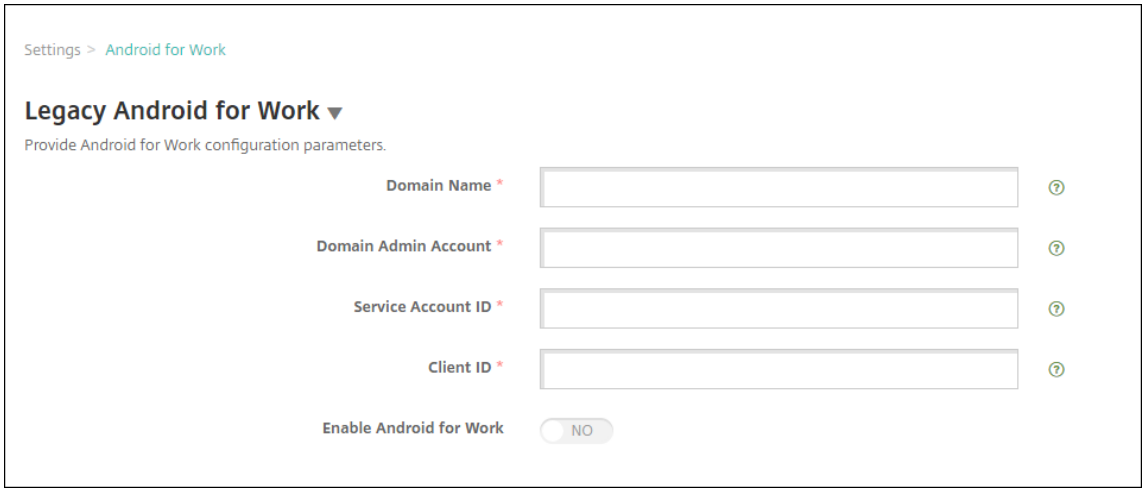
Configure los siguientes parámetros:

- **Importar:** Seleccione **Almacén de claves** en la lista.
- **Tipo de almacén de claves:** Seleccione **PKCS#12** en la lista.
- **Usar como:** Seleccione **Servidor** en la lista.
- **Archivo de almacén de claves:** Haga clic en **Examinar** y vaya al certificado P12.
- **Contraseña:** Escriba la contraseña del almacén de claves.
- **Descripción:** Escriba una descripción opcional del certificado.

4. Haga clic en **Importar**.

Configurar los parámetros de servidor de Android Enterprise

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 **Parámetros**.
2. En **Servidor**, haga clic en **Android Enterprise**. Aparecerá la página **Android Enterprise**.

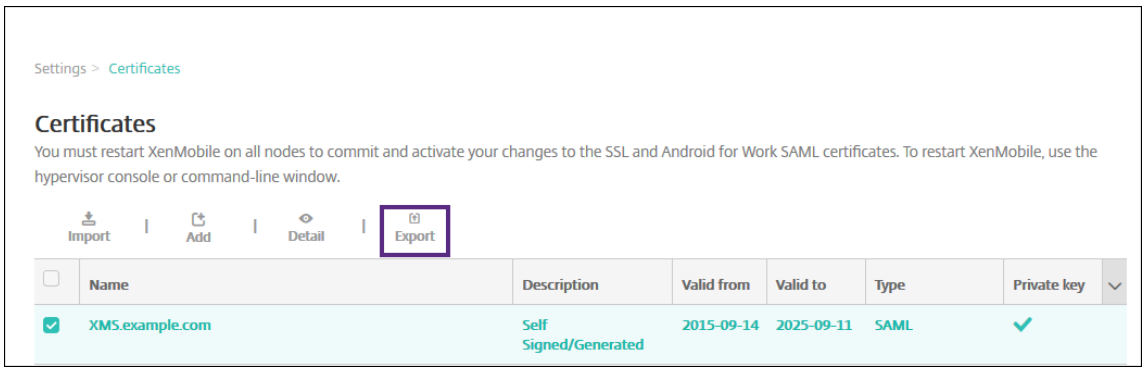


Configure estos parámetros y haga clic en **Guardar**.

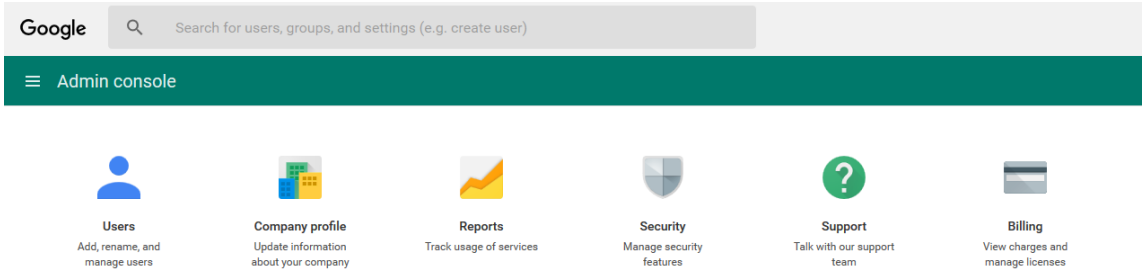
- **Nombre de dominio:** Introduzca el nombre del dominio de Android Enterprise. Por ejemplo: dominio.com
- **Cuenta de administrador de dominio:** Introduzca el nombre de usuario del administrador del dominio; por ejemplo, la cuenta de correo electrónico utilizada en el portal Google Developer Portal.
- **ID de cuenta de servicio:** 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`).
- **ID de cliente:** Escriba el ID numérico del cliente correspondiente a su cuenta de servicio de Google.
- **Habilitar Android Enterprise:** Seleccione para habilitar o inhabilitar Android Enterprise.

Habilitar Single Sign-On basado en SAML

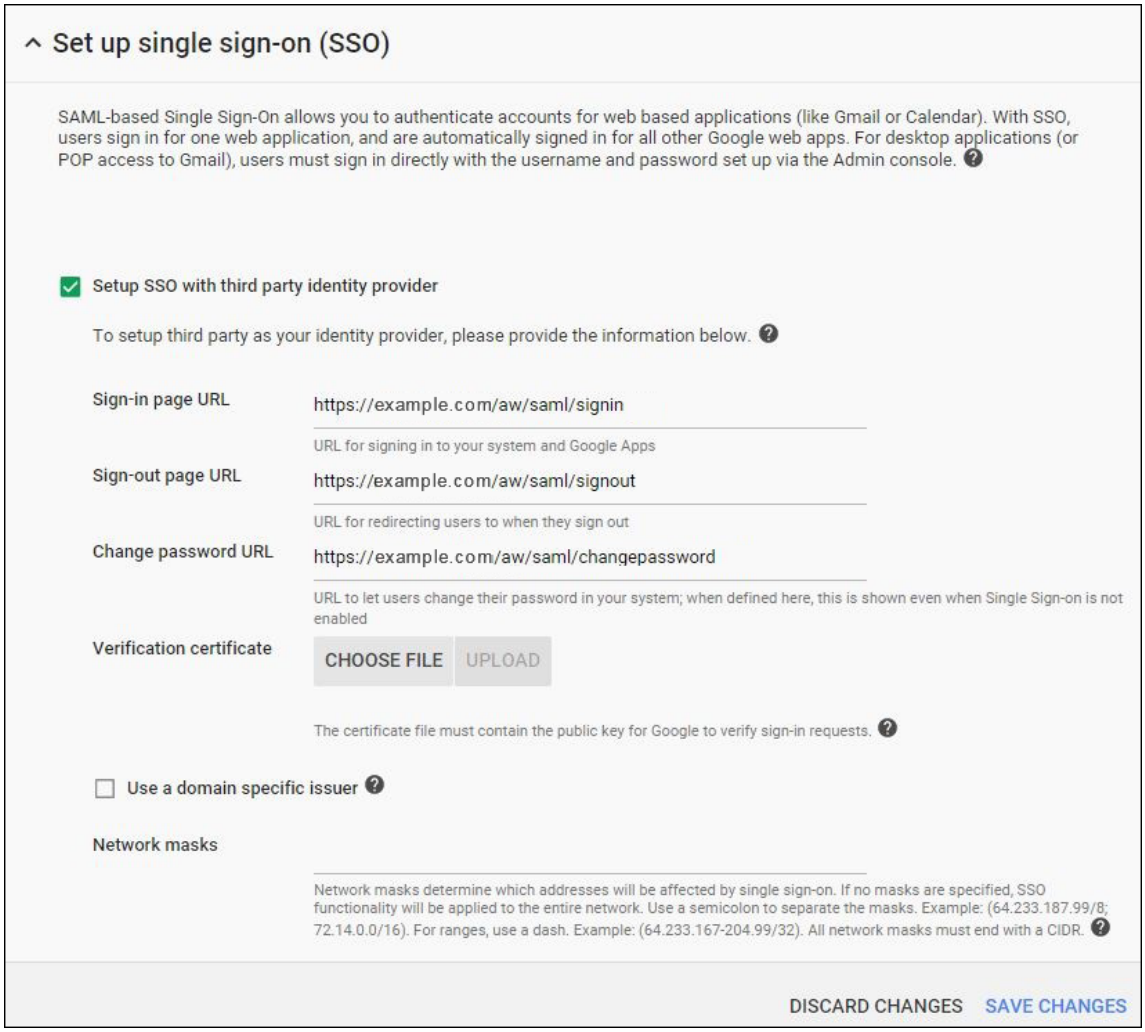
1. Inicie sesión en la consola de XenMobile.
2. Haga clic en el icono de engranaje en la esquina superior derecha de la consola. Aparecerá la página **Parámetros**.
3. Haga clic en **Certificados**. Aparecerá la página **Certificados**.



4. En la lista de certificados, haga clic en el certificado SAML.
5. Haga clic en **Exportar** y guarde el certificado en su equipo.
6. Inicie sesión en el portal de Google Admin con las credenciales de administrador de Android Enterprise. Para acceder al portal, consulte portal Google Admin.
7. Haga clic en **Seguridad**.



8. En **Seguridad**, haga clic en **Configurar inicio de sesión único (SSO)** y configure los parámetros siguientes:

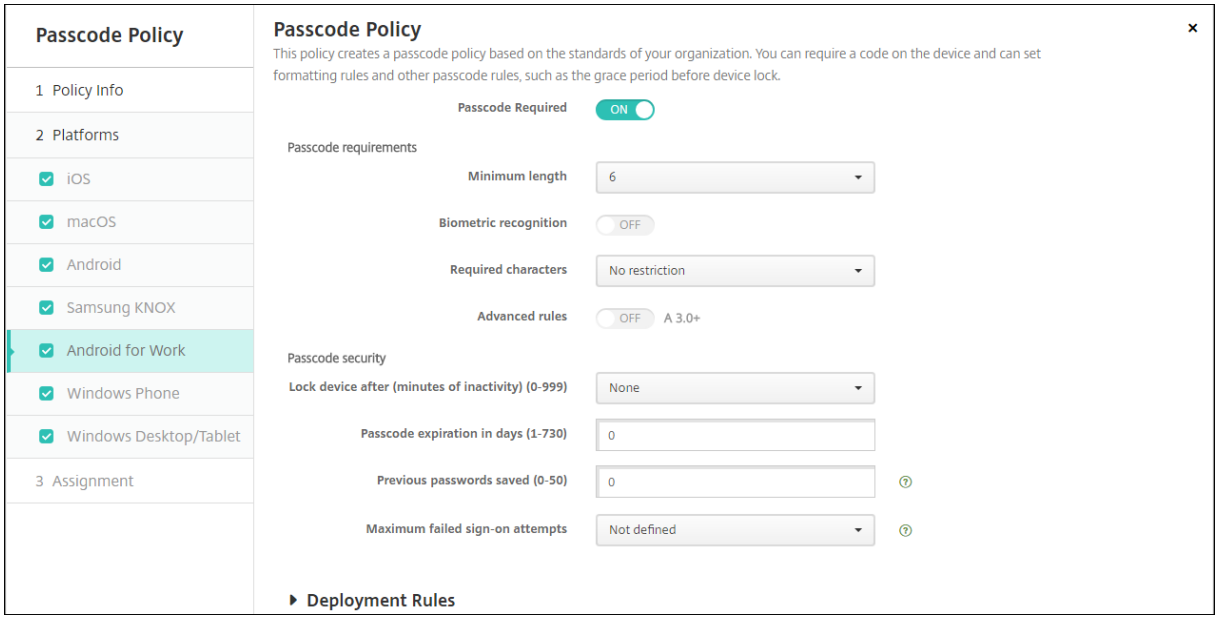


- **URL de la página de inicio de sesión:** Introduzca la URL para que los usuarios inicien sesiones en el sistema y Google Apps. Por ejemplo: `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **URL de la página de cierre de sesión:** Introduzca la URL a la que se redirige a los usuarios cuando cierran la sesión. Por ejemplo: `https://<Xenmobile-FQDN>/aw/saml/signout`.
- **Cambiar URL de contraseña:** Introduzca la URL para permitir que los usuarios cambien su contraseña en el sistema. Por ejemplo: `https://<Xenmobile-FQDN>/aw/saml/changepassword`. Si se define este campo, los usuarios verán esta solicitud incluso cuando SSO no esté disponible.
- **Certificado de verificación:** Haga clic en **ELEGIR ARCHIVO** y busque el certificado SAML exportado desde XenMobile.

9. Haga clic en **Guardar cambios**.

Configurar una directiva de dispositivo para Android Enterprise

Configure una directiva de códigos de acceso para requerir que los usuarios definan un código de acceso en sus dispositivos la primera vez que los inscriban.



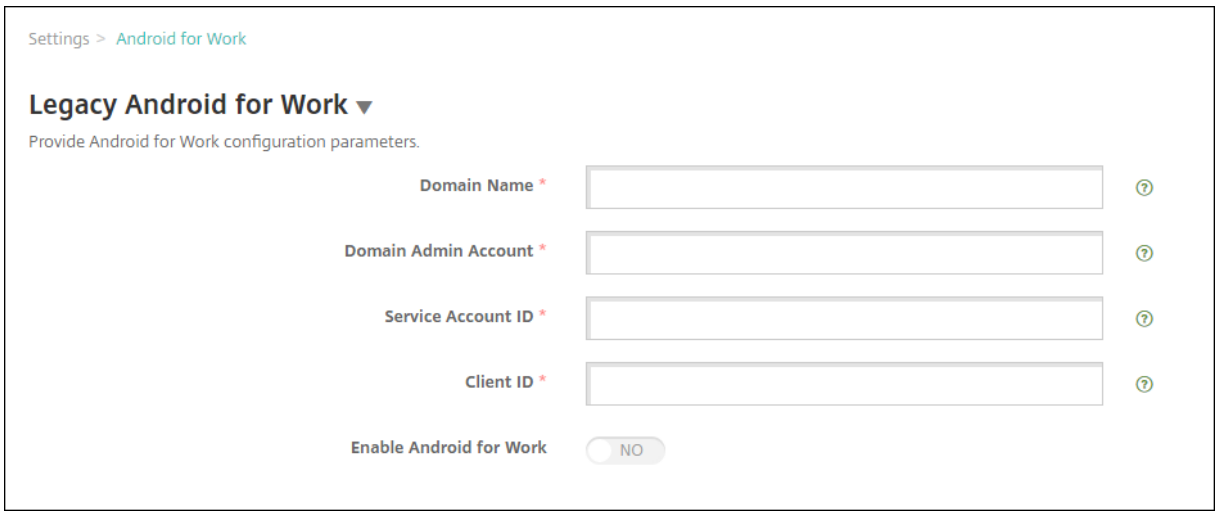
Estos son los pasos básicos para configurar una directiva de dispositivo:

1. Inicie sesión en la consola de XenMobile.
2. Haga clic en **Configurar** y, a continuación, en **Directivas de dispositivo**.
3. Haga clic en **Agregar** y seleccione la directiva que quiere agregar en el cuadro de diálogo **Agregar nueva directiva**. Para este ejemplo, haga clic en **Código de acceso**.
4. Complete la página **Información de directiva**.
5. Haga clic en **Android Enterprise** y defina las configuraciones de la directiva.
6. Asigne la directiva a un grupo de entrega.

Configurar parámetros de cuenta para Android Enterprise

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 Enterprise. Primero, debe completar las tareas de configuración de Android Enterprise en Google para definir un administrador de dominio y obtener un ID de cuenta de servicio, así como un token de vinculación.

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 **Parámetros**.
2. En **Servidor**, haga clic en **Android Enterprise**. Aparecerá la página de configuración **Android Enterprise**.



1. En la página **Android Enterprise**, configure los siguientes parámetros:
    - **Nombre de dominio:** Introduzca el nombre de dominio.
    - **Cuenta de administrador de dominio:** Escriba el nombre de usuario del administrador de dominio.
    - **ID de cuenta de servicio:** Escriba el ID de la cuenta de servicio de Google.
    - **ID de cliente:** Escriba el ID del cliente correspondiente a su cuenta de servicio de Google.
    - **Habilitar Android Enterprise:** Seleccione si habilitar o no Android Enterprise.
2. Haga clic en **Guardar**.

Configurar el acceso de socios de Google Workspace para XenMobile

Algunas funciones para la administración de dispositivos de punto final que ofrece Chrome usan las API de socios de Google para la comunicación entre XenMobile y el dominio de Google Workspace. Por ejemplo, XenMobile requiere las API para las directivas de dispositivo que administran las funciones de Chrome (como el modo incógnito y el modo invitado).

Para habilitar las API de socios, configure su dominio de Google Workspace en la consola de XenMobile y, a continuación, configure su cuenta de Google Workspace.

Configurar el dominio de Google Workspace (anteriormente G Suite) en XenMobile

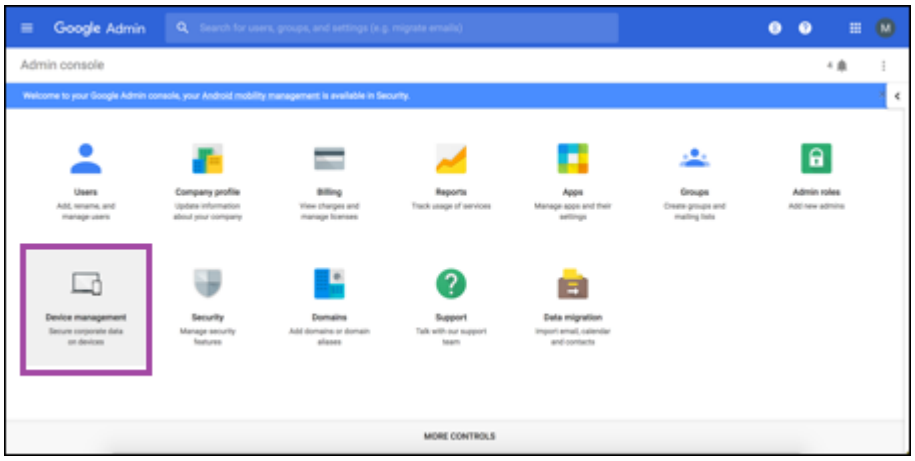
Para permitir que XenMobile se comunique con las API en su dominio de Google Workspace, vaya a **Parámetros > Configuración de Google Chrome** y defina estos parámetros.

- **Dominio de G Suite:** El dominio de Google Workspace que aloja las API que necesita XenMobile.
- **Administrador de G-Suite:** La cuenta de administrador del dominio de G Suite.
- **ID de cliente de G Suite:** El ID de cliente para Citrix. Utilice este valor para configurar el acceso de socio para su dominio de Google Workspace.

- **ID de G Suite Enterprise:** El ID de empresa de la cuenta, rellenado desde su cuenta empresarial de Google.

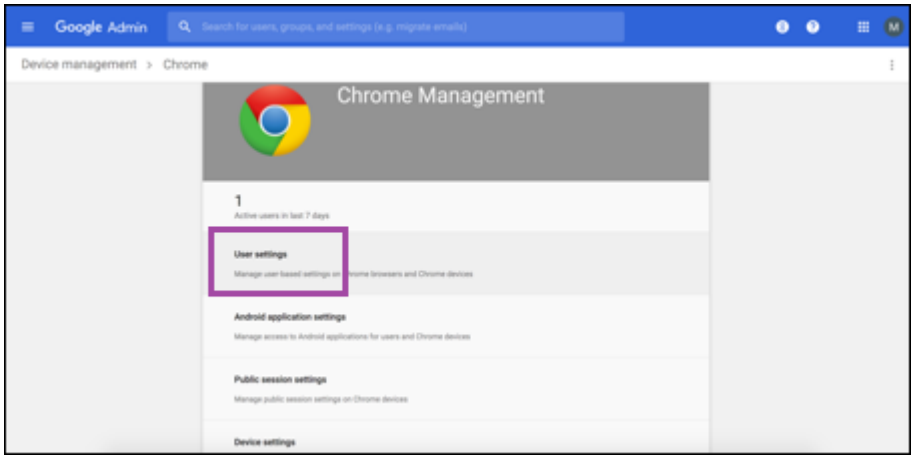
Habilitar el acceso de socios para dispositivos y usuarios en su dominio de Google Workspace

1. Inicie sesión en la Consola de administración de Google: https://admin.google.com.
2. Haga clic en **Administración de dispositivos**.



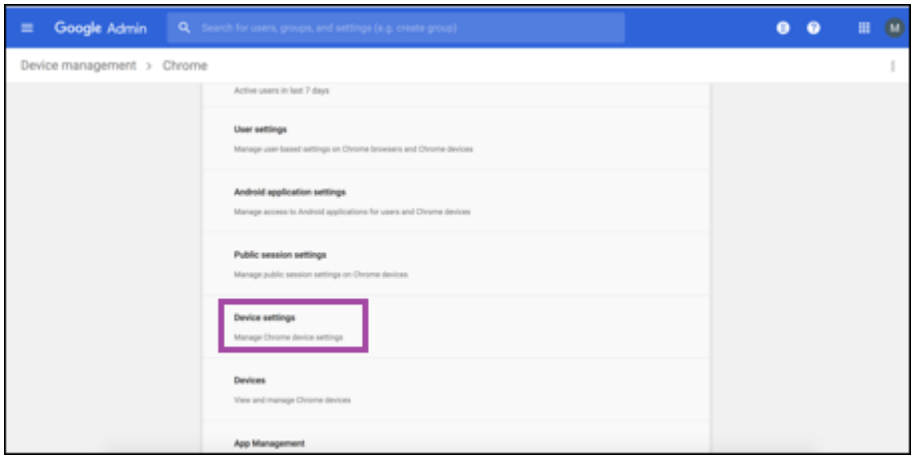
3. Haga clic en **Administración de Chrome**.

4. Haga clic en **Configuración de usuario**.



5. Busque **Administración de Chrome - Acceso de partners**.

6. Marque la casilla **Habilitar Administración de Chrome - Acceso de partners**.
7. Acepte el indicador de que comprende y quiere habilitar el acceso de socios. Haga clic en **Guardar**.
8. En la página de administración de Chrome, haga clic en **Configuración del dispositivo**.



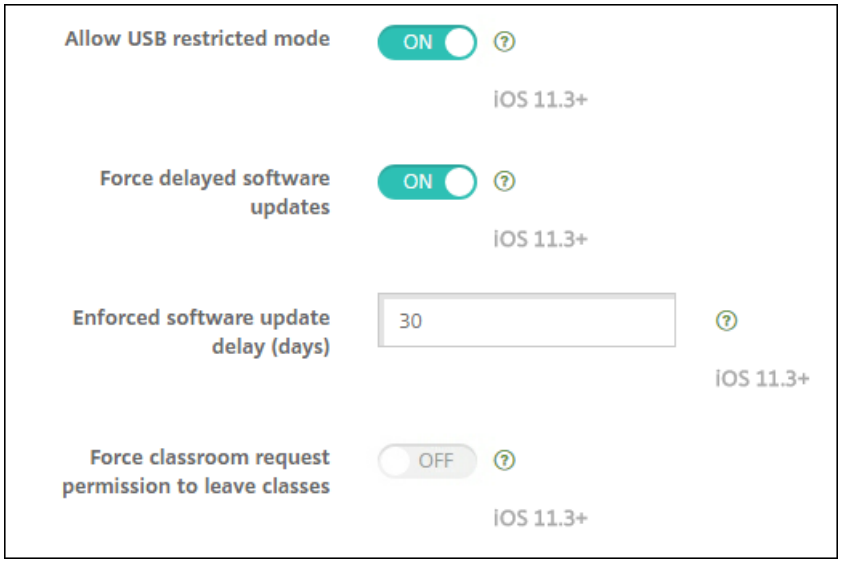
9. Busque **Administración de Chrome - Acceso de partners**.

10. Marque la casilla **Habilitar Administración de Chrome - Acceso de partners**.
11. Acepte el indicador de que comprende y quiere habilitar el acceso de socios. Haga clic en **Guardar**.
12. Vaya a la página **Seguridad** y haga clic en **Configuración avanzada**.

13. Haga clic en **Administrar el acceso de cliente API**.
14. En la consola de XenMobile, vaya a **Parámetros > Configuración de Google Chrome** y copie el valor de ID de cliente de Google Workspace. A continuación, vuelva a la página **Administrar el acceso de cliente API** y pegue el valor copiado en el campo **Nombre de cliente**.
15. En **Uno o más ámbitos API**, agregue la URL: `https://www.googleapis.com/auth/chromedevicemanagementapi`

16. Haga clic en **Autorizar**.

    Aparece el mensaje de configuración guardada.



Inscribir dispositivos Android Enterprise

Si el proceso de inscripción de dispositivos requiere que los usuarios introduzcan un ID o un nombre de usuario, el formato aceptado depende de cómo esté configurado el servidor de XenMobile para buscar usuarios (por nombre principal de usuario (UPN) o por nombre de cuenta SAM).

Si el servidor de XenMobile está configurado para buscar usuarios por nombre UPN, los usuarios deben introducir un nombre UPN en el formato:

- *nombre de usuario@dominio*

Si el servidor de XenMobile está configurado para buscar usuarios por SAM, los usuarios deben introducir un SAM en uno de estos formatos:

- *nombre de usuario@dominio*
- *dominio\nombre de usuario*

Para determinar para qué tipo de nombre de usuario está configurado su servidor de XenMobile:

1. En la consola del servidor de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Haga clic en **LDAP** para ver la configuración de la conexión LDAP.
3. En la parte inferior de la página, verá el campo **Buscar usuarios por**:
    - Si está establecido en **userPrincipalName**, el servidor de XenMobile está configurado para buscar usuarios por nombre UPN.
    - Si está establecido en **sAMAccountName**, el servidor de XenMobile está configurado para buscar usuarios por cuenta SAM.

Desinscribir una empresa de Android Enterprise

Puede desinscribir una empresa de Android Enterprise mediante la consola de XenMobile Server y las herramientas de XenMobile Tools.

Cuando realiza esta tarea, XenMobile Server abre una ventana emergente para XenMobile Tools. Antes de comenzar, asegúrese de que XenMobile Server tenga permiso para abrir ventanas emergentes en el explorador web que esté utilizando. Algunos exploradores web, como Google Chrome, requieren que se inhabilite el bloqueo de ventanas emergentes y se agregue la dirección del sitio de XenMobile a la lista de permitidos para bloquear ventanas emergentes.

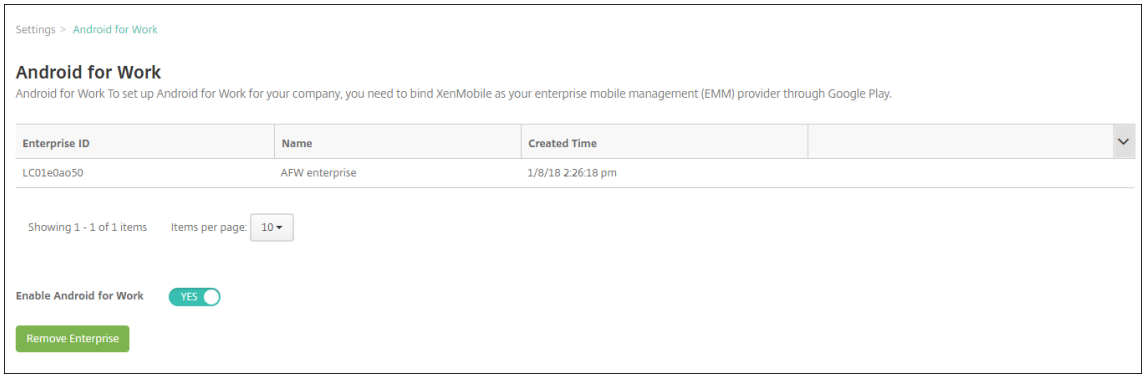
> **Advertencia:**
>
> Una vez que se haya desinscrito una empresa, las aplicaciones Android Enterprise en dispositivos ya inscritos a través de ella se restablecen a sus estados predeterminados. Google ya no administrará los dispositivos. Volver a inscribirlos en una empresa de Android Enterprise podría requerir una configuración adicional para restaurar la funcionalidad anterior.

Después de que la empresa Android Enterprise se ha desinscrito:

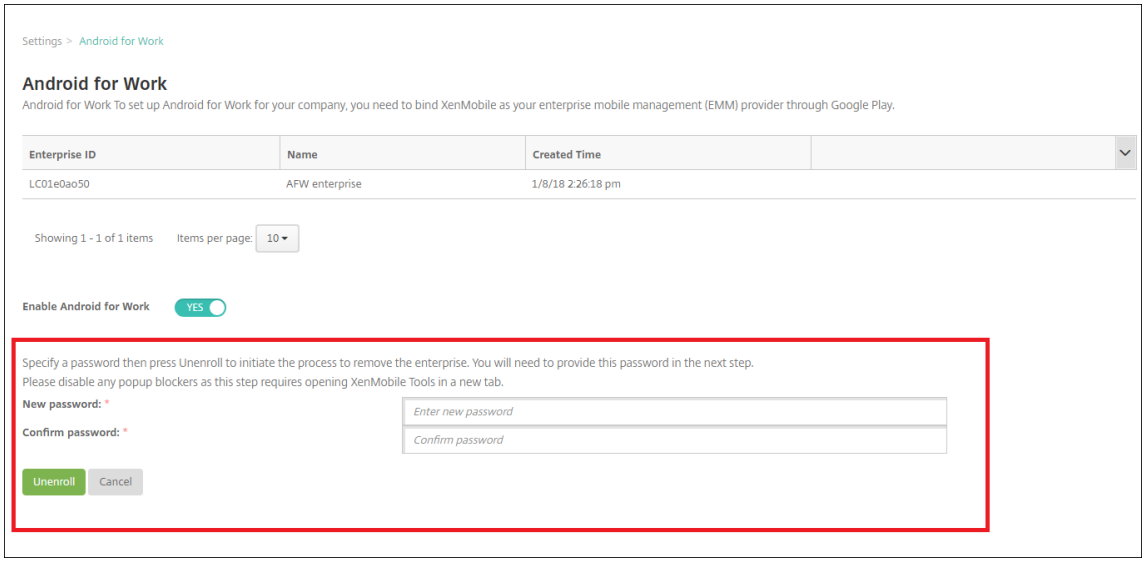
- En los dispositivos y los usuarios inscritos a través de la empresa, las aplicaciones de Android Enterprise se restablecen a sus estados predeterminados. Las directivas Permisos y Restricciones a aplicaciones de Android Enterprise aplicadas ya no tienen efecto.
- XenMobile administra los dispositivos inscritos a través de la empresa, pero se consideran no administradas desde el punto de vista de Google. No se pueden agregar nuevas aplicaciones Android Enterprise. No se pueden aplicar las directivas de Permisos ni Restricciones a las aplicaciones Android Enterprise. Sin embargo, aún se pueden aplicar otras directivas, tales como Programación, Contraseña y Restricciones, a estos dispositivos.
- Si intenta inscribir dispositivos en Android Enterprise, se inscriben como dispositivos Android, no como dispositivos Android Enterprise.

Para desinscribir una empresa de Android Enterprise

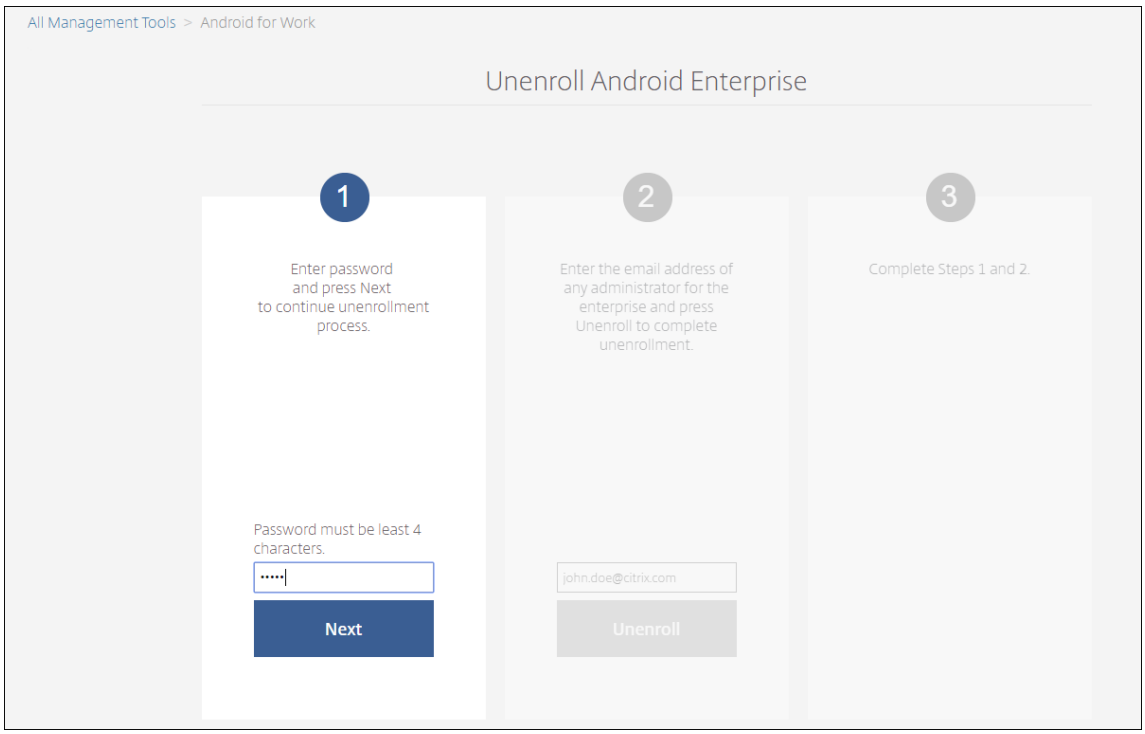
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página Parámetros.
2. En la página Parámetros, haga clic en **Android Enterprise**.
3. Haga clic en **Quitar empresa**.



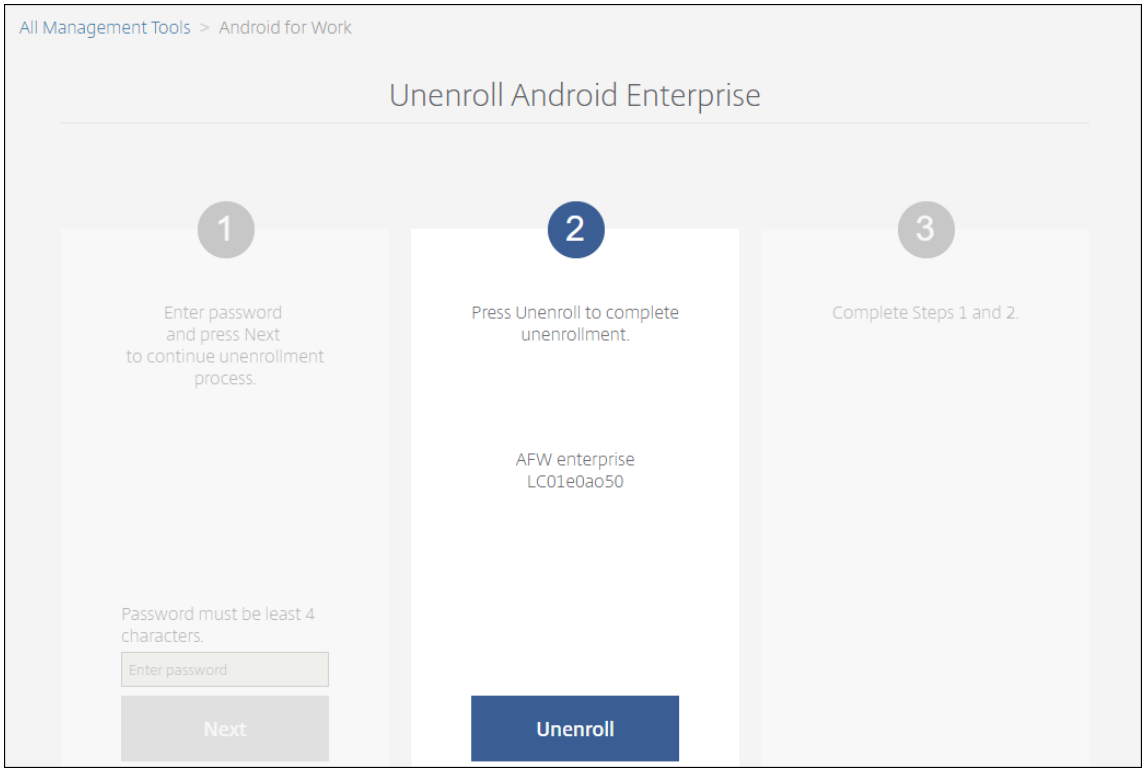
4. Especifique una contraseña. La necesitará en el próximo paso para completar la desinscripción. Haga clic en **Desinscribir**.



5. Cuando se abra la página de XenMobile Tools, introduzca la contraseña que creó en el paso anterior.



6. Haga clic en **Desinscribir**.



Aprovisionar dispositivos totalmente administrados en Android Enterprise

Solo los dispositivos propiedad de la empresa pueden ser dispositivos totalmente administrados para Android Enterprise. En dispositivos totalmente administrados, la empresa u organización controla todo el dispositivo, no solo el perfil de trabajo. Los dispositivos totalmente administrados también se conocen como dispositivos administrados de trabajo.

XenMobile admite estos métodos de inscripción para dispositivos totalmente administrados:

- **afw#xenmobile:** Con este método de inscripción, el usuario escribe los caracteres "afw#xenmobile" al configurar el dispositivo. Este token identifica el dispositivo como administrado por XenMobile y descarga Secure Hub.
- **Código QR:** El aprovisionamiento de códigos QR es una forma fácil de aprovisionar una flota distribuida de dispositivos que no admiten NFC, como las tabletas. Puede usar el método de inscripción por código QR en flotas de dispositivos que se han restablecido a sus valores de fábrica. El método de inscripción por código QR instala y configura dispositivos totalmente administrados mediante el escaneo de un código QR desde el asistente de configuración.
- **Conexión Near Field Communication (NFC):** Puede usar el método de inscripción por conexión NFC en flotas de dispositivos que se han restablecido a sus valores de fábrica. Una conexión NFC transfiere datos entre dos dispositivos por transmisión de datos en proximidad. Bluetooth, Wi-Fi y otros modos de comunicación están inhabilitados en un dispositivo que ha sido restablecido a sus valores de fábrica. NFC es el único protocolo de comunicación que el dispositivo puede utilizar en ese estado.

afw#xenmobile

El método de inscripción se usa después de encender un dispositivo nuevo o restablecido a los valores de fábrica para la configuración inicial. Los usuarios escriben "afw#xenmobile" cuando se les solicita que escriban una cuenta de Google. Esta acción descarga e instala Secure Hub. Los usuarios siguen las indicaciones de configuración de Secure Hub para completar la inscripción.

Se recomienda este método de inscripción para la mayoría de los clientes porque la versión más reciente de Secure Hub se descarga desde Google Play Store. A diferencia de otros métodos de inscripción, no es necesario proporcionar Secure Hub para descargarlo desde el servidor de XenMobile.

Requisitos previos:

- Se admite en todos los dispositivos con Android 5.0 y versiones posteriores.

Código QR

Para inscribir un dispositivo en el modo de dispositivo mediante un código QR, debe generar un código QR. Para ello, cree un JSON y conviértalo en un código QR. La cámara del dispositivo escanea el código QR para inscribir el dispositivo.

Requisitos previos:

- Se admite en todos los dispositivos con Android 7.0 y versiones posteriores.

Crear un código QR a partir de un JSON

Cree un JSON con los siguientes campos.

Estos campos son obligatorios:

Clave: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Valor: com.zenprise/com.zenprise.configuration.AdminFunction

Clave: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Valor: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Clave: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Valor: `https://path/to/securehub.apk`

> **Nota:**
>
> Si Secure Hub se carga en el servidor Citrix XenMobile como una aplicación de empresa, se puede descargar desde `https://<fqdn>:4443/*instanceName*/worxhome.apk`. Se debe poder acceder a la ruta del APK de Secure Hub a través de la conexión Wi-Fi a la que se conectará el dispositivo durante el aprovisionamiento.

Estos campos son opcionales:

- **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.

- **android.app.extra.PROVISIONING_TIME_ZONE:** La zona horaria en que se ejecuta el dispositivo.

  Introduzca un nombre Olson con el formato área/ciudad. Por ejemplo: America/Los_Angeles para la zona horaria del Pacífico en Estados Unidos. Si no introduce ninguno, la zona horaria se rellena automáticamente.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Tiempo en milisegundos desde epoch.

  El epoch de Unix (o la hora de Unix, la hora de POSIX o la marca de hora de Unix) es la cantidad de segundos que hayan transcurridos desde el 1 de enero de 1970 (medianoche UTC/GMT). En este tiempo no se cuentan los segundos intercalares (en ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** Establézcalo en **true** para omitir el cifrado durante la creación del perfil. Establezca esta opción en **false** para forzar el cifrado durante la creación del perfil.

Un archivo JSON típico es similar al siguiente:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

Valide el archivo JSON que se cree mediante una herramienta de validación JSON, como https://jsonlint.com. Convierta esa cadena JSON en un código QR mediante un generador de códigos QR en línea, como https://goqr.me.

Este código QR se escanea con un dispositivo restablecido a los valores de fábrica para inscribirlo en el modo de dispositivo administrado de trabajo.

Para inscribir el dispositivo

Para inscribir un dispositivo como un dispositivo totalmente administrado, el dispositivo debe haberse restablecido a los valores de fábrica.

1. Toque seis veces en la pantalla de bienvenida para iniciar la inscripción por código QR.
2. Cuando se le solicite, conéctese a la Wi-Fi. Se puede acceder a la ubicación de descarga que tenga establecido Secure Hub en el código QR (codificado en JSON) a través de esta red Wi-Fi.

   Una vez que el dispositivo se haya conectado a la red Wi-Fi, descarga un lector de códigos QR desde Google e inicia la cámara.
3. Apunte la cámara al código QR para escanear el código.

   Android descarga Secure Hub desde la ubicación de descarga establecida en el código QR, valida la firma del certificado de firma, instala Secure Hub y establece el modo de propietario del dispositivo.

Para obtener más información, consulte esta guía de Google para desarrolladores de Android EMM: https://developers.google.com/android/work/prov-devices#qr_code_method.

Conexión NFC

Para inscribir un dispositivo como dispositivo totalmente administrado mediante conexiones NFC, se necesitan dos dispositivos: uno que se haya restablecido a sus valores de fábrica y otro con la herramienta XenMobile Provisioning Tool.

Requisitos previos:

- Se admite en todos los dispositivos con Android 5.0, Android 5.1, Android 6.0 y versiones posteriores.
- XenMobile Server 10.4 habilitado para Android Enterprise.
- Un dispositivo nuevo o restablecido a los valores de fábrica, aprovisionado para Android Enterprise como un dispositivo totalmente administrado. 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 Enterprise, 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.

Datos transferidos a través de la conexión NFC

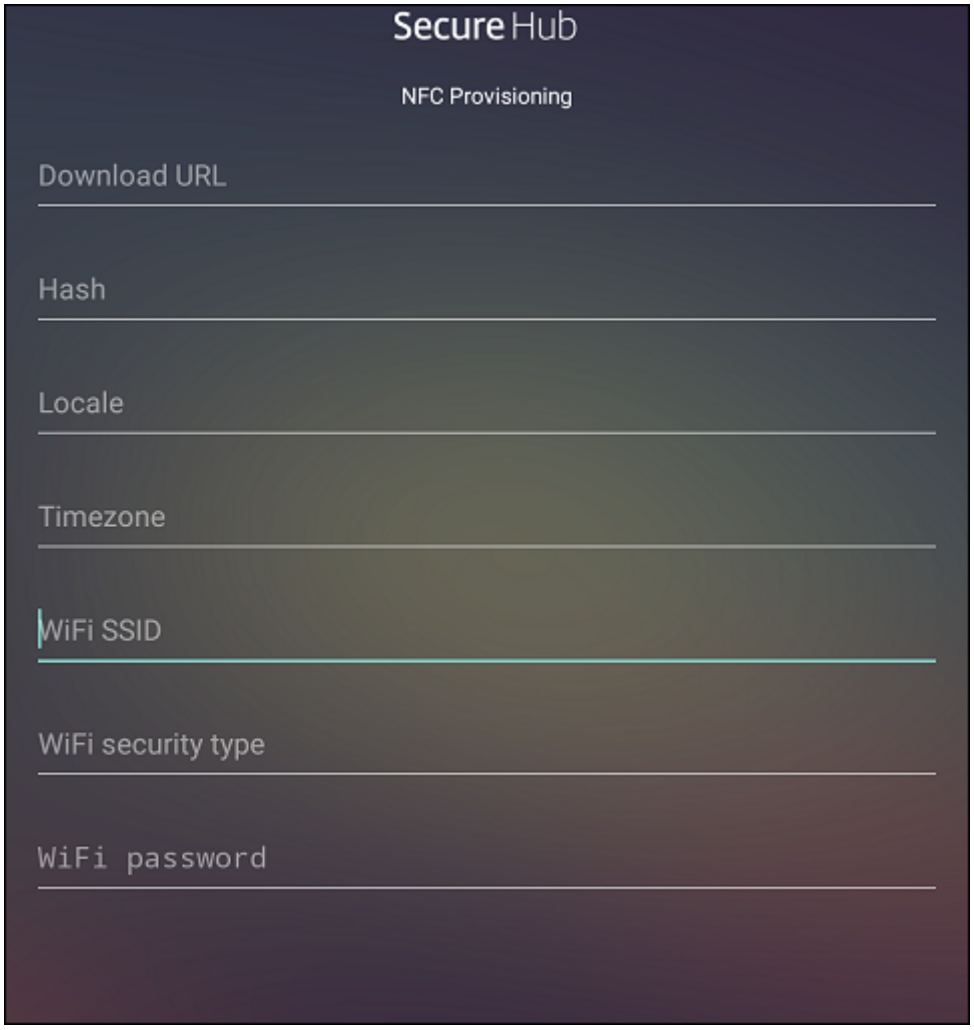
Para aprovisionar un dispositivo restablecido a sus valores de fábrica, debe enviar los siguientes datos vía una conexión NFC para inicializar Android Enterprise:

- Nombre del paquete de la aplicación de proveedor EMM que actuará como propietario del dispositivo (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 Wi-Fi 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 Wi-Fi 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 la herramienta XenMobile Provisioning Tool

Antes de una conexión NFC, es necesario configurar la herramienta Provisioning Tool. Esta configuración se transfiere, a continuación, al dispositivo restablecido a los valores de fábrica durante la conexión NFC.



Puede introducir los datos en los campos requeridos o rellenar los campos mediante un archivo de texto. En los pasos del siguiente procedimiento, se describe cómo configurar un archivo de texto que contenga descripciones para cada campo. La aplicación no guarda información una vez introducida esta, 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 /sd-card/). 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=<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 haya conectado a una red Wi-Fi por conexión NFC, el

dispositivo debe 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=<SHA1 hash>
```

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=<wifi ssid>
```

Esta línea es el SSID del dispositivo conectado por Wi-Fi donde se está ejecutando la herramienta Provisioning Tool.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

Los valores admitidos son WEP y WPA2. Si la red Wi-Fi no está protegida, este campo debe estar vacío.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

Si la red Wi-Fi no está protegida, este campo debe estar vacío.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

Introduzca 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=<timezone>
```

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=<package name>
```

Este dato no es necesario, porque el valor está codificado en la aplicación como “Secure Hub”. Se menciona aquí a título meramente informativo.

Si existe una red Wi-Fi protegida con WPA2, un archivo nfcprovisioning.txt completado puede tener el siguiente aspecto:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Cr
\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 Wi-Fi no protegida, un archivo nfcprovisioning.txt completado puede tener el siguiente aspecto:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\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 empresarial.

1. En la consola de XenMobile, vaya a **Configurar > Aplicaciones** y haga clic en **Agregar**.

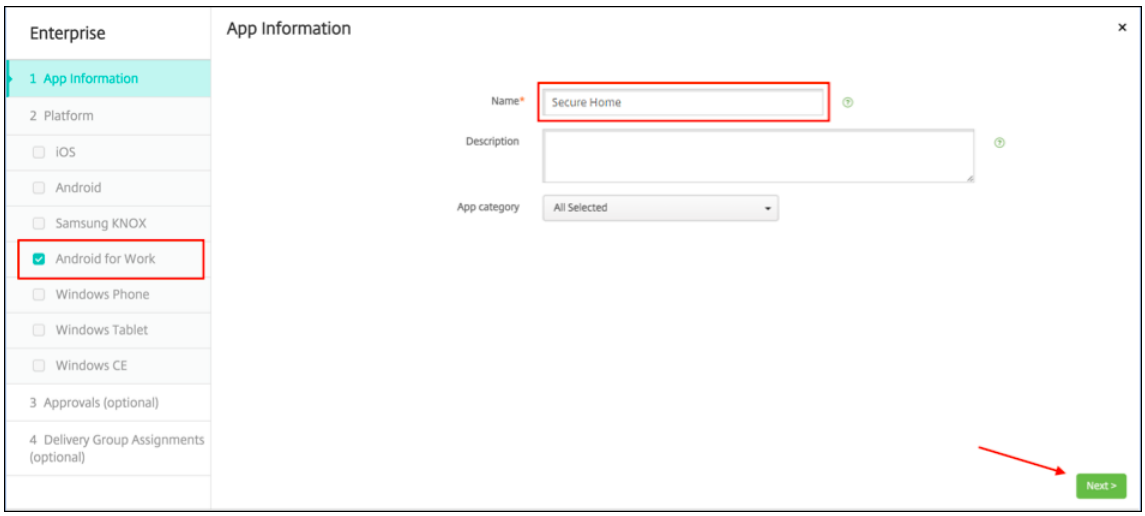
   Aparecerá la ventana **Agregar aplicaciones**.

2. Haga clic en **Empresa**.

   Aparecerá la página **Información de la aplicación**.

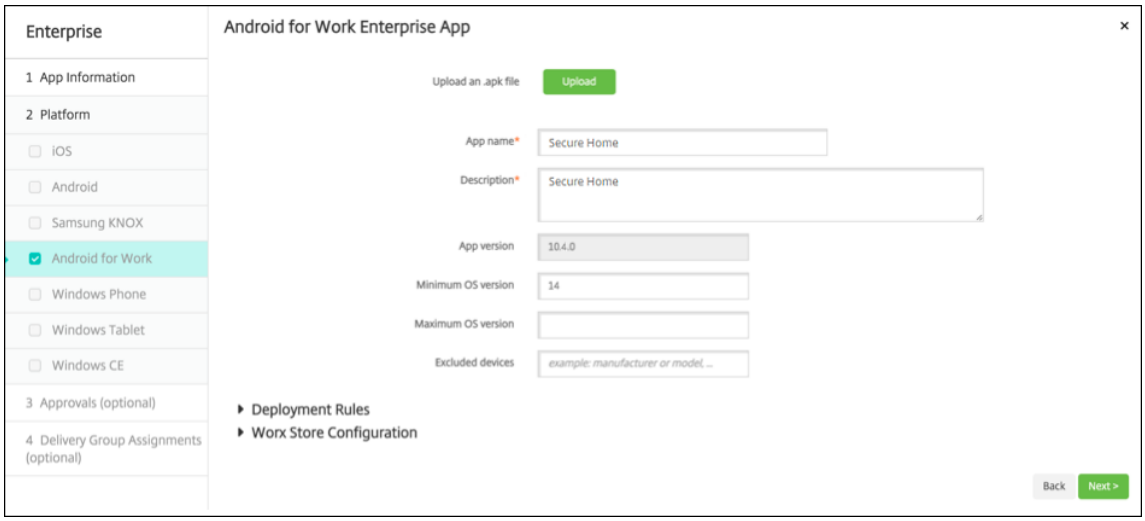
3. Seleccione la configuración siguiente y haga clic en **Siguiente**.

   Aparecerá la página **Aplicación de empresa para Android Enterprise**.



4. Facilite la ruta al archivo APK y haga clic en **Siguiente** para cargar el archivo.

   Una vez completada la carga, verá los datos del paquete cargado.



5. Haga clic en **Siguiente** para ver la página desde donde descargar el archivo JSON, que podrá utilizar para hacer cargas en Google Play. Para Secure Hub, la carga en Google Play no es obligatoria, pero necesita el archivo JSON para leer el valor SHA1 en él.

   Un archivo JSON típico es similar al siguiente:

6. Copie el valor **file_sha1_base64** y úselo en el campo **Hash** de la herramienta Provisioning Tool.

   > **Nota:**
   >
   > El hash debe contener caracteres que se puedan usar en las URL.

   - Convierta todos los símbolos **+** a **-**.
   - Convierta los símbolos **/** a **_**.
   - Reemplace **\u003d** 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 appcompat v7, biblioteca Design support y biblioteca Palette v7 de Google bajo la licencia de Apache 2.0

  Para obtener información, consulte Support Library Features Guide.

- Butter Knife de Jake Wharton bajo la licencia de Apache 2.0

Aprovisionar dispositivos de perfil de trabajo en Android Enterprise

En los dispositivos de perfil de trabajo de Android Enterprise, las áreas corporativas y personales de un dispositivo se separan de forma segura. Por ejemplo, los dispositivos BYOD pueden ser dispositivos de perfil de trabajo. La experiencia de inscripción para los dispositivos de perfil de trabajo es similar a la inscripción de Android en XenMobile. Los usuarios descargan Secure Hub desde Google Play e inscriben sus dispositivos.

De forma predeterminada, los parámetros de depuración por USB y fuentes desconocidas están inhabilitados en los dispositivos cuando estos se inscriben en Android Enterprise como dispositivos de perfil de trabajo.

> **Sugerencia:**
>
> Cuando inscriba dispositivos en Android Enterprise como dispositivos de perfil de trabajo, vaya siempre a Google Play. Desde allí, habilite Secure Hub para que aparezca en el perfil personal del usuario.

iOS

January 4, 2022

Para administrar dispositivos iOS en XenMobile Server, debe configurar un certificado del servicio de notificaciones push de Apple (APNs) proveniente de Apple. Para obtener información, consulte Certificados APNs.

Los perfiles de inscripción determinan si los dispositivos iOS se inscriben en MDM+MAM, con la posibilidad de que los usuarios se excluyan de MDM. XenMobile Server admite los siguientes tipos de aut-

enticación para dispositivos iOS en MDM+MAM. Para obtener más información, consulte los artículos de Certificados y autenticación.

- Dominio
- Dominio y token de seguridad
- Certificado del cliente
- Certificado de cliente y dominio

> **Requisitos para certificados de confianza en iOS 13:**
>
> Apple tiene nuevos requisitos para certificados de servidor TLS. Verifique que todos los certificados cumplen los nuevos requisitos de Apple. Consulte la publicación de Apple: https://support.apple.com/en-us/HT210176. Para obtener ayuda sobre la administración de certificados, consulte Cargar certificados en XenMobile Server.

Para conocer los sistemas operativos admitidos, consulte Sistemas operativos admitidos.

Compatibilidad con iOS 14

Las aplicaciones móviles de XenMobile Server y Citrix son compatibles con iOS 14, pero no son compatibles actualmente con las nuevas funcionalidades de iOS 14.

En el caso de los dispositivos iOS supervisados, puede demorar las actualizaciones de software hasta 90 días. En la directiva Restricciones para iOS, use estos parámetros:

- **Forzar demora de actualizaciones de software**
- **Demora forzosa para actualizaciones de software**

Consulte Parámetros de iOS. Esos parámetros no están disponibles para dispositivos en modo de inscripción de usuarios ni en modo no supervisado (MDM completo).

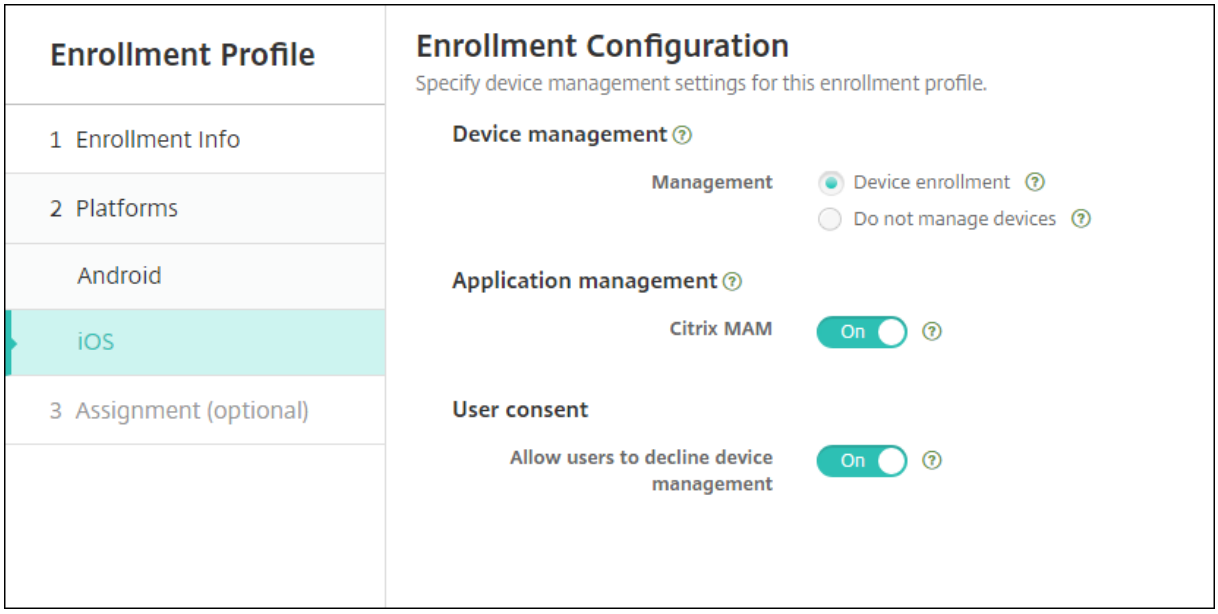
Nombres de host de Apple que deben permanecer abiertos

Algunos nombres de host de Apple deben permanecer abiertos para garantizar el correcto funcionamiento de iOS, macOS y el App Store. Bloquear dichos nombres de host puede afectar a la instalación, la actualización y el funcionamiento correcto de iOS, aplicaciones iOS, el funcionamiento de MDM y la inscripción de dispositivos y aplicaciones. Para obtener más información, consulte https://support.apple.com/en-us/HT201999.

Métodos de inscripción admitidos

La manera de administrar los dispositivos iOS se especifica en los perfiles de inscripción. Puede elegir inscripción de dispositivos o inscripción no MDM.

Para configurar los parámetros de inscripción de dispositivos iOS, vaya a **Configurar > Perfiles de inscripción > iOS**.



En la siguiente tabla, se indican los métodos de inscripción que XenMobile Server admite para dispositivos iOS:

Método	¿Se admite?
Programa de implementación de Apple	Sí
Apple School Manager	Sí
Apple Configurator	Sí
Inscripción manual	Sí
Invitaciones de inscripción	Sí

Apple dispone de programas de inscripción de dispositivos para las cuentas Empresas y Educación. Para las cuentas Business, debe inscribirse en el Programa de implementación de Apple para inscribir y administrar dispositivos en XenMobile Server. Ese programa es para dispositivos iOS y macOS. Consulte Implementar dispositivos mediante el Programa de implementación de Apple.

Para las cuentas Educación, cree una cuenta de Apple School Manager. Apple School Manager unifica el programa de implementación y las compras por volumen. Apple School Manager es un tipo de Programa de implementación de Apple Educación. Consulte Integrar en funciones de Apple Educación.

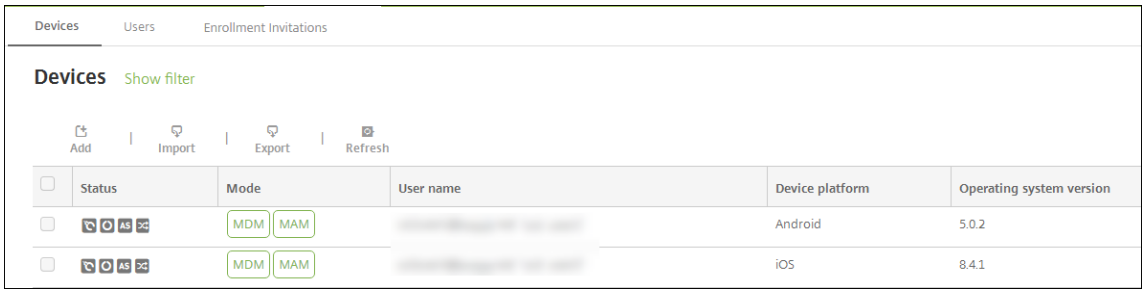
Puede utilizar el Programa de implementación de Apple para inscribir en bloque dispositivos iOS y macOS. Puede comprar esos dispositivos directamente de Apple, un distribuidor autorizado de Apple o un proveedor. Puede usar Apple Configurator para inscribir dispositivos iOS tanto si los adquirió

directamente de Apple como si no. Consulte Inscribir en bloque dispositivos Apple.

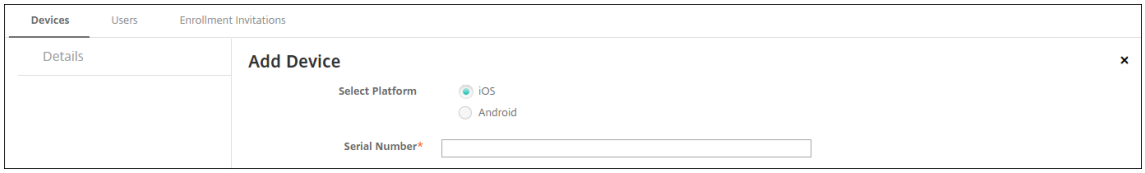
Agregar manualmente un dispositivo iOS

Si quiere agregar manualmente un dispositivo iOS (por ejemplo, para probarlo), siga estos pasos.

1. En la consola de XenMobile Server, haga clic en **Administrar > Dispositivos**. Aparecerá la página **Dispositivos**.



2. Haga clic en **Agregar**. Aparecerá la página **Agregar dispositivo**.



3. Configure estos parámetros:

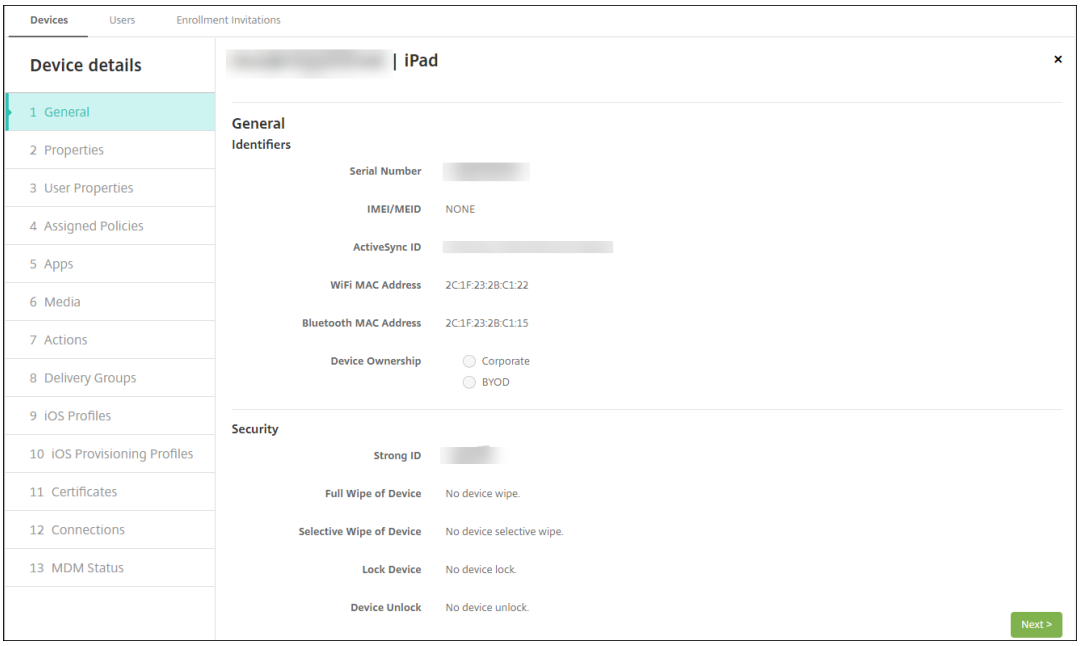
   - **Seleccione la plataforma:** Haga clic en **iOS**.
   - **Número de serie:** Escriba el número de serie del dispositivo.

4. Haga clic en **Agregar**. La tabla **Dispositivos** aparecerá con el dispositivo agregado al final de la lista. Seleccione el dispositivo agregado y, a continuación, en el menú que aparecerá, haga clic en **Modificar** para ver y confirmar los detalles del dispositivo.

   > **Nota:**
   >
   > Cuando se marca la casilla situada junto a un dispositivo, el menú de opciones aparece encima de la lista de dispositivos. Si hace clic en cualquier lugar de la lista, el menú de opciones aparece a la derecha de la lista.

   - LDAP configurado
   - Si utiliza grupos y usuarios locales:
     - Uno o varios grupos locales.
     - Usuarios locales asignados a grupos locales.
     - Los grupos de entrega se asocian con grupos locales.
   - Si usa Active Directory:

- Los grupos de entrega se asocian con grupos de Active Directory.



5. En la página **General** se muestra una lista de los **identificadores** de dispositivo, como el número de serie y otra información en función del tipo de plataforma. Para **Propietario del dispositivo**, seleccione **Empresa** 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. El campo **Borrado completo del dispositivo** contiene el código PIN del usuario. El usuario debe introducir ese código después de que se haya borrado el dispositivo. Si el usuario no consigue recordar el código, usted puede buscarlo en “Detalles del dispositivo”.

6. La página **Propiedades** muestra una lista de las propiedades de dispositivo que aprovisionará XenMobile Server. 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 **Agregar** y, a continuación, seleccione una propiedad de la lista. Para saber cuáles son los valores válidos para cada propiedad, consulte el PDF Valores y nombres de propiedades de dispositivo.

   Cuando se agrega una propiedad, esta aparece inicialmente en la categoría donde se haya agregado. Después de hacer clic en **Siguiente** y volver a la página **Propiedades**, 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 Server elimina inmediatamente el elemento.

7. Las secciones restantes de **Detalles del dispositivo** contienen información resumida acerca del

dispositivo.

- **Propiedades de usuario:** Muestra los roles de RBAC, los miembros del grupo, las cuentas de compras por volumen y las propiedades del usuario. Puede retirar una cuenta de compras por volumen desde esta página.
- **Directivas asignadas:** Muestra la cantidad de directivas asignadas, incluidas las directivas implementadas, pendientes y fallidas. También muestra el nombre, el tipo y la última información implementada de cada directiva.
- **Aplicaciones:** Muestra la cantidad de implementaciones de aplicaciones instaladas, pendientes y erróneas según el último inventario. Indica el nombre de la aplicación, el identificador y el tipo, entre otros datos. Para obtener una descripción de las claves de inventario de iOS y macOS, como **HasUpdateAvailable**, consulte Mobile Device Management (MDM) Protocol.
- **Multimedia:** Muestra la cantidad de implementaciones de archivos multimedia instalados, pendientes y erróneos según el último inventario.
- **Acciones:** Muestra la cantidad de acciones implementadas, pendientes y erróneas. Indica el nombre de la acción y la hora de la última implementación.
- **Grupos de entrega:** Muestra la cantidad de grupos de entrega en estado correcto, pendiente y fallido. 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).
- **Perfiles iOS:** Muestra el último inventario de perfiles iOS, que incluye el nombre, el tipo, la organización y la descripción.
- **Perfiles de datos de iOS:** Muestra información acerca del perfil de datos utilizado por la empresa para la distribución (como el UUID, la fecha de caducidad y si se administra o no).
- **Certificados:** 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.
- **Conexiones:** 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).
- **Estado de MDM:** Muestra información como el estado MDM, la hora del último envío push y la hora de la última respuesta del dispositivo.

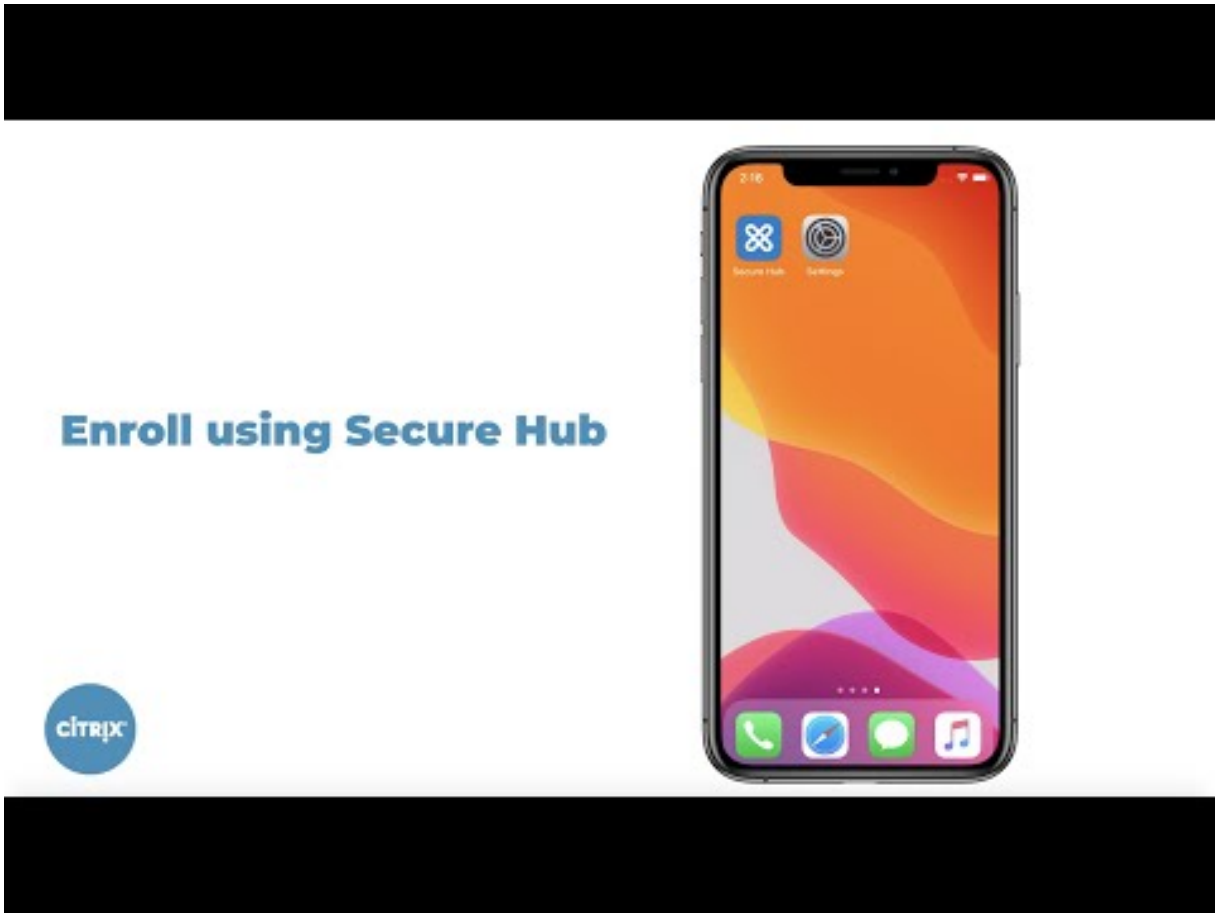
Configurar directivas para dispositivos iOS

Use estas directivas para configurar cómo interactúa XenMobile Server con los dispositivos iOS. En esta tabla se indican todas las directivas de dispositivo disponibles para dispositivos iOS.

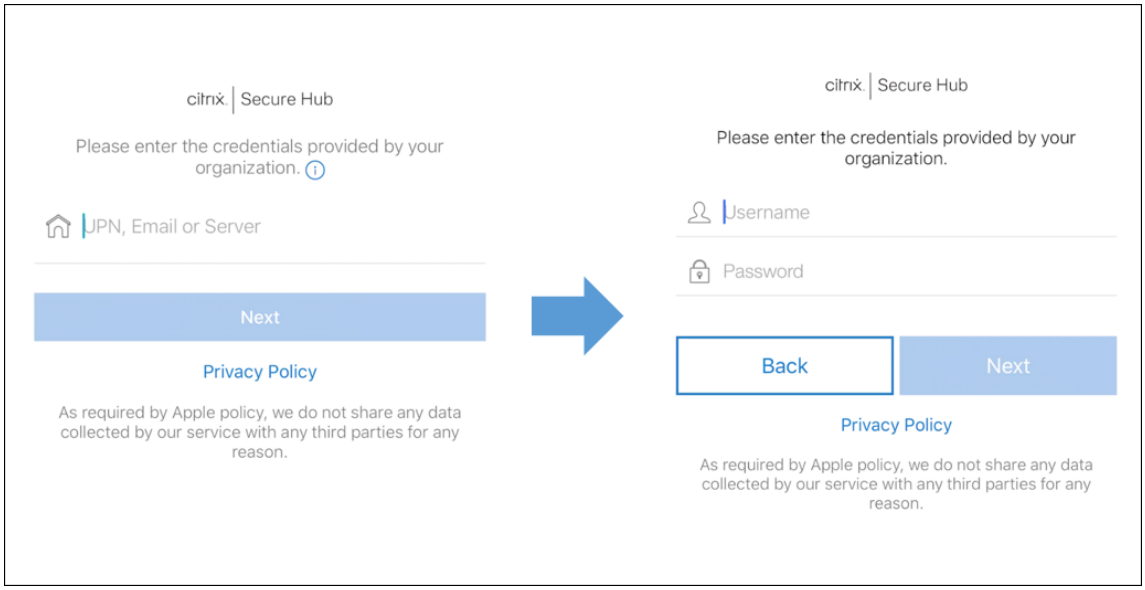
Duplicación AirPlay	AirPrint	APN
Acceso a aplicaciones	Atributos de aplicación	Configuración de aplicaciones
Inventario de aplicaciones	Bloqueo de aplicaciones	Uso de red de las aplicaciones
Desinstalación de aplicaciones	Notificaciones de aplicaciones	Calendario (CalDAV)
Móvil	Contactos (CardDAV)	Controlar actualización del SO
Credenciales	Nombre del dispositivo	Configuración de la educación
Exchange	Fuente	Diseño de pantalla inicial
Importar perfil de iOS y macOS	LDAP	Ubicación
Correo	Dominios administrados	Opciones de MDM
Información sobre la organización	Código de acceso	Hotspot personal
Eliminación de perfiles	Perfil de datos	Eliminación de perfiles de datos
Proxy	Restricciones	Itinerancia
SCEP	iPad compartido: Máximo de usuarios residentes	iPad compartido: Período de gracia de bloqueo de código de acceso
Cuenta SSO	Almacén	Calendarios suscritos
Términos y condiciones	VPN	Wallpaper
Filtro de contenido web	Clip web	Wi-Fi

Inscribir dispositivos iOS

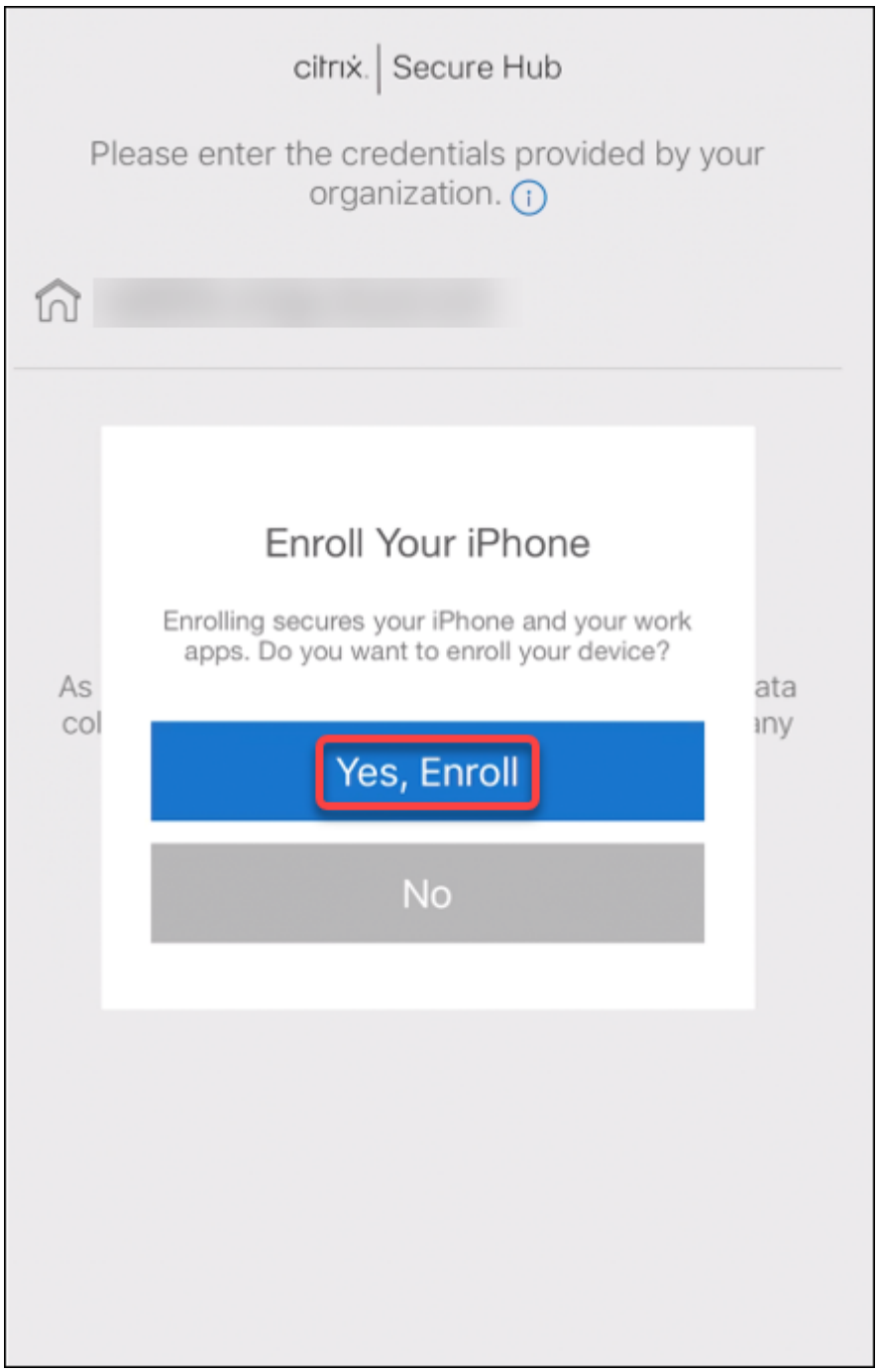
En esta sección se muestra cómo los usuarios inscriben dispositivos iOS (12.2 o una versión posterior) en XenMobile Server. Para obtener más información sobre la inscripción en iOS, abra el siguiente vídeo:



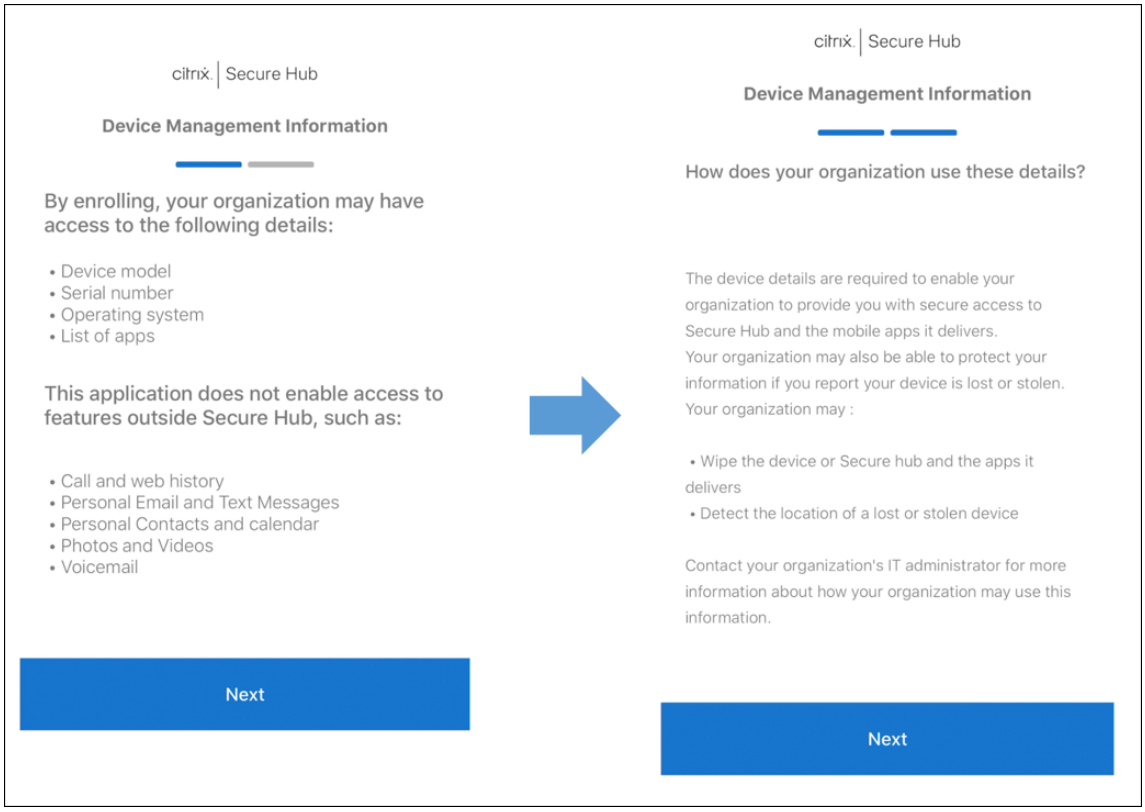
1. Vaya a la tienda Apple en su dispositivo iOS, descargue la aplicación Citrix Secure Hub y, a continuación, toque la aplicación.
2. Cuando se le pida instalar la aplicación, toque **Siguiente** y, a continuación, **Instalar**.
3. Después de que Secure Hub se instale, toque **Abrir**.
4. Introduzca las credenciales de empresa, como el nombre del servidor de XenMobile Server de su empresa, el nombre principal de usuario (UPN) o su dirección de correo electrónico. A continuación, haga clic en **Siguiente**.



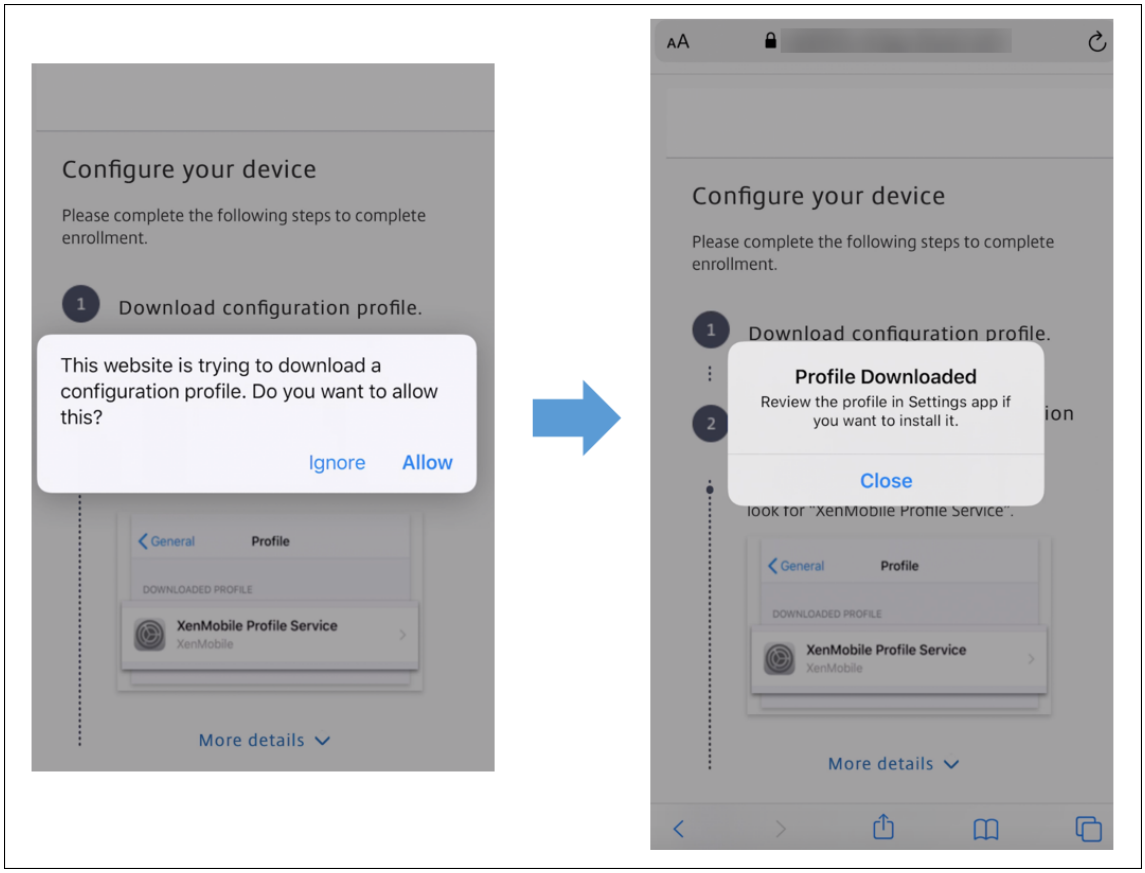
5. Toque **Sí, inscribirlo** para inscribir el dispositivo iOS.



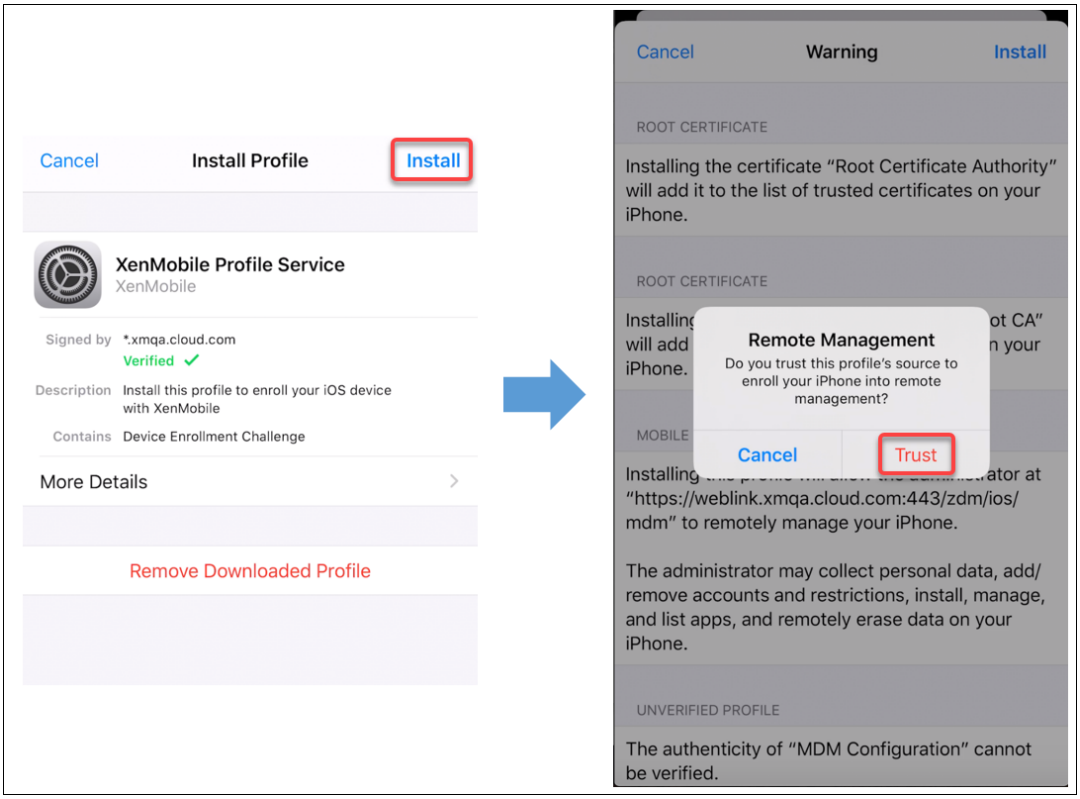
6. Aparecerá una lista de los datos que XenMobile Server recopila. Haga clic en **Siguiente**. Aparecerá una explicación del modo en que una organización utiliza esos datos. Haga clic en **Siguiente**.



7. Después de escribir las credenciales, toque **Permitir** cuando se le pida para descargar el perfil de configuración. Después de descargar el perfil de configuración, toque **Cerrar**.



8. En la configuración del dispositivo, instale el certificado de iOS y agregue el dispositivo a la lista de confianza.
   - Vaya a **Configuración > General > Perfil > XenMobile Profile Service** y toque **Instalar** para agregar el perfil.
   - En la ventana de notificaciones, toque **Confiar** para inscribir el dispositivo en la administración remota.



9. Una vez hecha correctamente la inscripción, abra Secure Hub. Si inscribe dispositivos en MDM+MAM: Una vez que se hayan validado las credenciales, cree el PIN de Citrix y confírmelo cuando se le solicite.
10. Una vez completado el flujo de trabajo, el dispositivo está inscrito. Ahora, puede acceder al almacén de aplicaciones para ver las aplicaciones que puede instalar en el dispositivo iOS.

Acciones de seguridad

iOS admite las siguientes acciones de seguridad. Para ver una descripción de cada acción de seguridad, consulte Acciones de seguridad.

Omisión del bloqueo de activación	Bloqueo de aplicaciones	Borrado de aplicaciones
Bloqueo de activación de ASM	Renovación de certificados	Desactivar restricciones
Habilitar o inhabilitar el modo perdido	Habilitar o inhabilitar el seguimiento	Borrado completo
Localizar	Bloquear	Hacer sonar
Solicitar o detener la duplicación AirPlay	Reiniciar o apagar	Revocar o autorizar

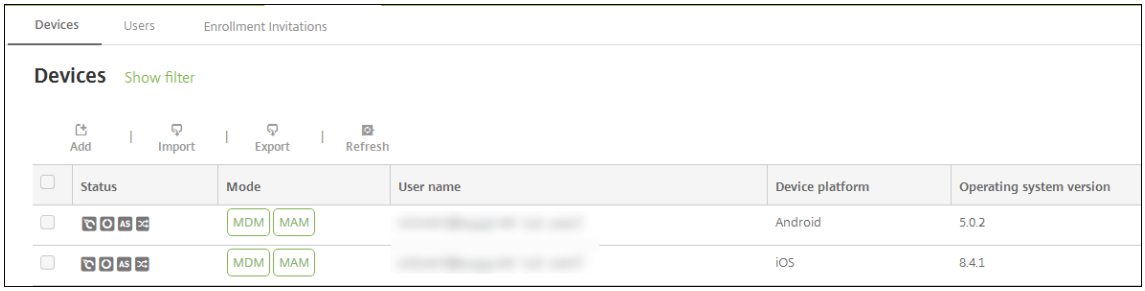
Borrado selectivo	Desbloquear

Bloquear dispositivos iOS

Puede bloquear un dispositivo iOS perdido y mostrar un mensaje y un número de teléfono en la pantalla de bloqueo.

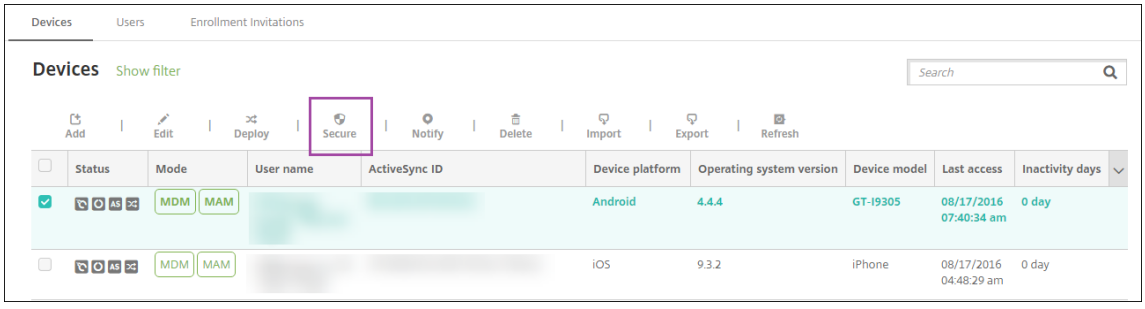
Para que se muestren un mensaje y un teléfono en un dispositivo bloqueado, establezca la directiva Código de acceso en **true** en la consola de XenMobile Server. De forma alternativa, los usuarios pueden habilitar manualmente el código de acceso en el dispositivo.

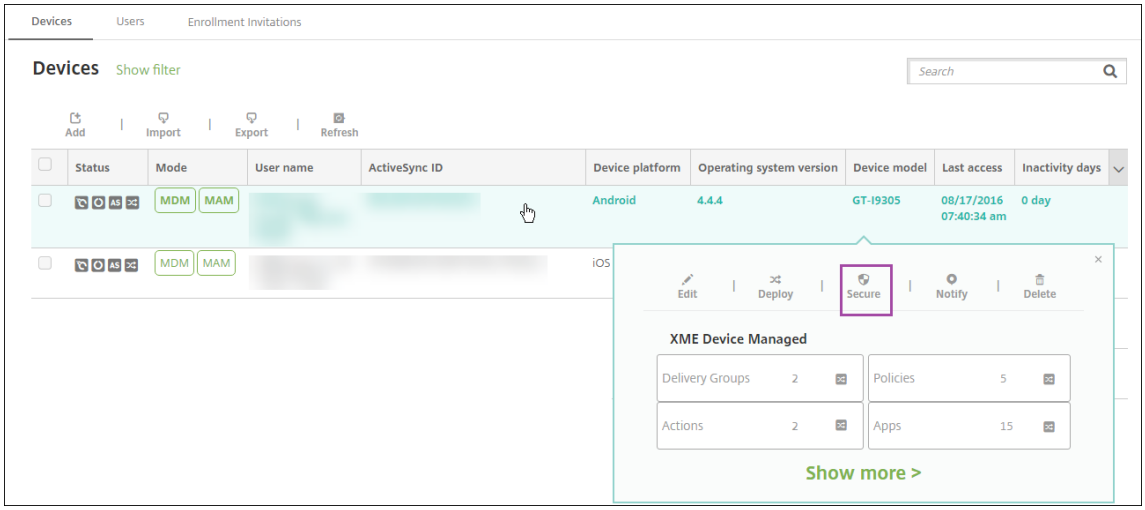
1. Haga clic en **Administrar > Dispositivos**. Aparecerá la página **Dispositivos**.



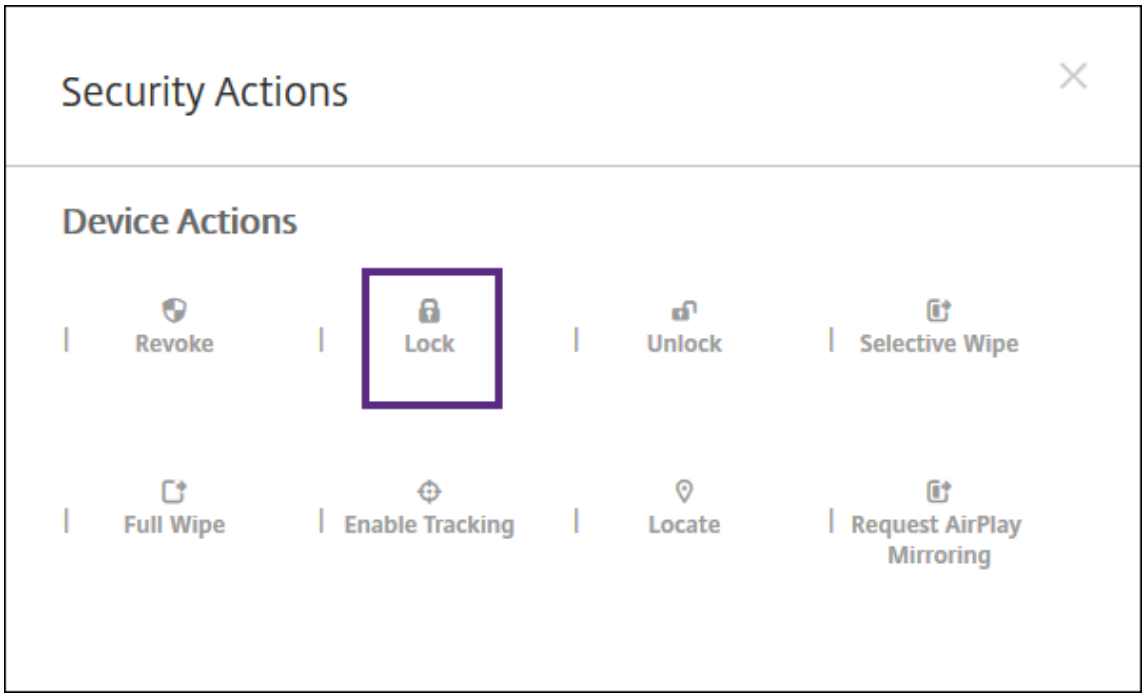
2. Seleccione el dispositivo iOS que quiere bloquear.

   Marque la casilla situada junto a un dispositivo para que el menú de opciones aparezca encima de la lista de dispositivos. Haga clic en cualquier lugar de la lista para que el menú de opciones aparezca a la derecha de la lista.

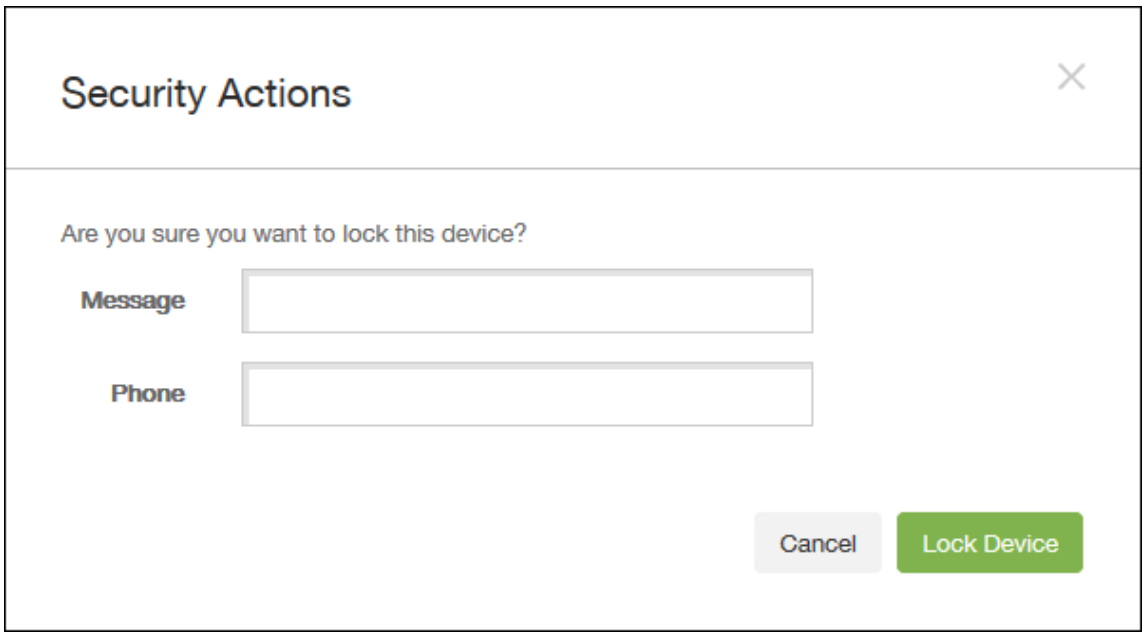




3. En el menú de opciones, seleccione **Proteger**. Aparecerá el cuadro de diálogo **Acciones de seguridad**.



4. Haga clic en **Bloquear**. Aparecerá el cuadro de confirmación **Acciones de seguridad**.



5. Si lo prefiere, puede introducir el mensaje y el número de teléfono que aparecerán en la pantalla de bloqueo del dispositivo.

   iOS agrega las palabras “iPad perdido” a lo que escriba en el campo **Mensaje**.

   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.

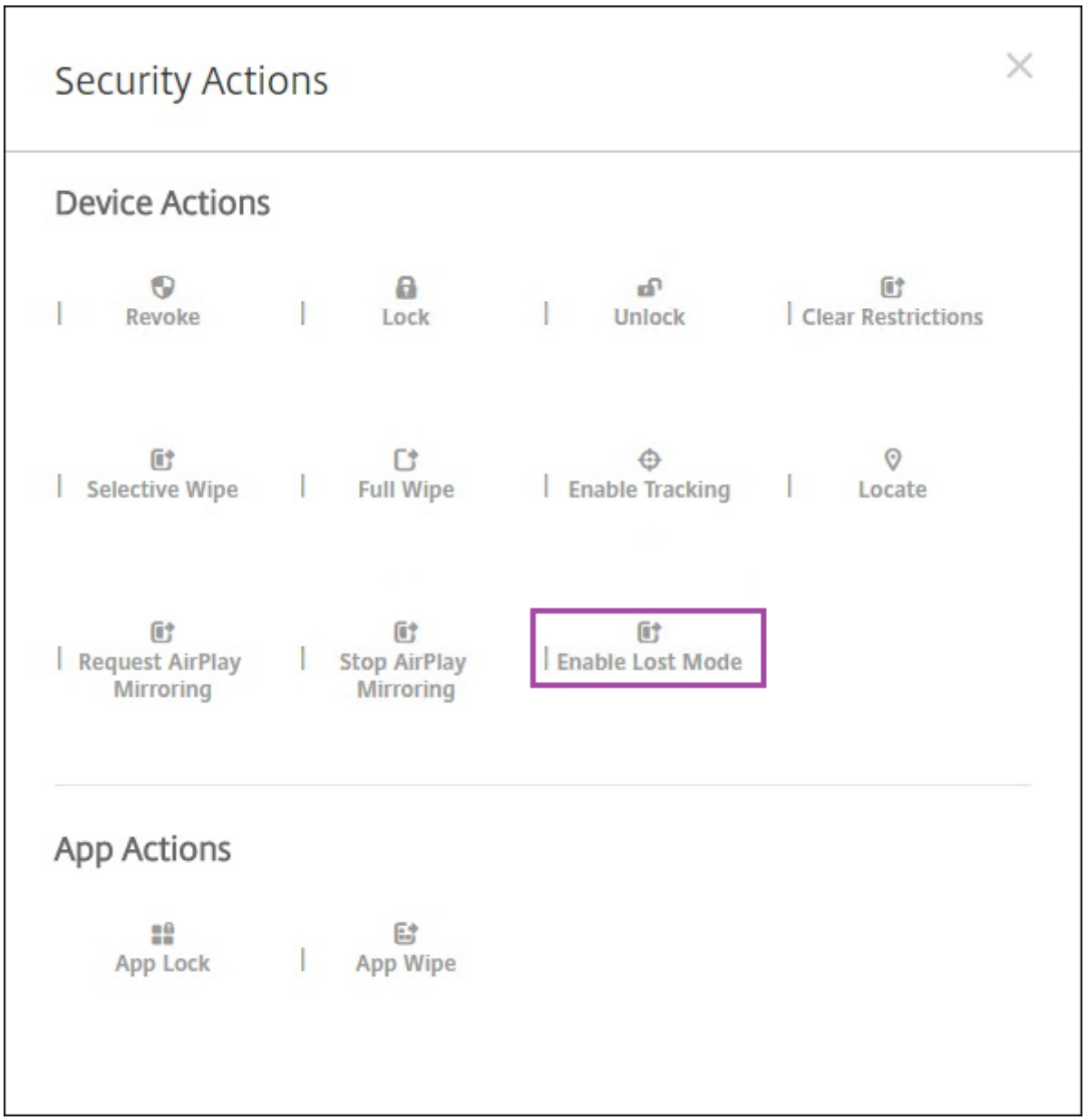
6. Haga clic en **Bloquear dispositivo**.

Colocar dispositivos iOS en modo perdido

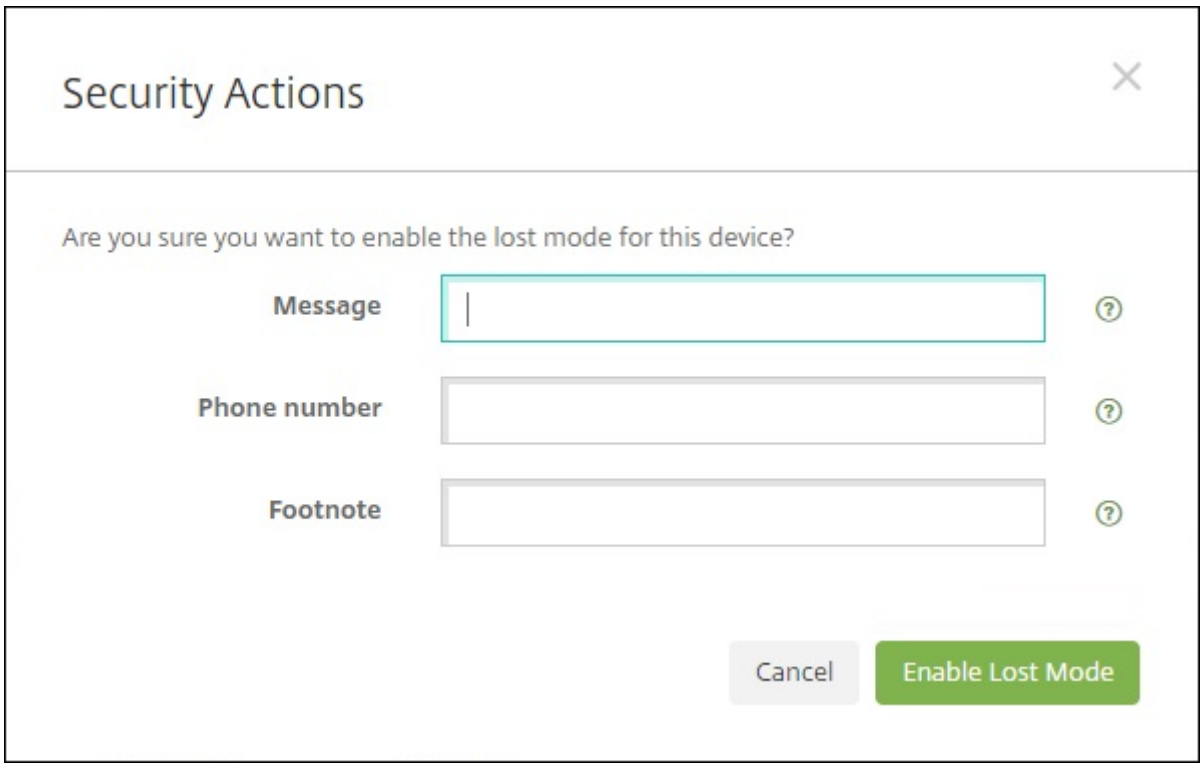
La propiedad de dispositivo “modo perdido” de XenMobile Server coloca un dispositivo iOS en el modo Perdido (de Apple). A diferencia del modo Perdido gestionado de Apple, el modo perdido de XenMobile Server no requiere que el usuario configure **Buscar mi iPhone o iPad** ni habilite los servicios de localización geográfica de Citrix Secure Hub para permitir la localización de su dispositivo.

En el modo perdido de XenMobile Server, solo XenMobile Server puede desbloquear el dispositivo. (En cambio, si usa la función de bloqueo del dispositivo de XenMobile Server, los usuarios pueden desbloquear el dispositivo directamente con un código PIN que proporcione.)

Para habilitar o inhabilitar el modo perdido, vaya a **Administrar > Dispositivos**, elija un dispositivo iOS supervisado y haga clic en **Proteger**. A continuación, haga clic en **Habilitar modo perdido** o **Inhabilitar modo perdido**.

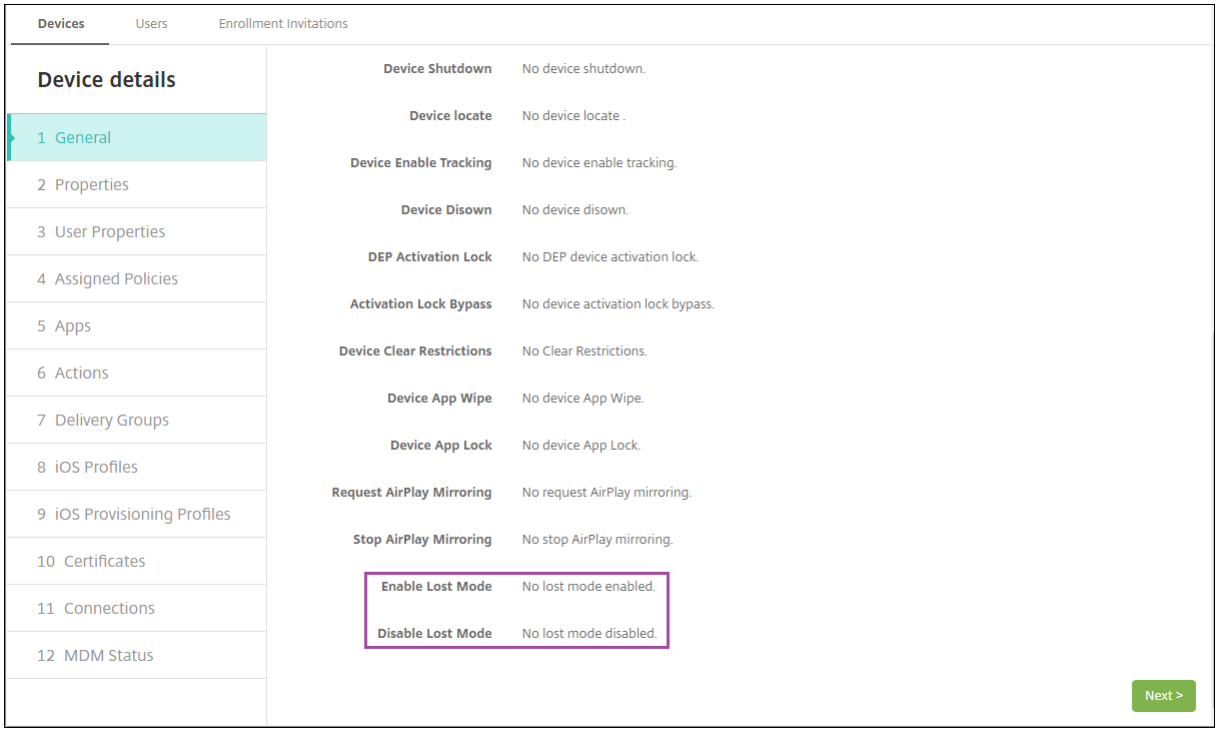


Si hace clic en **Habilitar modo perdido**, escriba la información que aparecerá en el dispositivo cuando esté en el modo perdido.

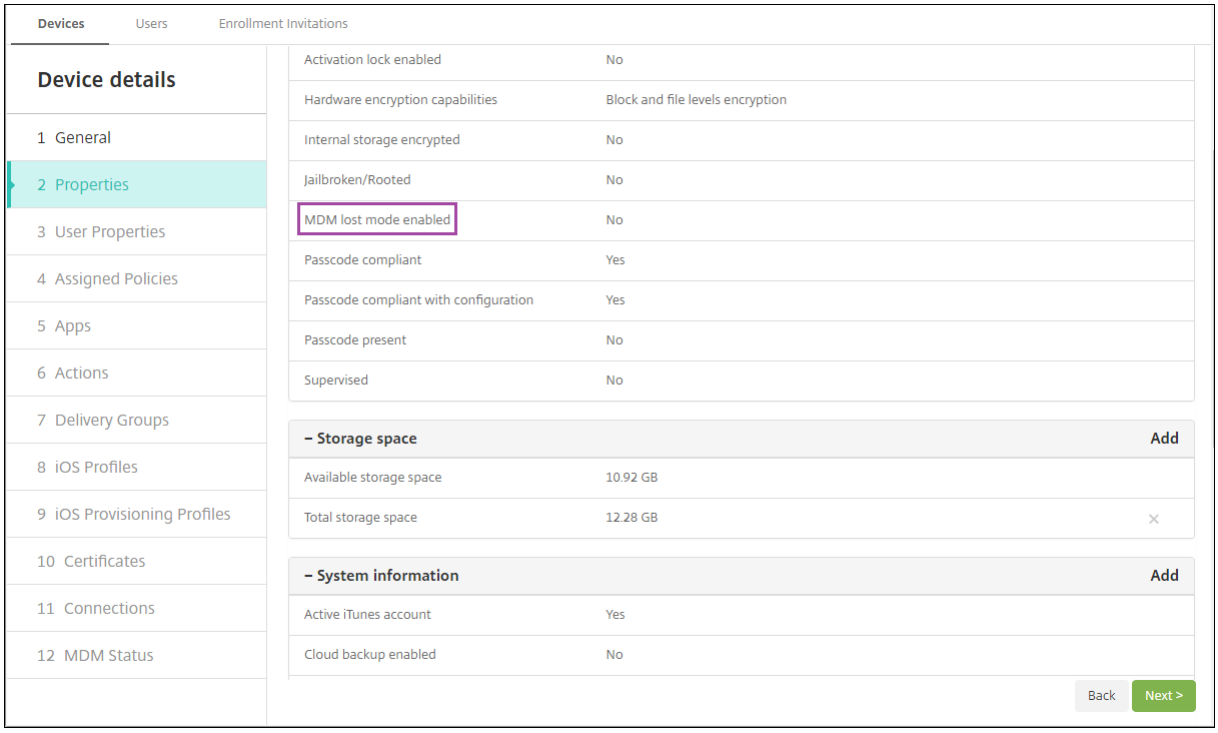


Para comprobar el estado del modo perdido, utilice cualquiera de los siguientes métodos:

- En la ventana **Acciones de seguridad**, compruebe si el botón es **Inhabilitar modo perdido**.
- Desde **Administrar > Dispositivos**, en la ficha **General**, en **Seguridad**, consulte la última acción de “Habilitar modo perdido” o “Inhabilitar modo perdido”.



- Desde **Administrar > Dispositivos**, en la ficha **Propiedades**, compruebe que el valor del parámetro **Modo perdido de MDM habilitado** es correcto.



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

- En **Configurar > Acciones**, la lista **Acciones** no incluye las siguientes acciones automatizadas: **Revocar el dispositivo**, **Borrar datos selectivamente del dispositivo** ni **Borrar datos completamente del dispositivo**.
- En **Administrar > Dispositivos**, la lista **Acciones de seguridad** ya no incluye las acciones de dispositivo **Revocar** ni **Borrado selectivo**. En cambio, puede llevar a cabo un **Borrado completo**, si fuera necesario.

iOS agrega las palabras “iPad perdido” a lo que escriba en el campo **Mensaje** de la pantalla **Acciones de seguridad**.

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.

Omitir un bloqueo de activación de iOS

El bloqueo de activación es una función de Buscar mi iPhone o iPad que evita la reactivación de un dispositivo supervisado que se haya perdido o haya sido robado. El bloqueo de activación requiere el ID de Apple del usuario y la contraseña para desactivar Buscar mi iPhone o iPad, borrar el dispositivo o volver a activarlo. Para los dispositivos propiedad de la organización, es necesario omitir un bloqueo

de activación para, por ejemplo, restablecer o reasignar dispositivos.

Para habilitar el bloqueo de activación, debe configurar e implementar la directiva de opciones MDM de XenMobile Server. A continuación, puede administrar un dispositivo desde la consola de XenMobile Server sin las credenciales de Apple del usuario. Para omitir el requisito de credenciales de Apple en un bloqueo de activación, debe emitir la acción de seguridad "Omisión del bloqueo de activación" desde la consola de XenMobile Server.

Por ejemplo, si un usuario devuelve un teléfono perdido o si usted quiere configurar uno antes o después de un borrado completo, cuando el teléfono le solicite las credenciales de la cuenta del App Store de Apple, puede omitir ese paso emitiendo la acción de seguridad "Omisión del bloqueo de activación" desde la consola de XenMobile Server.

Requisitos del dispositivo para la omisión del bloqueo de activación

- Supervisado a través de Apple Configurator o del Programa de implementación de Apple
- Configurado con una cuenta de iCloud
- Buscar mi iPhone o iPad habilitado
- Inscrito en XenMobile Server
- La directiva de opciones de MDM, con el bloqueo de activación habilitado, implementada en los dispositivos

Para omitir un bloqueo de activación antes de emitir el borrado completo de un dispositivo:

1. Vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Proteger** y, a continuación, haga clic en **Omisión del bloqueo de activación**.
2. Borre los datos del dispositivo. La pantalla del bloqueo de activación no aparece durante la configuración del dispositivo.

Para omitir un bloqueo de activación después de emitir el borrado completo de un dispositivo:

1. Borre los datos del dispositivo o restablézcalo. La pantalla del bloqueo de activación aparece durante la configuración del dispositivo.
2. Vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Proteger** y, a continuación, haga clic en **Omisión del bloqueo de activación**.
3. Toque el botón Atrás del dispositivo. Aparecerá la pantalla de inicio.

Tenga en cuenta lo siguiente:

- Recomiende a los usuarios que no desactiven Buscar mi iPhone o iPad. No realice ningún borrado completo desde el dispositivo. En cualquiera de estos casos, se pide al usuario que escriba la contraseña de la cuenta de iCloud. Tras validar la cuenta, el usuario no verá la pantalla "Activar iPhone o iPad" después de borrar todo el contenido y toda la configuración.
- Para un dispositivo con un código de omisión del bloqueo de activación generado y con el bloqueo de activación habilitado: si no puede omitir la página "Activar iPhone o iPad" después

de un borrado completo, no es necesario eliminar el dispositivo de XenMobile Server. Usted o el usuario pueden ponerse en contacto con la asistencia técnica de Apple para desbloquear el dispositivo directamente.

- Durante un inventario de hardware, XenMobile Server busca en el dispositivo un código de omisión del bloqueo de activación. Si hay disponible un código de omisión, el dispositivo lo envía a XenMobile Server. A continuación, para quitar ese código de omisión del dispositivo, envíe la acción de seguridad "Omisión del bloqueo de activación" desde la consola de XenMobile Server. En ese momento, XenMobile Server y Apple tienen el código de omisión requerido para desbloquear el dispositivo.
- La acción de seguridad "Omisión del bloqueo de activación" necesita la disponibilidad de un servicio de Apple. Si la acción no funciona, puede desbloquear un dispositivo como se indica a continuación. En el dispositivo, debe introducir manualmente las credenciales de la cuenta iCloud. O bien deje en blanco el campo del nombre de usuario y escriba el código de omisión en el campo de la contraseña. Para buscar el código de omisión, vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Modificar** > **Propiedades**. El **Código de omisión del bloqueo de activación** se encuentra en el apartado **Información de seguridad**.

macOS

January 4, 2022

Para administrar dispositivos macOS en XenMobile, debe configurar un certificado del servicio de notificaciones push de Apple (APNs) proveniente de Apple. Para obtener información, consulte Certificados APNs.

XenMobile inscribe los dispositivos macOS en MDM. XenMobile admite los siguientes tipos de autenticación de inscripción para dispositivos macOS en MDM.

- Dominio
- Dominio y contraseña de un solo uso
- URL de invitación y contraseña de un solo uso

> **Requisitos para certificados de confianza en macOS 15:**
>
> Apple tiene nuevos requisitos para certificados de servidor TLS. Verifique que todos los certificados cumplen los nuevos requisitos de Apple. Consulte la publicación de Apple: https://support.apple.com/en-us/HT210176. Para obtener ayuda sobre la administración de certificados, consulte Cargar certificados en XenMobile.

Un flujo de trabajo general para iniciar la administración de dispositivos macOS es el siguiente:

1. Configure directivas de dispositivo macOS.

2. Inscriba los dispositivos macOS.
3. Configure las acciones de seguridad para los dispositivos y las aplicaciones. Consulte Acciones de seguridad.

Para conocer los sistemas operativos admitidos, consulte Sistemas operativos admitidos.

Nombres de host de Apple que deben permanecer abiertos

Algunos nombres de host de Apple deben permanecer abiertos para garantizar el correcto funcionamiento de iOS, macOS y el App Store. Bloquear dichos nombres de host puede afectar a la instalación, la actualización y el funcionamiento correcto de iOS, aplicaciones iOS, el funcionamiento de MDM y la inscripción de dispositivos y aplicaciones. Para obtener más información, consulte https://support.apple.com/en-us/HT201999.

Métodos de inscripción admitidos

En la siguiente tabla se indican los métodos de inscripción que XenMobile admite para los dispositivos macOS:

Método	¿Se admite?
Programa de implementación de Apple	Sí
Apple School Manager	Sí
Apple Configurator	No
Inscripción manual	Sí
Invitaciones de inscripción	Sí

Apple dispone de programas de inscripción de dispositivos para las cuentas Empresas y Educación. Para las cuentas Business, debe inscribirse en el Programa de implementación de Apple para inscribir y administrar dispositivos en XenMobile. Ese programa es para dispositivos iOS y macOS. Consulte Implementar dispositivos mediante el Programa de implementación de Apple.

Para las cuentas Educación, cree una cuenta de Apple School Manager. Apple School Manager unifica el programa de implementación y las compras por volumen. Apple School Manager es un tipo de Programa de implementación de Apple Educación. Consulte Integrar en funciones de Apple Educación.

Puede utilizar el Programa de implementación de Apple para inscribir en bloque dispositivos iOS y macOS. Puede comprar esos dispositivos directamente de Apple, un distribuidor autorizado de Apple o un proveedor.

Configurar directivas de dispositivo macOS

Use estas directivas para configurar cómo interactúa XenMobile Server con los dispositivos macOS. En esta tabla se indican todas las directivas de dispositivo disponibles para dispositivos macOS.

Duplicación AirPlay	Inventario de aplicaciones	Calendario (CalDAV)
Contactos (CardDAV)	Controlar actualización del SO	Credenciales
Nombre del dispositivo	Exchange	FileVault
Firewall	Fuente	Importar perfil de iOS y macOS
LDAP	Correo	Código de acceso
Eliminación de perfiles	Restricciones	SCEP
VPN	Clip web	Wi-Fi

Inscribir dispositivos macOS

XenMobile ofrece dos métodos para inscribir dispositivos que ejecutan macOS. Ambos métodos permiten a los usuarios de macOS inscribirse de forma inalámbrica y directamente desde sus dispositivos.

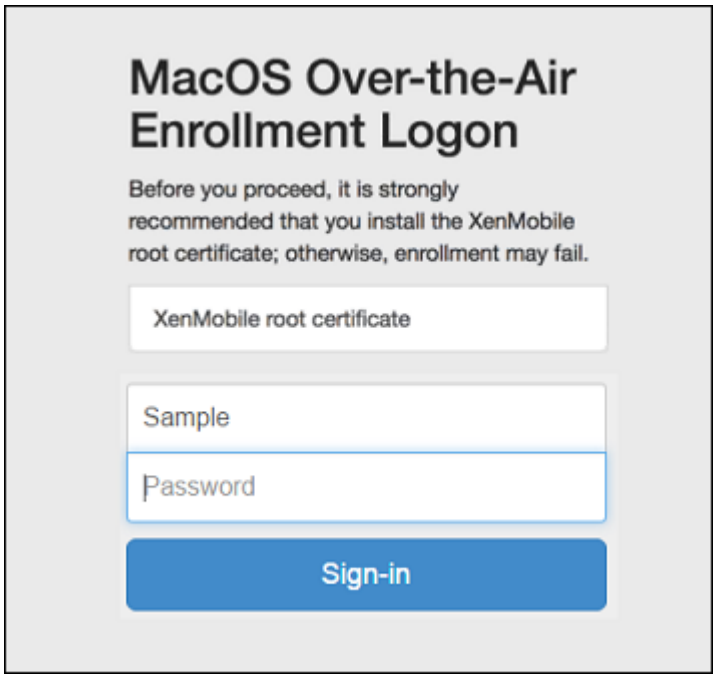
- **Enviar una invitación de inscripción a los usuarios:** Este método de inscripción permite definir uno de estos modos de seguridad de inscripción para dispositivos macOS:
  - Nombre de usuario y contraseña
  - Nombre de usuario + PIN
  - Autenticación de dos factores

  Cuando el usuario siga las instrucciones de la invitación a la inscripción, aparecerá una pantalla de inicio de sesión con el nombre de usuario ya rellenado.
- **Enviar un enlace de inscripción a los usuarios:** Este método de inscripción para dispositivos macOS envía a los usuarios un enlace de inscripción, que pueden abrir en los exploradores Safari o Chrome. A continuación, el usuario se inscribe suministrando su nombre de usuario y contraseña.

  Para impedir que se use un enlace de inscripción para dispositivos macOS, defina la propiedad de servidor **Enable macOS OTAE** en **False**. Como resultado, los usuarios de macOS solo podrán inscribirse mediante una invitación de inscripción.

Enviar una invitación de inscripción a los usuarios macOS

1. Agregue una invitación para la inscripción de usuarios de macOS. Consulte Crear una invitación de inscripción.
2. Cuando los usuarios reciban la invitación y hagan clic en el enlace, aparecerá la siguiente pantalla en el explorador Safari. XenMobile rellena el nombre de usuario. Si eligió **Dos factores** como modo de seguridad de inscripción, aparecerá un campo adicional.



3. Los usuarios deben instalar certificados según sea necesario. La solicitud a los usuarios para instalar certificados depende de si se ha configurado un certificado SSL público de confianza y un certificado de firma digital público de confianza para macOS. Para obtener información acerca de los certificados, consulte Certificados y autenticación.
4. Los usuarios proporcionan las credenciales solicitadas.

   Se instalan las directivas de dispositivos Mac. Ahora ya puede iniciar la administración de dispositivos macOS con XenMobile del mismo modo en que administra dispositivos móviles.

Enviar un enlace de inscripción a los usuarios macOS

1. Envíe el enlace de inscripción `https://serverFQDN:8443/instanceName/macos/otae`, que los usuarios abrirán en los exploradores web Safari o Chrome.
   - **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 puerto, en lugar de 8443.

- El elemento **instanceName** a menudo se muestra como `zdm` y es el nombre que se especificó durante la instalación del servidor.

Para obtener más información sobre el envío de enlaces de instalación, consulte Enviar una invitación de inscripción.

2. Los usuarios deben instalar certificados según sea necesario. Si ha configurado un certificado SSL público de confianza y un certificado de firma digital público de confianza para iOS y macOS, los usuarios verán el mensaje que pide instalar los certificados. Para obtener información acerca de los certificados, consulte Certificados y autenticación.
3. Los usuarios inician sesión en su Mac.

   Se instalan las directivas de dispositivos Mac. Ahora ya puede iniciar la administración de dispositivos macOS con XenMobile del mismo modo en que administra dispositivos móviles.

Acciones de seguridad

macOS admite las siguientes acciones de seguridad. Para ver una descripción de cada acción de seguridad, consulte Acciones de seguridad.

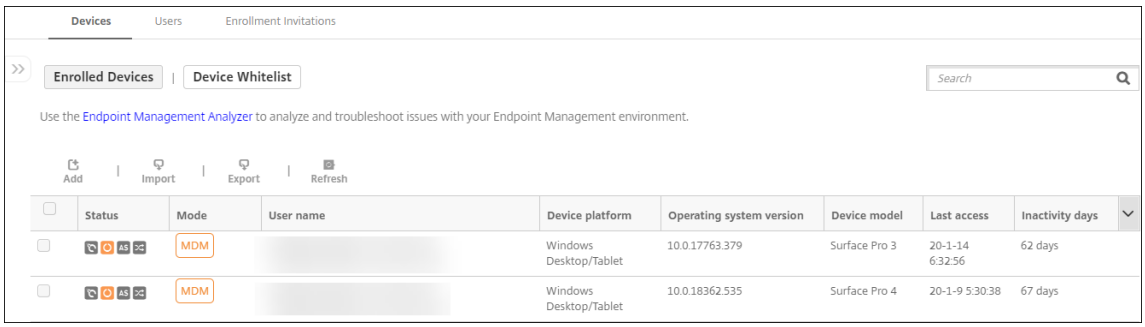
Revocar	Bloquear	Borrado selectivo
Borrado completo	Renovación de certificados	

Bloquear dispositivos macOS

Puede bloquear de forma remota dispositivos macOS perdidos. XenMobile bloquea el dispositivo. A continuación, genera un código PIN y lo establece en el dispositivo. Para acceder al dispositivo, el usuario deberá teclear ese código PIN. Use el comando **Cancelar bloqueo** para quitar el bloqueo desde la consola de XenMobile.

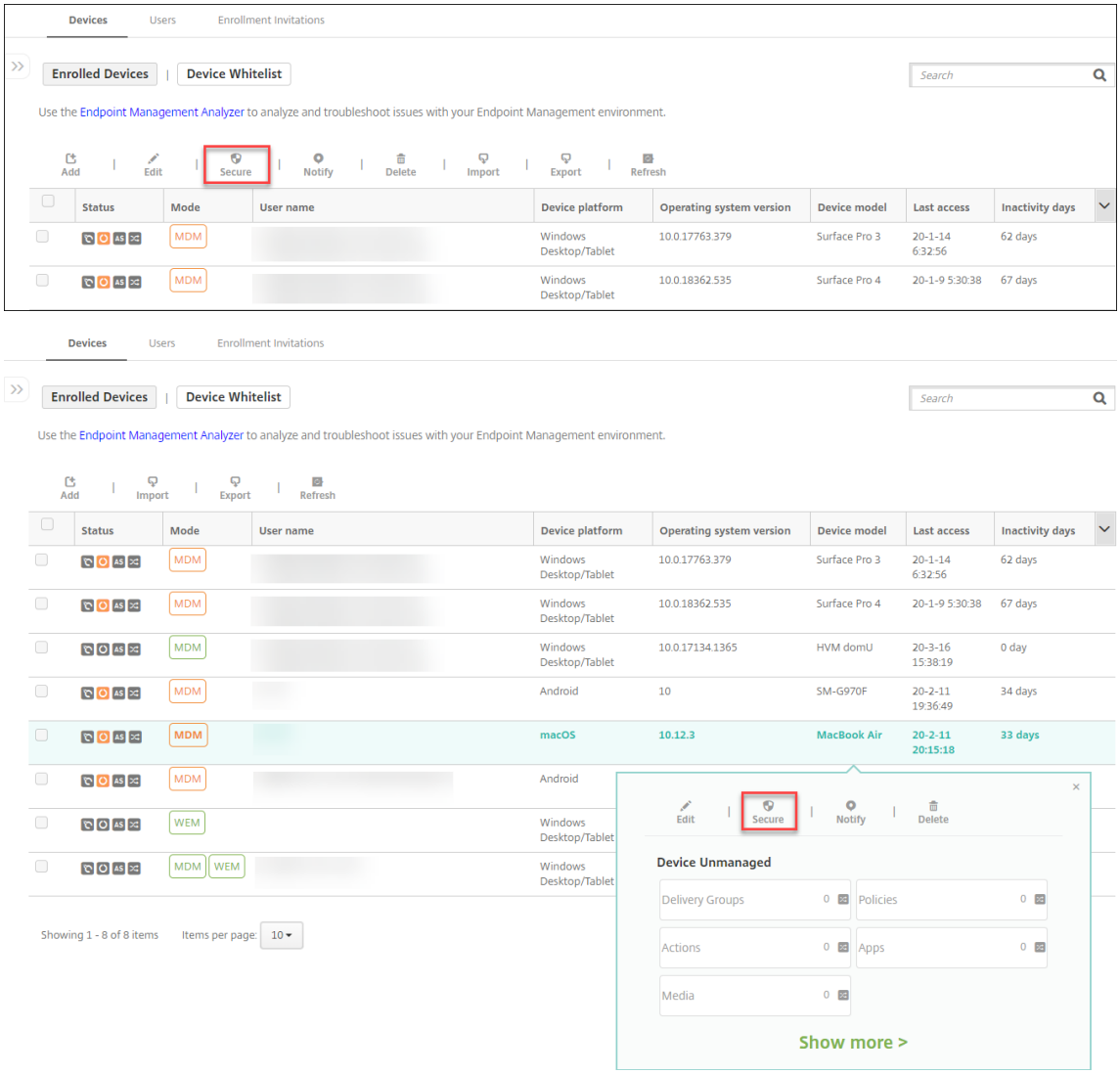
Puede utilizar la directiva Código de acceso para configurar más parámetros asociados al código PIN. Para obtener más información, consulte Parámetros de macOS.

1. Haga clic en **Administrar > Dispositivos**. Aparecerá la página **Dispositivos**.



2. Seleccione el dispositivo macOS que quiere bloquear.

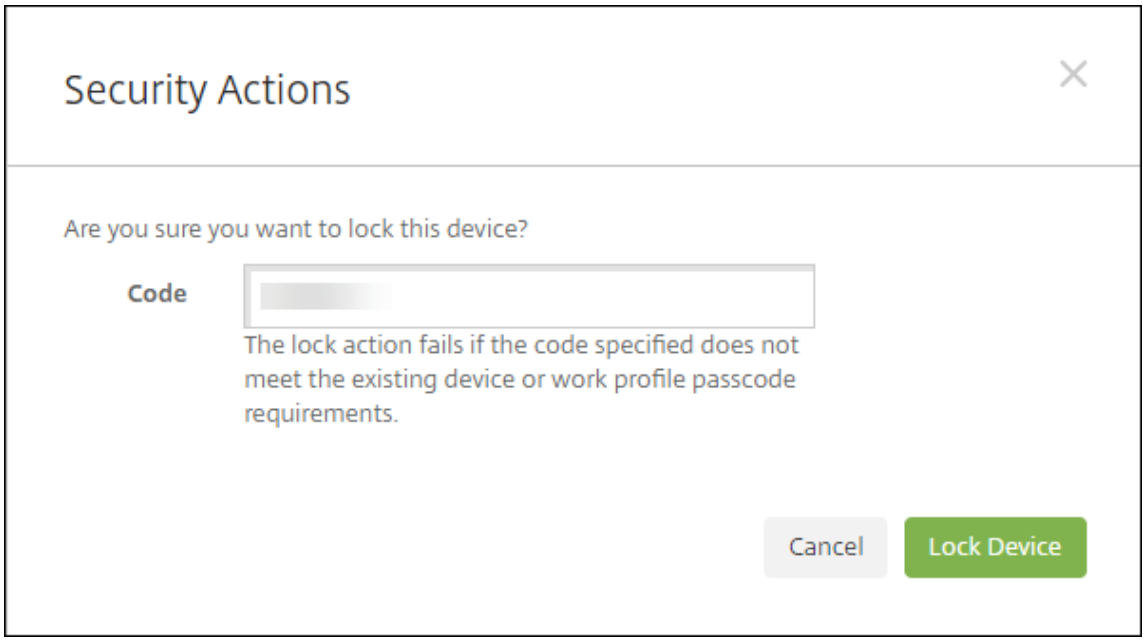
   Marque la casilla situada junto a un dispositivo para que el menú de opciones aparezca encima de la lista de dispositivos. También puede hacer clic en cualquier otro elemento de la lista para mostrar el menú de opciones en el lado derecho de la lista.



3. En el menú de opciones, seleccione **Proteger**. Aparecerá el cuadro de diálogo **Acciones de se-**

guridad.

4. Haga clic en **Bloquear**. Aparecerá el cuadro de confirmación **Acciones de seguridad**.



5. Haga clic en **Bloquear dispositivo**.

> **Importante:**
>
> También puede especificar un código de acceso, en lugar de utilizar el código que genera XenMobile. La acción de bloqueo falla si el código especificado no cumple los requisitos de código del

> dispositivo o del perfil de trabajo existente.

Inscribir en bloque dispositivos Apple

January 4, 2022

En XenMobile, puede inscribir una gran cantidad de dispositivos iOS, iPadOS y macOS de dos formas.

- Utilice el Programa de implementación de Apple para inscribir los dispositivos iOS, iPadOS y macOS adquiridos directamente de Apple, de un distribuidor autorizado de Apple o de un operador. Ahí se incluyen los iPads compartidos. XenMobile es compatible con el Programa de implementación de Apple para Apple Business Manager (ABM) y Apple School Manager (ASM) para Educación. En este artículo, se describe cómo integrar varios dispositivos en su cuenta de ABM. Para obtener información sobre cómo inscribirse en ABM y conectar su cuenta de ABM con XenMobile, consulte Implementar dispositivos mediante el Programa de implementación de Apple. Para obtener información sobre cuentas de Apple School Manager, consulte Integrar en funciones de Apple Educación.

  Para la inscripción de dispositivos macOS, XenMobile requiere que los dispositivos ejecuten macOS 10.10 o una versión posterior.

- Puede usar Apple Configurator 2 para inscribir dispositivos iOS tanto si los adquirió directamente de Apple como si no.

Con ABM:

- No tiene que tocar ni preparar los dispositivos. Basta con enviar los números de serie o de pedido de compra a través de ABM, y los dispositivos se configuran y se inscriben.
- Después de que XenMobile inscriba los dispositivos, puede entregárselos a los usuarios, y estos pueden comenzar a usarlos inmediatamente. Cuando se configuran los dispositivos con ABM, se pueden eliminar algunos de los pasos del asistente de configuración que los usuarios tendrían que completar al encender por primera vez sus dispositivos.
- Para obtener más información sobre la configuración de ABM, consulte la documentación disponible en Apple Business Manager.

Con Apple Configurator 2:

- Conecte los dispositivos iOS a un equipo Apple con macOS 10.7.2 o una versión posterior y la aplicación Apple Configurator 2. Debe preparar los dispositivos iOS y configurar las directivas a través de Apple Configurator 2.
- Después de aprovisionar los dispositivos con las directivas necesarias, la primera vez que los dispositivos se conectan a XenMobile, reciben las directivas de XenMobile. A partir de ahí puede empezar a administrar los dispositivos.

- Para obtener más información sobre cómo usar Apple Configurator 2, consulte la ayuda de Apple Configurator.

Requisitos previos

Abra los puertos necesarios para la conectividad entre XenMobile y Apple. Para obtener más información, consulte Requisitos de puertos.

Integrar la cuenta de Apple Business Manager con XenMobile

Si no tiene una cuenta de ABM configurada con XenMobile, complete los pasos que se indican a continuación, en Implementar dispositivos mediante el Programa de implementación de Apple.

- Inscríbase en Apple Business Manager.
- Conecte su cuenta de Apple Business Manager con XenMobile.
- Adquiera dispositivos habilitados para el Programa de implementación
- Administre los dispositivos habilitados para el Programa de implementación

Establecer un servidor predeterminado para la inscripción en bloque

Para asignar grandes pedidos de dispositivos iOS, iPadOS y macOS a un servidor MDM, puede establecer XenMobile como servidor predeterminado.

1. Inicie sesión en Apple Business Manager con una cuenta de administrador o de administrador de inscripción de dispositivos.
2. En la barra lateral, haga clic en **Settings > Device Management Settings**.
3. Elija un servidor MDM existente. En **Default Device Assignment**, haga clic en **Change**. Seleccione el servidor de XenMobile predeterminado para cada tipo de dispositivo. Haga clic en **Done**.

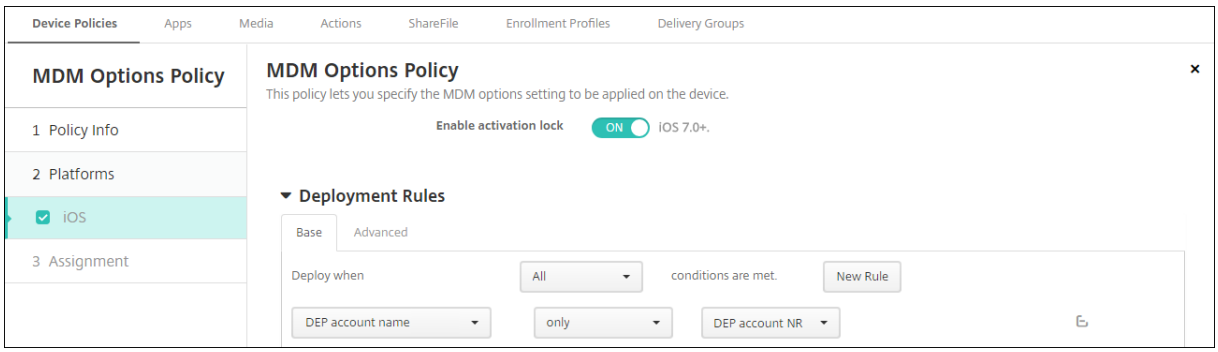
Configurar reglas de implementación de aplicaciones y directivas de dispositivos para cuentas de ABM

Puede asociar cuentas de ABM a aplicaciones y directivas de dispositivos desde la sección **Reglas de implementación**, en **Configurar > Directivas de dispositivo** y **Configurar > Aplicaciones**. Puede especificar que una directiva o aplicación:

- Se implementa solo para una cuenta concreta de ABM.
- Se implementa para todas las cuentas de ABM, excepto la seleccionada.

La lista de cuentas de ABM incluye solo aquellas cuentas que tengan el estado habilitado o inhabilitado. Si la cuenta de ABM está inhabilitada, el dispositivo de ABM no pertenece a esta cuenta. Por lo tanto, XenMobile no implementa la aplicación o la directiva en el dispositivo.

En el siguiente ejemplo, una directiva de dispositivos se implementa solo en dispositivos cuyo nombre de cuenta de ABM sea “ABM Account NR”.

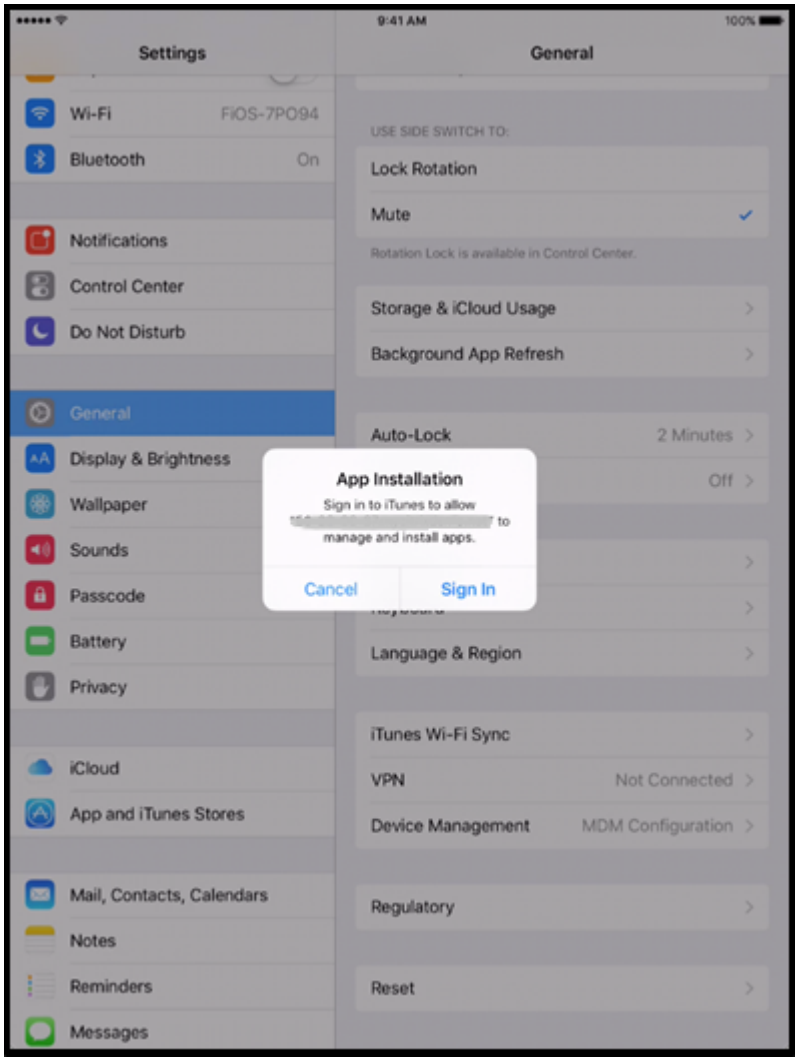


Experiencia del usuario al inscribir un dispositivo habilitado para el Programa de implementación de Apple

Cuando los usuarios inscriben un dispositivo habilitado para el Programa de implementación de Apple, su experiencia es la siguiente.

1. Los usuarios inician su dispositivo habilitado para el Programa de implementación de Apple.
2. XenMobile entrega la configuración del Programa de implementación de Apple que configuró en la consola de XenMobile al dispositivo habilitado para el Programa de implementación de Apple.
3. Los usuarios configuran los parámetros iniciales en el dispositivo.
4. El dispositivo inicia automáticamente el proceso de inscripción en XenMobile.
5. Los usuarios siguen configurando otros parámetros iniciales en el dispositivo.
6. En la pantalla de inicio, puede que se pida a los usuarios que inicien sesión en el App Store de Apple para descargar Citrix Secure Hub.

   > **Nota:**
   >
   > Este paso es opcional si configura XenMobile para implementar la aplicación Secure Hub mediante la asignación de aplicaciones de compras por volumen para cada dispositivo. En este caso, no es necesario crear una cuenta de App Store ni utilizar una cuenta existente.



7. Los usuarios abren Secure Hub y escriben sus credenciales. Si hay una directiva que lo requiera, puede que se pida a los usuarios que creen y confirmen un PIN de Citrix.

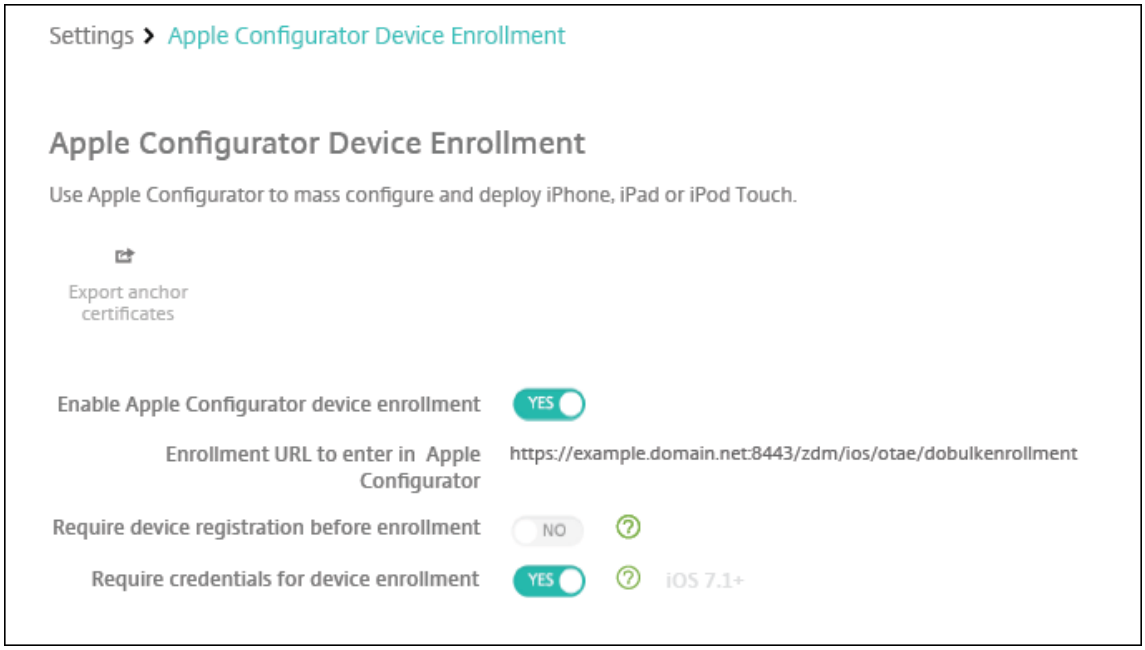
   XenMobile implementa las aplicaciones obligatorias restantes en el dispositivo.

Configurar parámetros de Apple Configurator 2

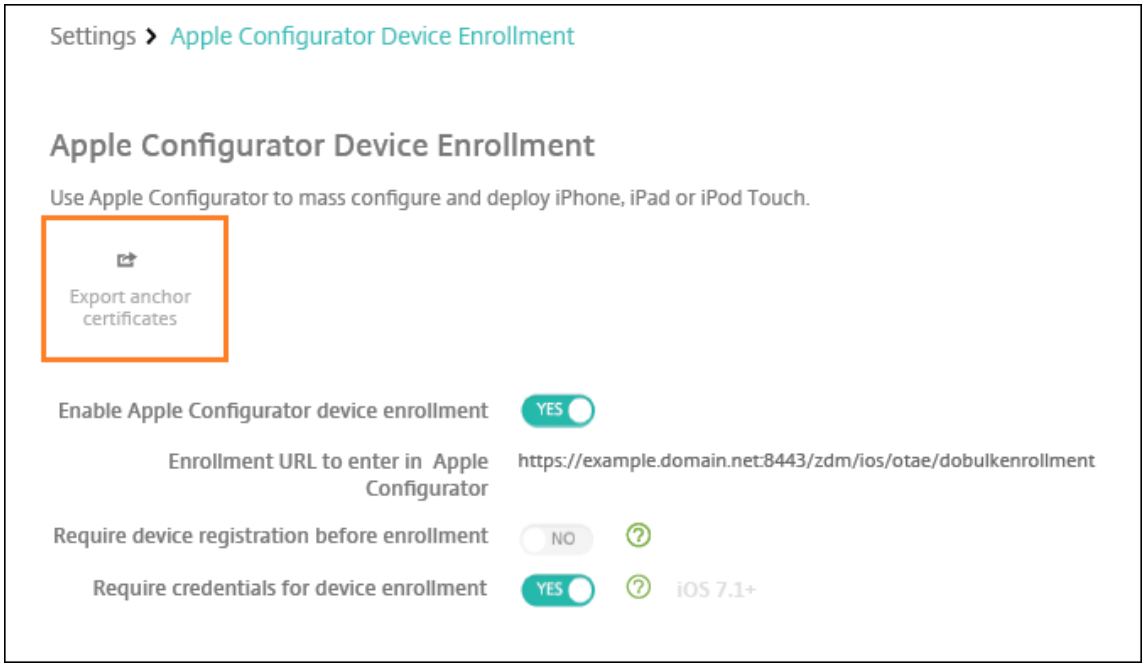
Puede configurar e implementar dispositivos iPhone y iPad en bloque con Apple Configurator 2, en lugar de Apple Business Manager.

Paso 1: Configurar los parámetros en XenMobile

1. En la consola de XenMobile, vaya a **Parámetros > Apple Configurator Device Enrollment**.



2. Establezca **Permitir inscripción de dispositivos en Apple Configurator** en **Sí**.
3. La **URL de inscripción a introducir en Apple Configurator** es un campo de solo lectura. Este valor proporciona la URL del servidor de XenMobile que se comunica con Apple. Copie y pegue esta URL cuando configure los ajustes en Apple Configurator 2. La URL de inscripción es el nombre FQDN (por ejemplo, `mdm.server.url.com`) o la dirección IP del servidor de XenMobile.
4. Para evitar que se inscriban dispositivos desconocidos, **active** el parámetro **Requerir registro del dispositivo antes de inscribirlo**. Nota: Si el valor de este parámetro es **Sí**, debe agregar los dispositivos configurados en **Administrar > Dispositivos** de XenMobile manualmente o a través de un archivo CSV antes de la inscripción.
5. Para obligar a los usuarios de los dispositivos iOS que introduzcan sus credenciales cuando se inscriban, **active** el parámetro **Requerir credenciales para inscripción de dispositivos**. El valor predeterminado es no requerir credenciales para la inscripción.
6. Nota: Si el servidor de XenMobile está usando un certificado SSL de confianza, omita el paso siguiente. Haga clic en **Exportar certificados de anclaje** y guarde el archivo certchain.pem en el llavero de macOS (Inicio de sesión o Sistema).



Paso 2: Configure los ajustes en Apple Configurator 2

1. Instale Apple Configurator 2 desde el App Store.
2. Use un cable de conector de Dock con USB para conectar los dispositivos al equipo Mac donde se ejecuta Apple Configurator 2. Puede configurar hasta 30 dispositivos conectados simultáneamente. Si no dispone de un conector de Dock, use varios concentradores USB 2.0 de alta velocidad para conectar los dispositivos.
3. Inicie Apple Configurator 2. El configurador muestra todos los dispositivos que puede preparar para supervisión.
4. Para preparar un dispositivo para supervisión:
   - Si quiere mantener el control del dispositivo aplicando periódicamente una configuración, seleccione **Supervise devices**. Haga clic en **Siguiente**.

     > **Importante:**
     >
     > Colocar un dispositivo en el modo supervisado instala la versión seleccionada de iOS en el dispositivo. Con este proceso, se borran del dispositivo todos los datos de usuario o aplicaciones almacenados previamente.

   - En iOS, haga clic en **Latest** para ver la versión más reciente de iOS que quiera instalar.
5. En **Enroll in MDM Server**, elija un servidor MDM. Para agregar un nuevo servidor, haga clic en **Next**.

6. En **Define an MDM server**, proporcione un nombre para el servidor y pegue la dirección URL del servidor MDM desde la consola de XenMobile.
7. En **Assign to organization**, elija una organización para supervisar el dispositivo.

   Para obtener más información sobre la preparación de dispositivos con Apple Configurator 2, consulte la página de ayuda Preparar dispositivos Apple Configurator.
8. A medida que prepare cada dispositivo, enciéndalo para iniciar el asistente de configuración de iOS, que prepara el dispositivo para su primer uso.

Para asignar dispositivos de Apple Configurator 2 a Apple Business Manager

Puede asociar dispositivos iPhone y iPad desde Apple Configurator 2 a su cuenta de Apple Business Manager. Cuando agrega dispositivos, estos aparecen en la sección **Devices**. Estos dispositivos ya no incluyen la configuración de inscripción asignada a través de Apple Configurator 2. Para obtener más información, consulte Asignar dispositivos agregados desde Apple Configurator 2 a Apple Business Manager.

Renovar o actualizar certificados al utilizar el Programa de implementación de Apple

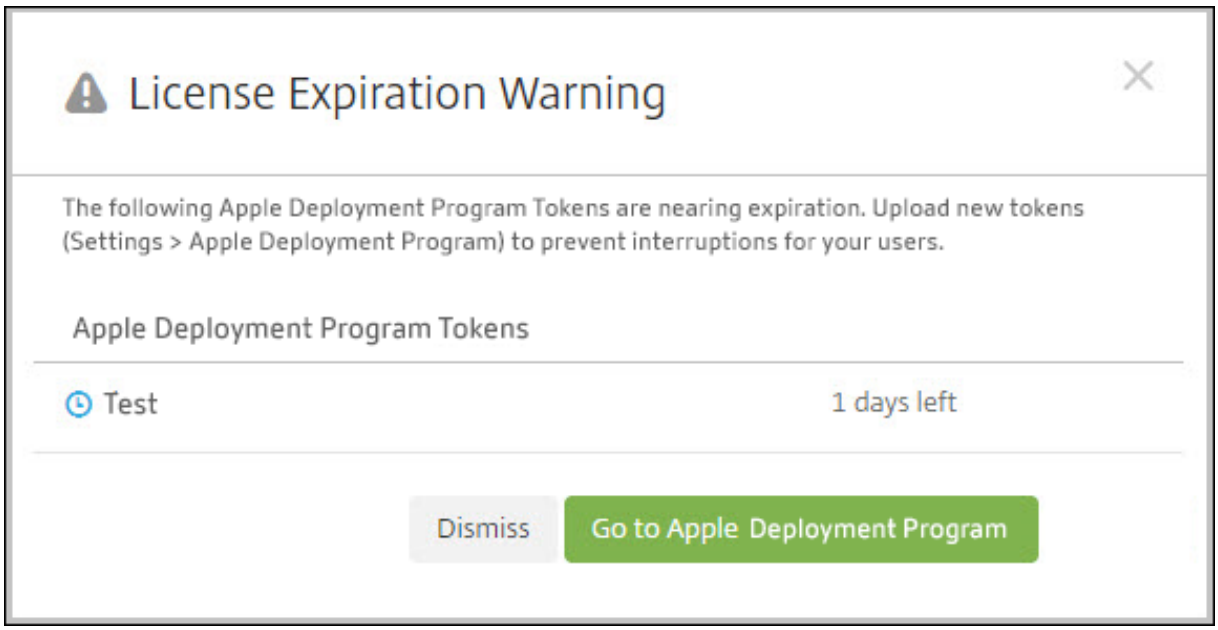
Cuando se renueva el certificado SSL (Secure Sockets Layer) de XenMobile, hay que cargar un nuevo certificado en la consola de XenMobile, en **Parámetros > Certificados**. En el cuadro de diálogo **Importar**, en **Usar como**, haga clic en **Escucha SSL** de forma que el certificado se utilice para 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 el Programa de implementación de Apple al renovar o actualizar el certificado SSL. Sin embargo, puede volver a configurar los parámetros del **Programa de implementación de Apple** en cualquier momento siguiendo los pasos anteriores de este artículo.

Para obtener más información acerca del Programa de implementación de Apple, consulte la documentación de Apple.

Renovar la conexión entre el Programa de implementación de Apple y XenMobile

XenMobile muestra una advertencia de caducidad de licencia cuando el token del servidor de inscripción automatizada de dispositivos caduca.



Sustituya el token de Apple School Manager/Apple Business Manager.

Paso 1: Cargue una clave pública desde el servidor de XenMobile

1. En la consola de XenMobile, vaya a **Parámetros > Programa de implementación de Apple (DEP)** para descargar una nueva clave pública.

Paso 2: Cree y descargue un archivo de token de servidor desde su cuenta de Apple

1. Inicie sesión en Apple Business Manager para descargar el token.
2. Abra **Settings** y seleccione el servidor del que necesita un token. Haga clic en **Edit**.
3. En **MDM Server Settings**, cargue la nueva clave pública que descargó de XenMobile y guarde los cambios.
4. Haga clic en **Download Token** para descargar el nuevo token.

Paso 3: Cargar un archivo de token de servidor en XenMobile

1. En Citrix XenMobile, vaya a **Parámetros > Programa de implementación de Apple**.
2. Seleccione la cuenta del Programa de implementación, haga clic en **Modificar** y cargue el archivo de token del servidor.
3. Haga clic en **Siguiente** y guarde los cambios.

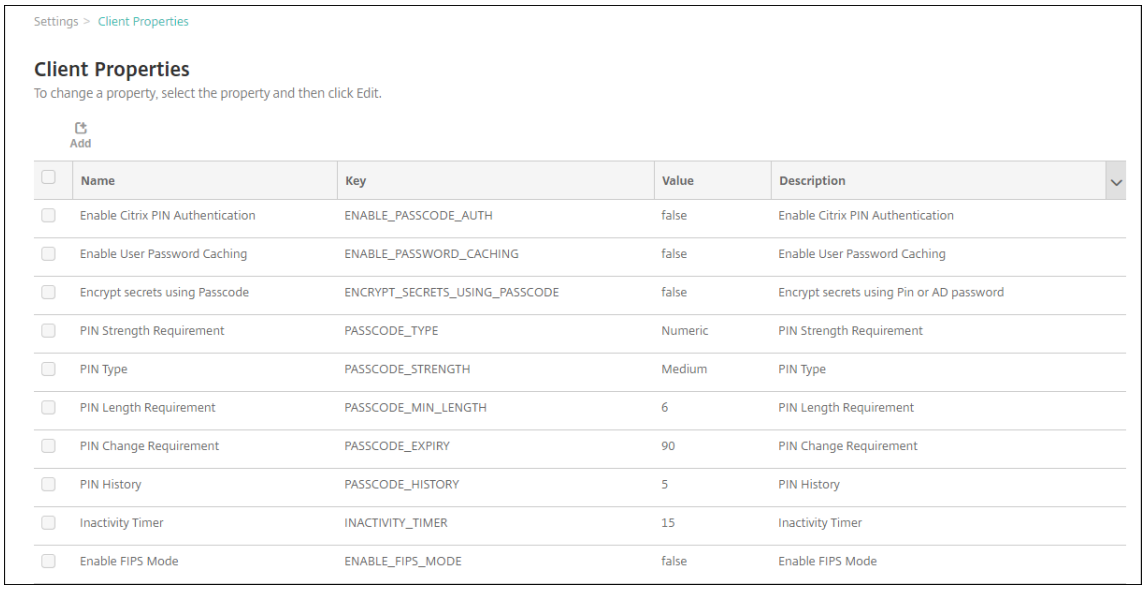
Propiedades de cliente

January 4, 2022

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 Secure Hub y, ocasionalmente, en las aplicaciones cliente. 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.

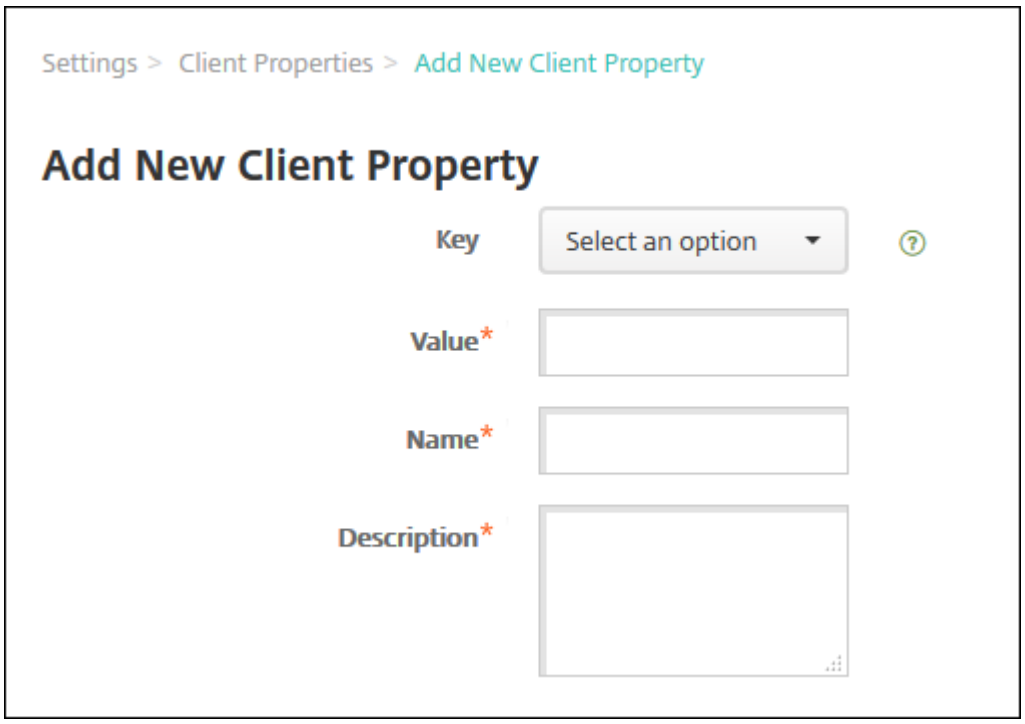
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Cliente**, haga clic en **Propiedades de cliente**. Aparecerá la página **Propiedades de cliente**. Puede agregar, modificar y eliminar las propiedades de cliente desde esta página.



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

Para agregar una propiedad de cliente

1. Haga clic en **Agregar**. Aparecerá la página **Agregar nueva propiedad de cliente**.

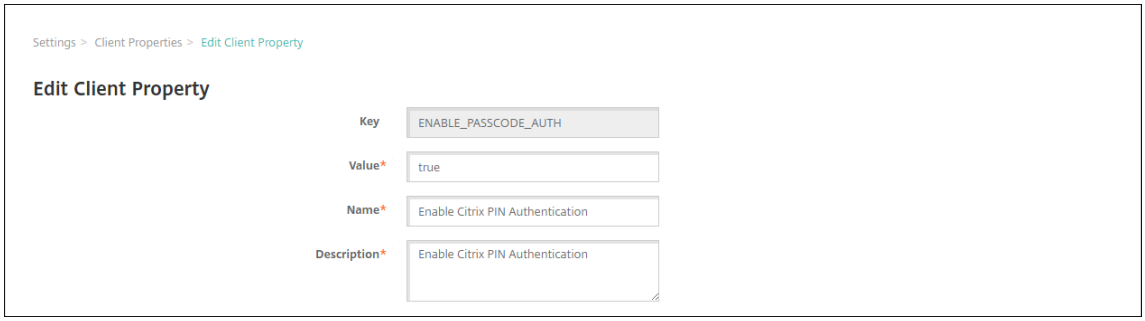


2. Configure estos parámetros:
   - **Clave:** En la lista, haga clic en la clave de propiedad que quiere agregar. Importante: Póngase en contacto con Citrix Support antes de actualizar los parámetros. Puede solicitar una clave especial.
   - **Valor:** El valor de la propiedad seleccionada.
   - **Nombre:** Introduzca un nombre para la propiedad.
   - **Descripción:** Introduzca una descripción de la propiedad.
3. Haga clic en **Guardar**.

Para modificar una propiedad de cliente

1. En la tabla **Propiedades de cliente**, seleccione la propiedad de cliente que quiere modificar.

   Si marca la casilla situada junto a una propiedad de cliente, el menú de opciones aparecerá encima de la lista de propiedades de cliente. Si hace clic en cualquier lugar de la lista, el menú de opciones aparece a la derecha de la lista.
2. Haga clic en **Edit**. Aparecerá la página **Modificar propiedad de cliente**.



3. Cambie la siguiente información como corresponda:
   - **Clave:** Este campo no puede cambiarse.
   - **Valor:** El valor de la propiedad.
   - **Nombre:** El nombre de la propiedad.
   - **Descripción:** La descripción de la propiedad.
4. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para descartarlos.

Para eliminar una propiedad de cliente

1. En la tabla **Propiedades de cliente**, seleccione la propiedad de cliente que quiere eliminar.

   Puede eliminar más de una propiedad. Para ello, marque 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 **Eliminar**.

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 (Periodo de autodestrucción del contenedor MDX)
  - La propiedad Autodestrucción impide el acceso a Secure Hub y a aplicaciones administradas después de una cantidad determinada de días de inactividad. Transcurrido el límite de tiempo, las aplicaciones ya no pueden utilizarse. 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 una aplicación 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 agregar o 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 (Enviar registros del dispositivo al servicio de asistencia)
  - 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
  - Utilice esta propiedad para impedir que los usuarios recopilen y carguen registros desde sus dispositivos. Esta propiedad inhabilita la captura de registros de Secure Hub y todas las aplicaciones MDX instaladas. Los usuarios no pueden enviar registros de cualquier aplicación desde la página de asistencia. Aunque aparezca el cuadro de diálogo para redactar el correo, los registros no se adjuntan. Un mensaje indica que el registro está inhabilitado. Este parámetro también le impide actualizar los parámetros de registro en la consola de XenMobile para Secure Hub y las aplicaciones MDX.

    Cuando esta propiedad se establece en **true**, Secure Hub establece **Bloquear registros de aplicaciones** en **true**. Como resultado, 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
  - Si tiene el valor **true**, Citrix recopila informes de errores y diagnósticos para ayudar a solucionar problemas con Secure Hub para iOS y Android. Si el valor es **false**, no se recopilan datos.
  - Valores posibles: **true** o **false**
  - Valor predeterminado: **true**

- **ENABLE_CREDENTIAL_STORE**
  - Nombre simplificado: Enable Credential Store
  - Habilitar el almacén de credenciales significa que los usuarios de iOS o Android introducen su contraseña una vez cuando acceden a las aplicaciones móviles de productividad. Puede utilizar el almacén de credenciales independientemente de si habilita el PIN de Citrix. Si no habilita el PIN de Citrix, los usuarios deberán introducir su contraseña de Active Directory. XenMobile admite contraseñas de Active Directory en el almacén de credenciales solo para Secure Hub y las aplicaciones de tienda pública. XenMobile no admite la autenticación con la infraestructura de clave pública si se utilizan contraseñas de Active Directory en el almacén de credenciales.
  - La inscripción automática en Secure Mail requiere que esta propiedad se establezca en **true**.
  - Para agregar o configurar esta directiva de cliente global, vaya a **Parámetros > Propiedades de cliente** y agregue la clave personalizada **ENABLE_CREDENTIAL_STORE** y defina el **Valor** en **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**
- **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.

    Para la autenticación sin conexión, el PIN de Citrix se valida localmente y se permite a los usuarios acceder a la aplicación o al contenido solicitado. Para la autenticación 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.

    Si ENABLE_PASSCODE_AUTH se establece en “true” y ENABLE_PASSWORD_CACHING se establece en “false”, la autenticación en línea siempre solicitará la contraseña debido a que Secure Hub no la guarda.

- Valores posibles: **true** o **false**
- Valor predeterminado: **false**

- **ENABLE_PASSWORD_CACHING**
  - Nombre simplificado: Enable User Password Caching
  - Esta propiedad permite que las contraseñas de Active Directory de los usuarios se almacenen en la memoria caché local del dispositivo móvil. Cuando establezca esta propiedad en **true**, también deberá establecer la propiedad **ENABLE_PASSCODE_AUTH** en **true**. Si se habilita el almacenamiento en caché de las contraseñas de usuario, XenMobile pide a los usuarios que definan un código de acceso o un PIN de Citrix.
  - Valores posibles: **true** o **false**
  - Valor predeterminado: **false**

- **ENABLE_TOUCH_ID_AUTH**
  - Nombre simplificado: Enable Touch ID Authentication
  - Para los dispositivos que admiten la autenticación Touch ID, esta propiedad habilita o inhabilita la autenticación Touch ID en el dispositivo. Requisitos:

    Los dispositivos de usuario deben tener el PIN de Citrix o LDAP habilitado. Si la autenticación de LDAP está desactivada (por ejemplo, debido a que solo se usa la autenticación por certificados), los usuarios deben establecer un PIN de Citrix. En este caso, XenMobile pide el PIN de Citrix, aunque la propiedad de cliente **ENABLE_PASSCODE_AUTH** esté establecida en **falso**.

    Establezca **ENABLE_PASSCODE_AUTH** en **false** de modo que, cuando los usuarios inicien una aplicación, deban responder a una solicitud de usar Touch ID.
  - Valores posibles: **true** o **false**
  - Valor predeterminado: **false**

- **ENABLE_WORXHOME_CEIP**
  - Nombre simplificado: Enable Worx Home CEIP
  - Esta propiedad activa el programa CEIP de mejora de la experiencia del cliente. Esa función envía 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 Secure Hub. Si cambia este parámetro, el nuevo valor se establece solamente cuando el usuario inicia sesión en Secure Hub (antes llamado Worx Home).
  - Valores posibles: **true** o **false**
  - Valor predeterminado: **true**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - Nombre simplificado: Encrypt secrets using Passcode
  - Esta propiedad almacena datos confidenciales 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 artefactos de la clave, aunque también agrega la entropía de usuario. La entropía de usuario es un código PIN aleatorio generado por el usuario y que solo este conoce.

    Citrix recomienda habilitar esta propiedad para una mayor seguridad en los dispositivos de usuario. En consecuencia, los usuarios ven más solicitudes de autenticación con el PIN de Citrix.
  - Valores posibles: **true** o **false**
  - Valor predeterminado: **false**

- **INACTIVITY_TIMER**
  - Nombre simplificado: Inactivity Timer
  - Esta propiedad define cuánto tiempo pueden dejar los usuarios su dispositivo inactivo y luego acceder a una aplicación sin que se les solicite un PIN o un código de acceso de Citrix. Si quiere habilitar este parámetro para una aplicación MDX, active el parámetro "Código de acceso de aplicación". Si el parámetro Código de acceso de aplicación está desactivado, se redirige a los usuarios a Secure Hub para realizar una autenticación completa. Al cambiar esta configuración, el valor se aplicará la próxima vez que los usuarios deban autenticarse.

    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** (minutos)

- **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 cuánto tiempo es válido el PIN o código de acceso de Citrix. 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 define un período de caducidad de entre 1 y 99 días y luego lo cambia a 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** (días)
- **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 este parámetro, el nuevo valor se establece la próxima vez que el usuario restablezca su PIN o código de acceso a Citrix.
  - Valores posibles: de **1** a **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 PIN o código de acceso de Citrix.
  - Valores posibles: Cualquier número entero positivo
  - Valor predeterminado: **15**
- **PASSCODE_MIN_LENGTH**
  - Nombre simplificado: PIN Length Requirement (Requisito de longitud de código PIN)
  - Esta propiedad define la longitud mínima de los PIN de Citrix.
  - Valores posibles: De **4** a **10**
  - 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 creen un PIN o código de acceso de Citrix la próxima vez que deban autenticarse.
- Valores posibles: **Low**, **Medium**, **High** o **Strong**
- Valor predeterminado: **Medium**
- En esta tabla se describen las reglas de contraseña para cada parámetro de nivel de seguridad, basadas en el parámetro PASSCODE_TYPE:

Reglas para códigos de acceso numéricos:

Nivel de seguridad de la contraseña	Reglas para el tipo de código de acceso numérico	Se permite	No se permite
Bajo	Se permiten todos los números y todas las secuencias	444444, 123456, 654321	
Medio (configuración predeterminada)	Los números no pueden ser los mismos ni consecutivos.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
Alto	Los números adyacentes no pueden ser iguales.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
Fuerte	No use el mismo número más de dos veces. No use tres o más números consecutivos seguidos. No use tres o más números consecutivos en el orden inverso.	102983, 085085, 824673, 132312	132132, 131313, 902030

Reglas para códigos de acceso alfanuméricos:

Nivel de seguridad de la contraseña	Reglas para el tipo de código de acceso alfanumérico	Se permite	No se permite
Bajo	Debe contener al menos una letra y un número.	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef
Medio (configuración predeterminada)	Además de las reglas de contraseñas con nivel bajo de seguridad, ni los números ni las letras pueden ser los mismos. Ni letras ni números pueden ser consecutivos.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, or aaa111; abcd12, bcd123, 123abc, xy1234, xyz345 o cba123
Alto	Incluya al menos una letra mayúscula y una letra minúscula.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Fuerte	Incluya al menos un número, un símbolo especial, una letra mayúscula y una letra minúscula.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

- **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.

    Si cambia este parámetro, los usuarios deberán establecer 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 **Parámetros > Propiedades de cliente**, agregue la clave personalizada **REFRESH-INTERVAL** y establezca el **Valor** en la cantidad de horas.
  - Valor predeterminado: **72** horas (3 días)

- **SEND_LDAP_ATTRIBUTES**
  - Para implementaciones de solo MAM de dispositivos Android, iOS o macOS: puede configurar XenMobile para que los usuarios que se inscriban en Secure Hub con las credenciales de correo electrónico queden automáticamente inscritos en Secure Mail. Como resultado, los usuarios no ofrecen información adicional ni realizan pasos adicionales para inscribirse en Secure Mail.
  - Para agregar o configurar esta directiva de cliente global, vaya a **Parámetros > Propiedades de cliente** y agregue la clave personalizada **SEND_LDAP_ATTRIBUTES** y defina el **Valor** de este modo.
  - Valor: `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:

    ```
    <property value="userPrincipalName=user@site.com,sAMAccountName=
    eng1,displayName=user\,test1,email=user@site.com\,user@site.com"
    name="SEND_LDAP_ATTRIBUTES"/>
    ```

  - En esta propiedad, XenMobile interpreta las comas como terminadores de cadenas. Por lo tanto, si un valor de atributo contiene una coma, debe ir precedida de una barra diagonal inversa. La barra diagonal inversa evita que el cliente interprete la coma como el final del valor del atributo. Los caracteres de barra diagonal invertida se representan así: `"\\"`.

- **HIDE_THREE_FINGER_TAP_MENU**
  - Cuando esta propiedad no está definida o está establecida en **false**, los usuarios pueden acceder al menú de funciones ocultas tras una pulsación con tres dedos en sus dispositivos. El menú de funciones ocultas permitía a los usuarios restablecer los datos de la aplicación. Establecer esta propiedad en **true** inhabilita el acceso de los usuarios al menú de funciones ocultas.
  - Para configurar esta directiva de cliente global, vaya a **Parámetros > Propiedades de cliente**, agregue la clave personalizada **HIDE_THREE_FINGER_TAP_MENU** y defina el **valor**.

- **TUNNEL_EXCLUDE_DOMAINS**

- Nombre simplificado: Tunnel Exclude Domains
- De forma predeterminada, MDX excluye de los túneles de micro VPN a algunos puntos finales de servicio que usen los SDK y las aplicaciones de XenMobile para varias funciones. Por ejemplo, esos dispositivos de punto final contienen servicios que no requieren el enrutamiento a través de redes de empresa (como Google Analytics, servicios de Citrix Cloud y servicios de Active Directory). Utilice esta propiedad de cliente para anular la lista predeterminada de dominios excluidos.
- Para agregar o configurar esta directiva de cliente global, vaya a **Parámetros > Propiedades de cliente** y agregue la clave personalizada **TUNNEL_EXCLUDE_DOMAINS** y defina el **Valor**.
- Valor: Para reemplazar la lista predeterminada por los dominios que quiere excluir del túnel, escriba una lista, separada por comas, de sufijos de dominio. Para incluir a todos los dominios en el túnel, escriba **none**. El valor predeterminado es:

  `app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream,launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com`

Implementar dispositivos mediante el Programa de implementación de Apple

January 4, 2022

Apple dispone de programas de inscripción de dispositivos para las cuentas Empresas y Educación. Para las cuentas Business, debe inscribirse en el Programa de implementación de Apple para utilizar Apple Business Manager (ABM) o Apple School Manager (ASM) con el fin de usarlo para inscribir y administrar dispositivos en XenMobile. Ese programa es para dispositivos iOS, iPadOS y macOS.

Tenga en cuenta que el Programa de implementación de Apple está disponible para las organizaciones, no para personas individuales. Debe proporcionar una cantidad considerable de detalles corporativos e información para crear una cuenta del Programa de implementación de Apple. Por lo tanto, podría tardar algún tiempo en solicitar y recibir aprobación para la cuenta.

Para las cuentas Educación, cree una cuenta de Apple School Manager. ASM unifica el Programa de implementación de Apple y las compras por volumen de Apple. Para crear una cuenta de Apple School Manager, vaya al sitio de Apple School.

Inscribirse en el programa de implementación de Apple (DEP)

Para inscribirse en Apple Business Manager, vaya a business.apple.com. Haga clic en **Enroll now** para solicitar una nueva cuenta. Se recomienda usar una dirección de correo electrónico asociada a la organización, como implementación@nombre-de-empresa.com. El proceso de inscripción puede tardar unos días. Después de recibir las credenciales de inicio de sesión, siga los pasos que se indican en Apple Business Manager para crear una cuenta.

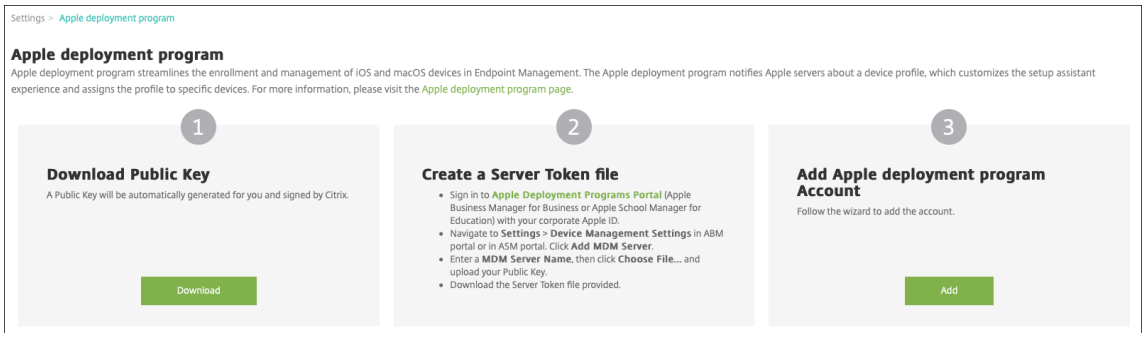
> **Nota:**
>
> Para cuentas educativas, consulte Integración en funciones de Apple Educación.

Conectar la cuenta de Apple Business Manager con XenMobile

Para conectar su cuenta de Apple Business Manager con la implementación de XenMobile, introduzca información en la consola de XenMobile y Apple Business Manager. Siga estos pasos:

Paso 1: Cargue una clave pública desde el servidor de XenMobile

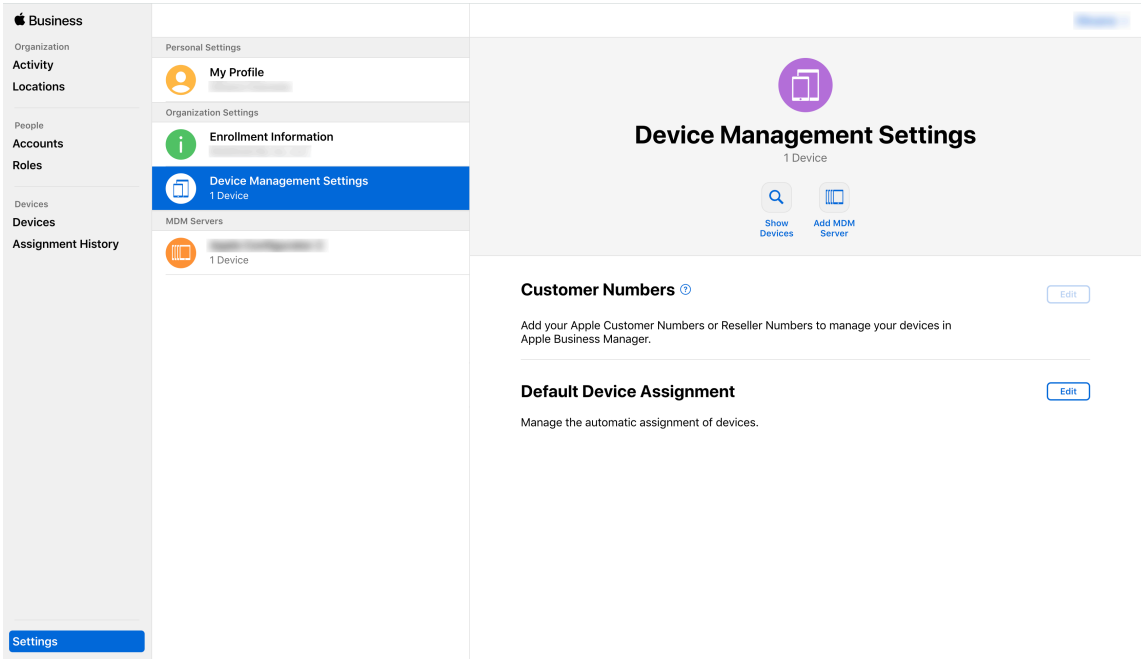
1. En la consola de XenMobile, vaya a **Parámetros > Programa de implementación de Apple**.



2. En **Descargar clave pública**, haga clic en **Descargar**.

Paso 2: Cree y descargue un archivo de token de servidor desde su cuenta de Apple

1. Inicie sesión en Apple Business Manager con una cuenta de administrador o de administrador de inscripción de dispositivos.
2. En la parte inferior de la barra lateral, haga clic en **Settings** y, a continuación, en **Device Management Settings > Add MDM Server**.



3. En el parámetro **MDM Server Name**, escriba un nombre para el servidor de XenMobile. El nombre del servidor que escriba le servirá de referencia. No es la URL o el nombre del servidor.
4. En **Upload Public Key**, haga clic en **Choose File**. Cargue la clave pública que descargó de XenMobile y, a continuación, guarde los cambios.
5. Haga clic en **Download Token** para descargar el archivo de token del servidor en su equipo.

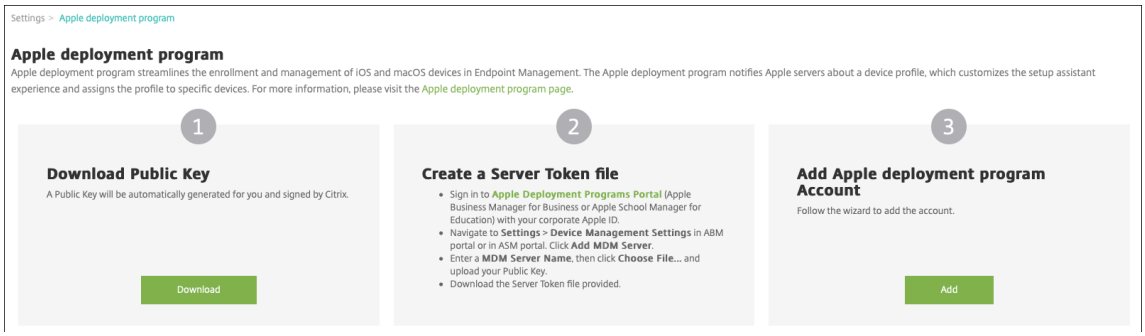
   Deberá cargar el archivo token del servidor cuando agregue la cuenta de ABM a XenMobile. La información del token de ABM aparece en la consola de XenMobile después de importar el archivo de token.
6. En **Default Device Assignment**, haga clic en **Change**. Elija cómo quiere asignar los dispositivos y, a continuación, proporcione la información solicitada. Para obtener información, consulte el Manual de uso de ABM.

Paso 3: Agregue una cuenta de ABM a XenMobile

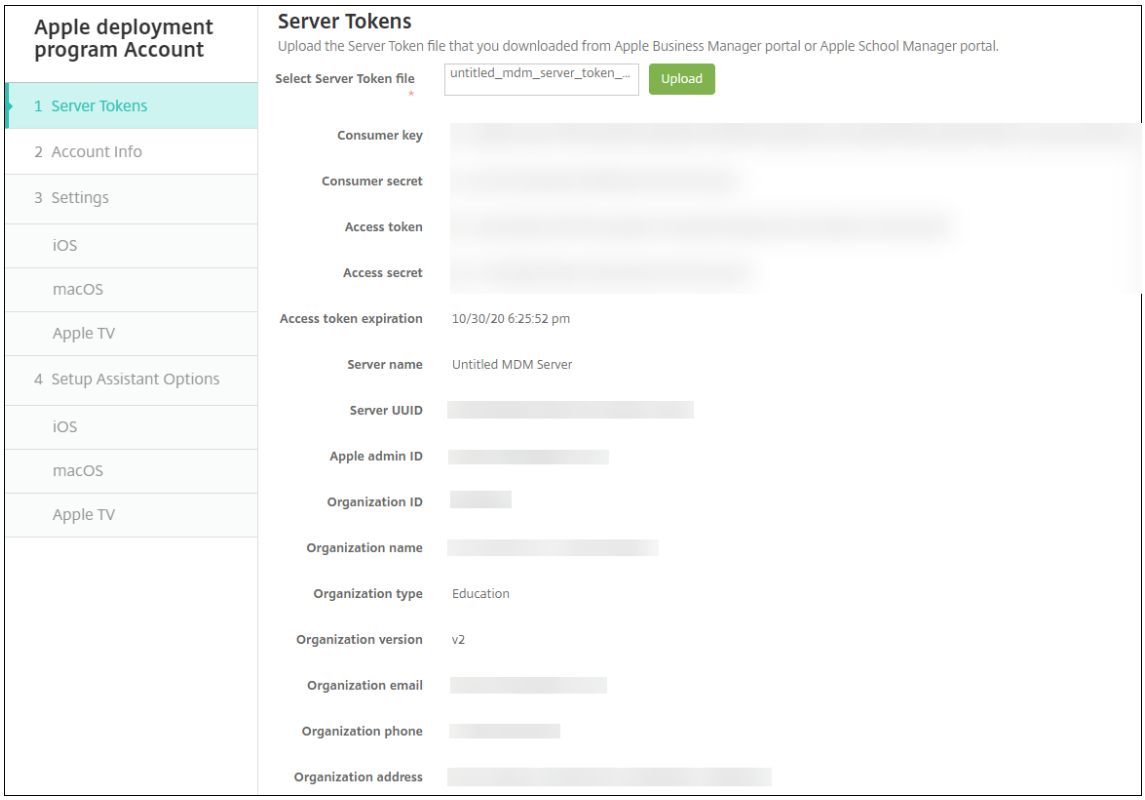
Puede agregar varias cuentas de ABM a XenMobile. Esta función permite utilizar distintos parámetros de inscripción y opciones del asistente de instalación según el país y el departamento, entre otros. A continuación, puede asociar las cuentas de ABM con distintas directivas de dispositivo.

Por ejemplo, puede centralizar todas las cuentas de ABM de diferentes países en el mismo servidor de XenMobile, para importar y supervisar todos los dispositivos ABM. Al personalizar los parámetros de inscripción y las opciones del asistente de instalación por departamento, jerarquía organizativa o cualquier otra estructura, las directivas suministran la funcionalidad adecuada a toda la organización y los usuarios reciben la ayuda necesaria.

1. En la consola de XenMobile, vaya a **Parámetros > Programa de implementación de Apple** y, en **Agregar cuenta de Programas de implementación de Apple**, haga clic en **Agregar**.

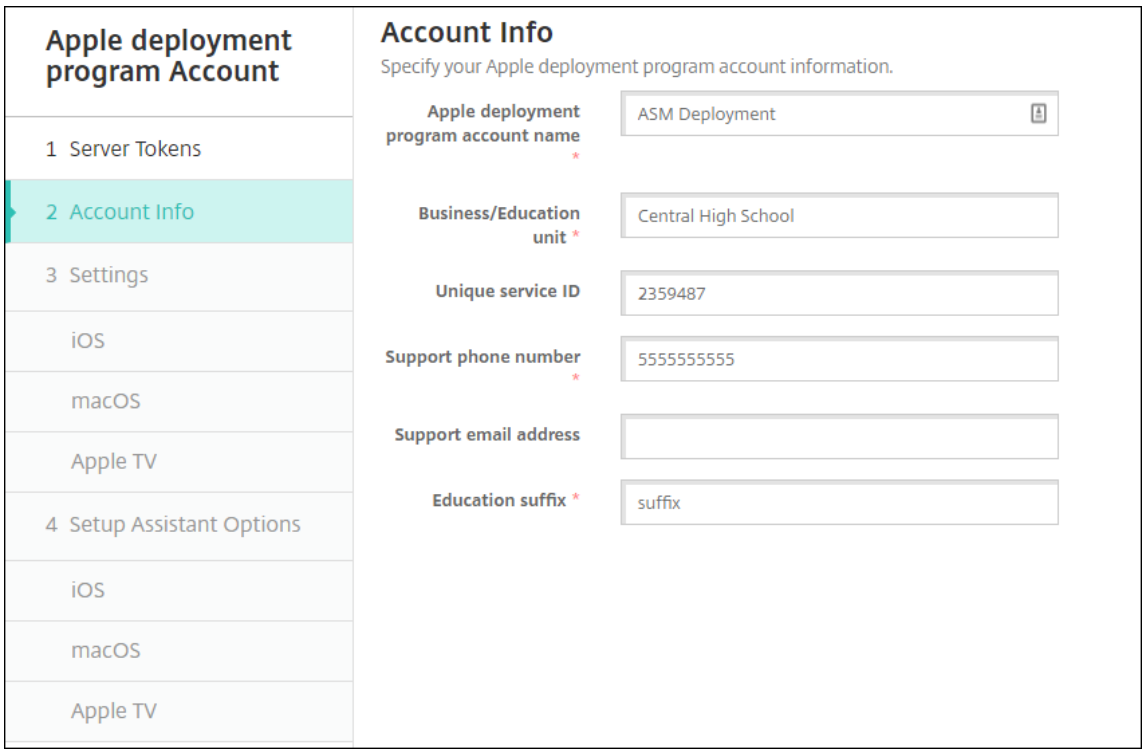


2. En la página **Tokens de servidor**, especifique su archivo de token de servidor y, a continuación, haga clic en **Cargar**.



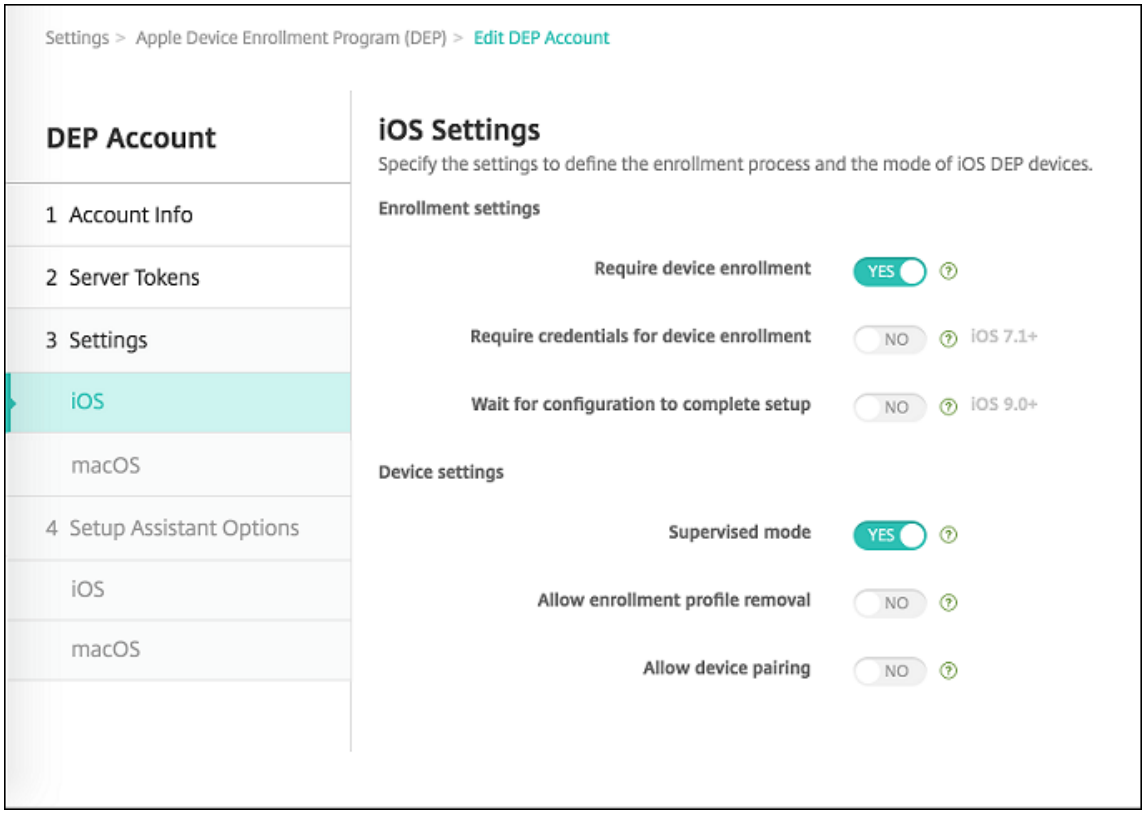
Aparecerá la información del token de servidor.

3. En la página **Información de cuenta**, especifique los siguientes parámetros:



- **Nombre de la cuenta del Programa de implementación de Apple:** Nombre único para esta cuenta del Programa de implementación de Apple. Use nombres que reflejen cómo organiza las cuentas del Programa de implementación de Apple (por ejemplo, por país u organización).
- **Unidad de negocio/educación:** El departamento o la unidad de negocio a la que se asigna el dispositivo. Este campo es obligatorio.
- **ID único de servicio:** Un ID exclusivo optativo para ayudarle a identificar la cuenta.
- **Número de teléfono de asistencia:** Un número de teléfono al que puedan llamar los usuarios para obtener ayuda durante la instalación. Este campo es obligatorio.
- **Dirección de correo electrónico de asistencia:** Una dirección opcional de correo electrónico de asistencia disponible para los usuarios finales.

4. En **Parámetros de iOS**, especifique los siguientes parámetros:



Parámetros de inscripción:

- **Requerir inscripción del dispositivo:** Puede requerir a los usuarios que inscriban sus dispositivos. De forma predeterminada está **activado**.
- **Requerir credenciales para inscripción de dispositivos:** Puede pedir a los usuarios que indiquen sus credenciales durante la configuración de ABM. Citrix recomienda que solicite a todos los usuarios que introduzcan sus credenciales durante la inscripción de dispositivos, permitiendo así que solo usuarios autorizados inscriban dispositivos. De forma predeterminada está **activado**.

  Si habilita ABM antes de la configuración y no selecciona esta opción, XenMobile crea los componentes de ABM. Este proceso de creación incluye componentes como usuario de ABM, Secure Hub, inventario de software y grupo de implementación de ABM. Si selecciona esta opción, XenMobile no crea los componentes. Como resultado, si posteriormente desactiva esta opción, los usuarios que no hayan introducido sus credenciales no podrán realizar la inscripción en ABM porque esos componentes de ABM no existen. Para agregar componentes de ABM, en ese caso es necesario inhabilitar y habilitar la cuenta de ABM.
- **Esperar a que se complete la configuración:** Puede requerir que los dispositivos de los usuarios permanezcan en el modo de asistente de instalación hasta implementar todos los recursos de MDM en ellos. Esta opción está disponible para dispositivos en modo supervisado. De forma predeterminada, está **desactivado**.

- En la documentación de Apple consta que los comandos siguientes pueden no funcionar mientras un dispositivo esté en modo de asistente de instalación:
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

Parámetros del dispositivo:

- **Modo supervisado:** Se debe **activar** si se usa el Apple Configurator para administrar los dispositivos de ABM inscritos o si está habilitada la opción **Esperar a que se complete la configuración**. De forma predeterminada está **activado**. Para obtener información sobre cómo colocar un dispositivo iOS en modo supervisado, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.
- **Permitir quitar el perfil de inscripción:** Puede permitir que los dispositivos usen un perfil que se pueda quitar de forma remota. De forma predeterminada, está **desactivado**.
- **Permitir emparejamiento de dispositivos:** Seleccione si permitir que los dispositivos inscritos mediante ABM se administren a través de Apple Music y Apple Configurator. De forma predeterminada, está **desactivado**.

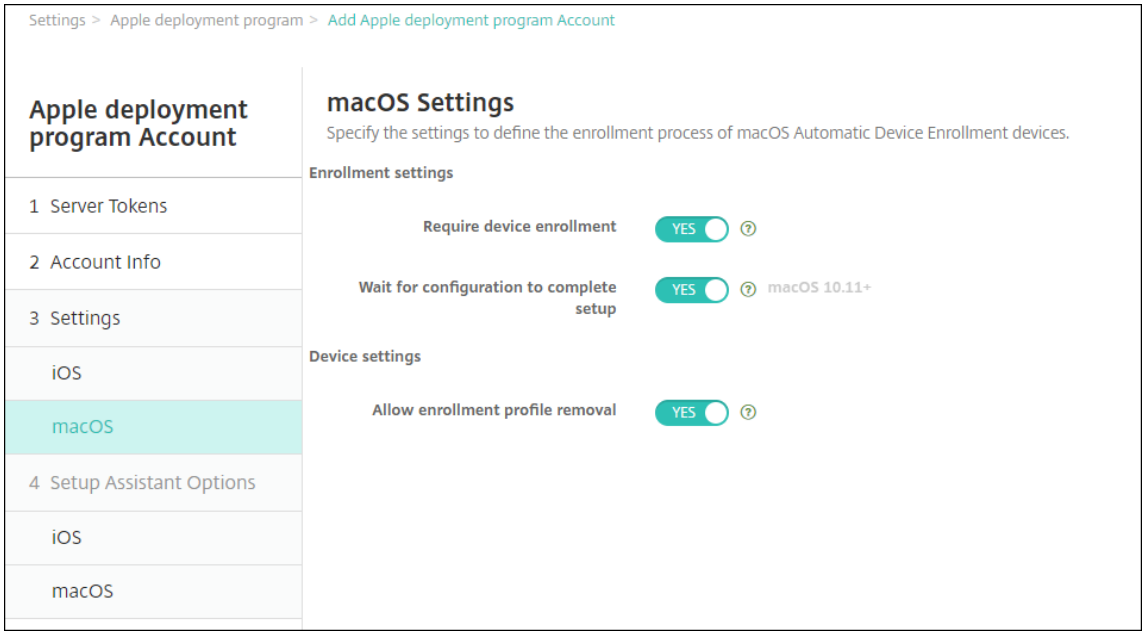
Identidades de supervisión

Si utiliza la herramienta GroundControl, puede agregar un certificado para hacer lo siguiente:

- Anular las restricciones de emparejamiento para evitar el mensaje “Confiar en este host”.
- Ampliar las acciones del dispositivo administrado por USB para que se puedan realizar acciones (como instalar perfiles sin interacción del usuario). Eso permite que GroundControl habilite el modo de aplicación única y el bloqueo del dispositivo hasta desprotegerlo.
- Restaurar una copia de seguridad en los dispositivos de ABM.

Para obtener más información sobre GroundControl, consulte el sitio web de GroundControl.

5. En **Parámetros de macOS**, especifique los siguientes parámetros:



Parámetros de inscripción:

- **Requerir inscripción del dispositivo:** Puede requerir a los usuarios que inscriban sus dispositivos. De forma predeterminada está **activado**.
- **Esperar a que se complete la configuración:** Si está **activado**, el dispositivo macOS no continúa con el Asistente de instalación hasta que el código de acceso a recursos MDM se implementa en el dispositivo. Esa implementación ocurre antes de la creación de la cuenta local. Esta configuración está disponible para macOS 10.11 y versiones posteriores. De forma predeterminada, está **desactivado**.

Parámetros del dispositivo:

- **Permitir quitar el perfil de inscripción:** Puede permitir que los dispositivos usen un perfil que se pueda quitar de forma remota. De forma predeterminada, está **desactivado**.

6. En **Opciones del asistente de configuración de iOS**, seleccione los pasos a omitir del Asistente de configuración de iOS cuando los usuarios inicien sus dispositivos por primera vez. Cuando se omite una pantalla, la función relacionada utiliza la configuración predeterminada. Los usuarios pueden configurar las funciones omitidas una vez finalizada la instalación, a menos que restrinja el acceso a esas funciones por completo. Para obtener más información sobre cómo restringir el acceso a funciones, consulte Directiva de restricciones. Se borra el valor predeterminado de todos los elementos. Las siguientes descripciones explican lo que ocurre cuando se selecciona un parámetro.

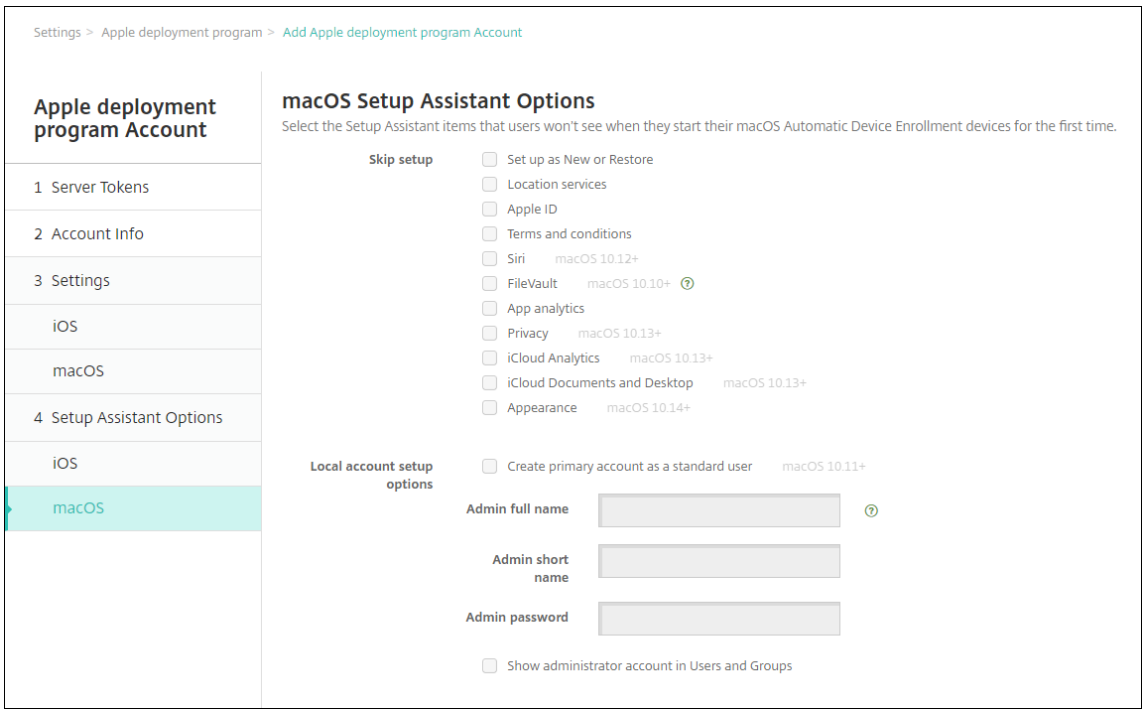
- **Servicios de localización:** Impide a los usuarios configurar el servicio de localización en el dispositivo.
- **Touch ID:** Impide que los usuarios configuren Touch ID o Face ID en dispositivos iOS.
- **Bloqueo de código de acceso:** Impide que los usuarios establezcan un código de acceso para el dispositivo. Si no existe ningún código, los usuarios no pueden usar Touch ID o Apple Pay.
- **Definir como nuevo o Restaurar:** Impide que los usuarios configuren el dispositivo como nuevo o a partir de una copia de seguridad de iCloud o del App Store de Apple.
- **Mover desde Android:** Impide que los usuarios transfieran datos de un dispositivo Android a un dispositivo iOS. Esta opción solo está disponible cuando la opción **Definir como nuevo o Restaurar** está seleccionada (es decir, se omite el paso).
- **ID de Apple:** Impide que los usuarios establezcan una cuenta de ID de Apple gestionado para el dispositivo.
- **Términos y condiciones:** Impide que los usuarios lean y acepten los términos y condiciones de uso del dispositivo.
- **Apple Pay:** Impide que los usuarios configuren Apple Pay. Si se desactiva esta opción, los usuarios deben configurar Touch ID y Apple ID. Compruebe que esos parámetros estén desactivados.
- **Siri:** Impide que el usuario configure Siri.
- **App Analytics:** Impide a los usuarios configurar si se pueden compartir los datos de fallos y estadísticas de uso con Apple.
- **Zoom de presentación:** Impide a los usuarios configurar la resolución de la pantalla (estándar o ampliada) en los dispositivos iOS.
- **True Tone:** Impide que los usuarios establezcan sensores de cuatro canales para ajustar dinámicamente el balance de blancos de la pantalla.
- **Botón de inicio:** Impide que los usuarios establezcan el estilo de retroalimentación del

botón de inicio.

- **Nuevas funciones destacadas:** Impide que los usuarios vean las pantallas que muestran información sobre las nuevas funciones del software Apple.
- **Privacidad:** Impide que los usuarios vean el panel de datos y privacidad. Para iOS 11.3 y versiones posteriores.
- **Actualización de software:** Impide que los usuarios actualicen iOS a la versión más reciente. Para iOS 12.0 y versiones posteriores.
- **Screen Time:** Impide que los usuarios activen Screen Time. Para iOS 12.0 y versiones posteriores.
- **Configuración de SIM:** Impide que los usuarios configuren un plan de datos móviles. Para iOS 12.0 y versiones posteriores.
- **iMessage y FaceTime:** Impide que el usuario vea la pantalla iMessage y FaceTime. Para iOS 12.0 y versiones posteriores.
- **Apariencia:** Impide que los usuarios seleccionen el modo de apariencia. Para iOS 13.0 y versiones posteriores.
- **Bienvenida:** Impide que el usuario vea la pantalla **Cómo empezar**. Para iOS 13.0 y versiones posteriores.
- **Restauración completada:** Impide que los usuarios vean si una restauración se completa durante la instalación. Para iOS 14.0 y versiones posteriores.
- **Actualización completada:** Impide que los usuarios vean si una actualización de software se completa durante la instalación. Para iOS 14.0 y versiones posteriores.

La cuenta de ABM aparece en **Parámetros > Programa de implementación de Apple**.

7. En **Opciones del asistente de configuración de macOS**, seleccione los pasos a omitir del Asistente de configuración de macOS cuando los usuarios inicien sus dispositivos por primera vez. Cuando se omite una pantalla, la función relacionada utiliza la configuración predeterminada. Los usuarios pueden configurar las funciones omitidas una vez finalizada la instalación, a menos que restrinja el acceso a esas funciones por completo. Para obtener más información sobre cómo restringir el acceso a funciones, consulte Directiva de restricciones. Se borra el valor predeterminado de todos los elementos. Las siguientes descripciones explican lo que ocurre cuando se selecciona un parámetro.



- **Definir como nuevo o Restaurar:** Impide que los usuarios configuren el dispositivo como nuevo o a partir de una copia de seguridad de Time Machine o migren el sistema.
- **Servicios de localización:** Impide a los usuarios configurar el servicio de localización en el dispositivo. Para macOS 10.11 y versiones posteriores.
- **ID de Apple:** Impide que los usuarios establezcan una cuenta de ID de Apple gestionado para el dispositivo.
- **Términos y condiciones:** Impide que los usuarios lean y acepten los términos y condiciones de uso del dispositivo.
- **Siri:** Impide que el usuario configure Siri. Para macOS 10.12 y versiones posteriores:
- **FileVault:** Usar FileVault para cifrar el disco de arranque. XenMobile aplica el parámetro FileVault si el sistema tiene una única cuenta de usuario local y esa cuenta se ha registrado en iCloud.

  Puede usar la funcionalidad de cifrado de disco FileVault en macOS para proteger el volumen del sistema mediante el cifrado de su contenido (https://support.apple.com/en-us/HT204837). Si ejecuta el Asistente de configuración en un modelo reciente de portátil Mac donde FileVault está desactivado, puede que le aparezca una solicitud para que habilite esta función. El mensaje aparece tanto en sistemas nuevos como en sistemas actualizados a OS X 10.10 o 10.11, pero solo si el sistema tiene una sola cuenta de administrador local y esa cuenta está registrada en iCloud.
- **App Analytics:** Impide a los usuarios configurar si se pueden compartir los datos de fallos

y estadísticas de uso con Apple.

- **Privacidad:** Impide que los usuarios vean el panel Datos y privacidad. Para macOS 10.13 y versiones posteriores.
- **Análisis de iCloud:** Impide que los usuarios elijan si enviar o no datos de diagnóstico de iCloud a Apple. Para macOS 10.13 y versiones posteriores.
- **Escritorio y documentos de iCloud:** Impide que los usuarios configuren el escritorio y los documentos de iCloud. Para macOS 10.13 y versiones posteriores.
- **Apariencia:** Impide que los usuarios seleccionen el modo de apariencia. Para macOS 10.14 y versiones posteriores.
- **Accesibilidad:** Impide que el usuario escuche VoiceOver automáticamente. Solo está disponible si el dispositivo está conectado a Ethernet. Para macOS 11 y versiones posteriores.
- **Biometría:** Impide que el usuario configure Touch ID y Face ID. Para macOS 10.12.4 y versiones posteriores:
- **True Tone:** Impide que los usuarios establezcan sensores de cuatro canales para ajustar dinámicamente el balance de blancos de la pantalla. Para macOS 10.13.6 y versiones posteriores.
- **Apple Pay:** Impide que los usuarios configuren Apple Pay. Si se desactiva esta opción, los usuarios deben configurar Touch ID y Apple ID. Asegúrese de que los parámetros **ID de Apple** y **Biometría** estén desactivados. Para macOS 10.12.4 y versiones posteriores:
- **Screen Time:** Impide que los usuarios activen Screen Time. Para macOS 10.15 y versiones posteriores:
- **Opciones de configuración de cuenta local:** Especifique los parámetros para crear una cuenta de administrador en el dispositivo. Los usuarios inician sesión en sus dispositivos macOS con esta información. XenMobile crea la cuenta a partir de la información especificada.
  - **Crear cuenta principal como usuario estándar:** En lugar de conceder a este usuario privilegios de administrador en el dispositivo, XenMobile crea el usuario con permisos estándar. Puesto que macOS requiere una cuenta de administrador, XenMobile crea primero una cuenta de administrador y, a continuación, crea una nueva cuenta estándar y la establece como principal.
  - **Nombre completo del administrador:** Escriba el nombre que mostrará el sistema para la cuenta de administrador.
  - **Nombre corto del administrador** Escriba el nombre que mostrará el dispositivo para la carpeta particular y en el shell.

- **Contraseña del administrador:** Introduzca una contraseña segura para la cuenta de administrador.
- **Mostrar la cuenta de administrador en Usuarios y grupos:** Si no está marcada, la cuenta de administrador no aparece en **Usuarios y grupos** en la configuración de macOS. Si crea la cuenta principal como usuario estándar, habilite esta opción para ocultar la cuenta de administrador que XenMobile crea en primer lugar.

Adquirir dispositivos habilitados para el Programa de implementación

Puede adquirir dispositivos habilitados para el Programa de implementación directamente desde Apple o de proveedores y operadores autorizados habilitados para el Programa de implementación. Para realizar el pedido en Apple, proporcione su ID de cliente de Apple en el portal del Programa de implementación de Apple. Su ID de cliente permite a Apple asociar los dispositivos adquiridos a la cuenta del Programa de implementación de Apple.

Para adquirirlos de un proveedor o de un operador autorizado de Apple, póngase en contacto con ellos para ver si participan en el Programa de implementación de Apple. Pida el ID del Programa de implementación de Apple del proveedor cuando compre los dispositivos. Apple necesitará este dato para agregar el proveedor del Programa de implementación de Apple a su cuenta del Programa de implementación de Apple. Después de agregar el ID del Programa de implementación de Apple del proveedor, recibirá un ID de cliente del Programa de implementación. Suministre su ID de cliente del Programa de implementación al proveedor, que lo usará para enviar información sobre sus compras de dispositivos a Apple. Para obtener más información, consulte este sitio de Apple sobre el uso de la inscripción de dispositivos.

Administrar dispositivos habilitados para el Programa de implementación

Una vez que se envíe el pedido, podrá asociar dispositivos iOS, iPadOS y macOS al servidor de XenMobile.

1. Inicie sesión en Apple Business Manager con una cuenta de administrador o de administrador de inscripción de dispositivos.
2. En la barra lateral, haga clic en **Devices**. Los dispositivos comprados directamente en Apple aparecerán automáticamente. Para asignar dispositivos de Apple Configurator 2 a Apple Business Manager, consulte Manual de uso de Apple Business Manager.
3. En la lista, seleccione un dispositivo o el número total de dispositivos y haga clic en **Edit Device Management**. Tiene dos opciones:
   - Para asignar un dispositivo a un servidor MDM, en **Assign to Server**, elija el nombre del servidor de XenMobile. Haga clic en **Continue**.
     Para asignar nuevos dispositivos a Apple Business Manager en bloque, establezca un servidor de XenMobile predeterminado para la implementación. Para obtener más informa-

ción, consulte Establecer un servidor predeterminado para la inscripción en bloque.

- Para desasignar un dispositivo del servidor de XenMobile, elija **Unassign**.

Sus dispositivos del Programa de implementación de Apple están ahora asociados al servidor de XenMobile seleccionado.

Si envía un dispositivo iOS, iPadOS o macOS para tareas de mantenimiento o reparación, debe quitarlo de Apple Business Manager. Cuando lo reciba de vuelta, deberá reasignarlo al servidor de XenMobile. Al reemplazar el dispositivo, puede asignar un nuevo dispositivo al servidor de XenMobile mediante un número de pedido.

Para revisar el historial de dispositivos asignados:

1. Inicie sesión en Apple Business Manager con una cuenta de administrador o de administrador de inscripción de dispositivos.
2. En la barra lateral, haga clic en **Assignment History**. A continuación, elija una asignación para ver más información.
3. Haga clic en **Download** para descargar un archivo CSV con los números de serie de todos los dispositivos asignados y no asignados.

Puede quitar dispositivos iOS, iPadOS y macOS de Apple Business Manager si el dispositivo se ha vendido, robado o no se puede reparar.

1. Inicie sesión en Apple Business Manager con una cuenta de administrador o de administrador de inscripción de dispositivos.
2. En la barra lateral, haga clic en **Devices** y busque un dispositivo.
3. Seleccione un dispositivo y haga clic en **Release Device**. En el cuadro de diálogo, confirme los cambios para quitar el dispositivo del programa. Para volver a agregar dispositivos iOS y iPadOS, use Apple Configurator 2. No puede volver a agregar dispositivos macOS con Apple Configurator 2.

Inscribir dispositivos

January 4, 2022

Para poder administrar dispositivos de usuario de forma remota y segura, dichos dispositivos deben inscribirse en XenMobile. El software cliente de XenMobile debe estar instalado en el dispositivo del usuario y el usuario debe haberse autenticado. Entonces, se instalan ambos, XenMobile y el perfil del usuario. A continuación, puede realizar tareas de administración de dispositivos desde la consola de XenMobile. Puede aplicar directivas, implementar aplicaciones, insertar datos en el dispositivo, bloquearlo, borrarle los datos y localizar dispositivos perdidos o robados.

Se admite la inscripción de Azure Active Directory para dispositivos iOS, Android, Windows 10 y Windows 11. Para obtener más información sobre cómo configurar Azure como proveedor de identidades (IdP), consulte Integración de XenMobile con Azure Active Directory como proveedor de identidades.

> **Nota:**
>
> Antes de poder inscribir usuarios de dispositivos iOS, debe solicitar un certificado APNs. Para obtener información más detallada, consulte Certificados y autenticación.

Puede actualizar las opciones de configuración de usuarios y dispositivos desde la página **Administrar > Invitaciones de inscripción**. Para obtener más información, consulte Enviar una invitación de inscripción en este artículo.

Dispositivos Android

> **Nota:**
>
> Para obtener información sobre la inscripción de dispositivos Android Enterprise, consulte Android Enterprise.

1. Vaya a Google Play Store en el dispositivo Android, descargue la aplicación Citrix Secure Hub y toque la aplicación para abrirla.
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 **Abrir**.
4. Introduzca las credenciales de empresa, como el nombre del servidor de XenMobile Server de su empresa, el nombre principal de usuario (UPN) o su dirección de correo electrónico. 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. Es posible que tenga que crear un PIN de Citrix (según la configuración de XenMobile). Puede usar el PIN para iniciar sesión en Secure Hub y en otras aplicaciones habilitadas para XenMobile, como Secure Mail y Citrix Files. Deberá introducir su PIN de Citrix dos veces. En la pantalla **Crear PIN de Citrix**, introduzca un PIN.
8. Vuelva a escribir el PIN. Se abrirá Secure Hub. Entonces, podrá acceder a XenMobile Store para ver las aplicaciones que puede instalar en el dispositivo Android.
9. Si ha configurado XenMobile de manera que las aplicaciones se envíen automáticamente a los dispositivos de los usuarios después de la inscripción, los usuarios verán mensajes con solicitudes de instalación de las aplicaciones. Además, las directivas que configure en XenMobile se implementan en el dispositivo. Toque **Instalar** para instalar las aplicaciones.

Para inscribir y reinscribir un dispositivo Android

Los usuarios pueden desinscribirse una vez dentro de Secure Hub. Cuando los usuarios se desinscriben con el siguiente procedimiento, el dispositivo sigue apareciendo en el inventario de dispositivos en la consola de XenMobile. No obstante, no es posible realizar acciones en el dispositivo. No puede realizar un seguimiento del dispositivo ni supervisar su estado de cumplimiento.

1. Toque Secure Hub para abrir la aplicación.
2. Dependiendo de si dispone de un teléfono o una tableta, lleve a cabo lo siguiente:

   En un teléfono:

   - Deslice desde la izquierda de la pantalla para abrir un panel de configuración.
   - Toque **Preferencias** > **Cuentas**. A continuación, toque **Eliminar cuenta**.

   En una tableta:

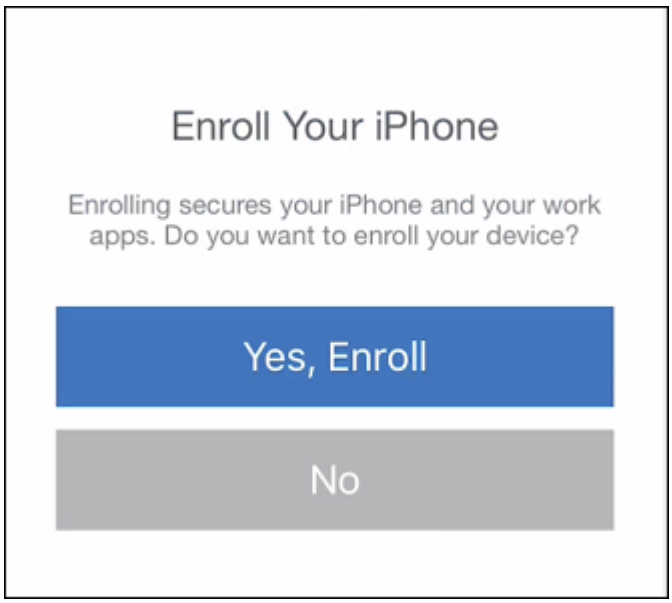
   - Toque la flecha situada junto a su dirección de correo electrónico en la esquina superior derecha.
   - Toque **Preferencias** > **Cuentas**. A continuación, toque **Eliminar cuenta**.
3. Toque **Reinscribir**. Aparecerá un mensaje para confirmar que quiere volver a inscribir el dispositivo.
4. Toque **Aceptar**.

   El dispositivo está desinscrito.
5. Siga las instrucciones que aparecen en la pantalla para reinscribir el dispositivo.

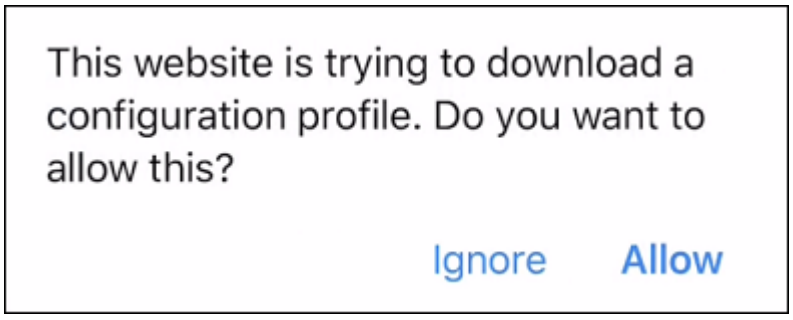
Inscribir dispositivos iOS

En esta sección se muestra cómo los usuarios inscriben dispositivos iOS (12.2 o una versión posterior) en XenMobile Server. Para obtener más información sobre la inscripción en iOS, abra el siguiente vídeo:

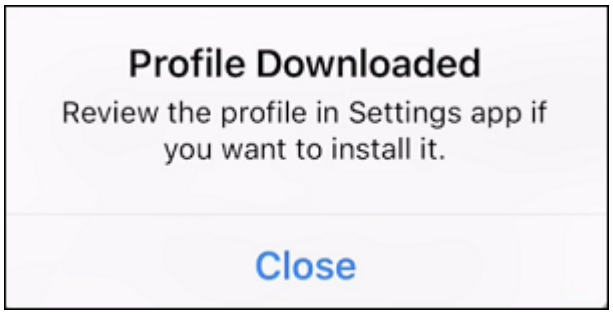
1. Vaya a la tienda Apple en su dispositivo iOS, descargue la aplicación Citrix Secure Hub y, a continuación, toque la aplicación.
2. Cuando se le pida instalar la aplicación, toque **Siguiente** y, a continuación, en **Instalar**.
3. Después de que Secure Hub se instale, toque **Abrir**.
4. Introduzca las credenciales de empresa, como el nombre del servidor de XenMobile Server de su empresa, el nombre principal de usuario (UPN) o su dirección de correo electrónico. A continuación, haga clic en **Siguiente**.
5. Toque **Sí, inscribirlo** para inscribir el dispositivo iOS.



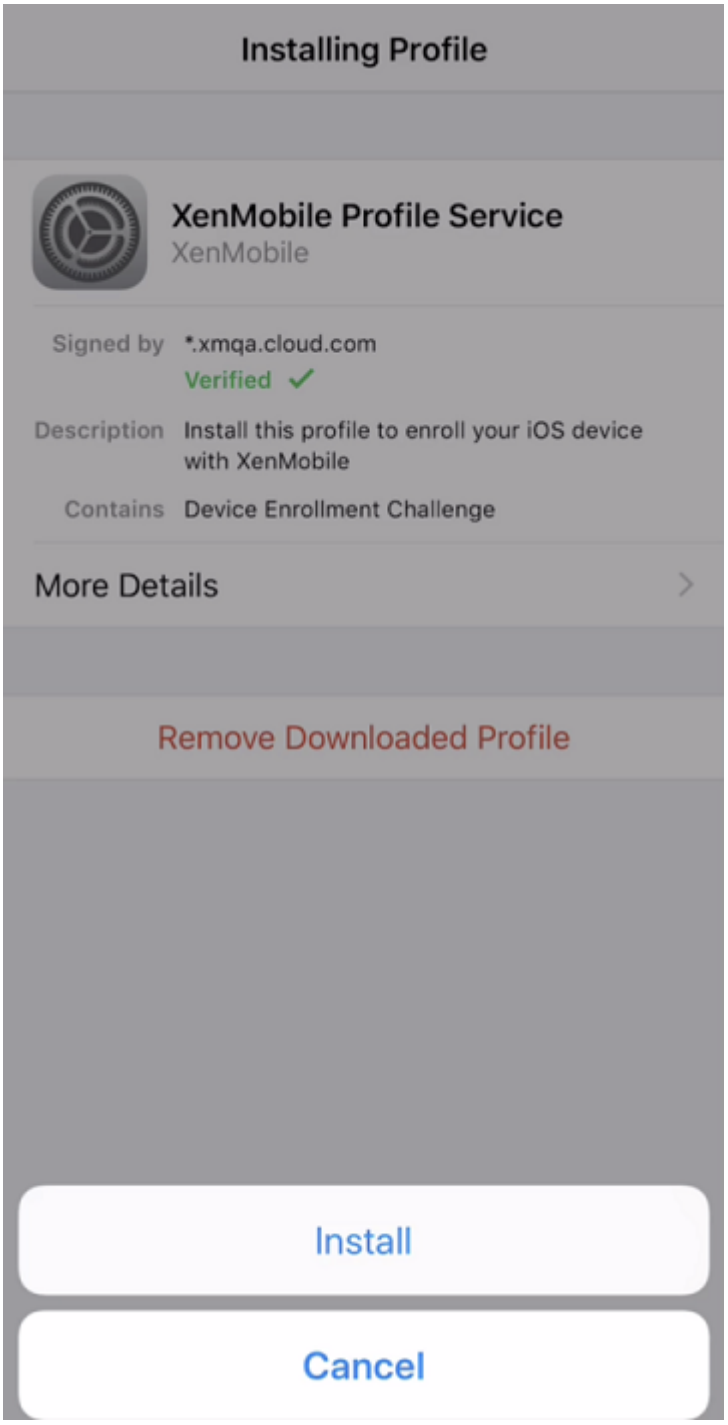
6. Después de escribir las credenciales, toque **Permitir** cuando se le pida para descargar el perfil de configuración.



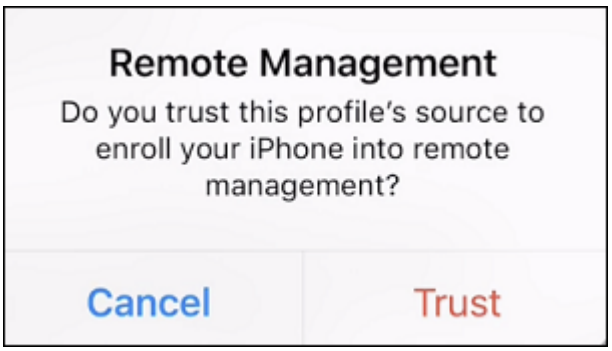
7. Después de descargar el perfil de configuración, toque **Cerrar**.



8. En la configuración del dispositivo, instale el certificado de iOS y agregue el dispositivo a la lista de confianza.
    - Vaya a **Configuración > General > Perfil > XenMobile Profile Service** y toque **Instalar** para agregar el perfil.



- En la ventana de notificaciones, toque **Confiar** para inscribir el dispositivo en la administración remota.



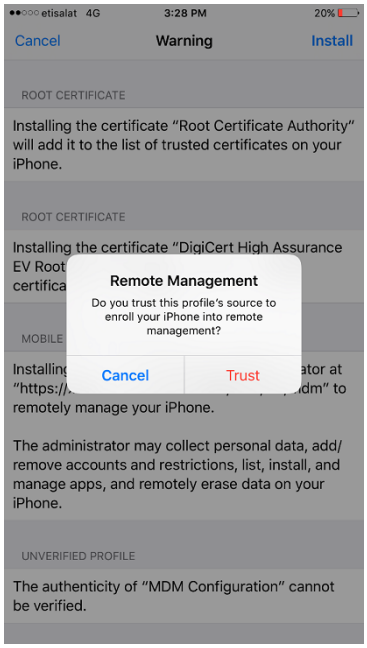
9. Inicie sesión en Secure Hub. Si inscribe dispositivos en MDM+MAM: Una vez que se hayan validado las credenciales, cree el PIN de Citrix y confírmelo cuando se le solicite.
10. Una vez completado el flujo de trabajo, el dispositivo está inscrito. Ahora, puede acceder al almacén de aplicaciones para ver las aplicaciones que puede instalar en el dispositivo iOS.

Dispositivos iOS

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 la aplicación Secure Hub.
3. Cuando se abra Secure Hub, 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 **Siguiente**.
5. Cuando se le solicite la inscripción, haga clic en **Sí, inscribirlo** y, a continuación, introduzca sus credenciales cuando se le pidan.
6. Toque **Instalar** para instalar el servicio de perfiles de Citrix.

7. Toque **Confiar**.



8. Toque **Abrir** e introduzca sus credenciales.

Dispositivos macOS

XenMobile ofrece dos métodos para inscribir dispositivos que ejecutan macOS. Ambos métodos permiten a los usuarios de macOS inscribirse de forma inalámbrica y directamente desde sus dispositivos.

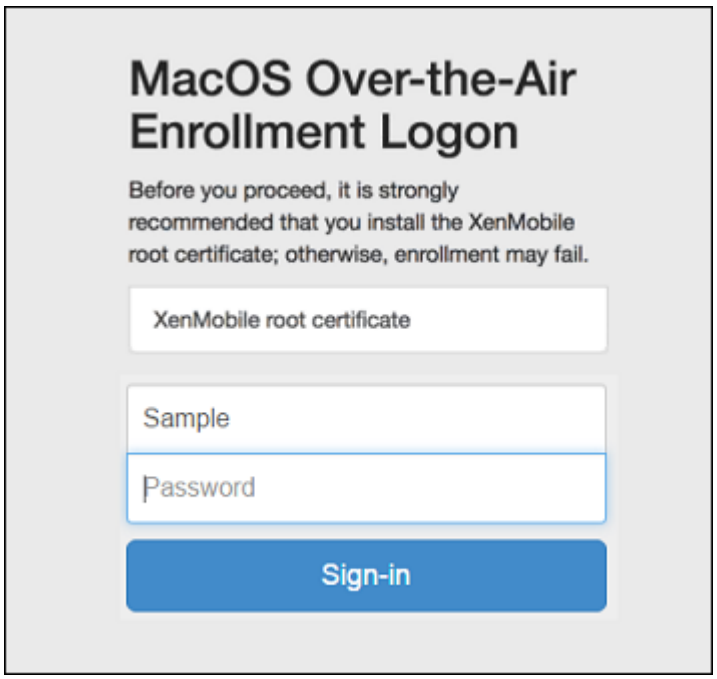
- **Enviar una invitación de inscripción a los usuarios:** Este método de inscripción permite definir uno de estos modos de seguridad de inscripción para dispositivos macOS:
  - Nombre de usuario y contraseña
  - Nombre de usuario + PIN
  - Dos factores

  Cuando el usuario siga las instrucciones de la invitación a la inscripción, aparecerá una pantalla de inicio de sesión con el nombre de usuario ya rellenado.
- **Enviar un enlace de instalación a los usuarios.** Este método de inscripción para dispositivos macOS envía a los usuarios un enlace de inscripción, que pueden abrir en los exploradores web Safari o Chrome. A continuación, el usuario se inscribe suministrando su nombre de usuario y contraseña.

  Para impedir que se use un enlace de inscripción para dispositivos macOS, defina la propiedad de servidor **Enable macOS OTAE** en **False**. Como resultado, los usuarios de macOS solo podrán inscribirse mediante una invitación de inscripción.

Enviar una invitación de inscripción a los usuarios

1. Si quiere, puede configurar directivas de dispositivo para macOS en la consola de XenMobile. Consulte Directivas de dispositivo para obtener más información acerca de las directivas de dispositivo.
2. Agregue una invitación para la inscripción de usuarios de macOS. Para obtener más información, consulte Enviar una invitación de inscripción en este artículo.
3. Cuando los usuarios reciban la invitación y hagan clic en el enlace, aparecerá la siguiente pantalla en el explorador Safari. XenMobile rellena el nombre de usuario. Si eligió **Dos factores** como modo de seguridad de inscripción, aparecerá un campo adicional.



4. Los usuarios deben instalar certificados según sea necesario. La solicitud a los usuarios para instalar certificados depende de si se ha configurado un certificado SSL público de confianza y un certificado de firma digital público de confianza para macOS. Para obtener más información acerca de los certificados, consulte Certificados y autenticación.
5. Los usuarios proporcionan las credenciales solicitadas.

   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.

Enviar un enlace de instalación a los usuarios

1. Si quiere, puede configurar directivas de dispositivo para macOS en la consola de XenMobile. Consulte Directivas de dispositivo para obtener más información acerca de las directivas de dispositivo.
2. Envíe el enlace de inscripción `https://serverFQDN:8443/instanceName/macos/otae`, que los usuarios abrirán en los exploradores web Safari o Chrome.

   - **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 puerto, en lugar de 8443.
   - El elemento **instanceName** a menudo se muestra como zdm y es el nombre que se especificó 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. Si ha configurado un certificado SSL público de confianza y un certificado de firma digital público de confianza para iOS y macOS, los usuarios verán el mensaje que pide instalar los certificados. Para obtener más información acerca de los certificados, consulte Certificados y autenticación.
4. Los usuarios inician sesión en su Mac.

   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

> **Nota:**
>
> Esta sección contiene referencias a dispositivos Windows Phone 8.1, que Microsoft dejó de desarrollar el 11 de julio de 2017. XenMobile admite dispositivos Windows Phone 8.1 solo para la inscripción MDM.

Los dispositivos con Windows 10 o Windows 11 se inscriben en Azure como método federado de la autenticación de Active Directory. Puede unir dispositivos con Windows 10 y Windows 11 a Microsoft Azure Active Directory de estas 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 se haya configurado.

En XenMobile, puede inscribir dispositivos que ejecuten los siguientes sistemas operativos Windows:

- Windows Phone 10
- Windows 10
- Windows 11
- Windows Phone 8.1

Los usuarios pueden inscribirse directamente a través de sus dispositivos.

> **Nota:**
>
> Para Windows 10 RS2 Phone y Tablet, durante la reinscripción, no se solicita al usuario que introduzca la URL del servidor. Para solucionar este problema, reinicie el dispositivo. O bien, en la pantalla de dirección del correo electrónico, toque la X situada al otro lado de **Conectando con un servicio** para ir a la página "Dirección URL del servidor". Este es un problema de terceros.

Debe configurar la detección automática y el servicio de detección de Windows para la inscripción de usuarios con el fin de permitir la administración de los dispositivos Windows admitidos.

Para que los usuarios de dispositivos Windows puedan inscribir sus dispositivos mediante Azure, debe configurar los parámetros del servidor Microsoft Azure en XenMobile. Para obtener más información, consulte Parámetros del servidor Microsoft Azure Active Directory.

Para inscribir dispositivos Windows con detección automática

Para habilitar la administración de dispositivos Windows, Citrix recomienda configurar Autodiscovery Service y el servicio de detección de Windows. Para obtener más información, consulte Servicio de detección automática de XenMobile.

1. En el dispositivo, busque e instale todas las actualizaciones disponibles de Windows.
2. Para Windows 10 y Windows 11: En el menú Accesos, toque **Configuración** > **Cuentas > Obtener acceso a trabajo o escuela > Conectarse a la red del trabajo o colegio**. Para teléfonos Windows 8.1: Toque **Configuración de PC > Red > Área de trabajo**.
3. Para Windows 10 y Windows 11: Escriba la dirección de correo electrónico de su empresa y toque **Continuar**. Para Windows 8.1: Toque **Activar administración de dispositivos**. Para inscribirse como un usuario local, introduzca una dirección de correo electrónico que no exista y un nombre de dominio correcto (por ejemplo, `foo@mydomain.com`). Esto le permite omitir una limitación conocida de Microsoft, por la que la inscripción se realiza en la Administración de dispositivos nativa de Windows; en el cuadro de diálogo **Conectando con un servicio**, escriba el nombre de usuario y la contraseña asociados al usuario local. El dispositivo detecta automáticamente un servidor de XenMobile Server y comienza el proceso de inscripción.
4. Introduzca la contraseña. Utilice la contraseña asociada a una cuenta que forme parte de un grupo de usuarios en XenMobile.
5. Para Windows 10 y Windows 11: En el cuadro de diálogo **Condiciones de uso**, indique que acepta que el dispositivo sea administrado y, a continuación, toque **Aceptar**. Para Windows 8.1: En el cuadro de diálogo **Permitir aplicaciones y servicios del administrador de TI**, indique que acepta que el dispositivo sea administrado y, a continuación, toque **Activar**.

Para inscribir dispositivos Windows sin detección automática

Puede inscribir dispositivos Windows sin detección automática. Sin embargo, Citrix recomienda configurar la detección automática. La inscripción sin la detección automática consiste en una llamada al puerto 80 antes de conectarse a la URL pertinente, por lo que no se aconseja para una implementación de producción. Citrix recomienda utilizar este proceso solo en entornos de prueba y en el contexto de una implementación de prueba de concepto.

1. En el dispositivo, busque e instale todas las actualizaciones disponibles de Windows.
2. Para Windows 10 y Windows 11: En el menú Accesos, toque **Configuración** > **Cuentas > Obtener acceso a trabajo o escuela > Conectarse a la red del trabajo o colegio**. Para Windows 8.1: Toque **Configuración de PC > Red > Área de trabajo**.
3. Introduzca la dirección de correo electrónico de empresa.

4. Para Windows 10 y Windows 11: Si no se ha configurado la detección automática, aparecerá una opción donde podrá introducir datos del servidor, como se describe en el paso 5. Para Windows 8.1: Si la opción de **detectar la dirección del servidor automáticamente** está **activada**, tóquela para **desactivarla**.
5. Para Windows 10 y Windows 11: En el campo **Escribir dirección del servidor**, escriba la dirección: `https://serverfqdn:8443/serverInstance/wpe`.

   Si se utiliza un puerto que no sea 8443 para las conexiones SSL sin autenticar, utilice ese puerto en lugar de 8443 en esta dirección.

   Para Windows 8.1: Escriba la dirección del servidor en el siguiente formato: `https://serverfqdn:8443/serverInstance/Discovery.svc`.

   Si se utiliza un puerto que no sea 8443 para las conexiones SSL sin autenticar, utilice ese puerto en lugar de 8443 en esta dirección.
6. Escriba la contraseña.
7. Para Windows 10 y Windows 11: En el cuadro de diálogo **Condiciones de uso**, indique que acepta que el dispositivo sea administrado y, a continuación, toque **Aceptar**. Para Windows 8.1: En el cuadro de diálogo **Permitir aplicaciones y servicios del administrador de TI**, indique que acepta que el dispositivo sea administrado y, a continuación, toque **Activar**.

Para inscribir dispositivos Windows Phone

Para inscribir dispositivos Windows Phone en XenMobile, los usuarios necesitan su dirección de correo electrónico y su contraseña de Active Directory o de la red interna. Si la detección automática no está configurada, los usuarios también necesitan la dirección de servidor web de XenMobile Server. 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 Hub empresarial (con una aplicación Secure Hub firmada, la aplicación Windows Phone para cada plataforma que quiera admitir).

1. En la pantalla principal del dispositivo Windows Phone, toque el icono **Configuración**.
   - Para Windows 10 y Windows 11: En función de la versión, toque **Cuentas > Obtener acceso a trabajo o escuela > Conectarse a la red del trabajo o colegio** o toque **Cuentas > Acceso al trabajo > Inscribir en administración de dispositivos (MDM)**.
   - Para Windows 8.1: Toque **Configuración de PC > Red > Área de trabajo**, y después toque **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@mydomain.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 de XenMobile Server, como: `https://<xenmobile_server>:<portnumber>/<instancename>/wpe`. Por ejemplo, `https://mycompany.mdm.com:8443/zdm/wpe`.

   > **Nota:**
   >
   > El número de puerto debe adaptarse a la implementación. 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 **Iniciar sesión**.

5. 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.

6. En Windows Phone 8.1, en la pantalla **Cuenta agregada**, toque **Listo**.

7. 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 de Windows**, 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 Secure Hub desde la pantalla **Todas las aplicaciones**.

Enviar una invitación de inscripción

Desde la consola de XenMobile, puede enviar a los usuarios una invitación para la inscripción de dispositivos iOS, macOS, Android Enterprise y Android antiguo. También puede enviar un enlace de instalación a usuarios con dispositivos iOS, Android Enterprise o Android antiguo.

Las invitaciones de inscripción se envían de la siguiente manera:

- Si la invitación de inscripción es para un usuario local o un usuario de Active Directory: el usuario recibe la invitación por SMS en el número de teléfono y nombre de operador que usted especifique.
- Si la invitación de inscripción es para un grupo: los usuarios reciben invitaciones por SMS. Si los usuarios de Active Directory tienen una dirección de correo electrónico y un número de teléfono móvil en Active Directory, recibirán la invitación. Los usuarios locales reciben la invitación en el número de teléfono y correo electrónico especificado en las propiedades de usuario.

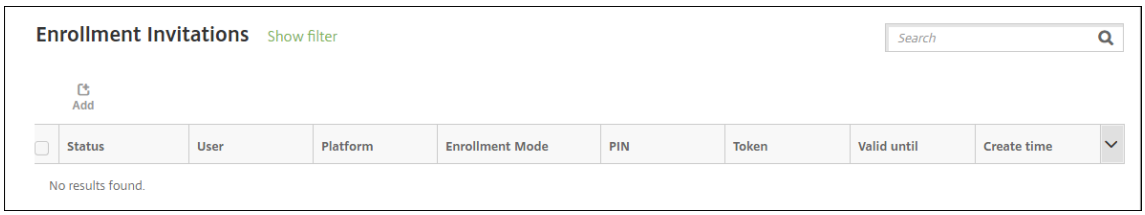
Después de que los usuarios se inscriban, sus dispositivos aparecen como administrados en **Administrar > Dispositivos**. El estado de la URL de invitación aparece como **Canjeado**.

Requisitos previos

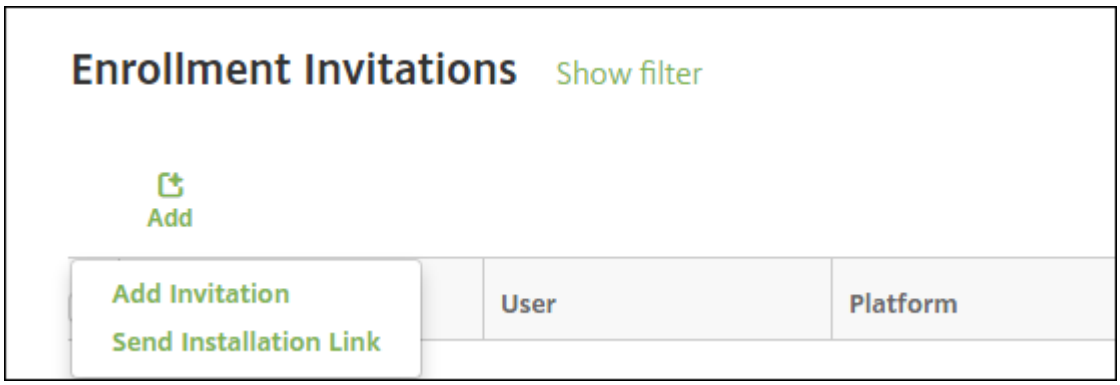
- XenMobile Server configurado en modo Enterprise (XME) o MDM
- LDAP configurado
- Si utiliza grupos y usuarios locales:
  - Uno o varios grupos locales.
  - Usuarios locales asignados a grupos locales.
  - Los grupos de entrega se asocian con grupos locales.
- Si usa Active Directory:
  - Los grupos de entrega se asocian con grupos de Active Directory.

Crear invitación de inscripción

1. En la consola de XenMobile, haga clic en **Administrar > Invitaciones de inscripción**. Aparecerá la página **Invitaciones de inscripción**.



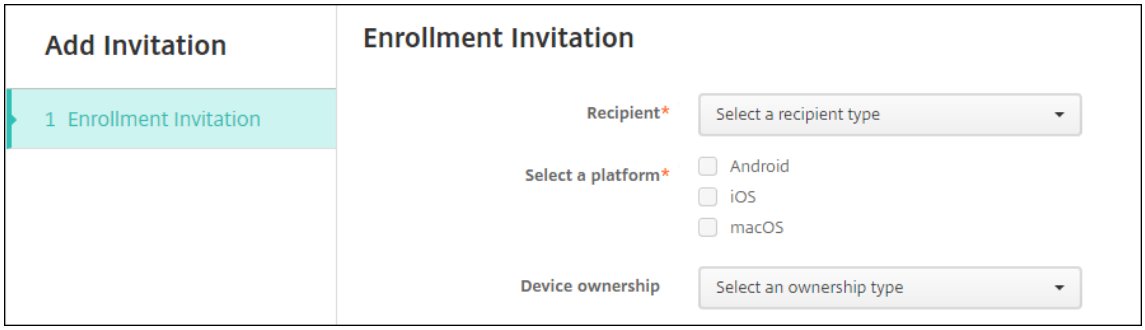
2. Haga clic en **Agregar**. Aparecerá un menú con opciones de inscripción.



- Para enviar una invitación de inscripción a un usuario o un grupo, haga clic en **Agregar invitación**.
- Si quiere enviar un enlace de instalación para la inscripción a una lista de destinatarios a través de SMTP o SMS, haga clic en **Enviar enlace de instalación**.

El envío de invitaciones de inscripción y enlaces de instalación se describe después de estos pasos.

3. Haga clic en **Agregar invitación**. Aparecerá la pantalla **Invitación de inscripción**.

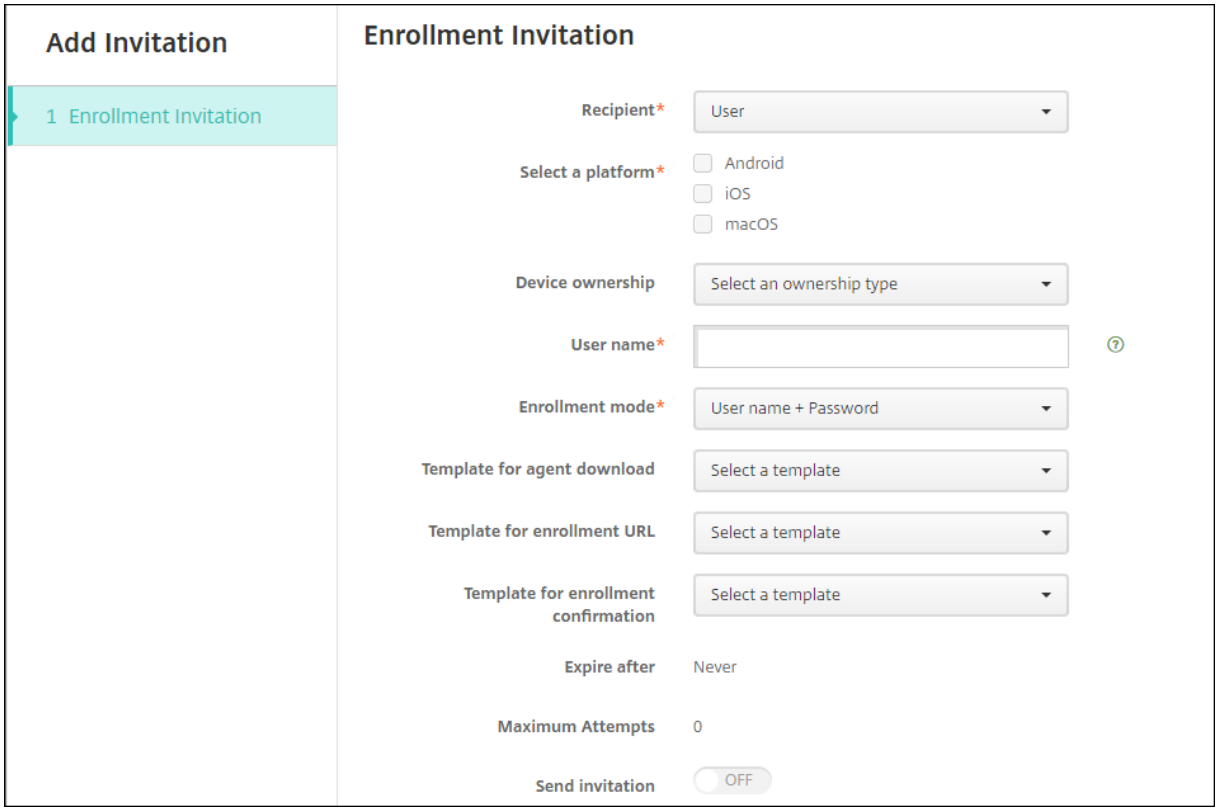


4. Configure estos parámetros:
   - **Destinatario:** Elija **Grupo** o **Usuario**.
   - **Seleccionar una plataforma:** Si el **Destinatario** es un **Grupo**, se seleccionan todas las plataformas. Puede cambiar las plataformas seleccionadas. Si el **Destinatario** es un **Usuario**, no se selecciona ninguna plataforma. Seleccione una plataforma.

     Para crear una invitación de inscripción para dispositivos Android Enterprise, seleccione **Android > Android Enterprise**.
   - **Propietario del dispositivo:** Seleccione **Empresa** o **Empleado**.

   Aparecerán parámetros para usuarios o grupos, como se describe en las secciones siguientes.

Para enviar una invitación de inscripción a un usuario



1. Configure estos parámetros de **Usuario**:
    - **Nombre de usuario:** Escriba un nombre de usuario. Este usuario debe existir como usuario local en XenMobile Server, o como usuario en Active Directory. Si el usuario es local, la propiedad de correo electrónico del usuario debe estar configurada para poder enviarle notificaciones. Si se trata de un usuario de Active Directory, compruebe que LDAP está configurado.
    - **Información del dispositivo:** Este parámetro no aparece si se seleccionan varias plataformas, o si se selecciona solo macOS. Elija **Número de serie**, **UDID** o **IMEI**. Después de elegir una opción, aparece un campo en el que puede escribir el valor correspondiente del dispositivo.
    - **Número de teléfono:** Este parámetro no aparece si se seleccionan varias plataformas, o si se selecciona solo macOS. Si quiere, introduzca el número de teléfono del usuario.
    - **Operador:** Este parámetro no aparece si se seleccionan varias plataformas, o si se selecciona solo macOS. Seleccione un operador para asociarlo con el número de teléfono del usuario.
    - **Modo de inscripción:** Elija el modo de seguridad de inscripción para los usuarios. El valor predeterminado es **Nombre de usuario y contraseña**. Algunas de las siguientes opciones no están disponibles para todas las plataformas:
        - Nombre de usuario y contraseña

  - High Security (Nivel alto de seguridad)
  - URL de invitación
  - URL de invitación y PIN
  - URL de invitación y contraseña
  - Dos factores
  - Nombre de usuario + PIN

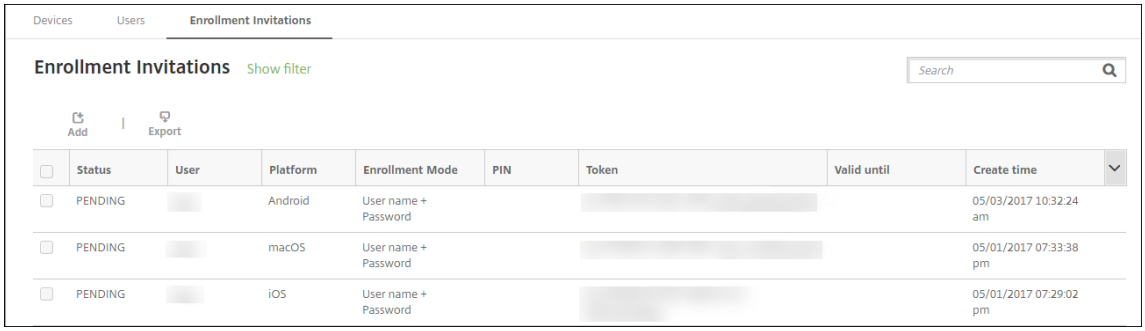
Para enviar invitaciones de inscripción, solo puede utilizar los modos de seguridad de inscripción **URL de invitación**, **URL de invitación + PIN** o **URL de invitación + contraseña**. Para los dispositivos que se inscriben con **Nombre de usuario + contraseña**, **Dos factores** o **Nombre de usuario + PIN**, los usuarios deben introducir manualmente sus credenciales en Secure Hub.

Un PIN de inscripción se denomina también un PIN de un solo uso. Este tipo de PIN es válido solamente cuando se inscribe el usuario.

> **Nota:**
>
> Cuando seleccione un modo de seguridad de inscripción que incluya un PIN, aparecerá el campo **Plantilla para PIN de inscripción**, donde deberá hacer clic en **PIN de inscripción**.

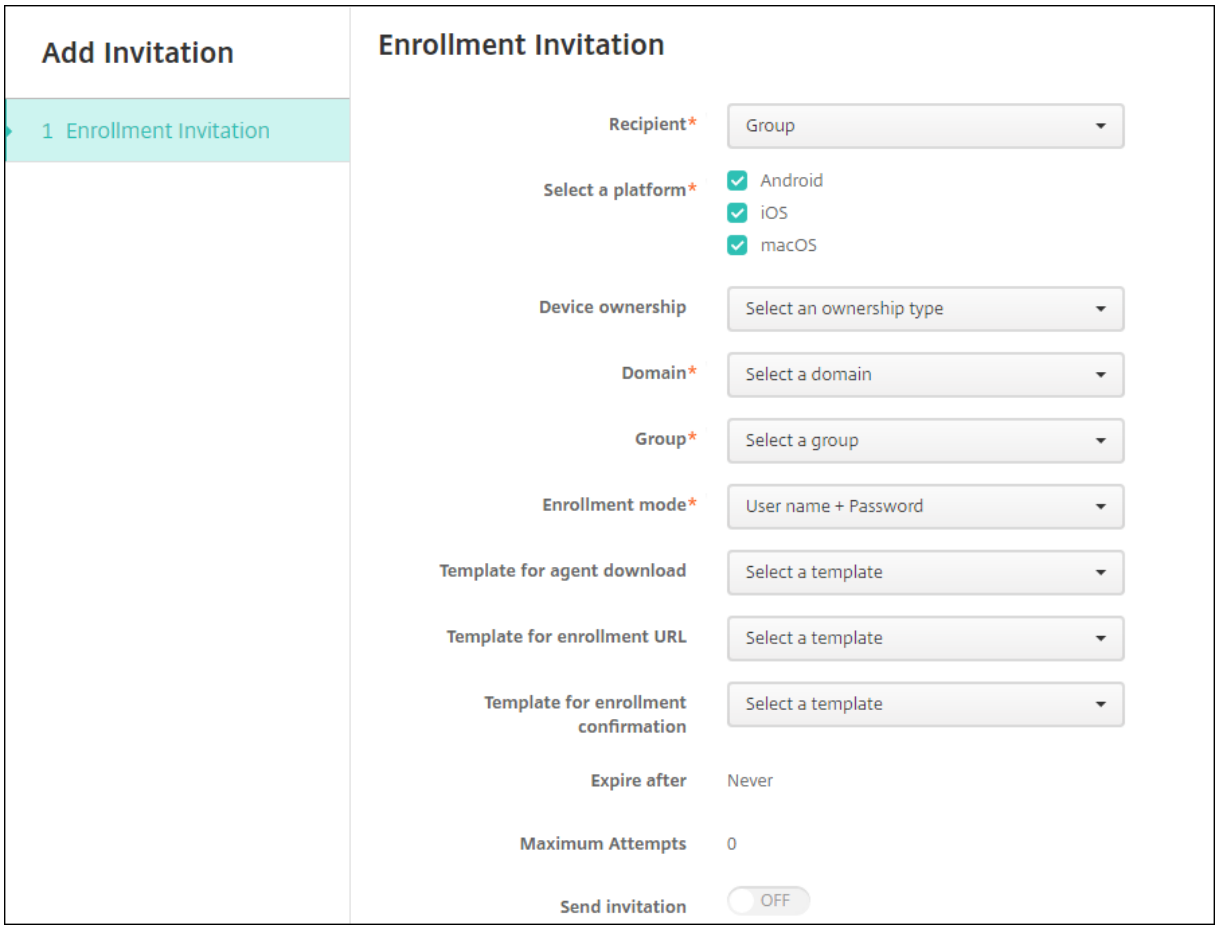
- **Plantilla para la descarga del agente:** Elija la plantilla de enlace de descarga denominada **Enlace de descarga**. Esa plantilla es para todas las plataformas compatibles.
- **Plantilla para URL de inscripción:** Elija **Invitación de inscripción**.
- **Plantilla para confirmación de la inscripción:** Elija **Confirmación de la inscripción**.
- **Caduca después de:** Este campo se establece cuando se configura el modo de inscripción y se indica cuándo caduca la inscripción. Para obtener más información sobre cómo configurar modos de seguridad de inscripción, consulte Configurar modos de seguridad de inscripción.
- **Máximo de intentos:** Este campo se define al configurar el **modo de inscripción** e indica el máximo de veces que tiene lugar el proceso de inscripción. Para obtener más información sobre cómo configurar modos de seguridad de inscripción, consulte Configurar modos de seguridad de inscripción.
- **Enviar invitación:** **Active** la opción para enviar la invitación inmediatamente. **Desactívela** para agregar la invitación a la tabla en la página **Invitaciones de inscripción** sin enviarla.

2. Haga clic en **Guardar y enviar** si habilitó **Enviar invitación**. De lo contrario, haga clic en **Guardar**. La invitación aparecerá en la tabla de la página **Invitaciones de inscripción**.



Para enviar una invitación de inscripción a un grupo

En la imagen siguiente, se muestran los parámetros de una invitación de inscripción para un grupo.



1. Configure estos parámetros:
    - **Dominio:** Elija el dominio del grupo que recibirá la invitación.
    - **Grupo:** Elija el grupo que recibirá la invitación.
    - **Modo de inscripción:** Elija cómo quiere que se inscriban los usuarios del grupo. El valor predeterminado es **Nombre de usuario y contraseña**. Algunas de las siguientes opciones no están disponibles para todas las plataformas:

- Nombre de usuario y contraseña
- High Security (Nivel alto de seguridad)
- URL de invitación
- URL de invitación y PIN
- URL de invitación y contraseña
- Dos factores
- Nombre de usuario + PIN

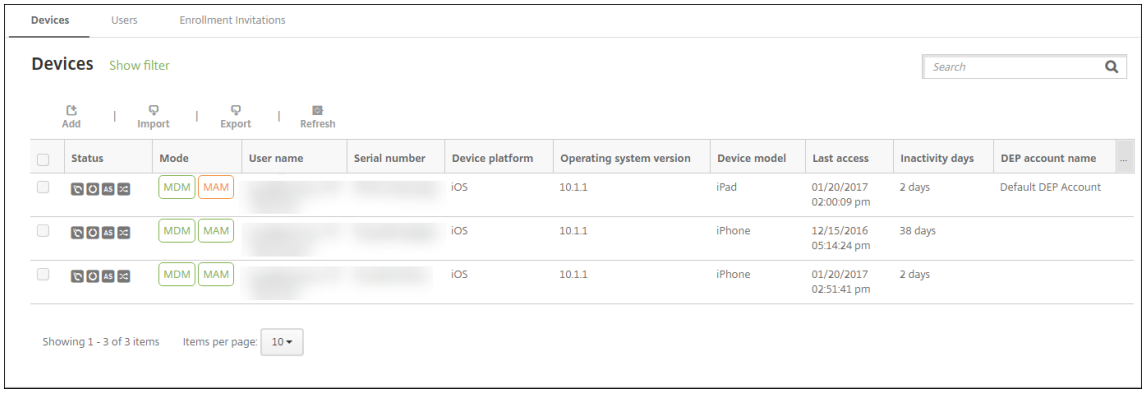
Para enviar invitaciones de inscripción, solo puede utilizar los modos de seguridad de inscripción **URL de invitación**, **URL de invitación + PIN** o **URL de invitación + contraseña**. Para los dispositivos que se inscriben con **Nombre de usuario + contraseña**, **Dos factores** o **Nombre de usuario + PIN**, los usuarios deben introducir manualmente sus credenciales en Secure Hub.

Solo aparecen los modos de seguridad de inscripción que son válidos para cada plataforma seleccionada.

> **Nota:**
>
> Cuando seleccione un modo de seguridad de inscripción que incluya un PIN, aparecerá el campo **Plantilla para PIN de inscripción**, donde deberá hacer clic en **PIN de inscripción**.

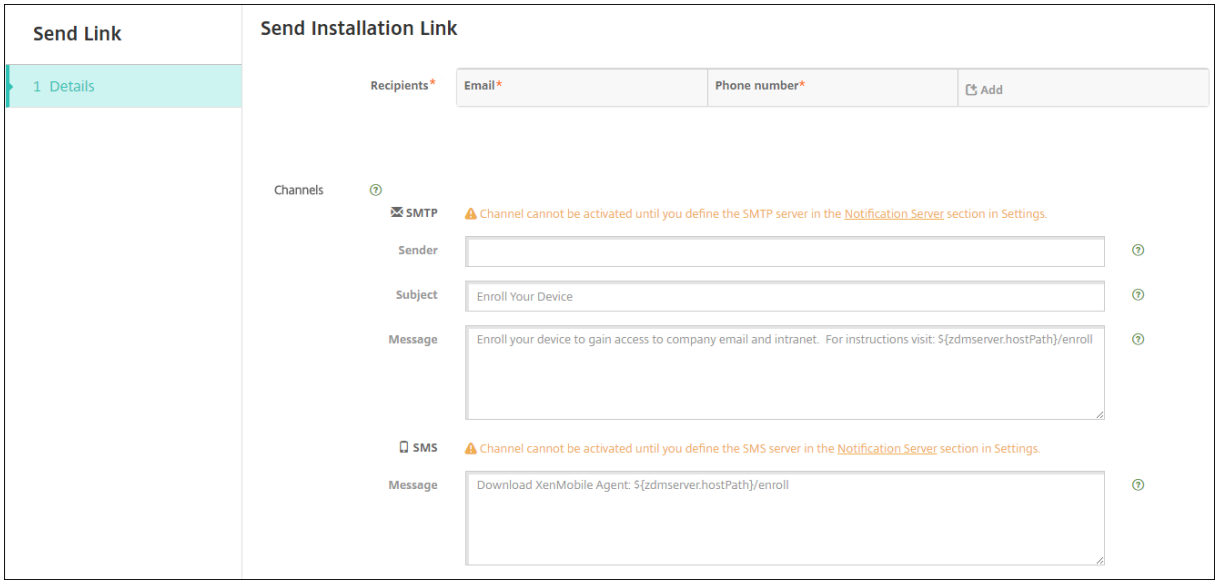
- **Plantilla para la descarga del agente:** Elija la plantilla de enlace de descarga denominada **Enlace de descarga**. Esa plantilla es para todas las plataformas compatibles.
- **Plantilla para URL de inscripción:** Elija **Invitación de inscripción**.
- **Plantilla para confirmación de la inscripción:** Elija **Confirmación de la inscripción**.
- **Caduca después de:** Este campo se establece cuando se configura el modo de inscripción y se indica cuándo caduca la inscripción. Para obtener más información sobre cómo configurar modos de seguridad de inscripción, consulte Configurar modos de seguridad de inscripción.
- **Máximo de intentos:** Este campo se define al configurar el modo de inscripción e indica el máximo de veces que tiene lugar el proceso de inscripción. Para obtener más información sobre cómo configurar modos de seguridad de inscripción, consulte Configurar modos de seguridad de inscripción.
- **Enviar invitación:** **Active** la opción para enviar la invitación inmediatamente. **Desactívela** para agregar la invitación a la tabla en la página **Invitaciones de inscripción** sin enviarla.

2. Haga clic en **Guardar y enviar** si habilitó **Enviar invitación**. De lo contrario, haga clic en **Guardar**. La invitación aparecerá en la tabla de la página **Invitaciones de inscripción**.



Para enviar un enlace de instalación

Para poder enviar un enlace de instalación para la inscripción, antes debe configurar canales (SMTP o SMS) en el servidor de notificaciones. Puede hacerlo desde la página **Parámetros**. Para obtener más información, consulte [Notificaciones](/es-es/xenmobile/server/users/notifications.html



1. Configure estos parámetros y haga clic en **Guardar**.
   - **Destinatario:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada destinatario:
     - **Correo electrónico:** Escriba la dirección de correo electrónico del destinatario. Este campo es obligatorio.
     - **Número de teléfono:** Escriba el número de teléfono del destinatario. Este campo es obligatorio.

> **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 **Eliminar** para eliminar el elemento, o bien haga clic en **Cancelar** 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 **Guardar** para guardar los cambios, o bien en **Cancelar** para descartarlos.

- **Canales:** 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 **Parámetros**, en **Servidor de notificaciones**. Para obtener más información, consulte Notificaciones.
- **SMTP:** La configuración de estos parámetros es opcional. Si no escribe nada en estos campos, se utilizarán los valores predeterminados que haya especificado en la plantilla de notificaciones definida para la plataforma seleccionada:
  - **Remitente:** Escriba un remitente opcional.
  - **Asunto:** Aquí puede escribir un asunto para el mensaje. Por ejemplo: “Inscriba su dispositivo”.
  - **Mensaje:** Escriba el mensaje opcional 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:
  - **Mensaje:** Escriba el mensaje que se enviará a los destinatarios. Este campo es obligatorio para las notificaciones por SMS.

> **Nota:** En América del Norte, los mensajes SMS que superen los 160 caracteres se entregan en varios mensajes.

2. Haga clic en **Enviar**.

> **Nota:**
>
> Si su entorno hace uso de nombres sAMAccountName, después de que los usuarios reciban la invitación y hagan clic en el enlace, deberán modificar el nombre de usuario para completar la autenticación. El nombre de usuario aparece como sAMAccount-

> Name@domainname.com. Los usuarios deben quitar la parte “@domainname.com”.

Modos de seguridad de inscripción por plataforma

En esta tabla se muestran los modos de seguridad que puede utilizar para inscribir dispositivos de usuario. En la tabla, **Sí** indica qué plataformas de dispositivos permiten modos de inscripción y administración específicos con distintos perfiles de inscripción.

Modo de seguridad de inscripción MDM	Modo de seguridad de inscripción MAM en Citrix Gateway	Modos de administración	Permite diferentes perfiles de inscripción	Android (heredado)	Android Enterprise	iOS (modo de inscripción de usuarios)	iOS	macOS	Windows
Azure AD y Okta como proveedores de identidades a través de Citrix Cloud	Certificado del cliente	MDM+MAM o MDM	Sí	Sí	Sí	Sí	Sí	No	No

Modo de seguridad de inscripción MDM	Modo de seguridad de inscripción MAM en Citrix Gateway	Modos de administración	Permite diferentes perfiles de inscripción	Android (heredado)	Android Enterprise	iOS (modo de inscripción de usuarios)	iOS	macOS	Windows
Nombre de usuario y contraseña	LDAP, LDAP + certificado de cliente y certificado de cliente únicamente	MDM+MAM, MDM o MAM (el modo solo MAM no admite certificados de cliente en Citrix Gateway)	Sí	Sí	Sí	Sí	Sí	Sí	Sí
URL de invitación	Certificado del cliente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	No	No
URL de invitación y PIN	Certificado del cliente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	No	No

Modo de seguridad de inscripción MDM	Modo de seguridad de inscripción MAM en Citrix Gateway	Modos de administración	Permite diferentes perfiles de inscripción	Android (heredado)	Android Enterprise	iOS (modo de inscripción de usuarios)	iOS	macOS	Windows
URL de invitación y contraseña	LDAP, LDAP + certificado de cliente y certificado de cliente únicamente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	No	No
Autenticación de dos factores (nombre de usuario + contraseña + PIN)	LDAP, LDAP + certificado de cliente y certificado de cliente únicamente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	Sí	No

Modo de seguridad de inscripción MDM	Modo de seguridad de inscripción MAM en Citrix Gateway	Modos de administración	Permite diferentes perfiles de inscripción	Android (heredado)	Android Enterprise	iOS (modo de inscripción de usuarios)	iOS	macOS	Windows
Nombre de usuario + PIN	Certificado del cliente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	Sí	No

A continuación se describe cómo se comportan los modos de seguridad de inscripción en dispositivos iOS, Android y Android Enterprise:

- **Nombre de usuario y contraseña** (predeterminado)
  - Envía a un usuario una sola notificación que contiene una URL de inscripción. Cuando el usuario hace clic en la URL, se abre Secure Hub. A continuación, el usuario escribe un nombre de usuario y una contraseña para inscribir el dispositivo en XenMobile.
- **URL de invitación**
  - Envía a un usuario una sola notificación que contiene una URL de inscripción. Cuando el usuario hace clic en la URL, se abre Secure Hub. Aparecen el nombre del servidor de XenMobile y el botón **Sí, inscribirlo**. El usuario toca **Sí, inscribirlo** para inscribir el dispositivo en XenMobile.
- **URL de invitación y PIN**
  - Envía a un usuario los siguientes correos electrónicos:
    - Un correo electrónico con una URL de inscripción, la cual permite al usuario inscribir el dispositivo en XenMobile a través de Secure Hub.
    - Un mensaje con un PIN de un solo uso que el usuario debe escribir al inscribir el dispositivo, junto con la contraseña del usuario de Active Directory (o local).
  - Con este modo, el usuario solo se inscribe mediante la URL de inscripción incluida en la notificación. Si el usuario pierde la notificación de invitación, no podrá inscribirse. No obstante, se puede enviar otra invitación.
- **URL de invitación y contraseña**

  - Envía a un usuario una sola notificación que contiene una URL de inscripción. Cuando el usuario hace clic en la URL, se abre Secure Hub. Aparece el nombre del servidor de XenMobile junto con un campo que permite al usuario escribir una contraseña.
- **Dos factores**
  - Envía al usuario una sola notificación que contiene una URL de inscripción y un PIN de un solo uso. Cuando el usuario hace clic en la URL, se abre Secure Hub. Aparece el nombre del servidor de XenMobile junto con dos campos que permiten al usuario escribir una contraseña y el número PIN.
- **Nombre de usuario + PIN**
  - Envía a un usuario los siguientes correos electrónicos:
    * Un correo electrónico con una URL de inscripción, la cual permite al usuario descargar e instalar Secure Hub. Después de abrir Secure Hub, se le pide al usuario que escriba un nombre de usuario y una contraseña para inscribir el dispositivo en XenMobile.
    * Un mensaje con un PIN de un solo uso que el usuario debe escribir al inscribir el dispositivo, junto con la contraseña del usuario de Active Directory (o local).
  - Si el usuario pierde la notificación de invitación, no podrá inscribirse. No obstante, se puede enviar otra invitación.

A continuación, se describe cómo se comportan los modos de seguridad de inscripción en dispositivos macOS:

- **Nombre de usuario y contraseña**
  - Envía a un usuario una sola notificación que contiene una URL de inscripción. Cuando el usuario hace clic en la URL, se abre el explorador Safari. Aparecerá una página de inicio de sesión en la que se solicita al usuario que escriba un nombre de usuario y una contraseña para inscribir el dispositivo en XenMobile.
- **Dos factores**
  - Envía al usuario una sola notificación que contiene una URL de inscripción y un PIN de un solo uso. Cuando el usuario hace clic en la URL, se abre el explorador Safari. Aparecerá una página de inicio de sesión en la que se muestran dos campos que permiten al usuario escribir una contraseña y el número PIN.
- **Nombre de usuario + PIN**
  - Envía a un usuario los siguientes correos electrónicos:
    * Un correo electrónico con una URL de inscripción. Cuando el usuario hace clic en la URL, se abre el explorador Safari. Aparecerá una página de inicio de sesión en la que se solicita al usuario que escriba un nombre de usuario y una contraseña para inscribir el dispositivo en XenMobile.
    * Un mensaje con un PIN de un solo uso que el usuario debe escribir al inscribir el dispositivo, junto con la contraseña del usuario de Active Directory (o local).
  - Si el usuario pierde la notificación de invitación, no podrá inscribirse. No obstante, se puede enviar otra invitación.

No puede enviar invitaciones de inscripción a los dispositivos Windows. Los usuarios de Windows se inscriben directamente a través de sus dispositivos.

Firebase Cloud Messaging

January 4, 2022

> **Nota:**
>
> Firebase Cloud Messaging (FCM) se conocía anteriormente como Google Cloud Messaging (GCM). Algunas etiquetas y mensajes de la consola de XenMobile aún se refieren a GCM.

Citrix le recomienda que utilice Firebase Cloud Messaging (FCM) para controlar cómo y cuándo los dispositivos Android se conectan a XenMobile. XenMobile, cuando se configura para FCM, envía notificaciones de conexión a dispositivos Android habilitados para FCM. Así, toda acción de seguridad o comando de implementación desencadena una notificación push para pedir al usuario que se reconecte al servidor de XenMobile.

Después de completar los pasos de configuración indicados en este artículo y después de que un dispositivo comience a usarse, este dispositivo se registrará en el servicio FCM de XenMobile Server. Esa conexión permite la comunicación casi en tiempo real entre XenMobile Service y el dispositivo mediante FCM. El registro de FCM funciona para inscripciones de nuevos dispositivos y dispositivos previamente inscritos.

Cuando XenMobile necesita iniciar una conexión con el dispositivo, se conecta al servicio FCM. Entonces, el servicio FCM notifica al dispositivo que se conecte. Este tipo de conexión es similar a lo que Apple utiliza para su servicio de notificaciones push.

Requisitos previos

- Cliente más reciente de Secure Hub
- Credenciales de cuenta de Google para desarrolladores
- Servicios de Google Play instalados en dispositivos Android habilitados para FCM

Puertos de firewall

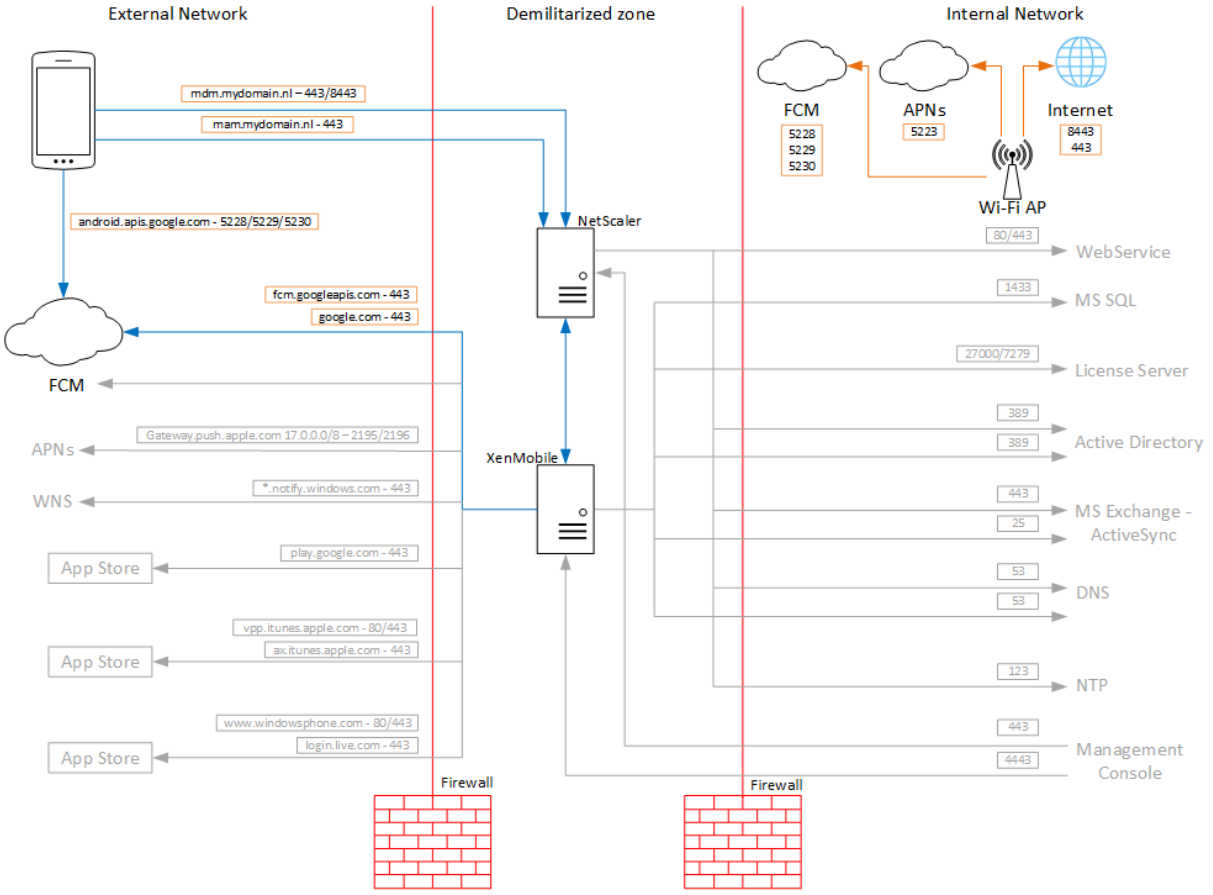
- Abra el puerto 443 en XenMobile para `fcm.googleapis.com` y `Google.com`.
- Abra una comunicación saliente por Internet para la red Wi-Fi de dispositivos en los puertos 5228, 5229 y 5230.
- Para permitir las conexiones salientes, FCM recomienda permitir los puertos 5228, 5229 y 5230 sin restricciones de IP. Sin embargo, si necesita restricciones de IP, FCM recomienda permitir

todas las direcciones IP en los bloques IPv4 e IPv6. Esos bloques se muestran en ASN de 15169 de Google. Actualice esa lista mensualmente.

Para obtener más información, consulte Requisitos de puertos.

Arquitectura

Este diagrama muestra el flujo de comunicación de FCM en la red interna y externa.

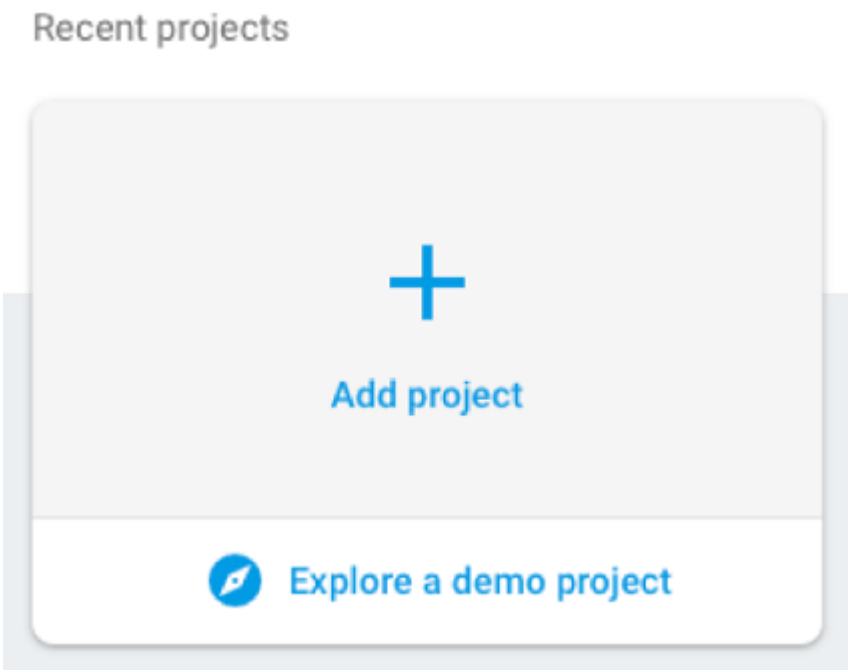


Para configurar su cuenta de Google para FCM

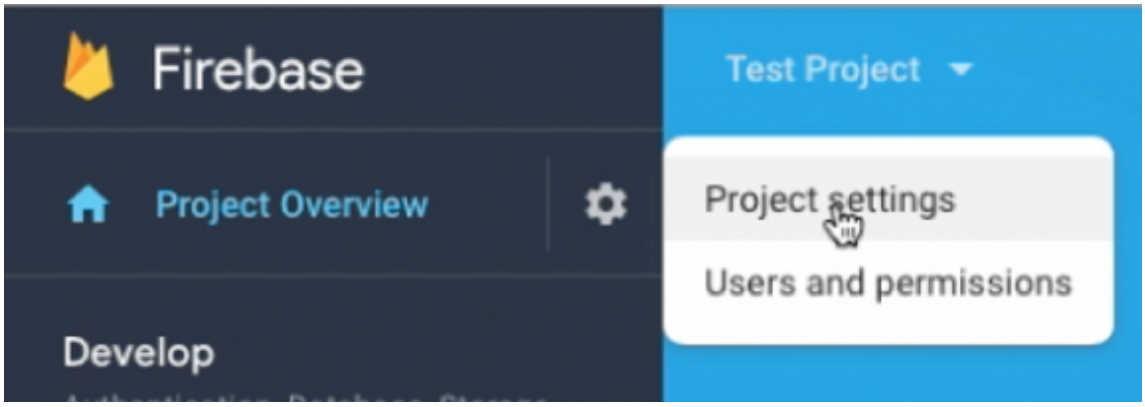
1. Inicie sesión en la siguiente URL con las credenciales de la cuenta de Google para desarrolladores:

   https://console.firebase.google.com/

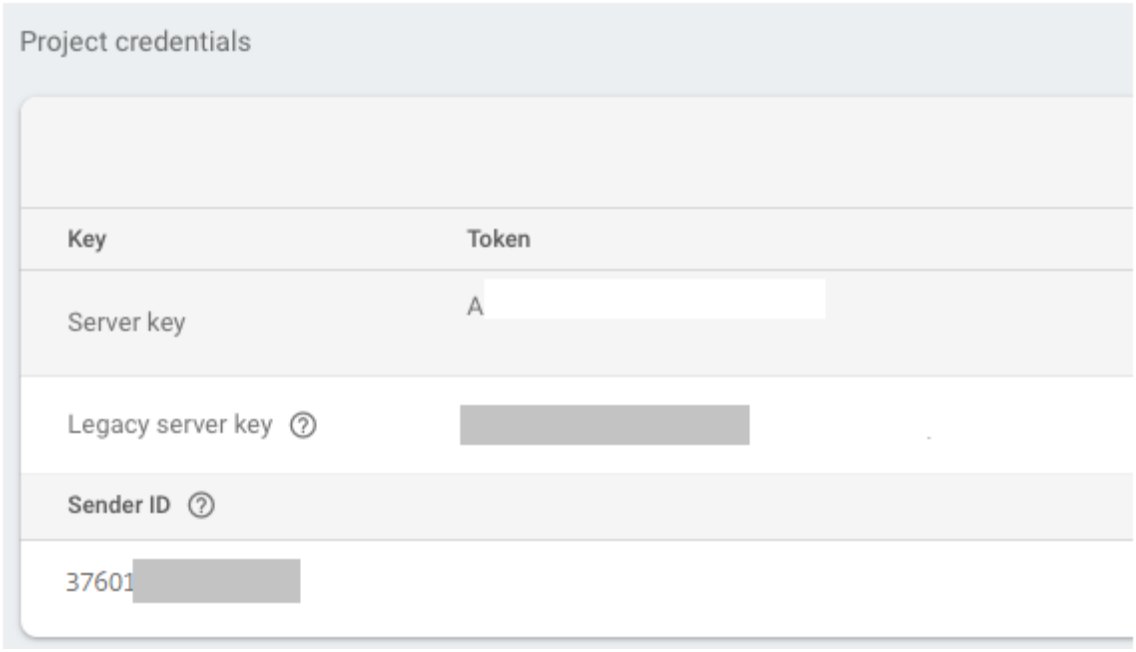
2. Haga clic en **Add project**.



3. Después de crear el proyecto, haga clic en **Project settings**.



4. Haga clic en la ficha **Cloud Messaging**. Copie los valores de **clave de servidor** e **ID de remitente**. En el siguiente procedimiento, pegue esos valores en la consola de XenMobile. A partir de octubre de 2016, debe crear claves de servidor en la consola de Firebase.

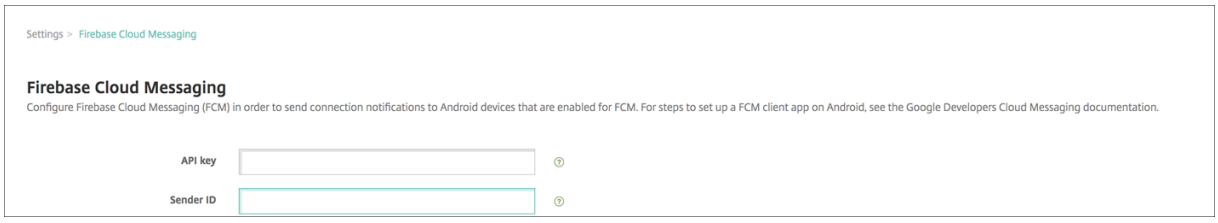


Para ver los pasos necesarios para configurar una aplicación cliente de FCM en Android, consulte este artículo de Google Developers Cloud Messaging: https://firebase.google.com/docs/cloud-messaging/android/client.

Para configurar XenMobile para FCM

En la consola de XenMobile, vaya a **Parámetros > Firebase Cloud Messaging**.

- Modifique la **clave de API** y escriba la **clave de servidor** de Firebase Cloud Messaging que copió en el último paso de la configuración de Firebase Cloud Messaging.
- Modifique el **ID de remitente** y escriba el **ID del remitente** que ha copiado en el procedimiento anterior.

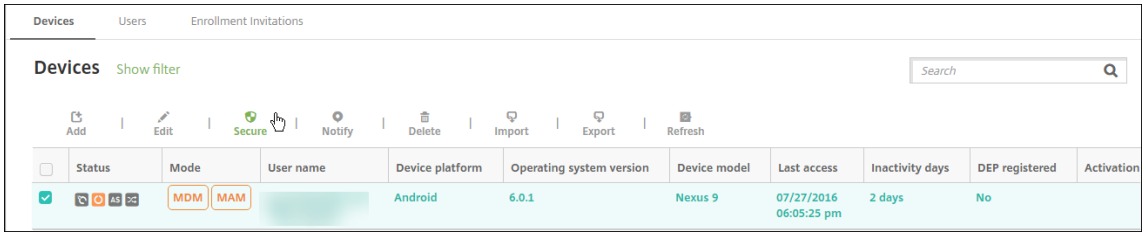


Después de completar la configuración, puede quitar la directiva de programación o cambiar esa directiva para conectarse con menos frecuencia.

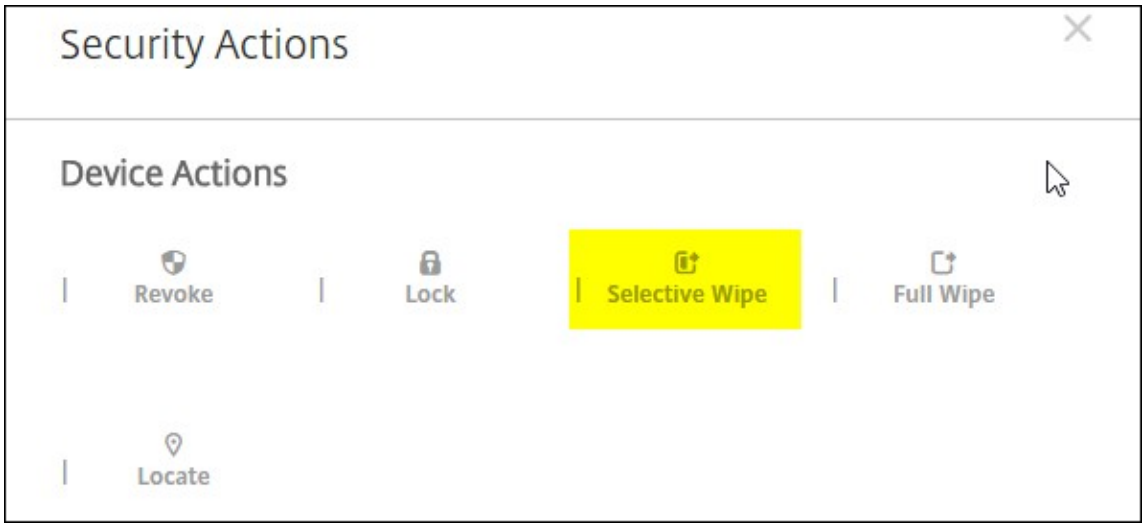
Para probar la configuración

1. Inscriba un dispositivo Android.

2. Deje el dispositivo inactivo durante algún tiempo, de forma que se desconecte de XenMobile.
3. Inicie sesión en la consola de XenMobile, haga clic en **Administrar**, seleccione el dispositivo Android, y, a continuación, haga clic en **Proteger**.



4. En **Acciones de dispositivo**, haga clic en **Borrado selectivo**.



Si la configuración es correcta, se lleva a cabo el borrado selectivo en el dispositivo.

Integración en funciones de Apple Educación

January 4, 2022

Puede usar XenMobile como solución de administración de dispositivos móviles (MDM) en un entorno que usa Apple Educación. XenMobile admite Apple School Manager (ASM) y la aplicación Aula para iPad. La directiva "Configuración de la educación" de XenMobile define los dispositivos de profesores y alumnos que van a usarse con Apple Educación.

En el marco de Apple Educación, ofrece iPads preconfigurados y supervisados a profesores y alumnos. Esa configuración incluye la inscripción de ASM en XenMobile, una cuenta administrada de ID de Apple configurada con una contraseña nueva y los iBooks y aplicaciones de compras por volumen obligatorios.

A continuación, dispone de las funciones destacadas de Apple Educación que admite XenMobile.

Apple School Manager

ASM es un servicio que permite configurar, implementar y administrar dispositivos iOS (iPadOS) y equipos portátiles macOS utilizados en las instituciones educativas. ASM incluye un portal web que permite a los administradores de TI:

- Asignar dispositivos del Programa de implementación de Apple a diferentes servidores MDM.
- Adquirir licencias de compras por volumen para aplicaciones e iBooks
- Crear varios **ID de Apple administrados** en bloque. Con esos ID de Apple personalizados, se puede acceder a servicios de Apple (por ejemplo, guardar documentos en iCloud Drive e inscribirse en cursos del App Store).

Puede agregar varias cuentas de ASM a XenMobile. Esta función permite utilizar, por ejemplo, parámetros de inscripción y opciones del asistente de instalación distintos en función de departamento o unidad de Apple Educación. A continuación, puede asociar las cuentas de ASM con distintas directivas de dispositivo.

Después de agregar una cuenta de ASM a la consola de XenMobile, XenMobile obtiene la información y la lista de las clases. Durante la configuración del dispositivo, XenMobile:

- Inscribe los dispositivos.
- Instala los recursos configurados para la implementación (directivas de dispositivo como, por ejemplo, “Configuración de la educación”, “Diseño de pantalla inicial”).
- También instala las aplicaciones y los iBooks comprados a través de las compras por volumen.

Después de ello, puede ofrecer los dispositivos preconfigurados a profesores y estudiantes. Si un dispositivo se pierde o es robado, puede usar la función MDM de Modo perdido para bloquearlo y localizarlo.

Aplicación Aula para iPad

La aplicación Aula para iPad permite a los profesores conectarse a los dispositivos de los alumnos y administrarlos. Puede ver las pantallas de los iPads, abrir aplicaciones en ellos, y abrir y compartir enlaces Web.

Aula es una aplicación gratuita disponible en el App Store. Se carga en la consola de XenMobile. Luego, se configura a través de la directiva de configuración de la educación, que se implementará a posteriori en los dispositivos de los profesores.

Para obtener más información acerca de las funciones de Apple Educación, consulte el sitio Educación de Apple y la guía de implantación para el sector educativo en el mismo sitio.

Requisitos previos

- Citrix Gateway

- Perfil de inscripción configurado para MDM+MAM.
- Apple iPad de 3.ª generación (versión mínima) o iPad Mini, con iOS 9.3 (versión mínima)

> **Nota:**
>
> XenMobile no valida cuentas de usuario de ASM en LDAP o Active Directory. Sin embargo, puede conectar XenMobile a LDAP o Active Directory para administrar usuarios y dispositivos no relacionados con profesores y estudiantes de ASM. Por ejemplo, puede usar Active Directory para proporcionar Secure Mail y Secure Web a otros miembros de ASM, como gestores y administradores de TI.
>
> Como los alumnos y los profesores de ASM son usuarios locales, no es necesario implementar Citrix Secure Hub en sus dispositivos.
>
> No se admiten usuarios locales (solo usuarios de Active Directory) en la inscripción MAM que incluye la autenticación de Citrix Gateway. Por lo tanto, XenMobile solo implementa los libros de iBooks y las aplicaciones de compras por volumen obligatorios en los dispositivos de profesores y alumnos.

Requisitos previos para iPads compartidos

- Cualquier iPad Pro, iPad de 5.ª generación, iPad Air 2 o posterior y iPad mini 4 o posterior
- Al menos 32 GB de almacenamiento
- Supervisado

Configurar Apple School Manager y XenMobile

Después de adquirir iPads en Apple o en proveedores u operadores autorizados de Apple: siga el flujo de trabajo indicado en esta sección para configurar sus dispositivos y su cuenta de ASM. Esta secuencia contiene los pasos que se llevan a cabo en el portal de ASM y en la consola de XenMobile.

Siga esas instrucciones para configurar la integración de los iPads que utilice mediante un modelo de uno a uno (un iPad por estudiante) o iPads de profesor (no compartidos). Para configurar iPads compartidos, consulte Configurar iPad Compartidos.

Paso 1: Cree una cuenta de Apple School Manager y complete el Asistente de configuración

Si piensa actualizar una versión del Programa de implementación de Apple, consulte el artículo de asistencia de Apple Actualizar tu centro a Apple School Manager. Para crear su cuenta de ASM, vaya a https://school.apple.com/ y siga las instrucciones para inscribirse. La primera vez que inicia sesión en ASM se abrirá el Asistente de configuración.

- Para obtener información sobre los requisitos previos de ASM, el Asistente de configuración y las tareas de administración, consulte el Manual de uso de Apple School Manager.

- Cuando configure un ASM, use un nombre de dominio diferente del nombre de dominio de Active Directory. Por ejemplo, puede anteponer un prefijo de tipo `appleid` al nombre de dominio de ASM.
- Cuando se conecta a ASM para ver los datos de la lista del aula, ASM crea ID de Apple administrados para profesores y alumnos. La lista contiene datos de profesores, alumnos y clases. Para obtener información sobre cómo agregar datos de listas a ASM, consulte la Guía del usuario de ASM, a la que se ha hecho referencia anteriormente.
- Puede personalizar el formato del ID de Apple administrado para que se ajuste a su institución como se describe en la Guía del usuario de ASM, a la que se ha hecho referencia anteriormente.

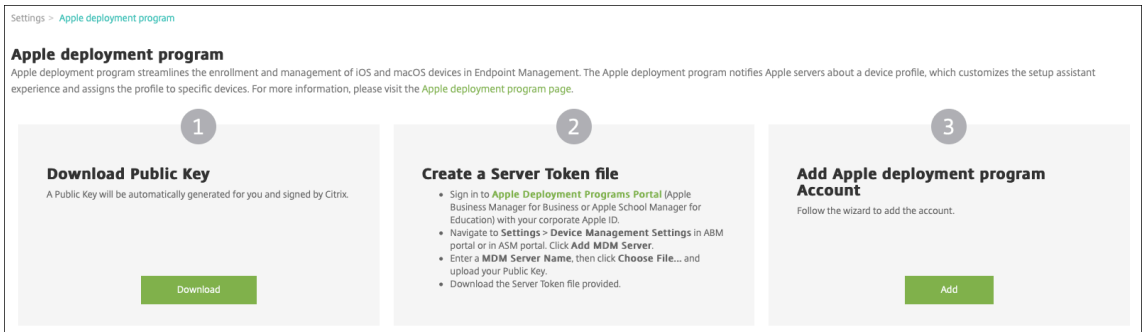
  > **Importante:**
  >
  > No cambie los ID de Apple administrados una vez que haya importado la información de ASM en XenMobile.

- Si ha adquirido los dispositivos por medio de distribuidores y operadores, vincule esos dispositivos a ASM. Para obtener información, consulte la Guía del usuario de ASM, a la que se ha hecho referencia anteriormente.

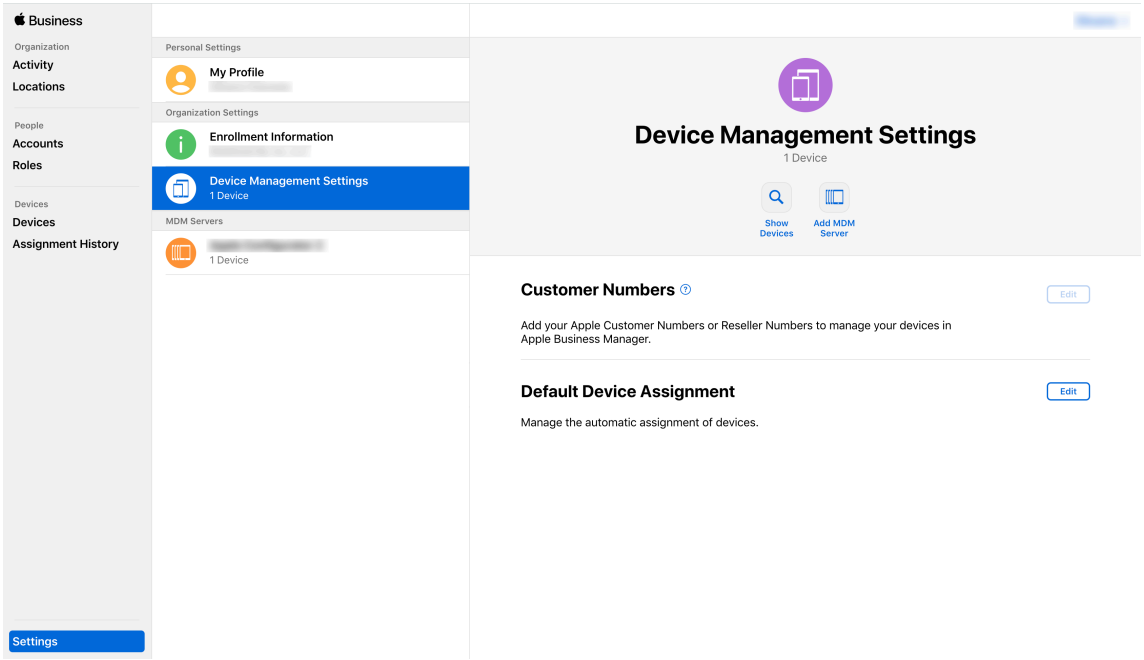
Paso 2: Configure XenMobile como el servidor MDM de Apple School Manager y configure asignaciones de dispositivos

El portal de ASM contiene una ficha llamada **Servidores MDM**. Se necesita el archivo de clave pública que proporciona XenMobile para completar esta configuración.

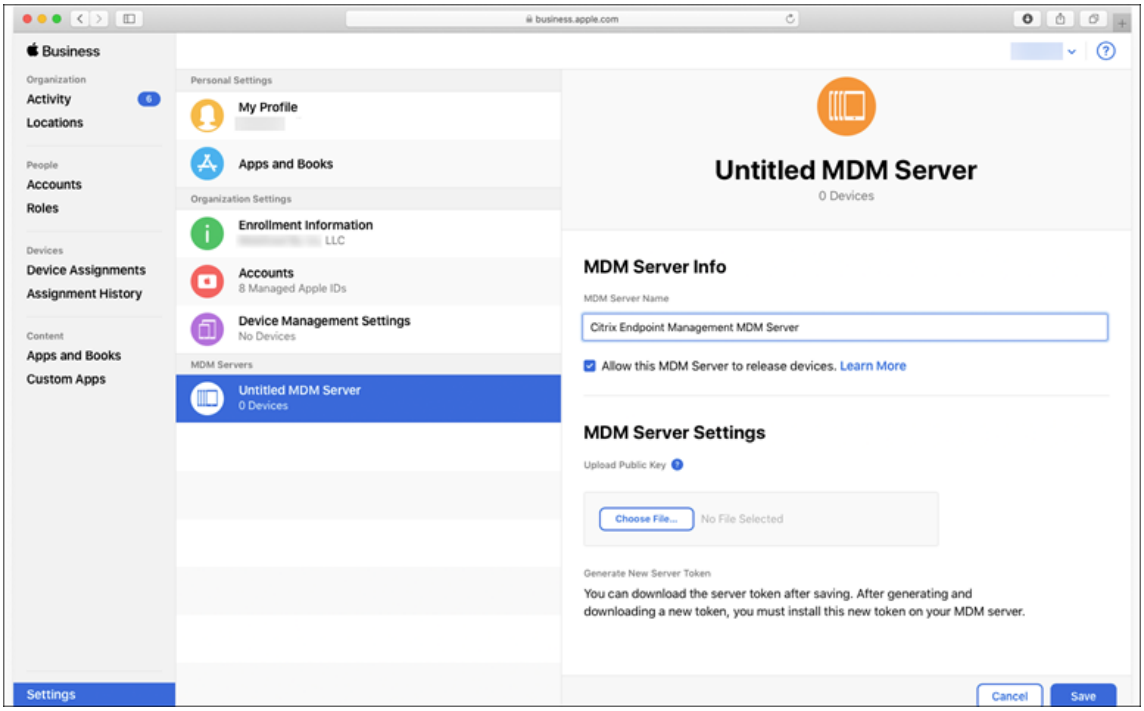
1. Descargue la clave pública de XenMobile en el equipo local: En la consola de XenMobile, vaya a **Parámetros > Programa de implementación de Apple**.



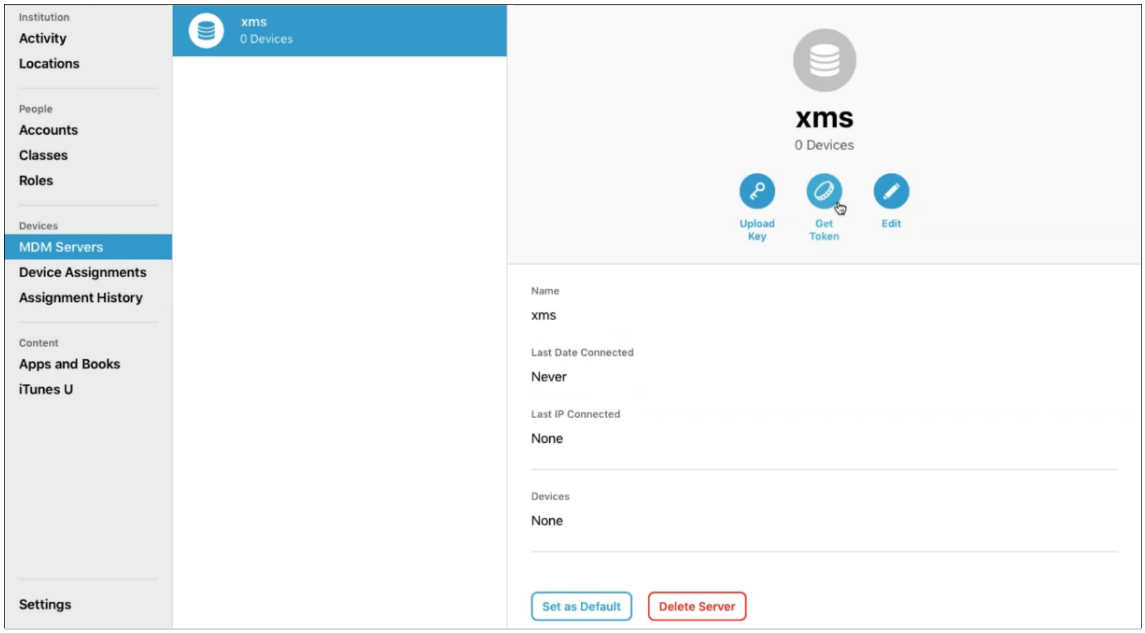
2. En **Descargar clave pública**, haga clic en **Descargar** y guarde el archivo PEM.
3. En el portal de **Apple School Manager**, haga clic en **Settings** y, a continuación, en **Device Management Settings**. Haga clic en **Add MDM Server**.



4. Escriba un nombre para XenMobile. El nombre de servidor que escriba es para su referencia personal, no es el nombre ni la dirección URL del servidor. En **Upload Public Key**, haga clic en **Choose File**.



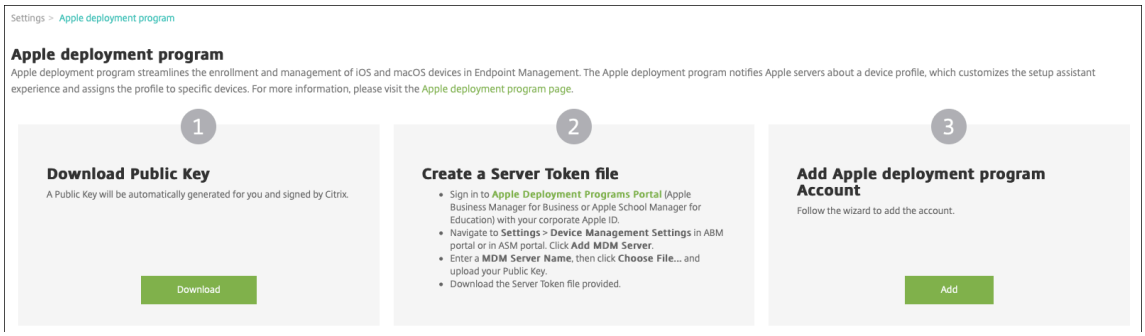
5. Cargue la clave pública que ha descargado de XenMobile y, a continuación, haga clic en **Guardar**.
6. Genere un token de servidor. Para ello, haga clic en **Descargar token** para descargar el archivo de token del servidor en el equipo.



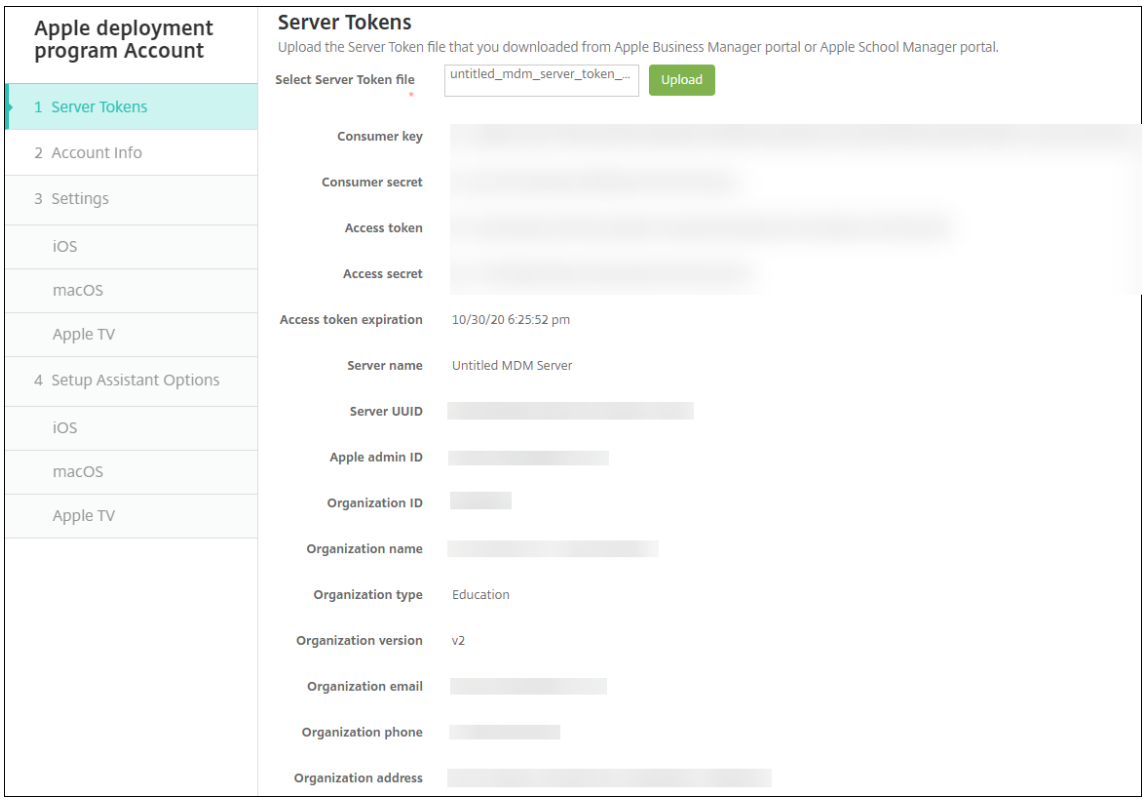
7. En **Default Device Assignment**, haga clic en **Change**. Elija cómo quiere asignar los dispositivos y, a continuación, proporcione la información solicitada. Para obtener información, consulte el Manual de uso de ASM.

Paso 3: Agregue la cuenta de Apple School Manager a XenMobile

1. En la consola de XenMobile, vaya a **Parámetros > Programa de implementación de Apple** y, en **Agregar cuenta de Programas de implementación de Apple**, haga clic en **Agregar**.



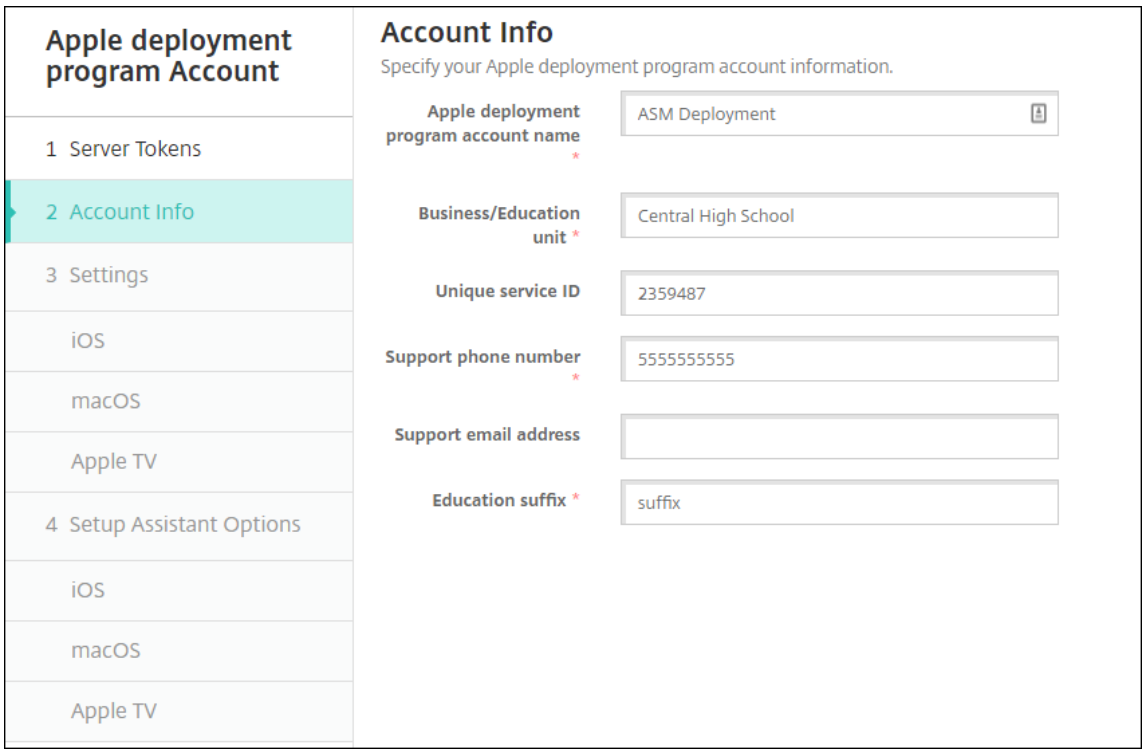
2. En la página **Tokens de servidor**, haga clic en **Cargar** y elija el archivo del token de servidor (un archivo P7M) que descargó del portal de ASM. Aparecerá la información del token.



Notas:

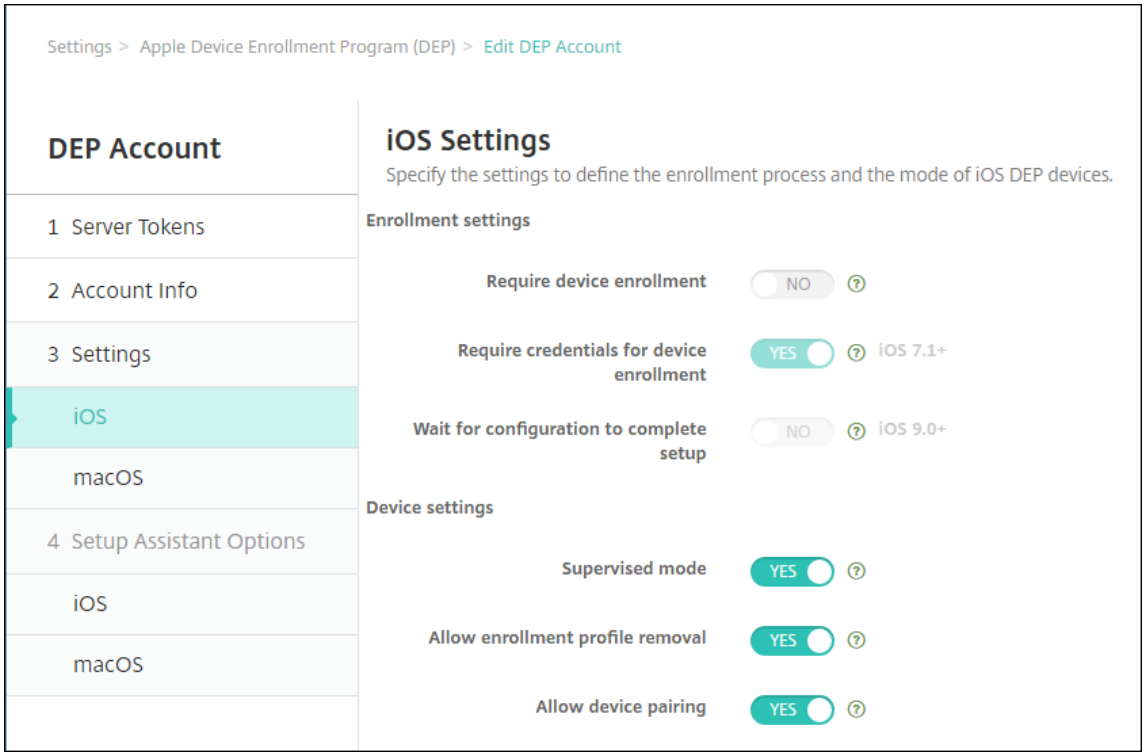
- El **ID de organización** es su identificador de cliente del Programa de implementación de Apple.
- El **Tipo de organización** de las cuentas de ASM es **Educación** y la **Versión de organización** es **v2**.

3. En la página **Información de cuenta**, especifique los siguientes parámetros.



- **Nombre de la cuenta del Programa de implementación de Apple:** Nombre único para esta cuenta del Programa de implementación de Apple. Use nombres que reflejen cómo organiza las cuentas del Programa de implementación de Apple (por ejemplo, por país u organización).
- **Business/Education unit:** El departamento o la unidad de educación para la asignación de dispositivos. Este campo es obligatorio.
- **ID único de servicio:** Un ID exclusivo optativo para ayudarle a identificar la cuenta.
- **Número de teléfono de asistencia:** Un número de teléfono al que puedan llamar los usuarios para obtener ayuda durante la instalación. Este campo es obligatorio.
- **Dirección de correo electrónico de asistencia:** Una dirección opcional de correo electrónico de asistencia disponible para los usuarios finales.
- **Sufijo de educación:** Marca las clases de una cuenta determinada del Programa de implementación de ASM (el sufijo de compras por volumen marca las aplicaciones y los iBooks de una cuenta de compras por volumen determinada). Se recomienda usar el mismo sufijo para ambas cuentas, el Programa de implementación de ASM y las compras por volumen de ASM.

4. Haga clic en **Siguiente**. En **Parámetros de iOS**, especifique los siguientes parámetros.



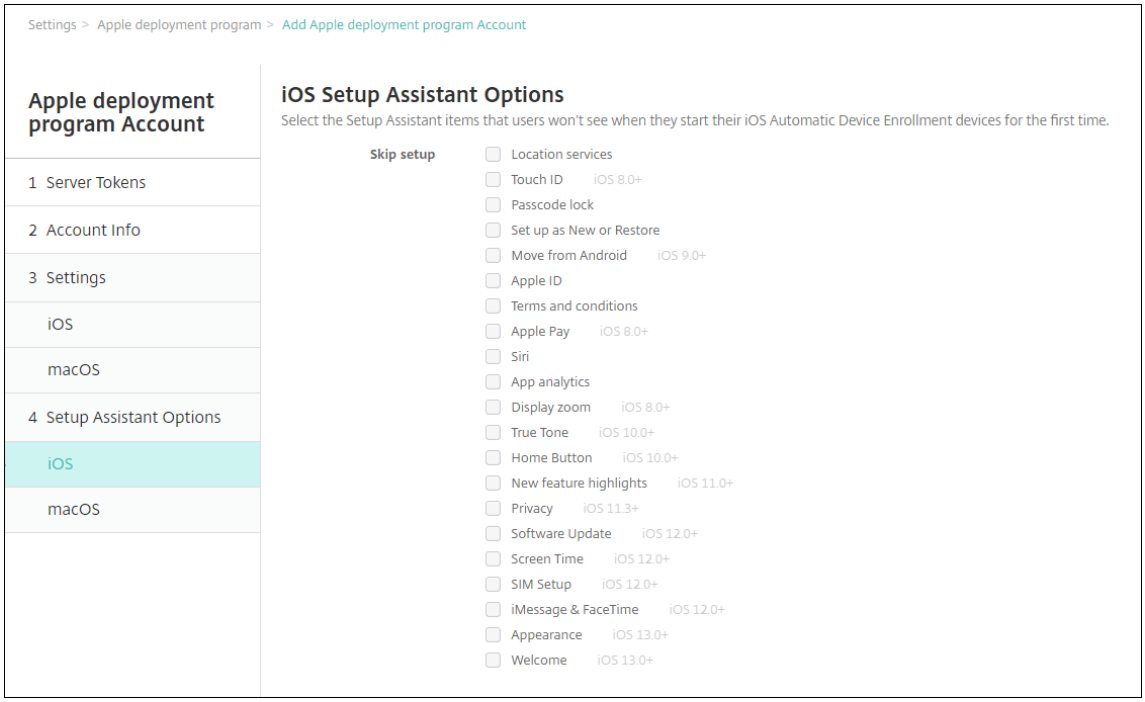
- **Parámetros de inscripción**
  - **Requerir inscripción del dispositivo:** Puede requerir a los usuarios que inscriban sus dispositivos. Cambie el parámetro a **No**.
  - **Requerir credenciales para inscripción de dispositivos:** Puede pedir a los usuarios que indiquen sus credenciales durante la configuración del Programa de implementación de Apple. Para la integración de ASM con XenMobile, este parámetro es **Sí** de forma predeterminada y no se puede cambiar. El Programa de implementación de Apple requiere credenciales para la inscripción de dispositivos.
  - **Esperar a que se complete la configuración:** Puede requerir que los dispositivos de los usuarios permanezcan en el modo del asistente de configuración hasta implementar todos los recursos de MDM en ellos. Para la integración de ASM con XenMobile, este parámetro es **No** de forma predeterminada. Según la documentación de Apple, los comandos siguientes pueden no funcionar mientras un dispositivo esté en el modo de asistente de configuración:
    - InviteToProgram
    - InstallApplication
    - InstallMedia
    - ApplyRedemptionCode
- **Parámetros del dispositivo**
  - **Modo supervisado:** Puede colocar los dispositivos iOS en el modo supervisado. No

cambie el valor predeterminado **Sí**. Para obtener información sobre cómo colocar un dispositivo iOS en modo supervisado, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.

- **Modo compartido:** Habilite el modo compartido en iPads. Los dispositivos que no cumplen los requisitos mínimos no pueden compartirse.
- **Permitir quitar el perfil de inscripción:** Para la integración de ASM, puede permitir que el usuario quite el perfil de inscripción del dispositivo. Cambie este parámetro a **Sí**.
- **Permitir emparejamiento de dispositivos:** Para la integración de ASM, puede permitir el emparejamiento de dispositivos para administrarlos desde el App Store de Apple y Apple Configurator. Cambie este parámetro a **Sí**.

5. En **Opciones del asistente de configuración de iOS**, seleccione los pasos a omitir del Asistente de configuración de iOS (es decir, los pasos que los usuarios no tienen que llevar a cabo) cuando inicien sus dispositivos por primera vez. De forma predeterminada, el Asistente de configuración incluye todos los pasos. Tenga en cuenta que quitar pasos desde el Asistente de configuración simplifica la experiencia del usuario.

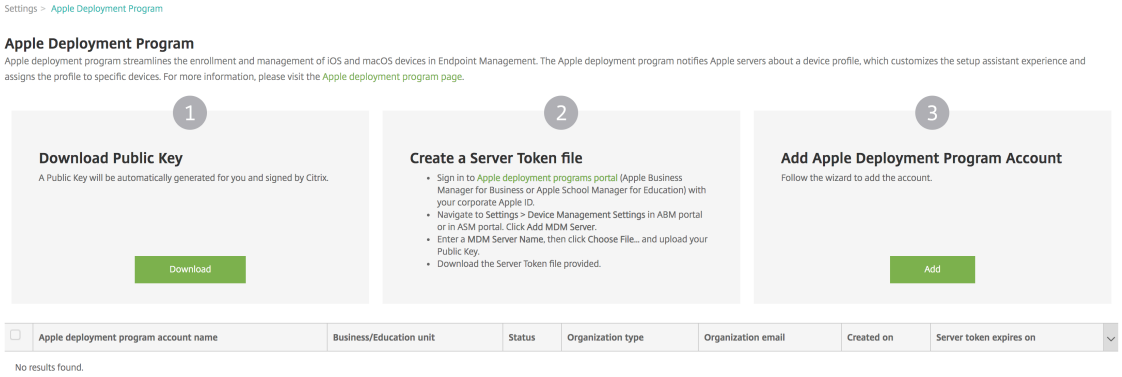
> **Importante:**
>
> Citrix recomienda incluir los pasos de **ID de Apple** y **Términos y condiciones**. Estos pasos permiten a profesores y estudiantes proporcionar sus nuevas contraseñas administradas de ID de Apple y aceptar los términos y condiciones necesarios.



- **Servicios de localización:** Puede configurar el servicio de localización en el dispositivo.
- **Touch ID:** Puede configurar Touch ID en dispositivos iOS.
- **Bloqueo con código:** Puede crear un código para acceder al dispositivo.
- **Definir como nuevo o Restaurar:** Puede configurar el dispositivo como nuevo o a partir de una copia de seguridad de iCloud o del App Store de Apple.
- **Mover desde Android:** Puede permitir la transferencia de datos desde un dispositivo Android a un dispositivo iOS. Esta opción solo está disponible cuando la opción **Definir como nuevo o Restaurar** está seleccionada (es decir, se omite el paso).
- **ID de Apple:** Configurar una cuenta de ID de Apple para el dispositivo. Citrix recomienda marcar la casilla con la que se incluye este paso.
- **Términos y condiciones:** Puede requerir que el usuario acepte los términos y condiciones para usar el dispositivo. Citrix recomienda marcar la casilla con la que se incluye este paso.
- **Apple Pay:** Puede configurar Apple Pay en dispositivos iOS.
- **Siri:** Usar o no usar Siri en el dispositivo.
- **App Analytics:** Puede configurar si se pueden compartir los datos de fallos y estadísticas de uso con Apple.
- **Zoom de presentación:** Puede configurar la resolución de la pantalla (estándar o ampliada) en los dispositivos iOS.
- **True Tone:** Puede configurar el Tono True en los dispositivos iOS.
- **Botón de inicio:** Puede definir la sensibilidad del botón de inicio.
- **Nuevas funciones destacadas:** Puede introducir las nuevas pantallas informativas “Accede al Dock desde cualquier sitio” y “Cambia entre las apps recientes” en dispositivos iOS 11.0 (versión mínima).
- **Privacidad:** Puede evitar que los usuarios vean el panel de datos y privacidad durante la configuración de dispositivos del Programa de implementación de Apple. Para iOS 11.3 y versiones posteriores.
- **Actualización de software:** Evita que el usuario vea la pantalla de actualización obligatoria del software durante la configuración de dispositivos del Programa de implementación de Apple. Para iOS 12.0 y versiones posteriores.
- **ScreenTime:** Evita que el usuario vea la pantalla Screen Time durante la configuración de dispositivos del Programa de implementación de Apple. Para iOS 12.0 y versiones posteriores.
- **Configuración de la tarjeta SIM:** Evita que el usuario vea la pantalla Add Cellular Plan durante la configuración de dispositivos del Programa de implementación de Apple. Para iOS 12.0 y versiones posteriores.
- **iMessage y FaceTime:** Evita que el usuario vea la pantalla iMessage y FaceTime durante la configuración de dispositivos del Programa de implementación de Apple. Para iOS 12.0 y versiones posteriores.

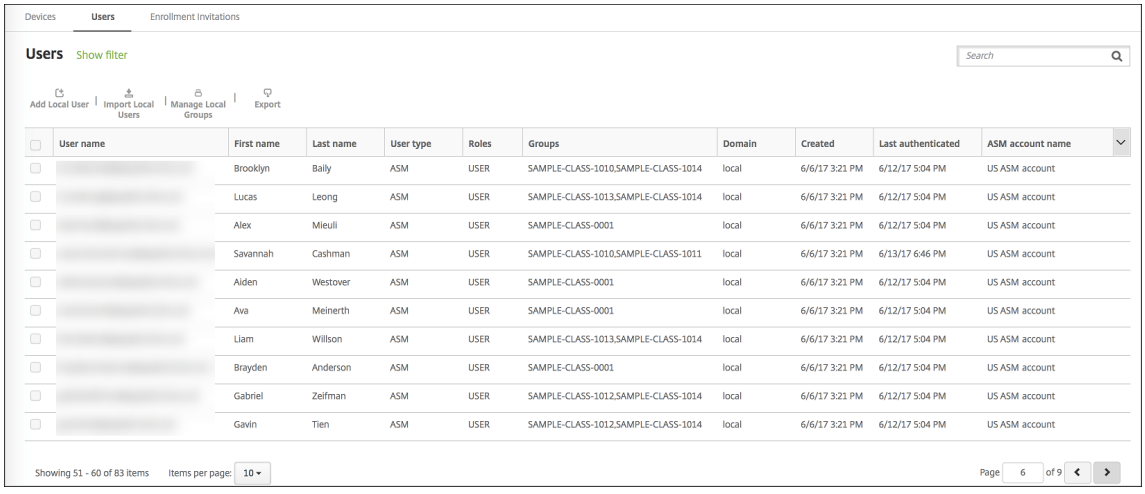
6. La cuenta aparece en **Parámetros > Programa de implementación de Apple**. Para probar la

conectividad entre XenMobile y su cuenta de ASM, seleccione la cuenta y haga clic en **Probar conectividad**.



Aparecerá un mensaje de estado.

Después de unos minutos, las cuentas que tenga el usuario en ASM aparecen en la página **Administrar > Usuarios**. XenMobile crea cuentas de usuario local en función del ID de Apple administrado que se haya importado para cada usuario. En el siguiente ejemplo, el prefijo del nombre de dominio que tienen los ID de Apple personalizados para las cuentas de usuario es `appleid`.

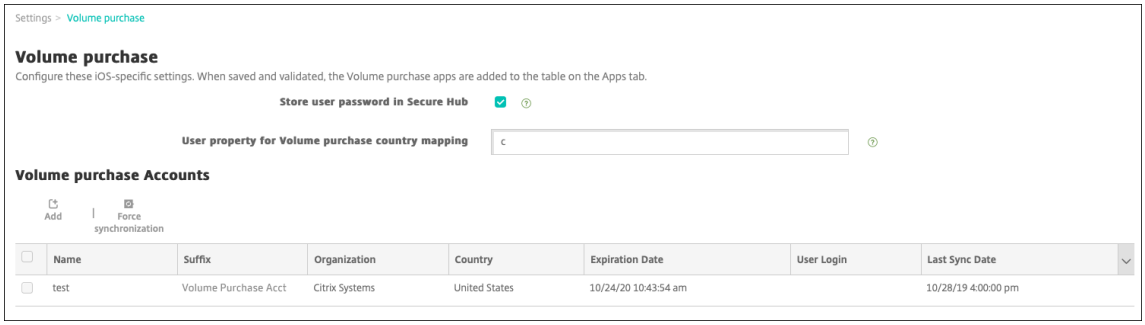


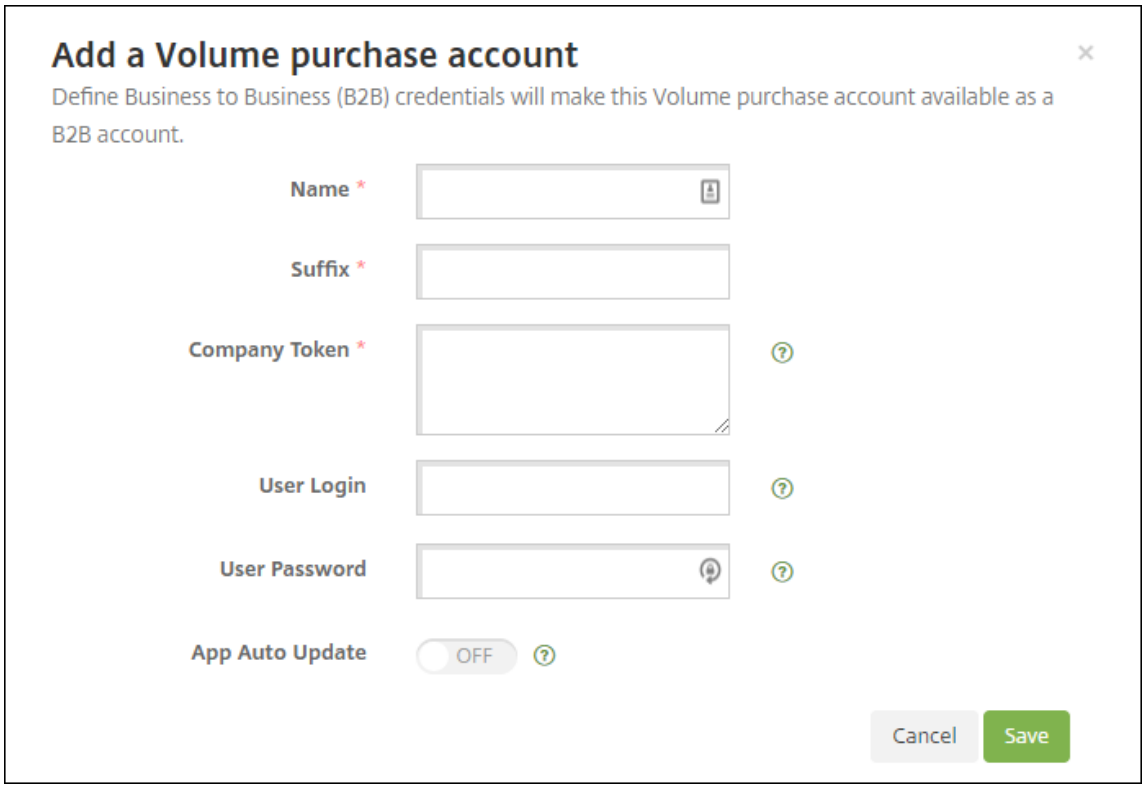
Para ver a todos los usuarios de una cuenta determinada de ASM, escriba el nombre de la cuenta en el filtro de búsqueda de usuarios.

Paso 4: Configure una cuenta de compras por volumen de Educación para Apple School Manager

En esta sección, debe configurar XenMobile para que apunte a la cuenta de compras por volumen que se va a usar para adquirir licencias de compras por volumen para las aplicaciones y los libros de iBooks.

1. Si quiere configurar una cuenta de compras por volumen de Educación para ASM, siga las instrucciones indicadas en Compras por volumen de Apple. La pantalla “Agregar una cuenta de compras por volumen” requiere un token de la empresa. Descargue el token directamente desde su cuenta de compras por volumen de Educación y péguelo en la pantalla **Agregar una cuenta de compras por volumen**.





2. Espere unos minutos a que se importen las licencias de compras por volumen en XenMobile.

Paso 5: Agregue contraseñas para los usuarios de Apple School Manager

Después de agregar una cuenta de ASM, XenMobile importa las clases y los usuarios desde ASM. XenMobile trata las clases como grupos locales y, en la consola, se usa el término "grupo" para ellas. Si una clase ya tiene un nombre de grupo en ASM, XenMobile asigna ese nombre de grupo a la clase. De lo contrario, XenMobile utiliza el ID del sistema de origen para formar el nombre del grupo. XenMobile no utiliza el nombre del curso para nombrar la clase debido a que los nombres de los cursos en ASM no son únicos.

XenMobile utiliza los ID de Apple administrados para crear usuarios locales con el tipo de usuario **ASM**. Los usuarios son locales porque ASM crea las credenciales independientemente de todos los orígenes de datos externos. Por eso, XenMobile no utiliza un servidor de directorio para autenticar a estos usuarios nuevos.

ASM no envía contraseñas de usuario temporales a XenMobile. Puede importarlas desde un archivo CSV o agregarlas manualmente. Para importar contraseñas de usuario temporales:

1. Obtenga el archivo CSV generado por ASM cuando cree las contraseñas temporales de los ID de Apple administrados.
2. Modifique ese archivo CSV, cambie las contraseñas temporales por las contraseñas nuevas que los usuarios deberán proporcionar para inscribirse en XenMobile. No hay ninguna restricción en el tipo de contraseña que se puede utilizar para este propósito.

   El formato de una entrada en el archivo CSV es el siguiente: `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`

   Donde:

   Usuario: `user@appleid.citrix.com`

   Nombre: `Firstname`

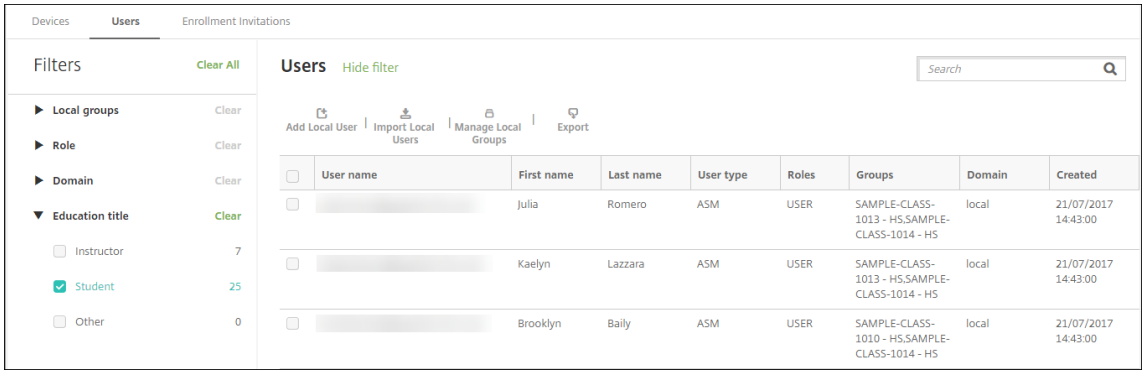
   Segundo nombre: `Middle`

   Apellido: `Lastname`

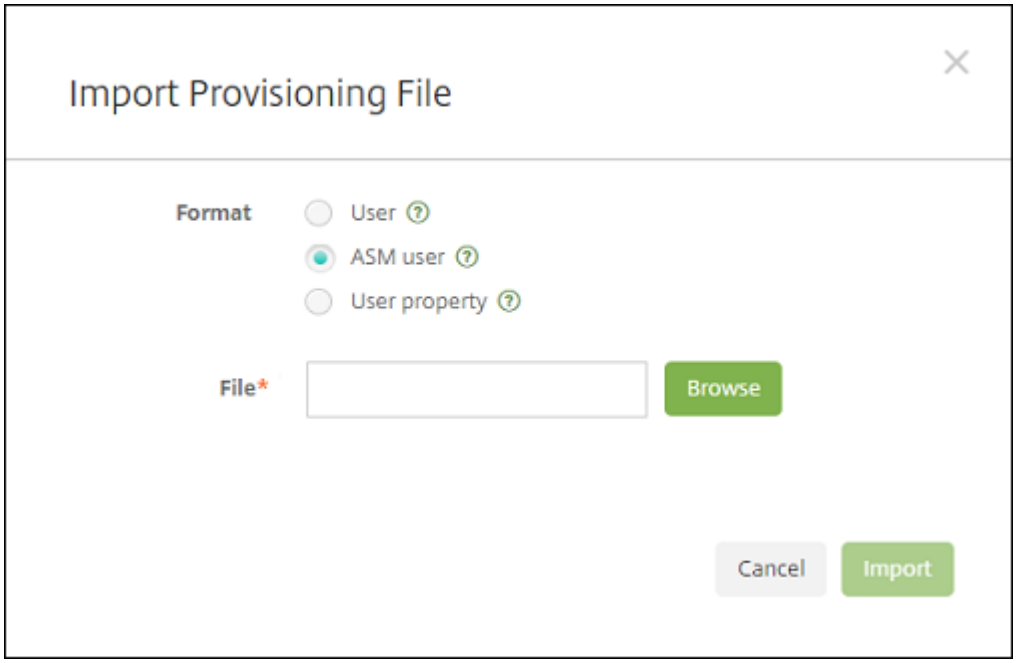
   Contraseña: `Password123!`
3. En la consola de XenMobile, haga clic en **Administrar > Usuarios**. Aparecerá la página **Usuarios**.

   En la siguiente página de ejemplo **Administrar > Usuarios** se muestra una lista de los usuarios importados desde ASM. En la lista **Usuarios**:

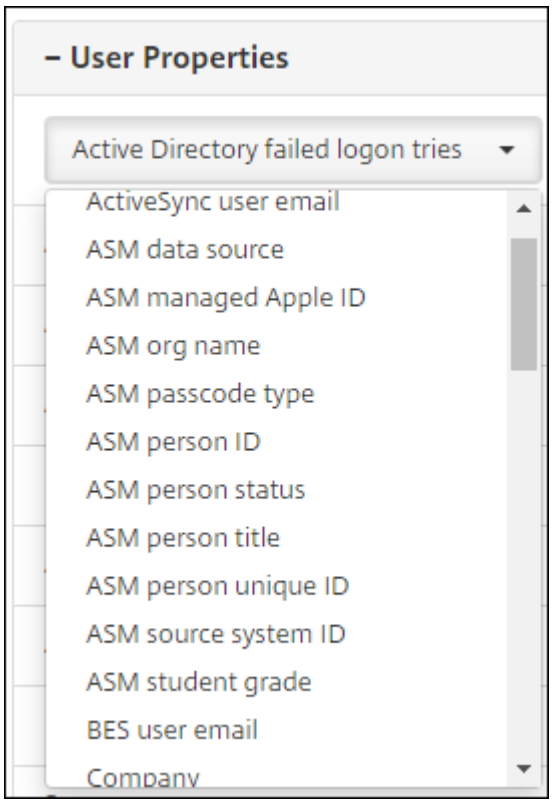
   - El **Nombre de usuario** es el ID de Apple administrado.
   - El tipo de usuario es **ASM**, para indicar que la cuenta proviene de ASM.
   - En **Grupos** se muestran las clases.



4. Haga clic en **Importar usuarios locales**. Aparece el cuadro de diálogo **Importar archivo de aprovisionamiento**.
5. En “Formato”, elija **Usuario ASM**, vaya al archivo CSV que ha preparado en el paso 2 y, a continuación, haga clic en **Importar**.



6. Para ver las propiedades de un usuario local, selecciónelo y haga clic en **Modificar**.



Además de las propiedades de nombre, están disponibles estas propiedades de ASM:

- **Origen de datos de ASM:** El origen de los datos de la clase, como **CSV** o **SFTP**.
- **ID de Apple administrado por ASM:** Un ID de Apple administrado puede incluir el nombre de la institución y `appleid`. Por ejemplo, el ID puede ser del tipo elsagomez@appleid.micolegio.edu. XenMobile requiere un ID de Apple administrado para la autenticación.
- **Nombre de la organización de ASM:** El nombre que dio a la cuenta en XenMobile.
- **Tipo de código de acceso de ASM:** La directiva Contraseña de la persona: **complejo** (una contraseña de no alumno con ocho o varios números y letras), **cuatro** (dígitos) o **seis** (dígitos).
- **ID personal único de ASM:** Un identificador del usuario.
- **Estado personal de ASM:** Especifica si el ID de Apple administrado está **Activo** o **Inactivo**. Este estado se activa después de que el usuario proporcione la nueva contraseña de la cuenta de ID de Apple administrado.
- **Título personal de ASM:** Puede ser profesor, alumno u otro.
- **ID personal único de ASM:** Un identificador único para el usuario.
- **ID del sistema de origen de ASM:** Identificador del origen del sistema.
- **Curso del alumno de ASM:** Información del curso del alumno (los profesores no usan esta opción).

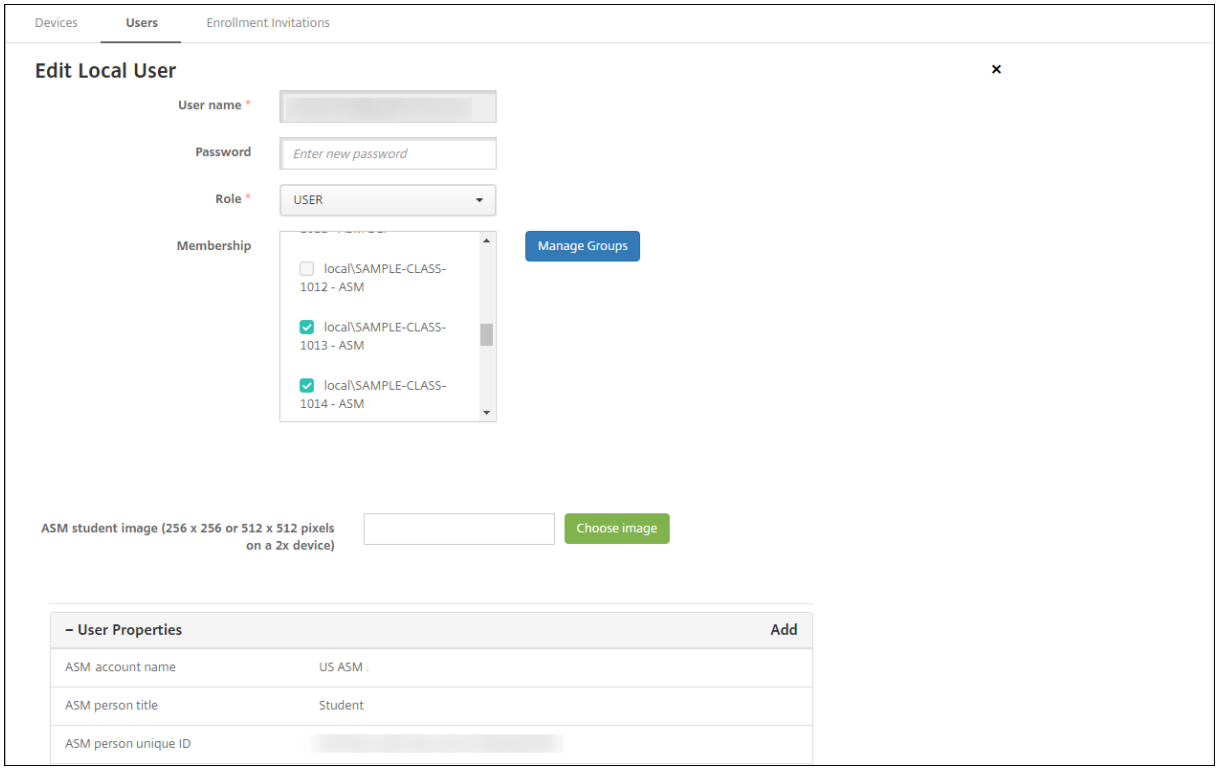
Paso 6: Agregue, si quiere, fotos de estudiantes

Puede agregar una foto de cada estudiante. Si los profesores utilizan la aplicación Aula de Apple, esas fotos aparecen en esa aplicación.

Para las fotos, se recomienda:

- Resolución: 256 x 256 píxeles (o 512 x 512 píxeles en un dispositivo 2x)
- Formato: JPEG, PNG o TIFF

Para agregar una foto, vaya a **Administrar > Usuarios**, seleccione un usuario, haga clic en **Modificar** y, a continuación, haga clic en **Elegir imagen**.



Paso 7: Planifique y agregue recursos y grupos de entrega a XenMobile

Con un grupo de entrega, se especifican los recursos que se van a implementar en categorías de usuarios. Por ejemplo, puede crear un grupo de entrega para profesores y alumnos. También puede optar por crear varios grupos de entrega para personalizar las aplicaciones, el contenido multimedia y las directivas que se enviarán a los diferentes profesores o alumnos. Asimismo, puede crear uno o varios grupos de entrega por clase. También puede crear uno o varios grupos de entrega para los administradores (otro personal existente en el centro educativo).

Los recursos que implemente en los dispositivos de usuario incluyen directivas de dispositivo, aplicaciones de compras por volumen y libros de iBooks.

- Directivas de dispositivo:

  Si los profesores utilizan la aplicación Aula, se necesita la directiva de configuración de la educación. No olvide consultar otras directivas de dispositivo para determinar cómo configurar y restringir los iPads de profesores y alumnos.

- Aplicaciones de compras por volumen:

  XenMobile requiere que implemente las aplicaciones de compras por volumen como aplicaciones obligatorias para los usuarios de Educación. XenMobile no admite la implementación de esas aplicaciones de compras por volumen como opcionales.

  Si usa la aplicación Aula de Apple, impleméntela solamente en los dispositivos de los profesores.

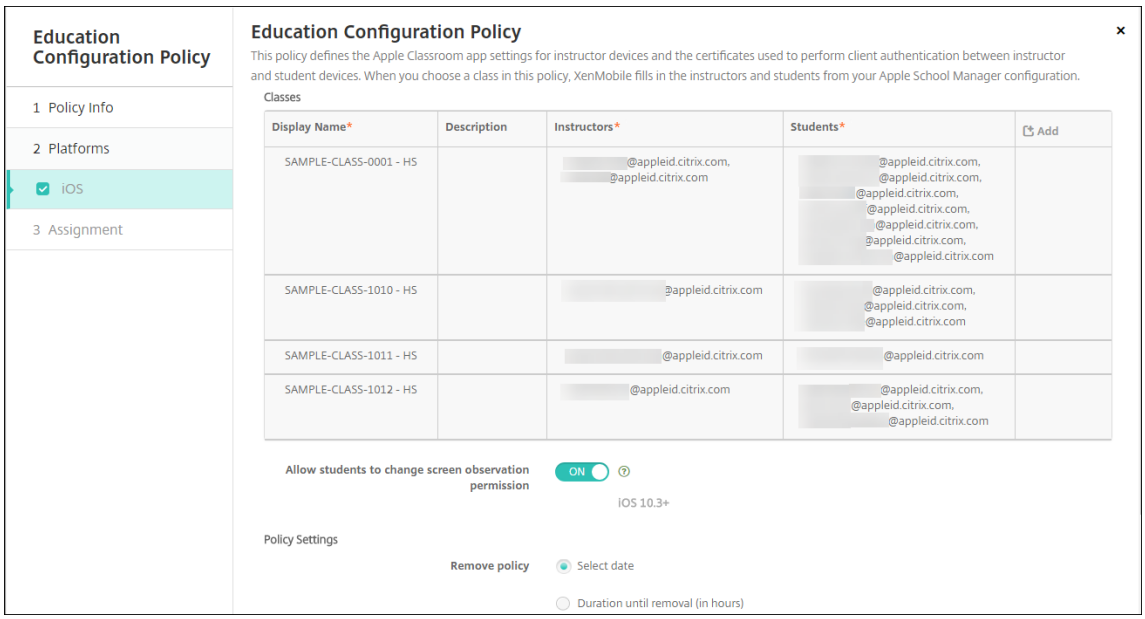
  Implemente las demás aplicaciones que quiera proporcionar a profesores o alumnos. Esta solución no usa la aplicación Citrix Secure Hub, de modo que no es necesario implementarla a profesores o alumnos.

- iBooks de compras por volumen:

  Una vez que XenMobile se conecte a su cuenta de ASM, los libros de iBooks que haya adquirido aparecen en la consola de XenMobile, en **Configurar > Multimedia**. Los libros de iBooks que figuran en dicha página están disponibles para agregarlos a grupos de entrega. XenMobile solo admite que se agreguen libros de iBooks como contenido multimedia obligatorio.

Tras determinar los recursos y los grupos de entrega correspondientes a profesores y alumnos, puede crear esos elementos en la consola de XenMobile.

1. Cree las directivas de dispositivo que quiera implementar en los dispositivos de profesores o alumnos. Para obtener información acerca de la directiva de dispositivo “Configuración de la educación”, consulte Directiva de configuración de la educación.

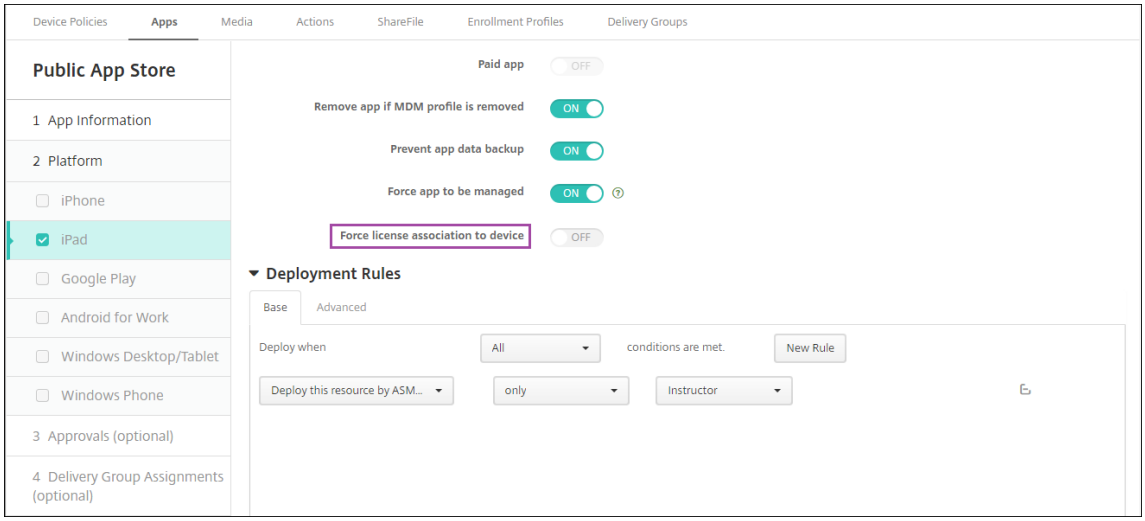


Para obtener más información acerca de las directivas de dispositivo, consulte Directivas de dispositivo y los artículos concretos de directiva.

2. Configure aplicaciones (**Configurar > Aplicaciones**) y iBooks (**Configurar > Multimedia**):

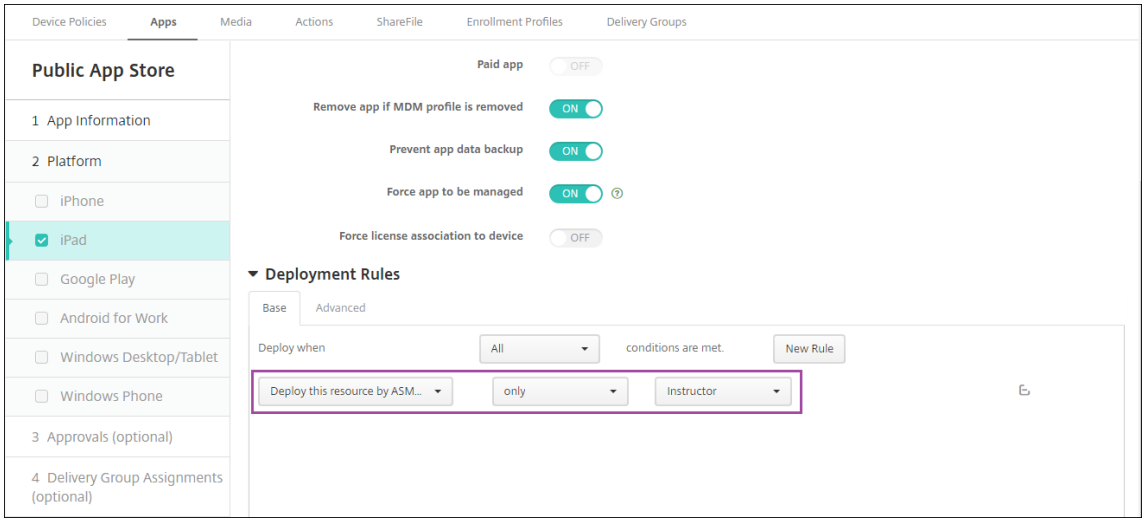
   - De forma predeterminada, XenMobile asigna aplicaciones y libros de iBooks por usuario. Durante la primera implementación, tanto profesores como alumnos reciben una solicitud para registrarse en ASM. Después de aceptar la invitación, los usuarios reciben sus aplicaciones y sus libros de iBooks de ASM durante la siguiente implementación (en las seis horas siguientes). Citrix recomienda forzar la implementación de aplicaciones y libros de iBooks a usuarios nuevos de ASM. Para ello, seleccione el grupo de entrega y haga clic en **Implementar**.

     Puede asignar aplicaciones (pero no libros de iBooks) por dispositivo. Para ello, **active** el parámetro **Forzar asociación de licencia con el dispositivo**. Cuando se asignan aplicaciones a nivel de dispositivo, los usuarios no reciben una invitación para participar en las compras por volumen de Apple.



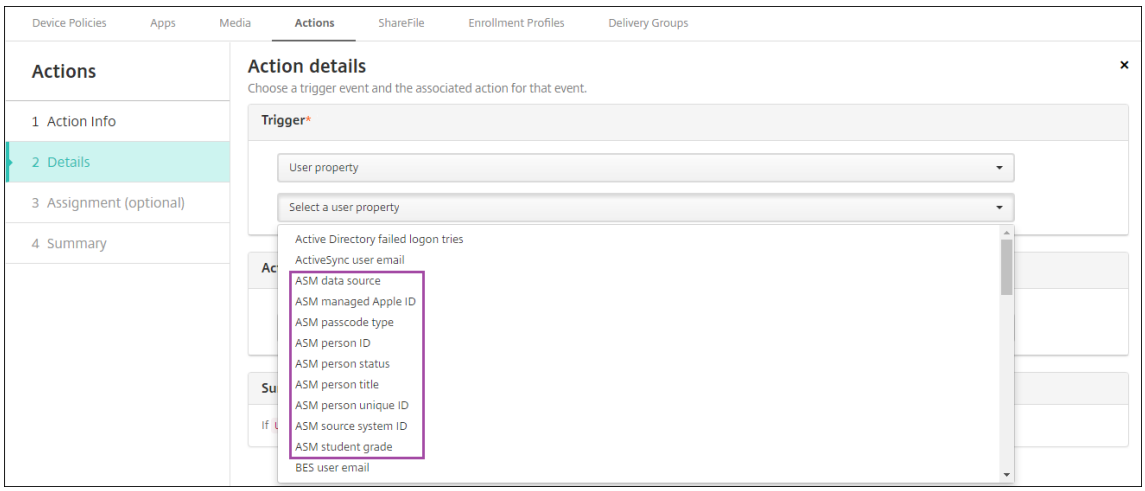
- Para implementar una aplicación solo a profesores, seleccione un grupo de entrega que incluya solo profesores o use la siguiente regla de implementación:

```
Deploy this resource by ASM device type
only
Instructor
<!--NeedCopy-->
```



- Si quiere obtener ayuda para agregar aplicaciones de compras por volumen, consulte Agregar una aplicación de tienda pública.

3. Opcional. Cree acciones basadas en las propiedades de usuario de ASM. Por ejemplo, puede crear una acción para enviar una notificación a los dispositivos de alumno cuando se instale una nueva aplicación en ellos. También puede optar por crear una acción que se active con una propiedad de usuario determinada, como se muestra en el siguiente ejemplo.

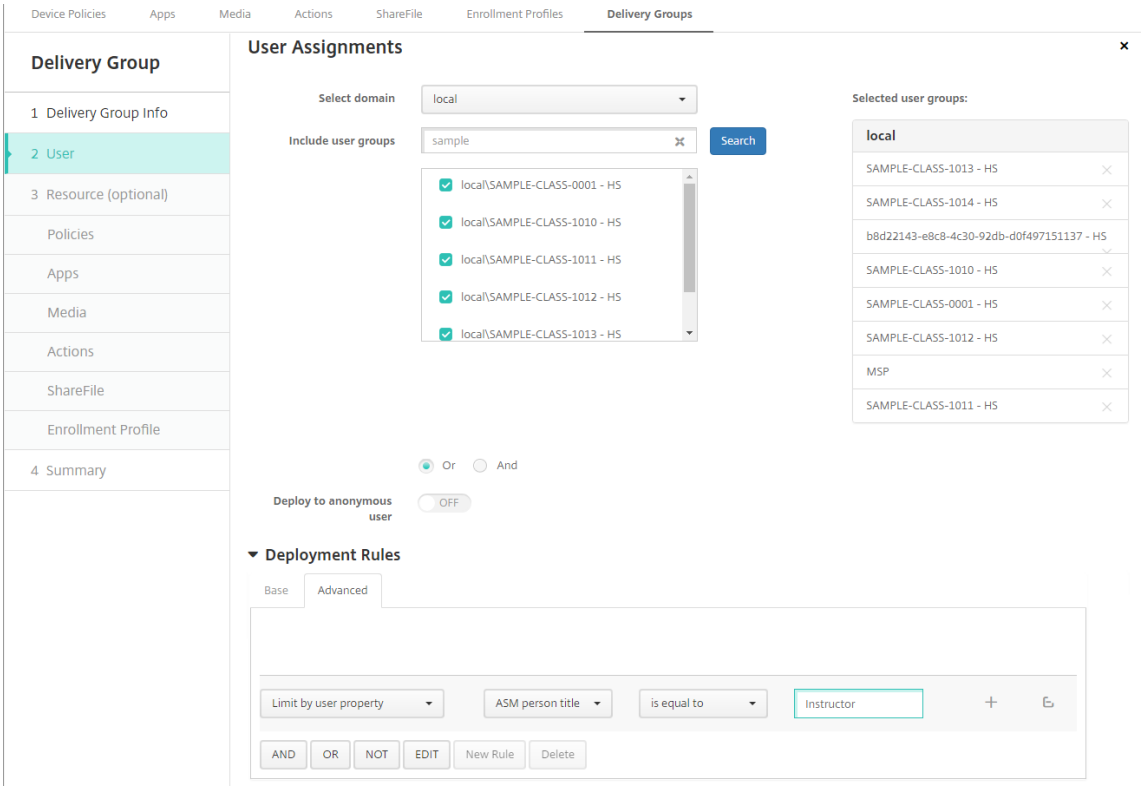


Para crear una acción, vaya a **Configurar > Acciones**. Para obtener información detallada sobre cómo configurar las acciones, consulte Acciones automatizadas.

4. En **Configurar > Grupos de entrega**, cree grupos de entrega para profesores y para alumnos. Elija las clases que se importaron desde ASM. Asimismo, cree una regla de implementación para profesores y alumnos.

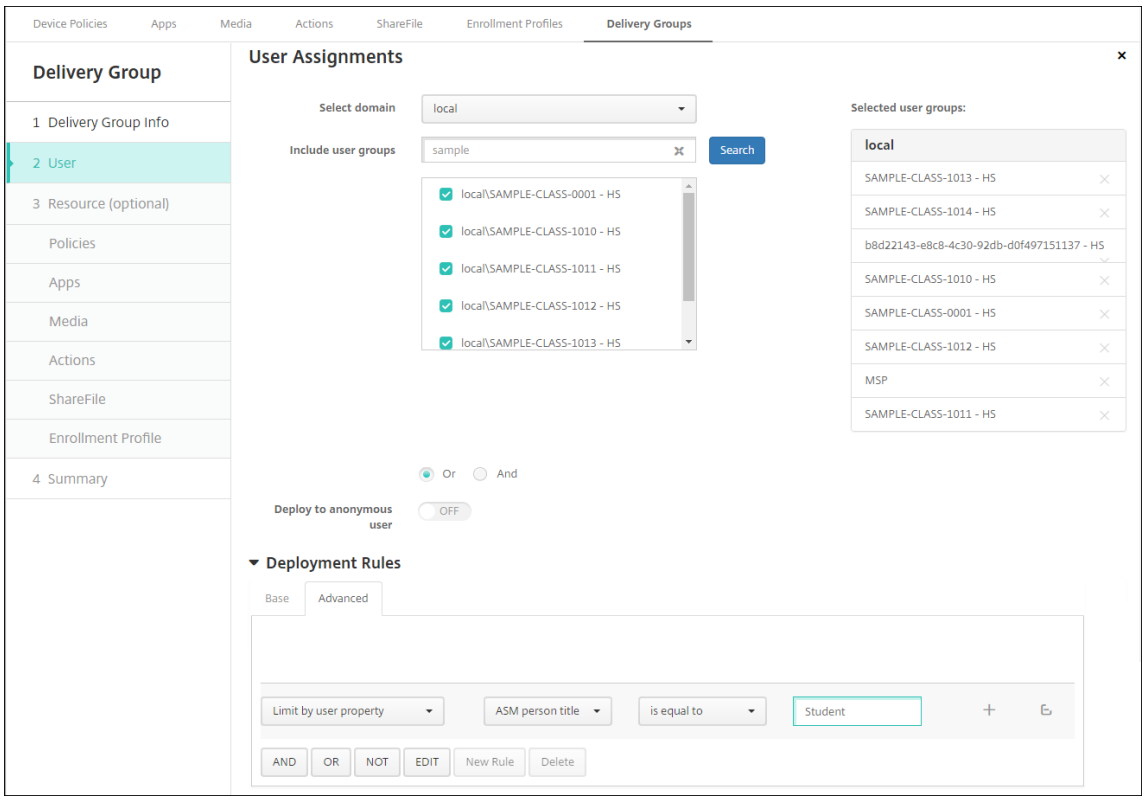
   Por ejemplo, las siguientes asignaciones de usuario son para profesores. La regla de implementación es:

```
Limit by user property
ASM person title
is equal to
Instructor
<!--NeedCopy-->
```

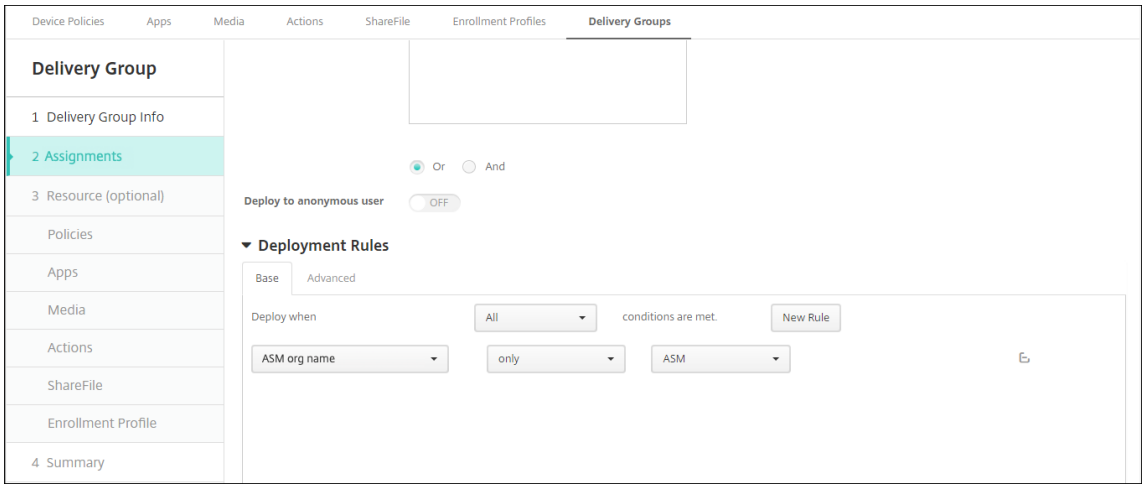



En cambio, las siguientes asignaciones de usuario son para los alumnos. La regla de implementación es:

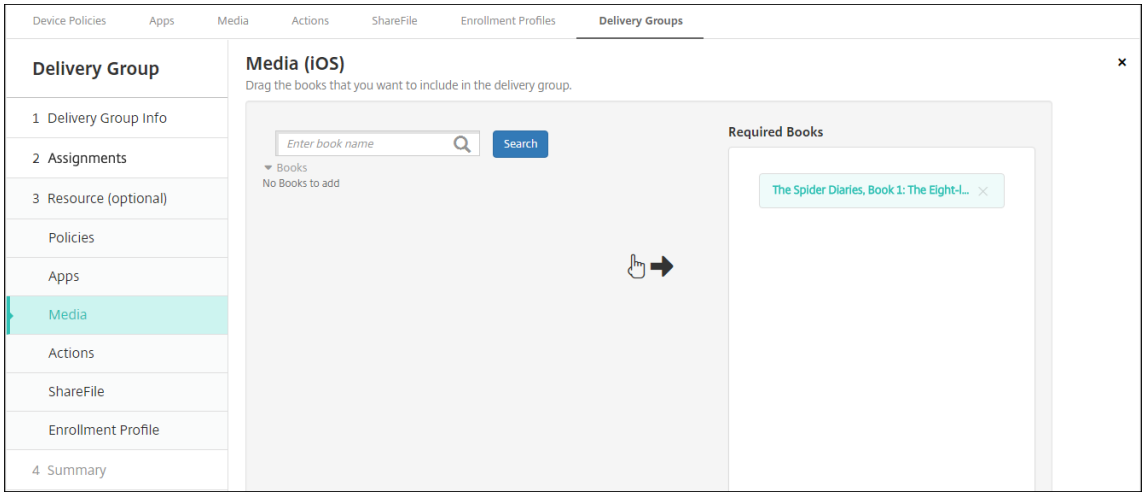
```
Limit by user property
ASM person title
is equal to
Student
<!--NeedCopy-->
```

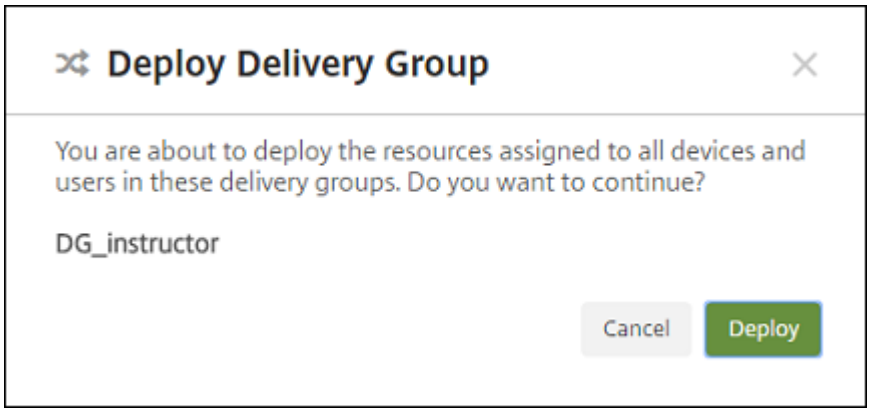
También puede filtrar un grupo de entrega mediante una regla de implementación basada en el nombre de organización de ASM.



5. Asigne los recursos a los grupos de entrega. En el siguiente ejemplo se muestra un libro de iBook que contiene un grupo de entrega.



En el siguiente ejemplo se muestra el cuadro de confirmación que aparece cuando se selecciona un grupo de entrega y se hace clic en **Implementar**.



Para obtener más información, consulte “Para modificar un grupo de entrega” y “Para implementar en grupos de entrega” en Implementar recursos.

Paso 8: Pruebe las inscripciones de dispositivos de profesor y estudiante

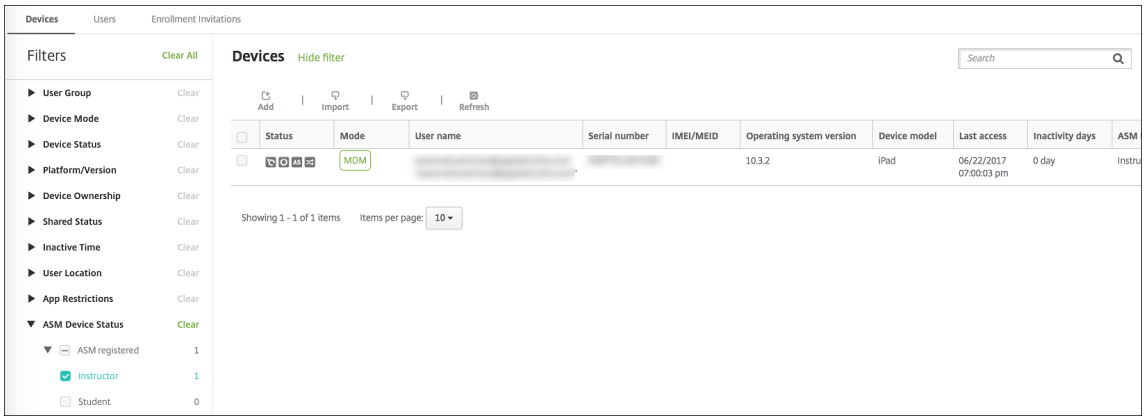
Puede inscribir dispositivos mediante uno de los siguientes métodos:

- Un administrador de centro educativo puede inscribir dispositivos de profesores y alumnos con la contraseña de usuario que se estableció en la consola de XenMobile. Por lo tanto, puede facilitar a los usuarios dispositivos que ya están configurados con las aplicaciones y el contenido multimedia pertinente.
- Tras recibir los dispositivos, los usuarios pueden inscribirse con la contraseña de usuario que se les haya dado. Una vez completada la inscripción, XenMobile envía las directivas de dispositivo, las aplicaciones y el contenido multimedia a los dispositivos.

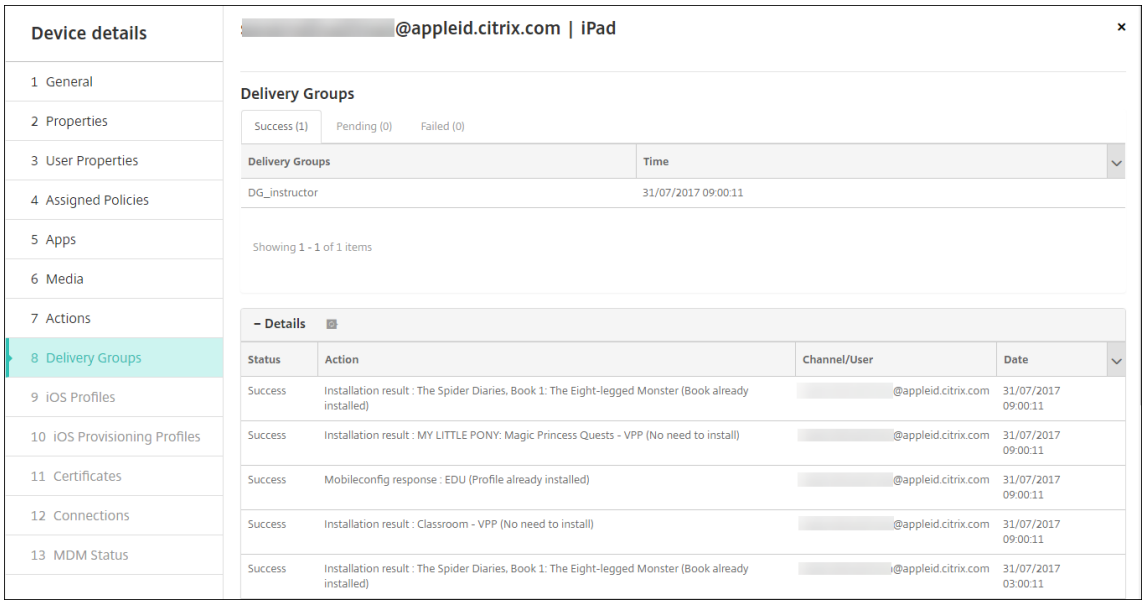
Para probar la inscripción, use los dispositivos del Programa de implementación de Apple que están vinculados a ASM.

1. Si los dispositivos no están vinculados a ASM, borre el contenido y los parámetros de estos. Para ello, restablezca el disco duro a los valores de fábrica.
2. Inscriba un dispositivo de ASM con un profesor. A continuación, inscriba un dispositivo de ASM con un alumno.
3. En la página **Administrar > Dispositivos**, compruebe que ambos dispositivos de ASM se inscribieron en modo de solo MDM.

   Puede filtrar la página **Dispositivos** por el estado del dispositivo de ASM: **Registrado en ASM**, **Compartido en ASM**, **Profesor** y **Alumno**.



4. Para verificar que los recursos MDM se hayan implementado correctamente en el dispositivo: seleccione cada dispositivo, haga clic en **Modificar** y revise la información de las distintas páginas.



Paso 9: Distribuya los dispositivos

Apple recomienda organizar un evento para poder distribuir dispositivos a profesores y alumnos.

Si no va a distribuir dispositivos preinscritos, también deberá dar lo siguiente a los usuarios:

- Contraseñas de XenMobile para la inscripción
- Contraseñas temporales de ASM para los ID de Apple administrados.

A continuación, se expone la primera experiencia que tendrá el usuario.

1. La primera vez que un usuario inicia su dispositivo después de un restablecimiento del disco duro, XenMobile solicita inscribir el dispositivo en la pantalla de inscripción.
2. El usuario proporciona su ID de Apple administrado y la contraseña de XenMobile que se usa para autenticarse en XenMobile.
3. En el paso de configuración del ID de Apple, el dispositivo pide al usuario que introduzca su ID de Apple administrado y su contraseña temporal de ASM. Esos elementos autentican al usuario en los servicios de Apple.
4. El dispositivo pide al usuario que cree una contraseña para su ID de Apple administrado. Esa contraseña se va a utilizar para proteger sus datos en iCloud.
5. Al final del Asistente de configuración, XenMobile empieza a instalar las directivas, las aplicaciones y el contenido multimedia en el dispositivo. En cuanto a las aplicaciones y los libros de iBooks asignados a cada usuario, el asistente pide a profesores y alumnos que se registren en compras por volumen. Después de aceptar la invitación, los usuarios reciben sus aplicaciones y sus libros de iBooks de compras por volumen durante la siguiente implementación (en las seis horas siguientes).

Configurar iPads compartidos

Varios alumnos de un aula pueden compartir un iPad para las diferentes materias o asignaturas impartidas por uno o varios profesores.

O usted o los profesores inscriben los iPads compartidos y luego implementan directivas de dispositivo, aplicaciones y archivos multimedia en ellos. A continuación, los alumnos proporcionan sus credenciales administradas de ID de Apple para iniciar sesión en un iPad compartido. Si implementó anteriormente una directiva de configuración de la educación en los dispositivos de los alumnos, no es necesario que inicien sesión como “Otro usuario” para compartir esos dispositivos.

XenMobile utiliza dos canales de comunicación para iPad Compartidos: el canal del sistema para el propietario del dispositivo (instructor) y el canal del usuario para el usuario residente actual (estudiante). XenMobile utiliza esos canales para enviar los comandos MDM apropiados para los recursos que admite Apple.

A continuación, dispone de los recursos que se implementan a través del canal del sistema:

- Directivas de dispositivo: Configuración de la educación, Mensaje de la pantalla bloqueada, Máximo de usuarios residentes y Período de gracia de bloqueo de código de acceso.
- Aplicaciones de compras por volumen basadas en dispositivos

  Apple no admite aplicaciones empresariales ni aplicaciones de compras por volumen basadas en el usuario en la función iPads compartidos. Las aplicaciones instaladas en un iPad compartido son para todo el dispositivo; no se pueden utilizar por usuario.
- iBooks de compras por volumen basados en el usuario

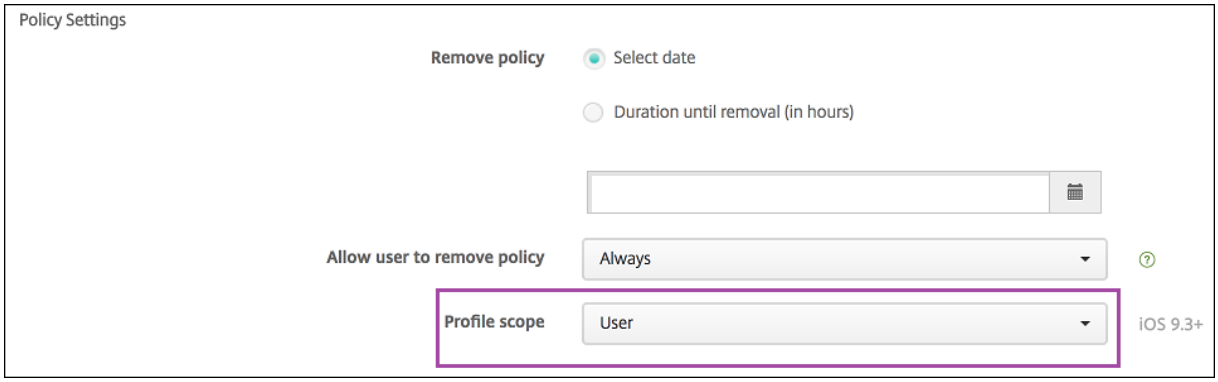
  Apple admite la asignación de iBooks de compras por volumen basados en el usuario en iPads compartidos.

A continuación, dispone de los recursos que se implementan a través del canal del usuario:

- Directivas de dispositivo: Notificaciones de aplicaciones, Diseño de pantalla inicial y Restricciones

  XenMobile solo admite estas directivas por el canal del usuario.

El canal de implementación se especifica cuando se configuran las directivas de dispositivo, en el parámetro **Ámbito del perfil**.



Para eliminar las directivas de dispositivo que implementó por el canal del usuario, debe elegir el **Ámbito de implementación** llamado **Usuario** para la directiva “Eliminación de perfiles”.

Flujo de trabajo general de las tareas

Por lo general, usted distribuye iPads compartidos, preconfigurados y supervisados a los profesores. Los profesores distribuyen a su vez los dispositivos a los alumnos. Si no distribuye iPads compartidos preinscritos a los instructores, deberá suministrarles contraseñas de servidor de XenMobile para que puedan inscribir sus dispositivos.

A continuación, dispone del flujo de trabajo general de las tareas necesarias para configurar e inscribir los iPads compartidos.

1. Utilice la consola de XenMobile Server para agregar cuentas de ASM (**Parámetros > Programa de implementación de Apple**) con el **Modo compartido** habilitado. Para obtener más información, consulte “Administrar cuentas de ASM para iPads compartidos” más adelante.
2. Tal y como se describe en esa sección, debe agregar las directivas, las aplicaciones y los archivos multimedia necesarios a XenMobile. Asigne esos recursos a los grupos de entrega.
3. Haga que los profesores realicen un restablecimiento completo de los iPads compartidos. Aparece la pantalla de administración remota para la inscripción.
4. Los profesores inscriben los iPads compartidos.
   XenMobile implementa los recursos configurados en cada iPad compartido que se haya inscrito. Después de un reinicio automático, los profesores pueden compartir los dispositivos con los alumnos. Aparece una página de inicio de sesión en el iPad.
5. Un alumno elige la clase y después introduce su ID de Apple administrado y la contraseña temporal de ASM.
   El iPad compartido se autentica en ASM y solicita al alumno que cree una contraseña de ASM. La próxima vez que el alumno inicie sesión en el iPad compartido, proporcionará la nueva contraseña de ASM.
6. Otro alumno que comparta el iPad puede iniciar sesión en él, solo será necesario que repita el paso anterior.

Administrar cuentas de ASM para iPads compartidos

Si ya usa XenMobile con Apple Educación, tiene una cuenta ASM configurada en XenMobile para dispositivos que no se comparten, como los dispositivos que utilizan los profesores. Puede usar el mismo ASM y el mismo servidor de XenMobile para dispositivos compartidos y no compartidos.

XenMobile admite estos casos de implementación:

- Un grupo de iPads compartidos por clase

  En este caso, usted asigna los iPads compartidos a una clase de alumnos. Los iPads se quedan en el aula. Los profesores que enseñan otras asignaturas en esa clase usan el mismo grupo de iPads.

- Un grupo de iPads compartidos por profesor

  En este caso, usted asigna los iPads compartidos a un profesor, y este los usa para las distintas clases que enseñe.

Organizar iPads compartidos en grupos de dispositivos

ASM permite agrupar dispositivos. Para ello, debe crear varios servidores MDM. Cuando asigna iPads compartidos a un servidor MDM, crea un grupo de dispositivos para cada grupo de iPads compartidos, por clase o por profesor:

- Grupo de iPads compartidos 1 > Grupo de dispositivos 1 del servidor MDM
- Grupo de iPads compartidos 2 > Grupo de dispositivos 2 del servidor MDM
- Grupo de iPads compartidos N > Grupo de dispositivos N del servidor MDM

Agregar cuentas de ASM a cada grupo de dispositivos

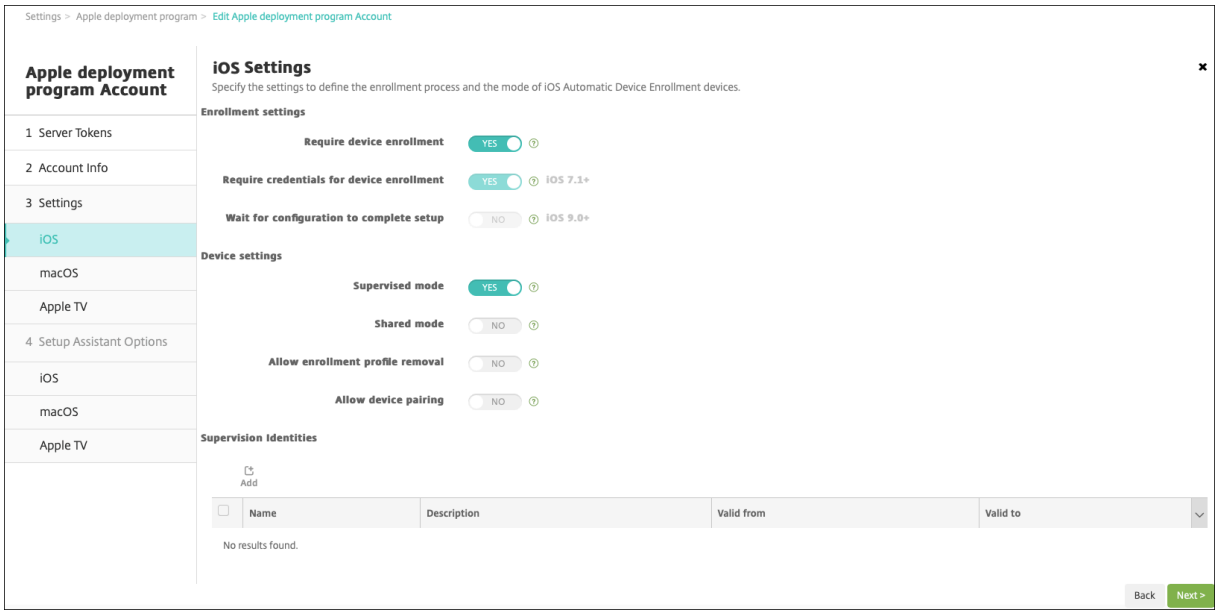
Cuando crea varias cuentas de ASM desde la consola del servidor de XenMobile, importa automáticamente los grupos de iPads compartidos (uno por clase o instructor):

- Grupo de dispositivos 1 del servidor MDM > Grupo de dispositivos 1 de la cuenta
- Grupo de dispositivos 2 del servidor MDM > Grupo de dispositivos 2 de la cuenta
- Grupo de dispositivos N del servidor MDM > Grupo de dispositivos N de la cuenta

A continuación, dispone de los requisitos específicos para iPads compartidos:

- Una cuenta de ASM para cada grupo de dispositivos con estos parámetros habilitados:
  - **Requerir inscripción del dispositivo**
  - **Modo supervisado**
  - **Modo compartido**
- Para una organización educativa determinada, debe usar el mismo **Sufijo de educación** para todas las cuentas de ASM.

Para agregar una cuenta, vaya a **Configuración > Programa de implementación de Apple**.



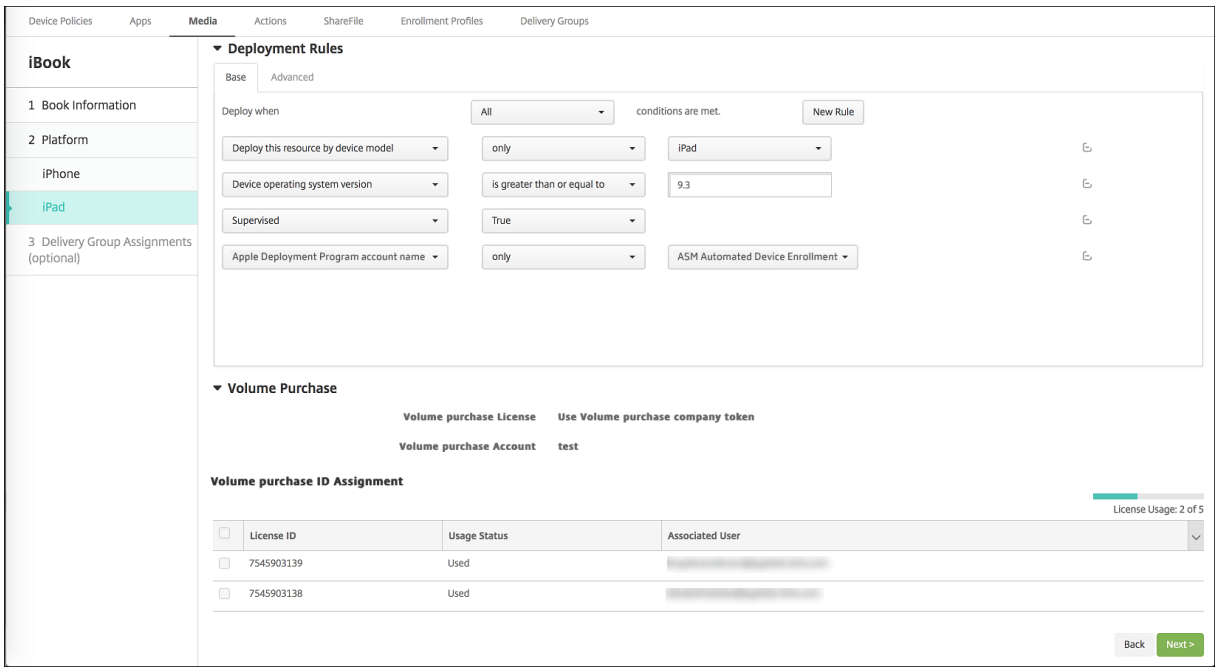
Aplicaciones para iPads compartidos

iPads compartidos admite la asignación de aplicaciones de compras por volumen basadas en el dispositivo. Antes de implementar una aplicación en un iPad compartido, XenMobile envía una solicitud

al servidor de compras por volumen de Apple para asignar licencias de compras por volumen a los dispositivos. Para consultar las asignaciones de compras por volumen, vaya a **Configurar > Aplicaciones > iPad** y expanda **Compras por volumen**.

Multimedia para iPads compartidos

iPads compartidos admite la asignación de iBooks de compras por volumen basada en el usuario. Antes de implementar libros de iBooks en un iPad compartido, XenMobile envía una solicitud al servidor de compras por volumen de Apple para asignar licencias de compras por volumen a los dispositivos. Para consultar las asignaciones de compras por volumen, vaya a **Configurar > Multimedia > iPad** y expanda **Compras por volumen**.



Reglas de implementación para iPads compartidos

Para la implementación de iPads compartidos, las reglas a nivel de grupo de entrega no se aplican porque están relacionadas con propiedades de usuario. Para filtrar las directivas, las aplicaciones y los archivos multimedia por grupo de dispositivos, agregue una regla de implementación para los recursos según el nombre de la cuenta. Por ejemplo:

- Para la cuenta del grupo de dispositivos 1, configure esta regla de implementación:

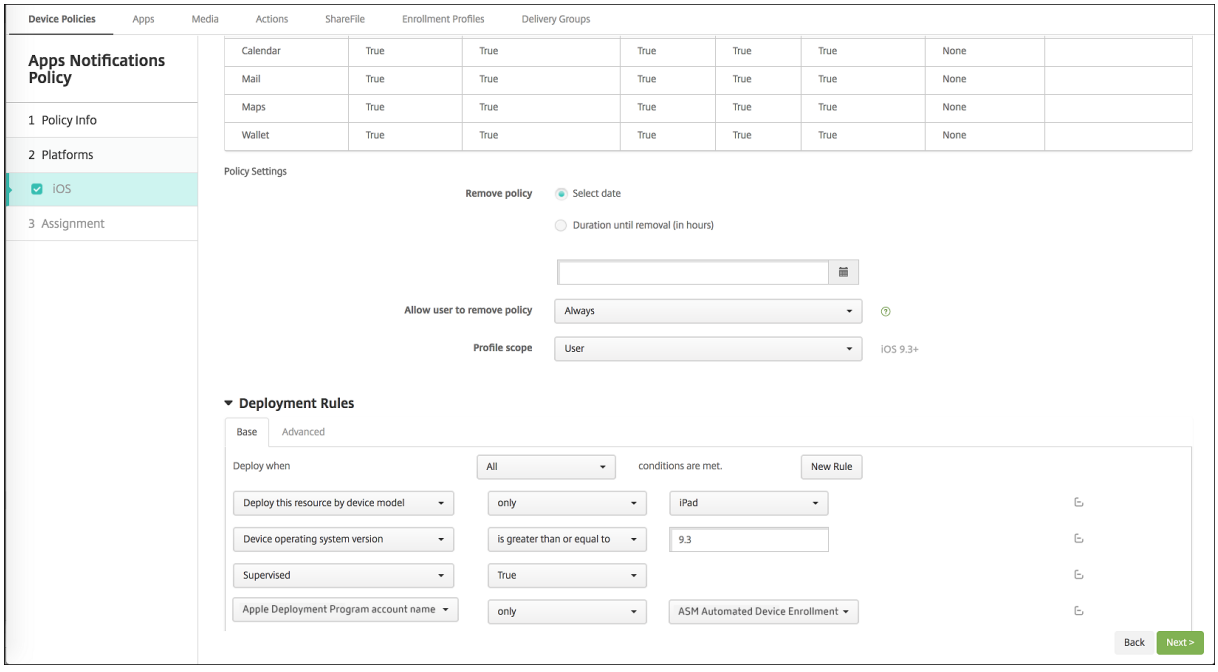
```
Apple Deployment Program account name
Only
Device Group 1 account

<!--NeedCopy-->
```


- Para la cuenta del grupo de dispositivos 2, configure esta regla de implementación:

```
Apple Deployment Program account name
Only
Device Group 2 account

<!--NeedCopy-->
```

- Para la cuenta del grupo de dispositivos N, configure esta regla de implementación:

```
Apple Deployment Program account name
Only
Device Group N account

<!--NeedCopy-->
```

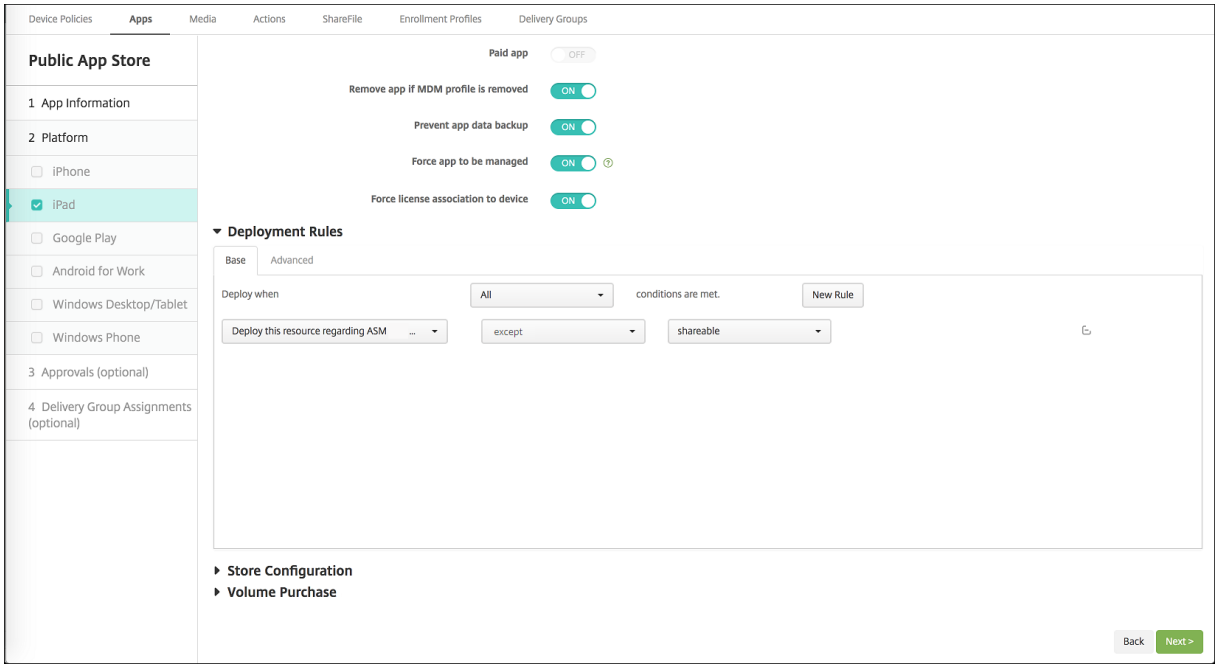


Para implementar la aplicación Aula de Apple solo a los profesores (que utilizan iPads no compartidos), filtre los recursos por estado compartido en ASM con estas reglas de implementación:

```
Deploy this resource regarding ASM shared mode
only
unshared

<!--NeedCopy-->
```

O bien:

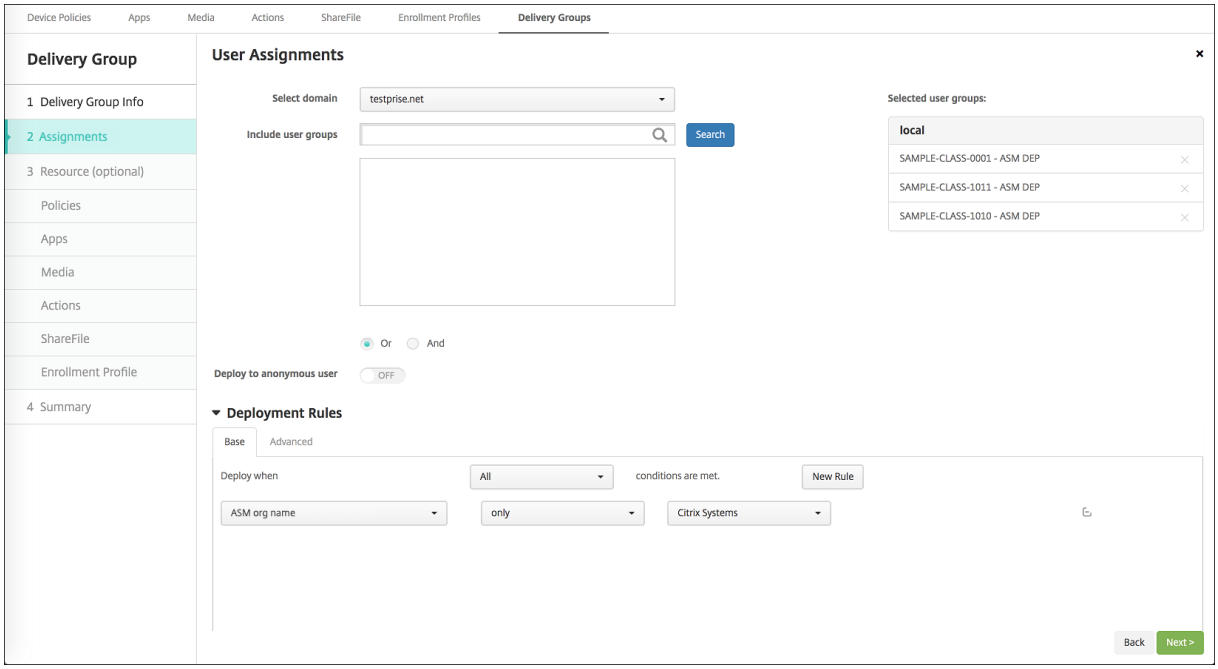

```
Deploy this resource regarding ASM shared mode
except
shareable

<!--NeedCopy-->
```



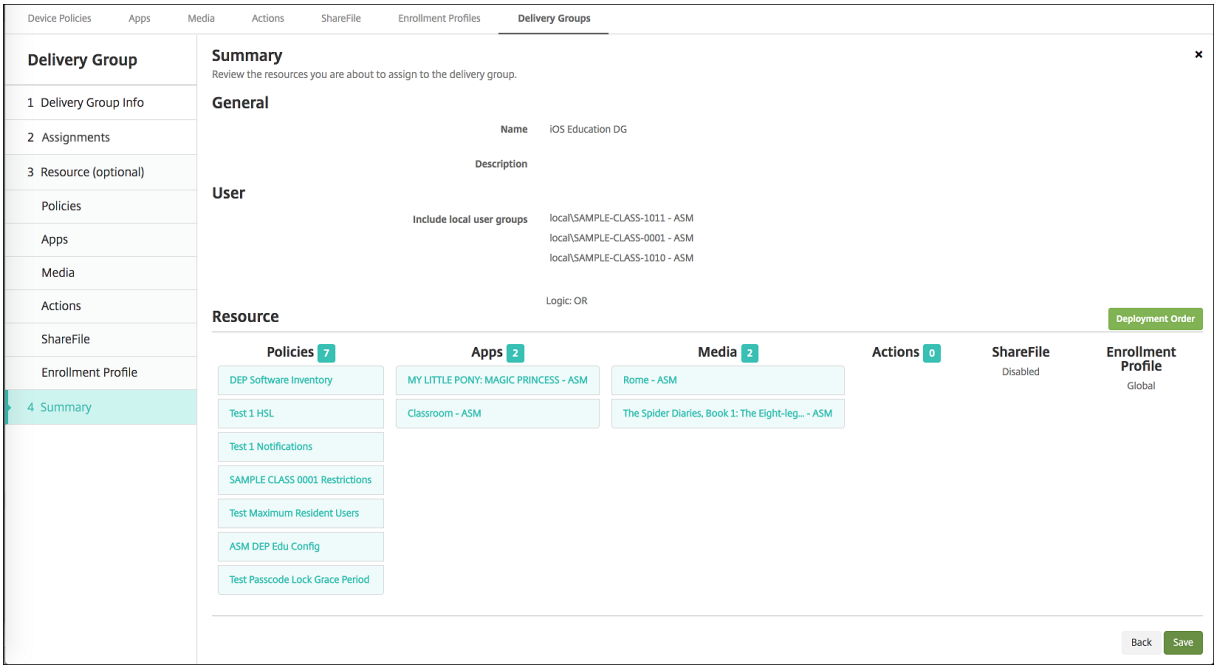
Grupos de entrega para iPads compartidos

Para el grupo de dispositivos de cada profesor:

- Configure un grupo de entrega. Para el profesor, asigne todas las clases definidas en la directiva Configuración de la educación.



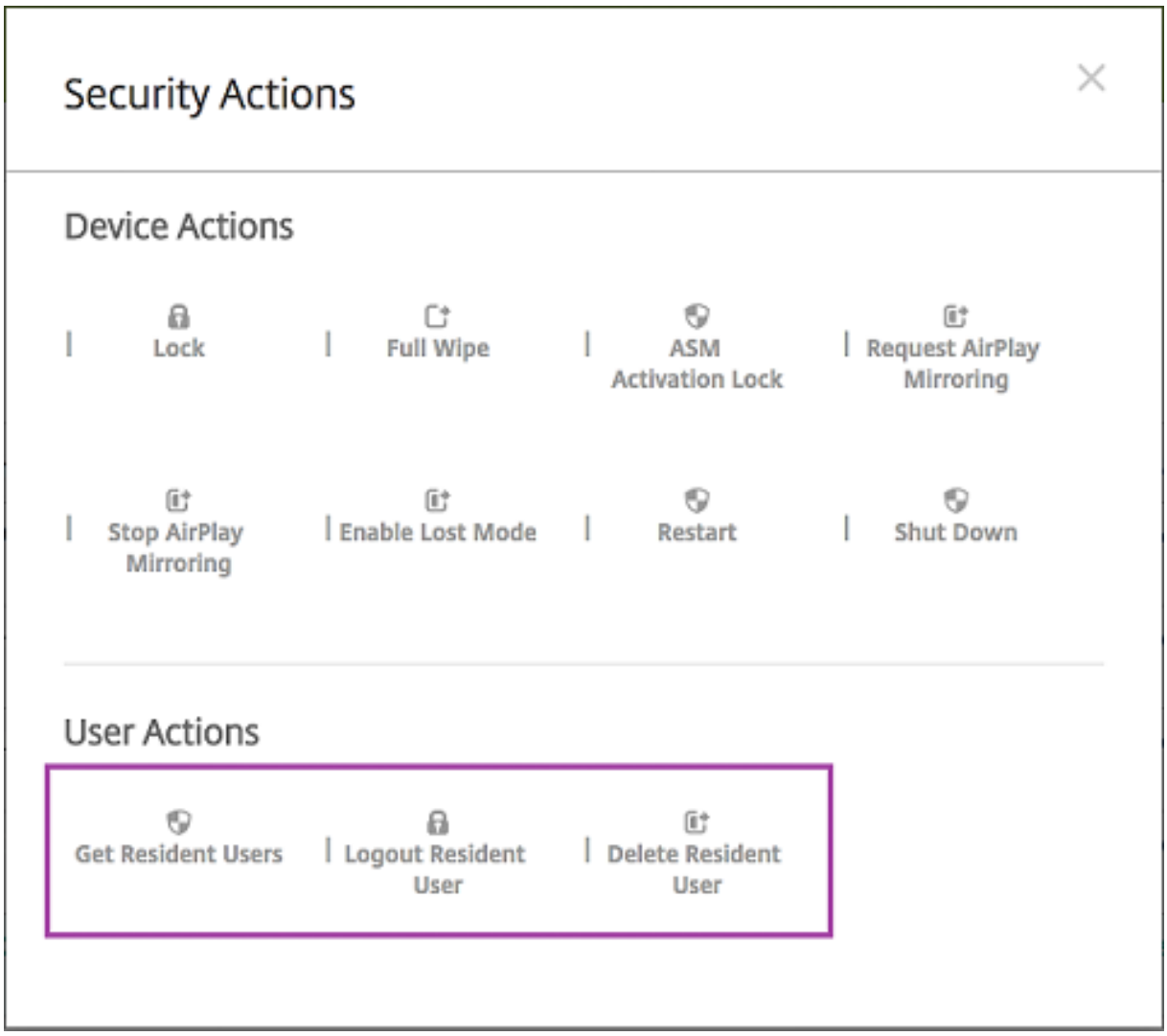
- Ese grupo de entrega debe incluir estos recursos de MDM:
  - Directivas de dispositivo:
    - Configuración de la educación
    - Mensaje de la pantalla bloqueada
    - Notificaciones de aplicaciones
    - Diseño de pantalla inicial
    - Restricciones
    - Máximo de usuarios residentes
    - Período de gracia de bloqueo de código de acceso
  - Aplicaciones de compras por volumen requeridas
  - iBooks de compras por volumen requeridos



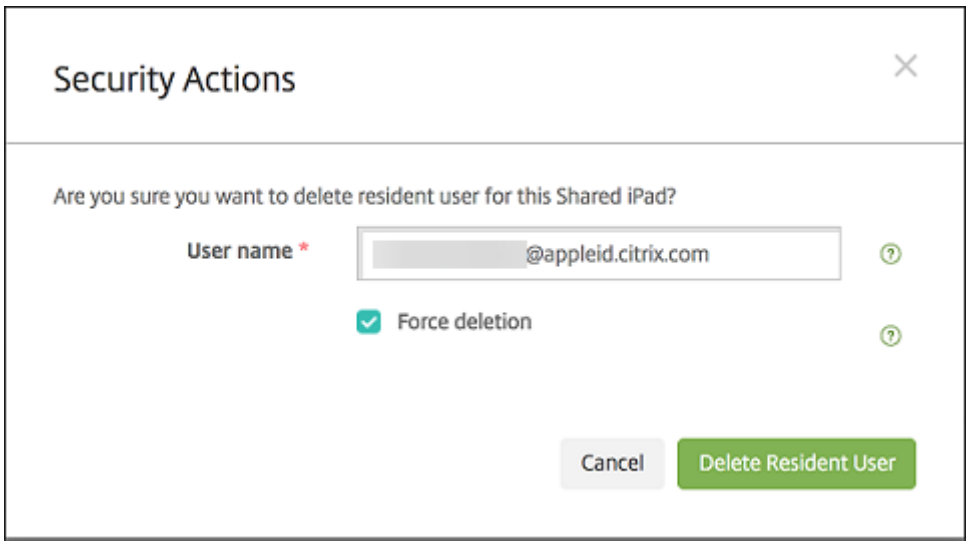
Acciones de seguridad para iPads compartidos

Además de las acciones de seguridad existentes, puede usar estas acciones de seguridad para iPads compartidos:

- **Obtener usuarios residentes:** Ofrece una lista de los usuarios que tienen cuentas activas en el dispositivo actual. Esta acción fuerza una sincronización entre el dispositivo y la consola de XenMobile.
- **Cerrar sesión de usuario residente:** Obliga al cierre de sesión del usuario actual.
- **Eliminar usuario residente:** Elimina la sesión actual de un usuario específico. El usuario puede volver a iniciar sesión.



Después de hacer clic en **Eliminar usuario residente**, puede especificar el nombre del usuario.

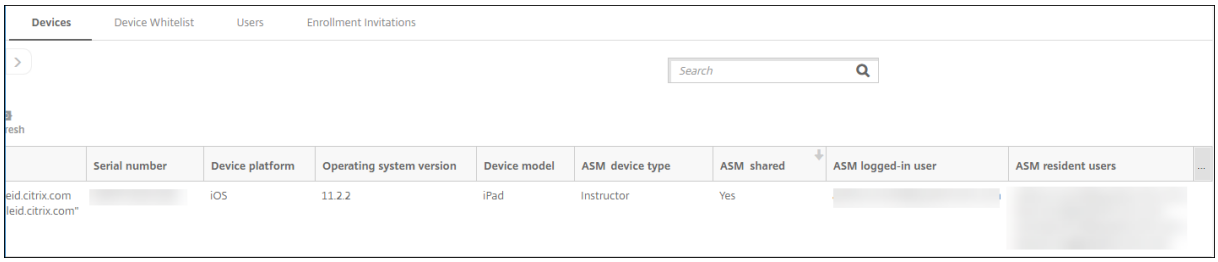


Los resultados de las acciones de seguridad aparecen en las páginas **Administrar > Dispositivos > General** y **Administrar > Dispositivos > Grupos de entrega**.

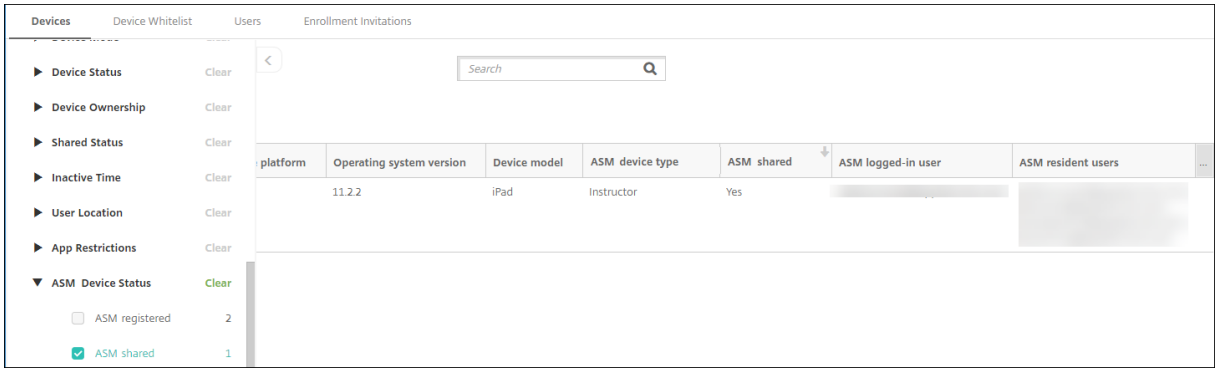
Obtener información sobre iPads compartidos

Dispone de información específica de iPads compartidos en la página **Administrar > Dispositivos**:

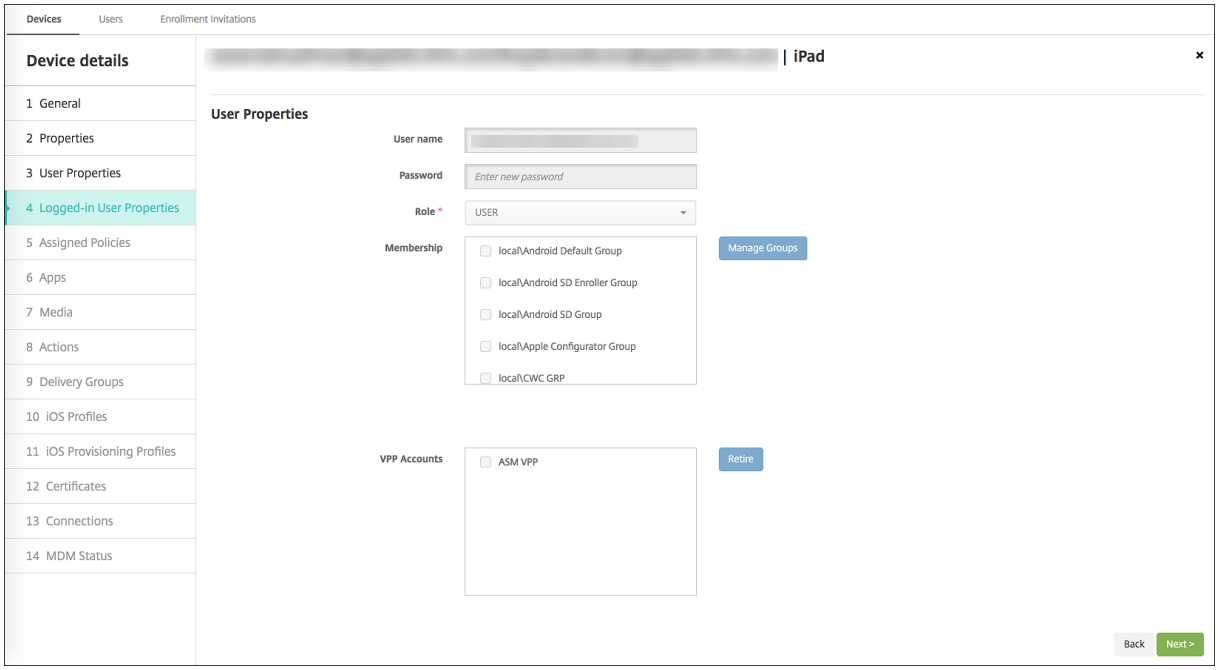
- Puede ver:
  - Si un dispositivo se comparte (**Compartido en ASM**)
  - Quién está conectado al dispositivo compartido (**Usuario ASM conectado**)
  - Todos los usuarios asignados al dispositivo compartido (**Usuarios residentes de ASM**)

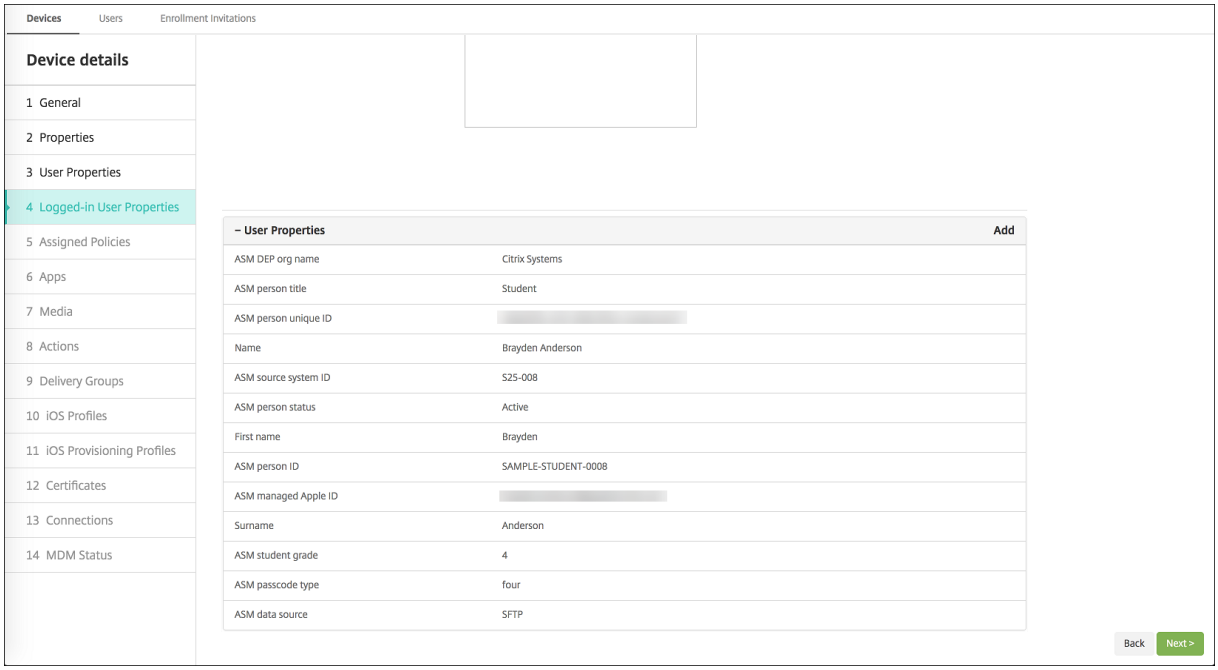


- Puede filtrar la lista de dispositivos por el **Estado del dispositivo ASM:**

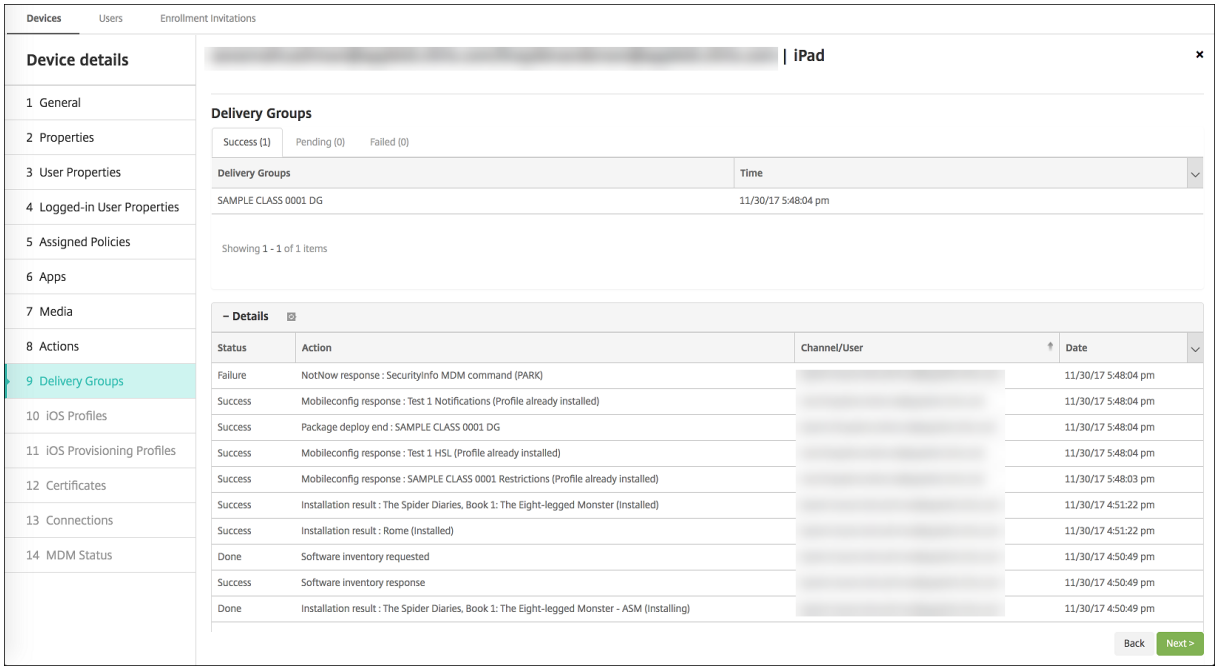


- Puede consultar datos sobre el usuario que inició sesión en un iPad compartido desde la página **Administrar > Dispositivos > Propiedades del usuario conectado**.

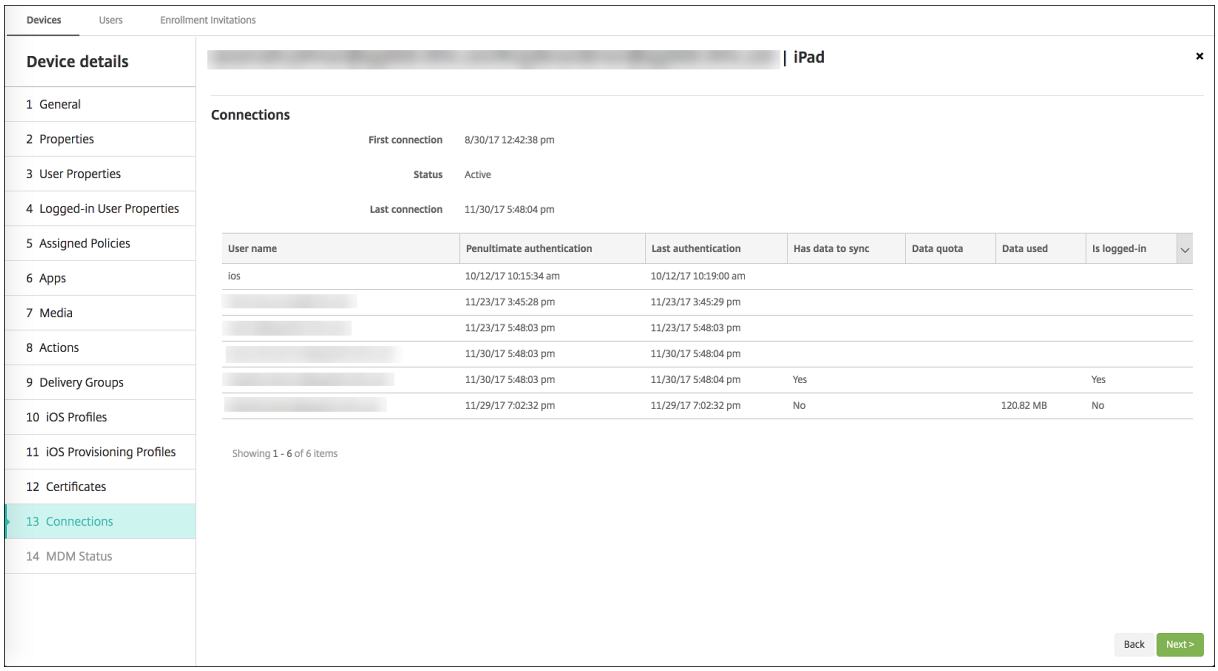




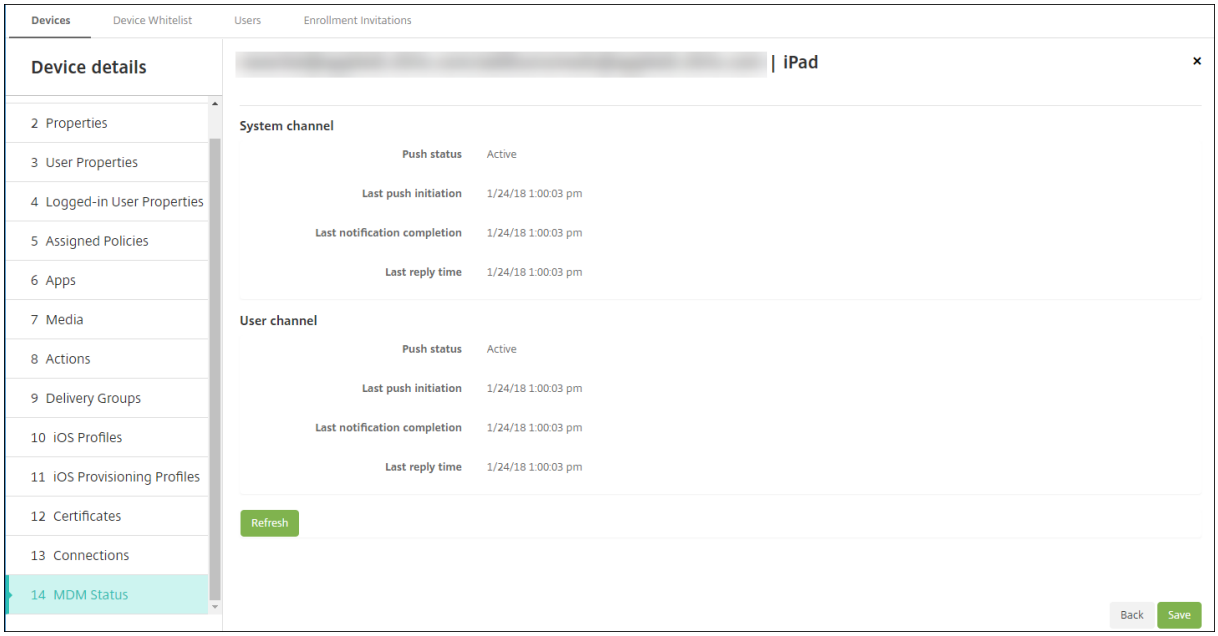
- Puede ver el canal utilizado para implementar recursos a los profesores y los usuarios en un grupo de entrega desde la página **Administrar > Dispositivos > Grupos de entrega**. La columna **Canal/usuario** muestra el tipo (**Sistema** o **Usuario**) y el destinatario (profesor o alumno).



- Puede obtener información sobre los usuarios residentes:
  - **Tiene datos para sincronizar:** Si el usuario tiene datos que sincronizar con la nube.
  - **Cuota de datos:** La cuota de datos establecida para el usuario en bytes. Puede que esta cuota no aparezca si las cuotas de los usuarios están temporalmente desactivadas o no se aplican al usuario.
  - **Datos utilizados:** La cantidad de datos utilizados por el usuario en bytes. Puede que no aparezca ningún valor si se produce un error mientras el sistema recopila la información.
  - **Está conectado:** Si el usuario inició sesión en el dispositivo.



- Puede ver el estado de envío por ambos canales.



Administrar datos de profesores, alumnos y clases

Cuando administre datos de profesores, alumnos y clases, tenga en cuenta lo siguiente:

- No cambie los ID de Apple administrados una vez que haya importado la información de ASM en XenMobile. XenMobile también utiliza los identificadores de usuario de ASM para identificar a los usuarios.
- Si agrega o modifica los datos de clase en ASM después de crear una o varias directivas “Configuración de la educación”: modifique las directivas y, a continuación, vuelva a implementarlas.
- Si una clase cambia de profesor después de que haya implementado la directiva “Configuración de la educación”, revise la directiva para comprobar que se haya actualizado en la consola de XenMobile y, a continuación, vuelva a implementarla.
- Si actualiza las propiedades de usuario en el portal de ASM, XenMobile también actualiza esas propiedades en la consola. Sin embargo, XenMobile no recibe la propiedad “Título personal de ASM” (alumno, profesor u otro) de la misma forma que recibe las demás propiedades. Por lo tanto, si cambia el “Título personal de ASM” en ASM, complete los siguientes pasos para reflejar ese cambio en XenMobile.

Para administrar los datos:

1. En el portal de ASM, actualice el curso del alumno y borre el curso del profesor.
2. Si cambia una cuenta de alumno a una cuenta de profesor, quite al usuario de la lista de alumnos que corresponda a la clase. A continuación, agregue el usuario a la lista de profesores de la

misma clase u otra.

Si cambia una cuenta de profesor a una cuenta de alumno, quite al usuario de la clase. A continuación, agregue el usuario a la lista de alumnos en la misma clase o en otra. Sus actualizaciones aparecerán en la consola de XenMobile tras la siguiente sincronización (cada cinco minutos de forma predeterminada) o la siguiente obtención de datos (cada 24 horas de forma predeterminada).

3. Modifique la directiva de configuración de la educación para aplicar el cambio y vuelva a implementarla.

    - Si elimina a un usuario en el portal de ASM, XenMobile también eliminará a ese usuario de la consola de XenMobile después de una obtención de datos.

      Puede reducir el intervalo entre dos puntos de referencia. Para ello, cambie este valor de propiedad de servidor: **bulk.enrollment.fetchRosterInfoDelay** (el valor predeterminado es **1440** minutos).

    - Después de implementar los recursos: si un alumno se une a una clase, cree un grupo de entrega que solo contenga a ese alumno e implemente los recursos en el dispositivo de ese alumno.

    - Si un alumno o profesor pierde su contraseña temporal, deberá ponerse en contacto con el administrador de ASM. El administrador puede proporcionar una contraseña temporal o generar una nueva.

Administrar un dispositivo perdido o robado inscrito en el Programa de implementación de Apple de Apple School Manager

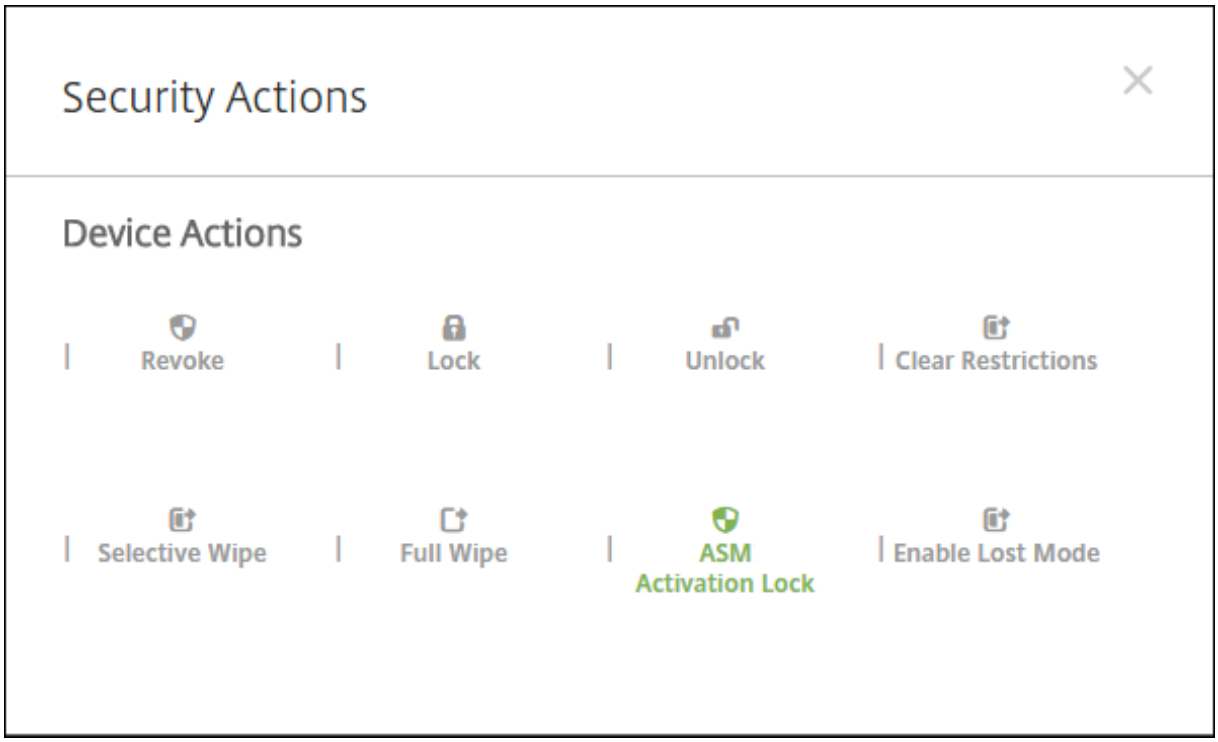
El servicio “Buscar Mi iPhone” o “Buscar Mi iPad” de Apple incluye la función “Bloqueo de activación”. El “Bloqueo de activación” impide que usuarios no autorizados usen o revendan un dispositivo perdido o robado que está inscrito en el Programa de implementación de Apple.

XenMobile incluye la acción de seguridad **Bloqueo de activación de ASM**, que permite enviar un código de bloqueo a un dispositivo inscrito en el Programa de implementación de Apple de ASM.

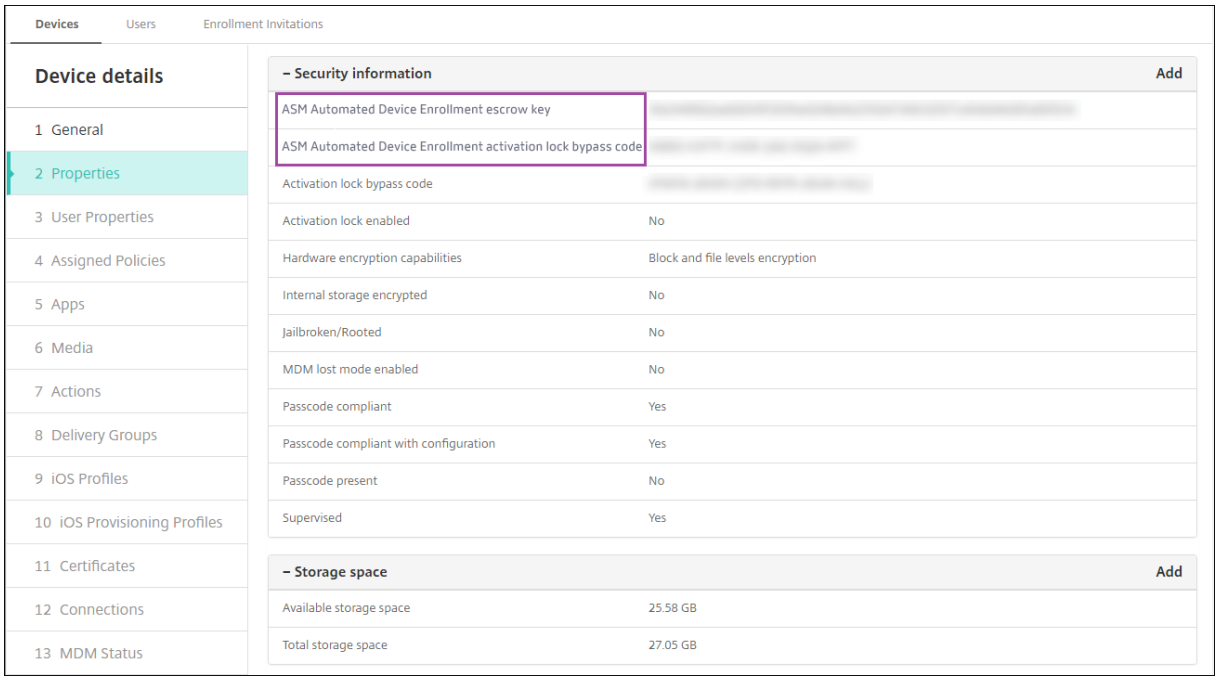
Cuando se usa la acción de seguridad **Bloqueo de activación de ASM**, XenMobile puede localizar dispositivos sin que los usuarios habiliten el servicio “Buscar Mi iPhone” o “Buscar Mi iPad”. Si un dispositivo de ASM se restablece a los valores de fábrica o se borran todos los datos que contiene, el usuario debe proporcionar su ID de Apple administrado y la contraseña para desbloquear el dispositivo.

Para quitar el bloqueo desde la consola, haga clic en la acción de seguridad **Omisión del bloqueo de activación**. Para obtener información sobre cómo omitir un bloqueo de activación, consulte Omitir un bloqueo de activación de iOS. El usuario también puede dejar en blanco el inicio de sesión y escribir el **Código de anulación del bloqueo de activación de ASM** en el lugar de la contraseña. Esa información está disponible en **Detalles del dispositivo**, en la ficha **Propiedades**.

Para establecer el bloqueo de activación, vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Seguridad** y, a continuación, haga clic en **Bloqueo de activación de ASM**.

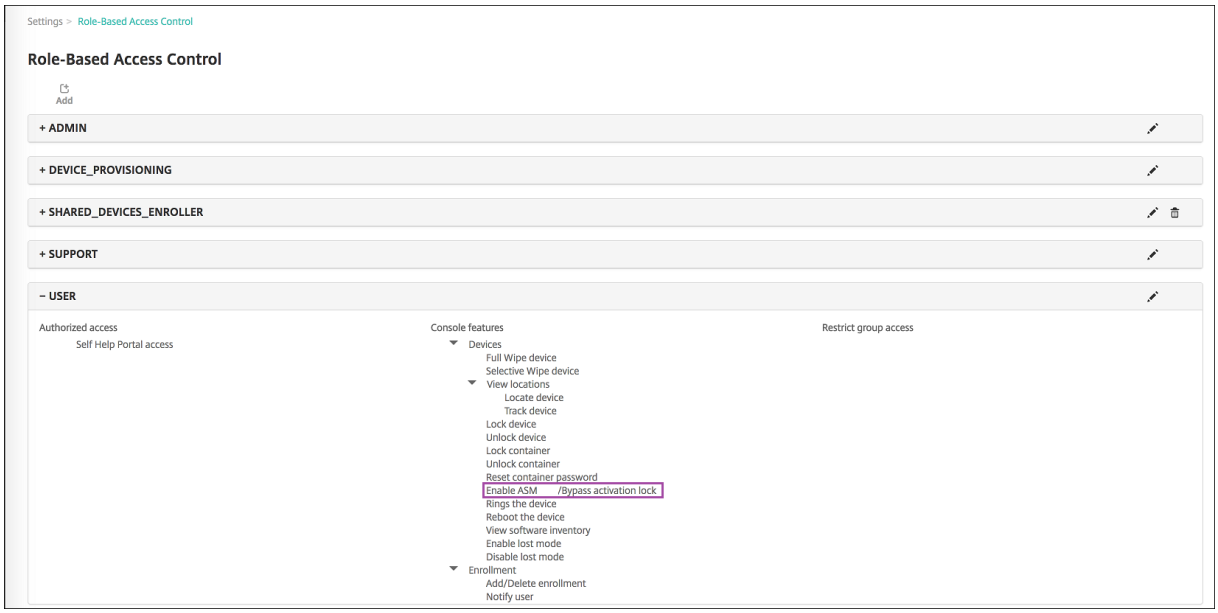


Las propiedades **Clave de custodia de ASM** y **Código de anulación del bloqueo de activación de ASM** aparecen en **Detalles del dispositivo**.



El permiso de RBAC para un bloqueo de activación ASM se encuentra en **Dispositivos > Habilitar**

omisión de bloqueo de activación de ASM.



Distribuir aplicaciones de Apple

January 4, 2022

XenMobile administra las aplicaciones implementadas en los dispositivos. Puede organizar e implementar los siguientes tipos de aplicaciones iOS, iPadOS y macOS.

- **Tienda pública de aplicaciones (solo para iOS/iPadOS):** Este grupo contiene las aplicaciones, gratuitas o de pago, disponibles en una tienda pública de aplicaciones, como App Store de Apple o Google Play. Por ejemplo, GoToMeeting.
- **Empresarial (para iOS, iPadOS y macOS):** Aplicaciones nativas que no están habilitadas para MDX y no contienen las directivas asociadas a aplicaciones MDX.
- **MDX (solo para iOS/iPadOS):** Aplicaciones preparadas con el SDK de MAM o empaquetadas con MDX Toolkit. Estas aplicaciones incluyen directivas MDX. Las aplicaciones MDX se obtienen de fuentes internas y tiendas públicas.
- **Compras por volumen (para iOS, iPadOS y macOS):** Aplicaciones con licencias administradas a través del Programa de compras por volumen de Apple.
- **Aplicaciones iOS personalizadas (solo para iOS/iPadOS):** Aplicaciones propietarias B2B desarrolladas por equipos internos o externos.

Para obtener más información sobre diferentes tipos de aplicaciones, consulte Agregar aplicaciones.

Algunas implementaciones requieren una cuenta de Apple Business Management (ABM) o de Apple School Management (ASM). Para obtener más información, consulte las secciones siguientes.

Para cada tipo de aplicación y método de distribución, Citrix recomienda una serie de directrices de configuración. Para obtener información sobre la distribución de aplicaciones para otras plataformas, consulte Agregar aplicaciones. Las secciones siguientes proporcionan información más detallada sobre la configuración de aplicaciones iOS.

Pasos generales para la distribución de aplicaciones

Caso	Paso 1: Vincular cuentas	Paso 2: Agregar y configurar aplicaciones	Paso 3: Configurar grupos de entrega e implementar aplicaciones
Aplicaciones de tienda pública de aplicaciones, incluidas las aplicaciones de movilidad de Citrix	No aplicable	**En XenMobile: Configurar > Aplicaciones**, agregue aplicaciones de **Tienda pública de aplicaciones** para iPhone o iPad. Configure las aplicaciones y asígnelas a grupos de entrega.	**En XenMobile:** Configure e implemente aplicaciones mediante grupos de entrega.
Aplicaciones de tienda pública de aplicaciones entregadas con las compras por volumen de Apple, incluidas las aplicaciones de movilidad de Citrix	Inscríbase en un Programa de implementación de Apple. **En XenMobile:** Vaya a **Parámetros > Compras por volumen** para agregar su cuenta de compras por volumen.	**En ABM o ASM:** Compre y agregue aplicaciones desde Aplicaciones y Libros. **En XenMobile:** Vaya a **Configurar > Aplicaciones**, configure las aplicaciones y asígnelas a grupos de entrega.	**En XenMobile:** Configure e implemente aplicaciones mediante grupos de entrega.

Caso	Paso 1: Vincular cuentas	Paso 2: Agregar y configurar aplicaciones	Paso 3: Configurar grupos de entrega e implementar aplicaciones
Aplicaciones de empresa	No aplicable	**En XenMobile:** Vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar** y, a continuación, en **Empresarial**. Cargue el archivo IPA. Configure las aplicaciones y asígnelas a grupos de entrega.	**En XenMobile:** Configure e implemente aplicaciones mediante grupos de entrega.
Aplicaciones MDX	No aplicable	**En XenMobile:** Vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar** y, a continuación, en **MDX**. Asegúrese de seleccionar **iPad**/**iPhone** para la plataforma. Cargue el archivo MDX. Configure las aplicaciones y asígnelas a grupos de entrega.	**En XenMobile:** Configure e implemente aplicaciones mediante grupos de entrega.

Caso	Paso 1: Vincular cuentas	Paso 2: Agregar y configurar aplicaciones	Paso 3: Configurar grupos de entrega e implementar aplicaciones
Aplicaciones MDX distribuidas mediante las compras por volumen de Apple	Inscríbase en un Programa de implementación de Apple. **En XenMobile:** Vaya a **Parámetros > Compras por volumen** para agregar su cuenta de compras por volumen.	**En ABM:** Compre y agregue aplicaciones MDX desde Aplicaciones y Libros. Vincule la aplicación con su cuenta de ABM. **En XenMobile:** Vaya a **Configurar > Aplicaciones**, configure las aplicaciones y asígnelas a grupos de entrega.	**En XenMobile:** Configure e implemente aplicaciones mediante grupos de entrega.
Aplicaciones personalizadas	Inscríbase en un Programa de implementación de Apple. **En XenMobile:** Vaya a **Parámetros > Compras por volumen** para agregar su cuenta de compras por volumen.	**En ABM:** Agregue su aplicación al App Store como aplicación privada. Vincúlela con su cuenta de ABM. **En XenMobile:** Vaya a **Configurar > Aplicaciones**, configure las aplicaciones y asígnelas a grupos de entrega.	**En XenMobile:** Configure e implemente aplicaciones mediante grupos de entrega.

Caso	Paso 1: Vincular cuentas	Paso 2: Agregar y configurar aplicaciones	Paso 3: Configurar grupos de entrega e implementar aplicaciones
Aplicaciones personalizadas que se han habilitado para MDX	Inscríbase en un Programa de implementación de Apple. **En XenMobile:** Vaya a **Parámetros > Compras por volumen** para agregar su cuenta de compras por volumen.	**En ABM:** Agregue su aplicación al App Store como aplicación privada. Vincúlela con su cuenta de ABM. **En XenMobile:** Vaya a **Configurar > Aplicaciones** y cargue el archivo MDX. Configure las aplicaciones y asígnelas a grupos de entrega.	**En XenMobile:** Configure e implemente aplicaciones mediante grupos de entrega.

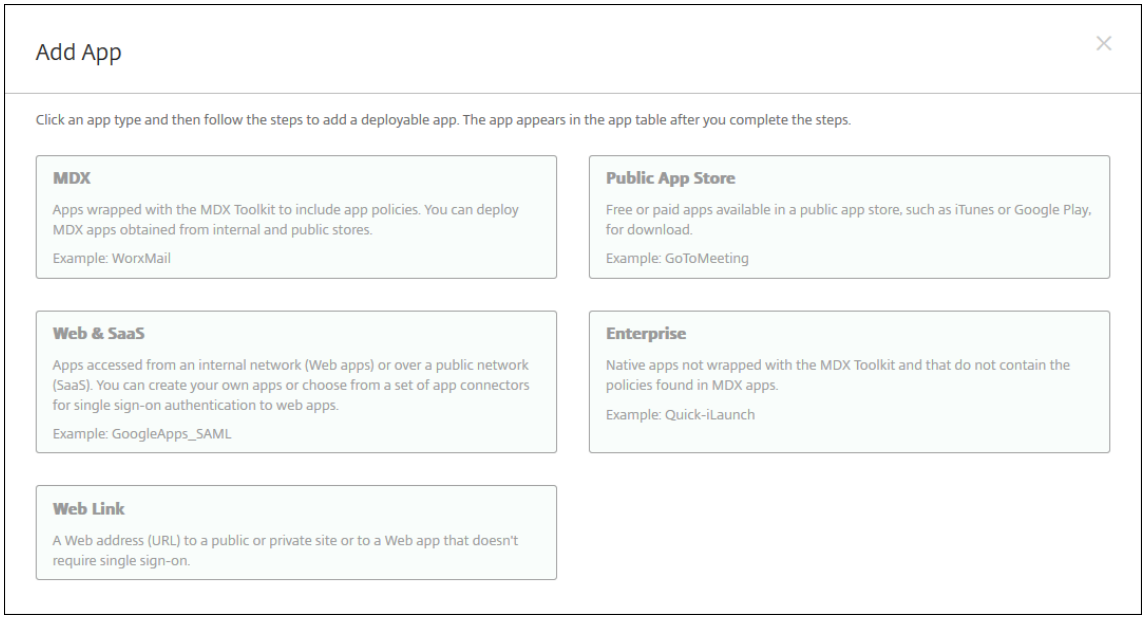
Aplicaciones de la tienda pública de aplicaciones

Puede agregar a XenMobile aplicaciones gratuitas y de pago disponibles en el App Store.

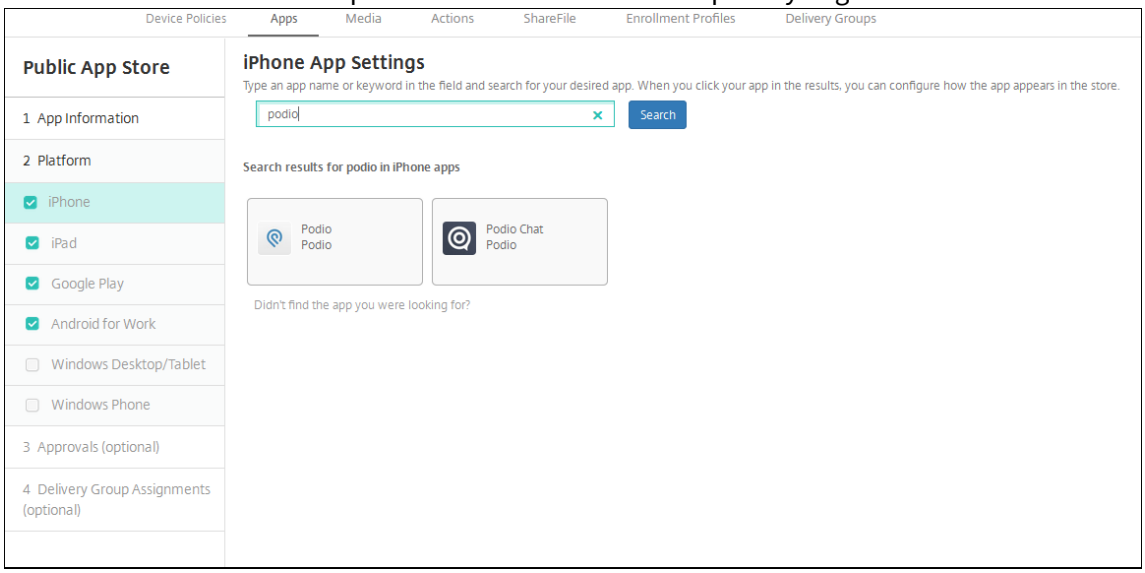
Disponibilidad de funciones	
Se necesita la supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	No
Disponible en	iOS/iPadOS

Paso 1: Agregar y configurar aplicaciones

1. En la consola de XenMobile, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.
2. Haga clic en **Tienda pública de aplicaciones**.



3. Seleccione **iPhone** o **iPad** como plataformas.
4. Introduzca el nombre de la aplicación en el cuadro de búsqueda y haga clic en **Buscar**.

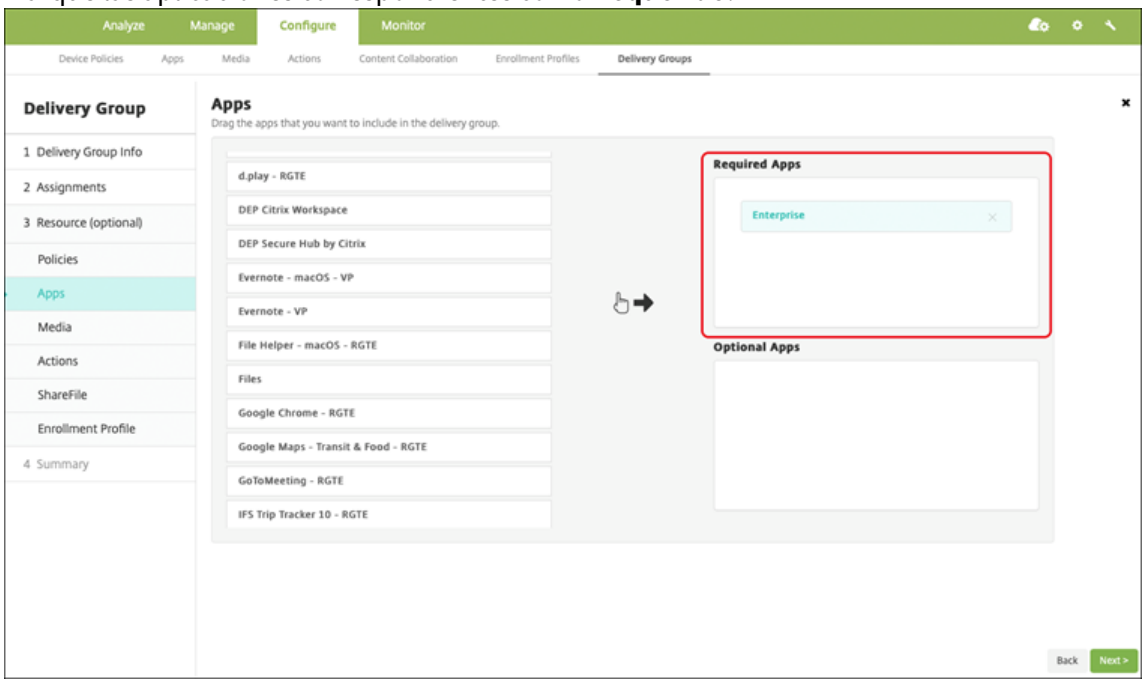


5. Aparecerán las aplicaciones que coincidan con los criterios de búsqueda. Haga clic en la aplicación correspondiente.
6. Asigne un grupo de entrega a la aplicación y haga clic en **Guardar**.

Paso 2: Configurar la implementación de aplicaciones

1. En la consola de XenMobile, vaya a **Configurar > Aplicaciones**.
2. Seleccione la aplicación que quiera configurar y haga clic en **Modificar**.
3. Citrix recomienda habilitar la función **Forzar administración de la aplicación**.
4. Asigne los grupos de entrega y haga clic en **Guardar**.

5. Vaya a **Configurar > Grupos de entrega > Aplicaciones**.
6. Marque las aplicaciones correspondientes como **Requerido**.



7. Vuelva a **Configurar > Grupos de entrega**.
8. Seleccione el grupo de entrega y haga clic en **Implementar**.
9. Los usuarios reciben una solicitud para instalar la aplicación, y la aplicación se instala en segundo plano después de que los usuarios la hayan aceptado.

Aplicaciones del tienda pública de aplicaciones entregadas con las compras por volumen de Apple

Puede administrar licencias de aplicaciones iOS/iPadOS a través del Programa de compras por volumen de Apple. Siga estos pasos para agregar a XenMobile aplicaciones de compras por volumen.

Disponibilidad de funciones	
Se necesita la supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
Disponible en	iOS/iPadOS/macOS

Paso 1: Vincular cuentas

1. Configure e inscríbase en Apple Business Manager (ABM) o en Apple School Manager (ASM). Para obtener más información sobre estos programas, consulte la documentación de Apple.
2. Vincule su cuenta de ABM/ASM a XenMobile. Para obtener más información sobre cómo vincular cuentas de compras por volumen, consulte Compras por volumen de Apple.

3. Al agregar su cuenta de compras por volumen, habilite **Actualización automática de aplicaciones**. Este parámetro garantiza que las aplicaciones de los dispositivos de usuario se actualicen automáticamente cuando aparece una actualización en el Apple Store.

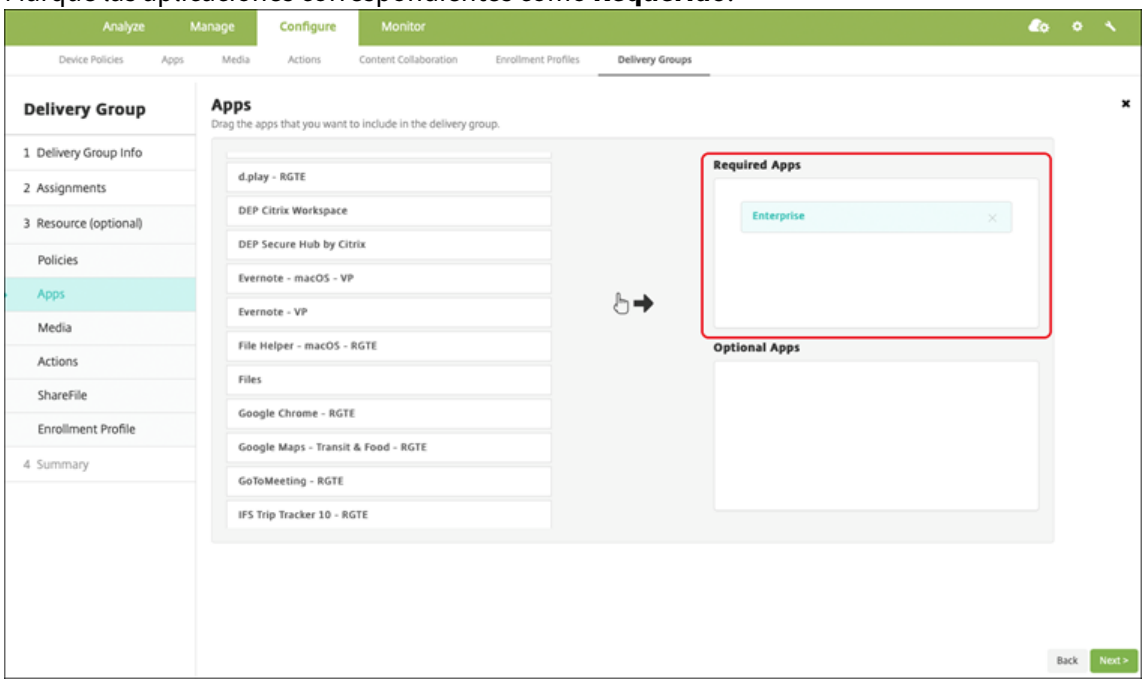
Paso 2: Obtener aplicaciones y licencias de Apple

Agregue aplicaciones a su cuenta de ABM/ASM. Puede agregar compras desde el App Store de Apple o desde Apple Books (solo para iOS/iPadOS). Tenga en cuenta que debe comprar todas las aplicaciones, incluso las que son gratuitas.

Para obtener información sobre cómo poner aplicaciones a disposición de su empresa, consulte la documentación de Apple.

Paso 3: Configurar la implementación de aplicaciones

1. En la consola de XenMobile, vaya a **Configurar > Aplicaciones**.
2. Seleccione la aplicación de compras por volumen que quiera configurar y haga clic en **Modificar**.
3. Seleccione las plataformas: **iPhone**, **iPad** o **macOS**.
4. Citrix recomienda habilitar la función **Forzar administración de la aplicación** (solo para iOS/iPadOS).
5. Asigne los grupos de entrega y haga clic en **Guardar**.
6. Vaya a **Configurar > Grupos de entrega > Aplicaciones**.
7. Marque las aplicaciones correspondientes como **Requerido**.



8. Vuelva a **Configurar > Grupos de entrega**.

9. Seleccione el grupo de entrega y haga clic en **Implementar**.
10. Los usuarios reciben una solicitud para instalar la aplicación, y la aplicación se instala en segundo plano después de que los usuarios la hayan aceptado.

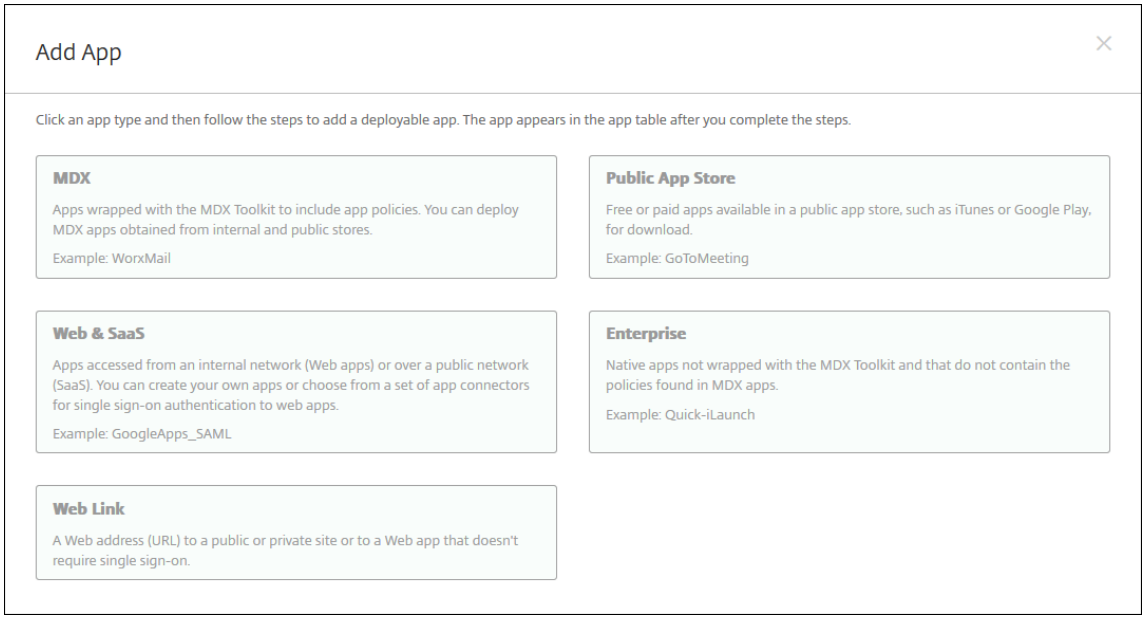
Aplicaciones de empresa

También puede agregar aplicaciones nativas que no tengan asociada ninguna directiva MDX. Siga estos pasos para agregar aplicaciones que no existen en el App Store.

Disponibilidad de funciones	
Se necesita la supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
OS	iOS/iPadOS/macOS

Paso 1: Agregar y configurar aplicaciones

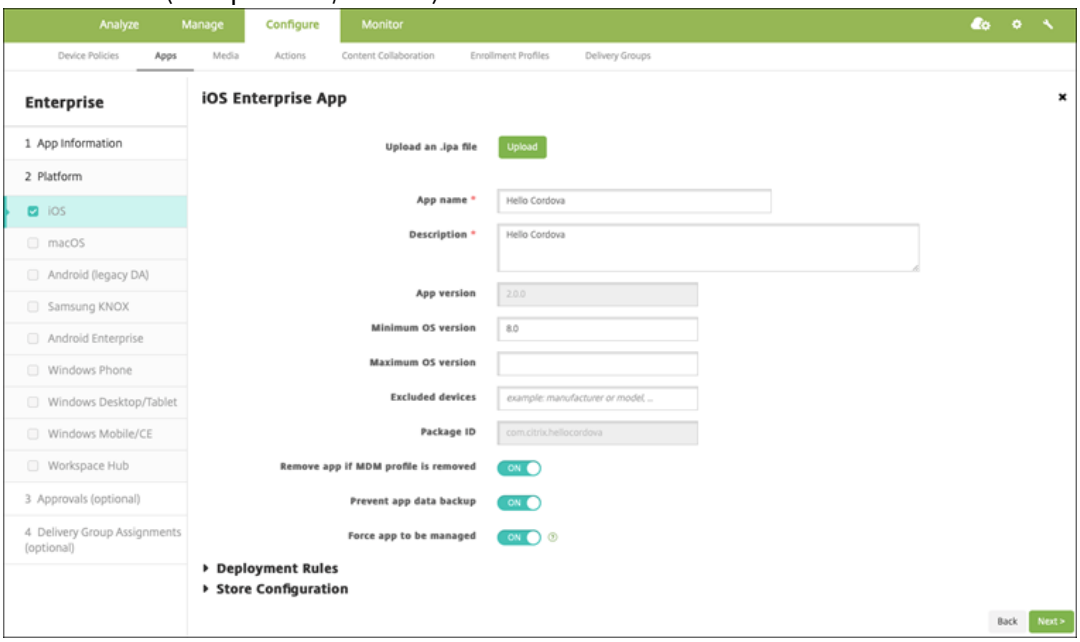
1. En la consola de XenMobile, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.
2. Haga clic en **Empresa**.



3. En la página **Información de la aplicación**, configure lo siguiente:
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en Nombre de la aplicación, en la tabla Aplicaciones.
   - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
   - **Categoría de la aplicación:** Si quiere, en la lista, haga clic en la categoría a la que se agregará la aplicación.
4. Haga clic en **Siguiente**. Aparecerá la página de las **plataformas de la aplicación**.
5. Seleccione las plataformas: **iPhone**, **iPad** o **macOS**.
6. Cargar el archivo IPA (para iOS y iPadOS) o cargar el archivo PKG (para macOS)
7. Haga clic en **Siguiente**. Aparecerá la página de **Detalles de la aplicación**.
8. Configure estos parámetros:
   - **Nombre de archivo:** Si quiere, escriba un nuevo nombre para la aplicación.
   - **Descripción de la aplicación:** Si quiere, indique una nueva descripción de la aplicación.
   - **Versión de la aplicación:** Este campo no se puede cambiar.
   - **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
   - **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
   - **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
   - **Quitar aplicación si se quita el perfil MDM:** Seleccione si quiere quitar la aplicación de un dispositivo cuando se quite el perfil de MDM. El valor predeterminado es SÍ. (solo iOS/iPadOS)
   - **Impedir copia de seguridad de datos de la aplicación:** Seleccione si quiere impedir que la aplicación realice copias de seguridad de los datos. El valor predeterminado es SÍ. (solo

iOS/iPadOS)

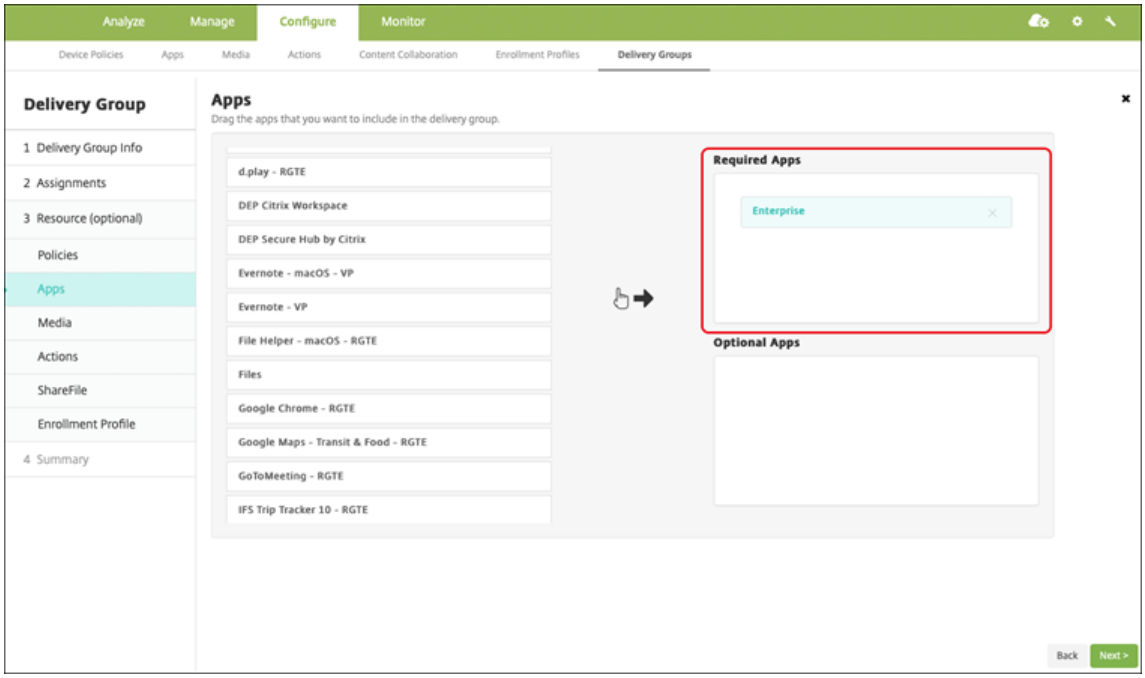
- **Forzar administración de la aplicación:** Si instala una aplicación no administrada, seleccione **SÍ** para que los usuarios de dispositivos no supervisados vean un mensaje en que se les solicita permiso para administrarla. Si el usuario acepta la solicitud, la aplicación se administrará (solo para iOS/iPadOS).



9. Asigne un grupo de entrega a la aplicación y haga clic en **Guardar**.

Paso 2: Configurar la implementación de aplicaciones

1. En la consola de XenMobile, vaya a **Configurar > Grupos de entrega**. Seleccione el grupo de entrega que quiera configurar y haga clic en la página **Aplicaciones**.
2. Marque las aplicaciones correspondientes como **Requerido**.



3. Vaya a **Configurar > Grupos de entrega**.
4. Seleccione el grupo de entrega y haga clic en **Implementar**.
5. Los usuarios reciben una solicitud para instalar la aplicación, y la aplicación se instala en segundo plano después de que los usuarios la hayan aceptado.

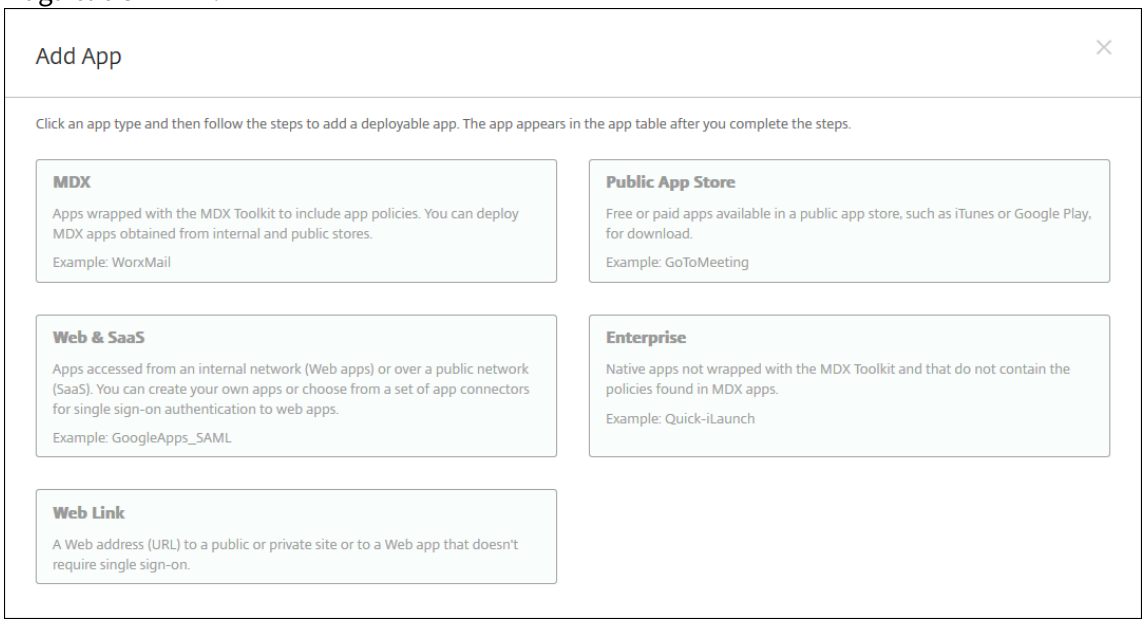
Aplicaciones MDX

Para usar las directivas MDX y las funciones de seguridad, agregue aplicaciones que estén habilitadas para el SDK de MAM o empaquetadas con MDX. Puede implementar aplicaciones MDX mediante las compras por volumen o sin ellas.

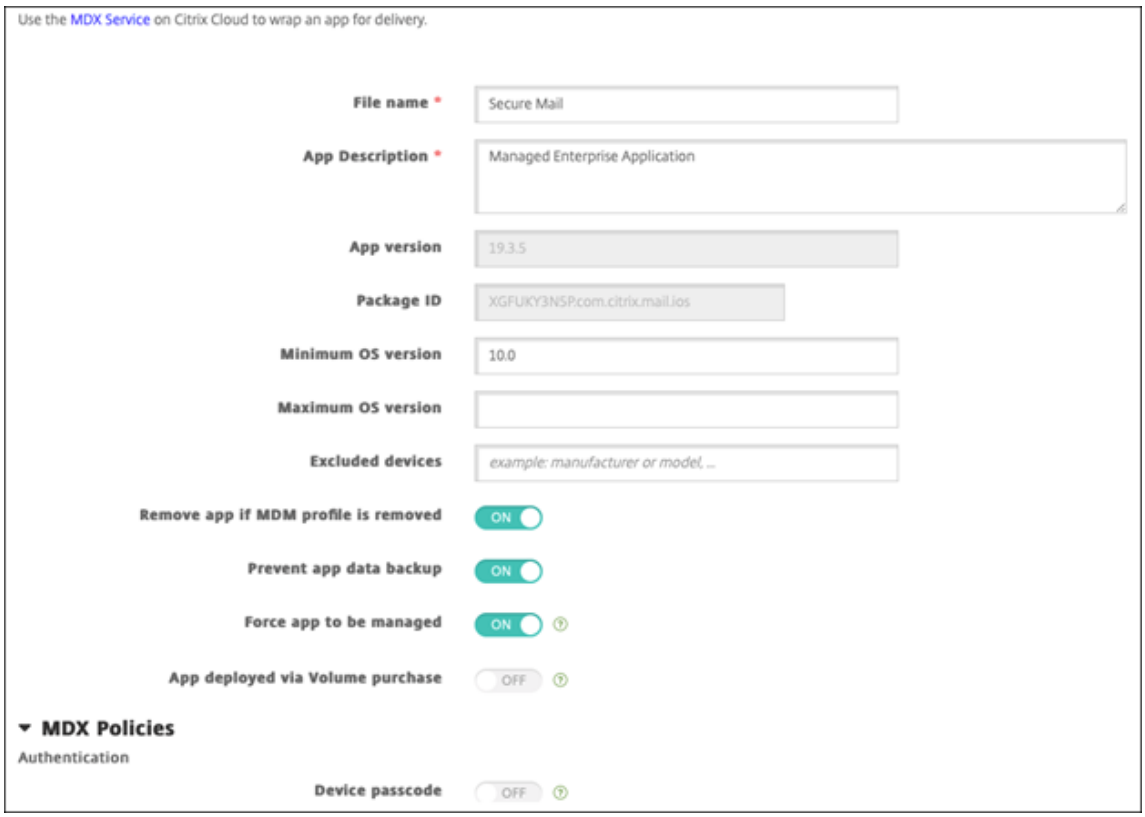
Disponibilidad de funciones	
Se necesita la supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
Disponible en	iOS/iPadOS

Paso 1: Agregar y configurar aplicaciones

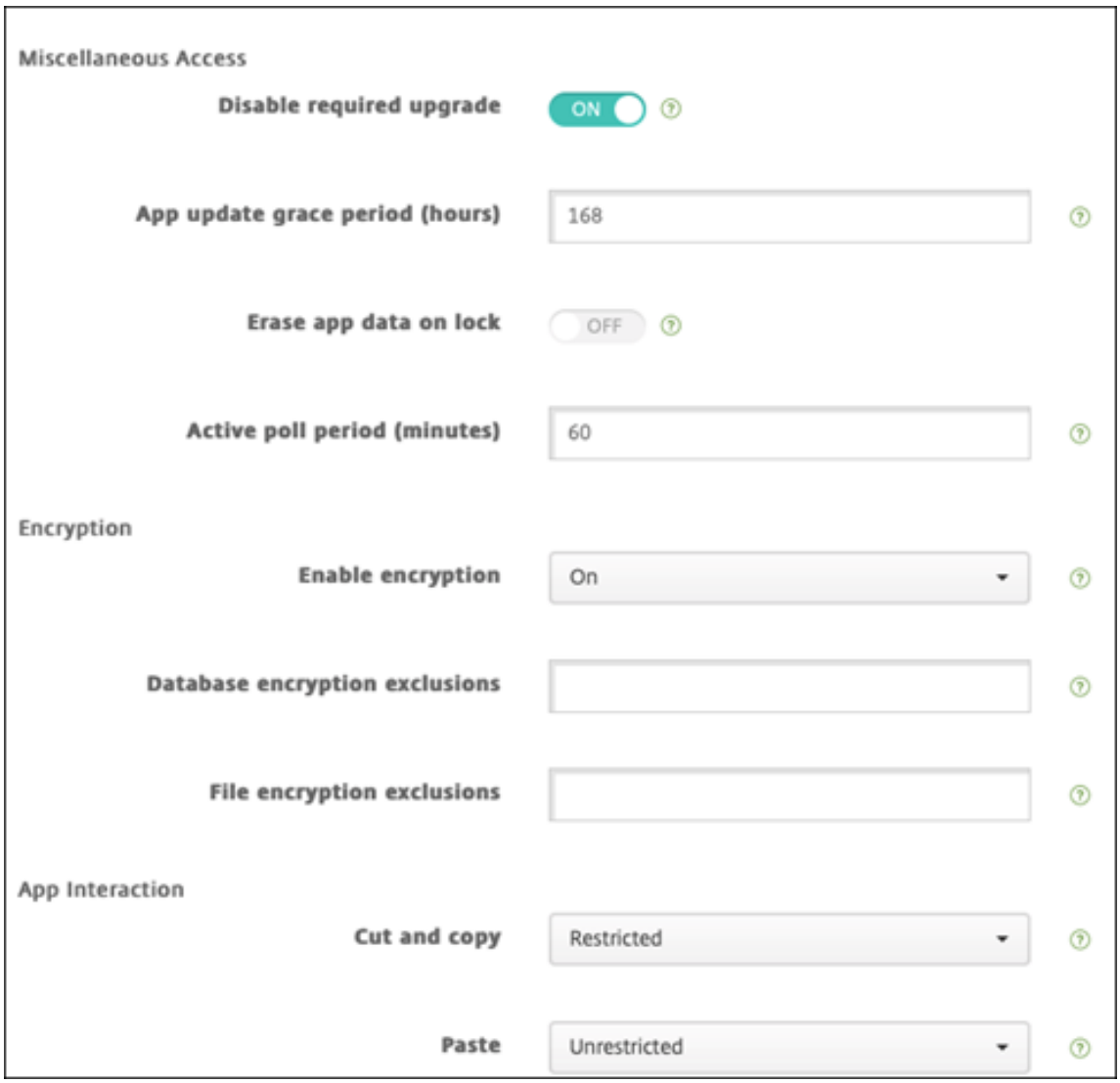
1. En la consola de XenMobile, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.
2. Haga clic en **MDX**.



3. Seleccione **iPhone** o **iPad** como plataformas.
4. Cargue el archivo MDX.
5. Configure los detalles de la aplicación. **Desactive Aplicación implementada mediante las compras por volumen**. Citrix también recomienda habilitar la función **Forzar administración de la aplicación**.



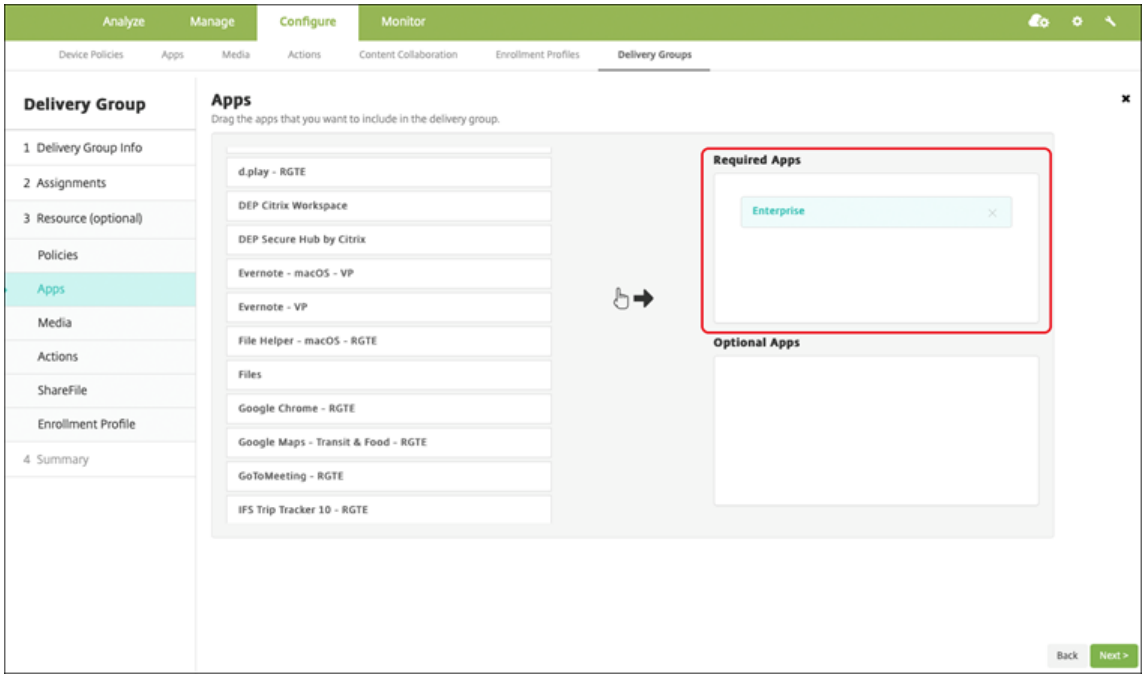
6. Configure las directivas MDX. **Active** la opción **Inhabilitar actualización obligatoria**.



7. Asigne un grupo de entrega a la aplicación y haga clic en **Guardar**.

Paso 2: Configurar la implementación de aplicaciones

1. En la consola de XenMobile, vaya a **Configurar > Grupos de entrega > Aplicaciones**.
2. Marque las aplicaciones correspondientes como **Requerido**.



3. Vaya a **Configurar > Grupos de entrega**.
4. Seleccione el grupo de entrega y haga clic en **Implementar**.
5. Los usuarios reciben una solicitud para instalar la aplicación, y la aplicación se instala en segundo plano después de que los usuarios la hayan aceptado.

Aplicaciones MDX distribuidas mediante las compras por volumen de Apple

Para usar las directivas MDX y las funciones de seguridad, agregue aplicaciones que estén habilitadas para el SDK de MAM o empaquetadas con MDX. Para implementar aplicaciones mediante las compras por volumen, las aplicaciones deben existir en la tienda de aplicaciones.

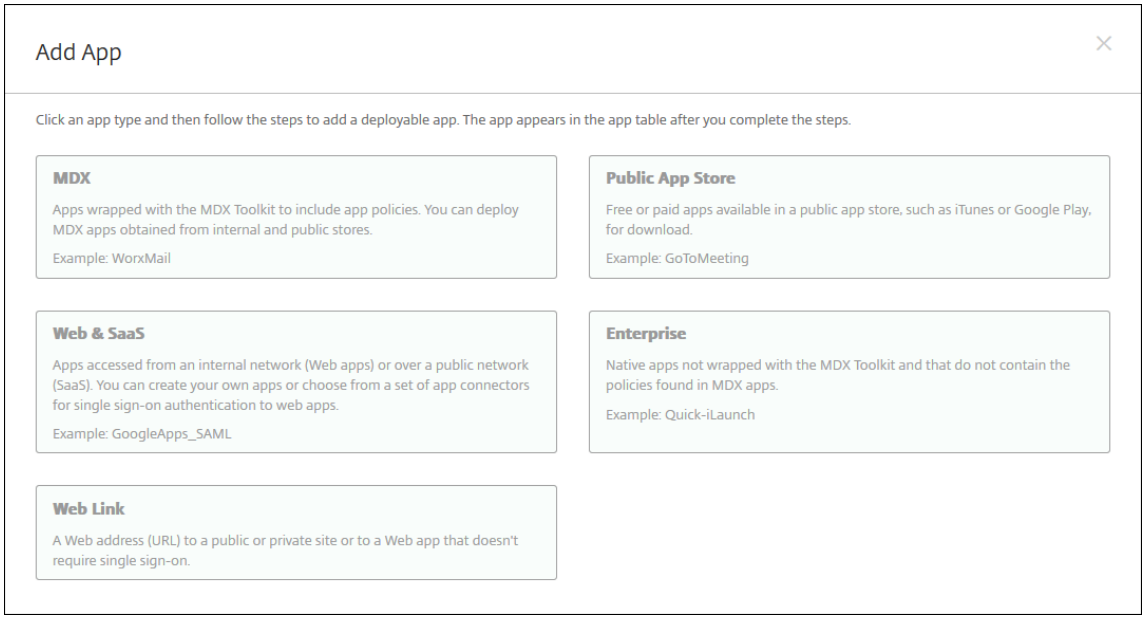
Disponibilidad de funciones	
Se necesita la supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
Disponible en	iOS/iPadOS

Paso 1: Vincular cuentas

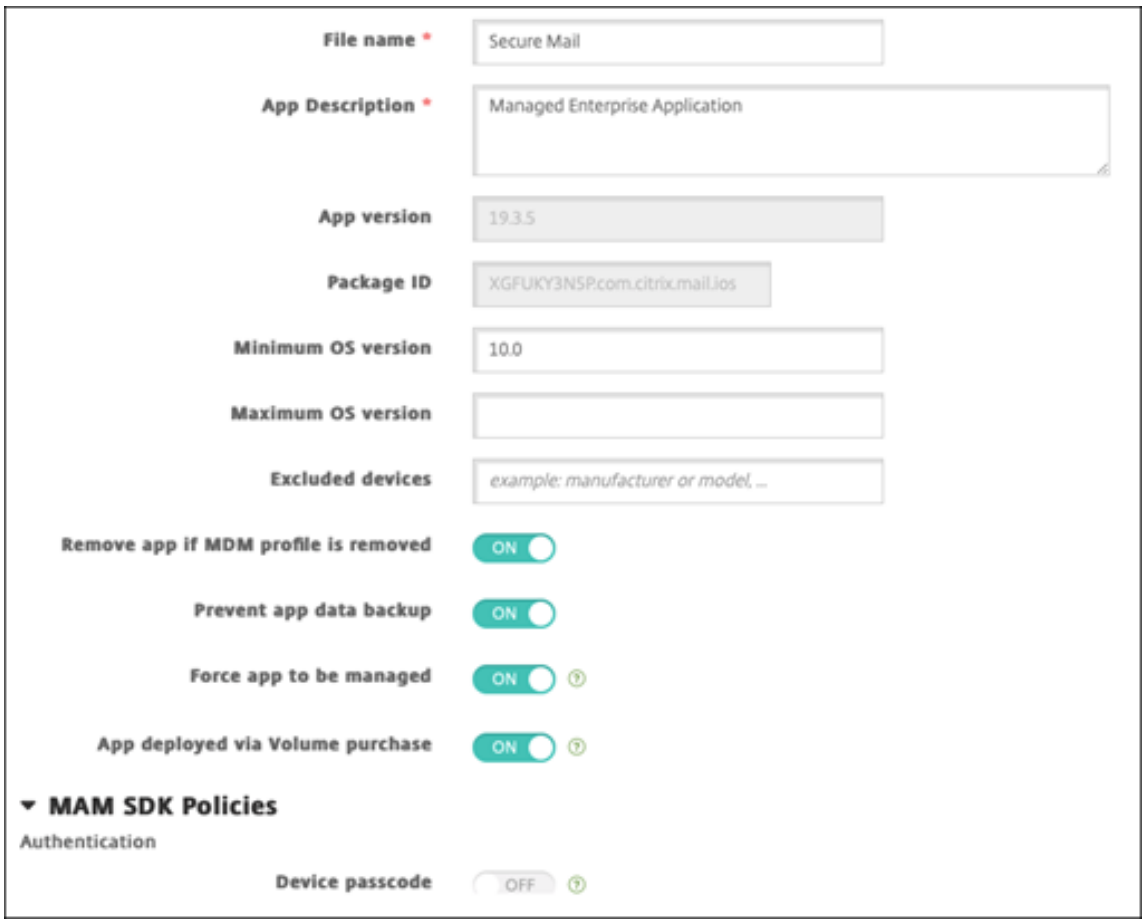
1. Configure e inscríbase en Apple Business Manager (ABM) o en Apple School Manager (ASM). Para obtener más información sobre estos programas, consulte la documentación de Apple.
2. Vincule su cuenta de ABM/ASM a XenMobile. Para obtener más información sobre cómo vincular cuentas de compras por volumen, consulte Compras por volumen de Apple.
3. Al agregar su cuenta de compras por volumen, habilite **Actualización automática de aplicaciones**. Este parámetro garantiza que las aplicaciones de los dispositivos de usuario se actualicen automáticamente cuando aparece una actualización en el Apple Store.

Paso 2: Agregar y configurar aplicaciones

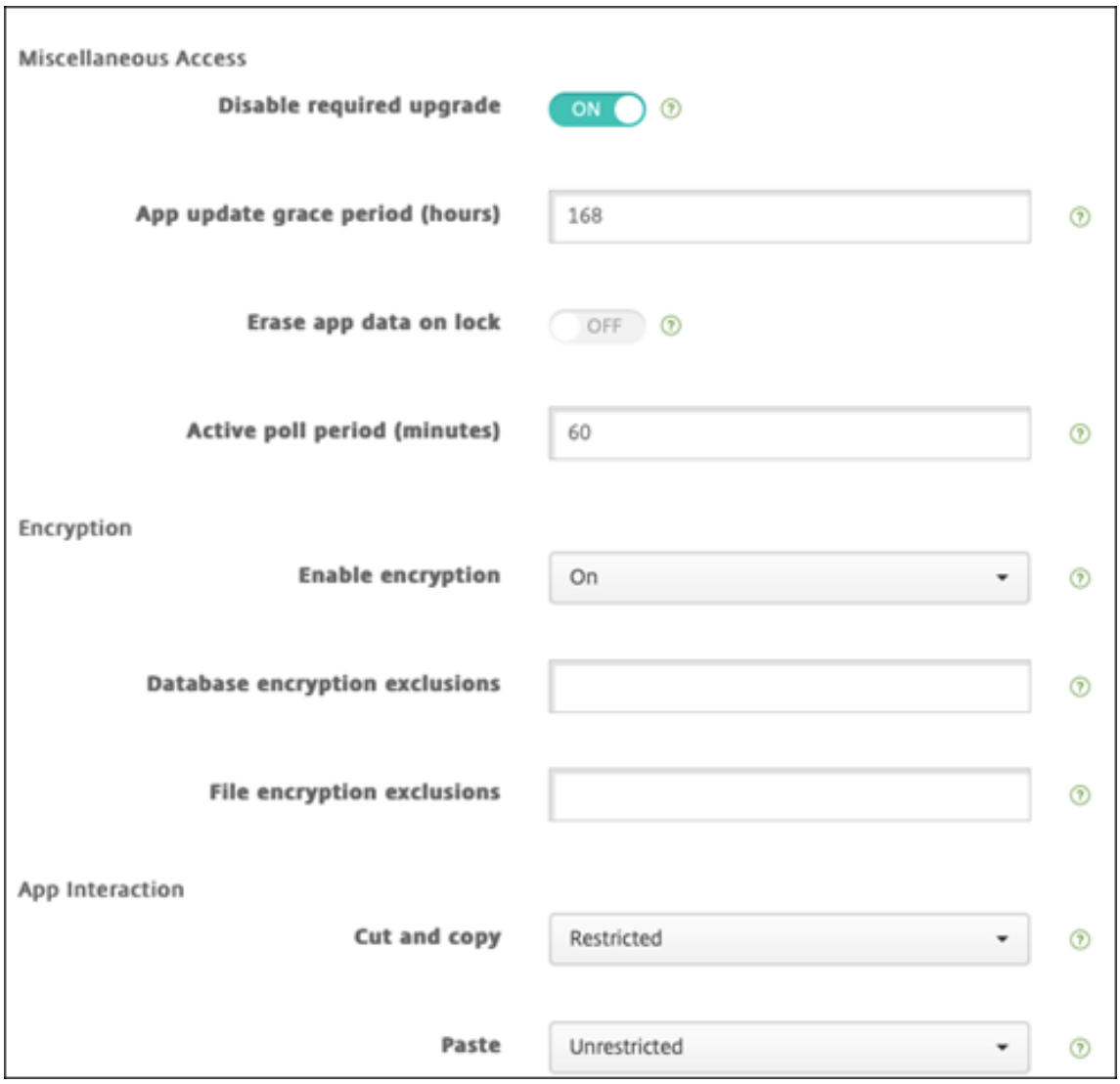
1. En la consola de XenMobile, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.
2. Haga clic en **MDX**.



3. Seleccione **iPhone** o **iPad** como plataformas.
4. Cargue el archivo MDX.
5. Configure los detalles de la aplicación. **Active Aplicación implementada mediante las compras por volumen**. Citrix también recomienda habilitar la función **Forzar administración de la aplicación**.



6. Configure las directivas MDX. **Active** la opción **Inhabilitar actualización obligatoria**.

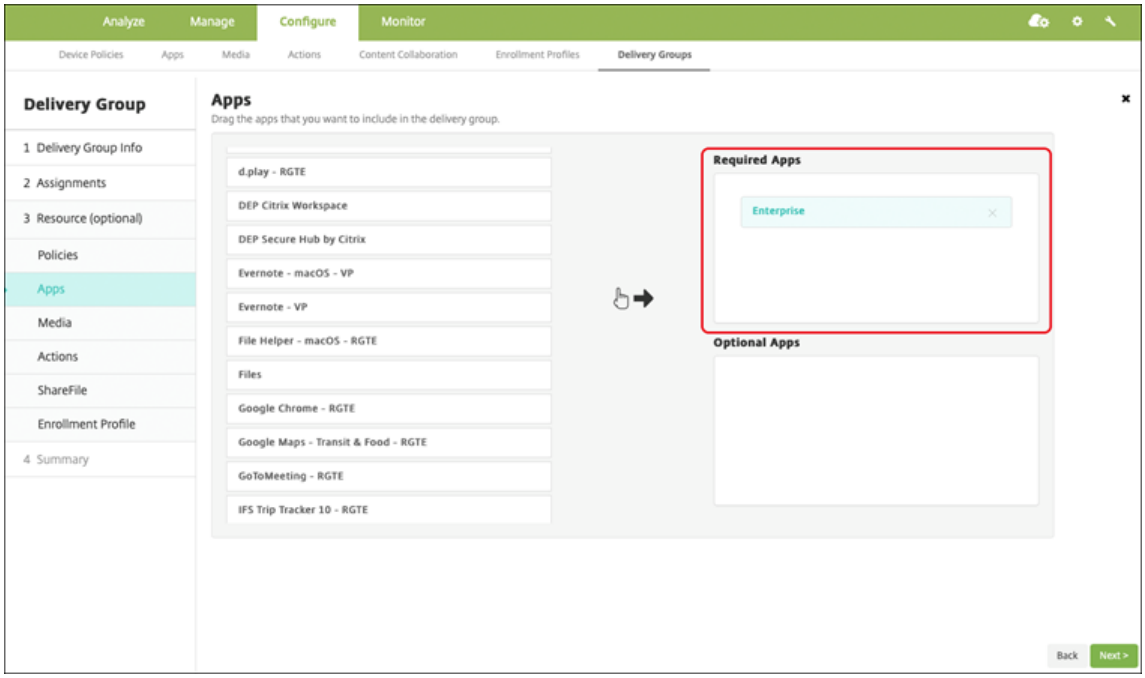


7. Asigne un grupo de entrega a la aplicación para cada plataforma y haga clic en **Guardar**.

Esta configuración genera dos entradas para esta aplicación en la lista de aplicaciones. Al seleccionar una aplicación que quiera configurar, seleccione la aplicación con **Tipo MDX**.

Paso 3: Configurar la implementación de aplicaciones

1. En la consola de XenMobile, vaya a **Configurar > Grupos de entrega > Aplicaciones**.
2. Marque las aplicaciones de las compras de volumen correspondientes como **Requerido**.



3. Vaya a **Configurar > Grupos de entrega**.
4. Seleccione el grupo de entrega y haga clic en **Implementar**.
5. Los usuarios reciben una solicitud para instalar la aplicación, y la aplicación se instala en segundo plano después de que los usuarios la hayan aceptado.

Aplicaciones personalizadas

Las aplicaciones personalizadas son aplicaciones propietarias B2B. Puede utilizar XenMobile y las compras por volumen de Apple para distribuir aplicaciones propietarias de forma privada y segura. Puede distribuir las aplicaciones a socios, clientes, franquiciados y empleados internos específicos.

Disponibilidad de funciones	
Se necesita la supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
Disponible en	iOS/iPadOS

Requisitos para aplicaciones personalizadas

- Cuenta de Apple Business Manager o Apple School Manager
- Cuenta de compras por volumen de Apple (requiere dispositivos con iOS 7 o una versión posterior)
- Inscriba dispositivos en XenMobile mediante uno de los siguientes modos de inscripción de Apple:
  - Inscripción automatizada de dispositivos
  - Inscripción de dispositivos
  - Inscripción de usuarios

Paso 1: Vincular cuentas

Para implementar aplicaciones personalizadas mediante las compras por volumen, vincule su cuenta de compras por volumen a XenMobile.

1. Configure e inscríbase en Apple Business Manager (ABM). Para obtener más información sobre estos programas, consulte la documentación de Apple.
2. Vincule su cuenta de ABM a XenMobile. Para obtener más información sobre cómo vincular cuentas de compras por volumen, consulte Compras por volumen de Apple.
3. Al agregar su cuenta de compras por volumen, habilite **Actualización automática de aplicaciones**. Este parámetro garantiza que las aplicaciones de los dispositivos de usuario se actualicen automáticamente cuando aparece una actualización en el Apple Store.

Paso 2: Configurar aplicaciones en ABM

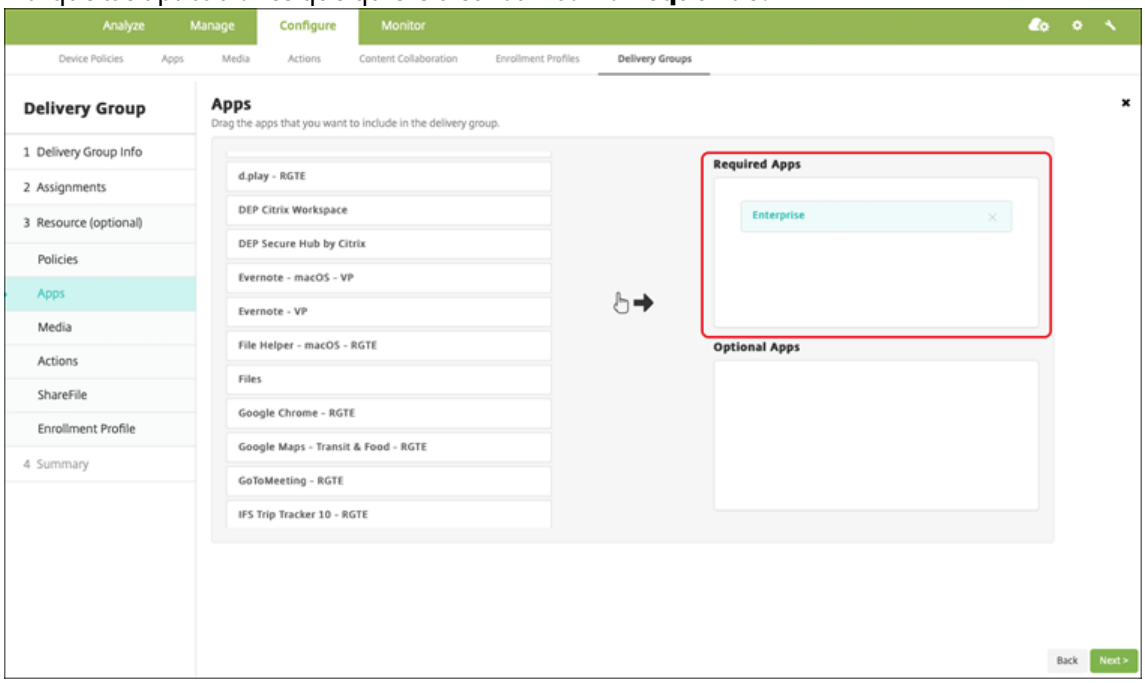
Agregue aplicaciones a su cuenta de ABM. Puede cargar y distribuir sus propias aplicaciones personalizadas o comprar licencias para aplicaciones personalizadas de otras organizaciones. Para obtener más información sobre cómo agregar y habilitar aplicaciones personalizadas en ABM, consulte la documentación de Apple.

Paso 3: Agregar y configurar aplicaciones en XenMobile

1. En la consola de XenMobile, vaya a **Configurar > Aplicaciones**. Las aplicaciones de compras por volumen aparecen en la lista de aplicaciones.
2. Seleccione la aplicación que quiere configurar. Haga clic en **Edit**.
3. Seleccione las plataformas: **iPhone**, **iPad** o **macOS**.
4. Elija los grupos de entrega a los que quiere distribuir la aplicación. Haga clic en **Guardar**.

Paso 4: Configurar la implementación de aplicaciones

1. En la consola de XenMobile, vaya a **Configurar > Grupos de entrega > Aplicaciones**.
2. Marque las aplicaciones que quiere distribuir como **Requerido**.



3. Vuelva a **Configurar > Grupos de entrega**.
4. Seleccione el grupo de entrega que quiere implementar y haga clic en **Implementar**.
5. Los usuarios recibirán una solicitud para implementar aplicaciones. Las aplicaciones se instalan en segundo plano una vez que los usuarios las hayan aceptado.

Aplicaciones personalizadas que se han habilitado para MDX

Para usar las directivas MDX y las funciones de seguridad, agregue aplicaciones personalizadas que estén habilitadas para el SDK de MAM o empaquetadas con MDX.

Disponibilidad de funciones	
Se necesita la supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
Disponible en	iOS/iPadOS

Paso 1: Vincular cuentas

Para implementar aplicaciones personalizadas mediante las compras por volumen, vincule su cuenta de compras por volumen a XenMobile.

1. Configure e inscríbase en Apple Business Manager (ABM). Para obtener más información sobre estos programas, consulte la documentación de Apple.
2. Vincule su cuenta de ABM a XenMobile. Para obtener más información sobre cómo vincular

cuentas de compras por volumen, consulte Compras por volumen de Apple.

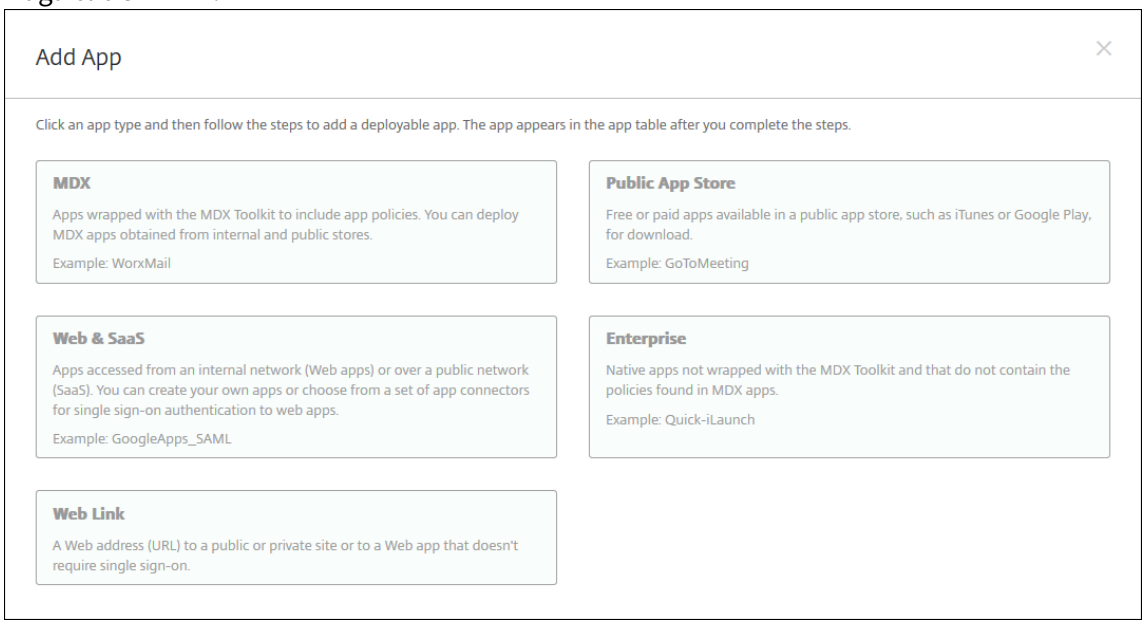
3. Al agregar su cuenta de compras por volumen, habilite **Actualización automática de aplicaciones**. Este parámetro garantiza que las aplicaciones de los dispositivos de usuario se actualicen automáticamente cuando aparece una actualización en el Apple Store.

Paso 2: Configurar aplicaciones en ABM

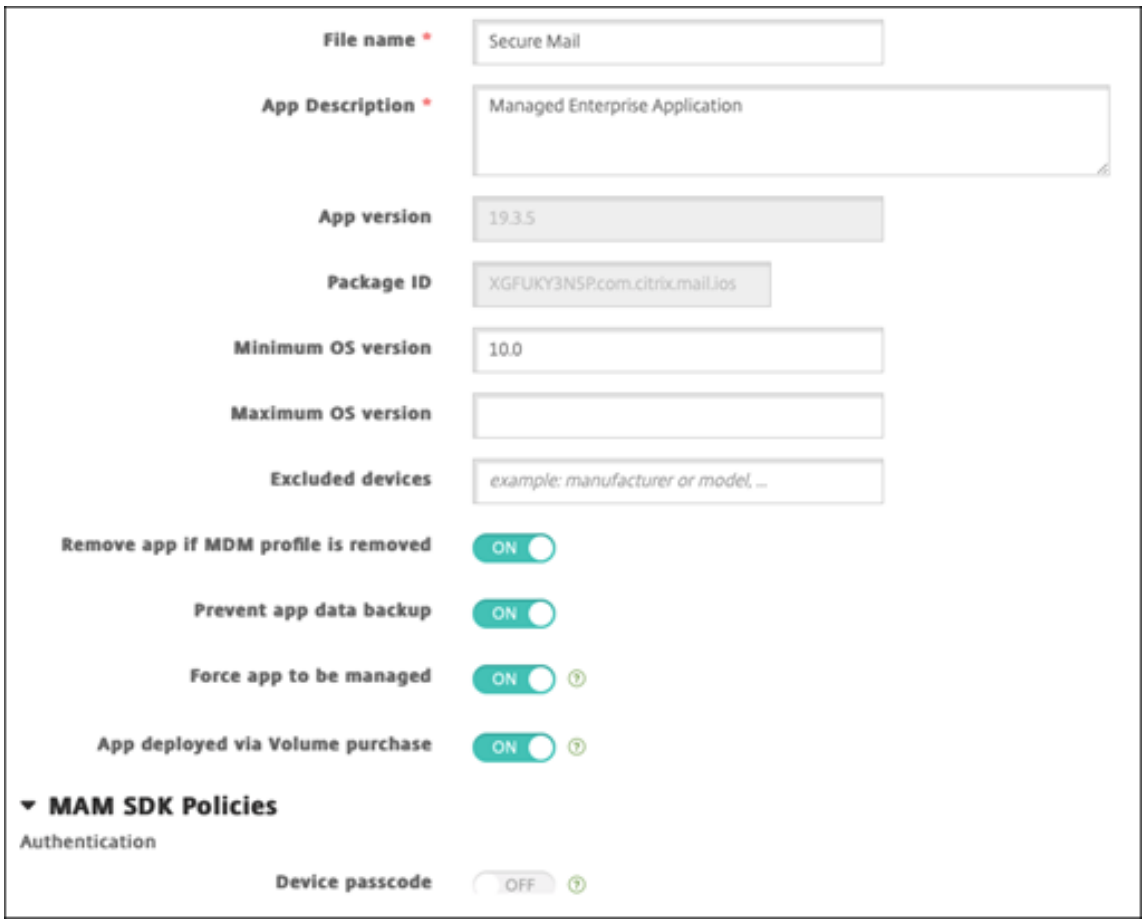
Agregue aplicaciones a su cuenta de ABM. Puede cargar y distribuir sus propias aplicaciones personalizadas o comprar licencias para aplicaciones personalizadas de otras organizaciones. Para obtener más información sobre cómo agregar y habilitar aplicaciones personalizadas en ABM, consulte la documentación de Apple.

Paso 3: Agregar y configurar aplicaciones en XenMobile

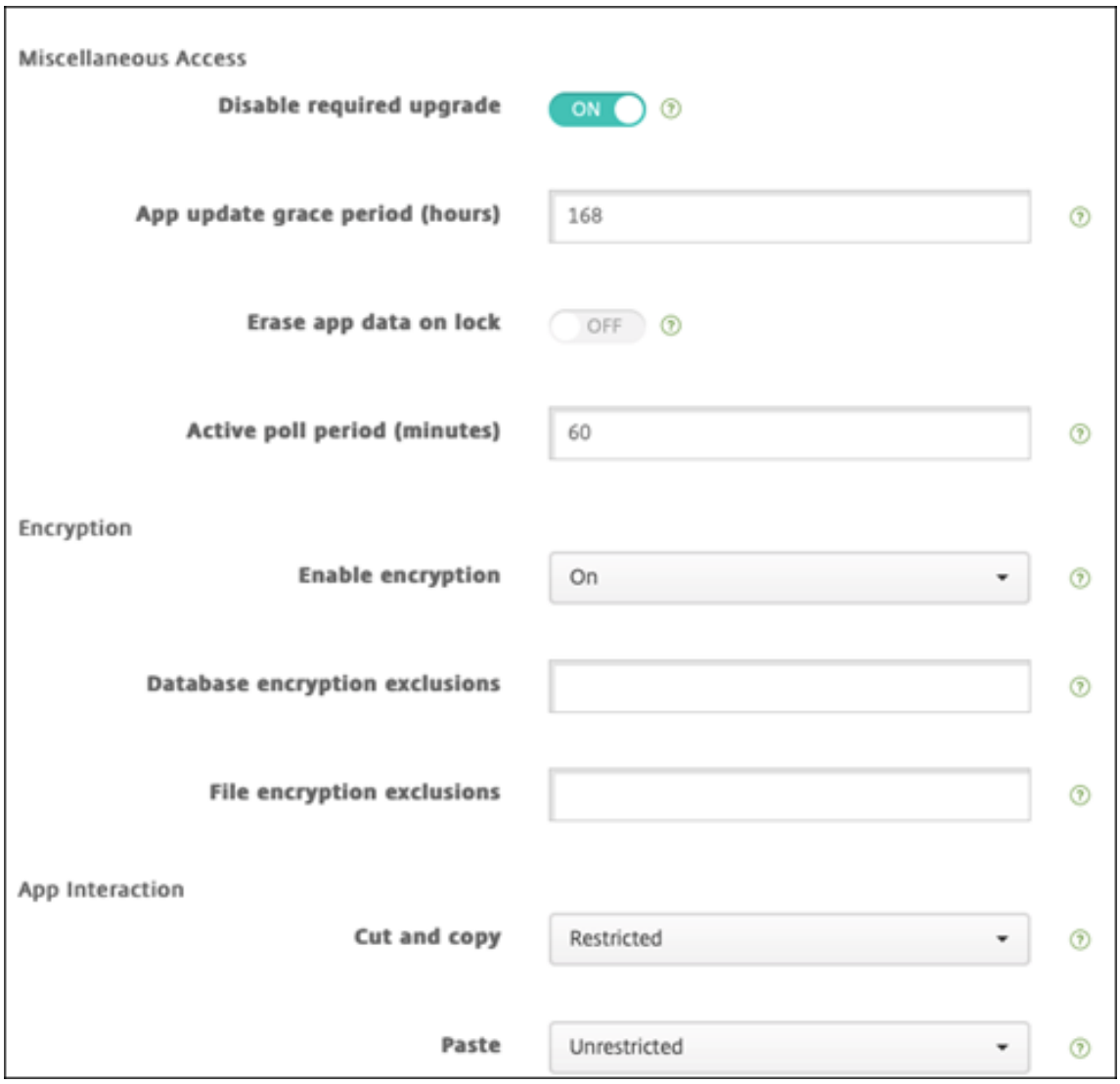
1. En la consola de XenMobile, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.
2. Haga clic en **MDX**.



3. Seleccione las plataformas **iPhone** o **iPad**.
4. Cargue el archivo MDX para la aplicación que quiera agregar.
5. Configure los detalles de la aplicación. **Active Aplicación implementada mediante las compras por volumen**. Citrix también recomienda habilitar la función **Forzar administración de la aplicación**.



6. Configure las directivas MDX. **Active** la opción **Inhabilitar actualización obligatoria**.

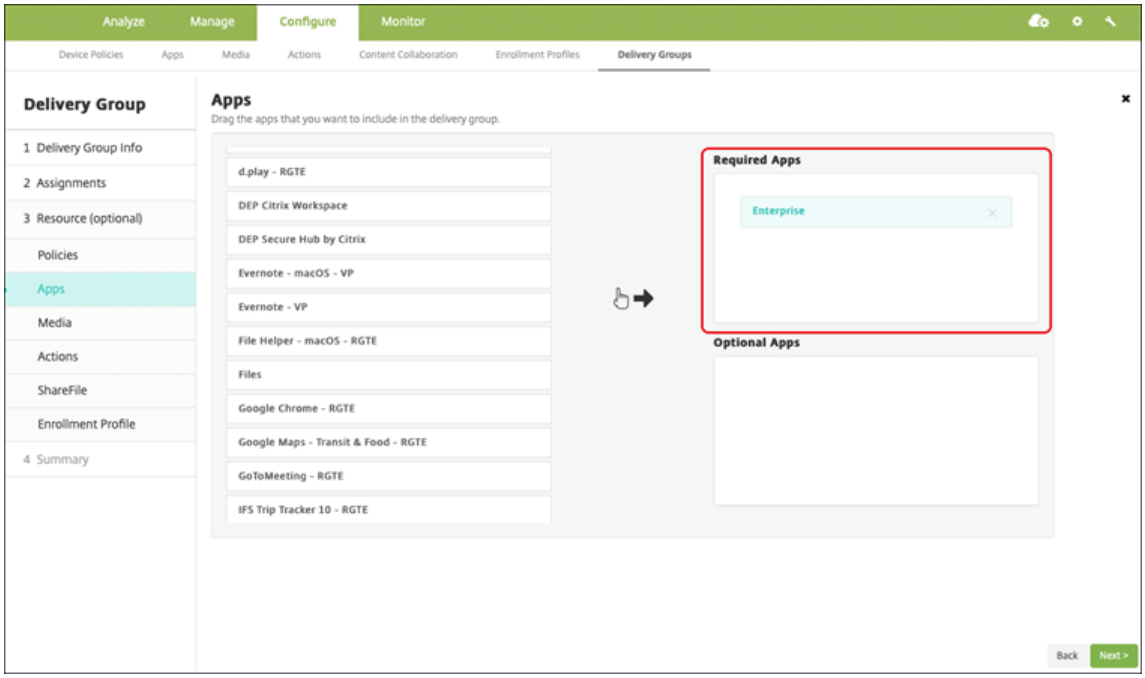


7. Asigne un grupo de entrega a la aplicación y haga clic en **Guardar**.

Esta configuración genera dos entradas para esta aplicación en la lista de aplicaciones. Al seleccionar una aplicación que quiera configurar, seleccione la aplicación con **Tipo MDX**.

Paso 4: Configurar la implementación de aplicaciones

1. En la consola de XenMobile, vaya a **Configurar > Aplicaciones**. Las aplicaciones de compras por volumen aparecen en la lista de aplicaciones.
2. Seleccione la aplicación que quiere configurar. Haga clic en **Edit**.
3. Elija los grupos de entrega a los que quiere distribuir la aplicación en cada plataforma. Haga clic en **Guardar**.
4. Vuelva a **Configurar > Grupos de entrega > Aplicaciones**.
5. Marque las aplicaciones que quiere distribuir como **Requerido**.



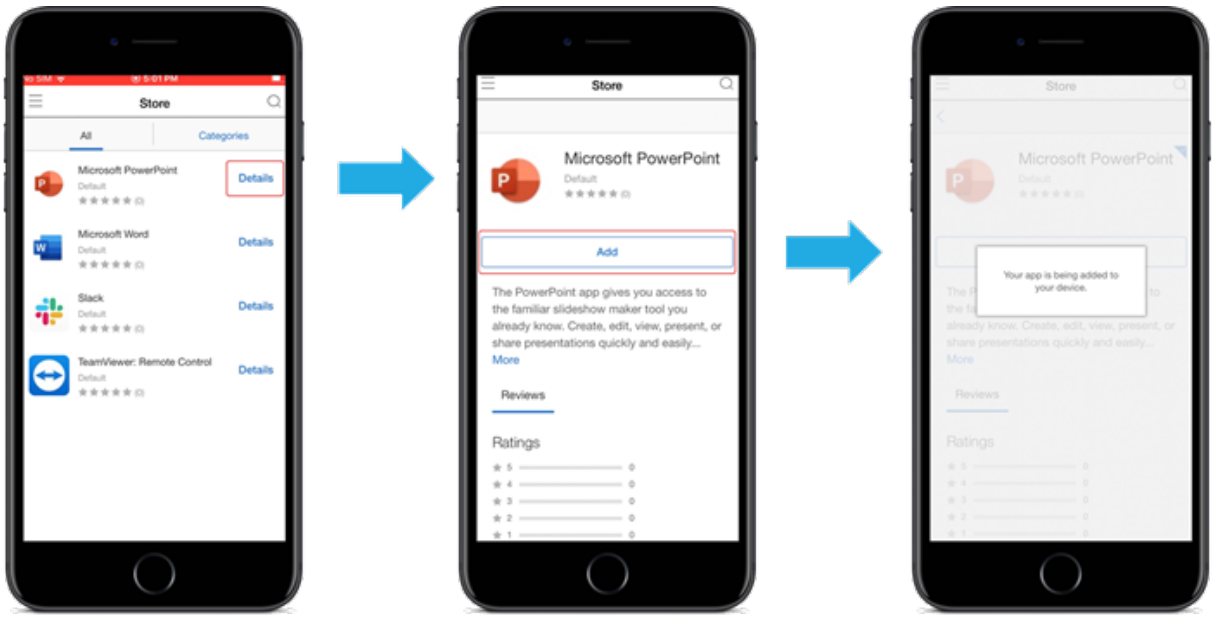
6. Vuelva a **Configurar > Grupos de entrega**.
7. Seleccione el grupo de entrega que quiere implementar y haga clic en **Implementar**.
8. Los usuarios recibirán una solicitud para implementar aplicaciones. Las aplicaciones se instalan en segundo plano una vez aceptadas.

Aplicaciones opcionales (solo iOS/iPadOS)

Citrix recomienda implementar aplicaciones con la opción **Requerido**. Las aplicaciones necesarias se instalan silenciosamente en los dispositivos del usuario, lo que minimiza la interacción con ellas. Tener esta función habilitada también permite que las aplicaciones se actualicen automáticamente.

Las aplicaciones opcionales permiten a los usuarios elegir qué aplicaciones instalar, pero los usuarios deben iniciar la instalación manualmente a través de Secure Hub.

Para instalar aplicaciones opcionales, los usuarios deben iniciar Secure Hub, ir a **Tienda**, seleccionar **Detalles** para la aplicación correspondiente y hacer clic en **Agregar**.



Control de acceso de red

January 4, 2022

Puede utilizar la solución de control de acceso de red (NAC) para ampliar la evaluación de seguridad que ofrece Endpoint Management para dispositivos Android y Apple. La solución NAC usa la evaluación de seguridad de XenMobile para facilitar y gestionar las decisiones de autenticación. Después de configurar el dispositivo NAC, se aplican las directivas de dispositivo y los filtros NAC que configure en XenMobile.

El uso de XenMobile con una solución NAC agrega QoS y un control más detallado sobre los dispositivos internos de la red. Para obtener un resumen de las ventajas de integrar NAC en XenMobile, consulte Control de acceso.

Citrix admite estas soluciones para la integración con XenMobile:

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

Citrix no garantiza la integración de otras soluciones NAC.

Con un dispositivo NAC en la red:

- XenMobile admite NAC como una función de seguridad para dispositivos iOS, Android Enterprise y Android de punto final.
- Puede habilitar filtros en XenMobile para establecer dispositivos como conformes o no conformes con NAC según una serie de reglas o propiedades. Por ejemplo:
  - Si un dispositivo administrado en XenMobile no cumple los criterios especificados, XenMobile lo marca como no conforme. Un dispositivo NAC bloquea dispositivos no conformes que haya presentes en su red.
  - Si un dispositivo administrado en XenMobile tiene instaladas aplicaciones no conformes, un filtro NAC puede bloquear la conexión VPN. Como resultado, un dispositivo de usuario no conforme no puede acceder a aplicaciones ni sitios web a través de la VPN.
  - Si utiliza Citrix Gateway para NAC, puede habilitar el túnel dividido para evitar que el plug-in de Citrix Gateway envíe tráfico de red innecesario a Citrix Gateway. Para obtener más información sobre los túneles divididos, consulte Configurar el túnel dividido.

Filtros de conformidad con NAC admitidos

XenMobile Server es compatible con los siguientes filtros de conformidad con NAC:

Dispositivos anónimos: Comprueba si un dispositivo está en modo anónimo. Esta comprobación está disponible si XenMobile no puede volver a autenticar al usuario cuando un dispositivo intenta reconectar.

Atestación de Samsung Knox fallida: Comprueba si un dispositivo falló una consulta del servidor de atestación de Samsung Knox.

Aplicaciones prohibidas: Comprueba si un dispositivo tiene aplicaciones prohibidas, según se definen en la directiva Acceso a aplicaciones. Para obtener información sobre esa directiva, consulte Directivas de acceso a aplicaciones.

Dispositivos inactivos: Comprueba si un dispositivo está inactivo según se define en el parámetro **Umbral de días de inactividad** en **Propiedades de servidor**. Para obtener más información, consulte Propiedades del servidor.

Aplicaciones obligatorias que faltan: Comprueba si en un dispositivo falta alguna aplicación obligatoria, según se definen en la directiva Acceso a aplicaciones.

Aplicaciones no sugeridas: Comprueba si un dispositivo tiene aplicaciones no sugeridas, según se definen en la directiva Acceso a aplicaciones.

Contraseña no conforme: 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 Código de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para definir una contraseña si XenMobile envía una directiva Código de acceso al dispositivo. Antes de que el usuario defina la contraseña, el código de acceso podría no cumplir los requisitos de conformidad.

Dispositivos no conformes: Comprueba si un dispositivo ya no es conforme, según lo definido en la propiedad de dispositivo No conforme. Normalmente, las acciones automatizadas o los terceros que utilizan las API de XenMobile cambian esa propiedad del dispositivo.

Estado revocado: Comprueba si el certificado del dispositivo se ha revocado. Un dispositivo revocado no se puede volver a inscribir hasta que se autorice de nuevo.

Dispositivos Android o iOS liberados por root/jailbreak: Comprueba si un dispositivo iOS está liberado por jailbreak o un dispositivo Android está liberado por rooting.

Dispositivos no administrados: Comprueba si un dispositivo aún está en estado administrado, bajo el control de XenMobile. Por ejemplo, un dispositivo inscrito en MAM o que se haya desinscrito no es un dispositivo administrado.

> **Nota:**
>
> El filtro "Conformidad/No conformidad implícita" establece el valor predeterminado solo en los dispositivos que administra XenMobile. Por ejemplo, los dispositivos que tengan instalada una aplicación bloqueada o que no estén inscritos se marcan como no conformes. El dispositivo NAC bloquea dichos dispositivos en la red.

Introducción a la configuración

Se recomienda configurar los componentes de NAC en el orden indicado.

1. Configure directivas de dispositivo para admitir NAC:

   Para dispositivos iOS: Consulte Configurar la directiva de VPN para admitir NAC.

   Para dispositivos Android Enterprise: Consulte Crear una configuración administrada por Android Enterprise para Citrix SSO.

   Para dispositivos Android: Consulte Configurar el protocolo Citrix SSO para Android.

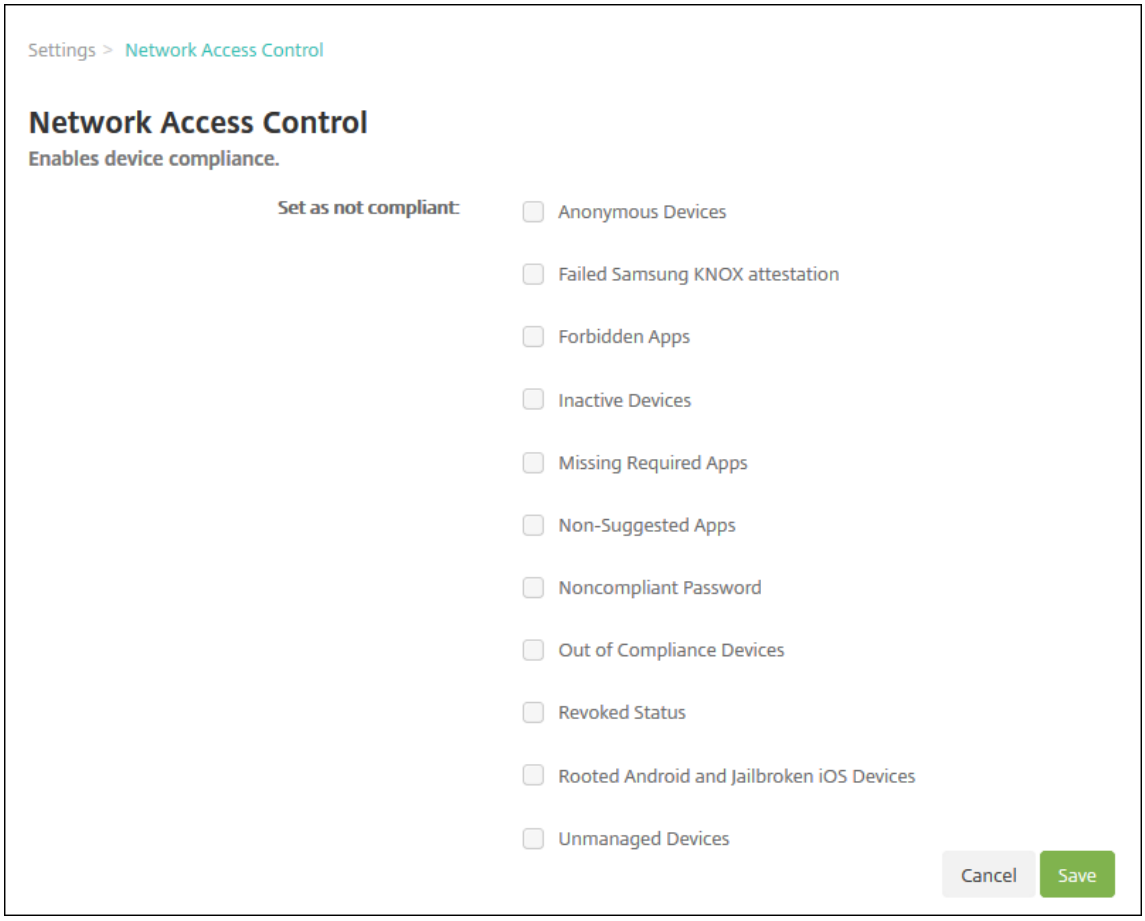
2. Habilite filtros NAC en XenMobile.
3. Configure una solución NAC:

- Citrix Gateway, detallado en Actualizar las directivas de Citrix Gateway para admitir NAC

  Requiere instalar Citrix SSO en los dispositivos. Consulte Clientes de Citrix Gateway.
- Cisco ISE: Consulte la documentación de Cisco.
- ForeScout: Consulte la documentación de ForeScout.

Habilitar filtros NAC en XenMobile

1. En la consola de XenMobile, vaya a **Parámetros > Control de acceso de red**.



2. Marque las casillas de los filtros **Establecer como no conforme** que quiera habilitar.
3. Haga clic en **Guardar**.

Actualizar las directivas de Citrix Gateway para admitir NAC

Debe configurar directivas avanzadas (no clásicas) de autenticación y de sesiones VPN en el servidor virtual de su VPN.

Estos pasos actualizan un dispositivo Citrix Gateway con cualquiera de estas características:

- Está integrado en un entorno de XenMobile Server.
- O bien, está configurado para VPN, no forma parte del entorno de XenMobile Server y puede establecer contacto con XenMobile.

En su servidor de VPN virtual desde una ventana de consola, haga lo siguiente. Las direcciones IP en los comandos y los ejemplos son ficticias.

1. Elimine y desenlace todas las directivas clásicas si las utiliza en su servidor de VPN virtual. Para verificar, escriba:

   ```
   show vpn vserver <VPN_VServer>
   ```

   Elimine todos los resultados que contengan la palabra Classic. Por ejemplo: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   Para eliminar la directiva, escriba:

   ```
   unbind vpn vserver <VPN_VServer> -policy <policy_name>
   ```

2. Cree la directiva de sesión avanzada correspondiente. Para ello, escriba lo siguiente.

   ```
   add vpn sessionPolicy <policy_name> <rule> <session action>
   ```

   Por ejemplo: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. Enlace la directiva a su servidor de VPN virtual. Para ello, escriba lo siguiente.

   ```
   bind vpn vserver _XM_XenMobileGateway -policy vpn_nac -priority 100
   ```

4. Cree un servidor virtual de autenticación. Para ello, escriba lo siguiente.

   ```
   add authentication vserver <authentication vserver name> <service type>
    <ip address>
   ```

   Por ejemplo:`add authentication vserver authvs SSL 0.0.0.0`
   En el ejemplo, `0.0.0.0` significa que el servidor virtual de autenticación no es público.

5. Enlace un certificado SSL con el servidor virtual. Para ello, escriba lo siguiente.

   ```
   bind ssl vserver <authentication vserver name> -certkeyName <Webserver
   certificate>
   ```

   Por ejemplo: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Asocie un perfil de autenticación al servidor virtual de autenticación desde el servidor de VPN virtual. Primero, cree el perfil de autenticación. Para ello, escriba lo siguiente.

   ```
   add authentication authnProfile <profile name> -authnVsName <authentication
    vserver name>
   ```

   Por ejemplo:

   ```
   add authentication authnProfile xm_nac_prof -authnVsName authvs
   ```


7. Asocie el perfil de autenticación al servidor de VPN virtual. Para ello, escriba lo siguiente.

   ```
   set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
   ```

   Por ejemplo:

   ```
   set vpn vserver _XM_XenMobileGateway -authnProfile xm_nac_prof
   ```

8. Compruebe la conexión desde Citrix Gateway a un dispositivo. Para ello, escriba lo siguiente.

   ```
   curl -v -k https://<XenMobile server>:4443/Citrix/Device/v1/Check --
   header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
   ```

   Por ejemplo, esta consulta verifica la conectividad obteniendo el estado de cumplimiento del primer dispositivo (`deviceid_1`) inscrito en el entorno:

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-
   Citrix-VPN-Device-ID: deviceid_1"
   ```

   Un resultado correcto es similar al siguiente ejemplo.

   ```
   1 HTTP/1.1 200 OK
   2 < Server: Apache-Coyote/1.1
   3 < X-Citrix-Device-State: Non Compliant
   4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   5 <!--NeedCopy-->
   ```

9. Si el paso anterior da el resultado correcto, cree la acción de autenticación Web en XenMobile. Primero, cree una expresión de directiva para extraer el ID del dispositivo desde el complemento VPN de iOS. Escriba lo siguiente.

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).
   TYPECAST_NVLIST_T(\'=\',\'&\').VALUE(\"deviceidvalue\")"
   ```

10. Envíe la solicitud a XenMobile. Para ello, escriba lo siguiente. En este ejemplo, la dirección IP de XenMobile Server es `10.207.87.82` y el FQDN es `example.em.server.com:4443`.

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort
     4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n"+ "
    Host: example.em.server.com:4443\r\n"+ "X-Citrix-VPN-Device-ID: "+
    xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.
    RES.STATUS.EQ(\"200\")&&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ
    (\"Compliant\")"
    ```

    El resultado correcto para XenMobile NAC es `HTTP status 200 OK`. El encabezado `X-Citrix-Device-State` debe tener el valor `Compliant`.

11. Cree una directiva Autenticación con la que asociar la acción. Para ello, escriba lo siguiente.


```
add authentication Policy <policy name> -rule <rule> -action <web
authentication action>
```

Por ejemplo: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")"-action xm_nac`

12. Convierta la directiva de LDAP existente en una directiva avanzada. Para ello, escriba lo siguiente.

```
add authentication Policy <policy_name> -rule <rule> -action <LDAP
action name>
```

Por ejemplo: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Agregue una etiqueta de directiva con la que asociar la directiva de LDAP. Para ello, escriba lo siguiente.

```
add authentication policylabel <policy_label_name>
```

Por ejemplo: `add authentication policylabel ldap_pol_label`

14. Asocie la directiva de LDAP a la etiqueta de directiva. Para ello, escriba lo siguiente.

```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol
 -priority 100 -gotoPriorityExpression NEXT
```

15. Conecte un dispositivo conforme para hacer una prueba de NAC y confirmar la autenticación LDAP correcta. Escriba lo siguiente.

```
bind authentication vserver <authentication vserver> -policy <web
authentication policy> -priority 100 -nextFactor <ldap policy label> -
gotoPriorityExpression END
```

16. Agregue la interfaz de usuario a asociar con el servidor virtual de autenticación. Escriba el siguiente comando para recuperar la identificación del dispositivo.

```
add authentication loginSchemaPolicy <schema policy>-rule <rule> -
action lschema_single_factor_deviceid
```

17. Enlace el servidor virtual de autenticación. Para ello, escriba lo siguiente.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority
 100 -gotoPriorityExpression END
```

18. Cree una directiva de LDAP avanzada de autenticación para permitir la conexión de Secure Hub. Escriba lo siguiente.

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"NAC\").NOT"-action 10.200.80.60_LDAP
```



```
bind authentication vserver authvs -policy ldap_xm_test_pol -priority
110 -gotoPriorityExpression NEXT
```

Samsung Knox

January 4, 2022

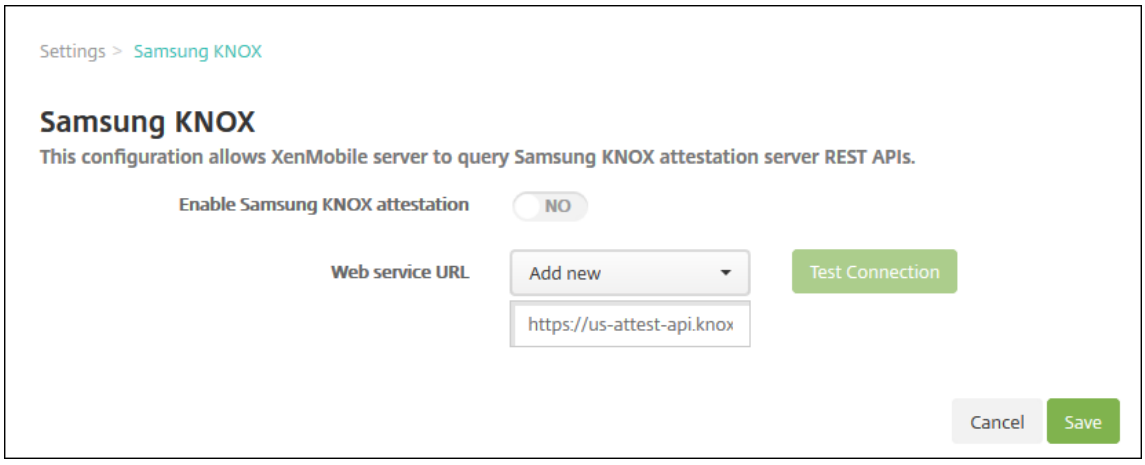
Samsung ofrece varias soluciones compatibles con XenMobile Server.

- XenMobile admite y amplía las directivas de Samsung Knox en dispositivos Samsung compatibles.
- Knox Service Plugin (KSP) es una aplicación que ofrece un subconjunto de funciones de Knox Platform for Enterprise (KPE). Para obtener información de Samsung sobre KPE, consulte Configure Knox Platform for Enterprise y Overview.

Puede configurar XenMobile para consultar las API de REST del servidor de atestación de Samsung Knox.

Samsung Knox utiliza las funcionalidades de seguridad del hardware y ofrece varios niveles de protección para el sistema operativo y las aplicaciones. Un nivel de esta seguridad se encuentra en la plataforma mediante la atestación. Un servidor de atestación ofrece la comprobación del software del sistema principal del dispositivo móvil (por ejemplo, los cargadores de arranque y el kernel). La verificación se produce en tiempo de ejecución en función de los datos recopilados durante el arranque seguro.

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



3. En **Habilitar atestación de Samsung Knox**, seleccione si habilitar la atestación de Samsung Knox. De forma predeterminada, está **desactivado**.

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:
    - Haga clic en el servidor de atestación adecuado.
    - Haga clic en **Agregar nuevo** e introduzca la dirección URL del servicio web.
5. Haga clic en **Probar conexión** 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 **Guardar**.

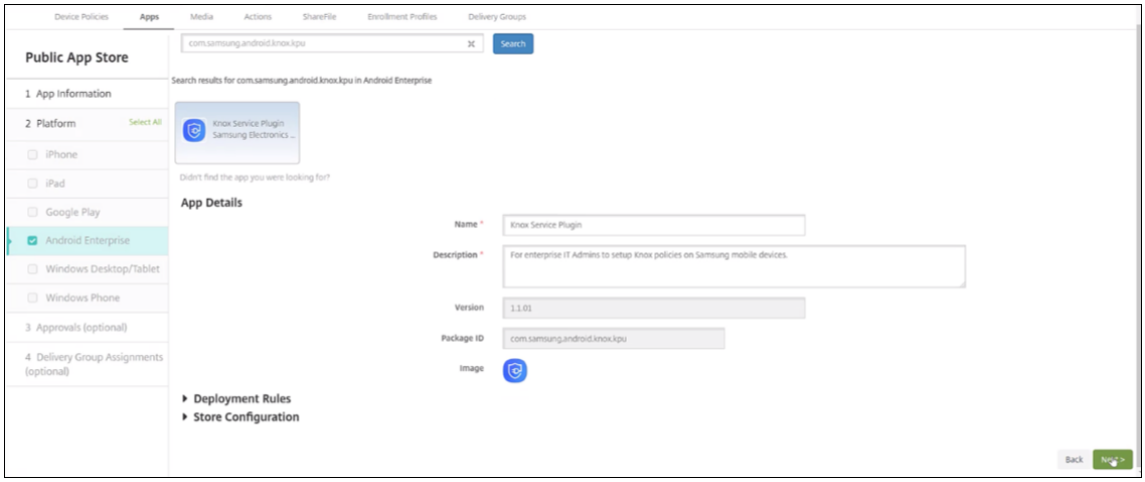
> **Nota:**
>
> Puede usar Samsung Knox Mobile Enrollment para inscribir varios dispositivos Samsung Knox en XenMobile (o en cualquier administrador de dispositivos móviles) sin necesidad de configurar manualmente cada uno de los dispositivos. Para obtener información, consulte Inscribir en bloque dispositivos Samsung Knox.

Agregar la aplicación Knox Service Plugin

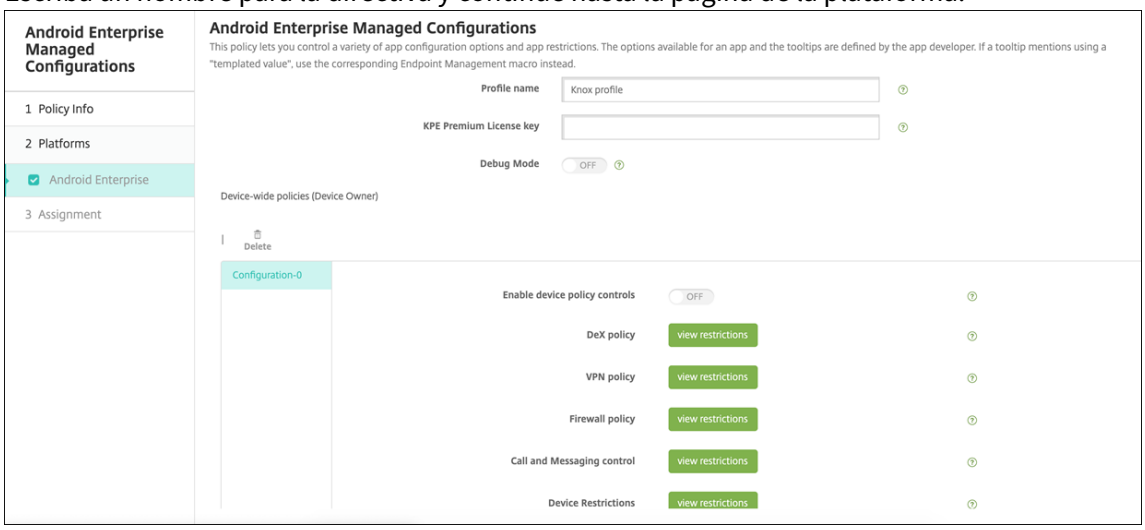
Si piensa usar Android Enterprise con Knox, agregue Knox Service Plug-in a XenMobile. La aplicación KSP utiliza AndroidOEMConfig para ofrecer funciones tales como directivas de seguridad, configuración flexible de VPN y controles de autenticación biométrica. AndroidOEMConfig permite a los fabricantes de equipos originales (OEM) y a los administradores de movilidad de dispositivos finales (EMM) ofrecer API de OEM personalizadas. Estas API cubren casos de uso que no ofrece Android Enterprise.

Para obtener más información sobre KSP, consulte Knox Service Plug-in Admin Guide.

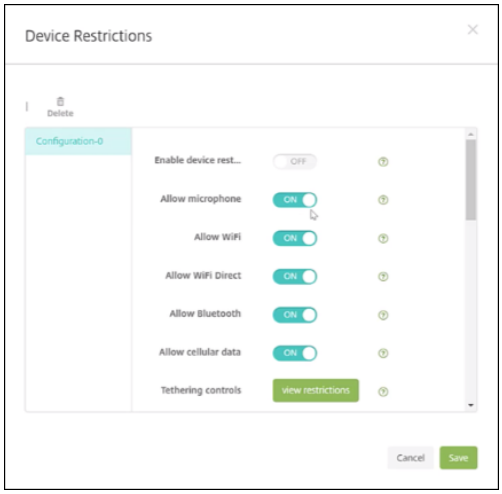
1. Inicie sesión en su cuenta de Google y vaya a `https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu`. Apruebe la aplicación Knox Service Plug-in.
2. Inicie sesión en la consola de XenMobile y agregue Knox Service Plugin como una aplicación de tienda pública de aplicaciones. Para obtener más información sobre cómo agregar aplicaciones de tienda pública de aplicaciones, consulte Agregar una aplicación de la tienda pública de aplicaciones.



3. En la consola de XenMobile, vaya a **Configurar > Directivas de dispositivo**. Haga clic en **Agregar**.
4. Haga clic en **Configuración administrada de Android Enterprise**. En el cuadro de diálogo que aparece, seleccione **Knox Service Plugin** en el menú. Para obtener más información sobre la directiva de configuraciones administradas por Android Enterprise, consulte Directiva Configuraciones administradas por Android Enterprise.
5. Escriba un nombre para la directiva y continúe hasta la página de la plataforma.



6. En la página de la plataforma, escriba un **nombre de perfil** para su perfil de Knox e introduzca la **clave de licencia Premium de KPE** de Samsung. Las directivas que aparecen debajo de estos campos provienen de su implementación de Knox. Para obtener más información sobre las directivas de Knox, consulte la guía Knox Service Admin Plug-in Guide a la que se ha hecho referencia en esta sección.



7. Haga clic en **Siguiente** y configure las reglas de implementación de la directiva.
8. Haga clic en **Guardar**.

Inscribir en bloque dispositivos Samsung Knox

January 4, 2022

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, use Knox Mobile Enrollment. La inscripción tiene lugar la primera vez que se usa el dispositivo o después de restablecerlo a sus valores de fábrica. Los administradores también pueden pasar nombres de usuarios y contraseñas directamente al dispositivo, por lo que los usuarios no necesitan escribir ningún dato en el momento de la inscripción.

> **Nota:**
>
> La configuración de Knox Mobile Enrollment no está relacionada con el contenedor Knox de XenMobile. Para obtener más información sobre Knox Mobile Enrollment, consulte Knox Mobile Enrollment Admin Guide.

Requisitos previos para Knox Mobile Enrollment

- XenMobile debe estar configurado (incluidas las licencias y los certificados) y en ejecución.
- Archivo APK de Secure Hub. Hay que cargar este archivo al configurar Knox Mobile Enrollment.
- Para obtener una lista de los requisitos de KME, consulte Knox Mobile Enrollment Introduction.
- Licencia de Knox Platform for Enterprise (PKE) de Samsung, necesaria para aplicar directivas de dispositivos. Proporcione la clave de licencia en la directiva de XenMobile, Knox Platform for Enterprise.

Para descargar el archivo APK de Secure Hub

Vaya a la tienda de Google Play para descargar el archivo de Citrix Secure Hub para Android.

Configurar excepciones del firewall

Para acceder a Knox Mobile Enrollment, configure las siguientes excepciones del firewall. Algunas excepciones de firewall son necesarias para todos los dispositivos y algunas son específicas de la región geográfica de cada dispositivo.

Región del dispositivo	URL	Port	Destino
Todas	https://gslb.secb2b.com	443	Equilibrador de carga global para iniciar Knox Mobile Enrollment
Todas	https://gslb.secb2b.com	80	Equilibrador de carga global para iniciar Knox Mobile Enrollment en algunos dispositivos antiguos limitados
Todas	umc-cdn.secb2b.com	443	Servidores de actualización de agentes Samsung
Todas	bulkenrollment.s3.amazonaws.com	80	Contratos EULA de cliente para Knox Mobile Enrollment
Todas	eula.secb2b.com	443	Contratos EULA de cliente para Knox Mobile Enrollment
Todas	us-be-api-mssl.samsungknox.com	443	Servidores Samsung para verificación de IMEI
Estados Unidos	https://us-segd-api.secb2b.com	443	Samsung Enterprise Gateway para la región de EE. UU.

Región del dispositivo	URL	Port	Destino
Europa	`https://eu-segd-api.secb2b.com`	443	Samsung Enterprise Gateway para la región de Europa
China	`https://china-segd-api.secb2b.com`	443	Samsung Enterprise Gateway para la región de China

> **Nota:**
>
> Puede ver una lista completa de excepciones de firewall en Knox Mobile Enrollment Admin Guide.

Obtener acceso a Knox Mobile Enrollment

Siga las instrucciones de la documentación de Samsung para obtener acceso a Knox Mobile Enrollment en Get started with KME.

Configurar Knox Mobile Enrollment

Después de obtener acceso a Knox Mobile Enrollment, inicie sesión en el portal Knox.

El proceso de inscripción sigue estos pasos generales.

1. Crear un perfil MDM con los parámetros y la información de su consola MDM.

   El perfil MDM indica a los dispositivos cómo conectarse al MDM.

2. Agregar dispositivos a su perfil de MDM.

   Puede cargar un archivo CSV con la información de los dispositivos o instalar y utilizar la aplicación de implementaciones de Knox desde Google Play.

3. Samsung le avisa cuando el propietario de los dispositivos se haya verificado.

4. Proporcionar a los usuarios unas credenciales de MDM. Indíqueles que se conecten a Internet por Wi-Fi y que acepten la petición de inscribir sus dispositivos.

Para crear un perfil MDM

Siga los pasos descritos en la documentación de Samsung en Profile Configuration.

Cuando encuentre los siguientes campos o pasos, configúrelos como se describe:

- **Pick your MDM:** Seleccione **Citrix** en el menú. Solo para perfiles de propietario de dispositivos.

- **MDM Agent APK:** Solo para perfiles de propietario de dispositivos. Introduzca la URL de descarga del archivo APK de Secure Hub: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

  El archivo APK puede residir en cualquier servidor al que los dispositivos puedan acceder durante la inscripción. Durante la inscripción, un dispositivo:

  - Descarga Secure Hub de una URL de descarga de APK
  - Instala Secure Hub
  - A continuación, abre Secure Hub con los datos JSON personalizados que se describen a continuación.

  Las mayúsculas y minúsculas del nombre del archivo APK deben coincidir con la dirección URL que se especifique. Por ejemplo, si el nombre de archivo va todo en minúscula, también debe figurar todo en minúscula en la dirección URL.

- **MDM Server URI:** No especifique ninguna URI de servidor MDM. XenMobile no usa el protocolo MDM de Samsung.

- **Custom JSON Data**: Secure Hub necesita la dirección del servidor de XenMobile Server, el nombre de usuario y la contraseña para la inscripción. Puede proporcionar esos datos en JSON para que Secure Hub no los solicite a los usuarios. Secure Hub pide a los usuarios la dirección del servidor, el nombre de usuario o la contraseña solo si el campo se omite en el JSON.

  El formato para los datos JSON personalizados es:

  ```
  { "serverURL": "URL", "xm_username":"Username", "xm_password":"Password
  "}
  ```

  En este ejemplo, típico para la inscripción en bloque, Secure Hub no solicita a los usuarios la dirección del servidor ni sus credenciales durante la inscripción:

  ```
  { "serverURL":"https://example.com/zdm", "xm_username":"userN", "
  xm_password":"password1234"}
  { "serverURL":"https://pmdm.mycorp-inc.net/zdm", "xm_username":"userN2"
  , "xm_password":"password7890"}
  ```

  En este ejemplo, típico para dispositivos en quiosco, Secure Hub solicita credenciales a los usuarios:

  ```
  { "serverURL":"https://example.com/zdm"}
  ```

  También puede escribir datos JSON personalizados para la inscripción automática de Android Enterprise.

  ```
  1       {
  2
  3           "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
  ```



```
4           {
5
6               "serverURL":"URL","xm_username":"username","
                    xm_password":"password"
7            }
8
9       }
10
11  <!--NeedCopy-->
```

Cuando un dispositivo inicia la inscripción, este descarga Secure Hub desde la URL indicada, lo instala y lo abre.

Configuración adicional

Consulte las siguientes páginas de documentación de Samsung para obtener más información sobre la configuración:

- Device configuration: Agregue dispositivos en bloque.
- Samsung Knox Deployment App: Inscriba dispositivos por Bluetooth, NFC o Wi-Fi Direct.
- Knox Mobile Enrollment: Consulte la documentación de Samsung para obtener más información sobre Samsung Knox.

Para inscribir dispositivos con una interfaz API de Knox anterior a la versión 2.4

En dispositivos que tienen la API de Knox anterior a la versión 2.4, la inscripción en bloque no se inicia durante la configuración inicial del dispositivo. En su lugar, son los usuarios quienes deben iniciar la inscripción. Para ellos, deben ir a un sitio de Samsung para descargar el nuevo cliente de Mobile Enrollment e iniciar la inscripción.

El cliente de inscripción descargado usa el mismo perfil MDM y los mismos archivos APK configurados en el portal de Knox Bulk Enrollment para los dispositivos Knox 2.4/2.4.1.

Los usuarios, por lo general, deben seguir estos pasos:

1. Encienda el dispositivo y conéctese a una red Wi-Fi. Si Mobile Enrollment no se abre o si no hay redes inalámbricas disponibles:
   a) Vaya a Samsung Knox Mobile Enrollment.
   b) Toque el botón **Next** para inscribir dispositivos a través de una conexión de datos móviles.
2. Cuando aparezca el diálogo **Enroll with Knox**, toque **Continue**.
3. Lea los Contratos de licencia del usuario final (EULA), si están disponibles. Toque **Siguiente**.

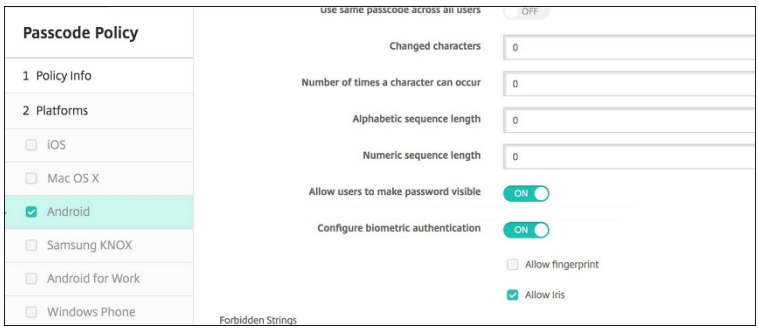
4. Si el sistema lo pide, introduzca el ID de usuario y la contraseña que le haya entregado su administrador de TI, en **User ID** y **Password**.

En este punto, se validan las credenciales de usuario y el dispositivo se inscribe en el entorno de TI empresarial de la organización.

Habilitar e inhabilitar la autenticación biométrica para dispositivos Samsung

XenMobile admite la autenticación de escaneo de huellas digitales e iris, también conocida como autenticación biométrica. Puede habilitar e inhabilitar la autenticación biométrica para dispositivos Samsung sin requerir ninguna acción por parte de los usuarios. Si inhabilita la autenticación biométrica en XenMobile, los usuarios y las aplicaciones de terceros no podrán habilitar esta función.

1. En la consola de XenMobile, haga clic en **Configurar** > **Directivas de dispositivo**. Aparecerá la página **Directivas de dispositivo**.
2. Haga clic en **Agregar**. Aparecerá la página **Agregar nueva directiva**.
3. Haga clic en **Código de acceso**. Aparecerá la página de información **Directiva de código de acceso**.
4. En el panel **Información de directiva**, escriba la información siguiente:
   - **Nombre de directiva:** Escriba un nombre descriptivo para la directiva.
   - **Descripción:** Escriba una descripción opcional de la directiva.
5. Haga clic en **Siguiente**. Aparecerá la página **Plataformas** de la directiva.
6. En **Plataformas**, seleccione **Android** o **Samsung Knox**.
7. **Active** el parámetro **Configurar la autenticación biométrica**.
8. Si ha seleccionado **Android**, en **Samsung SAFE**, seleccione Permite **huella dactilar**, **Permite iris** o ambas opciones.



Acciones de seguridad

January 4, 2022

Puede realizar acciones de seguridad en dispositivos y aplicaciones desde la página **Administrar** > **Dispositivos**. Las acciones de seguridad en los dispositivos son: revocar, bloquear, desbloquear y borrar. Las acciones de seguridad en las aplicaciones son: bloquear y borrar.

- **Omisión del bloqueo de activación:** En dispositivos iOS supervisados, quita el Bloqueo de activación antes de la activación del dispositivo. Este comando no requiere el ID de Apple ni la contraseña personal de un usuario.
- **Bloqueo de aplicaciones:** Deniega el acceso a todas las aplicaciones de un dispositivo. En Android, después de un bloqueo de aplicaciones, los usuarios no pueden iniciar sesión en XenMobile. En iOS, los usuarios pueden iniciar sesión, pero no pueden acceder a ninguna aplicación.
- **Eliminación de aplicaciones:** Elimina la cuenta de usuario que consta en Secure Hub y desinscribe el dispositivo. Los usuarios no pueden volver a inscribirse hasta que se realice la acción **Anular borrado de aplicaciones**.
- **Bloqueo de activación del Programa de implementación de ASM:** Crea un código de anulación del bloqueo de activación para dispositivos iOS inscritos en DEP de Apple School Manager.
- **Desactivar restricciones:** En dispositivos iOS supervisados, este comando permite que XenMobile borre la contraseña de restricciones y los parámetros de restricciones configurados por el usuario.
- **Habilitar o inhabilitar el modo perdido:** Coloca un dispositivo iOS supervisado en el modo Perdido y envía un mensaje, un número de teléfono y una nota al pie que aparecen en el dispositivo. La segunda vez que se envíe este comando, el dispositivo sale del modo Perdido.
- **Habilitar seguimiento:** En dispositivos Android o iOS, este comando permite a XenMobile sondear la ubicación de dispositivos concretos con la frecuencia que defina. Para ver las coordenadas y la ubicación del dispositivo en un mapa, vaya a **Administrar > Dispositivos**, seleccione un dispositivo y, a continuación, haga clic en **Modificar**. La información del dispositivo se encuentra en la ficha **General**, en **Seguridad** . Utilice **Habilitar seguimiento** para hacer seguimiento del dispositivo de forma continua. Secure Hub informa periódicamente de la ubicación cuando el dispositivo está en funcionamiento.
- **Borrado completo:** Borra inmediatamente todos los datos y todas las aplicaciones que hubiera presentes en un dispositivo, incluidas las tarjetas de memoria.
  - En caso de dispositivos Android, esta solicitud puede incluir la opción de borrar las tarjetas de memoria.

  - Para dispositivos Android Enterprise totalmente administrados con un perfil de trabajo (dispositivos COPE), puede realizar un borrado completo después de la eliminación del perfil de trabajo mediante un borrado selectivo.
  - Para dispositivos iOS y macOS, el borrado se aplica inmediatamente, incluso aunque el dispositivo esté bloqueado. Para dispositivos iOS 11 (versión mínima): Tras confirmar el borrado completo, puede optar por conservar el plan de datos móviles que hubiera presente en el dispositivo.
  - En caso de dispositivos Windows Phone, un borrado completo elimina toda la información de XenMobile, además de todos los datos del usuario. En los datos, se incluye contenido personal (como aplicaciones, mensajes de correo electrónico, contactos y archivos multimedia).
  - Si los dispositivos Windows Mobile ejecutan Windows Mobile 6 o una versión anterior, después del borrado, es posible que deba enviar el dispositivo al fabricante para que este vuelva a cargar el sistema operativo original, el software original o ambos.
  - Si el usuario apaga el dispositivo antes de que se elimine el contenido de la tarjeta de memoria, aún podría tener acceso a los datos del dispositivo.
  - Puede cancelar la solicitud de borrado hasta que se envíe al dispositivo.

- **Localizar:** Busca un dispositivo y notifica su ubicación con un mapa en la página **Administrar > Dispositivos**, en **Detalles del dispositivo > General**. Localizar es una acción que tiene lugar una sola vez. Use **Localizar** para mostrar la ubicación actual del dispositivo en el momento en que se realiza la acción. Para realizar un seguimiento continuo del dispositivo durante un período de tiempo, utilice **Habilitar seguimiento**.
  - Al aplicar esta acción a dispositivos Android (excepto Android Enterprise) o a dispositivos Android Enterprise (propiedad de la empresa o BYOD), tenga en cuenta el siguiente comportamiento:
    * **Localizar** requiere que el usuario conceda permiso de localización durante la inscripción. El usuario puede optar por no conceder permiso de localización. Si el usuario no concede el permiso durante la inscripción, XenMobile vuelve a solicitarlo cuando envía el comando **Localizar**.
  - Al aplicar esta funcionalidad a dispositivos iOS o Android Enterprise, tenga en cuenta las siguientes limitaciones:
    * Para dispositivos Android Enterprise, esta solicitud falla, a menos que la directiva Localización haya establecido el modo de ubicación para el dispositivo en **Alta precisión** o **Ahorro de batería**.
    * Para los dispositivos iOS, este comando solo se ejecuta correctamente si los dispositivos se encuentran en el modo perdido de MDM.

- **Bloqueo:** Bloquea a distancia un dispositivo. Esta acción es útil cuando se pierde un dispositivo

y no se sabe si ha sido robado. Cuando se envía este comando, XenMobile genera un código PIN y lo establece en el dispositivo. Para acceder al dispositivo, el usuario deberá teclear ese código PIN. Use el comando **Cancelar bloqueo** para quitar el bloqueo desde la consola de XenMobile.

- **Bloquear y restablecer contraseña:** Bloquea a distancia un dispositivo y restablece el código de acceso en él.
  - No se admite para dispositivos inscritos en Android Enterprise en el modo de perfil de trabajo con versiones de Android anteriores a Android 8.0.
  - En dispositivos inscritos en Android Enterprise en el modo de perfil de trabajo con Android 8.0 o una versión posterior:
    * El código de acceso enviado bloquea el perfil de trabajo. El dispositivo no se bloquea.
    * Si no se envía ningún código de acceso o el código enviado no cumple los requisitos de código de acceso y no se había establecido ningún código de acceso en el perfil de trabajo, el dispositivo se bloquea.
    * Si no se envía ningún código de acceso o el código enviado no cumple los requisitos de código de acceso, pero ya se había establecido un código de acceso en el perfil de trabajo, el perfil de trabajo se bloquea, pero el dispositivo no se bloquea.
- **Notificar (Hacer sonar):** Reproduce un sonido en dispositivos Android.
- **Reiniciar:** Reinicia dispositivos con Windows 10 o Windows 11. Para tabletas y equipos Windows, aparece el mensaje "El sistema va a reiniciase" y el reinicio se produce en cinco minutos. En Windows Phone, no aparece ningún mensaje de advertencia a los usuarios y el reinicio se produce después de unos minutos.
- **Solicitar o detener duplicación AirPlay:** Inicia y detiene la duplicación AirPlay en los dispositivos iOS supervisados.
- **Reiniciar o apagar:** Reinicia o apaga inmediatamente dispositivos iOS supervisados.
- **Revocar:** Prohíbe a un dispositivo que se conecte a XenMobile Server.
- **Revocar o autorizar (iOS, macOS):** Realiza las mismas acciones que el borrado selectivo. Después de la revocación, puede volver a autorizar el dispositivo para la reinscripción.
- **Hacer sonar:** Si el dispositivo está en el modo perdido, esta acción reproduce un sonido en un dispositivo iOS supervisado. El sonido se reproduce hasta que se saque al dispositivo del modo perdido o hasta que el usuario quite el sonido.
- **Borrado selectivo:** Borra todas las aplicaciones y los datos de empresa de un dispositivo, pero no afecta a las aplicaciones ni los datos personales. Después de un borrado selectivo, un usuario puede volver a inscribir el dispositivo.
  - Borrar un dispositivo Android de forma selectiva no lo desconecta de Device Manager ni de la red corporativa. Para evitar que el dispositivo acceda a Device Manager, también debe revocar los certificados de dispositivo.

  - Borrar selectivamente los datos de un dispositivo Android también revoca el dispositivo. Puede volver a inscribir el dispositivo solo después de reautorizarlo o eliminarlo de la consola.
  - Para dispositivos Android Enterprise totalmente administrados con un perfil de trabajo (dispositivos COPE), puede realizar un borrado completo después de la eliminación del perfil de trabajo mediante un borrado selectivo. O bien, puede volver a inscribir el dispositivo con el mismo nombre de usuario. Al reinscribir el dispositivo, se vuelve a crear el perfil de trabajo.
  - Si habilita la API de Samsung Knox, el borrado selectivo también quita el contenedor Samsung Knox del dispositivo.
  - Para dispositivos iOS y macOS, este comando elimina cualquier perfil instalado a través de MDM.
  - El borrado selectivo en un dispositivo Windows también elimina el contenido de la carpeta de perfil del usuario que haya iniciado sesión en el dispositivo en ese momento. En un borrado selectivo, no se elimina ningún clip web que entregue a los usuarios a través de una configuración. Los clips web se eliminan cuando los usuarios desinscriben sus dispositivos de forma manual. No se puede volver a inscribir un dispositivo en el que se ha realizado el borrado selectivo.
  - El borrado selectivo de un dispositivo Windows Phone quita el token de empresa, el cual permite que XenMobile instale aplicaciones en el dispositivo. El borrado también elimina todos los certificados y todas las configuraciones de XenMobile que se hayan implementan en el dispositivo. No se puede volver a inscribir un dispositivo Windows Phone en el que se ha realizado el borrado selectivo.

- **Desbloquear:** Borra el código de acceso que se envía al dispositivo cuando este se bloquea. Este comando no desbloquea el dispositivo.

En **Administrar > Dispositivos**, la página **Detalles del dispositivo** muestra también las propiedades de seguridad del dispositivo. Entre esas propiedades, se encuentran: el ID seguro, el bloqueo del dispositivo, la omisión del bloqueo de activación, así como otra información en función del tipo de plataforma. El campo **Borrado completo del dispositivo** contiene el código PIN del usuario. El usuario debe introducir ese código después de que se haya borrado el dispositivo. Si el usuario no consigue recordar el código, usted puede buscarlo en “Detalles del dispositivo”.

Acciones de seguridad para dispositivos Android

Acción de seguridad	Android (excepto para dispositivos Android Enterprise)	Android Enterprise (uso de dispositivos personales en el trabajo)	Android Enterprise (dispositivos de la empresa)
Bloqueo de aplicaciones	Sí	No	No
Borrado de aplicaciones	Sí	No	No
Borrado completo	Sí	No	Sí
Localizar	Sí: Para dispositivos que ejecutan Android 6.0+, el comando “Localizar” requiere que el usuario conceda permisos de localización durante la inscripción. El usuario puede optar por no conceder permisos de localización. Si el usuario no concede el permiso durante la inscripción, XenMobile vuelve a solicitarlo cuando envía el comando de localización.	Sí: Para dispositivos que ejecutan Android 6.0+, el comando “Localizar” requiere que el usuario conceda permisos de localización durante la inscripción. El usuario puede optar por no conceder permisos de localización. Si el usuario no concede el permiso durante la inscripción, XenMobile vuelve a solicitarlo cuando envía el comando de localización.	Sí: Para dispositivos que ejecutan Android 6.0+, el comando “Localizar” requiere que el usuario conceda permisos de localización durante la inscripción. El usuario puede optar por no conceder permisos de localización. Si el usuario no concede el permiso durante la inscripción, XenMobile vuelve a solicitarlo cuando envía el comando de localización.
Bloquear	Sí	Sí	Sí
Bloqueo y restablecimiento de contraseña	Sí	No	Sí
Notificar (Hacer sonar)	Sí	Sí	Sí
Revocar	Sí	Sí	Sí
Borrado selectivo	Sí	Sí	No

Acciones de seguridad para dispositivos iOS y macOS

Acción de seguridad	iOS	macOS
Omisión del bloqueo de activación	Sí	No
Bloqueo de aplicaciones	Sí	No
Borrado de aplicaciones	Sí	No
Bloqueo de activación del programa de implementación de ASM	Sí	No
Desactivar restricciones	Sí	No
Habilitar o inhabilitar el modo perdido	Sí	No
Habilitar o inhabilitar el seguimiento	Sí	No
Borrado completo	Sí	Sí
Localizar	Sí	No
Bloquear	Sí	Sí
Hacer sonar	Sí	Sí
Solicitar o detener la duplicación AirPlay	Sí	No
Reiniciar o apagar	Sí	No
Revocar o autorizar	Sí	Sí
Borrado selectivo	Sí	Sí
Desbloquear	Sí	No

Acciones de seguridad para dispositivos Windows

Acción de seguridad	Windows Phone 10	Windows Tablet 10	Windows Phone 8.1
Localizar	Sí	Sí	No
Bloquear	Sí	Sí	Sí

Acción de seguridad	Windows Phone 10	Windows Tablet 10	Windows Phone 8.1
Bloqueo y restablecimiento de contraseña	Sí	No	Sí
Reiniciar	Sí	Sí	No
Revocar	Sí	Sí	Sí
Hacer sonar	Sí	No	Sí
Borrado selectivo	Sí	Sí	Sí
Borrar	Sí	Sí	Sí

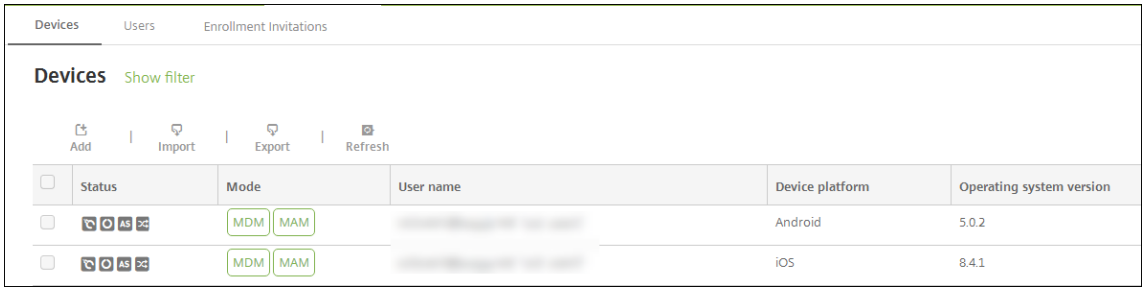
En el resto de este artículo se indican los pasos a seguir para realizar diversas acciones de seguridad. También se pueden automatizar algunas acciones. Para obtener información detallada, consulte Acciones automatizadas.

Bloquear dispositivos iOS

Puede bloquear un dispositivo iOS perdido y mostrar un mensaje y un número de teléfono en la pantalla de bloqueo. Esta función se admite en dispositivos iOS 7 y versiones posteriores.

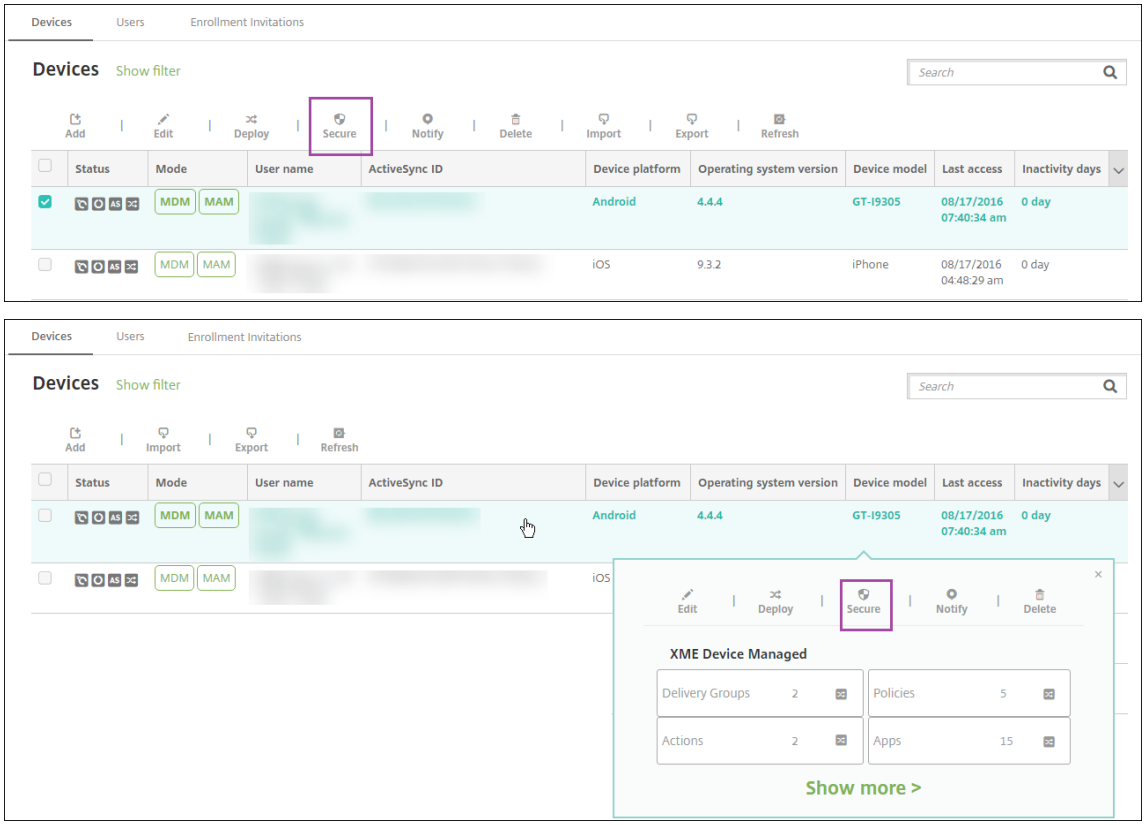
Para que se muestren un mensaje y un teléfono en un dispositivo bloqueado, establezca la directiva Código de acceso en **true** en la consola de XenMobile. De forma alternativa, los usuarios pueden habilitar manualmente el código de acceso en el dispositivo.

1. Haga clic en **Administrar > Dispositivos**. Aparecerá la página **Dispositivos**.

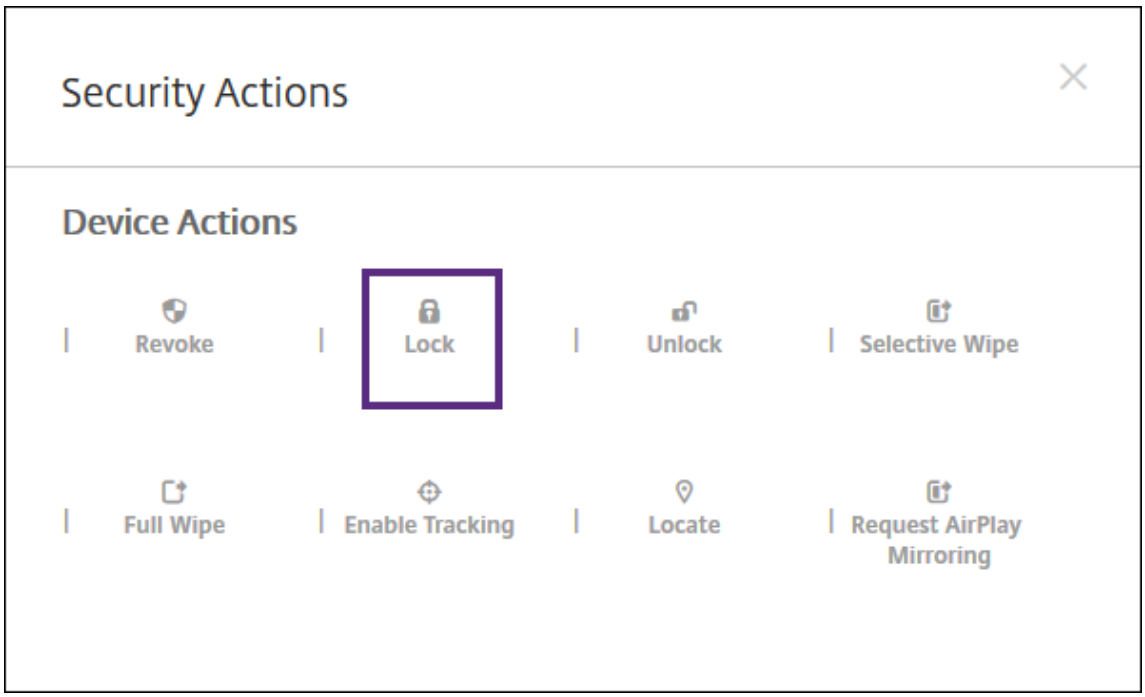


2. Seleccione el dispositivo iOS que quiere bloquear.

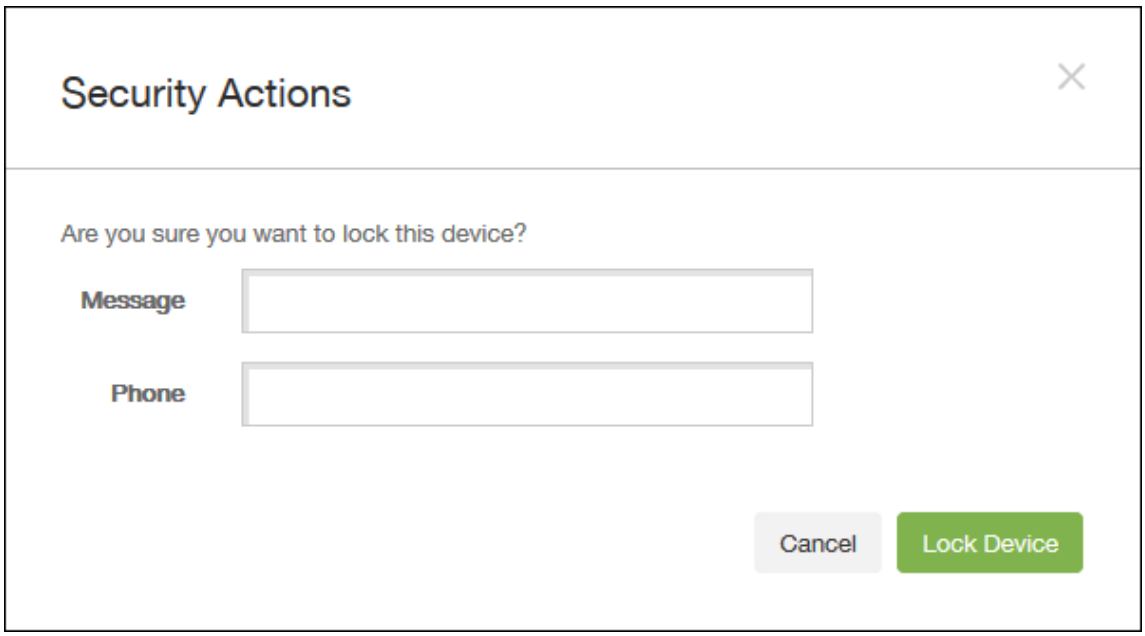
   Cuando se marca la casilla de verificación situada junto a un dispositivo, el menú de opciones aparece encima de la lista de dispositivos. Si hace clic en cualquier lugar de la lista, el menú de opciones aparece a la derecha de la lista.



3. En el menú de opciones, seleccione **Proteger**. Aparecerá el cuadro de diálogo **Acciones de seguridad**.



4. Haga clic en **Bloquear**. Aparecerá el cuadro de confirmación **Acciones de seguridad**.



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**.

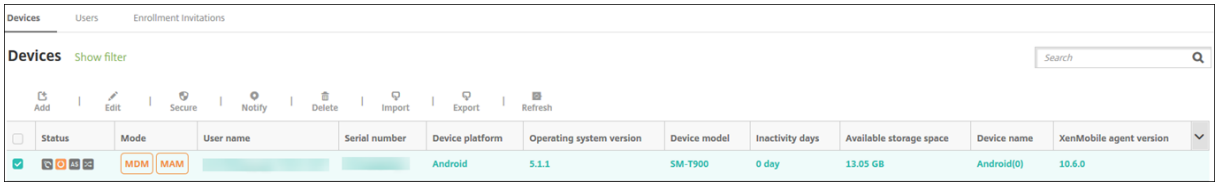
   Para iPhones que ejecutan iOS 7 y versiones posteriores: Si deja el campo **Mensaje** vacío y proporciona un número de teléfono, Apple mostrará un mensaje del tipo “Llamar al propietario” en la pantalla de bloqueo del dispositivo.

6. Haga clic en **Bloquear dispositivo**.

Quitar un dispositivo de la consola de XenMobile

> **Importante:**
>
> Cuando se quita un dispositivo de la consola de XenMobile, las aplicaciones administradas y los datos permanecen en el dispositivo. Para quitar las aplicaciones administradas y los datos que contiene el dispositivo, consulte “Eliminar un dispositivo” más adelante en este artículo.

Para eliminar un dispositivo de la consola de XenMobile, vaya a **Administrar > Dispositivos**, seleccione el dispositivo administrado y, a continuación, haga clic en **Eliminar**.



Borrar datos selectivamente de un dispositivo

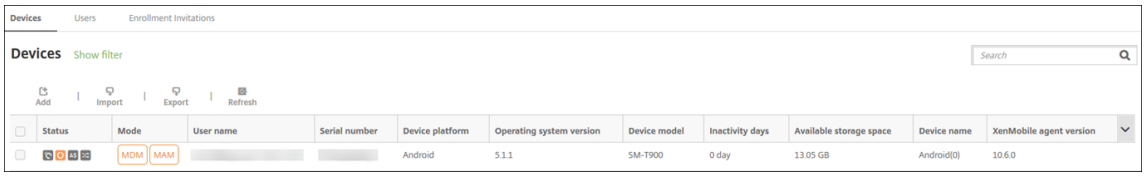
1. Vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado y haga clic en **Proteger**.
2. En **Acciones de seguridad**, haga clic en **Borrado selectivo**.
3. En los dispositivos Android (y únicamente en ellos), desconecte el dispositivo de la red corporativa. Para ello, después de que se borre el dispositivo, en **Acciones de seguridad**, haga clic en **Revocar**.

   Para anular una solicitud de borrado selectivo antes de que se haya llevado a cabo, en **Acciones de seguridad**, haga clic en **Cancelar borrado selectivo**.

Eliminar un dispositivo

Este procedimiento elimina las aplicaciones administradas y los datos que contiene un dispositivo. Asimismo, se elimina el dispositivo de la lista "Dispositivos" en la consola de XenMobile. Puede utilizar la API de REST pública de Endpoint Management para eliminar dispositivos en bloque.

1. Vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado y haga clic en **Proteger**.
2. Haga clic en **Borrado selectivo**. Cuando se le solicite, haga clic en **Ejecutar borrado selectivo**.
3. Para verificar que el comando de borrado se ha realizado, actualice **Administrar > Dispositivos**. En la columna **Modo**, el color anaranjado de MAM y MDM indica que el comando de borrado se ha realizado.



4. En **Administrar > Dispositivos**, seleccione el dispositivo y haga clic en **Eliminar**. Cuando se le solicite, haga clic en **Eliminar** de nuevo.

Bloquear, desbloquear, borrar o anular el borrado de aplicaciones

1. Vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado y haga clic en **Proteger**.
2. En el cuadro de diálogo **Acciones de seguridad**, haga clic en la acción de aplicaciones pertinente.

   También puede utilizar el cuadro de diálogo **Acciones de seguridad** para consultar el estado del dispositivo de un usuario cuya cuenta se haya inhabilitado o eliminado de Active Directory.

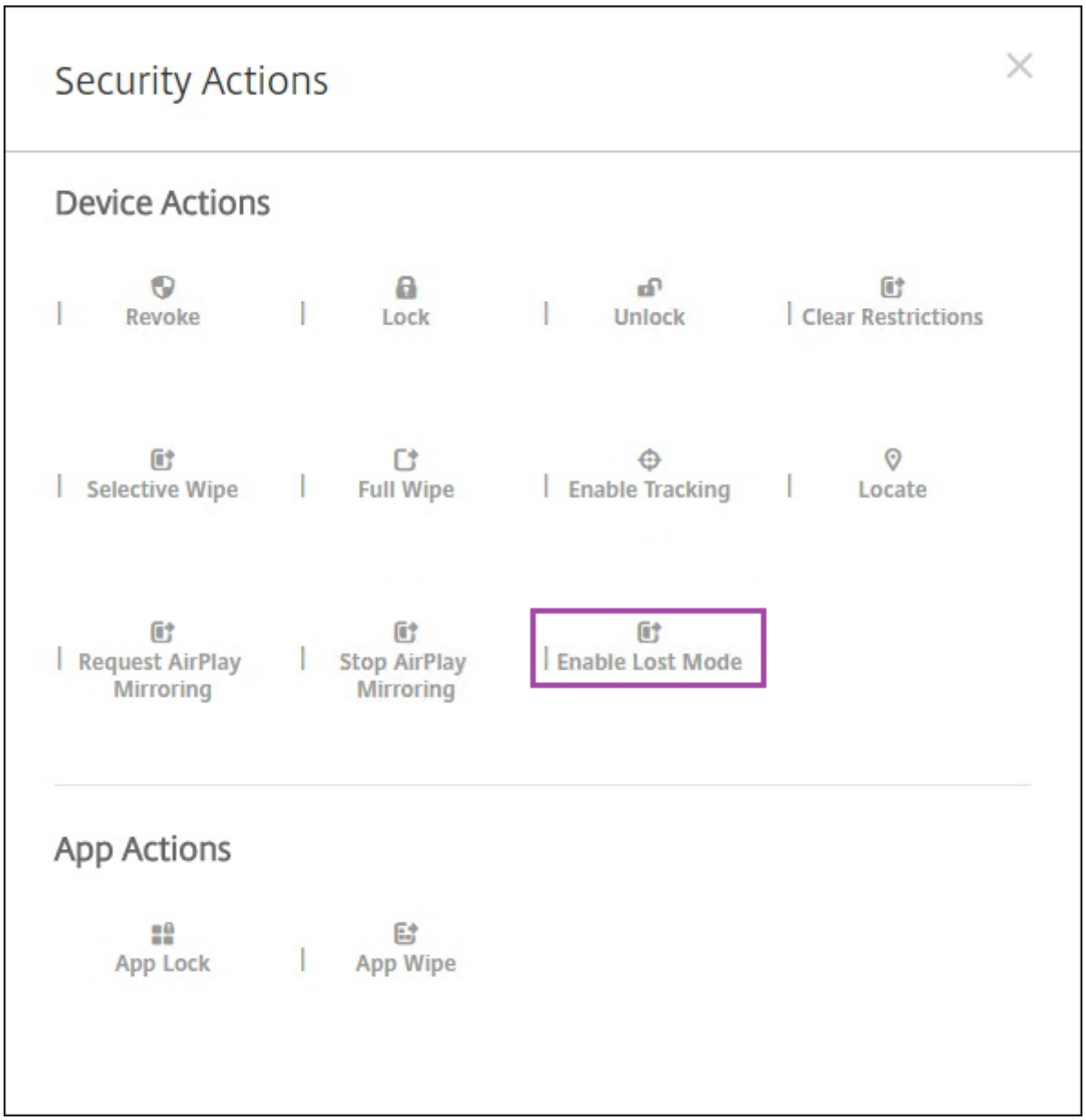
La presencia de las acciones “Desbloqueo de aplicaciones” o “Anular borrado de aplicaciones” indica que hay aplicaciones que se han bloqueado o borrado.

Colocar dispositivos iOS en modo perdido

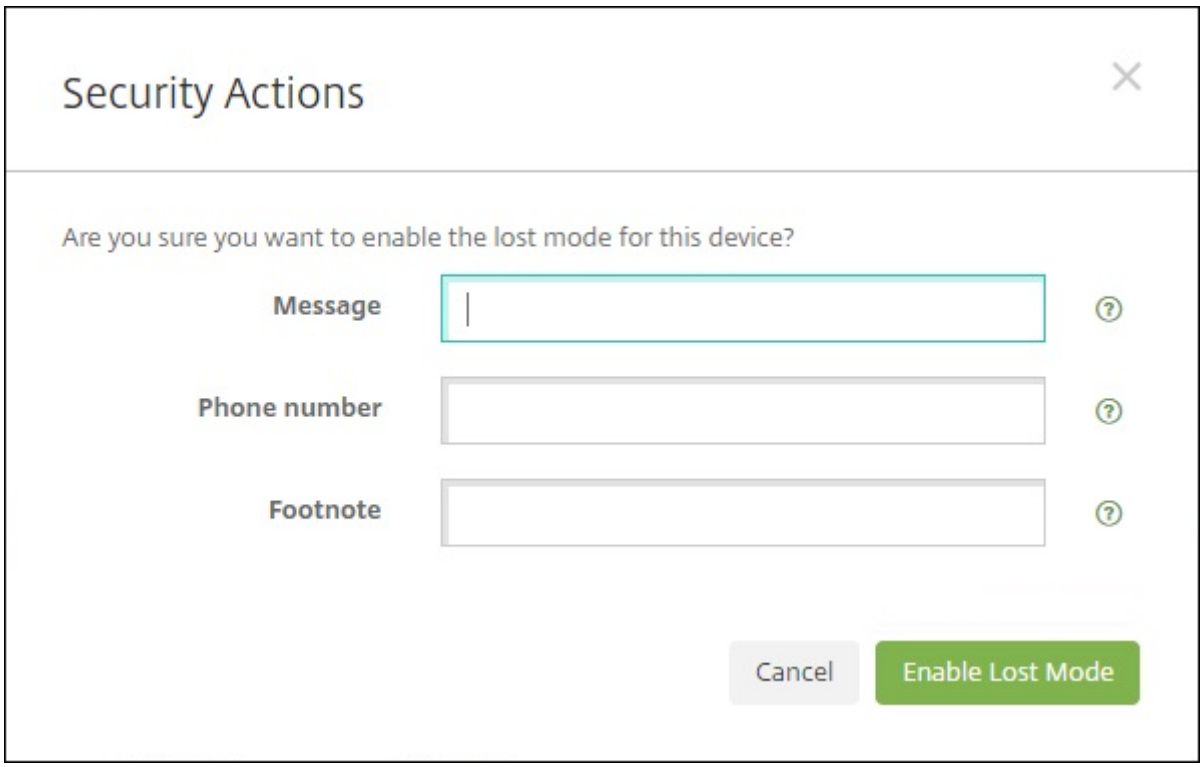
La propiedad de dispositivo “modo perdido” de XenMobile coloca un dispositivo iOS en el modo Perdido (de Apple). A diferencia del modo Perdido gestionado de Apple, el modo perdido de XenMobile no requiere que el usuario configure **Buscar mi iPhone o iPad** ni habilite los servicios de localización geográfica de Citrix Secure Hub para permitir la localización de su dispositivo.

En el modo perdido de XenMobile, solo XenMobile Server puede desbloquear el dispositivo. (En cambio, si usa la función de bloqueo del dispositivo de XenMobile, los usuarios pueden desbloquear el dispositivo directamente con un código PIN que proporcione.)

Para habilitar o inhabilitar el modo perdido, vaya a **Administrar > Dispositivos**, elija un dispositivo iOS supervisado y haga clic en **Proteger**. A continuación, haga clic en **Habilitar modo perdido** o **Inhabilitar modo perdido**.

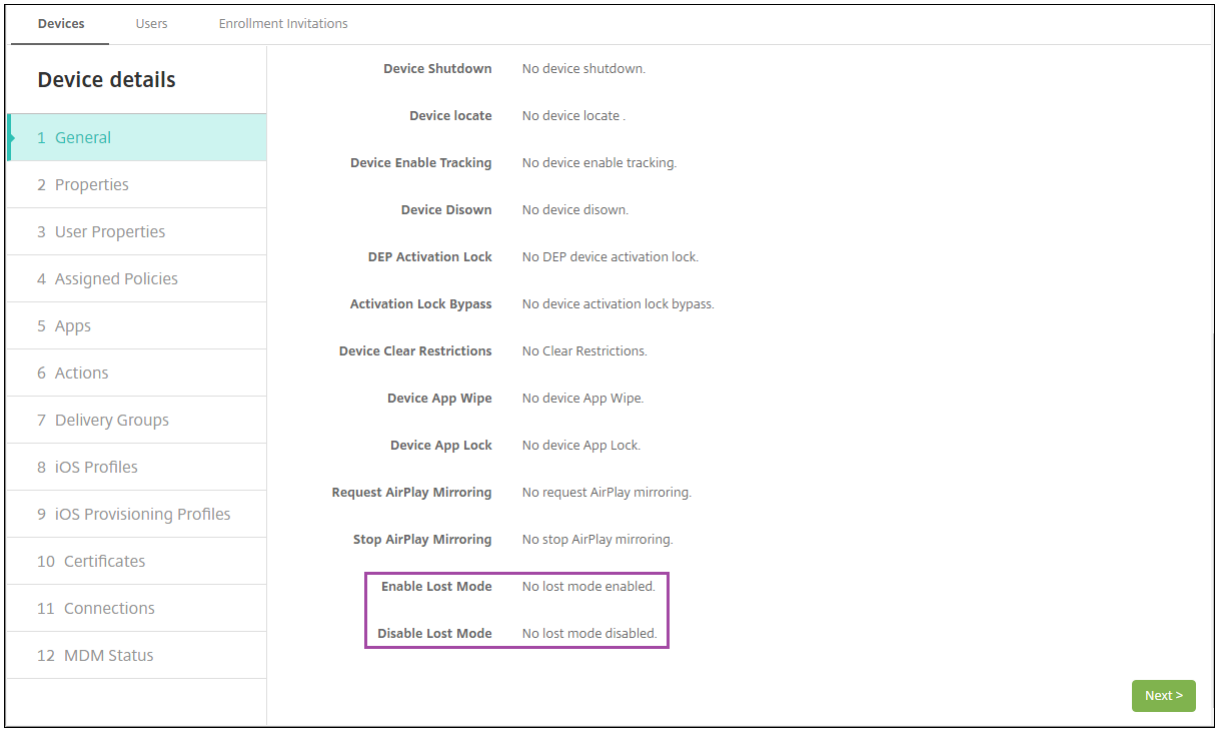


Si hace clic en **Habilitar modo perdido**, escriba la información que aparecerá en el dispositivo cuando esté en el modo perdido.

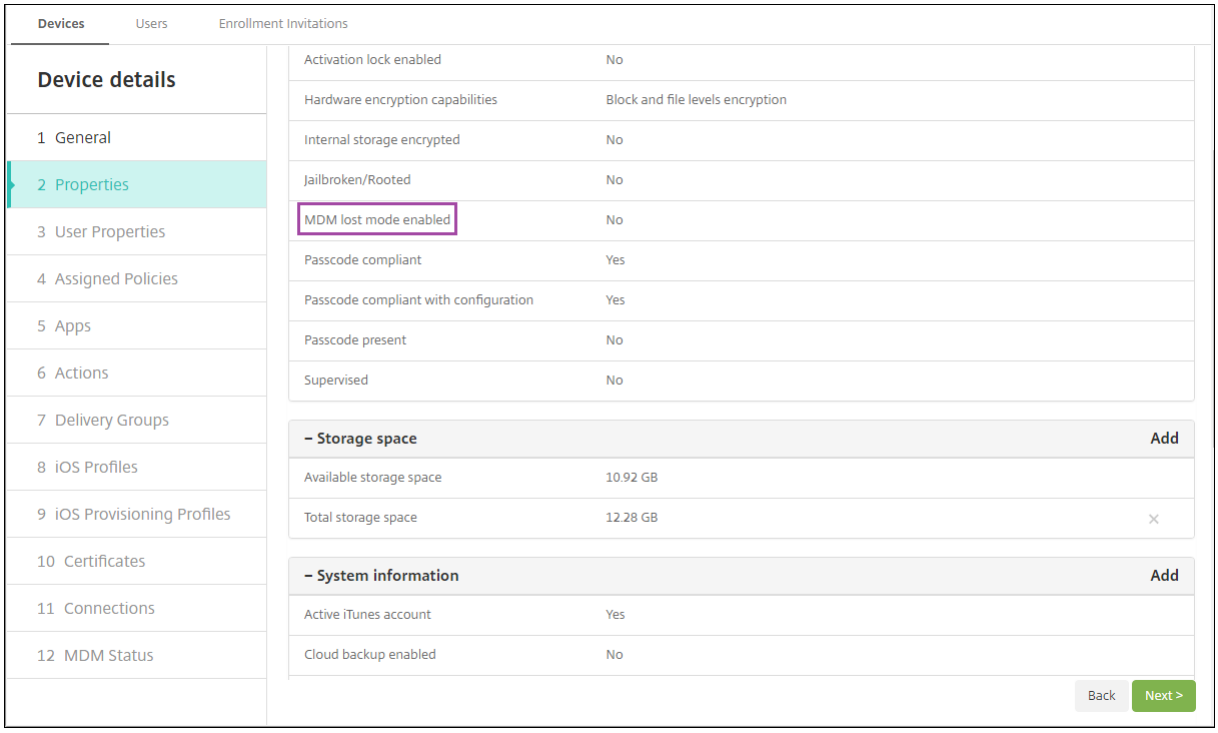


Para comprobar el estado del modo perdido, utilice cualquiera de los siguientes métodos:

- En la ventana **Acciones de seguridad**, compruebe si el botón es **Inhabilitar modo perdido**.
- Desde **Administrar > Dispositivos**, en la ficha **General**, en **Seguridad**, consulte la última acción de “Habilitar modo perdido” o “Inhabilitar modo perdido”.



- Desde **Administrar > Dispositivos**, en la ficha **Propiedades**, compruebe que el valor del parámetro **Modo perdido de MDM habilitado** es correcto.



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

- En **Configurar > Acciones**, la lista **Acciones** no incluye las siguientes acciones automatizadas: **Revocar el dispositivo**, **Borrar datos selectivamente del dispositivo** ni **Borrar datos completamente del dispositivo**.
- En **Administrar > Dispositivos**, la lista **Acciones de seguridad** ya no incluye las acciones de dispositivo **Revocar** ni **Borrado selectivo**. En cambio, puede llevar a cabo un **Borrado completo**, si fuera necesario.

En caso de iPads con iOS 7 y versiones posteriores, iOS añade las palabras “iPad perdido” a lo que escriba en el campo **Mensaje** de la pantalla **Acciones de seguridad**.

En caso de iPhones con 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.

Omitir un bloqueo de activación de iOS

El bloqueo de activación es una función de Buscar mi iPhone o iPad que evita la reactivación de un dispositivo supervisado que se haya perdido o haya sido robado. El bloqueo de activación requiere el ID de Apple del usuario y la contraseña para poder inhabilitar Buscar mi iPhone o iPad, borrar el

dispositivo o volver a activarlo. Para los dispositivos propiedad de la organización, es necesario omitir un bloqueo de activación para, por ejemplo, restablecer o reasignar dispositivos.

Para habilitar el bloqueo de activación, debe configurar e implementar la directiva de opciones MDM de XenMobile. A continuación, puede administrar un dispositivo desde la consola de XenMobile sin las credenciales de Apple del usuario. Para omitir el requisito de credenciales de Apple en un bloqueo de activación, debe emitir la acción de seguridad "Omisión del bloqueo de activación" desde la consola de XenMobile.

Por ejemplo, si un usuario devuelve un teléfono perdido o si usted quiere configurar uno antes o después de un borrado completo, cuando el teléfono le solicite las credenciales de la cuenta de iTunes, puede omitir ese paso emitiendo la acción de seguridad "Omisión del bloqueo de activación" desde la consola de XenMobile.

Requisitos del dispositivo para la omisión del bloqueo de activación

- iOS 7.1 (versión mínima)
- Supervisado a través de Apple Configurator o Apple DEP
- Configurado con una cuenta de iCloud
- Buscar mi iPhone o iPad habilitado
- Inscrito en XenMobile
- La directiva de opciones de MDM, con el bloqueo de activación habilitado, implementada en los dispositivos

Para omitir un bloqueo de activación antes de emitir el borrado completo de un dispositivo:

1. Vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Proteger** y, a continuación, haga clic en **Omisión del bloqueo de activación**.
2. Borre los datos del dispositivo. La pantalla del bloqueo de activación no aparece durante la configuración del dispositivo.

Para omitir un bloqueo de activación después de emitir el borrado completo de un dispositivo:

1. Borre los datos del dispositivo o restablézcalo. La pantalla del bloqueo de activación aparece durante la configuración del dispositivo.
2. Vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Proteger** y, a continuación, haga clic en **Omisión del bloqueo de activación**.
3. Toque el botón Atrás del dispositivo. Aparecerá la pantalla de inicio.

Tenga en cuenta lo siguiente:

- Recomiende a los usuarios que no inhabiliten Buscar mi iPhone o iPad. No realice ningún borrado completo desde el dispositivo. En cualquiera de estos casos, se pide al usuario que escriba la contraseña de la cuenta de iCloud. Tras validar la cuenta, el usuario no verá la pantalla "Activar iPhone o iPad" después de borrar todo el contenido y toda la configuración.

- Para un dispositivo con un código de omisión del bloqueo de activación generado y con el bloqueo de activación habilitado: si no puede omitir la página “Activar iPhone o iPad” después de un borrado completo, no es necesario eliminar el dispositivo de XenMobile. Usted o el usuario pueden ponerse en contacto con la asistencia técnica de Apple para desbloquear el dispositivo directamente.
- Durante un inventario de hardware, XenMobile busca en el dispositivo un código de omisión del bloqueo de activación. Si hay disponible un código de omisión, el dispositivo lo envía a XenMobile. A continuación, para quitar ese código de omisión del dispositivo, envíe la acción de seguridad “Omisión del bloqueo de activación” desde la consola de XenMobile. En ese momento, XenMobile Server y Apple tienen el código de omisión requerido para desbloquear el dispositivo.
- La acción de seguridad “Omisión del bloqueo de activación” necesita la disponibilidad de un servicio de Apple. Si la acción no funciona, puede desbloquear un dispositivo como se indica a continuación. En el dispositivo, debe introducir manualmente las credenciales de la cuenta iCloud. O bien deje en blanco el campo del nombre de usuario y escriba el código de omisión en el campo de la contraseña. Para buscar el código de omisión, vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Modificar** > **Propiedades**. El **Código de omisión del bloqueo de activación** se encuentra en el apartado **Información de seguridad**.

Dispositivos compartidos

January 4, 2022

XenMobile permite configurar dispositivos que se puedan compartir entre varios usuarios. La función de dispositivos compartidos permite, por ejemplo, que los médicos, en los hospitales, usen cualquier dispositivo cercano para acceder a las aplicaciones y a los datos, en lugar de tener que llevar encima un dispositivo concreto. También puede interesarle intercambiar dispositivos en ámbitos judiciales, comerciales y de fabricación para compartir los dispositivos entre sí y, de esta manera, reducir costes de equipamiento.

Puntos clave sobre dispositivos compartidos

Puede usar cualquiera de los dispositivos iOS y Android compatibles en calidad de dispositivos compartidos. Para obtener una lista de las plataformas compatibles, consulte Sistemas operativos compatibles.

Inscripción MDM

- Disponible en teléfonos y tabletas iOS y Android. No se admite la inscripción básica del Programa de implementación de Apple para dispositivos compartidos de XenMobile Enterprise. Debe utilizar un Programa de implementación de Apple autorizado 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.

Inscripción en MDM+MAM

- Disponible solo en dispositivos iOS y Android.
- Solo se admite la autenticación de nombre de usuario y contraseña de Active Directory.
- No se admiten la autenticación de certificados de cliente, el código de acceso de Secure Hub, Touch ID, la entropía de usuario ni la autenticación de dos factores.
- No se admite la inscripción solo en MAM- Los dispositivos deben inscribirse en MDM.
- Solo se admiten Secure Mail, Secure Web y las aplicaciones móviles de ShareFile. No se admiten las aplicaciones HDX.
- Solo se admiten usuarios de Active Directory. No se admiten usuarios ni grupos locales.
- Para actualizar al modo MDM+MAM, es necesario reinscribir los dispositivos compartidos existentes que están en modo solo MDM.
- Los usuarios no pueden compartir las aplicaciones nativas presentes en los dispositivos.
- Una vez se han descargado durante la primera inscripción, las aplicaciones móviles de productividad no vuelven a descargarse cuando un usuario inicia sesión.
- En Android, para aislar los datos de cada usuario por motivos de seguridad, **active** la directiva **Disallow rooted devices** de la consola de XenMobile.

Requisitos previos para la inscripción de dispositivos compartidos

Antes de inscribir dispositivos compartidos, debe realizar lo siguiente:

- Cree un rol de usuario de inscripción de dispositivos compartidos. Consulte Configurar roles con RBAC.
- Cree un usuario de dispositivos compartidos. Consulte Para agregar, modificar, desbloquear o eliminar cuentas de usuarios locales.
- Cree un grupo de entrega que contenga las aplicaciones, las acciones y las directivas base que quiera que se apliquen al usuario de dispositivos compartidos. Consulte Implementar recursos.

Requisitos previos para la inscripción en MDM+MAM

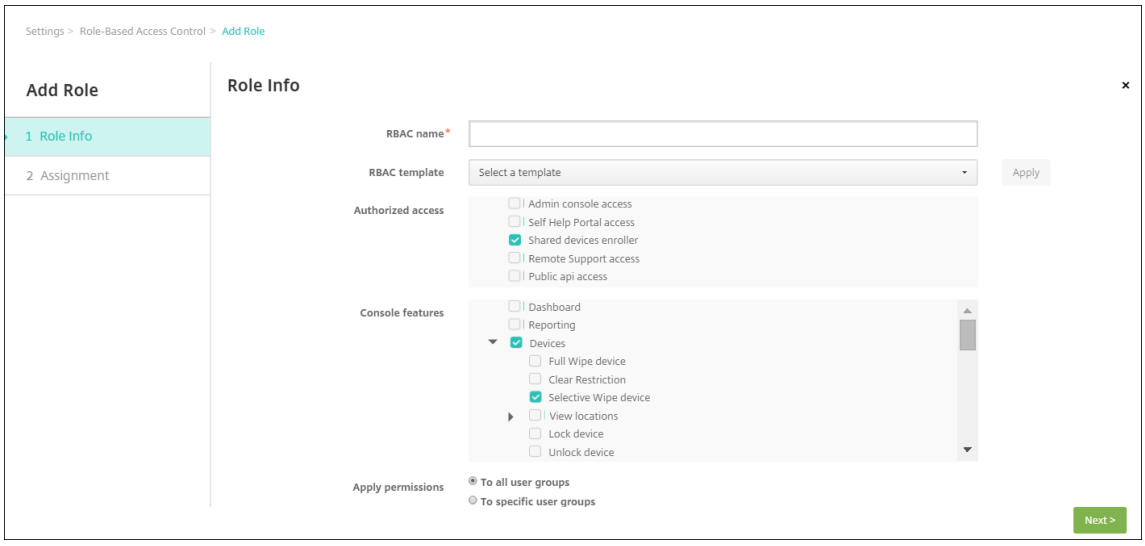
1. Cree un grupo de Active Directory. Asígnele un nombre descriptivo, como **Inscriptores de dispositivos compartidos**.
2. Agregue al grupo los usuarios de Active Directory que inscribirán dispositivos compartidos. Si quiere una nueva cuenta para este fin, cree un nuevo usuario de Active Directory (por ejemplo, **sdenroll**) y agréguelo al grupo de Active Directory.

Configurar un dispositivo compartido

Siga estos pasos para configurar un dispositivo compartido.

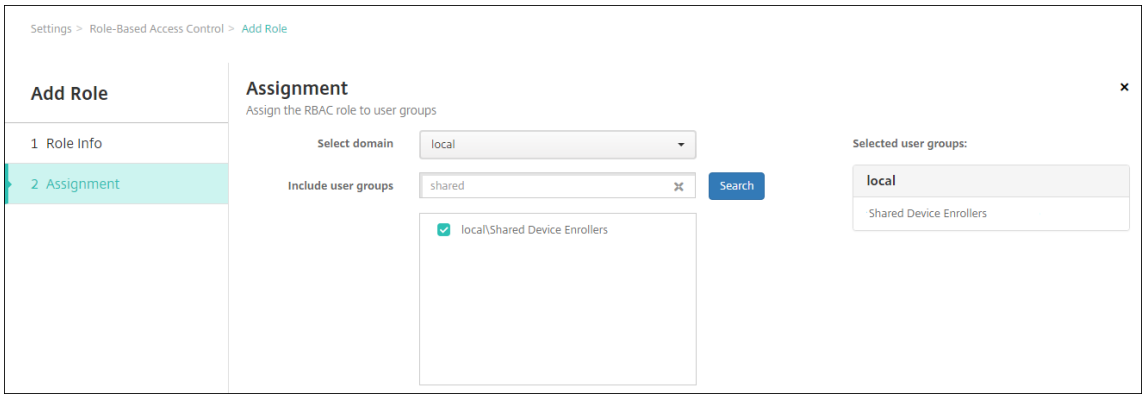
1. Desde la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Haga clic en **Control de acceso por roles** y, a continuación, haga clic en **Agregar**. Aparecerá la página **Agregar rol**.
3. Cree un rol de usuario de inscripción de dispositivo compartido denominado **usuario de inscripción de dispositivos compartidos** con permisos de **Inscripción de dispositivos compartidos** en **Acceso autorizado**. Expanda **Dispositivos**, en la sección **Funcionalidad de la consola** y, a continuación, seleccione **Borrado selectivo del dispositivo**. 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 desinscriba el dispositivo.

   En **Aplicar permisos**, puede conservar la configuración predeterminada **Para todos los grupos de usuarios**, o bien asignar permisos a grupos de usuarios de Active Directory específicos con **Para grupos de usuarios específicos**.

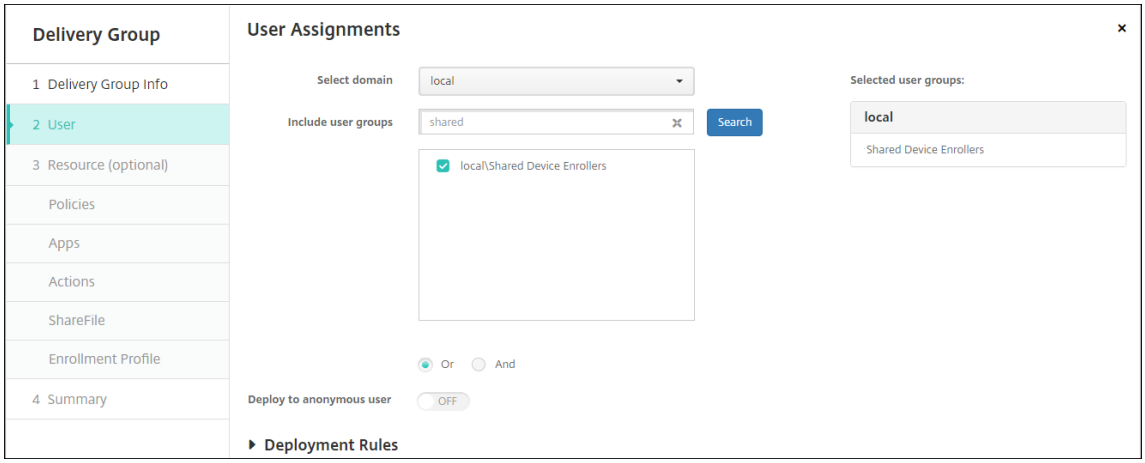


   Haga clic en **Siguiente** para pasar a la pantalla **Asignación**. Asigne el rol de inscripción de dispositivo compartido al grupo de Active Directory que se creó en el paso 1 de requisitos previos

para los usuarios de inscripción de dispositivos compartidos. En la siguiente imagen, **citrix.lab** es el dominio de Active Directory y **Shared Device Enrollers** es el grupo de Active Directory.



4. Cree un grupo de entrega que contenga las aplicaciones, las acciones y las directivas base que quiera que se apliquen al dispositivo cuando el usuario no esté conectado. A continuación, asocie ese grupo de entrega al grupo de usuarios de inscripción de dispositivos compartidos de Active Directory.



5. Instale Secure Hub en el dispositivo compartido e inscríbalo en XenMobile con la cuenta del usuario de inscripción de dispositivos compartidos. Ahora, puede ver y administrar el dispositivo a través de la consola XenMobile. Para obtener más información, consulte Inscribir dispositivos.
6. Si quiere aplicar directivas diferentes u ofrecer aplicaciones adicionales a los usuarios autenticados, cree un grupo de entrega asociado a esos usuarios e impleméntelo solo en los dispositivos compartidos. Al crear los grupos, configure reglas de implementación para que los paquetes se implementen en dispositivos compartidos. Para obtener más información, consulte Implementar recursos.
7. Si quiere dejar de compartir el dispositivo, realice un borrado selectivo para quitar la cuenta de usuario de inscripción de dispositivos compartidos que hubiera en el dispositivo. Quite las aplicaciones y las directivas implementadas en el dispositivo.

Experiencia de usuario en dispositivos compartidos

Inscripción MDM

Los usuarios solo ven los recursos disponibles para ellos, y obtienen la misma experiencia en cada dispositivo compartido. Las aplicaciones y las directivas de inscripción de dispositivos compartidos permanecen en el dispositivo. Cuando un usuario que no se ha inscrito en dispositivos compartidos inicia sesión en Secure Hub, las aplicaciones y las directivas de esa persona se implementan en el dispositivo. Cuando dicho usuario cierra la sesión, se quitan todas las directivas y aplicaciones que no forman parte de las de la inscripción de dispositivos compartidos. Los recursos de inscripción de dispositivos compartidos permanecen intactos.

Inscripción en MDM+MAM

Secure Mail y Secure Web se implementan en el dispositivo cuando el usuario de inscripción de dispositivos compartidos los inscribe. Los datos de usuario se conservan de forma segura en el dispositivo. Los datos no se expondrán a otros usuarios cuando estos usen Secure Mail o Secure Web.

Solo un usuario a la vez puede iniciar sesión en Secure Hub. El usuario anterior debe finalizar la sesión antes de que el siguiente pueda iniciarla. Por motivos de seguridad, Secure Hub no almacena credenciales de usuario en dispositivos compartidos, de modo que los usuarios deben introducir sus credenciales cada vez que inicien sesión. Secure Hub bloquea los nuevos inicios de sesión hasta que quita 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 el **período de sincronización máximo** según la cantidad de usuarios que compartirán el dispositivo. No se recomienda permitir una sincronización ilimitada.

Cantidad de usuarios que comparten el dispositivo	Período de sincronización máximo recomendado
De 21 a 25	1 semana o menos
De 6 a 20	2 semanas o menos
Hasta 5	1 mes o menos

- Bloquee **Enable contact export** para evitar exponer los contactos de un usuario a los demás

usuarios que comparten el dispositivo.

- En iOS, solo se pueden definir los parámetros siguientes para cada usuario. Todos los demás parámetros serán comunes a todos los usuarios que compartan el dispositivo:
  - Notificaciones
  - Firma
  - Fuera de la oficina
  - Período de sincronización de correo
  - S/MIME
  - Comprobar ortografía

XenMobile AutoDiscovery Service (ADS)

January 4, 2022

El servicio de detección automática simplifica el proceso de inscripción de los usuarios mediante detección de URL basada en direcciones de correo electrónico. El servicio de detección automática también proporciona funciones como verificación de inscripción, fijación de certificados y otras ventajas para los clientes de Citrix Workspace. El servicio, alojado en Citrix Cloud, es una parte importante de muchas implementaciones de XenMobile.

Con el servicio de detección automática, los usuarios:

- Pueden utilizar sus credenciales de red corporativa para inscribir sus dispositivos.
- No necesitan introducir detalles sobre la dirección de XenMobile Server.
- Introducen su nombre de usuario en formato de nombre principal de usuario (UPN). Por ejemplo, `user@mycompany.com`.

Se recomienda utilizar el servicio de detección automática para entornos de alta seguridad. El servicio de detección automática admite la fijación de certificados de clave pública, que impide ataques de intermediarios (ataques de tipo “Man in the middle”). La fijación de certificados garantiza que se utilice el certificado firmado por la empresa cuando los clientes de Citrix se comuniquen con XenMobile. Para configurar la fijación de certificados para los sitios de XenMobile, póngase en contacto con Citrix Support. Para obtener información sobre la fijación de certificados, consulte Fijación de certificados.

Para acceder al servicio de detección automática, vaya a https://adsui.cloud.com (acceso comercial) o https://adsui.cem.cloud.us (acceso gubernamental).

Requisitos previos

- El nuevo servicio de detección automática de Citrix Cloud requiere la versión más reciente de Secure Hub:

  - Para iOS, Secure Hub 21.6.0 o una versión posterior
  - Para Android, Secure Hub 21.8.5 o una versión posterior

    Es posible que los dispositivos con versiones anteriores de Secure Hub sufran interrupciones del servicio.

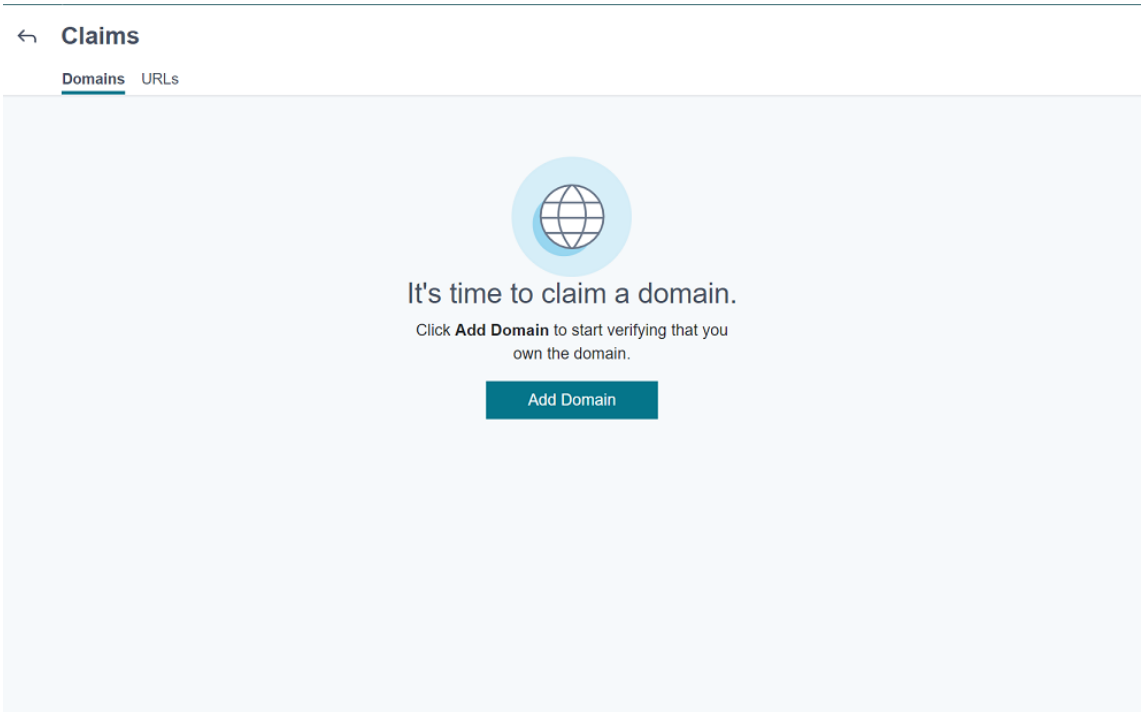
- Para acceder al nuevo servicio de detección automática, debe tener una cuenta de administrador de Citrix Cloud con acceso total. El servicio de detección automática no permite usar cuentas de administrador con acceso personalizado. Si no tiene cuenta, consulte Registrarse en Citrix Cloud.

  Citrix migró todos los registros existentes de la detección automática a Citrix Cloud sin interrumpir el servicio. Los registros migrados no aparecen automáticamente en la nueva consola. Debe recuperar los dominios en el nuevo servicio de detección automática para demostrar que le pertenecen. Para obtener más información, consulte CTX312339.

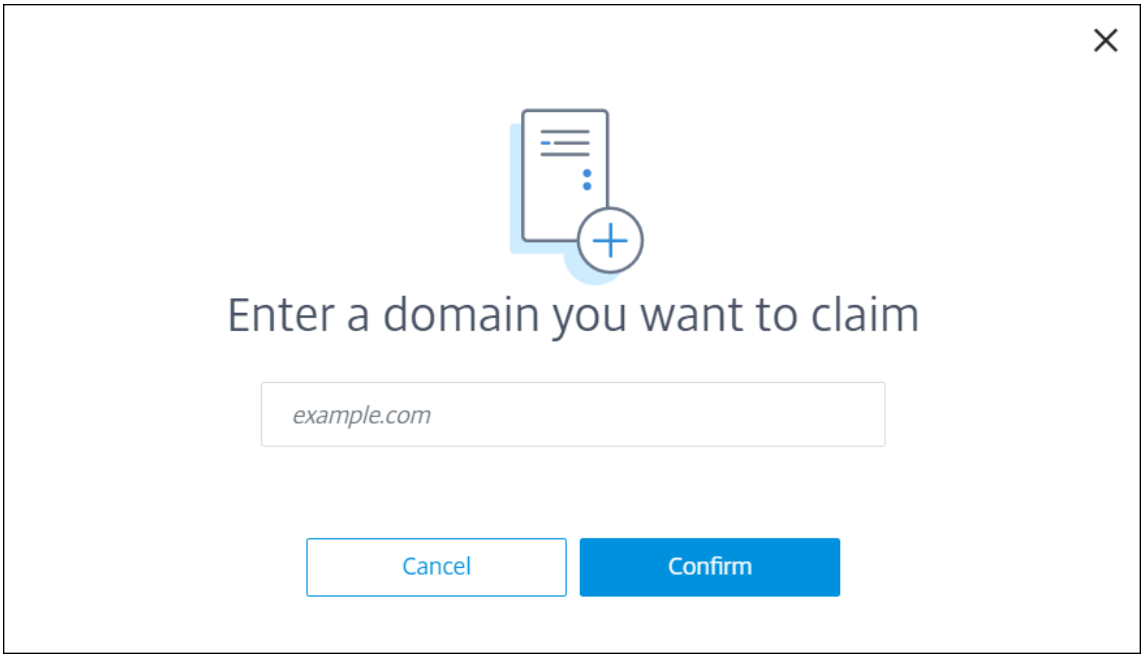
- Antes de empezar a usar el servicio de detección automática para las implementaciones de Endpoint Management, verifique y reclame su dominio. Puede reclamar hasta 10 dominios. La notificación asocia el dominio verificado al servicio de detección automática. Para reclamar más de 10 dominios, cree un tíquet de SRE o póngase en contacto con el servicio de asistencia técnica de Citrix.
- Utilice el parámetro Puerto MAM, en lugar de FQDN de Citrix Gateway, para dirigir el tráfico MAM al centro de datos. Si introduce un nombre de dominio completo (FQDN) junto con el puerto de Citrix Gateway, el dispositivo cliente utiliza la configuración del parámetro **Puerto MAM**.
- Si un bloqueador de anuncios impide que el sitio se abra, inhabilite el bloqueador de anuncios para todo el sitio web.

Reclamar un dominio

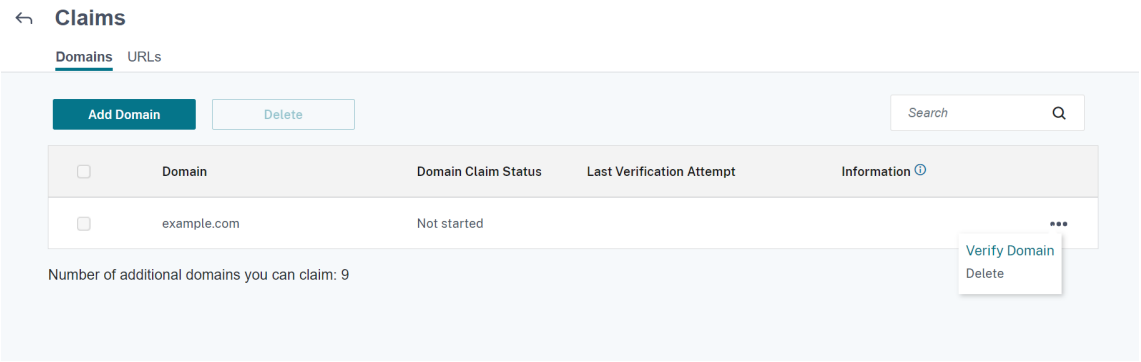
1. En la ficha **Notificaciones > Dominios**, haga clic en **Agregar dominio**.



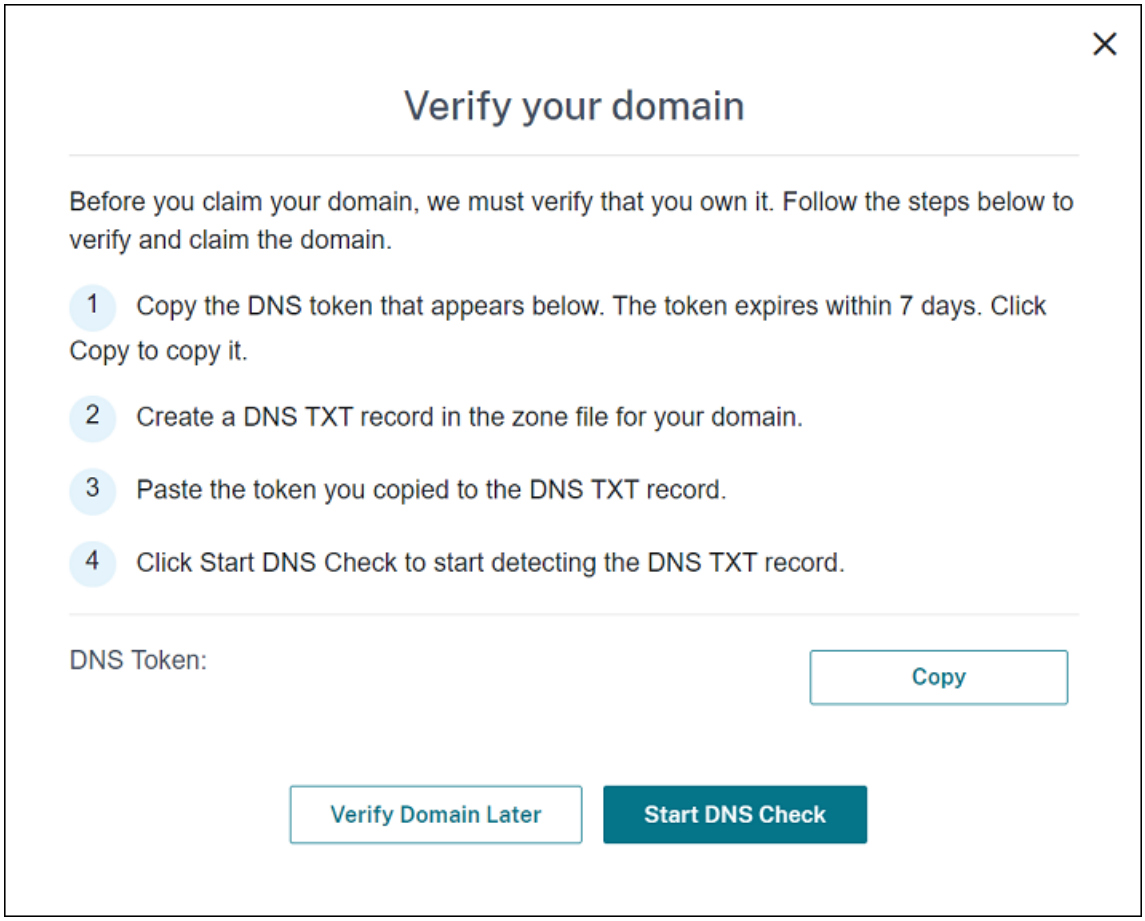
2. En el cuadro de diálogo que aparece, introduzca el nombre de dominio de su entorno de XenMobile y, a continuación, haga clic en **Confirmar**. Su dominio aparecerá en **Notificaciones > Dominios**.



3. En el dominio que agregó, haga clic en el menú de puntos suspensivos y seleccione **Verificar dominio** para iniciar el proceso de verificación. Aparecerá la página **Verificar el dominio**.



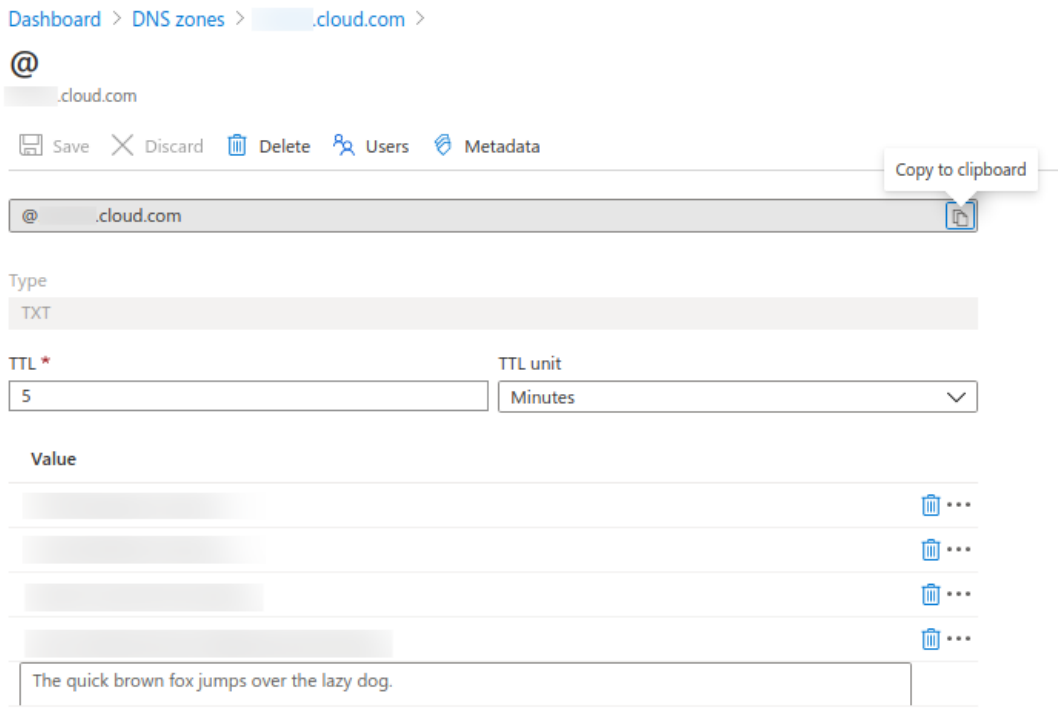
4. En la página **Verificar el dominio**, siga las instrucciones para comprobar que es propietario del dominio.



   a) Haga clic en **Copiar** para copiar el token de DNS en el portapapeles.

   b) Cree un registro TXT de DNS en el archivo de zona de su dominio. Para ello, vaya al portal del proveedor que aloja su dominio y agregue el token de DNS que copió.

      En la siguiente captura de pantalla, se muestra un portal de proveedor de alojamiento de dominios. Su portal puede tener un aspecto diferente.



c) En Citrix Cloud, en la página **Verificar el dominio**, haga clic en **Iniciar comprobación de DNS** para iniciar la detección de su registro TXT de DNS. Si quiere verificar el dominio más adelante, haga clic en **Verificar dominio más tarde**.

El proceso de verificación tarda, por lo general, aproximadamente una hora. Sin embargo, puede tardar hasta dos días en dar una respuesta. Puede cerrar sesión e iniciar sesión de nuevo durante la comprobación de estado.

Una vez completada la configuración, el estado del dominio cambia de **Pendiente** a **Verificado**.

5. Después de reclamar su dominio, introduzca la información sobre el servicio de detección automática. Haga clic en el menú de puntos suspensivos del dominio que agregó y, a continuación, en la opción para **agregar información de Endpoint Management**. Aparecerá la página **Información sobre el servicio de detección automática**.
6. Introduzca la información siguiente y, a continuación, haga clic en **Guardar**.
   - **FQDN del servidor de Endpoint Management:** Introduzca el nombre de dominio completo del servidor de XenMobile Server. Por ejemplo: `example.xm.cloud.com`. Este parámetro se utiliza para el tráfico de control de MDM y MAM.
   - **FQDN de Citrix Gateway:** Introduzca el nombre de dominio completo de Citrix Gateway, con el formato FQDN o FQDN:puerto. Por ejemplo: `example.com`. Esta configuración se utiliza para dirigir el tráfico MAM al centro de datos. Para implementaciones de solo MDM, deje este campo en blanco.

> **Nota:**
>
> Citrix recomienda utilizar el parámetro **Puerto MAM**, en lugar de **FQDN de Citrix Gateway**, para controlar el tráfico MAM. Si introduce un nombre de dominio completo (FQDN) junto con el puerto de Citrix Gateway, el dispositivo cliente utiliza la configuración del parámetro **Puerto MAM**.

- **Nombre de la instancia:** Introduzca el nombre de la instancia de XenMobile Server configurado anteriormente. Si no está seguro del nombre de instancia, deje el valor predeterminado, **zdm**.
- **Puerto MDM:** Introduzca el puerto utilizado para el tráfico de control de MDM y la inscripción MDM. Para los servicios basados en la nube, el valor predeterminado es 443.
- **Puerto MAM:** Introduzca el puerto utilizado para el tráfico de control de MAM, la inscripción MAM, la inscripción iOS y la enumeración de aplicaciones. Para los servicios basados en la nube, el valor predeterminado es 8443.

Solicitar detección automática para dispositivos Windows

Para inscribir dispositivos Windows, lleve a cabo lo siguiente:

1. Póngase en contacto con Citrix Support y cree una solicitud de asistencia para habilitar la detección automática de Windows.
2. Obtenga un certificado SSL sin comodín firmado públicamente para `enterpriseenrollment.mycompany.com`. La parte `mycompany.com` es el dominio que contiene las cuentas que los usuarios utilizan para inscribirse. Adjunte el certificado SSL en formato .pfx y su contraseña a la solicitud de asistencia creada en el paso anterior.

   Para utilizar más de un dominio para inscribir dispositivos Windows, también puede utilizar un multidominio con 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).
3. Cree un registro de nombre canónico (CNAME) en el servidor DNS y asigne la dirección del certificado SSL (enterpriseenrollment.mycompany.com) a autodisc.xm.cloud.com.

   Cuando un usuario de un dispositivo Windows se inscribe con un UPN, el servidor de inscripción de Citrix:

   - Proporciona los detalles del servidor de XenMobile Server.

- Indica al dispositivo que solicite un certificado válido de XenMobile.

A partir de ahora, puede inscribir todos los dispositivos compatibles. Continúe a la siguiente sección si quiere prepararse para la entrega de recursos a los dispositivos.

Directivas de dispositivo

January 4, 2022

Puede configurar la interacción entre XenMobile y los dispositivos mediante directivas. Aunque muchas directivas sean las mismas para todos los dispositivos, cada dispositivo tiene un conjunto específico de directivas para su sistema operativo. En consecuencia, se pueden encontrar muchas diferencias entre plataformas e incluso entre dispositivos Android de diferentes fabricantes.

Para una descripción resumida de cada directiva de dispositivo, consulte Directivas de dispositivo resumidas en este artículo.

> **Nota:**
>
> Si el entorno está configurado con objetos de directiva de grupo (GPO):
>
> Al configurar directivas de dispositivo de XenMobile para dispositivos con Windows 10 y Windows 11, tenga en cuenta esta regla. Si una directiva que esté presente en uno o varios dispositivos inscritos entra en conflicto, tiene prioridad la directiva que concuerde con el GPO.

Para ver las directivas que admite el contenedor de Android Enterprise, consulte Android Enterprise.

Requisitos previos

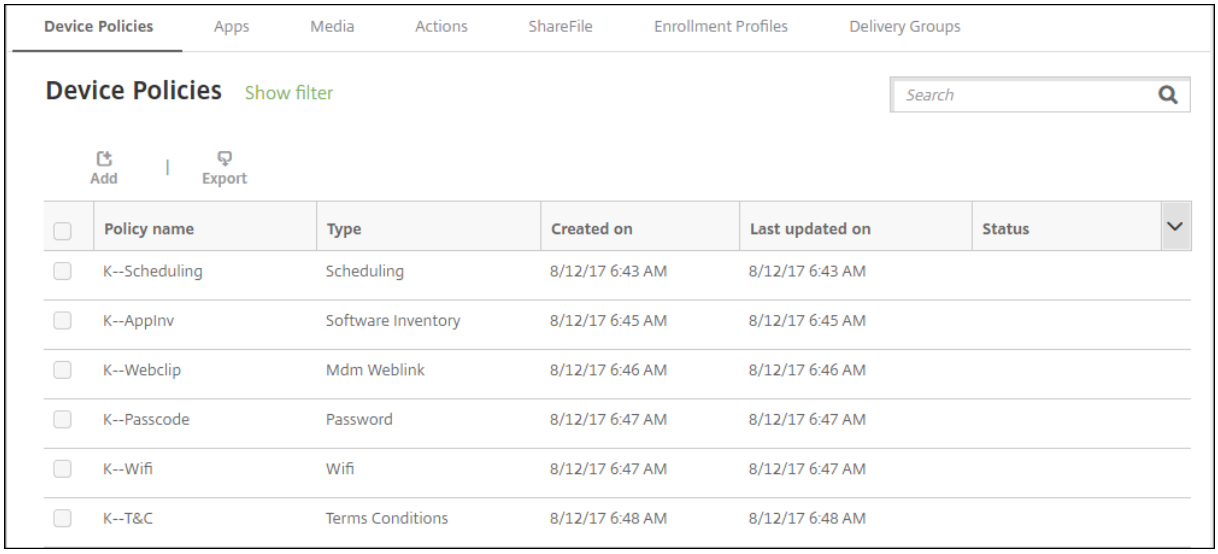
- Crear los grupos de entrega que se van a utilizar.
- Instalar los certificados de CA necesarios.

Agregar una directiva de dispositivo

A continuación, se presentan los pasos básicos necesarios para crear una directiva de dispositivo:

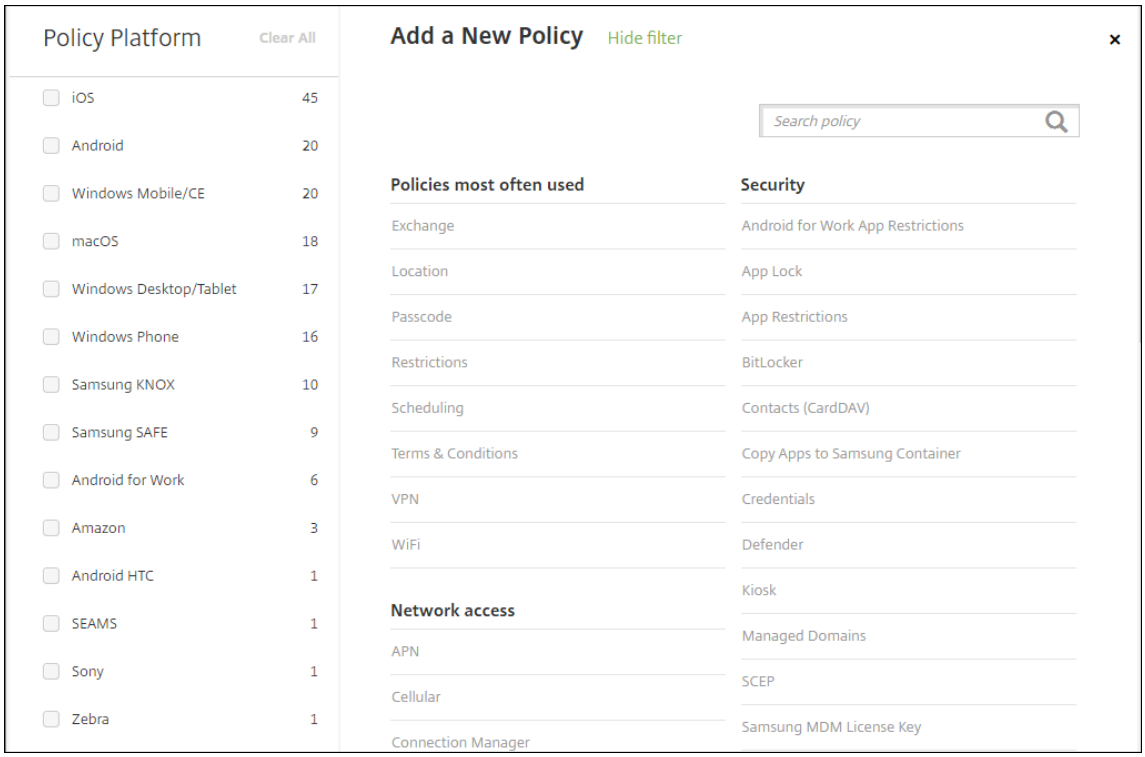
1. Especificar el nombre y la descripción de la directiva.
2. Configurar la directiva para una o varias plataformas.
3. Crear las reglas de implementación (opcional).
4. Asignar la directiva a grupos de entrega.
5. Configurar la programación de las implementaciones (opcional).

Para crear y administrar directivas de dispositivo, vaya a **Configurar > Directivas de dispositivo**.

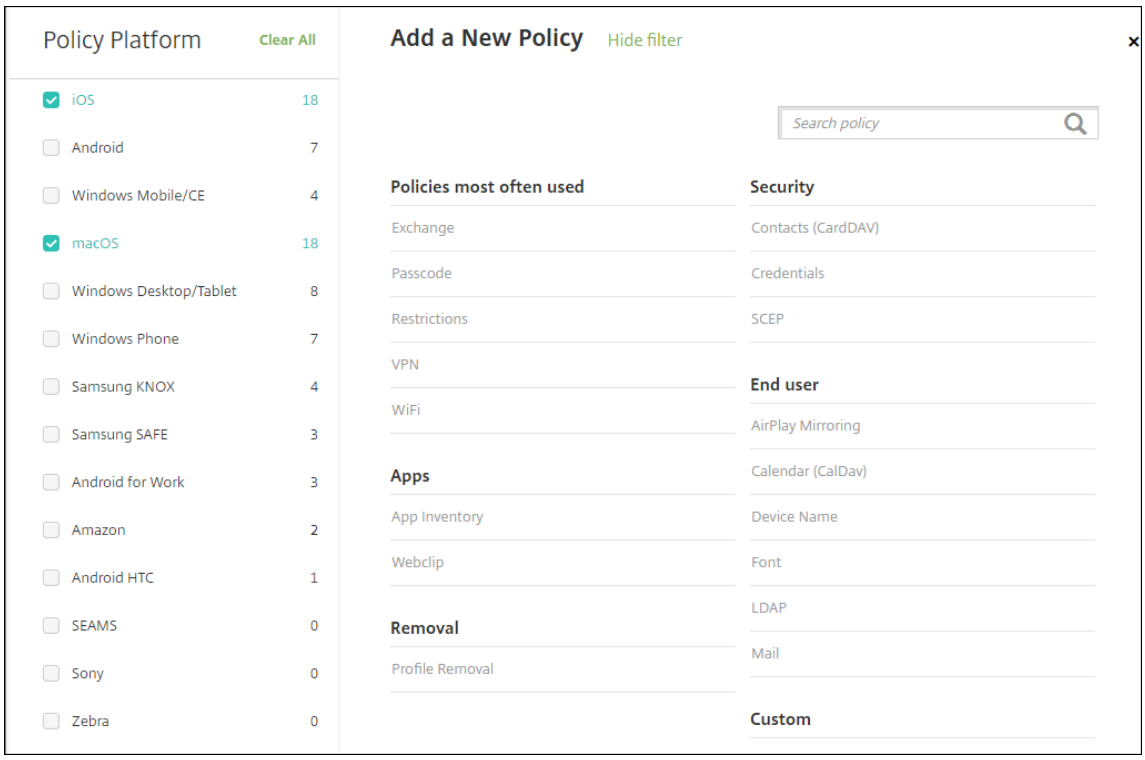


Para agregar una directiva:

1. En la página **Directivas de dispositivo**, haga clic en **Agregar**. Aparecerá la página **Agregar nueva directiva**.



2. Haga clic en una o varias plataformas para ver una lista de las directivas de dispositivo para las plataformas seleccionadas. Haga clic en el nombre de la directiva para continuar y agregar la directiva.



También puede escribir el nombre de la directiva en el cuadro de búsqueda. Cuando escriba, aparecerán posibles coincidencias. Si la directiva está en la lista, haga clic en ella. Solo permanecerá en los resultados la directiva que seleccione. Haga clic en la directiva para abrir la página **Información de directiva** referente a ella.

3. Seleccione las plataformas a incluir en la directiva. Las páginas de configuración referentes a las plataformas seleccionadas aparecerán en el paso 5.
4. Complete los datos de la página **Información de directiva** y haga clic en **Siguiente**. La página **Información de directiva** recopila información (como el nombre de la directiva) para ayudarle a identificar sus directivas y realizar un seguimiento de ellas. Esta página es similar para todas las directivas.
5. Complete las páginas de plataformas. Aparecerán páginas de cada plataforma que haya seleccionado en el paso 3. Estas páginas son distintas para cada directiva. Una directiva puede ser diferente en función de las plataformas. No todas las directivas se aplican a todas las plataformas.

   Algunas páginas contienen tablas de elementos. 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. En el cuadro de diálogo de confirmación, haga clic en **Eliminar**.

   Para modificar un elemento existente, coloque el cursor sobre la línea que lo contiene y haga clic en el icono de lápiz situado a la derecha.

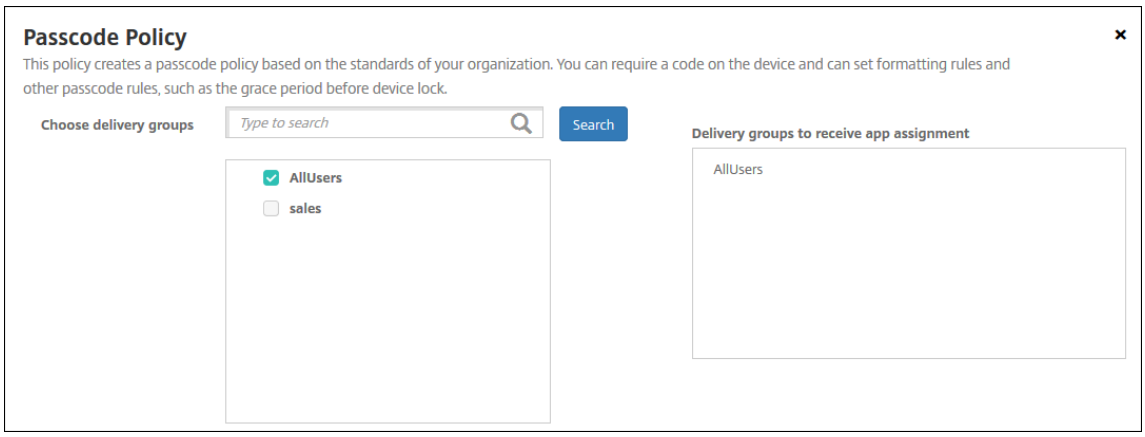
Para configurar reglas de implementación, asignaciones y programación

Para obtener más información sobre cómo configurar las reglas de implementación, consulte Implementación de recursos.

1. En la página de una plataforma, expanda **Reglas de implementación** y, a continuación, configure los siguientes parámetros. La ficha **Base** aparece de forma predeterminada.
   - En las listas, haga clic en las diferentes opciones para determinar cuándo debe implementarse la directiva. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es **Todas**.
   - Haga clic en **Nueva regla** para definir las condiciones.
   - En las listas, haga clic en las condiciones (por ejemplo, **Propietario del dispositivo** y **BYOD**).
   - Si quiere agregar más condiciones, haga clic en **Nueva regla** de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha **Avanzado** para combinar las reglas con opciones booleanas. Las condiciones que haya elegido aparecerán en la ficha **Base**.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
   - Haga clic en **AND**, **OR** o **NOT**.
   - En la lista, seleccione las condiciones que quiere agregar a la regla. A continuación, haga clic en el signo más (**+**) situado en el lado derecho para agregar la condición a la regla.

     En cualquier momento, puede seleccionar una condición para modificarla o eliminarla si hace clic en **Modificar** o en **Eliminar** respectivamente.
   - Haga clic en **Nueva regla** para agregar otra condición.
4. Haga clic en **Siguiente** para ir a la página de la siguiente plataforma o, cuando haya completado todas las páginas de plataforma, para ir a la página **Asignaciones**.
5. En la página **Asignaciones**, 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 **Grupos de entrega a recibir asignaciones de aplicaciones**.

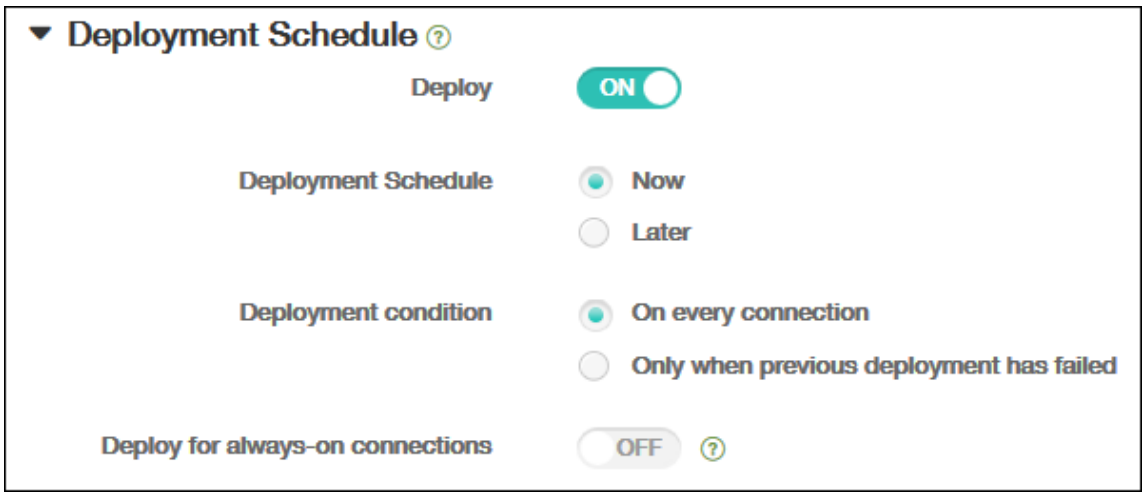
   El cuadro **Grupos de entrega a recibir asignaciones de aplicaciones** no aparecerá hasta que seleccione un grupo de entrega.



6. En la página **Asignaciones**, expanda **Programación de implementación** y, a continuación, configure los siguientes parámetros:

   - Junto a **Implementar**, haga clic en **Sí** para programar la implementación, o bien, haga clic en **No** para cancelarla. Está **activado** de forma predeterminada.
   - Junto a **Programación de implementación**, haga clic en **Ahora** o en **Más tarde**. La opción predeterminada es **Ahora**.
   - Si hace clic en **Más tarde**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
   - Junto a **Condición de implementación**, puede hacer clic en **En cada conexión** o en **Solo cuando haya fallado la implementación anterior**. La opción predeterminada es **En cada conexión**.
   - Junto a **Implementar para conexiones permanentes**, haga clic en **Sí** o **No**. Está **desactivado** de forma predeterminada.

     > **Nota:**
     >
     > Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Parámetros > Propiedades de servidor**. La opción "Implementar para conexiones permanentes" 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 **Implementar para conexiones permanentes**, que no se aplicará para iOS.



7. Haga clic en **Guardar**.

   La directiva aparecerá en la tabla **Directivas de dispositivo**.

Eliminar una directiva de un dispositivo

Los pasos para eliminar una directiva de dispositivo que hubiera en un dispositivo dependen de la plataforma.

- Android

  Para eliminar una directiva de un dispositivo Android, use la directiva Desinstalación de XenMobile. Para obtener más información, consulte Directiva de desinstalación de XenMobile.

- iOS y macOS

  Para eliminar una directiva de dispositivo que hubiera en un dispositivo iOS o macOS, use la directiva Eliminación de perfiles. En dispositivos iOS y macOS, todas las directivas forman parte del perfil MDM. Por lo tanto, puede crear una directiva Eliminación de perfiles solo para la directiva que quiere eliminar. El resto de las directivas y el perfil se conservan en el dispositivo. Para obtener más información, consulte Directiva de eliminación de perfiles.

- Windows 10 y Windows 11

  No puede quitar directamente una directiva de dispositivo que haya en un dispositivo de escritorio o tableta Windows. Sin embargo, puede utilizar cualquiera de los siguientes métodos:

  - Anule la inscripción del dispositivo y envíe un nuevo conjunto de directivas a este. Los usuarios deben volver a inscribirse para continuar.
  - Envíe una acción de seguridad para borrar selectivamente el dispositivo específico. Esta acción elimina todos los datos de empresa y todas las aplicaciones empresariales que hubiera en el dispositivo. A continuación, elimine la directiva de dispositivo que hubiera en

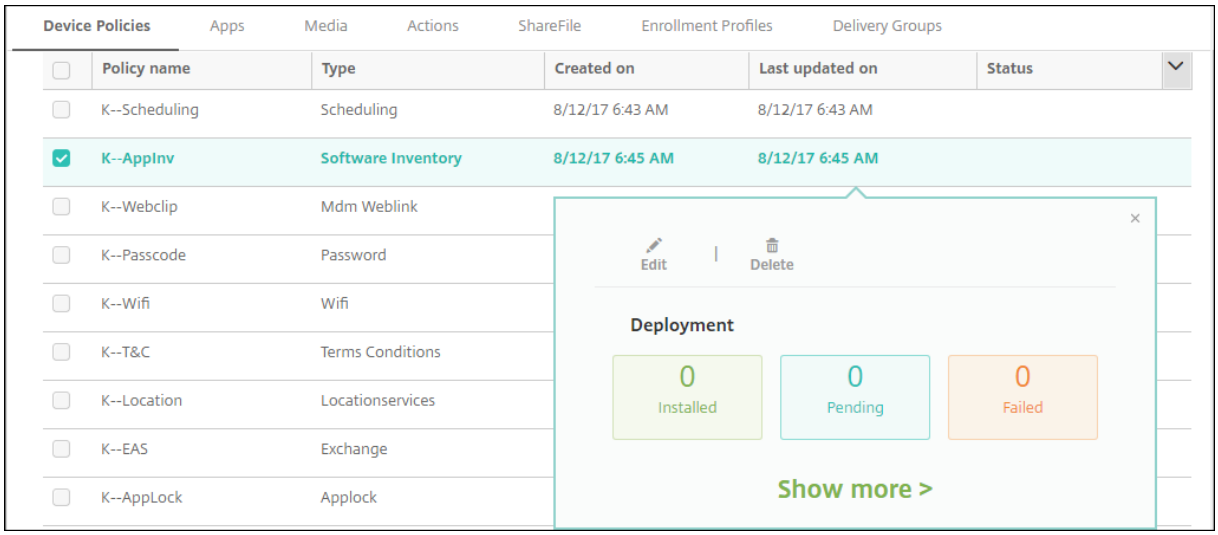
el grupo de entrega que contiene solo ese dispositivo y envíe el grupo de entrega al dispositivo. Los usuarios deben volver a inscribirse para continuar.

- Chrome OS

  Para eliminar una directiva de dispositivo que hubiera en un dispositivo Chrome OS, puede eliminar la directiva de un grupo de entrega que contenga solo ese dispositivo. A continuación, envíe el grupo de entrega al dispositivo.

Modificar una directiva de dispositivo

Para modificar una directiva de dispositivo, marque la casilla ubicada junto a una directiva para que el menú de opciones aparezca sobre la lista de directivas. O bien, haga clic en una directiva de la lista para que el menú de opciones aparezca en el lado derecho de la lista.



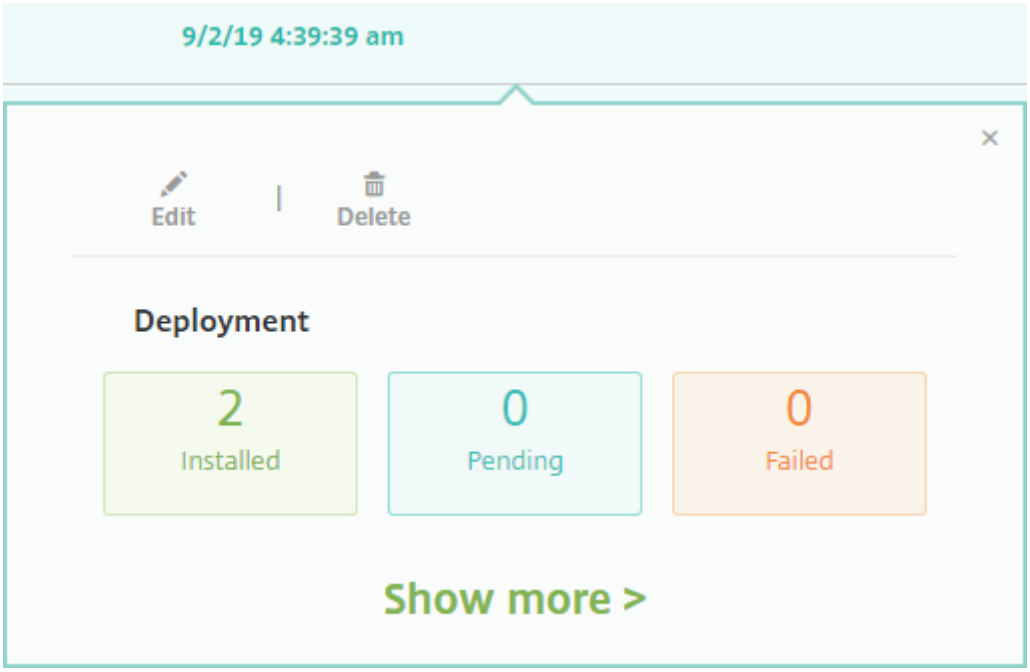
Para ver los detalles de la directiva, haga clic en **Mostrar más**.

Para modificar toda la configuración de una directiva de dispositivo, haga clic en **Modificar**.

Aparecerá un cuadro de diálogo de confirmación si hace clic en **Eliminar**. Haga clic en **Eliminar** de nuevo para eliminar la directiva.

Consultar el estado de implementación de directivas

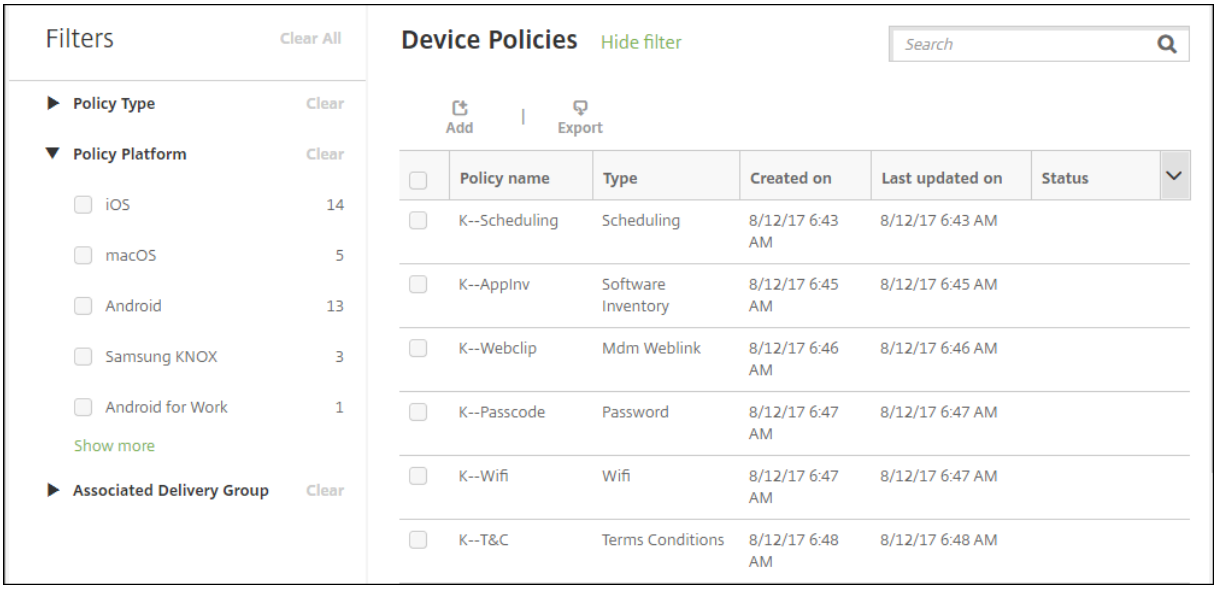
En la página **Configurar > Directivas de dispositivo**, haga clic en la fila de una directiva para consultar el estado de su implementación.



Cuando está pendiente la implementación de una directiva, los usuarios pueden actualizar la directiva desde Secure Hub. Para ello, deben tocar **Preferencias > Información del dispositivo > Actualizar directiva**.

Filtrar la lista de las directivas de dispositivo agregadas

Puede filtrar la lista de las directivas agregadas por tipos de directivas, plataformas y grupos de entrega asociados. En la página **Configurar > Directivas de dispositivo**, haga clic en **Mostrar filtro**. En la lista, marque las casillas de los elementos que quiere ver.



Haga clic en **GUARDAR ESTA VISTA** para guardar un filtro. Entonces, el nombre del filtro aparecerá en el botón situado debajo del botón **GUARDAR ESTA VISTA**.

Directivas de dispositivo resumidas

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Duplicación AirPlay	Agrega dispositivos AirPlay específicos (tales como otro equipo Mac) a dispositivos iOS. También tiene la opción de agregar dispositivos a una lista de dispositivos supervisados permitidos. Esa opción limitará a los usuarios a solamente dispositivos AirPlay en la lista de permitidos.
AirPrint	Agrega impresoras AirPrint a la lista de impresoras AirPrint que aparece en los dispositivos iOS. Esta directiva facilita los entornos en los que las impresoras y los dispositivos están en subredes diferentes.
Permisos de aplicación de Android Enterprise	Configura cómo gestionan las solicitudes a aplicaciones Android Enterprise incluidas en los perfiles de trabajo lo que Google considera permisos “peligrosos”.
Restricciones de aplicación de Android Enterprise	Actualiza las restricciones asociadas a aplicaciones Android.
APN	Determina los parámetros utilizados para conectar sus dispositivos al servicio GPRS (General Packet Radio Service) de un operador de teléfonos concreto. Esta configuración ya está definida en la mayoría de los teléfonos recientes. Use esta directiva si su organización no usa un APN de consumidor para conectarse a Internet desde un dispositivo móvil.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Acceso a aplicaciones	Define una lista de las aplicaciones que son obligatorias, opcionales o prohibidas 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	Especifica atributos (por ejemplo, un ID de paquete de aplicación administrada o un identificador de red VPN por aplicación) para dispositivos iOS.
Configuración de aplicaciones	Permite configurar de forma remota varias opciones y comportamientos de las aplicaciones que admiten la configuración administrada. Para ello, debe implementar un archivo de configuración XML (llamado lista de propiedades o plist) en dispositivos iOS. También puede implementar pares de clave/valor en teléfonos con Windows 10 o en tabletas o equipos de escritorio con Windows 10 o Windows 11.
Inventario de aplicaciones	Permite realizar un inventario de las aplicaciones presentes en los dispositivos administrados. Una vez realizado, XenMobile compara el inventario con las directivas de acceso a aplicaciones que se hayan implementado en esos dispositivos. De esta forma, puede detectar aplicaciones que se encuentren en una lista de permitidos o en una lista de bloqueados (para acceder a ellas o no) y actuar en consecuencia.
Bloqueo de aplicaciones	Permite definir una lista de las aplicaciones que los usuarios pueden ejecutar o no en dispositivos iOS o en determinados dispositivos Android.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Uso de red de las aplicaciones	Permite definir reglas de uso de la red para especificar la forma en que las aplicaciones administradas deben usar, por ejemplo, redes de datos móviles en dispositivos iOS. Las reglas solo se aplican a aplicaciones administradas. Las aplicaciones administradas son aquellas que se implementan en los dispositivos de los usuarios por medio de XenMobile.
Restricciones de aplicaciones	Permite crear listas de bloqueados para las aplicaciones que quiere impedir que los usuarios instalen en dispositivos Samsung Knox. También puede crear listas de permitidos para las aplicaciones que permite que los usuarios instalen.
Desinstalación de aplicaciones	Permite quitar aplicaciones de los dispositivos de usuario.
Restricciones de desinstalación de aplicaciones	Permite especificar las aplicaciones que los usuarios pueden o no pueden desinstalar.
Notificaciones de aplicaciones	Controla cómo reciben los usuarios de iOS las notificaciones provenientes de aplicaciones concretas.
Actualizar automáticamente aplicaciones administradas	Controla cómo se actualizan en dispositivos Android Enterprise las aplicaciones administradas instaladas.
BitLocker	Permite configurar los parámetros disponibles en la interfaz de BitLocker en dispositivos con Windows 10 o Windows 11.
Explorador web	Permite definir si los dispositivos de los usuarios pueden usar el explorador web o limitar las funciones de explorador web que se puedan usar.
Calendario (CalDav)	Permite agregar una cuenta de calendario (CalDAV) a dispositivos iOS o macOS. La cuenta de CalDAV permite a los usuarios sincronizar datos de programación con cualquier servidor compatible con CalDAV.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Móvil	Permite configurar las opciones de red móvil.
Administrador de conexiones	Permite especificar los parámetros de conexión para las aplicaciones que se conectan automáticamente a Internet y a redes privadas. Esta directiva solo está disponible para dispositivos Pocket PC de Windows.
Contactos (CardDAV)	Permite agregar una cuenta de contacto de iOS (CardDAV) a dispositivos iOS o macOS. La cuenta de CardDAV permite a los usuarios sincronizar datos de contacto con cualquier servidor compatible con CardDAV.
Controlar actualizaciones del SO	Permite implementar las actualizaciones más recientes del sistema operativo en los dispositivos admitidos y supervisados.
Copiar aplicaciones al contenedor de Samsung	Permite que las aplicaciones que ya están instaladas en un dispositivo se copien a un contenedor KNOX en dispositivos Samsung admitidos. Las aplicaciones que se copien al contenedor Knox solo estarán disponibles cuando los usuarios inicien sesión en dicho contenedor.
Credenciales	Permite la autenticación integrada con la configuración de PKI en XenMobile. Por ejemplo, con una entidad PKI, un almacén de claves, un proveedor de credenciales o un certificado de servidor.
XML personalizado	Permite personalizar funciones tales como el aprovisionamiento de dispositivos, la habilitación de las funciones de los dispositivos, la configuración de dispositivos y la administración de fallos.
Defender	Configura los parámetros de Windows Defender para tabletas y escritorios con Windows 10 o Windows 11.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Eliminar archivos y carpetas	Permite eliminar archivos específicos o carpetas concretas de los dispositivos Windows Mobile/CE.
Eliminar claves y valores del Registro	Permite eliminar, de los dispositivos Windows Mobile/CE, claves y valores específicos de Registro.
Device Health Attestation (Atestación del estado de dispositivos)	Requiere que los dispositivos con Windows 10 o Windows 11 informen de su estado. Para ello, deben enviar datos concretos e información del tiempo de ejecución al servicio Health Attestation Service (HAS) para el análisis. El servicio HAS crea y devuelve un certificado de atestación de estado que el dispositivo envía a XenMobile. Cuando XenMobile recibe el certificado de atestación de estado, según el contenido de este, puede implementar las acciones automatizadas que haya configurado.
Nombre del dispositivo	Permite definir los nombres de los dispositivos iOS y macOS de forma que pueda identificarlos. Puede usar macros, texto o una combinación de ambos para definir el nombre del dispositivo.
Configuración de la educación	Permite configurar los dispositivos de profesores y alumnos para que se usen con Educación de Apple. Si los profesores utilizan la aplicación Aula, se necesita la directiva de configuración de la educación.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Hub empresarial	Permite distribuir aplicaciones en dispositivos Windows Phone a través del almacén central de la empresa. XenMobile solo admite una directiva Hub empresarial por modo de Windows Phone Secure Hub. Por ejemplo, no debe crear varias directivas Hub empresarial con versiones diferentes de Secure Home para XenMobile Enterprise Edition. Solo puede implementar la directiva de hub empresarial inicial durante la inscripción del dispositivo.
Exchange	Permite habilitar el correo electrónico de ActiveSync para el cliente de correo electrónico nativo en el dispositivo.
Archivos	Permite agregar, a XenMobile, scripts que realizan determinadas funciones para los usuarios. También puede agregar archivos de documento a los que quiere que los usuarios de dispositivos Android tengan acceso en sus dispositivos. Al agregar el archivo, también puede especificar el directorio donde se almacenará el archivo en ese dispositivo.
FileVault	Esta directiva le permite habilitar el cifrado de dispositivos FileVault en los dispositivos macOS inscritos. También puede controlar cuántas veces puede omitir un usuario la configuración de FileVault durante el inicio de sesión. Disponible para macOS 10.7 o versiones posteriores.
Firewall	Permite configurar los parámetros de firewall. Puede proporcionar las direcciones IP, los puertos y los nombres de host a los que quiera permitir o bloquear el acceso de los dispositivos. También puede configurar el proxy y las opciones de redirección de este.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Fuente	Permite agregar fuentes a dispositivos iOS y macOS. Las fuentes deben tener el formato TrueType (TTF) u OpenType (OFT). XenMobile no admite colecciones de fuentes (.TTC o .OTC).
Diseño de pantalla inicial	Permite especificar la distribución de aplicaciones y carpetas en la pantalla de inicio de iOS en iOS 9.3 y versiones posteriores de los dispositivos supervisados.
Importar perfil de iOS y macOS	Permite importar, en XenMobile, archivos XML de configuración para dispositivos iOS y macOS. El archivo contiene las restricciones y las directivas seguridad de los dispositivos que se preparan con Apple Configurator.
Administración de Keyguard	Permite especificar las funciones disponibles para los usuarios antes de que desbloqueen el Keyguard del dispositivo y el Keyguard de Work Challenge. En el caso de dispositivos totalmente administrados y dedicados, también permite controlar funciones de Keyguard del dispositivo. Por ejemplo, es posible inhabilitar funciones de la pantalla de bloqueo, como desbloqueo mediante huella digital, agentes de confianza y notificaciones.
Quiosco	Permite restringir el uso de aplicaciones en dispositivos Samsung SAFE. Puede limitar las aplicaciones disponibles a una aplicación o aplicaciones específicas. Esta directiva es útil para los dispositivos de empresa diseñados para ejecutar solo un tipo o clase específicos de aplicaciones. Asimismo, esta directiva permite elegir imágenes personalizadas para la pantalla de inicio y fondos para la pantalla de bloqueo del dispositivo cuando está en modo quiosco.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Configuración de Launcher	Especifica la configuración de Citrix Launcher en dispositivos Android, como las aplicaciones permitidas y una imagen de logotipo personalizado para el icono de Launcher.
LDAP	En dispositivos iOS, esta directiva permite proporcionar información sobre el servidor LDAP a utilizar, incluida la información de cuenta necesaria (como el nombre de host del servidor LDAP). La directiva también ofrece un conjunto de directivas de búsquedas LDAP a usar cuando se consulta el servidor LDAP.
Ubicación	Permite ubicar geográficamente los dispositivos en un mapa, siempre que el dispositivo tenga habilitado GPS para Secure Hub. Después de implementar esta directiva en el dispositivo, puede enviar el comando "locate" desde XenMobile Server. El dispositivo responde con sus coordenadas de ubicación. XenMobile también admite directivas de geocerca y seguimiento geográfico.
Correo	Permite configurar una cuenta de correo electrónico en dispositivos iOS o macOS.
Dominios administrados	Permite definir los dominios administrados que se aplicarán al correo electrónico y al explorador web Safari. Los dominios administrados ayudan a proteger la información empresarial porque gestionan las aplicaciones que pueden abrir los documentos descargados desde dominios mediante Safari. Así, puede especificar las direcciones URL o los subdominios para controlar la forma en que los usuarios pueden abrir documentos, datos adjuntos y archivos descargados del explorador web en dispositivos supervisados iOS 8 y versiones posteriores.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Opciones de MDM	Permite administrar las funciones Bloqueo de activación y Buscar mi iPhone o iPad en teléfonos supervisados iOS 7.0 y versiones posteriores.
Información sobre la organización	Permite especificar la información de la organización para los mensajes de alertas que XenMobile implementa en los dispositivos iOS.
Código de acceso	Permite imponer un código de acceso (PIN o contraseña) en un dispositivo administrado. Además, puede definir la complejidad y el tiempo de espera del código de acceso en el dispositivo.
Hotspot personal	Permite a los usuarios conectarse a Internet cuando no tienen una red Wi-Fi al alcance. Los usuarios se conectan a través de una conexión de datos móviles en su dispositivo iOS con la funcionalidad de hotspot personal.
Eliminación de perfiles	Permite eliminar el perfil de aplicación que haya presente en los dispositivos iOS o macOS.
Perfil de datos	Permite indicar un perfil de datos de distribución empresarial que se envía a los dispositivos. Cuando desarrolla y firma el código de una aplicación iOS de empresa, generalmente incluye un perfil de datos. Apple requiere ese perfil para que la aplicación se pueda ejecutar en un dispositivo iOS. Si falta o ha caducado un perfil de datos, la aplicación se bloquea cuando un usuario toca en ella para abrirla.
Eliminación de perfiles de datos	Permite eliminar perfiles de datos de iOS.
Proxy	Permite especificar la configuración global de proxy HTTP en dispositivos iOS o Windows Mobile/CE. Puede implementar solamente una directiva global de proxy HTTP por dispositivo.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Registro	Permite definir los valores y las claves de Registro que le permitirán administrar dispositivos Windows Mobile/CE. El Registro de Windows Mobile/CE almacena datos sobre las aplicaciones, los controladores, las preferencias del usuario y los parámetros de configuración.
Remote Support	Permite el acceso remoto a dispositivos Samsung Knox. Remote Support no está disponible para nuevos clientes desde el 1 de enero de 2019. Los clientes existentes pueden seguir utilizando el producto, pero Citrix no proporcionará mejoras ni correcciones.
Restricciones	Ofrece numerosas opciones para bloquear y controlar funciones y funcionalidades en los dispositivos administrados. Ejemplos de opciones de restricción: inhabilitar la cámara o el micrófono, aplicar reglas de itinerancia o pedir el acceso a servicios externos, como almacenes de aplicaciones.
Itinerancia	Permite configurar si se permite el roaming de voz y de datos en los dispositivos iOS o Windows Mobile/CE. Si se inhabilita la itinerancia de voz, la itinerancia de datos se inhabilita automáticamente.
Clave de licencia MDM de Samsung	Permite indicar la clave integrada de Samsung Enterprise License Management (ELM) que debe implementar en un dispositivo para poder implementar después directivas y restricciones de SAFE. XenMobile también admite el servicio Enterprise Firmware-Over-The-Air (E-FOTA) de Samsung. XenMobile admite y extiende directivas de Samsung for Enterprise (SAFE) y Samsung Knox.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Programación	Es necesaria para que los dispositivos Android y Windows Mobile se conecten de vuelta a XenMobile Server para la administración MDM, el envío de aplicaciones y la implementación de directivas. Si no envía esta directiva y no habilita Google FCM, el dispositivo no podrá volver a conectarse al servidor.
SCEP	Permite configurar dispositivos iOS y macOS para obtener un certificado desde un servidor SCEP externo. También puede entregar un certificado al dispositivo mediante SCEP de una PKI que está conectada a XenMobile. Para ello, cree un proveedor PKI y una entidad PKI en el modo distribuido.
Cuenta SSO	Permite crear cuentas de inicio de sesión único (SSO) para que los usuarios solo deban iniciar sesión una vez para acceder a XenMobile y a los recursos internos de la empresa. Así, no es necesario que los usuarios almacenen credenciales en el dispositivo. XenMobile utiliza las credenciales del usuario de empresa de una cuenta SSO para varias aplicaciones, incluidas las aplicaciones del App Store de Apple. Esta directiva es compatible con la autenticación Kerberos. Disponible para iOS.
Cifrado de almacenamiento	Permite cifrar el almacenamiento interno y el externo. En algunos dispositivos, esta directiva impide que los usuarios usen una tarjeta de almacenamiento en sus dispositivos.
Calendarios suscritos	Permite agregar un calendario suscrito a la lista de calendarios en dispositivos iOS. Debe haberse suscrito a un calendario para poder agregarlo a la lista de calendarios suscritos ubicada en los dispositivos de los usuarios.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Términos y condiciones	Permite requerir que los usuarios acepten las directivas específicas de la empresa que regulan las conexiones a la red corporativa. Cuando los usuarios inscriban sus dispositivos en XenMobile, deberán aceptar los términos y las condiciones para llevar a cabo la inscripción. Si rechazan dichos términos y condiciones, se cancelará el proceso de inscripción.
Túnel	Se utiliza solo para Remote Support. La asistencia remota (Remote Support) permite que el personal del servicio de asistencia tome el control remoto de los dispositivos móviles Windows CE y Android administrados. Remote Support no está disponible para implementaciones locales en clúster de XenMobile Server. Remote Support no está disponible para nuevos clientes desde el 1 de enero de 2019. Los clientes existentes pueden seguir utilizando el producto, pero Citrix no proporcionará mejoras ni correcciones.
VPN	Permite acceder a sistemas back-end que utilizan tecnología antigua de puerta de enlace VPN. Esta directiva ofrece datos de conexión de puerta de enlace VPN que se pueden implementar en los dispositivos. XenMobile es compatible con varios proveedores de VPN, como Cisco AnyConnect, Juniper y Citrix VPN. También es posible vincular esta directiva a una entidad de certificación (CA) y habilitar VPN a demanda (siempre que la puerta de enlace VPN admita esta opción).

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Wallpaper	Permite agregar un archivo JPG o PNG para establecer un fondo de escritorio en un dispositivo iOS para la pantalla de bloqueo, la pantalla de inicio o ambas pantallas. Para usar fondos de pantalla diferentes en iPads y iPhones, debe crear varias directivas de fondo de escritorio y aplicarlas a los usuarios correspondientes.
Filtro de contenido web	Permite filtrar el contenido web en dispositivos iOS. XenMobile utiliza la función Autofiltro de Apple y los sitios que usted agregue a las listas de permitidos y bloqueados. Disponible solamente para dispositivos iOS supervisados.
Clip web	Permite colocar accesos directos (o clips Web) que acceden a sitios web de forma que aparezcan junto a las aplicaciones en los dispositivos de los usuarios. Puede especificar sus propios iconos para representar los clips Web en dispositivos iOS, macOS y Android. Las tabletas Windows solo requieren una etiqueta y una URL.
Wi-Fi	Permite a los administradores implementar datos del enrutador Wi-Fi en los dispositivos administrados. Los datos de enrutador son: el SSID, los datos de autenticación y los datos de configuración.
Certificado de Windows CE	Permite crear y entregar certificados de Windows Mobile/CE desde una infraestructura PKI externa a los dispositivos de los usuarios.
Windows Information Protection	Permite especificar las aplicaciones que requieren Windows Information Protection en el nivel de exigencia que usted establezca para la directiva. La directiva es para dispositivos supervisados con Windows 10 o Windows 11.

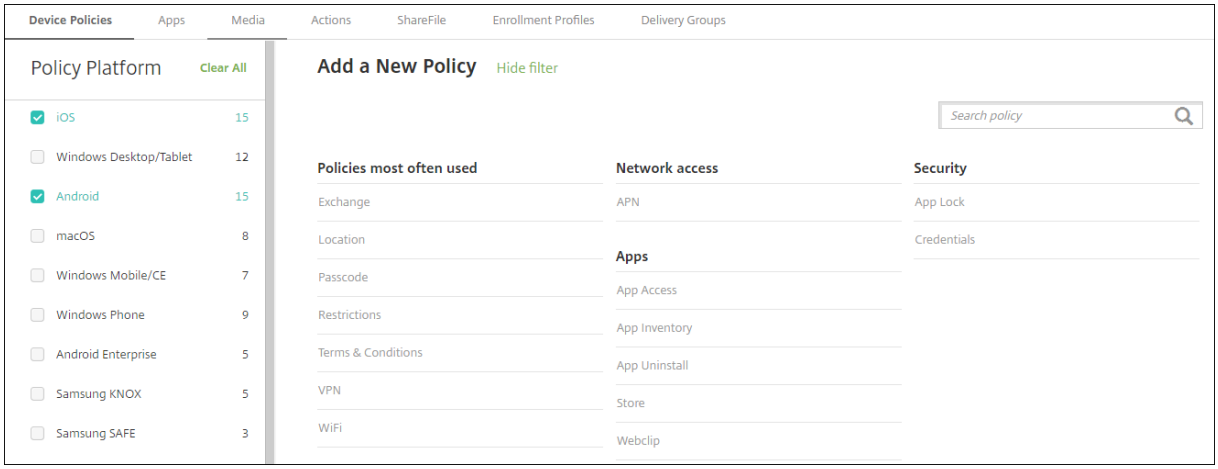
Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
XenMobile Store	Permite especificar si aparecerá un clip Web de XenMobile Store en la pantalla de inicio de los dispositivos de usuario.
Opciones de XenMobile	Permite configurar el comportamiento de Secure Hub al conectarse a XenMobile desde dispositivos Android y Windows Mobile/CE.
Desinstalación de XenMobile	Permite desinstalar XenMobile de dispositivos Android y Windows Mobile/CE. Cuando se implementa, esta directiva elimina XenMobile de todos los dispositivos que contenga el grupo de implementación.

Directivas de dispositivo por plataforma

January 4, 2022

Para ver las directivas que están disponibles por plataforma:

1. En la consola de XenMobile, vaya a **Configurar > Directivas de dispositivo**.
2. Haga clic en **Agregar**.
3. Cada plataforma de dispositivo aparece en una lista del panel **Plataforma de directiva**. Si ese panel no está abierto, haga clic en **Mostrar filtro**.
4. Para ver una lista de todas las directivas disponibles para una plataforma, seleccione esa plataforma. Para ver una lista de las directivas disponibles para varias plataformas, seleccione cada una de esas plataformas. Una directiva aparece en la lista solo si se aplica a cada plataforma seleccionada.



La versión más reciente de XenMobile admite las directivas de dispositivo para las plataformas siguientes:

- Amazon
- Android
- Android Enterprise
- Android Zebra
- iOS
- macOS
- Samsung SAFE
- Samsung Knox
- Tabletas o equipos de escritorio con Windows 10 y Windows 11
- Windows Phone 10
- Windows Mobile/CE

Para obtener más información sobre dispositivos compatibles en la versión más reciente de XenMobile, consulte Plataformas de dispositivos compatibles.

> **Nota:**
>
> Si el entorno está configurado con objetos de directiva de grupo (GPO):
>
> Al configurar las directivas de dispositivo de XenMobile para Windows 10 y Windows 11, tenga en cuenta esta regla. Si una directiva que esté presente en uno o varios dispositivos inscritos entra en conflicto, tiene prioridad la directiva que concuerde con el GPO.

Directiva de duplicación AirPlay

January 4, 2022

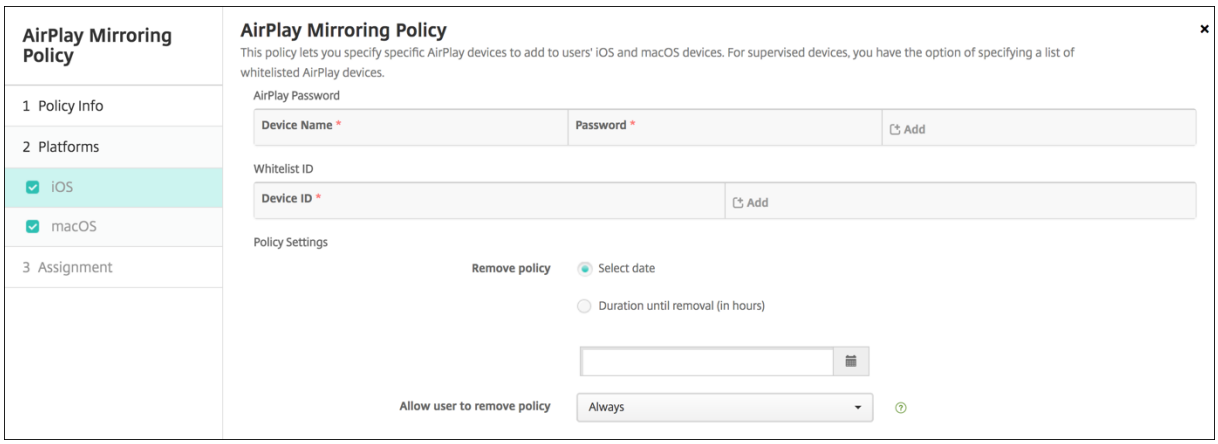
La funcionalidad AirPlay de Apple permite a los usuarios reproducir exactamente lo que aparece en la pantalla de un dispositivo en otro equipo Mac.

En XenMobile, puede agregar una directiva de dispositivo para agregar dispositivos AirPlay específicos (como otro equipo Mac) a los dispositivos iOS. También tiene la opción de agregar dispositivos a una lista de dispositivos supervisados permitidos, lo que limita a los usuarios a esos dispositivos AirPlay únicamente. 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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS



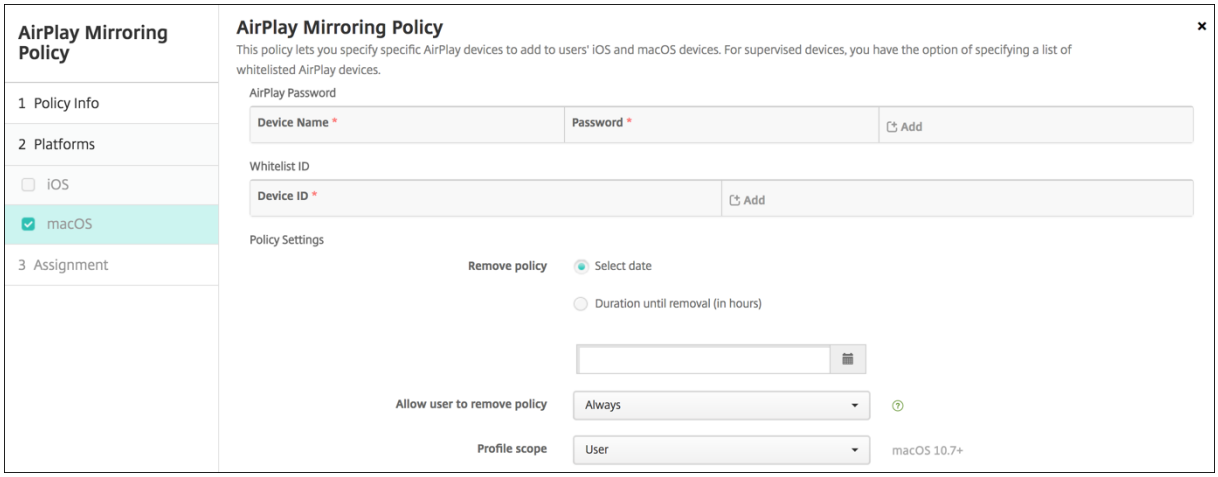
- **Contraseña de AirPlay:** Para agregar cada dispositivo, haga clic en **Agregar** y lleve a cabo lo siguiente:
  - **ID del dispositivo:** Escriba la dirección de hardware (dirección MAC) en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - **Contraseña:** Escriba una contraseña opcional para el dispositivo.
  - Haga clic en **Agregar** para agregar el dispositivo, o bien haga clic en **Cancelar** para no agregarlo.
- **ID de lista blanca:** Esta lista se omite en caso de dispositivos no supervisados. Los ID de dispositivo de esta lista pertenecen a 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 **Agregar** y lleve a cabo lo siguiente:

  > **Nota:**
  >
  > La consola de XenMobile Server contiene los términos “lista negra” y “lista blanca”. Estamos cambiando esos términos en una próxima versión a “lista de bloqueados” y “lista de permitidos”.

  - **ID del dispositivo:** 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 **Agregar** para agregar el dispositivo, o bien haga clic en **Cancelar** para no agregarlo.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.

* **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
* **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.

Parámetros de macOS



- **Contraseña de AirPlay:** Para agregar cada dispositivo, haga clic en **Agregar** y lleve a cabo lo siguiente:
  - **ID del dispositivo:** Escriba la dirección de hardware (dirección MAC) en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - **Contraseña:** Escriba una contraseña opcional para el dispositivo.
  - Haga clic en **Agregar** para agregar el dispositivo, o bien haga clic en **Cancelar** para no agregarlo.
- **ID de lista blanca:** Esta lista se omite en caso de dispositivos no supervisados. Los ID de dispositivo de esta lista pertenecen a los únicos dispositivos AirPlay que se encuentran a disposición de los dispositivos de usuario. Para agregar cada dispositivo AirPlay a la lista, haga clic en **Agregar** y lleve a cabo lo siguiente:
  - **ID del dispositivo:** 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 **Agregar** para agregar el dispositivo, o bien haga clic en **Cancelar** para no agregarlo.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que

tenga lugar la eliminación de la directiva.
- **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Directiva de AirPrint

January 4, 2022

En XenMobile, puede agregar una directiva de dispositivo para añadir impresoras AirPrint a la lista de impresoras AirPrint de los dispositivos iOS. Esta directiva facilita los entornos en los que las impresoras y los dispositivos están en subredes diferentes.

Esta directiva se aplica a iOS 7.0 y versiones posteriores.

> **Nota:**
>
> Compruebe que dispone de la dirección IP y de la ruta de recursos para cada impresora.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Destino de AirPrint:** Para agregar cada destino de AirPrint, haga clic en **Agregar** y lleve a cabo lo siguiente:
  - **Dirección IP:** Escriba la dirección IP de la impresora AirPrint.
  - **Ruta del recurso:** Escriba la ruta del recurso 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 **Guardar** para agregar la impresora, o bien haga clic en **Cancelar** para no agregarla.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.

* **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva Configuraciones administradas por Android Enterprise

January 4, 2022

La directiva Configuraciones administradas por Android Enterprise controla varias opciones de configuración y restricciones de aplicaciones. El desarrollador de aplicaciones define las opciones y los textos de ayuda disponibles para la aplicación. Si en un texto de ayuda se menciona el uso de un "valor de plantilla", use en su lugar la macro correspondiente de XenMobile. Para obtener más información, consulte Remote configuration overview (en el sitio para desarrolladores de Android) y Macros.

Los parámetros de configuración de una aplicación pueden incluir elementos tales como:

- Parámetros de correo electrónico de la aplicación
- Permitir o bloquear direcciones URL para un explorador web
- Opción para controlar la sincronización del contenido de aplicaciones a través de una conexión móvil o solo mediante una conexión Wi-Fi

Para obtener información sobre la configuración que aparece para las aplicaciones, contacte con el desarrollador de la aplicación.

Requisitos previos

- Complete las tareas de configuración de Android Enterprise en Google y conecte Android Enterprise a Google Play administrado. Para obtener más información, consulte Android Enterprise.
- Agregue aplicaciones Android Enterprise a XenMobile. Para obtener más información, consulte Agregar aplicaciones a XenMobile.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos para las redes VPN por aplicación

Para crear una VPN por aplicación para AE, debe realizar otros pasos, además de configurar la directiva de configuraciones administradas por Android Enterprise. Además, debe comprobar que se cumplen estos requisitos previos:

- Dispositivo Citrix Gateway local
- Estas aplicaciones están instaladas en el dispositivo:

- Citrix SSO
- Citrix Secure Hub

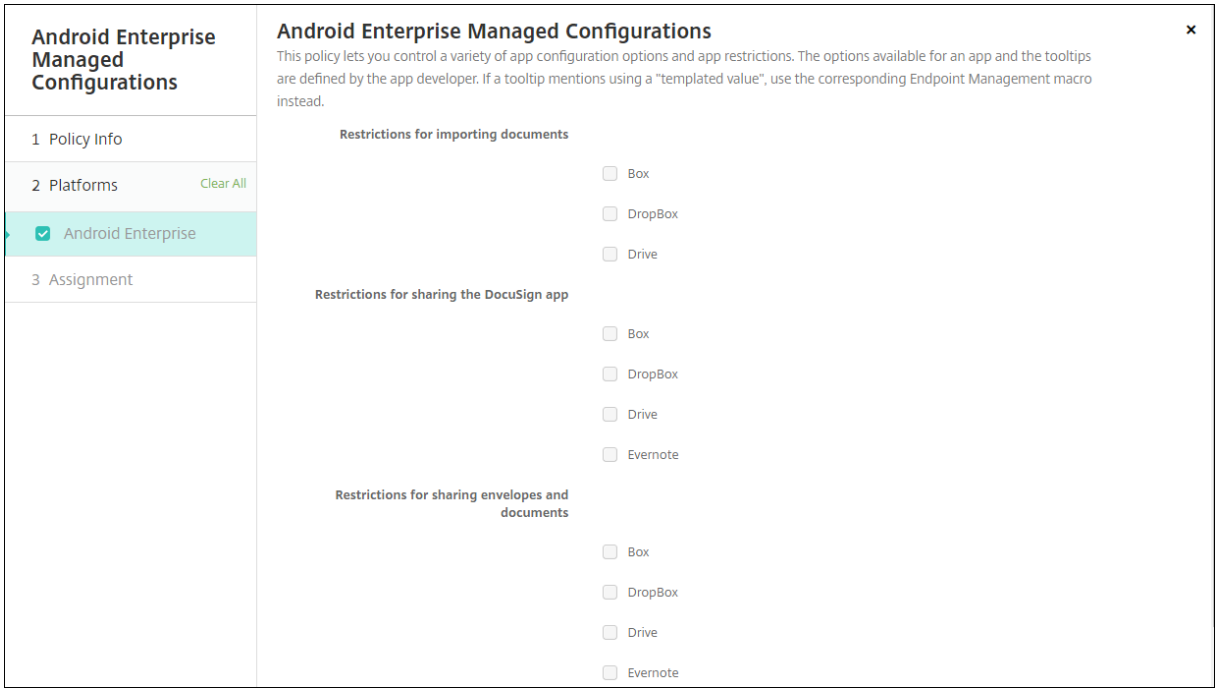
He aquí un flujo de trabajo general para configurar una VPN por aplicación para dispositivos AE:

1. Configure un perfil de VPN tal y como se describe en este artículo.
2. Configure Citrix ADC para aceptar el tráfico de la VPN por aplicación. Para obtener información detallada, consulte Configuración de VPN completa en Citrix Gateway.

Parámetros de Android Enterprise

Una vez que haya optado por agregar una directiva Configuraciones administradas por Android Enterprise, aparece un mensaje para seleccionar una aplicación concreta. Si no hay aplicaciones Android Enterprise agregadas a XenMobile, no podrá continuar.

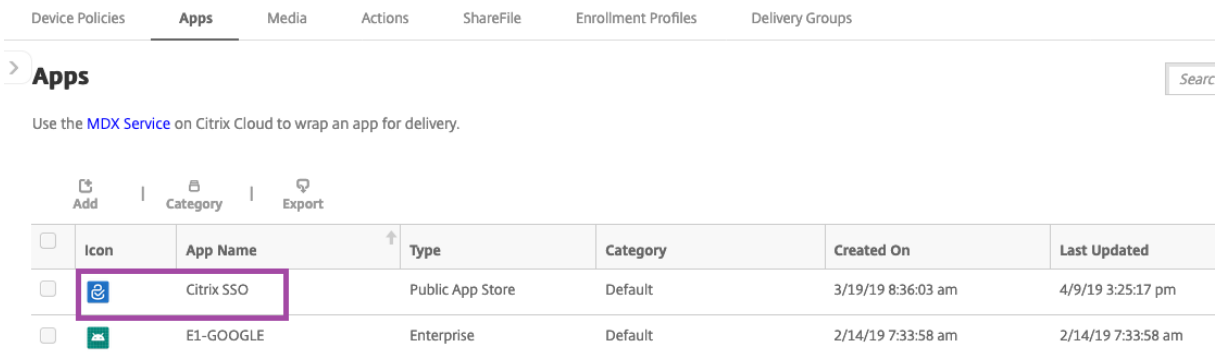
Después de seleccionar una aplicación, defina las configuraciones de la directiva. Las configuraciones son específicas de cada aplicación.



Configurar perfiles de VPN para Android Enterprise

Haga que los perfiles de VPN estén disponibles para los dispositivos Android Enterprise mediante la aplicación Citrix SSO con la directiva Configuraciones administradas por Android Enterprise.

Comience por agregar Citrix SSO a la consola de XenMobile como una aplicación de la tienda de Google Play. Consulte Agregar una aplicación de la tienda pública de aplicaciones.

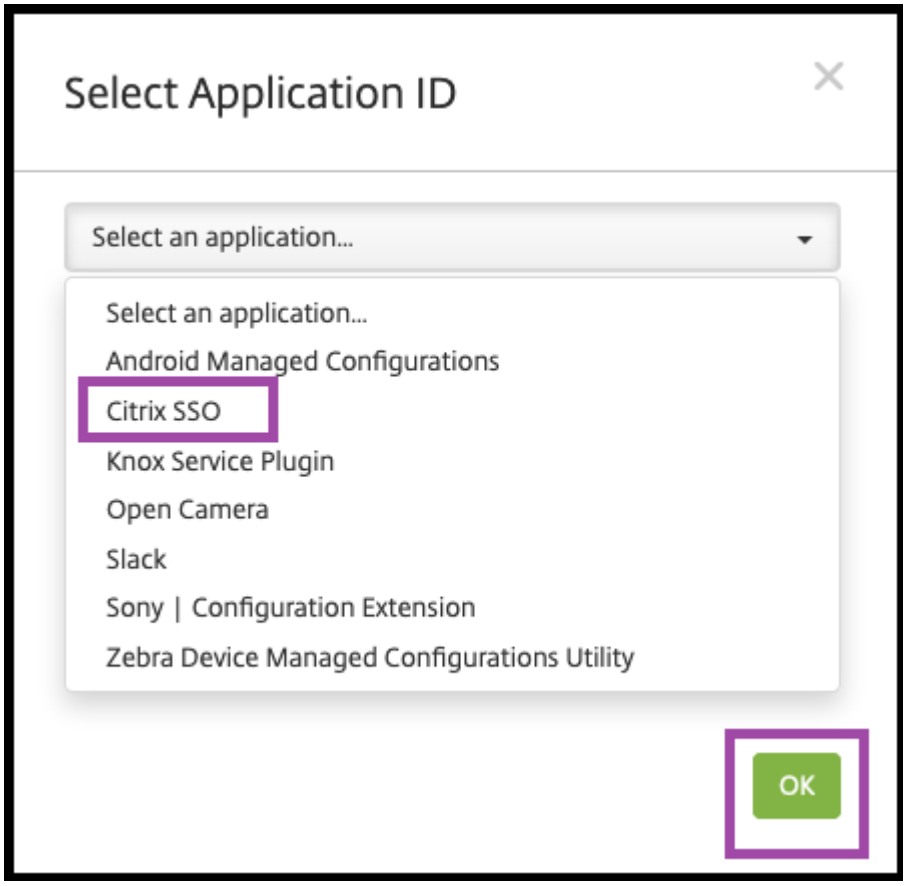


Crear una configuración administrada por Android Enterprise para Citrix SSO

Configure la directiva Configuraciones administradas por Android Enterprise para que Citrix SSO pueda crear perfiles de VPN. Los dispositivos que tienen instalada la aplicación Citrix SSO y la directiva implementada tienen acceso a los perfiles de VPN que cree.

Necesita el FQDN y el puerto de Citrix Gateway.

1. En la consola de XenMobile, haga clic en **Configurar > Directivas de dispositivo**. Haga clic en **Agregar**.
2. Seleccione **Android Enterprise**. Haga clic en **Configuraciones administradas por Android Enterprise**.
3. Cuando aparezca la ventana **Seleccionar ID de aplicación**, elija **Citrix SSO** de la lista y haga clic en **Aceptar**.



4. Escriba un nombre y una descripción para la configuración de la VPN de Citrix SSO. Haga clic en **Siguiente**.

5. Configure los parámetros del perfil de VPN.
   - **Nombre del perfil de VPN**. Escriba un nombre para el perfil de VPN. Si va a crear más de

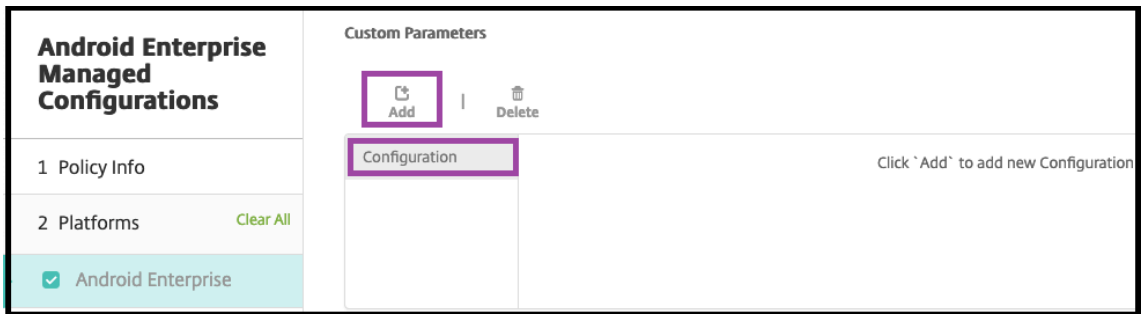
un perfil de VPN, utilice un nombre único para cada perfil. Si no proporciona un nombre, la dirección que puso en el campo **Dirección del servidor** se utiliza como nombre del perfil de VPN.

- **Dirección del servidor (*)**. Escriba el FQDN de Citrix Gateway. Si el puerto de Citrix Gateway no es 443, escriba también el puerto. Utilice un formato de URL. Por ejemplo, `https://gateway.mycompany.com:8443`.
- **Nombre de usuario (opcional).** Proporcione el nombre de usuario que utilizan los usuarios finales para autenticarse en Citrix Gateway. Puede utilizar la macro {user.username} de XenMobile para este campo (consulte Macros). Si usted no proporciona un nombre de usuario, se pedirá a los usuarios que proporcionen uno cuando se conecten a Citrix Gateway.
- **Contraseña (optativa)**. Proporcione la contraseña que utilizan los usuarios finales para autenticarse en Citrix Gateway. Si usted no proporciona una contraseña, se pedirá a los usuarios que proporcionen una contraseña cuando se conecten a Citrix Gateway.
- **Alias de certificado (opcional).** Escriba un alias de certificado. El alias de certificado facilita a la aplicación el acceso al certificado. Cuando se utiliza el mismo alias de certificado con la directiva Credenciales, la aplicación obtiene el certificado y autentica la VPN sin ninguna acción por parte de los usuarios.
- **Tipo de VPN por aplicación (opcional).** Si utiliza VPN por aplicación para restringir las aplicaciones que usan esta VPN, puede configurar este parámetro. Si selecciona **Permitir**, el tráfico de red de los nombres de paquetes de aplicaciones indicados en la **lista de aplicaciones de Per App VPN** se redirige a través de la VPN. El tráfico de red de todas las demás aplicaciones se redirige fuera de la VPN. Si selecciona **No permitir**, el tráfico de red de los nombres de paquetes de aplicaciones indicados en la **lista de aplicaciones de Per App VPN** se redirige fuera de la VPN. El tráfico de red de todas las demás aplicaciones se redirige a través de la VPN. El valor predeterminado es **Permitir**.
- **Lista de aplicaciones de Per App VPN**. Una lista de aplicaciones cuyo tráfico está permitido o no permitido en la VPN, en función del valor de **Tipo de VPN por aplicación**. Indique los nombres de los paquetes de aplicaciones separados por comas o puntos y comas. Los nombres de los paquetes de aplicaciones distinguen entre mayúsculas y minúsculas y deben estar escritos en esta lista tal y como lo están en la tienda de Google Play. Esta lista es opcional. Mantenga esta lista vacía para aprovisionar la VPN en todo el dispositivo.
- **Perfil de VPN predeterminado.** Escriba el nombre del perfil de VPN que quiere utilizar cuando los usuarios toquen en el botón de conexión de la interfaz de usuario de la aplicación Citrix SSO en lugar de tocar en un perfil específico. Si este campo se deja vacío, se utiliza el perfil principal para la conexión. Si solo se configura un perfil, este se marca

como perfil predeterminado. Para la VPN permanente, este campo debe establecerse en el nombre del perfil de VPN que se utilizará para establecer la VPN permanente.

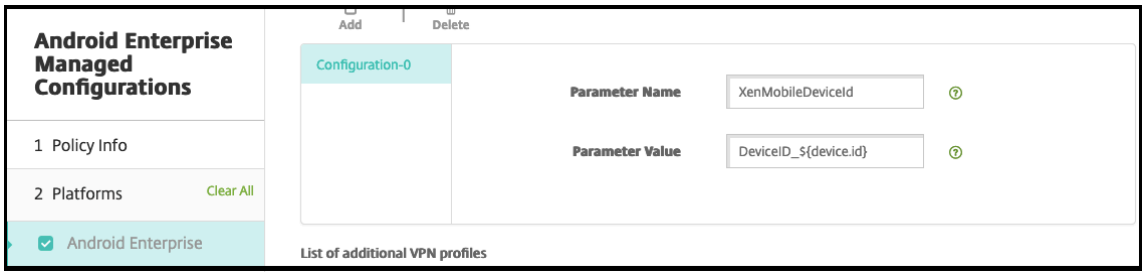
- **Inhabilitar perfiles de usuario.** Si este parámetro está activado, los usuarios no pueden crear sus propias VPN en sus dispositivos. Si este parámetro está desactivado, los usuarios pueden crear sus propias VPN en sus dispositivos. Está desactivado de forma predeterminada.
- **Bloquear servidores que no son de confianza**. Este parámetro se desactiva al utilizar un certificado autofirmado para Citrix Gateway o cuando el certificado raíz de la entidad de certificación que emite el certificado de Citrix Gateway no está en la lista de entidades de certificación del sistema. Si este parámetro está activado, el sistema operativo Android valida el certificado de Citrix Gateway. Si se produce un error en la validación, no se permite la conexión. Está activada de forma predeterminada.

6. También puede crear parámetros personalizados. Se admiten los parámetros personalizados **XenMobileDeviceId** y **UserAgent**. Seleccione la configuración de VPN actual y haga clic en **Agregar**.



a) Cree un parámetro personalizado:

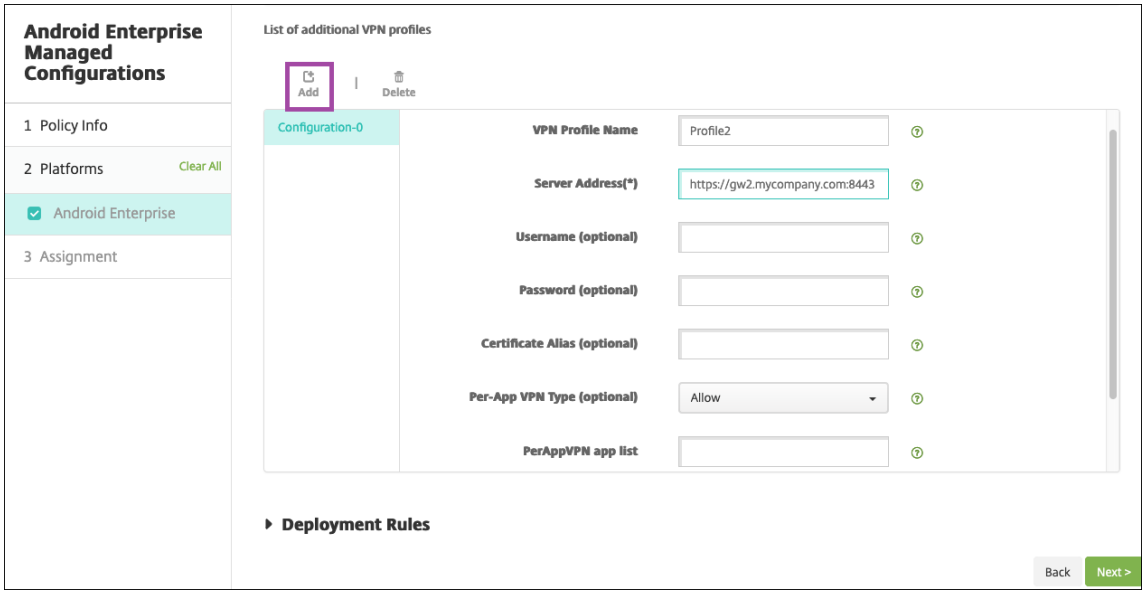
- **Nombre del parámetro.** Escriba **XenMobileDeviceId**. Este campo es el ID de dispositivo que se utilizará para la comprobación de acceso a la red basado en la inscripción de dispositivos en XenMobile. Si XenMobile inscribe y administra el dispositivo, se permite la conexión VPN. De lo contrario, la autenticación queda denegada al establecer la VPN.
- **Valor del parámetro.** Para que XenMobile determine el estado de inscripción y administración de los dispositivos, el valor de XenMobileDeviceID debe establecerse en `DeviceID_${ device.id }`.



a) Para crear otro parámetro personalizado, haga clic de nuevo en **Agregar**. Cree este parámetro personalizado.

- **Nombre del parámetro.** Escriba **UserAgent**. Este texto se agrega al encabezado HTTP User-Agent para realizar una comprobación adicional en Citrix Gateway. La aplicación Citrix SSO agrega el valor de este texto al encabezado HTTP User-Agent durante la comunicación con Citrix Gateway.
- **Valor del parámetro.** Escriba el texto que quiere agregar al encabezado HTTP User-Agent. Este texto debe ajustarse a las especificaciones HTTP de User-Agent.

7. También puede crear más configuraciones de perfil de VPN. Haga clic en **Agregar** en la lista de configuraciones. Aparecerá una nueva configuración en la lista. Seleccione la nueva configuración y repita el paso 5 y, si quiere, el paso 6.



8. Cuando haya creado todos los perfiles de VPN que quiera, haga clic en **Siguiente**.
9. Configure las reglas de implementación de esta configuración administrada para Citrix SSO.
10. Haga clic en **Guardar**.

Esta configuración administrada para Citrix SSO aparece ahora en la lista de directivas de dispositivo configuradas.

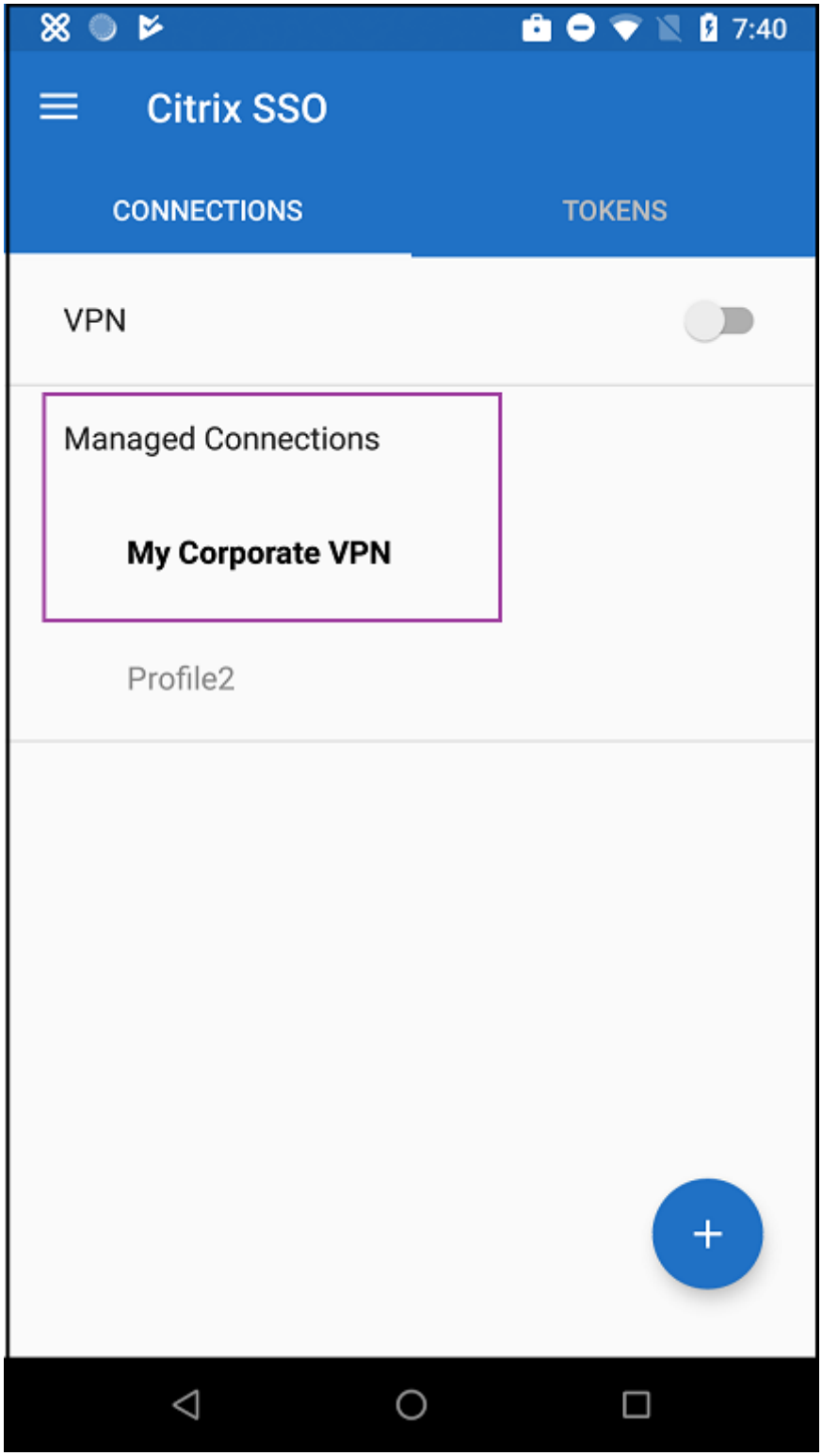
Para habilitar la permanencia de los perfiles de VPN configurados, establezca la directiva de opciones de XenMobile.

> **Nota:**
> Es necesario Citrix Secure Hub 19.5.5 o superior para la VPN permanente en Android Enterprise.

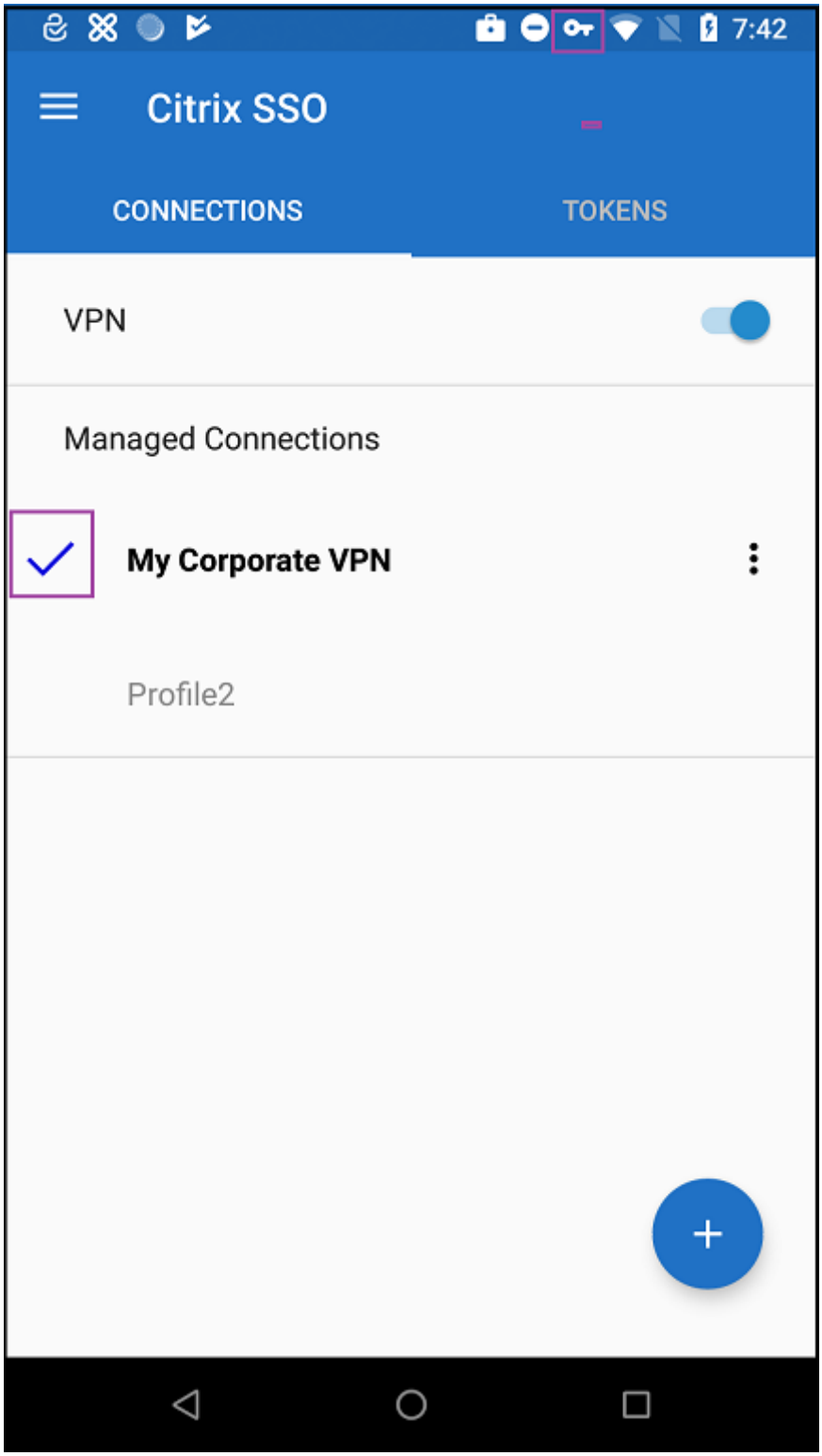
Acceder a perfiles de VPN desde el dispositivo

Para acceder a los perfiles de VPN creados, los usuarios de Android Enterprise instalan Citrix SSO desde la tienda de Google Play.

Los perfiles de VPN configurados aparecen en el área **Conexiones administradas** de la aplicación. Los usuarios tocan en el perfil de VPN para conectarse a través de ese perfil de VPN.



Después de que los usuarios se hayan autenticado y conectado, aparece una marca de verificación junto al perfil de VPN. El icono con forma de llave indica que la VPN está conectada.



Administrar dispositivos Zebra Android con Zebra OEMConfig

Administre dispositivos Zebra Android con la herramienta administrativa OEMConfig de Zebra Technologies. Para obtener información sobre la aplicación Zebra OEMConfig, consulte el sitio web de Zebra Technologies.

XenMobile es compatible con Zebra OEMConfig 9.2 y versiones posteriores. Para obtener información sobre los requisitos del sistema para instalar Zebra OEMConfig en dispositivos, consulte OEMConfig Setup en el sitio web de Zebra Technologies.

Comience por agregar la aplicación Zebra OEMConfig a la consola de XenMobile como una aplicación de la tienda de Google Play. Consulte Agregar una aplicación de la tienda pública de aplicaciones.

Crear una configuración administrada por Android Enterprise para la aplicación Zebra OEMConfig

Configure la directiva de dispositivo de configuraciones administradas por Android Enterprise para la aplicación Zebra OEMConfig. Esta directiva se aplica a los dispositivos Zebra que tienen instalada la aplicación Zebra OEMConfig y la directiva implementada.

1. En la consola de XenMobile, haga clic en **Configurar > Directivas de dispositivo**. Haga clic en **Agregar**.
2. Seleccione **Android Enterprise**. Haga clic en **Configuraciones administradas por Android Enterprise**.
3. Cuando aparezca la ventana **Seleccionar ID de aplicación**, elija **Zebra OEMConfig powered by MX** de la lista y haga clic en **Aceptar**.
4. Escriba un nombre y una descripción para la configuración de Zebra OEMConfig. Haga clic en **Siguiente**.
5. Escriba un nombre para la configuración de Zebra OEMConfig.
6. Configure los parámetros disponibles. Por ejemplo:
    - Para desactivar la cámara frontal del dispositivo, seleccione **Camera Configuration** y establezca **Use of Front Camera** en **Off**.
    - Para cambiar el formato de la hora de los dispositivos, seleccione **Clock Configuration** y establezca **Time Format** en **12** para el formato de 12 horas o en **24** para el formato de 24 horas.

Para obtener una lista y descripciones de toda la configuración disponible, consulte Zebra Managed Configurations en el sitio web de Zebra Technologies.

1. Si quiere, también puede crear más configuraciones de Zebra OEMConfig. Haga clic en **Agregar** en la lista de configuraciones. Aparecerá una nueva configuración en la lista. Seleccione la nueva configuración y configure los parámetros.

2. Cuando haya creado todas las configuraciones de Zebra OEMConfig correspondientes, haga clic en **Siguiente**.
3. Configure las reglas de implementación de esta configuración administrada para Zebra OEMConfig.
4. Haga clic en **Guardar**.

Permisos de aplicación de Android Enterprise

January 4, 2022

Puede definir cómo las solicitudes a aplicaciones Android Enterprise, incluidas en los perfiles de trabajo, gestionan lo que Google considera permisos "peligrosos". Usted controla si solicitar a los usuarios que concedan o denieguen una solicitud de permiso por parte de las aplicaciones. Esta función se aplica a dispositivos que ejecutan Android 7.0 y versiones posteriores.

Según Google, los permisos peligrosos son aquellos que otorgan a la aplicación acceso a datos o recursos que pueden contener información privada del usuario o podrían afectar los datos almacenados del usuario o el funcionamiento de otras aplicaciones. Por ejemplo, la capacidad de leer contactos del usuario es un permiso peligroso.

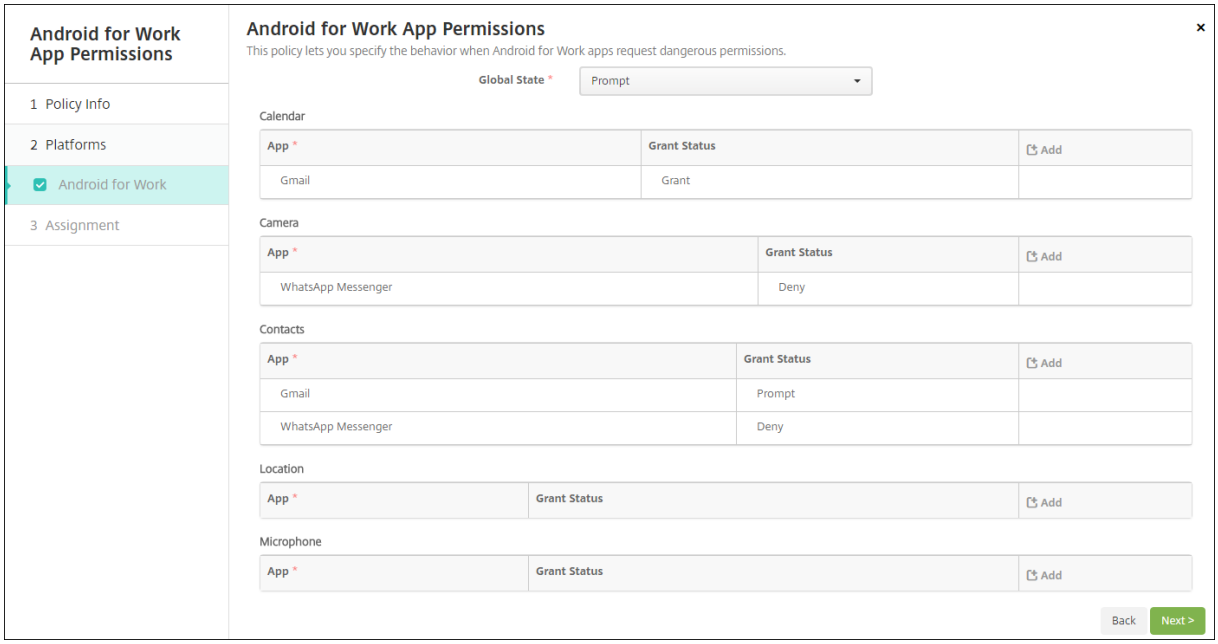
En caso de aplicaciones Android Enterprise incluidas en los perfiles de trabajo, puede configurar un estado global que controle el comportamiento de todas las solicitudes de permisos peligrosos a las aplicaciones. También puede controlar el comportamiento de la solicitud de permisos peligrosos para grupos de permisos individuales, según lo definido por Google, para cada aplicación. Esas configuraciones individuales prevalecen sobre el estado global.

Para obtener información sobre cómo define Google los grupos de permisos, consulte "Permission groups" en la guía de desarrolladores de Android.

De forma predeterminada, se solicitará a los usuarios que concedan o denieguen las solicitudes de permisos peligrosos.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Android Enterprise



- **Estado global:** Controla el comportamiento de todas las solicitudes de permisos peligrosos. En la lista, haga clic en **Preguntar**, **Conceder** o **Denegar**.
  - **Preguntar:** Se solicita a los usuarios que concedan o denieguen las solicitudes de permisos peligrosos.
  - **Conceder:** Se conceden todas las solicitudes de permisos peligrosos. No se pregunta al usuario.
  - **Denegar:** Se deniegan todas las solicitudes de permisos peligrosos. No se pregunta al usuario.

  El valor predeterminado es **Preguntar**.
- Puede configurar un comportamiento individual de cada grupo de permisos para cada aplicación. Para configurar el comportamiento de un grupo de permisos, haga clic en **Agregar** y, a continuación, en **Aplicación**, elija una aplicación de la lista. Si configura las aplicaciones del sistema Android Enterprise, haga clic en **Agregar** e indique el nombre del paquete de aplicaciones que habilitó en la directiva de restricciones. En el apartado "Estado de acceso", elija **Preguntar**, **Conceder** o **Denegar**. Este estado de acceso prevalece sobre el estado global.
  - **Preguntar:** Se solicita a los usuarios que concedan o denieguen las solicitudes de permisos peligrosos de este grupo para esta aplicación.
  - **Conceder:** Se conceden las solicitudes de permisos peligrosos de este grupo para esta aplicación. No se pregunta al usuario.
  - **Denegar:** Se rechazan las solicitudes de permisos peligrosos de este grupo para esta aplicación. No se pregunta al usuario.

El valor predeterminado es **Preguntar**.

- Haga clic en **Guardar**, situado junto a la aplicación y el estado de acceso.
- Para agregar más aplicaciones al grupo de permisos, haga clic en **Agregar** de nuevo y repita estos pasos.
- Cuando haya terminado de configurar los estados de acceso para todos los grupos de permisos pertinentes, haga clic en **Siguiente**.

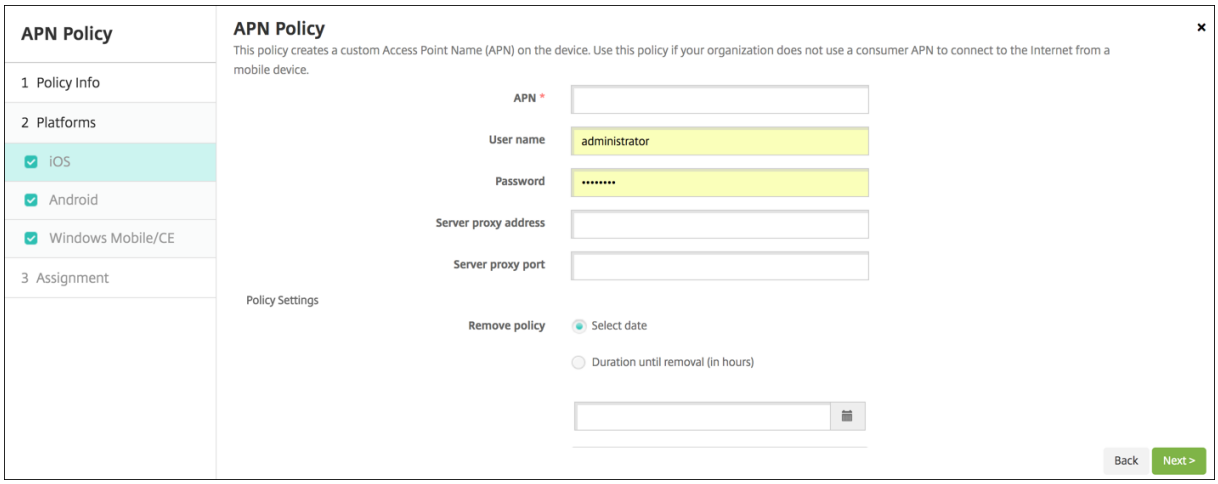
Directiva de APN

January 4, 2022

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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

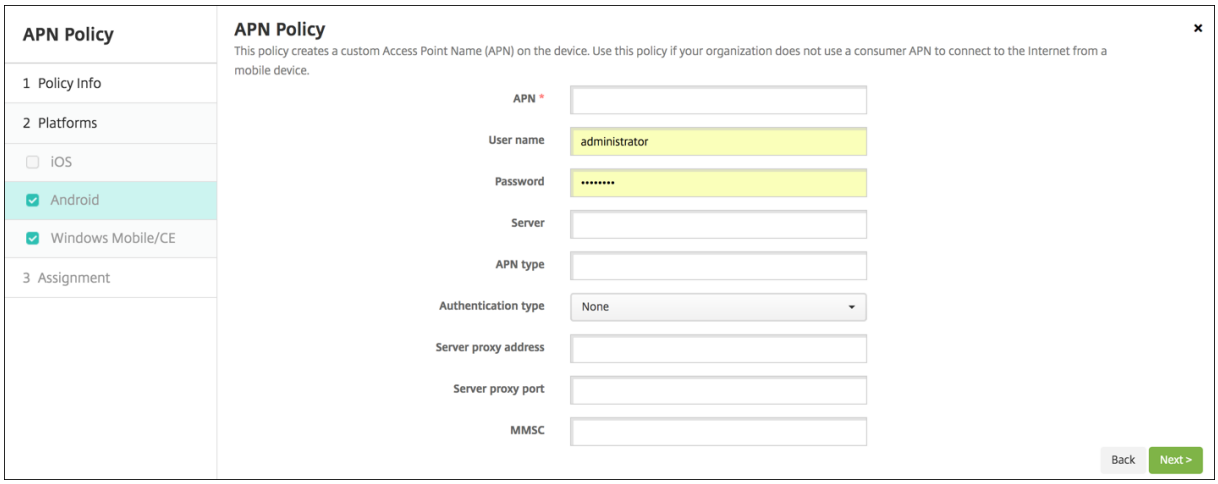
Parámetros de iOS



- **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.
- **Nombre de usuario:** 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.

- **Contraseña:** 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.
- **Dirección del servidor proxy:** La dirección IP o dirección URL del proxy de APN.
- **Puerto del servidor proxy:** El número de puerto del proxy de APN. Esto es necesario si especificó una dirección de servidor proxy.
- En **Configuraciones de directivas**, junto a **Quitar directiva**, haga clic en **Seleccionar fecha** o **Demora hasta la eliminación (en horas)**.
  - Si hace clic en **Seleccionar fecha**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista **Permitir al usuario quitar la directiva**, haga clic en **Siempre**, **Requerir código de acceso** o **Nunca**.
  - Si hace clic en **Requerir código de acceso**, junto a **Código de acceso para la eliminación**, introduzca la contraseña en cuestión.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de Android

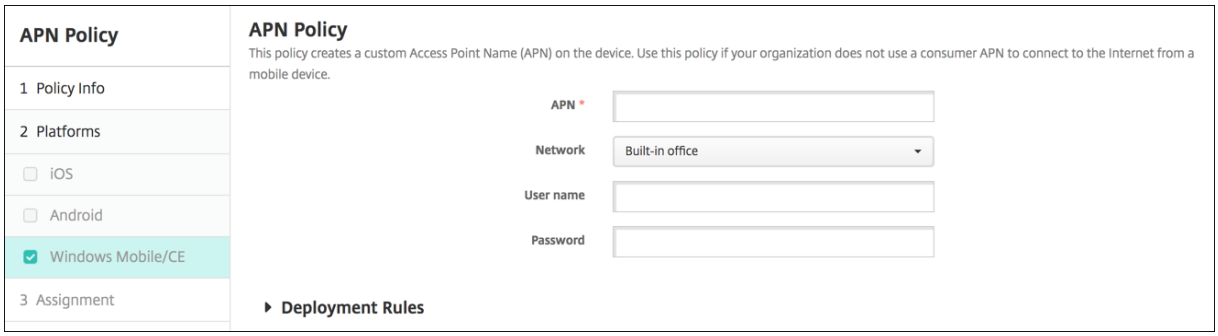


- **APN:** Introduzca el nombre del punto de acceso. Este valor debe coincidir con un nombre APN de Android aceptado. De lo contrario, la directiva fallará.
- **Nombre de usuario:** Esta cadena especifica el nombre de usuario para este APN. Si falta el

nombre de usuario, el dispositivo solicitará la cadena durante la instalación de perfil.

- **Contraseña:** 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.
- **Servidor:** 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.
- **Tipo de APN:** 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 (predeterminado). 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) se ha retirado y no se usa con frecuencia.
  - hipri. Redes de alta prioridad.
  - fota. El firmware over-the-air se usa para recibir actualizaciones de firmware.
- **Tipo de autenticación:** En la lista, haga clic en el tipo de autenticación que se va a usar. El valor predeterminado es “Ninguna”.
- **Dirección del servidor proxy:** La dirección IP o dirección URL del proxy HTTP de APN del operador.
- **Puerto del servidor proxy:** 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.
- **Dirección del proxy de MMS:** 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).
- **Puerto MMS:** El puerto utilizado para el proxy MMS.

Parámetros de Windows Mobile/CE



- **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.
- **Red:** En la lista, haga clic en el tipo de red que quiere usar. El valor predeterminado es **Oficina integrada**.
- **Nombre de usuario:** 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.
- **Contraseña:** 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.

Directiva de acceso a aplicaciones

January 3, 2020

En XenMobile, la directiva “Acceso a 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 obligatorias, de aplicaciones recomendadas o de aplicaciones prohibidas, pero no puede mezclar el tipo de aplicaciones en una misma directiva de acceso. Si crea una directiva para cada tipo de lista, se recomienda nombrar cada directiva de manera explícita, para saber qué directiva se aplica exactamente a qué lista de aplicaciones concreta en XenMobile.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de plataforma

- **Directiva de acceso:** Haga clic en **Requerido**, **Sugerido** o **Prohibido**. El valor predeterminado es **Requerido**.
- Para agregar una o varias aplicaciones a la lista, haga clic en **Agregar** y lleve a cabo lo siguiente:
  - **Nombre de la aplicación:** Escriba el nombre de la aplicación.
  - **Identificador de la aplicación:** Escriba un identificador opcional de la aplicación.
  - Haga clic en **Guardar** o **Cancelar**.
  - Repita estos pasos para cada aplicación que quiera agregar.

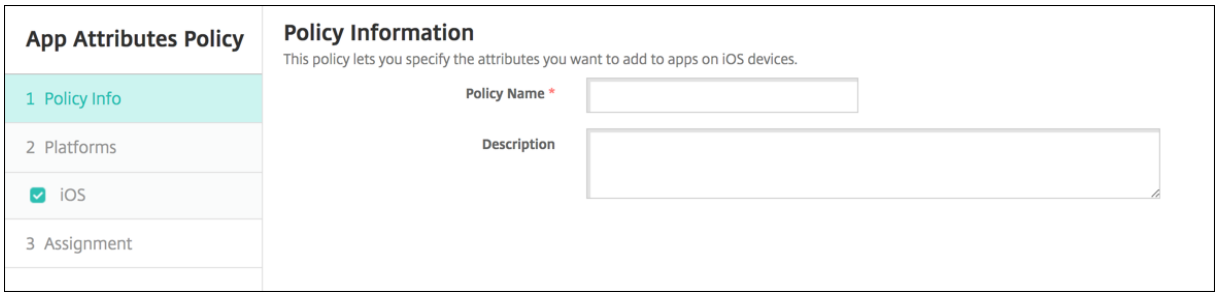
Directiva de atributos de aplicación

January 3, 2020

La directiva de atributos de aplicación permite especificar atributos (por ejemplo, un ID de paquete de aplicación administrada o un identificador de red VPN por aplicación) para dispositivos iOS.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS



- **ID de paquete de la aplicación administrada:** En la lista, haga clic en un ID de paquete de aplicación o en **Agregar nuevo**.
  - Si hace clic en **Agregar nuevo**, escriba el ID del paquete de aplicación en el campo que aparece.
- **Identificador de VPN por aplicación:** En la lista, haga clic en el identificador de red VPN destinado a cada aplicación.

Directiva de configuración de aplicaciones

January 4, 2022

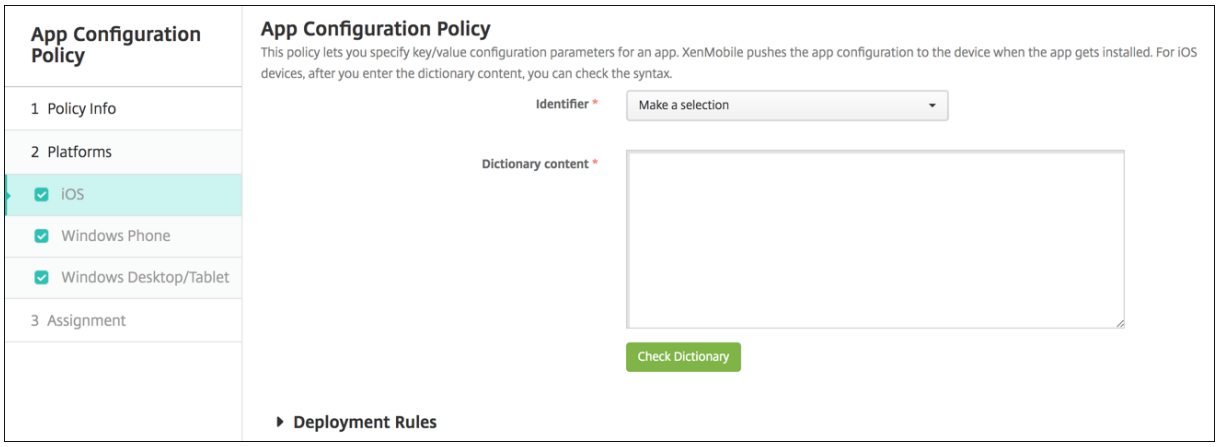
Puede configurar, de forma remota, aplicaciones que admitan la configuración administrada. Para ello, debe implementar:

- Un archivo de configuración XML (llamado lista de propiedades o plist) en los dispositivos iOS.
- O pares de clave/valor para teléfonos con Windows 10 o tabletas o equipos de escritorio con Windows 10 o Windows 11.

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.

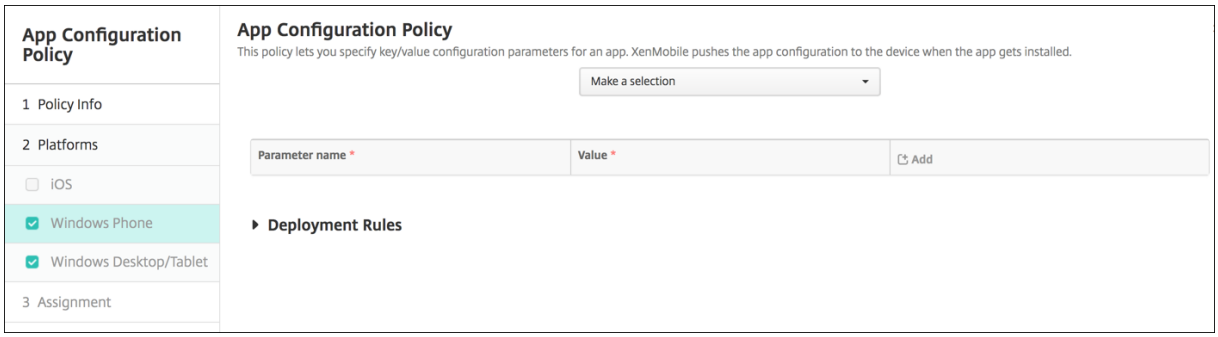
Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

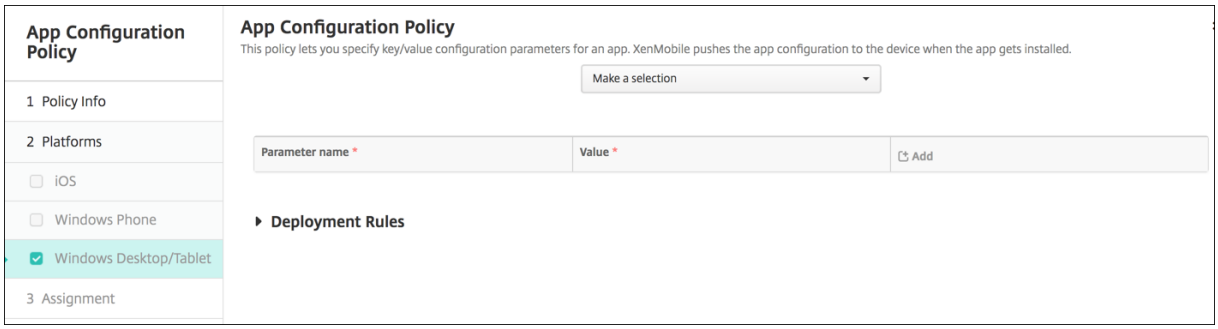
Parámetros de iOS



- **Identificador:** En la lista, haga clic en la aplicación que quiera configurar, o bien haga clic en **Agregar nuevo** para agregar una nueva aplicación a la lista.
  - Si hace clic en **Agregar nuevo**, escriba el identificador de la aplicación en el campo que aparece.
- **Contenido del diccionario:** Escriba, o copie y pegue, la información de configuración de la lista de propiedades XML (plist).
- Haga clic en **Diccionario de comprobación**. XenMobile verifica el archivo XML. Si no hay errores, verá **XML válido** bajo el cuadro de contenido. Si apareciera algún error de sintaxis bajo el cuadro de contenido, deberá corregirlo antes de continuar.

Parámetros de escritorios, tabletas y teléfonos Windows





- En la lista **Seleccionar**, haga clic en la aplicación que quiera configurar, o bien haga clic en **Agregar nuevo** para agregar una nueva aplicación a la lista.
  - Si hace clic en **Agregar nuevo**, escriba el nombre de familia del paquete en el campo que aparece.
- Haga clic en **Agregar** para agregar cada parámetro de configuración y lleve a cabo lo siguiente:
  - **Nombre del parámetro:** Escriba el nombre clave de un parámetro de aplicación para el dispositivo Windows. Para obtener más información acerca de los parámetros de aplicación de Windows, consulte la documentación de Microsoft.
  - **Valor:** Escriba el valor del parámetro especificado.
  - Haga clic en **Agregar** para agregar el parámetro, o bien haga clic en **Cancelar** para no agregarlo.

Directiva de inventario de aplicaciones

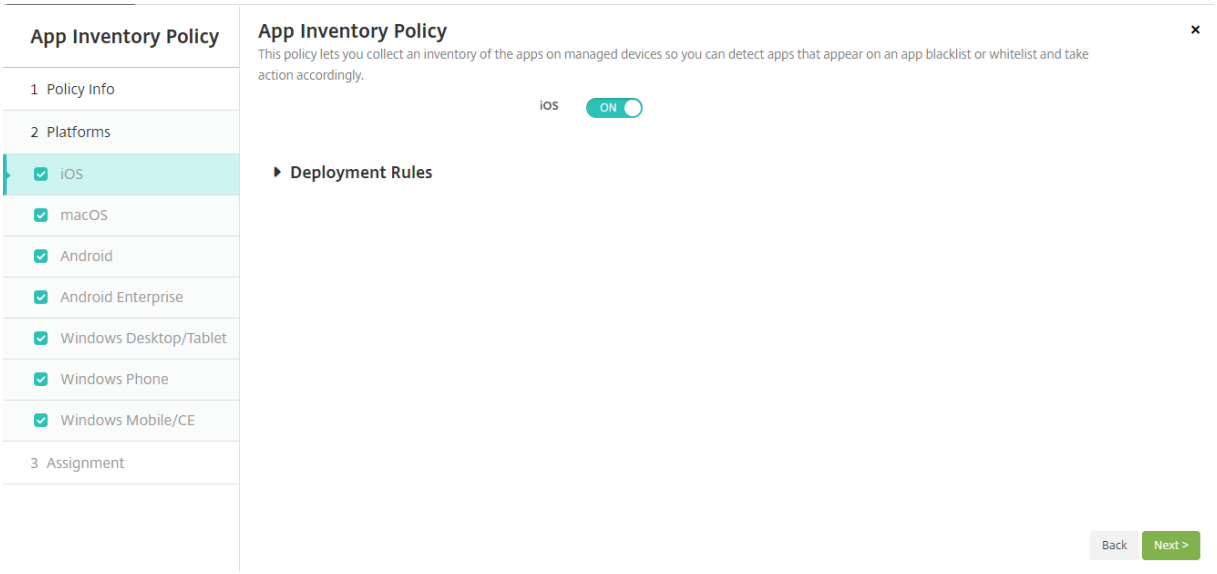
January 4, 2022

La directiva “Inventario de aplicaciones” permite realizar un inventario de las aplicaciones presentes en los dispositivos administrados. Una vez realizado el inventario, XenMobile puede cotejarlo con las directivas de acceso a aplicaciones que se hayan implementado en esos dispositivos. De esta manera, puede detectar aplicaciones que aparecen en una lista de aplicaciones permitidas o en una lista de aplicaciones bloqueadas y actuar en consecuencia.

Puede crear directivas de acceso a aplicaciones para dispositivos iOS, macOS, Android, Android Enterprise, tabletas y escritorios Windows, Windows Mobile/CE y Windows Phone.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de plataforma



- Para cada plataforma que seleccione, deje el valor predeterminado o **desactive** la opción. Está **activado** de forma predeterminada.

Directiva de bloqueo de aplicaciones

January 4, 2022

La directiva “Bloqueo de aplicaciones” permite definir una lista de las aplicaciones que se pueden ejecutar o una lista de aquellas aplicaciones que no se pueden ejecutar en un dispositivo. Puede configurar esta directiva para dispositivos Android y iOS, pero su funcionamiento difiere según la plataforma. Por ejemplo, no se pueden bloquear múltiples aplicaciones en un dispositivo iOS.

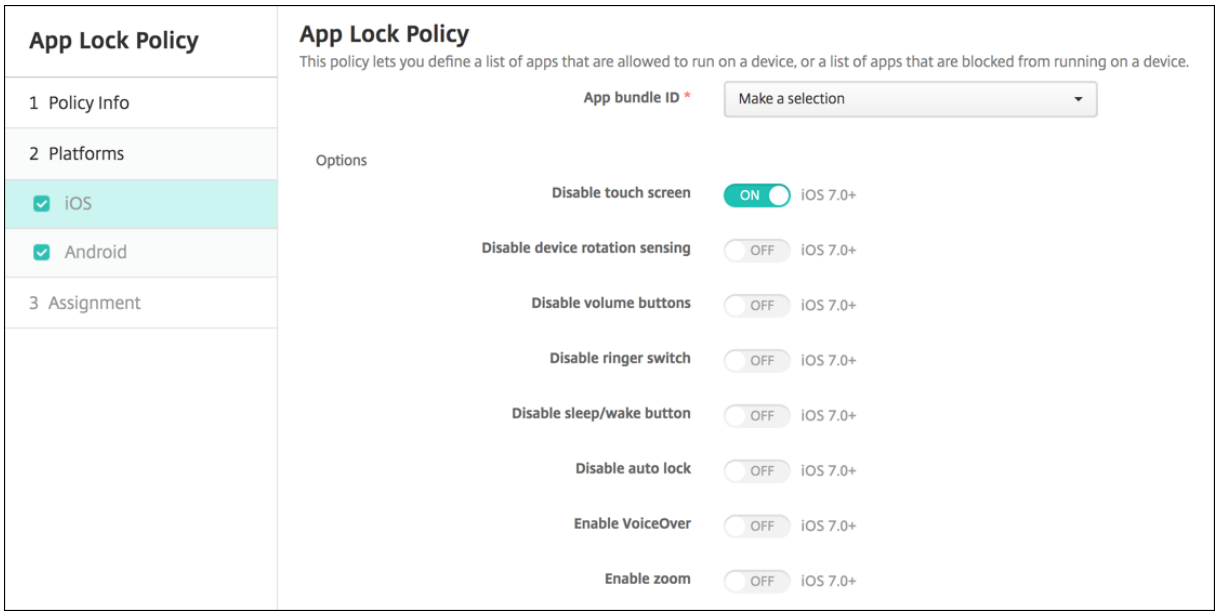
Además, en dispositivos iOS, solo se puede seleccionar una aplicación iOS en cada directiva. Lo que significa que los usuarios solo pueden usar su dispositivo para ejecutar una aplicación. Por tanto, no pueden realizar ninguna otra actividad en el dispositivo, excepto las opciones que usted permita específicamente cuando aplique la directiva Bloqueo de aplicaciones.

Además, los dispositivos iOS deben estar supervisados para poder enviarles las directivas Bloqueo de aplicaciones.

Aunque la directiva funcione en la mayoría de dispositivos Android L y M, el bloqueo de aplicaciones no funciona en dispositivos Android N ni versiones posteriores porque Google dejó de desarrollar la API necesaria.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS



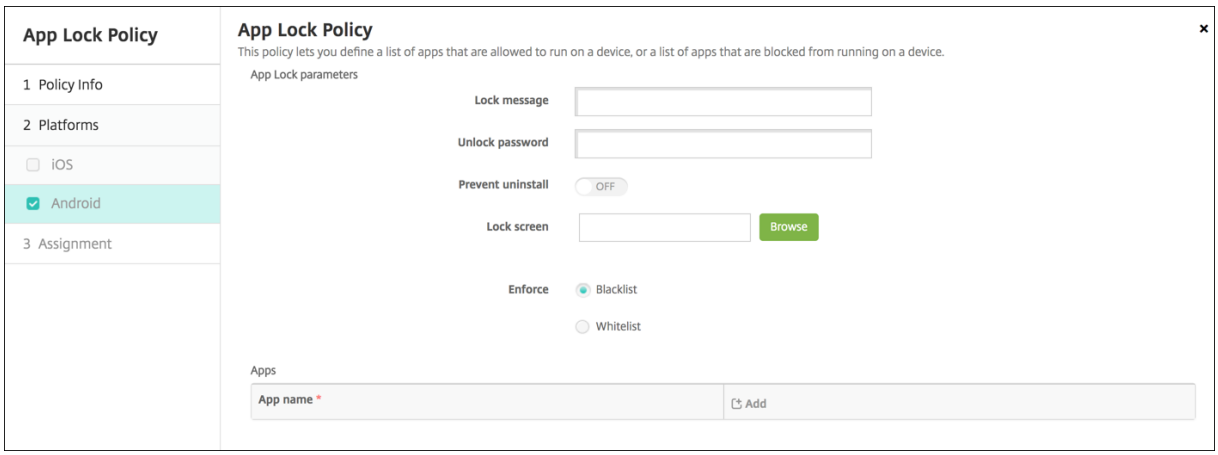
- **ID de paquete de la aplicación:** En la lista, haga clic en la aplicación a la que se aplica esta directiva, o bien haga clic en **Agregar nuevo** para agregar una nueva aplicación a la lista. Si hace clic en **Agregar nuevo**, escriba el nombre de la aplicación en el campo que aparece.
- **Opciones:** Todas las opciones siguientes solo se aplican a iOS 7.0 o versiones posteriores. Todas ellas están **desactivadas** de forma predeterminada, excepto “Inhabilitar pantalla táctil”, **activada** de forma predeterminada.
  - Inhabilitar pantalla táctil
  - Inhabilitar detección de rotación de dispositivo
  - Inhabilitar botones de volumen
  - Inhabilitar botón de timbre

    Si Inhabilitar botón de timbre está **activado**, los tonos dependen de la posición que tenía el modificador cuando se inhabilitó.
  - Inhabilitar botón de reposo/activación
  - Inhabilitar bloqueo automático
  - Inhabilitar VoiceOver
  - Habilitar zoom
  - Habilitar la inversión de colores

  - Habilitar AssistiveTouch
  - Habilitar Leer selección
  - Habilitar Audio mono
- **Opciones habilitadas por los usuarios:** Todas las siguientes opciones solo se aplican a iOS 7.0 o versiones posteriores. Todas ellas están **desactivadas** de forma predeterminada.
  - Permitir ajuste de VoiceOver
  - Permitir ajuste de zoom
  - Permitir ajuste de inversión de colores
  - Permitir ajuste de AssistiveTouch
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de Android

> **Nota:**
>
> No puede bloquear la aplicación Ajustes de Android mediante la directiva Bloqueo de aplicaciones.



- **Parámetros de la directiva Bloqueo de aplicaciones**
  - **Mensaje de bloqueo:** Escriba el mensaje que verán los usuarios cuando intenten abrir una aplicación bloqueada.
  - **Contraseña de desbloqueo:** Escriba la contraseña para desbloquear la aplicación.
  - **Impedir desinstalación:** Seleccione si permitir a los usuarios desinstalar aplicaciones.

Está **desactivado** de forma predeterminada.
- **Pantalla de bloqueo:** Seleccione la imagen que aparecerá en la pantalla de bloqueo del dispositivo. Para ello, haga clic en Examinar y vaya a la ubicación del archivo.
- **Aplicar:** Haga clic en **Lista negra** para crear una lista de las aplicaciones que no se pueden ejecutar en los dispositivos, o bien haga clic en **Lista blanca** para crear una lista de las aplicaciones que se pueden ejecutar en los dispositivos.

> **Nota:**
> La consola de XenMobile Server contiene los términos “lista negra” y “lista blanca”. Estamos cambiando esos términos en una próxima versión a “lista de bloqueados” y “lista de permitidos”.

- **Aplicaciones:** Haga clic en **Agregar** y lleve a cabo lo siguiente:
  - **Nombre de la aplicación:** 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 **Agregar nuevo** para agregar una nueva aplicación a la lista de las aplicaciones disponibles.
  - Si hace clic en **Agregar nuevo**, escriba el nombre de la aplicación en el campo que aparece.
  - Haga clic en **Guardar** o **Cancelar**.
  - Repita estos pasos para cada aplicación que quiera agregar a las listas de aplicaciones permitidas o prohibidas.

Directiva de uso de red de las aplicaciones

January 4, 2022

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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Permitir itinerancia de datos móviles:** Seleccione si las aplicaciones indicadas pueden usar una conexión de datos móviles durante la itinerancia. Está **desactivado** de forma predeterminada.

- **Permitir datos móviles:** Seleccione si las aplicaciones especificadas pueden usar la conexión de datos móviles. Está **desactivado** de forma predeterminada.
- **Coincidencias de identificador de aplicación:** Haga clic en **Agregar** para agregar cada aplicación a la lista y haga lo siguiente:
  - **Identificador de la aplicación:** Escriba un identificador de la aplicación.
  - Haga clic en **Guardar** para guardar la aplicación en la lista, o bien haga clic en **Cancelar** para no guardarla.

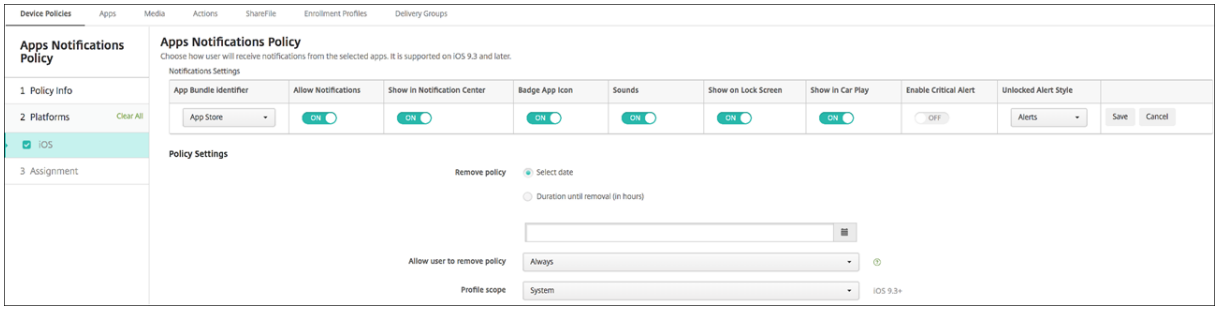
Directiva de notificaciones de aplicaciones

January 4, 2022

La directiva de notificaciones de aplicaciones permite controlar cómo reciben los usuarios de iOS las notificaciones provenientes de las aplicaciones especificadas. Esta directiva se admite en dispositivos que ejecutan iOS 9.3 o versiones posteriores.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS



- **Identificador de paquete de aplicación:** Especifique las aplicaciones a las que aplicar esta directiva.
- **Permitir notificaciones:** Debe **activar** esta opción para permitir las notificaciones.
- **Mostrar en el Centro de notificaciones:** Debe **activar** esta opción para mostrar notificaciones en el Centro de notificaciones de los dispositivos de usuario.
- **Insignia en icono de aplicación:** Debe **activar** esta opción para que aparezca una insignia en el icono de la aplicación con las notificaciones.
- **Sonidos:** Debe **activar** esta opción para incluir sonidos en las notificaciones.
- **Mostrar en pantalla de bloqueo:** Debe **activar** esta opción para mostrar notificaciones en la pantalla de bloqueo de los dispositivos de usuario.

- **Mostrar en CarPlay:** Si está **activado**, se muestran notificaciones en Apple CarPlay. Disponible en iOS 12 y versiones posteriores. De forma predeterminada, está **activado**.
- **Habilitar alerta crítica:** Si está **activado**, permite que una aplicación marque una notificación como crítica, con lo que esa aplicación ignora los parámetros de No molestar y de tono. Disponible en iOS 12 y versiones posteriores. Está **desactivado** de forma predeterminada.
- **Estilo de alerta en desbloqueo:** En la lista, seleccione **Ninguno**, **Pancarta** o **Alertas** para configurar la apariencia de las alertas mientras el dispositivo está desbloqueado.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible en iOS 9.3 y versiones posteriores.

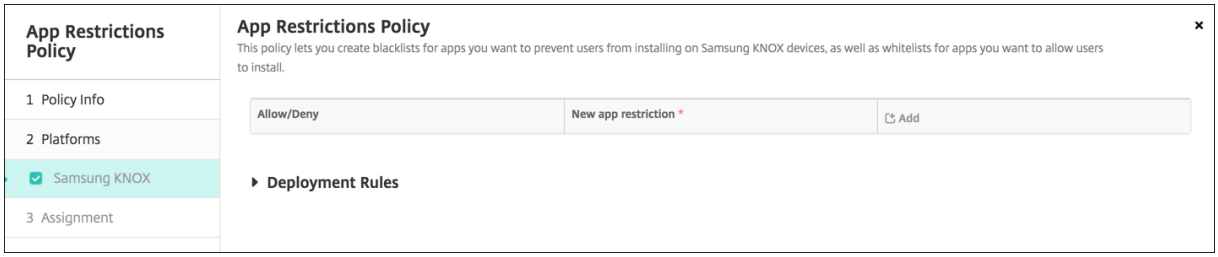
Directiva de restricciones a aplicaciones

July 10, 2020

Puede crear listas de bloqueados para las aplicaciones que quiere impedir que los usuarios instalen en dispositivos Samsung Knox. También puede crear listas de aplicaciones para aquellas aplicaciones que quiera permitir instalar a los usuarios.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Samsung Knox



Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada aplicación a la lista Permitir o Denegar:

- **Permitir/Denegar:** Seleccione si permitir a los usuarios instalar la aplicación.
- **Nueva restricción de aplicación:** Escriba el ID del paquete de la aplicación; por ejemplo, com.kmdm.af.crackle.
- Haga clic en **Guardar** para guardar la aplicación en la lista Permitir/Denegar, o bien haga clic en **Cancelar** para no guardarla.

Directiva de túnel de aplicaciones

January 4, 2022

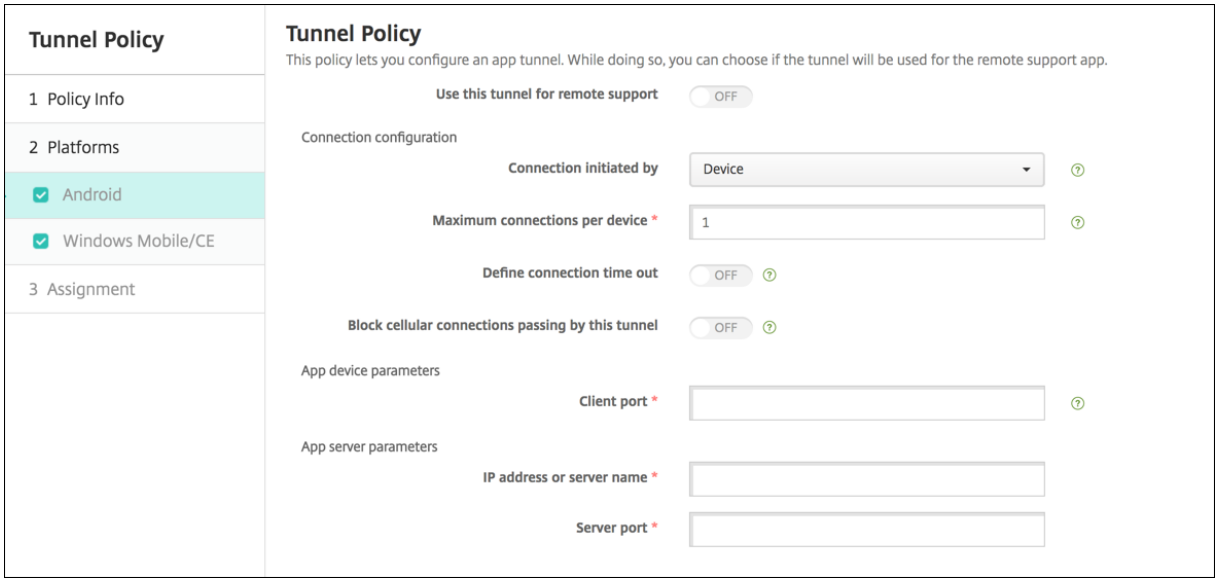
> **Importante:**
>
> La directiva "Túneles de aplicaciones" solo se usa para Remote Support. Para obtener más información acerca de Remote Support, consulte Opciones de asistencia y Remote Support. Remote Support no está disponible para nuevos clientes desde el 1 de enero de 2019. Los clientes existentes pueden seguir utilizando el producto, pero Citrix no proporcionará mejoras ni correcciones.

Los túneles de aplicaciones están diseñados 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. Puede configurar la directiva Túneles de aplicaciones para dispositivos Android y Windows Mobile/CE.

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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Android



- **Usar este túnel para la asistencia remota.** Seleccione si el túnel se usará para la asistencia remota.

  Los pasos de configuración son distintos según si se selecciona la asistencia remota o no.

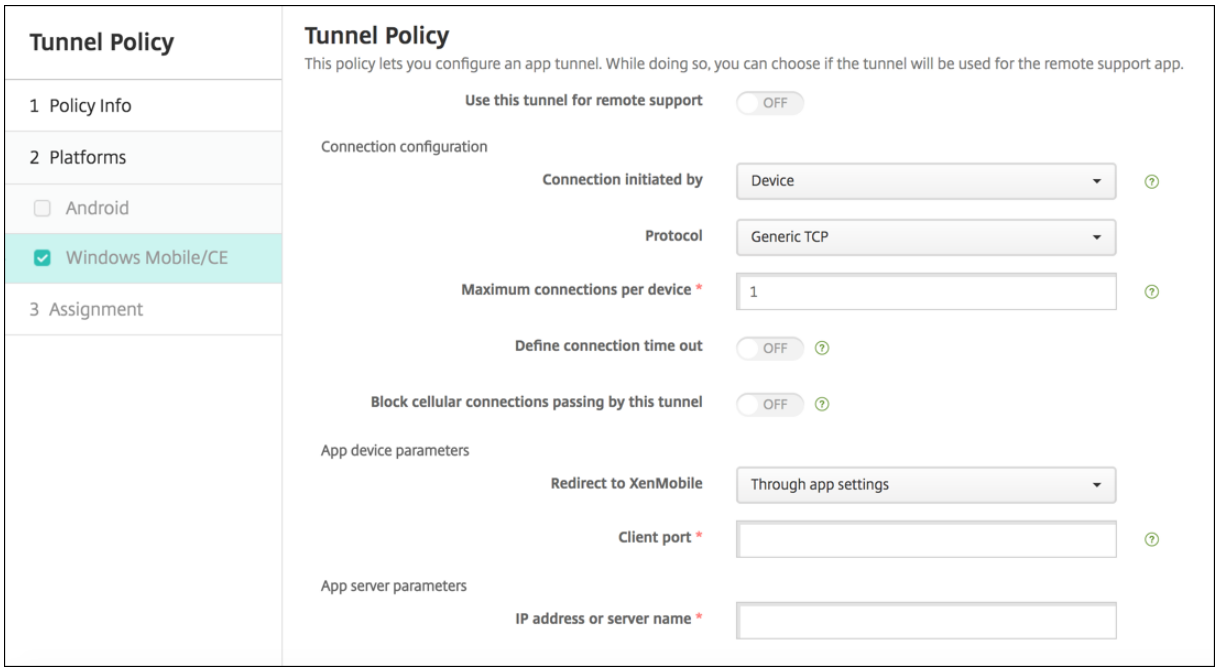
- Si no selecciona la asistencia remota, lleve a cabo lo siguiente:
  - **Conexión iniciada por.** Haga clic en **Dispositivo** o **Servidor** para indicar la fuente que inicia la conexión.
  - **Conexiones máximas por dispositivo:** Escriba la cantidad de conexiones TCP simultáneas que puede establecer la aplicación. Este campo solo se aplica a conexiones iniciadas desde un dispositivo.
  - **Definir el tiempo de espera de la conexión:** Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
    - **Tiempo de espera de la conexión.** Si **activa** el parámetro **Definir el tiempo de espera de la conexión**, escriba la cantidad de tiempo en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
  - **Bloquear el paso de las conexiones de móvil por este túnel.** Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en el modo de itinerancia.

    > **Nota:**
    >
    > Las conexiones Wi-Fi y USB no se bloquearán.

  - **Puerto cliente:** Escriba el número de puerto del cliente. En la mayoría de los casos, este es el mismo valor que el del puerto del servidor.

  - **Dirección IP o nombre del servidor.** Escriba el nombre o la dirección IP del servidor de aplicaciones. Este campo solo se aplica a conexiones iniciadas desde un dispositivo.
  - **Puerto del servidor.** Escriba el número de puerto del servidor.
- Si selecciona la asistencia remota, lleve a cabo lo siguiente:
  - **Usar este túnel para la asistencia remota.** Establezca esta opción en **Sí**.
  - **Definir el tiempo de espera de la conexión:** Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
    * **Tiempo de espera de la conexión.** Si **activa** el parámetro **Definir el tiempo de espera de la conexión**, escriba la cantidad de tiempo en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
  - **Usar conexión SSL.** Seleccione si usar una conexión SSL segura para este túnel.
  - **Bloquear el paso de las conexiones de móvil por este túnel.** Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en el modo de itinerancia. Esta configuración no bloquea las conexiones Wi-Fi y USB.

Parámetros de Windows Mobile/CE



- **Usar este túnel para la asistencia remota.** Seleccione si el túnel se usará para la asistencia remota.

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:

- **Conexión iniciada por.** Haga clic en **Dispositivo** o **Servidor** para indicar la fuente que inicia la conexión.
- **Protocolo.** En la lista, haga clic en el protocolo que se va a utilizar. El valor predeterminado es **TCP genérico**.
- **Conexiones máximas por dispositivo:** Escriba la cantidad de conexiones TCP simultáneas que puede establecer la aplicación. Este campo solo se aplica a conexiones iniciadas desde un dispositivo.
- **Definir el tiempo de espera de la conexión:** Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
  - **Tiempo de espera de la conexión.** Si **activa** el parámetro **Definir el tiempo de espera de la conexión**, escriba la cantidad de tiempo en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
- **Bloquear el paso de las conexiones de móvil por este túnel.** Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en el modo de itinerancia.

  > **Nota:**
  > Las conexiones Wi-Fi y USB no se bloquearán.

- **Redirigir a XenMobile.** En la lista, haga clic en la forma en que se conecta el dispositivo a XenMobile. El valor predeterminado es **A través de parámetros de la aplicación**.
  - Si selecciona **Con un alias local**, escriba el alias en **Alias local**. El valor predeterminado es **localhost**.
  - Si selecciona **Un intervalo de direcciones IP**, escriba la dirección IP inicial del intervalo en **Desde la dirección IP** y la dirección IP final del intervalo en **Hasta la dirección IP**.
- **Puerto cliente:** Escriba el número de puerto del cliente. En la mayoría de los casos, este es el mismo valor que el del puerto del servidor.
- **Dirección IP o nombre del servidor.** Escriba el nombre o la dirección IP del servidor de aplicaciones. Este campo solo se aplica a conexiones iniciadas desde un dispositivo.
- **Puerto del servidor.** Escriba el número de puerto del servidor.

- Si selecciona la asistencia remota, lleve a cabo lo siguiente:
  - **Usar este túnel para la asistencia remota.** Establezca esta opción en **Sí**.
  - **Definir el tiempo de espera de la conexión:** Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
    - **Tiempo de espera de la conexión.** Si **activa** el parámetro **Definir el tiempo de espera de la conexión**, escriba la cantidad de tiempo en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
  - **Usar conexión SSL.** Seleccione si usar una conexión SSL segura para este túnel.
  - **Bloquear el paso de las conexiones de móvil por este túnel.** Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en el modo de itinerancia. Las conexiones Wi-Fi y USB no se bloquean.

Directiva de desinstalación de aplicaciones

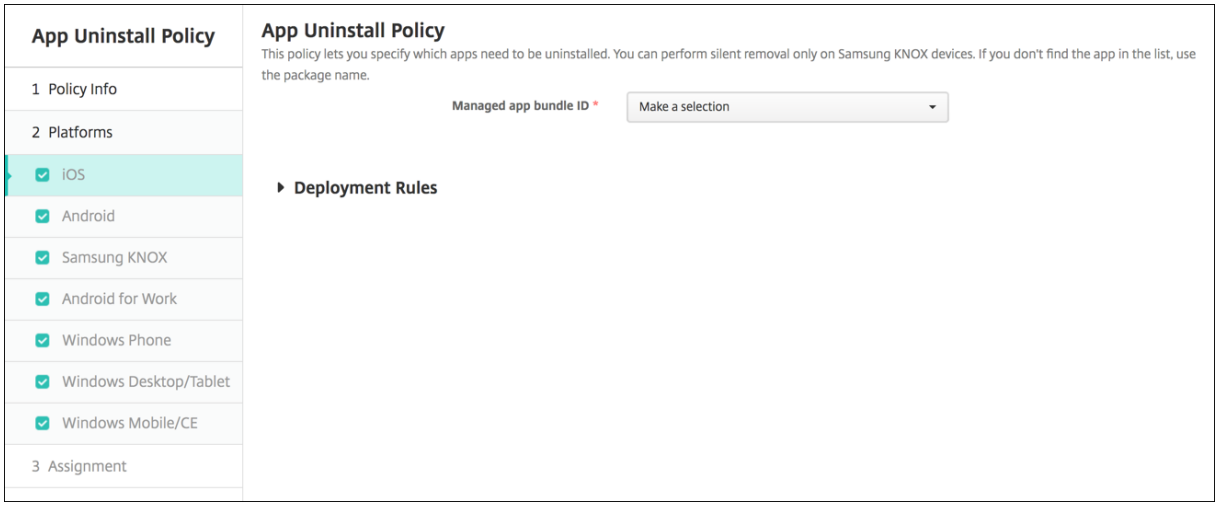
January 4, 2022

Puede crear una directiva “Desinstalación de aplicaciones” para las plataformas iOS, Android, Samsung Knox, Android Enterprise, escritorios y tabletas Windows y Windows Mobile/CE. Una directiva Desinstalación de aplicaciones permite quitar aplicaciones de los dispositivos de usuario por varias razones. Por ejemplo, puede que ya no quiera ofrecer soporte a 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).

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS



- **ID de paquete de la aplicación administrada:** En la lista, haga clic en una aplicación existente o en **Agregar nuevo**. Si no hay ninguna aplicación configurada para esta plataforma, la lista estará vacía y deberá agregar una nueva aplicación.
  - Cuando haga clic en **Agregar**, aparecerá un campo donde podrá escribir un nombre de aplicación.

Parámetros de todas las demás plataformas

- **Aplicaciones que desinstalar:** Haga clic en **Agregar** y lleve a cabo lo siguiente para cada aplicación que quiera agregar:
  - **Nombre de la aplicación:** En la lista, haga clic en una aplicación existente, o bien haga clic en **Agregar nuevo** 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 **Agregar** para agregar la aplicación, o bien haga clic en **Cancelar** para no agregarla.

Desinstalación automática de una aplicación empresarial después de instalarse la aplicación correspondiente de la tienda pública

Puede configurar XenMobile para que quite la versión de empresa de las aplicaciones Citrix cuando se instale la versión correspondiente desde una tienda pública de aplicaciones. Esta función impide que los dispositivos de usuario muestren dos iconos de aplicación idénticos después de instalar la versión de la tienda pública de aplicaciones.

Una condición de implementación para la directiva Desinstalación de aplicaciones hace que XenMobile quite de los dispositivos la versión antigua de una aplicación cuando se instala la versión nueva. Esta función solo está disponible para dispositivos iOS administrados conectados a XenMobile Server en modo Enterprise (XME).

Para configurar una regla de implementación mediante como condición el nombre de la aplicación instalada:

- Especifique el **ID de paquete de la aplicación administrada** para la aplicación empresarial.
- Para agregar una regla, haga clic en **Nueva regla** y, a continuación, como se muestra en el ejemplo, elija **Nombre de la aplicación instalada** y **es igual que**. Escriba el ID del paquete de la aplicación de tienda pública de aplicaciones.

En el ejemplo, cuando la aplicación de la tienda pública de aplicaciones (com.citrix.mail.ios) se instala en un dispositivo de los grupos de entrega especificados, XenMobile quita la versión de empresa de esa aplicación (com.citrix.mail).

Directiva de restricciones de desinstalación de aplicaciones

January 3, 2020

Puede especificar las aplicaciones que los usuarios pueden o no pueden instalarse en un dispositivo Amazon o Samsung SAFE.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Samsung SAFE o Amazon

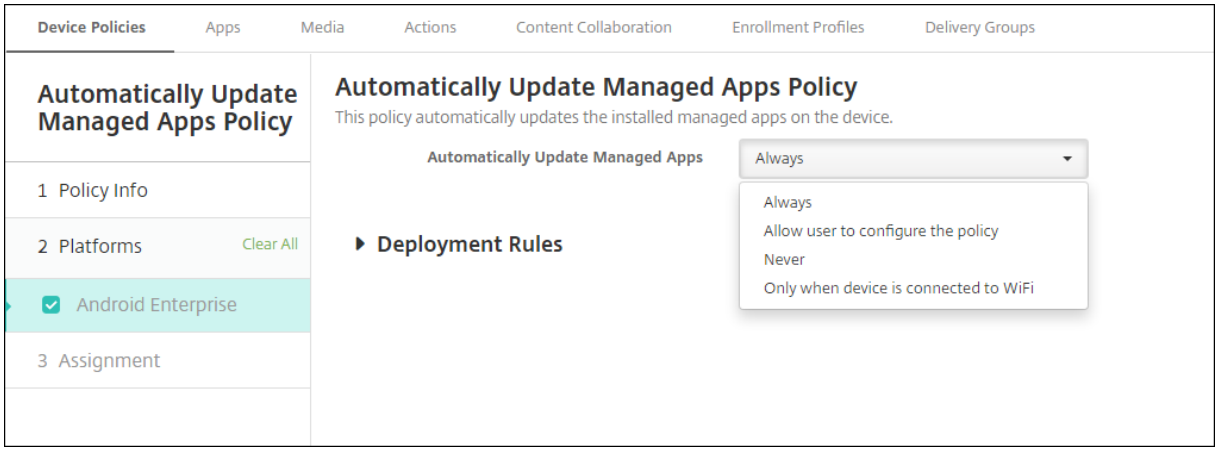
- **Parámetros de restricción a la desinstalación de aplicaciones.** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada regla:
  - **Nombre de la aplicación:** En la lista, haga clic en una aplicación, o bien haga clic en **Agregar nuevo** para agregar una nueva aplicación.
  - **Regla:** Seleccione si los usuarios pueden desinstalar la aplicación. El valor predeterminado es permitir la desinstalación.
  - Haga clic en **Guardar** o **Cancelar**.

Directiva de dispositivo para actualizar automáticamente aplicaciones administradas

January 4, 2022

Esta directiva controla cómo se actualizan en dispositivos Android Enterprise las aplicaciones administradas instaladas. Se puede restringir la capacidad de los usuarios de permitir la actualización automática de aplicaciones en sus dispositivos. Si permite que los usuarios controlen la actualización automática de aplicaciones en sus dispositivos, ellos establecen las directivas de actualización automática de aplicaciones en la tienda Google Play administrada.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.



Configure **Actualizar automáticamente aplicaciones administradas**.

- **Siempre:** Habilita la actualización automática de aplicaciones. **Siempre** es el valor predeterminado.
- **Permitir que el usuario configure la directiva:** Permite que el usuario configure la directiva de actualización automática de aplicaciones para el dispositivo en la tienda Google Play administrada.
- **Nunca:** Inhabilita la actualización automática de aplicaciones.
- **Solo cuando el dispositivo está conectado a una red Wi-Fi:** Permite la actualización automática de aplicaciones solo cuando el dispositivo está conectado a una red Wi-Fi.

Directiva de BitLocker

January 4, 2022

Windows 10 y Windows 11 incluyen una función de cifrado de disco llamada BitLocker, que proporciona protección adicional a archivos y al sistema frente al acceso no autorizado en un dispositivo Windows extraviado o robado. Para obtener una mayor protección, puede usar BitLocker con chips del Módulo de plataforma segura (TPM), versión 1.2 o posterior. Un chip TPM gestiona las operaciones de cifrado. Asimismo, genera, almacena y limita el uso de claves de cifrado.

A partir de Windows 10, compilación 1703, se puede controlar BitLocker mediante las directivas MDM. En XenMobile, puede usar la directiva BitLocker para configurar los parámetros disponibles en el Asistente de BitLocker en dispositivos con Windows 10 y Windows 11. Por ejemplo, en un dispositivo con BitLocker habilitado, BitLocker puede pedir a los usuarios cómo quieren desbloquear sus unidades de disco durante el inicio del sistema, cómo quieren crear copias de seguridad de su clave de recuperación y cómo quieren desbloquear una unidad fija. Con la directiva de BitLocker, también se puede configurar si:

- Habilitar BitLocker en dispositivos que no tienen chip TPM.
- Mostrar opciones de recuperación en la interfaz de BitLocker.
- Denegar el acceso de escritura en una unidad fija o extraíble cuando BitLocker no está habilitado.

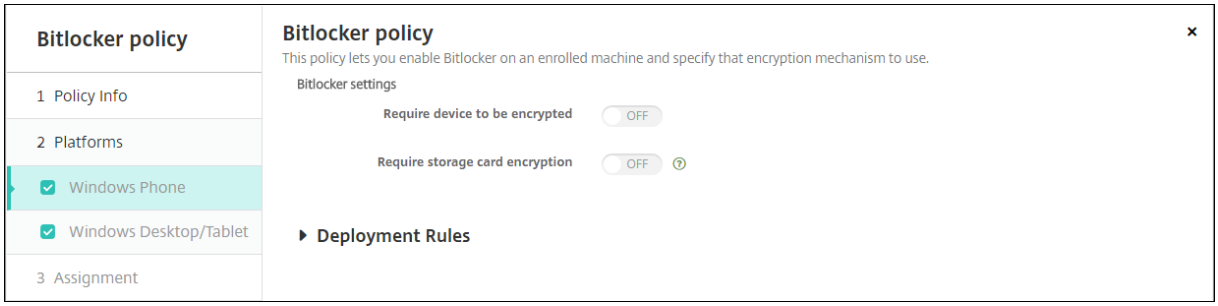
> **Nota:**
>
> Una vez que el cifrado de BitLocker se haya iniciado en un dispositivo, no puede cambiar la configuración de BitLocker con la implementación de una directiva de BitLocker actualizada.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos

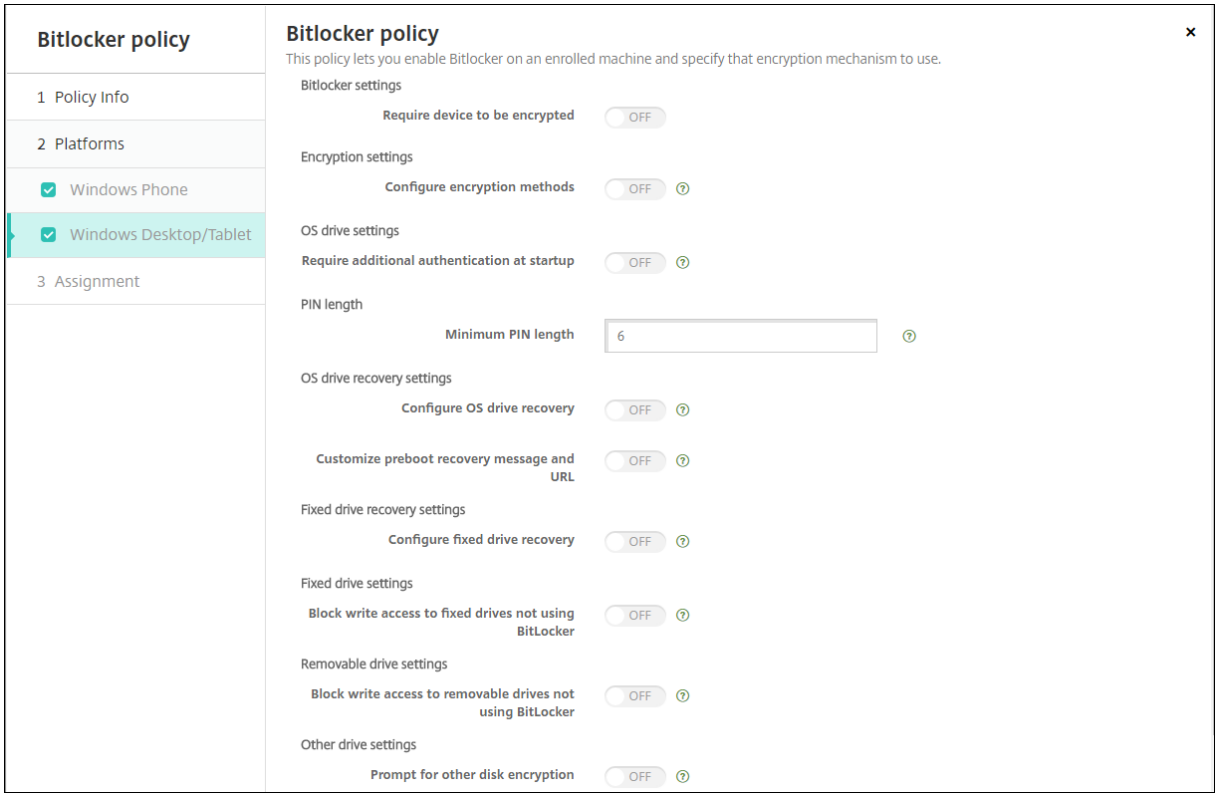
- La directiva de BitLocker requiere las ediciones Enterprise de Windows 10 o Windows 11.
- Antes de implementar la directiva de BitLocker, prepare el entorno para BitLocker. Para obtener información detallada de Microsoft, incluidos la configuración y los requisitos del sistema para BitLocker, consulte BitLocker y los artículos de ese nodo.

Parámetros de Windows Phone



- **Requerir cifrado del dispositivo:** Determina si solicitar a los usuarios que habiliten el cifrado de BitLocker en una tarjeta del sistema Windows Phone. Si tiene el valor **Sí**, los dispositivos muestran un mensaje, una vez finalizada la inscripción, que indica que la empresa requiere el cifrado del dispositivo. Si el usuario opta por no cifrar el dispositivo, no se le concede acceso de escritura en la tarjeta del sistema. Si tiene el valor **No**, el usuario no ve solicitudes y la directiva de BitLocker determina si el dispositivo se cifra o no. Está **desactivado** de forma predeterminada.
- **Requerir cifrado de tarjeta de almacenamiento:** Determina si solicitar a los usuarios que habiliten el cifrado de BitLocker en una tarjeta de almacenamiento Windows Phone. Si tiene el valor **Sí**, se requiere el cifrado de las tarjetas de almacenamiento para obtener el permiso de escritura en la tarjeta. Está **desactivado** de forma predeterminada.

Parámetros de tabletas y escritorios Windows



- **Requerir cifrado del dispositivo:** Determina si solicitar a los usuarios que habiliten el cifrado de BitLocker en escritorios y tabletas Windows. Si tiene el valor **Sí**, los dispositivos muestran un mensaje, una vez finalizada la inscripción, que indica que la empresa requiere el cifrado del dispositivo. Si tiene el valor **No**, el usuario no ve solicitudes y BitLocker usa los parámetros de la directiva. Está **desactivado** de forma predeterminada.
- **Configurar métodos de cifrado:** Determina los métodos de cifrado que se utilizarán para los tipos concretos de unidades. Si tiene el valor **No**, el Asistente de BitLocker pide al usuario el método de cifrado que se utilizará para el tipo de unidad. El método predeterminado para el cifrado de todas las unidades es XTS-AES de 128 bits. El método predeterminado para el cifrado de las unidades extraíbles es AES-CBC de 128 bits. Si se **activa**, BitLocker utiliza el método de cifrado especificado en la directiva. Asimismo, si se **activa**, aparecen los parámetros adicionales **Unidad del sistema operativo**, **Unidad fija** y **Unidad extraíble**. Elija el método predeterminado para el cifrado de cada tipo de unidad. Está **desactivado** de forma predeterminada.
- **Requerir autenticación adicional al inicio:** Especifica la autenticación adicional necesaria durante el inicio del dispositivo. También especifica si permitir que BitLocker esté presente en dispositivos que no tienen chip TPM. Si tiene el valor **No**, los dispositivos sin TPM no pueden utilizar el cifrado de BitLocker. Para obtener información acerca de TPM, consulte el artículo de Microsoft Información general sobre la tecnología del Módulo de plataforma segura. Si tiene el valor **Sí**, aparecen los siguientes parámetros adicionales. Está **desactivado** de forma predeter-

minada.

  - **Bloquear BitLocker en dispositivos sin chip TPM:** En un dispositivo sin chip TPM, BitLocker requiere que los usuarios creen una contraseña de desbloqueo o una clave de inicio. La clave de inicio se almacena en una unidad USB que el usuario debe conectar al dispositivo antes de iniciarlo. La contraseña de desbloqueo contiene un mínimo de ocho caracteres. Está **desactivado** de forma predeterminada.
  - **Inicio de TPM:** En un dispositivo con TPM, hay cuatro modos de desbloqueo: solo TPM, TPM + PIN, TPM + clave y TPM + PIN + clave. El inicio de TPM es para el modo solo TPM. En este modo, las claves de cifrado se almacenan en el chip TPM. Este modo no requiere que el usuario facilite más datos de desbloqueo. El dispositivo del usuario se desbloquea automáticamente durante el reinicio con la clave de cifrado obtenida del chip TPM. El valor predeterminado es **Permitir TPM**.
  - **PIN de inicio de TPM:** Este parámetro es el modo de desbloqueo TPM + PIN. Un PIN puede contener un máximo de 20 dígitos. Use el parámetro **Longitud mínima del PIN** para especificar la longitud mínima del PIN. El usuario configura un PIN durante la configuración de BitLocker y facilita ese PIN durante el inicio del dispositivo.
  - **Clave de inicio de TPM:** Este parámetro es el modo de desbloqueo TPM + clave. La clave de inicio se almacena en una unidad USB u otra unidad extraíble que el usuario debe conectar al dispositivo antes de iniciarlo.
  - **PIN y clave de inicio de TPM:** Este parámetro es el modo de desbloqueo TPM + PIN + clave.

    Si el desbloqueo se realiza correctamente, el sistema operativo empieza a cargarse. Si el desbloqueo falla, el dispositivo entra en el modo de recuperación.

- **Longitud mínima del PIN:** La longitud mínima que debe tener el PIN para el inicio de TPM. El valor predeterminado es **6**.
- **Configurar la recuperación de la unidad del SO:** Si se produce un error en el paso de desbloqueo, BitLocker pide al usuario la clave de recuperación configurada. Este parámetro configura las opciones de recuperación de unidades del sistema operativo disponibles para los usuarios si no tienen la contraseña de desbloqueo o la clave de inicio USB. Está **desactivado** de forma predeterminada.
  - **Permitir agente de recuperación de datos basado en certificado:** Especifica si permitir un agente de recuperación de datos basado en certificados. Agregue un agente de recuperación de datos desde las directivas de clave pública, ubicado en la Consola de administración de directivas de grupo (GPMC) o en el Editor de directivas de grupo local. Para obtener más información acerca de los agentes de recuperación de datos, consulte el artículo de Microsoft BitLocker Group Policy settings. Está **desactivado** de forma predeterminada.

  - **Crear contraseña de 48 bits para la recuperación de la unidad del SO:** Especifica si permitir o exigir que los usuarios usen una contraseña de recuperación. BitLocker genera la contraseña y la guarda en un archivo o una cuenta de Microsoft Cloud. El valor predeterminado es **Permitir contraseña de 48 bits**.
  - **Crear clave de recuperación de 256 bits:** Especifica si permitir o exigir que los usuarios usen una clave de recuperación. Una clave de recuperación es un archivo BEK, almacenado en una unidad USB. El valor predeterminado es **Permitir clave de recuperación de 256 bits**.
  - **Ocultar opciones de recuperación de unidad de SO:** Especifica si mostrar u ocultar las opciones de recuperación en la interfaz de BitLocker. Si se **activa**, no aparecen opciones de recuperación en la interfaz de BitLocker. En ese caso, registre los dispositivos en Active Directory, guarde las opciones de recuperación en Active Directory y **active** la opción **Guardar información de recuperación en AD DS**. Está **desactivado** de forma predeterminada.
  - **Guardar información de recuperación en AD DS:** Especifica si guardar las opciones de recuperación en Active Directory Domain Services. Está **desactivado** de forma predeterminada.
  - **Configurar información de recuperación guardada en AD DS:** Especifica si almacenar la contraseña de recuperación de BitLocker o el paquete de claves y la contraseña de recuperación en Active Directory Domain Services. Si almacena el paquete de claves, se admite la recuperación de datos desde una unidad que se haya dañado de físicamente. El valor predeterminado es **Contraseña de recuperación de copia de seguridad**.
  - **Habilitar BitLocker después de almacenar información de recuperación en AD DS:** Especifica si impedir que los usuarios habiliten BitLocker a menos que el dispositivo esté conectado por dominio y la copia de seguridad de la información de recuperación de BitLocker en Active Directory se haya realizado correctamente. Si se **activa**, el dispositivo debe estar unido a un dominio antes de iniciar BitLocker. Está **desactivado** de forma predeterminada.

- **Personalizar mensaje y URL de recuperación de preinicio:** Especifica si BitLocker muestra un mensaje y una dirección URL personalizados en la pantalla de recuperación. Si se **activa**, aparecen los siguientes parámetros adicionales: **Usar mensaje y URL de recuperación predeterminados**, **Usar mensaje y URL de recuperación vacíos**, **Usar mensaje de recuperación personalizado** y **Usar URL de recuperación personalizada**. Si se **desactiva**, aparece la URL y el mensaje de recuperación predeterminados. Está **desactivado** de forma predeterminada.
- **Configurar la recuperación de unidades fijas:** Configura las opciones de recuperación que tienen los usuarios para unidades fijas cifradas con BitLocker. BitLocker no muestra mensajes a los usuarios acerca del cifrado de la unidad fija. Para desbloquear una unidad durante el ini-

cio, un usuario suministra una contraseña o una tarjeta inteligente. Loa parámetros de desbloqueo de inicio (no incluidos en esta directiva), aparecen en la interfaz de BitLocker cuando un usuario habilita el cifrado de BitLocker en una unidad fija. Para obtener información sobre los parámetros relacionados, consulte la opción **Configurar la recuperación de la unidad del SO**, ya mencionada en esta lista. Está **desactivado** de forma predeterminada.

- **Bloquear acceso de escritura en unidades fijas que no usen BitLocker:** Si se **activa**, los usuarios solo pueden escribir en las unidades fijas cuando están cifradas con BitLocker. Está **desactivado** de forma predeterminada.
- **Bloquear acceso de escritura en unidades extraíbles que no usen BitLocker:** Si se **activa**, los usuarios solo pueden escribir en las unidades extraíbles cuando están cifradas con BitLocker. Configure este parámetro de acuerdo con el acceso de escritura que permite la organización en otras unidades extraíbles de la organización. Está **desactivado** de forma predeterminada.
- **Pedir otro cifrado de disco:** Permite inhabilitar el diálogo de advertencia para otro cifrado de disco en los dispositivos. Está **desactivado** de forma predeterminada.

Directiva de explorador web

January 4, 2022

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 web, 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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Samsung SAFE y Samsung Knox

- **Inhabilitar explorador web:** Seleccione esta opción para inhabilitar completamente el explorador web de Samsung en los dispositivos de los usuarios. El valor predeterminado es **No**, con lo que los usuarios pueden utilizar el explorador. Si inhabilita el explorador web, las siguientes opciones desaparecerán.
- **Inhabilitar ventanas emergentes:** Seleccione si permitir o no los mensajes emergentes en el explorador.
- **Inhabilitar JavaScript:** Seleccione si permitir o no que se ejecute JavaScript en el explorador.

- **Inhabilitar cookies:** Seleccione si permitir o no las cookies.
- **Inhabilitar autorrelleno:** Seleccionar si permitir a los usuarios activar la función de completado automático del explorador.
- **Forzar advertencia de fraude:** Seleccione si mostrar una advertencia cuando los usuarios visiten un sitio web fraudulento o no seguro.

Directiva de calendario (CalDAV)

January 4, 2022

En XenMobile, puede agregar una directiva para agregar una cuenta de calendarios (CalDAV) a los dispositivos iOS o macOS de los usuarios. De esta manera, los usuarios podrán sincronizar los datos de eventos programados con cualquier servidor que admita CalDAV.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Descripción de la cuenta:** Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Nombre de host:** Escriba la dirección del servidor CalDAV. Este campo es obligatorio.
- **Puerto:** Especifique el puerto por el que conectarse al servidor CalDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **URL principal:** Indique la URL base de acceso al calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña opcional de usuario.
- **Usar SSL:** Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CalDAV. Está **activado** de forma predeterminada.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de macOS

- **Descripción de la cuenta:** Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Nombre de host:** Escriba la dirección del servidor CalDAV. Este campo es obligatorio.
- **Puerto:** Especifique el puerto por el que conectarse al servidor CalDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **URL principal:** Indique la URL base de acceso al calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña opcional de usuario.
- **Usar SSL:** Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CalDAV. Está **activado** de forma predeterminada.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Directiva de red de telefonía móvil

January 4, 2022

Esta directiva permite configurar parámetros de redes de telefonía móvil en un dispositivo iOS.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Asociar APN**
  - **Nombre:** Escriba un nombre para esta configuración.
  - **Tipo de autenticación:** 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**.
  - En **Nombre de usuario** y **Contraseña**, introduzca el nombre de usuario y la contraseña para la autenticación.
- **APN**
  - **Nombre:** Escriba un nombre para la configuración del nombre de punto de acceso (APN).
  - **Tipo de autenticación:** En la lista, haga clic en **CHAP** o **PAP**. El valor predeterminado es **PAP**.
  - En **Nombre de usuario** y **Contraseña**, introduzca el nombre de usuario y la contraseña para la autenticación.
  - **Servidor proxy:** Escriba la dirección de red del servidor proxy.
  - **Puerto del servidor proxy:** Escriba el puerto del servidor proxy.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva de administrador de conexiones

January 3, 2020

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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Windows Mobile/CE

> **Nota:**
>
> La opción **Oficina integrada** significa que todas las conexiones se realizan a la intranet de la empresa. La opción **Internet integrado** significa que todas las conexiones se realizan a Internet.

- **Las aplicaciones que se conectan a una red privada usan automáticamente:** En la lista, haga clic en **Oficina integrada** o **Internet integrado**. El valor predeterminado es **Oficina integrada**.
- **Las aplicaciones que se conectan a Internet usan automáticamente:** En la lista, haga clic en **Oficina integrada** o **Internet integrado**. El valor predeterminado es **Oficina integrada**.

Directiva de programación de conexiones

January 4, 2022

> **Importante:**
>
> Citrix recomienda utilizar Firebase Cloud Messaging (FCM) para controlar las conexiones desde dispositivos Android, Android Enterprise y Chrome OS a XenMobile Server. Para obtener más información sobre el uso de FCM, consulte Firebase Cloud Messaging.

Si opta por no usar FCM, puede crear directivas de programación de conexiones para controlar cómo y cuándo se conectan los dispositivos de usuario a XenMobile Server.

Puede especificar que los usuarios conecten sus dispositivos manualmente o que los dispositivos se conecten dentro de un período de tiempo definido.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de plataforma

- **Requerir la conexión de los dispositivos:** Haga clic en la opción que quiera establecer para esta programación.
  - **Siempre:** Mantiene la conexión activa de forma permanente. La instancia de XenMobile en el dispositivo del usuario intenta volver a conectarse al servidor de 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 **Siempre**, use también la opción **Directiva de túnel** del dispositivo, con el valor **Definir el tiempo de espera de la conexión** para que la conexión no consuma toda la batería. Manteniendo la conexión activa, puede enviar comandos de seguridad, tales como borrado o bloqueo del dispositivo, a demanda. También debe se-

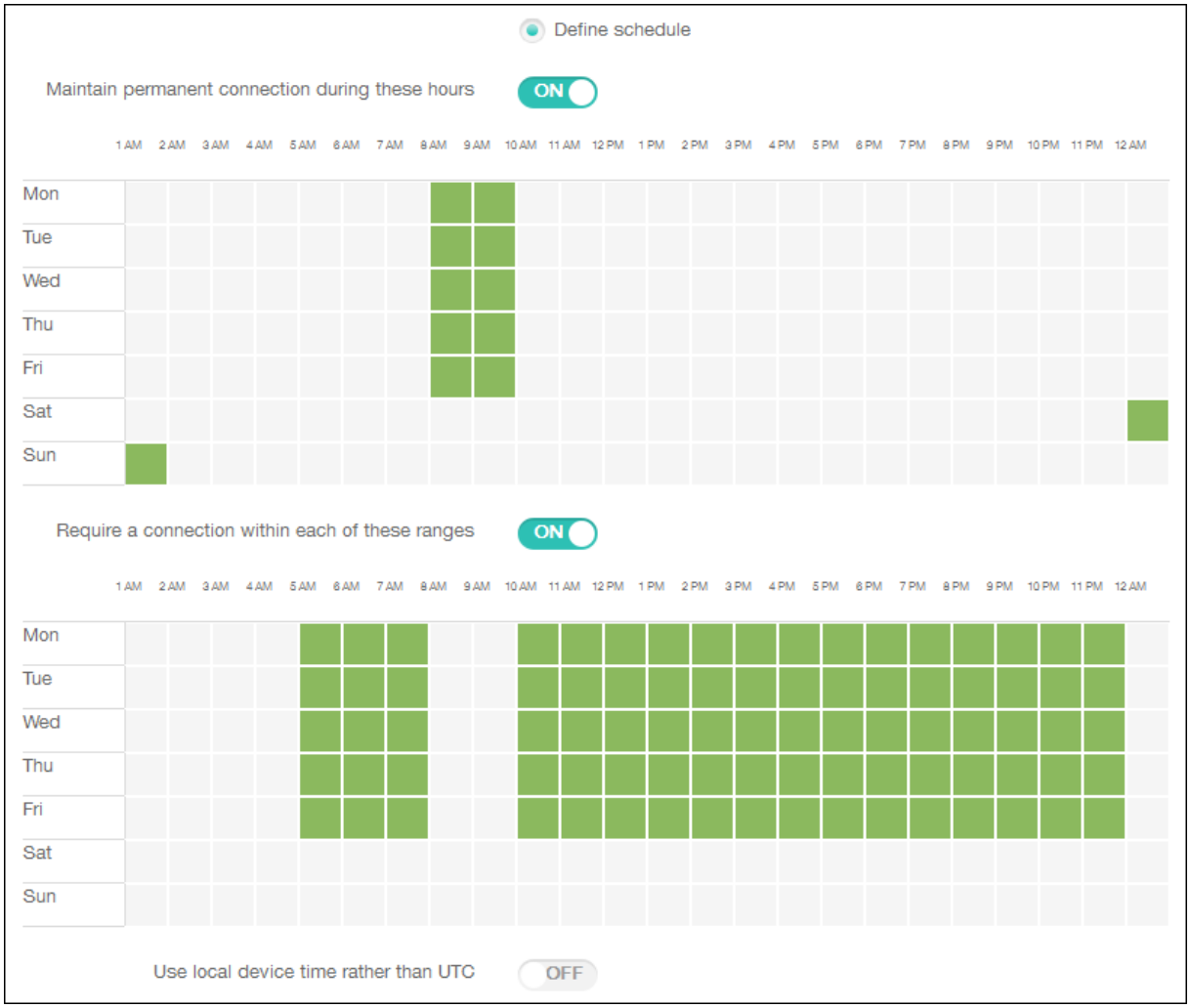
leccionar la opción **Implementar para conexiones permanentes** en **Programación de implementación** en cada directiva implementada en el dispositivo.

- **Nunca:** 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.
- **Cada:** 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 **Conectar cada N minutos**. En él, debe introducir la cantidad de minutos tras los que el dispositivo debe volver a conectarse. El valor predeterminado es **20**.
- **Definir programación:** Cuando se activa, la instancia de XenMobile en el dispositivo del usuario intenta volver a conectarse al servidor de 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 "Definir un período de tiempo de conexión" para configurar un período de tiempo de conexión.
  * **Mantener conexión permanente durante estas horas:** Los dispositivos de los usuarios deben estar conectados durante el período de tiempo definido.
  * **Requerir una conexión dentro de cada uno de estos intervalos:** Los dispositivos de usuario deben conectarse al menos una vez durante uno de los períodos de tiempo definidos.
  * **Usar la hora local del dispositivo en lugar de UTC:** Sincroniza los períodos de tiempo definidos con la hora local del dispositivo en lugar de la hora universal coordinada (UTC).

Definir un período de tiempo de conexión

Cuando se habilitan las siguientes opciones, aparece una escala de tiempo en la que puede definir los períodos de tiempo pertinentes. Es posible habilitar una de las dos opciones o ambas: mantener una conexión permanente durante horas específicas o requerir una conexión dentro de períodos de tiempo determinados. Cada cuadrado de la escala de tiempo es de 30 minutos, de modo que, si quiere una conexión entre las 8:00 a. m. y las 9:00 a. m. todos los días de la semana, haga clic en los dos cuadrados ubicados entre 8 a. m. y 9 a. m. todos los días de la semana.

Por ejemplo: las dos escalas de tiempo de la siguiente ilustración requieren una conexión permanente entre las 8:00 a. m. y las 9:00 a. m. todos los días laborables de la semana, una conexión permanente entre las 12:00 a. m. del sábado y la 1:00 a. m. del domingo, además de al menos una conexión cada día laborable entre las 5:00 a. m. y las 8:00 a. m. o entre las 10:00 y a. m. las 11:00 p. m.



Directiva de contactos (CardDAV)

January 4, 2022

En XenMobile, puede agregar una directiva para añadir una cuenta de contactos iOS (CardDAV) a los dispositivos iOS o macOS de los usuarios. De esta manera, los usuarios podrán sincronizar los datos de contacto con cualquier servidor que admita CardDAV.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Descripción de la cuenta:** Escriba la descripción de la cuenta. Este campo es obligatorio.

- **Nombre de host:** Escriba la dirección del servidor CardDAV. Este campo es obligatorio.
- **Puerto:** Especifique el puerto por el que conectarse al servidor CardDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **URL principal:** Indique la URL base de acceso al calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña opcional de usuario.
- **Usar SSL:** Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CardDAV. Está **activado** de forma predeterminada.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de macOS

- **Descripción de la cuenta:** Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Nombre de host:** Escriba la dirección del servidor CardDAV. Este campo es obligatorio.
- **Puerto:** Especifique el puerto por el que conectarse al servidor CardDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **URL principal:** Indique la URL base de acceso al calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña opcional de usuario.
- **Usar SSL:** Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el servidor CardDAV. Está **activado** de forma predeterminada.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.

    * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Directiva de control de actualizaciones de SO

January 4, 2022

La directiva "Control de actualizaciones del SO" permite implementar:

- Las actualizaciones más recientes del sistema operativo en dispositivos iOS supervisados.

  La directiva "Actualización de SO" solo funciona con dispositivos supervisados e inscritos en el Programa de implementación de Apple.

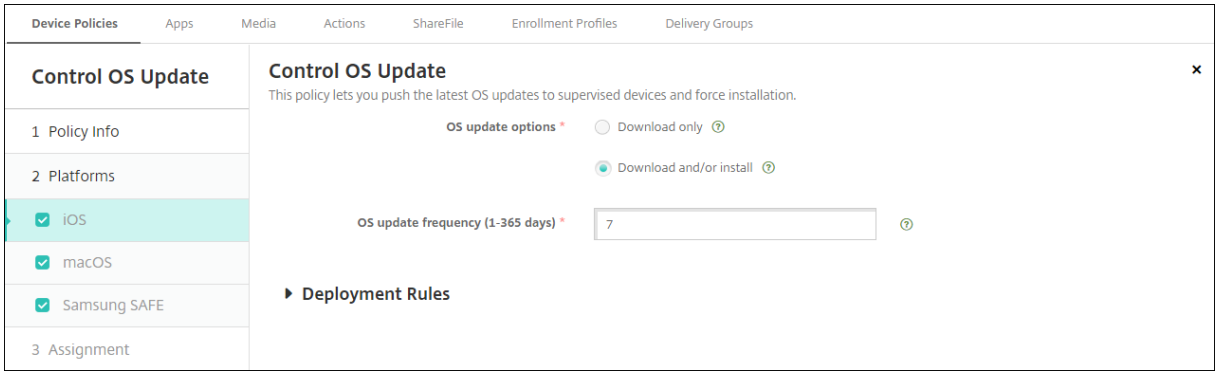
- Las actualizaciones de software más recientes (de sistema operativo y de aplicaciones) en dispositivos macOS inscritos con DEP que usan macOS 10.11.5 y versiones posteriores.

- Las actualizaciones más recientes del sistema operativo en dispositivos Samsung SAFE supervisados.

  En caso de dispositivos Samsung SAFE, XenMobile envía la directiva Control de actualizaciones del SO a Secure Hub, y este la aplica al dispositivo. En la página **Administrar > Dispositivos**, se muestra cuándo envía XenMobile Server la directiva y cuándo la recibe el dispositivo.

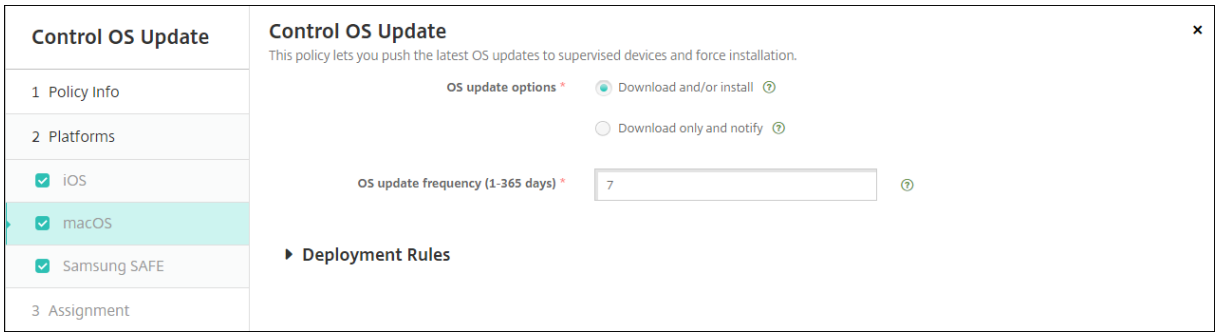
Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS



- **Opciones de actualización de SO:** Ambas opciones descargan las actualizaciones más recientes del sistema operativo en los dispositivos supervisados siguiendo la frecuencia de **Frecuencia de actualización de SO**. El dispositivo pide al usuario que instale las actualizaciones. La solicitud sigue visible después de que el usuario desbloquee el dispositivo.
- **Frecuencia de actualización de SO:** Determina la frecuencia con que XenMobile comprueba el estado de las actualizaciones y actualiza el sistema operativo del dispositivo. El valor predeterminado es de **7** días.

Parámetros de macOS



- **Opciones de actualización de SO:** Ambas opciones descargan las actualizaciones más recientes de macOS siguiendo la **Frecuencia de actualización de SO**. Puede optar por instalar las actualizaciones o notificar al usuario a través de la App Store que hay actualizaciones disponibles.
- **Frecuencia de actualización de SO:** Determina la frecuencia con que XenMobile comprueba el estado de las actualizaciones y actualiza el sistema operativo del dispositivo. El valor predeterminado es de **7** días.

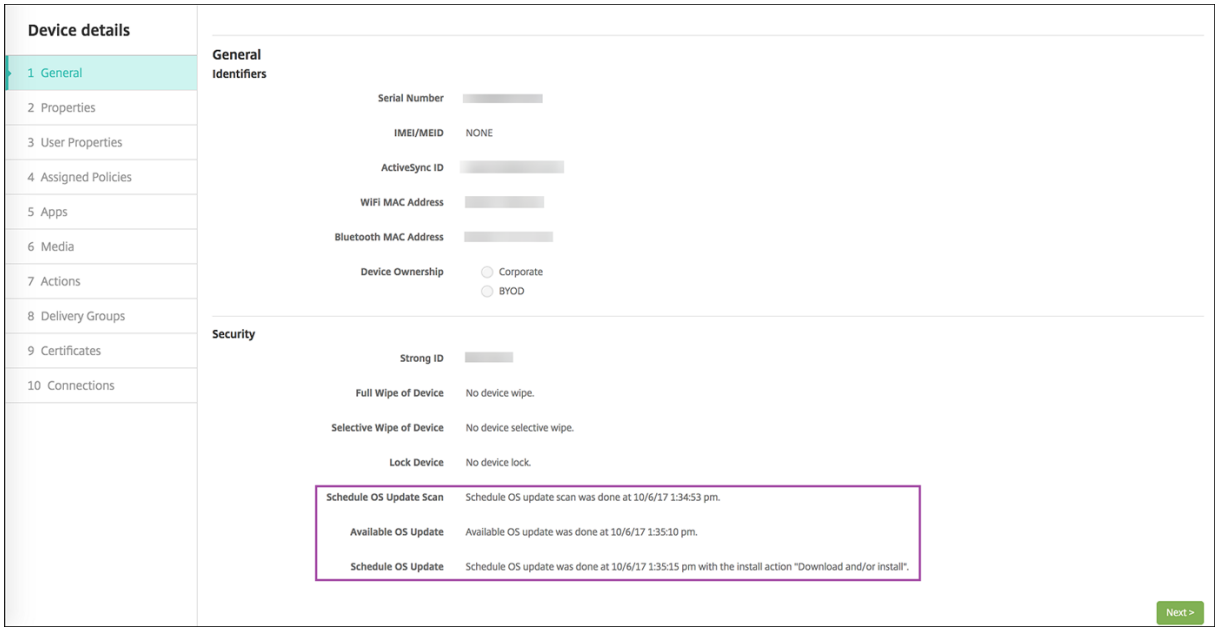
Obtener el estado para las acciones de actualización de iOS y macOS

Para iOS y macOS, XenMobile no implementa la directiva Control de actualizaciones del SO en los dispositivos. En su lugar, XenMobile utiliza la directiva para enviar estos comandos MDM a los dispos-

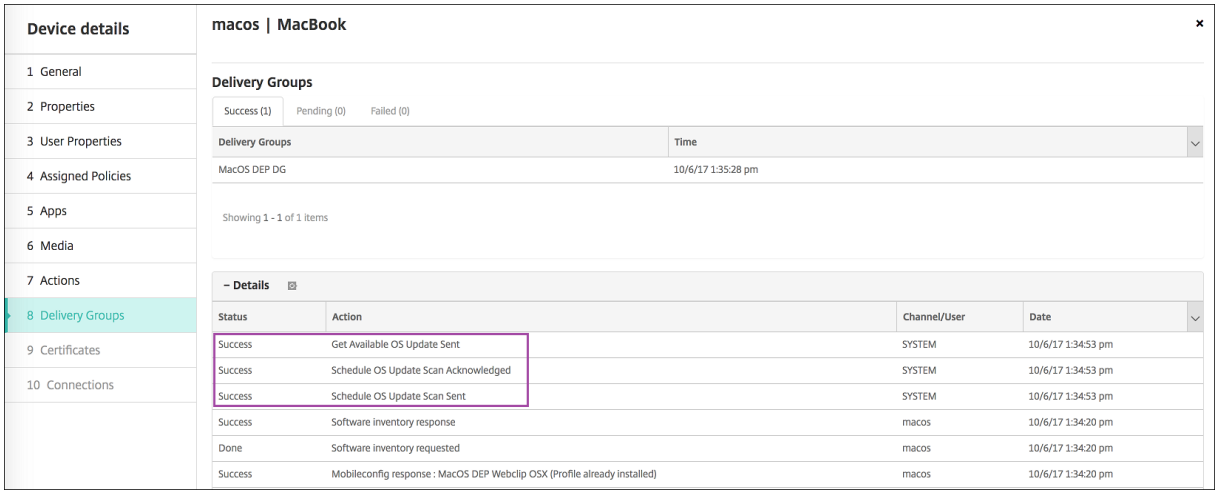
itivos:

- Programación del examen de actualizaciones de SO: Solicita que el dispositivo realice un examen exhaustivo para buscar actualizaciones del sistema operativo (opcional para iOS).
- Actualizaciones disponibles del sistema operativo: Consulta el dispositivo para obtener una lista de las actualizaciones del sistema operativo disponibles.
- Programación de actualización de SO: Solicita que el dispositivo realice actualizaciones de macOS, actualizaciones de aplicaciones o ambas. Por lo tanto, el sistema operativo del dispositivo determina cuándo debe descargar o instalar el sistema operativo y las actualizaciones de las aplicaciones.

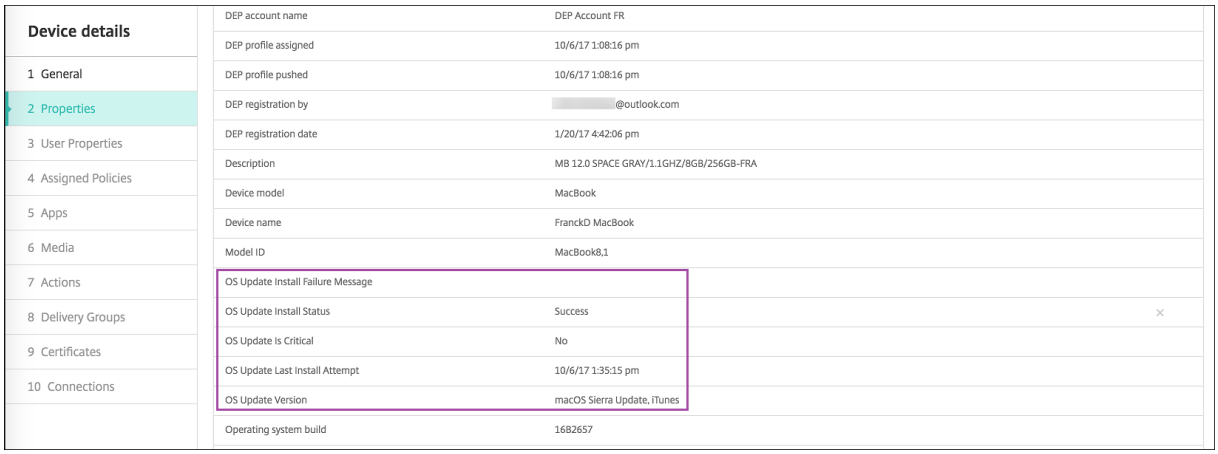
La página **Administrar > Dispositivos > Detalles del dispositivo** muestra el estado de los exámenes programados de actualizaciones del SO, las actualizaciones disponibles del SO y las actualizaciones programadas de macOS y aplicaciones.

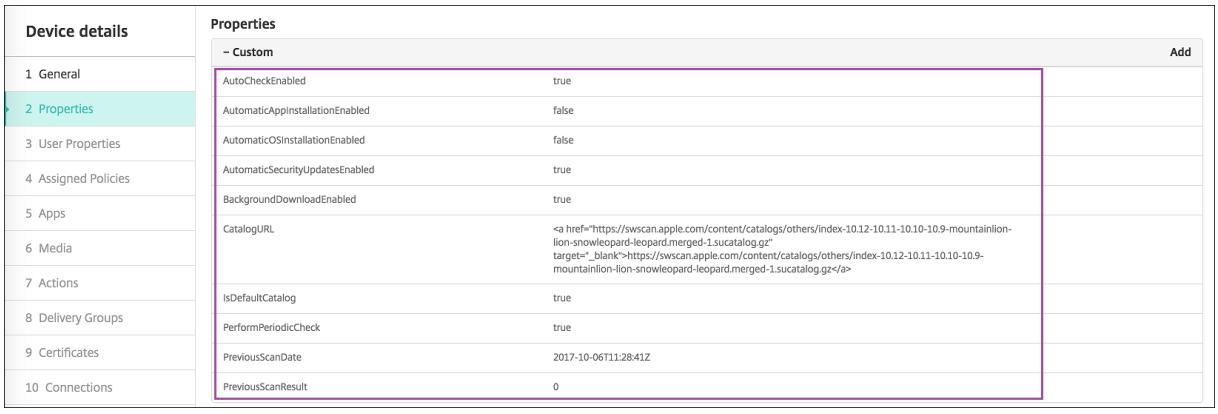


Para obtener más información sobre el estado de las acciones de actualización, vaya a la página **Administrar > Dispositivos > Detalles del dispositivo (Grupos de entrega)**.



Para obtener más información, como la lista de las actualizaciones disponibles del sistema operativo y el último intento de instalación, vaya a la página **Administrar > Dispositivos > Detalles del dispositivo (Propiedades)**.

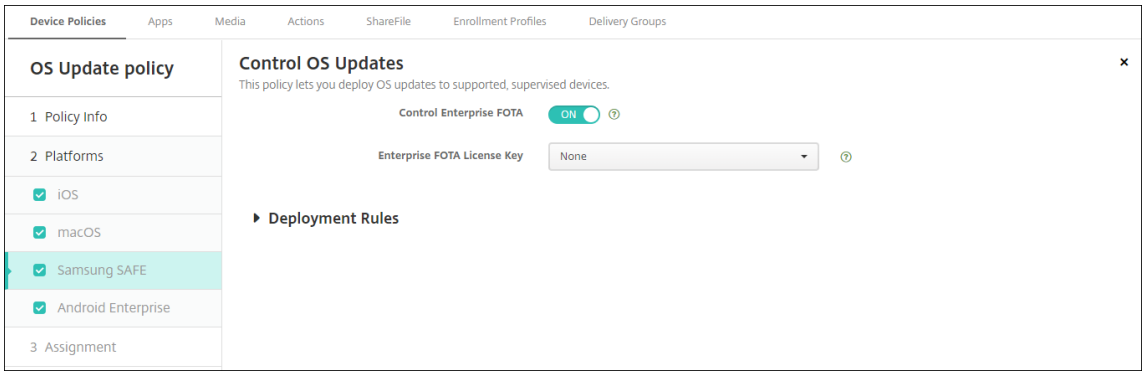




Parámetros de Samsung SAFE

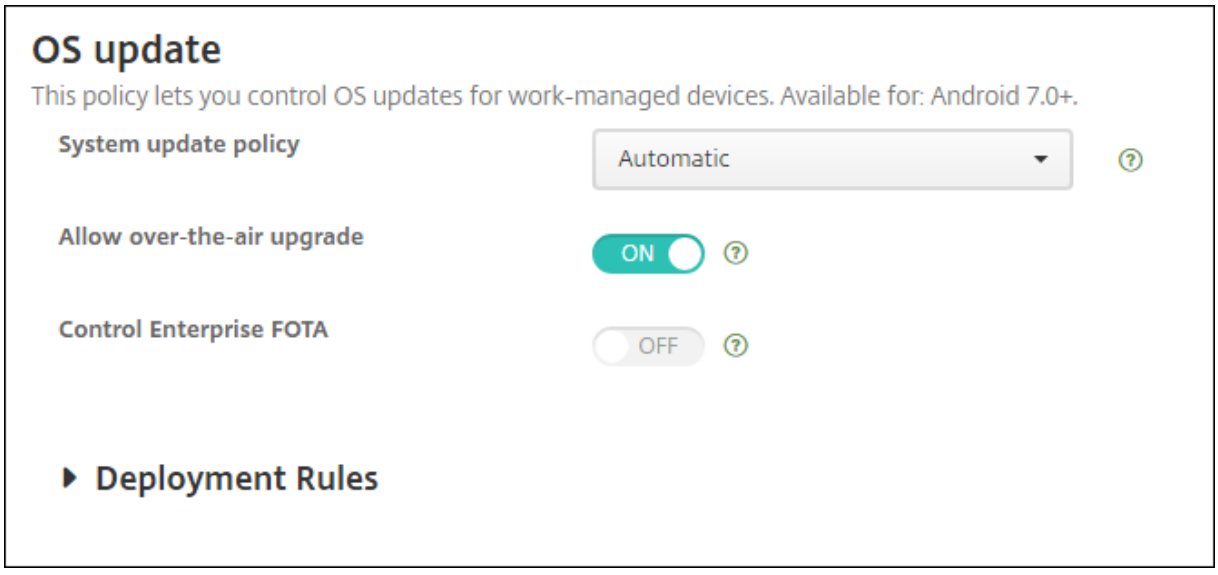
Enterprise FOTA (E-FOTA) de Samsung permite determinar cuándo se actualizan los dispositivos y la versión de firmware que se va a usar. Para usar E-FOTA:

1. Cree una directiva "Clave de licencia para MDM de Samsung" con las claves y la información de licencia que haya recibido de Samsung. Para obtener más información, consulte Directiva de clave de licencia para la administración de dispositivos móviles (MDM) Samsung.
2. Cree una directiva Control de actualizaciones del SO para habilitar Enterprise FOTA.



- **Enterprise FOTA:** Elija **Sí** para este parámetro.
- **Clave de licencia de Enterprise FOTA:** Seleccione el nombre de la directiva Clave de licencia MDM para Samsung.

Parámetros de Android Enterprise



- **Directiva de actualización del sistema:** Determina cuándo se producen las actualizaciones del sistema. Si habilita el parámetro **Controlar Enterprise FOTA**, las actualizaciones se producen automáticamente, independientemente de la configuración de este parámetro.

  - **Automática**: Las actualizaciones se instalan en cuanto están disponibles.
  - **Intervalo**: Las actualizaciones se instalan automáticamente durante el intervalo de mantenimiento diario, especificado en los campos **Hora de inicio** y **Hora de fin**.
    * **Hora de inicio:** El inicio del intervalo de mantenimiento, medido en cantidad de minutos (de **0** a **1440**) desde la medianoche según la hora local del dispositivo. El valor predeterminado es **0**.
    * **Hora de fin:** La finalización del intervalo de mantenimiento, medido en cantidad de minutos (de **0** a **1440**) desde la medianoche según la hora local del dispositivo. El valor predeterminado es **120**.
  - **Posponer**: Permite a los usuarios posponer una actualización hasta 30 días.
- **Permitir actualización inalámbrica:** Si se inhabilita, los dispositivos de usuario no pueden recibir actualizaciones de software por conexión inalámbrica. Está **activado** de forma predeterminada.
- **Controlar Enterprise FOTA:** Si se habilita, los dispositivos Samsung comprueban si hay actualizaciones disponibles y las instalan automáticamente. Si no se habilita, los usuarios pueden buscarlas ellos mismos e instalarlas manualmente. Para dispositivos Android Enterprise con Samsung Knox 3.0 o una versión posterior. Está **desactivado** de forma predeterminada.
  - **Clave de licencia de Enterprise FOTA:** Seleccione la clave de licencia que quiere utilizar al comprobar si hay actualizaciones. Puede configurar este parámetro en la directiva Clave de licencia de Samsung MDM. Para dispositivos Android Enterprise con Samsung Knox 3.0 o una versión posterior. El valor predeterminado es **Ninguno**. La clave se puede configurar mediante la directiva de dispositivo de **clave de licencia MDM de Samsung**. Consulte Directiva de clave de licencia MDM de Samsung.

Directiva de copia de aplicaciones al contenedor de Samsung

January 4, 2022

Puede especificar que las aplicaciones que ya están instaladas en un dispositivo se copien en un contenedor KNOX en dispositivos Samsung admitidos. Para obtener información sobre los dispositivos compatibles, consulte el artículo Dispositivos incorporados en KNOX de Samsung.

Las aplicaciones que se copien al contenedor Knox solo estarán disponibles cuando los usuarios inicien sesión en dicho contenedor.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

- Inscriba los dispositivos en XenMobile.
- Implemente las claves MDM de Samsung (ELM y KLM). Para obtener más información, consulte Directiva de clave de licencia para la administración de dispositivos móviles (MDM) Samsung.
- Instale aplicaciones en el dispositivo.
- Inicialice Knox en el dispositivo para copiar las aplicaciones al contenedor Knox.

Parámetros de plataforma

- **Nueva aplicación:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada aplicación a la lista:
  - Escriba un ID de paquete, por ejemplo: com.mobiwolf.lacingart para la aplicación LacingArt.
  - Haga clic en **Guardar** o **Cancelar**.

Directiva Credenciales

January 4, 2022

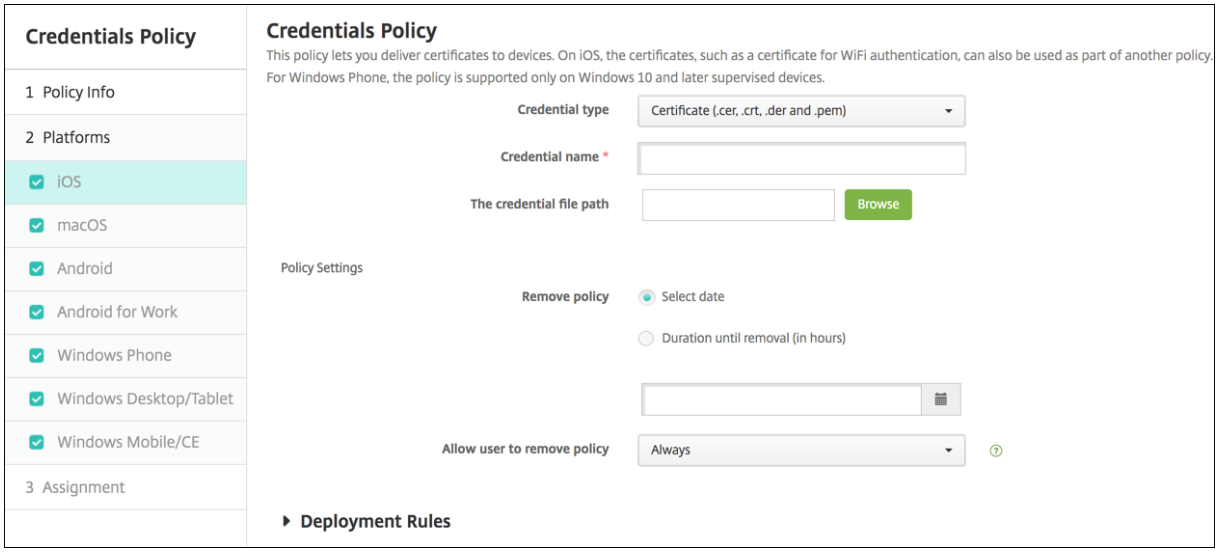
Las directivas de credenciales apuntan a una PKI configurada en XenMobile. Por ejemplo, la configuración de PKI puede incluir una entidad PKI, un almacén de claves, un proveedor de credenciales o un certificado de servidor. Para obtener más información acerca de las credenciales, consulte Certificados y autenticación.

Cada plataforma compatible requiere un conjunto diferente de valores, que se describen en este artículo.

> **Nota:**
>
> 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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

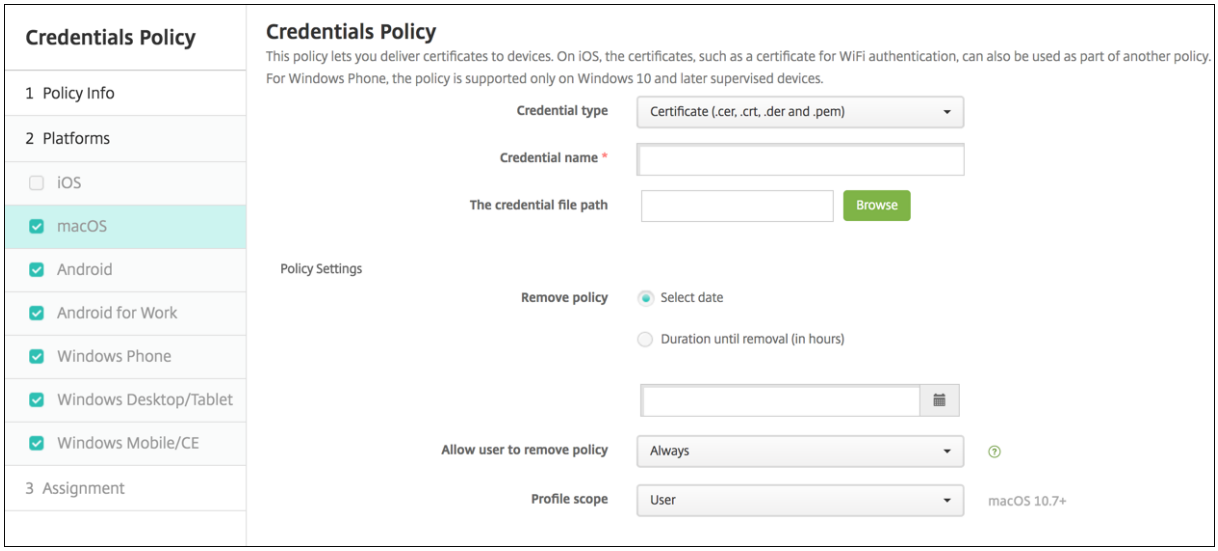


Configure los siguientes parámetros:

- **Tipo de credencial:** 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**
    - **Nombre de credencial:** Escriba un nombre único para la credencial.
    - **Ruta del archivo de credenciales:** Para seleccionar el archivo de credenciales, haga clic en Examinar y vaya a la ubicación del archivo.
  - **Almacén de claves**
    - **Nombre de credencial:** Escriba un nombre único para la credencial.
    - **Ruta del archivo de credenciales:** Para seleccionar el archivo de credenciales, haga clic en Examinar y vaya a la ubicación del archivo.
    - **Contraseña:** Escriba una contraseña de almacén de claves para la credencial.
  - **Certificado de servidor**
    - **Certificado de servidor:** En la lista, haga clic en el certificado que se va a utilizar.
  - **Proveedor de credenciales**
    - **Proveedor de credenciales:** En la lista, haga clic en el nombre del proveedor de credenciales.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones

posteriores.

Parámetros de macOS

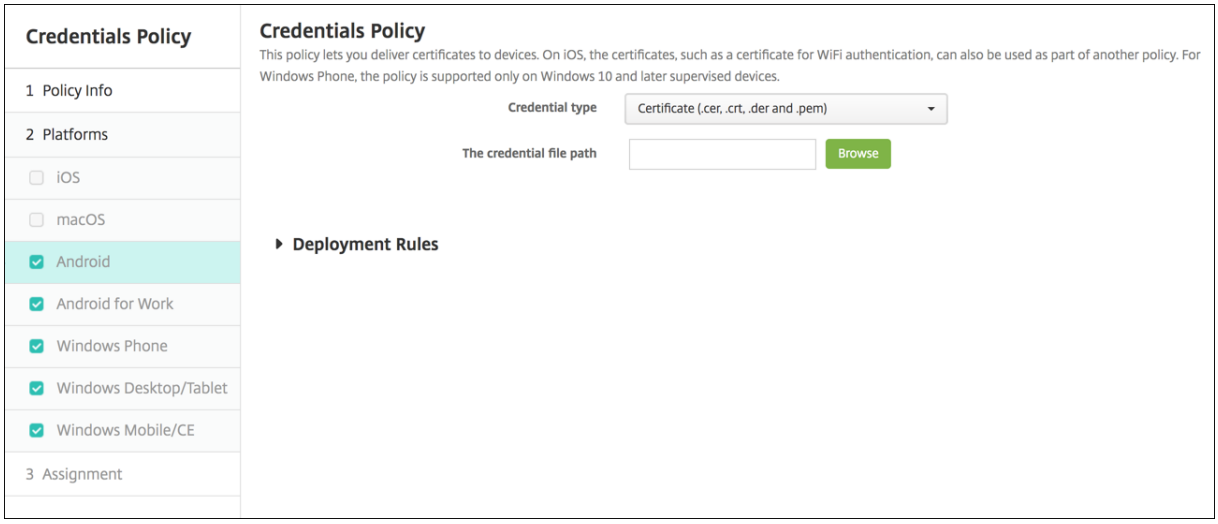


Configure los siguientes parámetros:

- **Tipo de credencial:** 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**
    - **Nombre de credencial:** Escriba un nombre único para la credencial.
    - **Ruta del archivo de credenciales:** Para seleccionar el archivo de credenciales, haga clic en **Examinar** y vaya a la ubicación del archivo.
  - **Almacén de claves**
    - **Nombre de credencial:** Escriba un nombre único para la credencial.
    - **Ruta del archivo de credenciales:** Para seleccionar el archivo de credenciales, haga clic en **Examinar** y vaya a la ubicación del archivo.
    - **Contraseña:** Escriba una contraseña de almacén de claves para la credencial.
  - **Certificado de servidor**
    - **Certificado de servidor:** En la lista, haga clic en el certificado que se va a utilizar.
  - **Proveedor de credenciales**
    - **Proveedor de credenciales:** En la lista, haga clic en el nombre del proveedor de credenciales.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de

la eliminación.
    * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Parámetros de Android

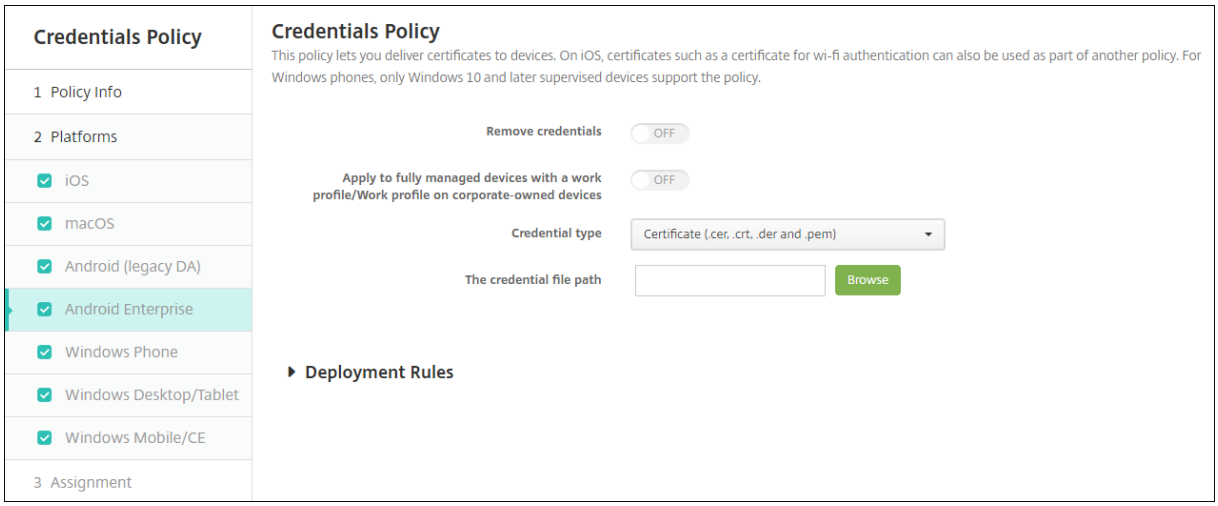


Configure los siguientes parámetros:

- **Tipo de credencial:** 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**
    * **Nombre de credencial:** Escriba un nombre único para la credencial.
    * **Ruta del archivo de credenciales:** Para seleccionar el archivo de credenciales, haga clic en Examinar y vaya a la ubicación del archivo.
  - **Almacén de claves**
    * **Nombre de credencial:** Escriba un nombre único para la credencial.
    * **Ruta del archivo de credenciales:** Seleccione el archivo de credenciales. Para ello, deberá hacer clic en **Examinar** y, a continuación, ir a la ubicación del archivo.
    * **Contraseña:** Escriba una contraseña de almacén de claves para la credencial.
  - **Certificado de servidor**

        * **Certificado de servidor:** En la lista, haga clic en el certificado que se va a utilizar.
    - **Proveedor de credenciales**
        * **Proveedor de credenciales:** En la lista, haga clic en el nombre del proveedor de credenciales.

Parámetros de Android Enterprise



Configure estas opciones para determinar cómo aplicará XenMobile los parámetros de credenciales:

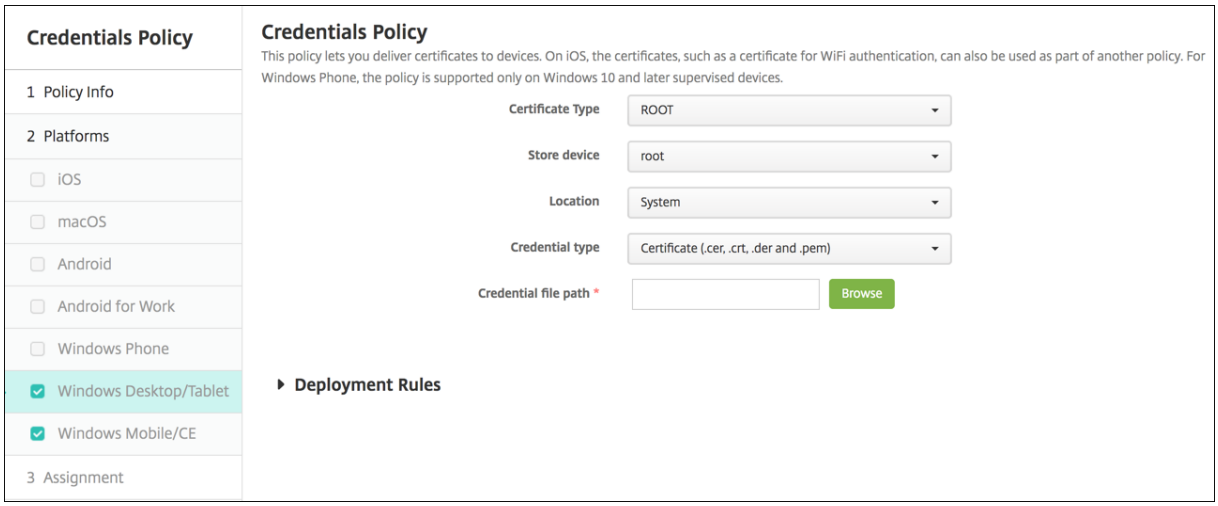
- **Quitar credenciales:** Establezca el valor **Sí** para configurar los siguientes parámetros. Está **desactivado** de forma predeterminada.
    - **Quitar credenciales de usuario:** Quita los certificados del almacén de claves administrado. Está **desactivado** de forma predeterminada.
    - **Quitar certificados raíz de confianza:** Desinstala todos los certificados de CA que no son del sistema. Está **desactivado** de forma predeterminada.
- **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa:** Le permite configurar los parámetros de la directiva de credenciales para dispositivos totalmente administrados con perfiles de trabajo. Si este parámetro está **activado**, los parámetros de credenciales que configure se aplicarán únicamente al perfil de trabajo. Si está **desactivado**, los parámetros de credenciales que configure se aplicarán únicamente al dispositivo. Está **desactivado** de forma predeterminada.

Configure los parámetros de credenciales:

- **Tipo de credencial:** 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**
        * **Ruta del archivo de credenciales:** Seleccione el archivo de credenciales. Para ello, deberá hacer clic en **Examinar** y, a continuación, ir a la ubicación del archivo.

- **Almacén de claves**
  - **Ruta del archivo de credenciales:** Seleccione el archivo de credenciales. Para ello, deberá hacer clic en **Examinar** y, a continuación, ir a la ubicación del archivo.
  - **Alias de certificado:** Un alias de certificado facilita a las aplicaciones el acceso al certificado. Configure un alias de certificado en la directiva de dispositivo Configuración administrada de Android Enterprise. A continuación, escriba el alias en el campo **Alias de certificado**, en la directiva de dispositivo Credenciales. Las aplicaciones recuperan el certificado y autentican la VPN sin que se requiera ninguna acción por parte de los usuarios.
  - **Contraseña:** Escriba una contraseña de almacén de claves para la credencial.
- **Certificado de servidor**
  - **Certificado de servidor:** En la lista, haga clic en el certificado que se va a utilizar.
- **Proveedor de credenciales**
  - **Alias de certificado:** Un alias de certificado facilita a las aplicaciones el acceso al certificado. Configure un alias de certificado en la directiva de dispositivo Configuración administrada de Android Enterprise. A continuación, escriba el alias en el campo **Alias de certificado**, en la directiva de dispositivo Credenciales. Las aplicaciones recuperan el certificado y autentican la VPN sin que se requiera ninguna acción por parte de los usuarios.
  - **Proveedor de credenciales:** En la lista, haga clic en el nombre del proveedor de credenciales.
  - **Aplicaciones para usar certificados:** Para especificar las aplicaciones que tengan acceso silencioso a las credenciales de este proveedor, haga clic en **Agregar**, seleccione una aplicación y haga clic en **Guardar**.

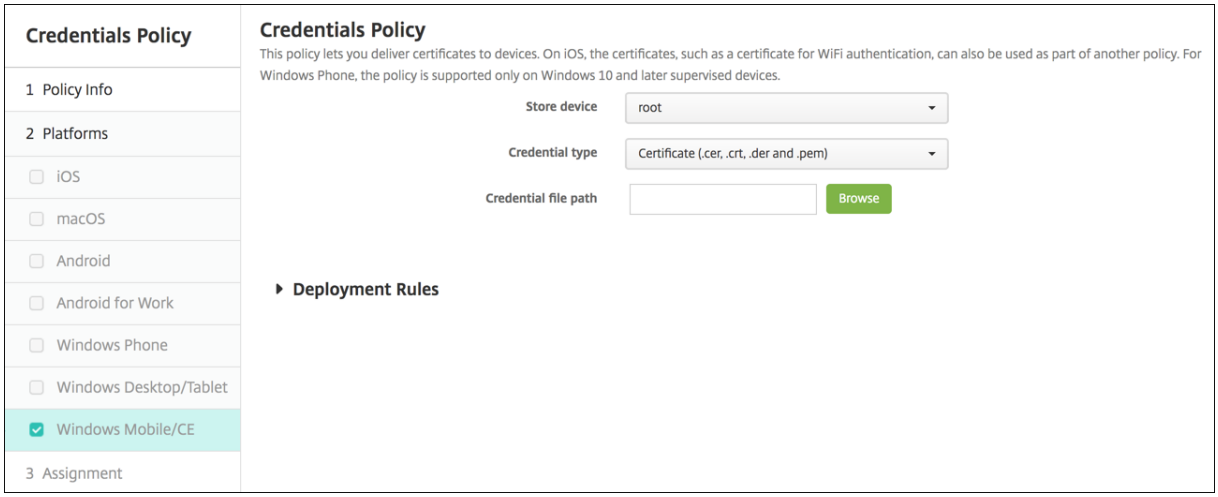
Parámetros de escritorios y tabletas Windows



- **Tipo de certificado:** En la lista, haga clic en **RAÍZ** o **CLIENTE**.

- Si hace clic en **RAÍZ**, configure los siguientes parámetros:
  - **Dispositivo de almacenamiento:** En la lista, haga clic en **raíz**, **Mi** o **CA** para designar la ubicación del almacén de certificados para la credencial. Con la opción **Mi**, el certificado se guarda en los almacenes de certificados de los usuarios.
  - **Ubicación:** Para tabletas con Windows 10 o Windows 11, **Sistema** es la única ubicación disponible.
  - **Tipo de credencial:** Para tabletas con Windows 10 o Windows 11, **Certificado** es el único tipo de credencial disponible.
  - **Ruta del archivo de credenciales:** Seleccione el archivo de certificado. Para ello, deberá hacer clic en **Examinar** y, a continuación, ir a la ubicación del archivo.
- Si hace clic en **CLIENTE**, configure los siguientes parámetros:
- **Ubicación:** Para tabletas con Windows 10 o Windows 11, **Sistema** es la única ubicación disponible.
- **Tipo de credencial:** Para tabletas con Windows 10 o Windows 11, **Almacén de claves** es el único tipo de credencial disponible.
- **Nombre de credencial:** Escriba el nombre de la credencial. Este campo es obligatorio.
- **Ruta del archivo de credenciales:** Seleccione el archivo de certificado. Para ello, deberá hacer clic en **Examinar** y, a continuación, ir a la ubicación del archivo.
- **Contraseña:** Escriba la contraseña asociada a la credencial. Este campo es obligatorio.

Parámetros de Windows Mobile/CE



- **Dispositivo de almacenamiento:** En la lista, haga clic en la ubicación del almacén de certificados de la credencial. El valor predeterminado es **raíz**. Las opciones son:
  - **Autoridades de confianza de ejecución con privilegios:** Las aplicaciones firmadas con un certificado perteneciente a este almacén se ejecutarán con un nivel de confianza con privilegios.
  - **Autoridades de confianza de ejecución sin privilegios:** Las aplicaciones firmadas con

un certificado perteneciente a este almacén se ejecutarán con un nivel de confianza normal.
  - **SPC (Certificado de publicador de software):** Este certificado se usa para firmar archivos CAB.
  - **raíz:** Un almacén de certificados que contiene certificados raíz.
  - **CA:** Un almacén de certificados que contiene información de cifrado, incluidas las entidades de certificación intermedia.
  - **MI:** Un almacén de certificados que contiene los certificados personales del usuario final.
- **Tipo de credencial:** El certificado es el único tipo de credencial para dispositivos Windows Mobile/CE.
- **Ruta del archivo de credenciales:** Seleccione el archivo de credenciales. Para ello, deberá hacer clic en **Examinar** y, a continuación, ir a la ubicación del archivo.

Directiva de XML personalizado

January 4, 2022

En XenMobile, puede crear directivas de XML personalizado para adaptar las siguientes funciones en dispositivos Windows, Android Zebra y Android Enterprise que sean compatibles:

- 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 incluyen la capacidad para proporcionar software nuevo o correcciones de errores para cargarlos 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.

> **Nota:**
>
> Al crear contenido XML, use el símbolo % con precaución. El símbolo % es un carácter XML reservado que solo se utiliza para escapar caracteres XML especiales. Para usar % en un nombre, codifíquelo como %25.

Para dispositivos Windows: Puede crear su propia configuración XML personalizada mediante la API de Open Mobile Alliance Device Management (OMA DM) en Windows. La creación de contenido XML personalizado con la API de OMA DM no se cubre en esta sección. Para obtener más información sobre el uso de la API de OMA DM, consulte OMA Device Management en el sitio Microsoft Developer Network.

Para dispositivos Android Zebra y Android Enterprise: Puede crear su propia configuración XML personalizada mediante el sistema de administración de MX (MXMS). La creación de contenido XML personalizado con la API de MXMS no se describe en este artículo. Para obtener más información sobre el uso de MXMS, consulte About MX en el sitio de Zebra.

> **Nota:**
>
> Para Windows 10 RS2 Phone: después de implementar en el teléfono una directiva de XML personalizado o una directiva de restricciones que inhabilita Internet Explorer, el explorador web permanece habilitado. Para solucionar este problema, reinicie el teléfono. Este es un problema de terceros.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Windows Phone y escritorios y tabletas Windows, Android Zebra y Android Enterprise

- **Contenido XML:** Escriba, o copie y pegue, el código XML personalizado que se va a agregar a la directiva.

  Tras hacer clic en **Siguiente**, 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 **Directiva XML personalizada**.

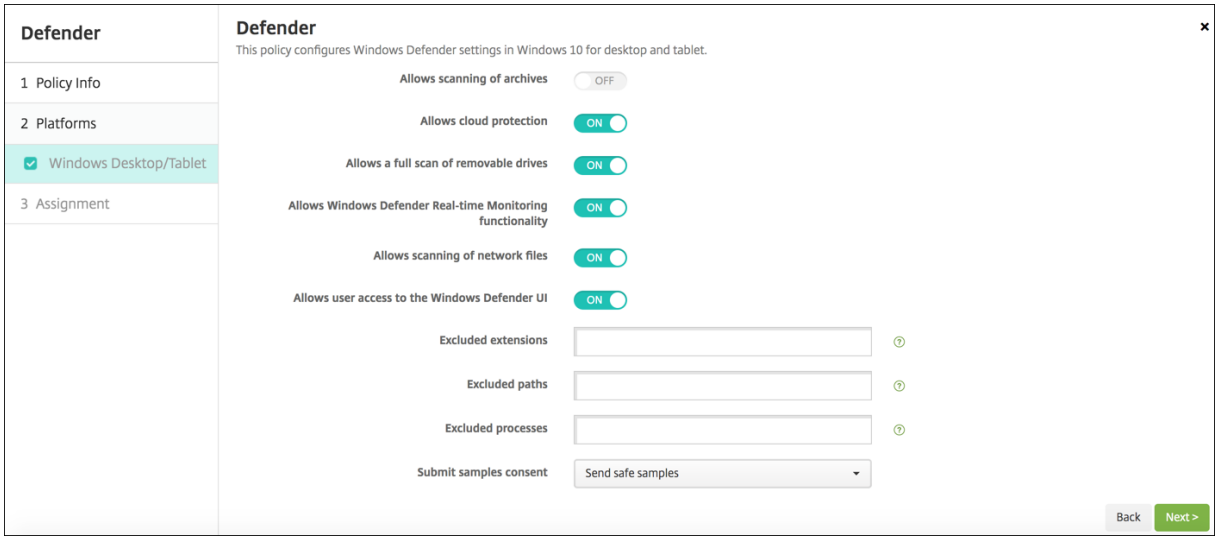
Directiva de Defender

January 4, 2022

Windows Defender es una protección contra malware incluida en Windows 10 y Windows 11. En XenMobile, puede usar la directiva de Defender para configurar la directiva de Microsoft Defender en escritorios y tabletas con Windows 10 y Windows 11.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de tabletas y escritorios Windows



- **Permite el examen de datos archivados:** Permite o prohíbe que Defender analice archivos ya archivados. Está **desactivado** de forma predeterminada.
- **Permite usar la protección de la nube:** Permite o prohíbe que Defender envíe información a Microsoft sobre la actividad de malware. Está **activado** de forma predeterminada.
- **Permite un examen completo de las unidades extraíbles:** Permite o prohíbe que Defender examine las unidades extraíbles, como dispositivos USB. Está **activado** de forma predeterminada.
- **Permite usar la funcionalidad Supervisión en tiempo real de Windows Defender:** De forma predeterminada está **activado**.
- **Permite examinar archivos de red:** Permite o prohíbe que Defender examine archivos de red. Está **activado** de forma predeterminada.
- **Permite que el usuario acceda a la interfaz de usuario de Windows Defender:** Especifica si los usuarios pueden acceder a la interfaz del usuario de Windows Defender. Esta configuración se aplica la próxima vez que se inicie el dispositivo del usuario. Si tiene el valor **No**, los usuarios no recibirán ninguna notificación de Windows Defender. Está **activado** de forma predeterminada.
- **Extensiones excluidas:** Las extensiones a excluir de los exámenes en tiempo real o programados. Para separar las extensiones, use el carácter **|**. Por ejemplo, “lib|obj”.
- **Rutas excluidas:** Las rutas a excluir de los exámenes en tiempo real o programados. Para separar las rutas, use el carácter **|**. Por ejemplo, “C:\Ejemplo|C:\Ejemplo1”.
- **Procesos excluidos:** Los procesos a excluir de los exámenes en tiempo real o programados. Para separar los procesos, use el carácter **|**. Por ejemplo, “C:\Ejemplo.exe|C:\Ejemplo1.exe”.
- **Enviar muestras voluntariamente:** Controla si se envían a Microsoft archivos que pueden requerir mayor análisis para determinar si son malintencionados. Opciones: **Preguntar siempre**, **Enviar muestras seguras**, **Nunca enviar**, **Enviar todas las muestras**. El valor predeterminado

es **Enviar muestras seguras**.

Directiva de eliminación de archivos y carpetas

January 3, 2020

En XenMobile, puede crear una directiva para eliminar archivos o carpetas específicas de los dispositivos Windows Mobile/CE.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Windows Mobile/CE

- **Archivos y carpetas a eliminar:** Haga clic en "Agregar" y lleve a cabo lo siguiente para eliminar cada archivo o carpeta:
  - **Ruta:** Escriba la ruta al archivo o carpeta.
  - **Tipo:** En la lista, haga clic en "Archivo" o "Carpeta". El valor predeterminado es "Archivo".
  - Haga clic en **Guardar** para guardar el archivo o la carpeta, o bien haga clic en **Cancelar** para no guardarlos.

Directiva de eliminación de valores y claves del Registro

January 3, 2020

En XenMobile, puede crear una directiva para eliminar de los dispositivos Windows Mobile/CE claves y valores específicos del Registro.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Windows Mobile/CE

- **Claves y valores de Registro a eliminar:** Haga clic en **Agregar** y lleve a cabo lo siguiente para eliminar cada valor y clave del Registro:
  - **Clave:** Escriba la ruta a 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\.

- **Valor:** 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 **Guardar** para guardar la clave y el valor, o bien haga clic en **Cancelar** para no guardarlos.

Directiva de Device Health Attestation

January 4, 2022

En XenMobile, puede requerir que los dispositivos con Windows 10 o Windows 11 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
- Directiva del programa de implementación de Apple
- ELAMDriverLoaded
- IssuedAt
- KernelDebuggingEnabled
- PCR
- ResetCount
- RestartCount
- SafeModeEnabled
- SBCPHash
- SecureBootEnabled
- TestSigningEnabled
- VSMEnabled
- WinPEEnabled

Para obtener información, consulte la página Device HealthAttestation CSP de Microsoft.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener

más información, consulte Directivas de dispositivo.

Para configurar DHA desde Microsoft Cloud

Agregue una directiva de Device Health Attestation y defina esta configuración para cada plataforma que elija:

- **Habilitar Device Health Attestation:** Seleccione si se debe requerir Device Health Attestation. Está **desactivado** de forma predeterminada.

Para configurar DHA a través de un servidor DHA Windows local

Para habilitar DHA local, primero debe configurar un servidor DHA. A continuación, cree una directiva de XenMobile Server para habilitar el servicio DHA local.

1. Para configurar un servidor DHA, instale el rol de servidor DHA en una máquina con Windows Server 2016 Technical Preview 5 o una versión posterior. Para obtener instrucciones, consulte Configurar un servidor Device Health Attestation local.
2. Agregue una directiva de Device Health Attestation y defina estos parámetros:
    - **Habilitar Device Health Attestation:** Establezca el parámetro en **Sí**.
    - **Configurar Health Attestation Service local:** Establezca el parámetro en **Sí**.
    - **Nombre FQDN del servidor DHA local:** Introduzca el nombre de dominio completo del servidor DHA que configuró.
    - **Versión de API de DHA local:** Elija la versión del servicio DHA instalado en el servidor DHA.

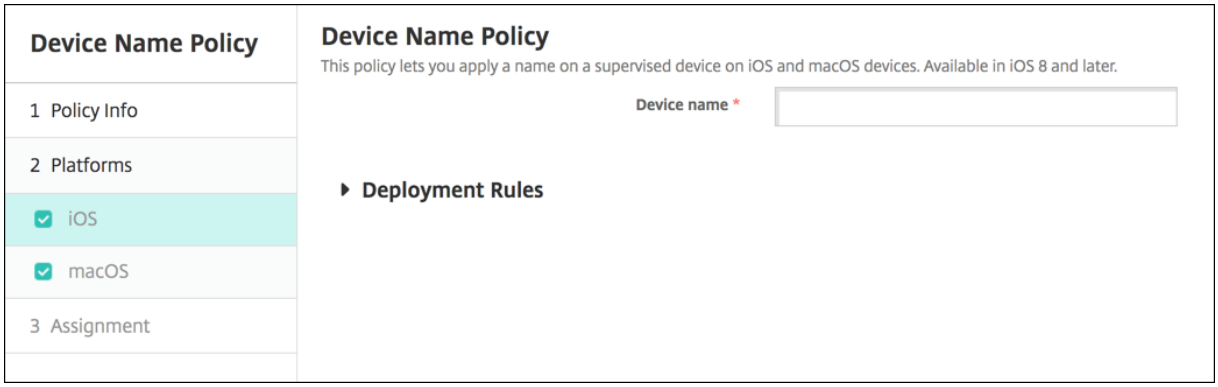
Directiva de nombre de dispositivo

January 3, 2020

Puede definir nombres para dispositivos iOS y macOS supervisados 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. Para obtener más información acerca de las macros, consulte Macros en XenMobile.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS y macOS



- **Nombre del dispositivo:** 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.

Directiva de configuración de la educación

January 4, 2022

La directiva de configuración de la educación define:

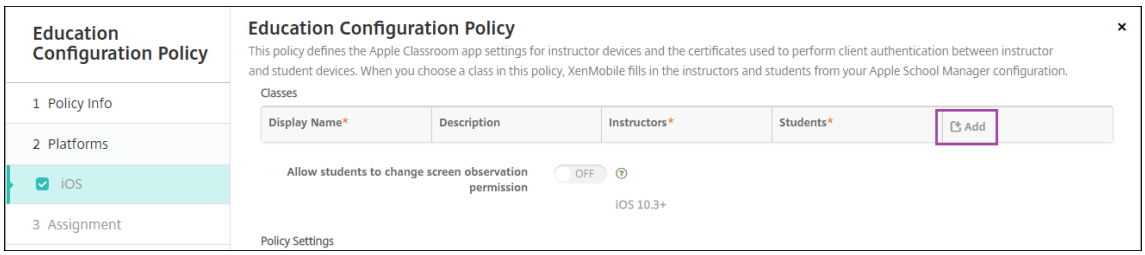
- Los parámetros de la aplicación Aula de Apple para dispositivos de profesores.
- Los certificados que se utilizan para la autenticación de cliente entre los dispositivos de profesores y estudiantes.

Cuando elige una clase en esta directiva, la consola de XenMobile rellena los profesores y los estudiantes a partir de la configuración de Apple School Manager. Cree una sola directiva si los parámetros de la aplicación Aula de Apple en esa directiva son los mismos para todas las clases.

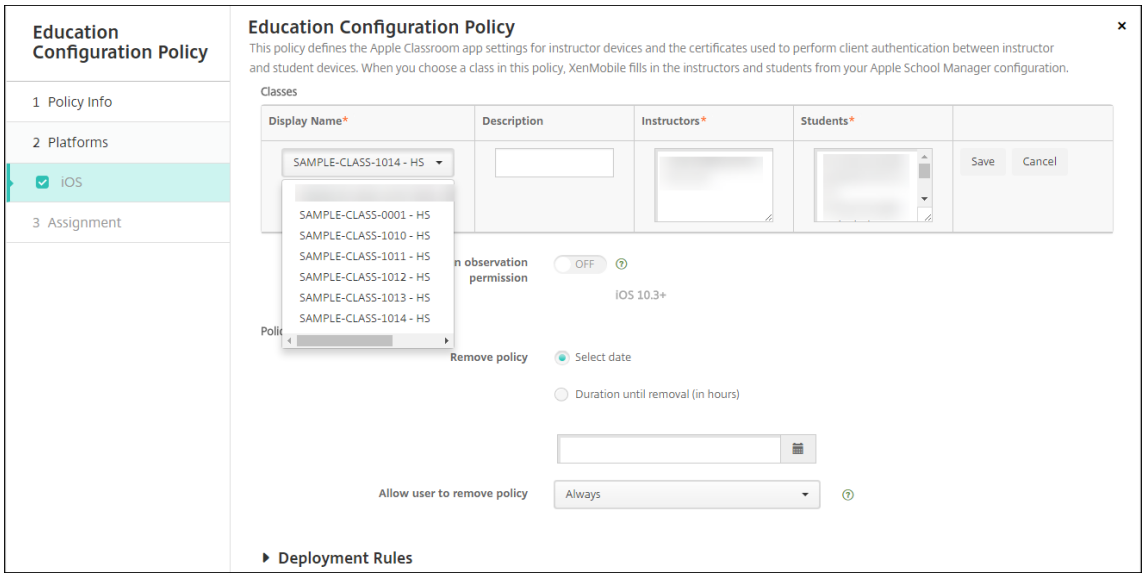
Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

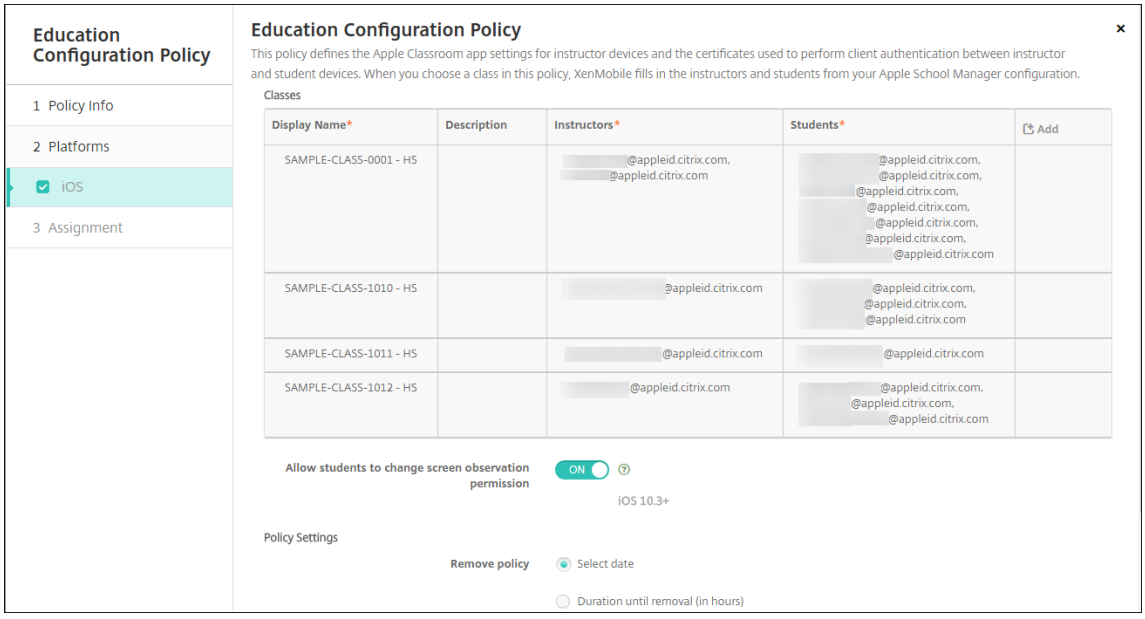
- **Clases:** Para agregar una clase, haga clic en **Agregar**.



Haga clic en la lista **Nombre simplificado**. Aparecerá una lista de las clases, obtenida a partir de su cuenta conectada de Apple School Manager.



Cuando elige una clase de **Nombre simplificado**, XenMobile rellena los profesores y los estudiantes. Continúe agregando clases.

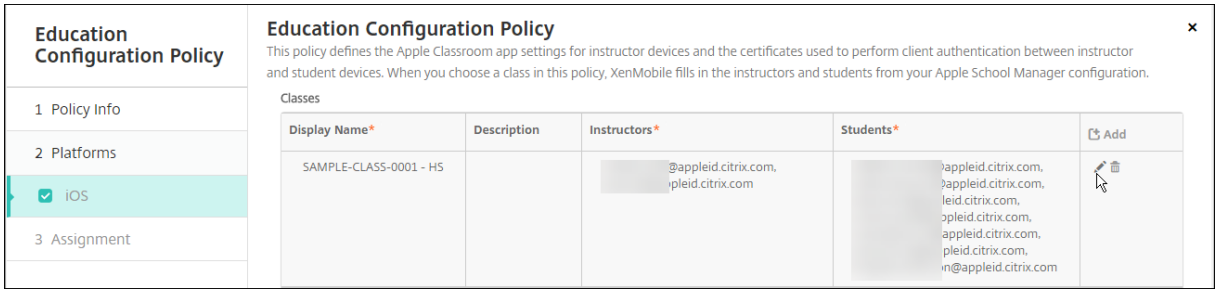


- **Permitir a los estudiantes cambiar permisos de observación de pantalla:** Si está **activado**, los estudiantes inscritos en clases administradas pueden elegir si permiten que su profesor vea las pantallas de sus dispositivos o no. Está **desactivado** de forma predeterminada.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.

Para modificar la información de clases en la directiva

Puede agregar una descripción a una clase (el "Nombre simplificado" en la aplicación Aula). También puede agregar o quitar profesores y estudiantes. XenMobile no guarda dichos cambios en la cuenta de Apple School Manager. Para obtener más información, consulte "Administrar datos de profesores, estudiantes y clases" en Integrar en funciones de Apple Educación.

Coloque el puntero sobre la columna **Agregar** de la clase que quiere modificar y, a continuación, haga clic en el icono de lápiz.



Para eliminar una clase de la directiva, coloque el cursor sobre la columna **Agregar** de la clase que quiere eliminar y, a continuación, haga clic en el icono de papelera.

Directiva de hub empresarial

October 18, 2019

Una directiva de hub empresarial para dispositivos Windows Phone permite distribuir aplicaciones a través del almacén central de la empresa.

Antes de crear la directiva, necesita lo siguiente:

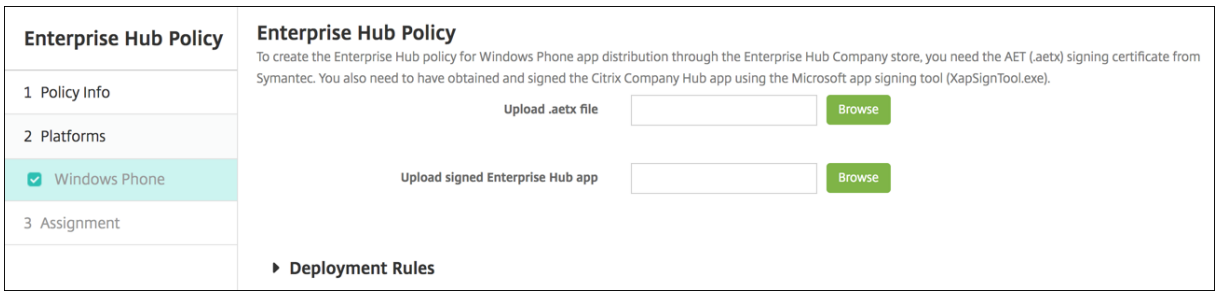
- Un certificado de firma AET (.aetx) de DigiCert

- La aplicación Citrix Company Hub firmada mediante la herramienta de firma de aplicaciones de Microsoft (XapSignTool.exe)

> **Nota:**
>
> XenMobile solo admite una directiva Hub empresarial por modo de Windows Phone Secure Hub. Por ejemplo, para cargar Windows Phone Secure Hub en XenMobile Enterprise Edition, no debe crear varias directivas de hub empresarial con versiones diferentes de Secure Hub para XenMobile Enterprise Edition. Puede implementar la directiva de hub empresarial inicial durante la inscripción del dispositivo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Windows Phone



- **Cargar archivo .aetx:** Seleccione el archivo AETX. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.
- **Cargar aplicación firmada de hub empresarial:** Seleccione la aplicación de hub empresarial. Para ello, haga clic en **Examinar** y vaya a la ubicación de la aplicación.

Directiva de Exchange

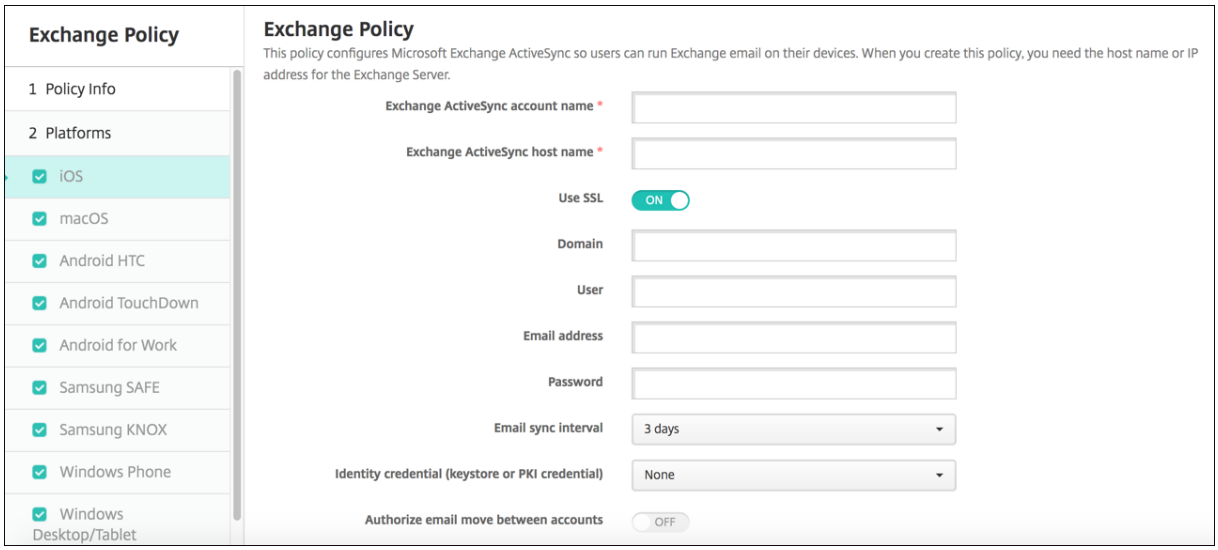
January 4, 2022

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, macOS, Android Enterprise, Samsung SAFE, Samsung KNOX, Windows Phone y tabletas Windows. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en los siguientes apartados.

Para poder crear esta directiva, debe conocer el nombre de host o la dirección IP del servidor Exchange. Para obtener más información acerca de los parámetros de ActiveSync, consulte el artículo de Microsoft ActiveSync CSP.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

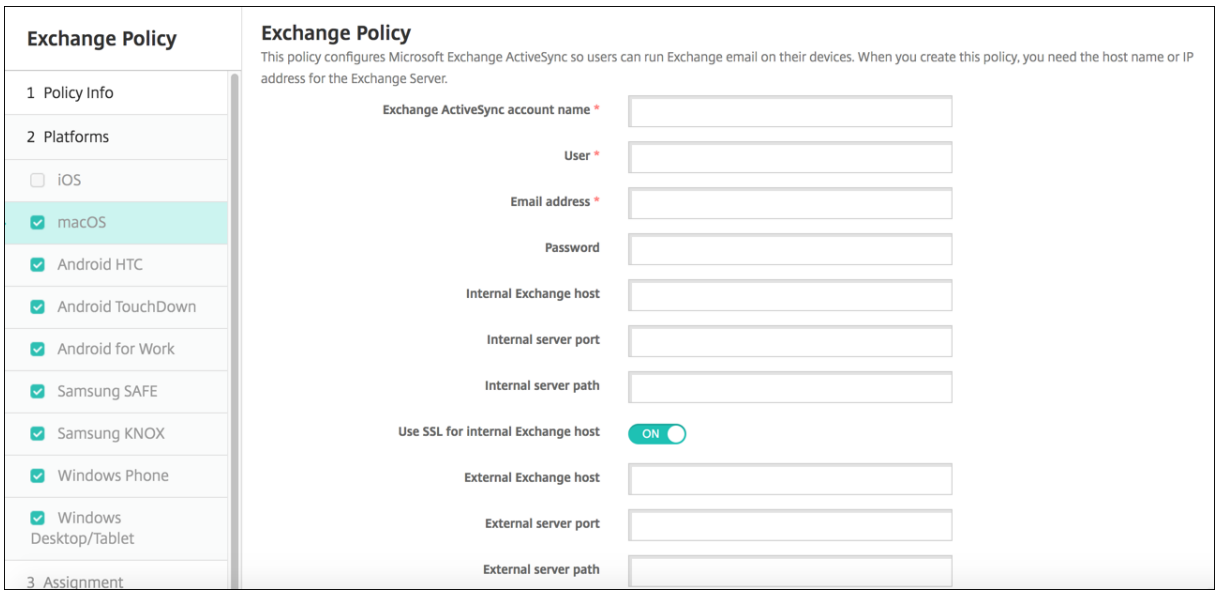


- **Nombre de la cuenta de Exchange ActiveSync.** Escriba la descripción de la cuenta de correo electrónico que se muestra en los dispositivos de los usuarios.
- **Nombre de host de Exchange ActiveSync.** Escriba la dirección del servidor de correo electrónico.
- **Usar SSL.** Seleccione si proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. Está **activado** de forma predeterminada.
- **Dominio:** Escriba el dominio donde reside el servidor Exchange. Puede utilizar la macro de sistema $user.domainname en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **Usuario.** 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.
- **Dirección de correo electrónico:** Especifique la dirección completa de correo electrónico. Puede utilizar la macro de sistema $user.mail en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Usar OAuth:** Si está **activado**, la conexión usa OAuth para la autenticación. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.
- **Contraseña:** Escriba una contraseña opcional para la cuenta de usuario de Exchange. Esta configuración no aparece cuando **Usar OAuth** está **activado**.
- **Intervalo de sincronización de correo electrónico.** En la lista, seleccione la frecuencia de sincronización del correo electrónico con el servidor Exchange Server. El valor predeterminado es de **3 días**.

- **Credencial de identidad (PKI o almacén de claves).** 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 **Ninguno**.
- **Autorizar el movimiento de correo entre cuentas.** Seleccione si permitir a los usuarios transferir correos electrónicos de esta cuenta a otra cuenta, reenviarlos y responder a ellos desde otra cuenta. Está **desactivado** de forma predeterminada.
- **Enviar correo electrónico solo desde aplicación de correo electrónico.** Seleccione esta opción para obligar a los usuarios a utilizar la aplicación Correo de iOS para enviar correos electrónicos. Está **desactivado** de forma predeterminada.
- **Inhabilitar sincronización de correo reciente.** Seleccione esta opción si quiere evitar que los usuarios sincronicen direcciones recientes. Está **desactivado** de forma predeterminada. Esta opción solo se aplica a iOS 6.0 y versiones posteriores.
- **Habilitar firma S/MIME:** Seleccione si esta cuenta admite la firma S/MIME. Está **activado** de forma predeterminada. Si se **activa**, aparecen los siguientes campos.
  - **Credencial de identidad para firma.** Seleccione la credencial de firma que se va a usar.
  - **Firma S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden activar y desactivar la firma S/MIME en la configuración de sus dispositivos. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.
  - **UUID de certificado de firma S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden seleccionar, en la configuración de sus dispositivos, la credencial de firma que se va a usar. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.
- **Habilitar cifrado S/MIME:** Seleccione si esta cuenta admite el cifrado S/MIME. Está **desactivado** de forma predeterminada. Si se **activa**, aparecen los siguientes campos.
  - **Credencial de identidad para cifrado.** Seleccione la credencial de cifrado que se va a usar.
  - **Habilitar cambio de opción S/MIME para cada mensaje:** Cuando se **activa**, los usuarios ven una opción para activar o desactivar el cifrado S/MIME para cada mensaje que escriban. Está **desactivado** de forma predeterminada.
  - **Cifrado S/MIME predeterminado reemplazable por el usuario:** Si se **activa**, los usuarios pueden, en la configuración de sus dispositivos, seleccionar si S/MIME está activado de forma predeterminada. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.
  - **UUID de certificado de cifrado S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden activar y desactivar el cifrado S/MIME y la identidad del cifrado S/MIME en la configuración de sus dispositivos. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.
- **Configuraciones de directivas**

- **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
  - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de macOS

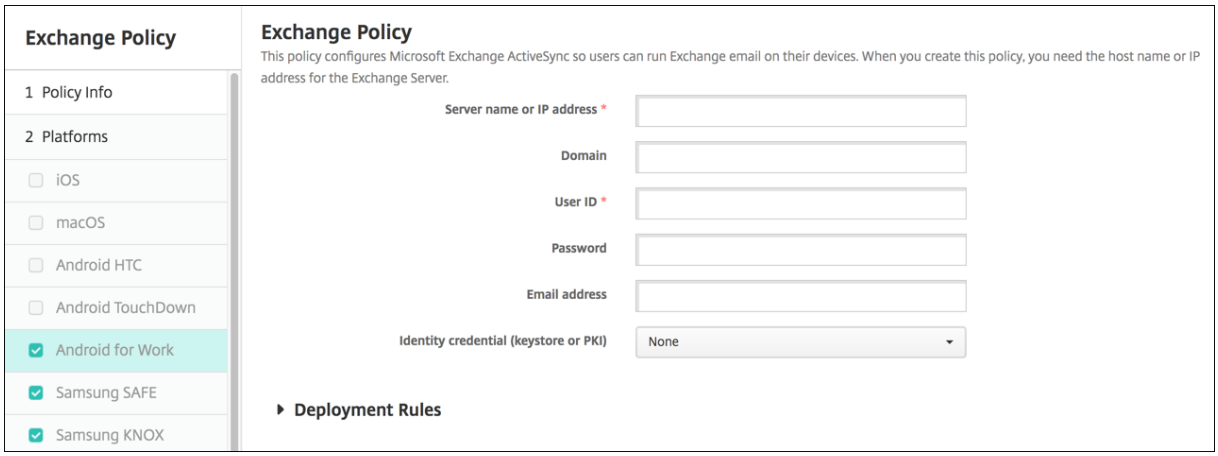


- **Nombre de la cuenta de Exchange ActiveSync.** Escriba la descripción de la cuenta de correo electrónico que se muestra en los dispositivos de los usuarios.
- **Usuario.** Especifique el nombre de usuario de la cuenta de usuario de Exchange. Puede utilizar la macro de sistema $user.username en este campo para buscar automáticamente los nombres de los usuarios.
- **Dirección de correo electrónico:** Especifique la dirección completa de correo electrónico. Puede utilizar la macro de sistema $user.mail en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Usar OAuth:** Si está **activado**, la conexión usa OAuth para la autenticación. Está **desactivado** de forma predeterminada. Esta opción se aplica a macOS 10.14 y versiones posteriores.
- **URL de inicio de sesión de OAuth:** En este campo se indica la URL a cargar en una vista web para autenticarse mediante OAuth cuando no se usa Autodiscovery Service. Este campo aparece tras **activarse** la configuración **Usar OAuth**.

- **Contraseña:** Escriba una contraseña opcional para la cuenta de usuario de Exchange. Esta configuración no aparece cuando **Usar OAuth** está **activado**.
- **Host de Exchange interno.** Si quiere que los nombres de host interno y externo de Exchange difieran, puede escribir un nombre de host interno de Exchange.
- **Puerto del servidor interno.** Si quiere que los puertos de servidor interno y externo de Exchange difieran, puede escribir un número de puerto para el servidor interno de Exchange.
- **Ruta del servidor interno.** Si quiere que las rutas de servidor interno y externo de Exchange difieran, puede escribir una ruta de servidor interno de Exchange.
- **Usar SSL para el host de Exchange interno.** Seleccione si proteger las conexiones entre los dispositivos de los usuarios y el host interno de Exchange. Está **activado** de forma predeterminada.
- **Host de Exchange externo.** Si quiere que los nombres de host interno y externo de Exchange difieran, puede escribir un nombre de host externo de Exchange.
- **Puerto del servidor externo.** Si quiere que los puertos de servidor interno y externo de Exchange difieran, puede escribir un número de puerto para el servidor externo de Exchange.
- **Ruta del servidor externo.** Si quiere que las rutas de servidor interno y externo de Exchange difieran, puede escribir una ruta de servidor externo de Exchange.
- **Usar SSL para el host de Exchange externo.** Seleccione si proteger las conexiones entre los dispositivos de los usuarios y el host interno de Exchange. Está **activado** de forma predeterminada.
- **Permitir 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). Está **desactivado** de forma predeterminada.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y

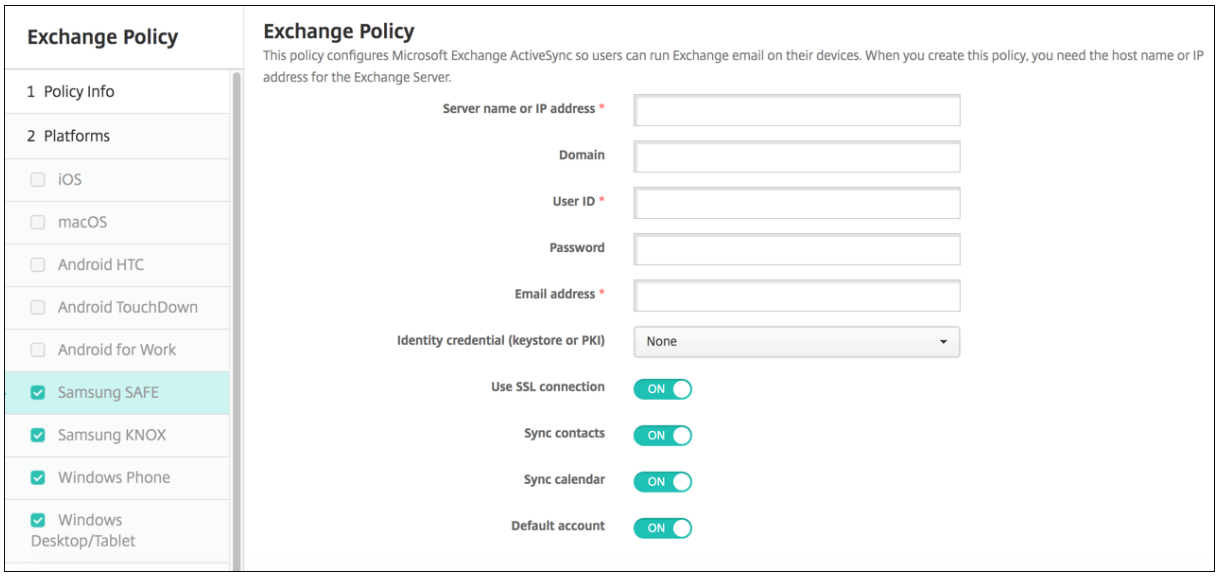
versiones posteriores.

Android Enterprise



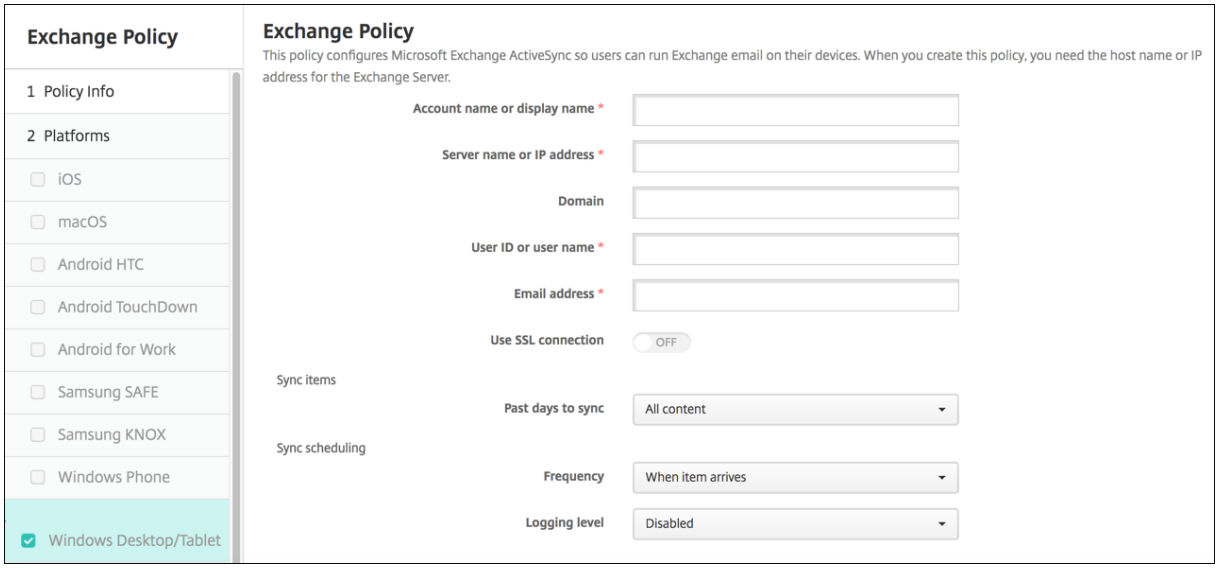
- **Nombre o dirección IP del servidor:** Escriba el nombre de host o la dirección IP del servidor Exchange.
- **Dominio:** Escriba el dominio donde reside el servidor Exchange. Puede utilizar la macro de sistema $user.domainname en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **ID de usuario:** Especifique el nombre de usuario de la cuenta de Exchange. Puede utilizar la macro de sistema $user.username en este campo para buscar automáticamente los nombres de los usuarios.
- **Contraseña:** Escriba una contraseña opcional para la cuenta de usuario de Exchange.
- **Dirección de correo electrónico:** Especifique la dirección completa de correo electrónico. Puede utilizar la macro de sistema $user.mail en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Credencial de identidad (PKI o almacén de claves).** 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 **Ninguno**.

Parámetros de Samsung SAFE y Samsung Knox



- **Nombre o dirección IP del servidor:** Escriba el nombre de host o la dirección IP del servidor Exchange.
- **Dominio:** Escriba el dominio donde reside el servidor Exchange. Puede utilizar la macro de sistema $user.domainname en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **ID de usuario:** Especifique el nombre de usuario de la cuenta de Exchange. Puede utilizar la macro de sistema $user.username en este campo para buscar automáticamente los nombres de los usuarios.
- **Contraseña:** Escriba una contraseña opcional para la cuenta de usuario de Exchange.
- **Dirección de correo electrónico:** Especifique la dirección completa de correo electrónico. Puede utilizar la macro de sistema $user.mail en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Credencial de identidad (PKI o almacén de claves).** 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.
- **Usar conexión SSL:** Seleccione si proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. Está **activado** de forma predeterminada.
- **Sincronizar contactos.** Seleccione si habilitar la sincronización de los contactos de los usuarios entre los dispositivos y el servidor Exchange. Está **activado** de forma predeterminada.
- **Sincronizar calendario.** Seleccione si habilitar la sincronización de los calendarios de los usuarios entre los dispositivos y el servidor Exchange. Está **activado** de forma predeterminada.
- **Cuenta predeterminada.** Marque la casilla para que la cuenta de usuarios Exchange sea la predeterminada para enviar correos electrónicos desde los dispositivos. Está **activado** de forma predeterminada.

Parámetros de Windows Phone y escritorios y tabletas Windows



Nota:

Esta directiva no permite establecer la contraseña de usuario. Los usuarios deben establecer ese parámetro desde sus dispositivos después de que se envíe la directiva.

- **Nombre de cuenta o nombre simplificado.** Escriba el nombre de la cuenta de Exchange ActiveSync.
- **Nombre o dirección IP del servidor:** Escriba el nombre de host o la dirección IP del servidor Exchange.
- **Dominio:** Escriba el dominio donde reside el servidor Exchange. Puede utilizar la macro de sistema $user.domainname en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **ID de usuario o nombre de usuario:** Especifique el nombre de usuario para la cuenta de Exchange. Puede utilizar la macro de sistema $user.username en este campo para buscar automáticamente los nombres de los usuarios.
- **Dirección de correo electrónico:** Especifique la dirección completa de correo electrónico. Puede utilizar la macro de sistema $user.mail en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Usar conexión SSL:** Seleccione si proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. Está **desactivado** de forma predeterminada.
- **Días pasados a sincronizar:** En la lista, haga clic en la cantidad de días pasados con los que se sincronizará todo el contenido del dispositivo con el servidor Exchange. El valor predeterminado es **Todo el contenido**.
- **Frecuencia:** 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 **Cuando llega el mensaje**.

- **Nivel de registro:** En la lista, haga clic en **Inhabilitado**, **Básico** o **Avanzado** para especificar el nivel de detalle que se seguirá a la hora de registrar la actividad de Exchange. De forma predeterminada, está **inhabilitado**.

Directiva de archivos

January 4, 2022

Puede agregar e implementar archivos para que los usuarios accedan en sus dispositivos Android y Android Enterprise. Especifique el directorio donde quiere almacenar el archivo en el dispositivo. Por ejemplo, quiere que los usuarios reciban un documento de empresa o un archivo .pdf. Implemente el archivo en los dispositivos e informe a los usuarios de dónde se encuentra el archivo.

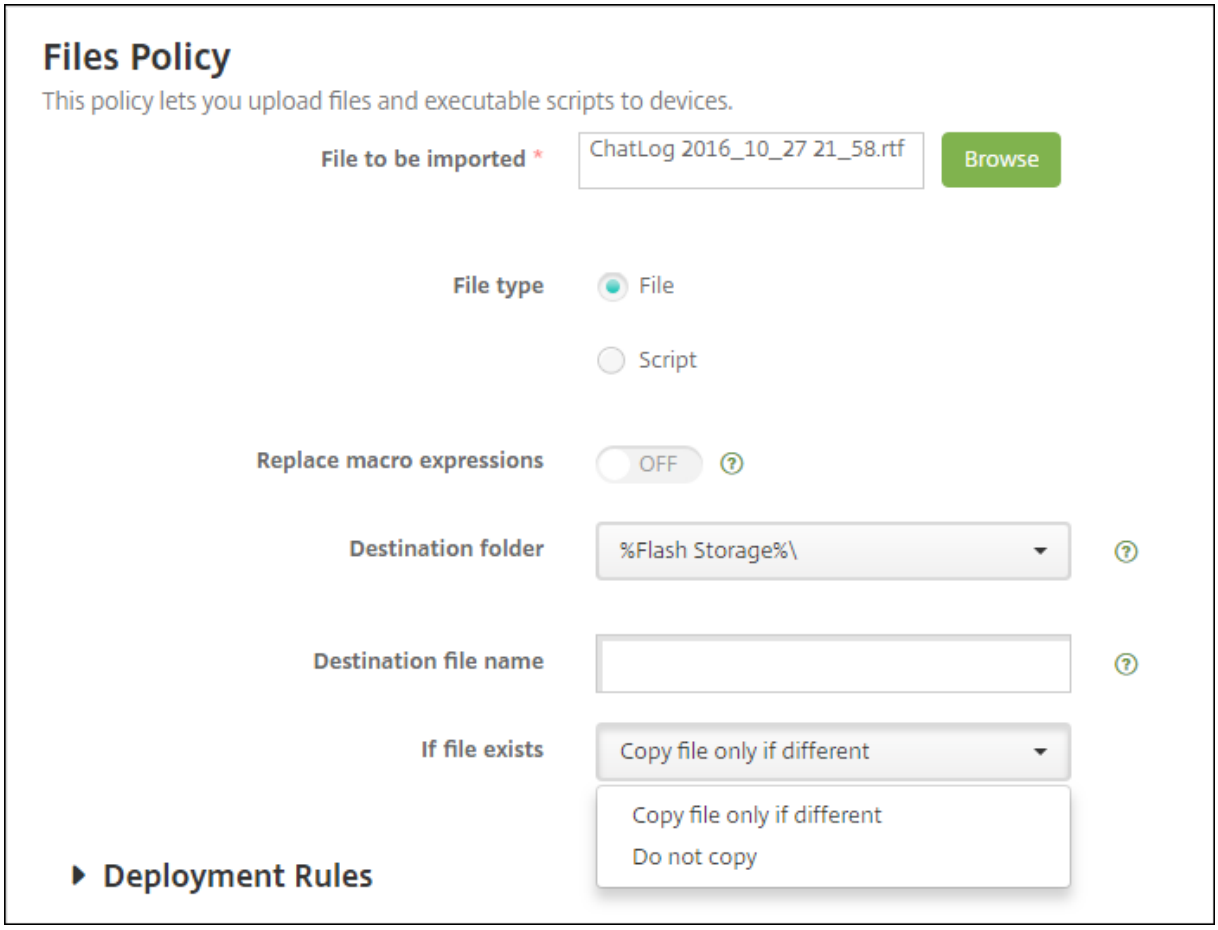
Los dispositivos Android no admiten la ejecución de scripts de forma nativa. Los usuarios necesitan software de terceros para ejecutar scripts.

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

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Android Enterprise



- **Archivo para importar:** Para seleccionar el archivo que quiere importar, haga clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.
- **Tipo de archivo:** Seleccione **Archivo** o **Script**.
- **Ejecutar inmediatamente:** Al seleccionar **Script**, aparece la opción **Ejecutar inmediatamente**. No sucede nada cuando se habilita este parámetro. Los usuarios deben ejecutar el script manualmente. **Reemplazar expresiones de macros:** Seleccione si quiere reemplazar nombres de token de macro en un script por una propiedad de usuario o de dispositivo. Para obtener la sintaxis de las macros, consulte Macros. Está **desactivado** de forma predeterminada.
- **Carpeta de destino:** En la lista, seleccione la ubicación en que almacenar el archivo cargado, o bien haga clic en **Agregar nuevo** para elegir una ubicación de archivo no incluida en la lista. También puede usar las macros %XenMobile Folder%\ o %Flash Storage%\ como inicio del identificador de ruta.
- **Nombre del archivo de destino:** Opcional. Si debe cambiar el nombre de un archivo antes de implementarlo en un dispositivo, escriba el nombre del archivo.
- **Si ya existe el archivo:** en la lista, seleccione si quiere copiar un archivo existente. La opción predeterminada es **Copiar el archivo solo si es diferente**.

Parámetros de Android

- **Archivo para importar:** Seleccione el archivo a importar; para ello, haga clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.
- **Tipo de archivo:** Seleccione **Archivo** o **Script**.
- **Ejecutar inmediatamente:** Al seleccionar **Script**, aparece la opción **Ejecutar inmediatamente**. No sucede nada cuando se habilita este parámetro. Los usuarios deben ejecutar el script manualmente. **Reemplazar expresiones de macros:** Seleccione si quiere reemplazar nombres de token de macro en un script por una propiedad de usuario o de dispositivo. Está **desactivado** de forma predeterminada.
- **Carpeta de destino:** En la lista, seleccione la ubicación en que almacenar el archivo cargado, o bien haga clic en **Agregar nuevo** 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.
- **Nombre del archivo de destino.** Si quiere, puede dar aquí un nombre diferente al archivo en caso de que sea necesario cambiarlo antes de implementarlo en un dispositivo.
- **Copiar el archivo solo si es diferente.** 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”.

Parámetros de Windows Mobile/CE

- **Archivo para importar:** Seleccione el archivo a importar; para ello, haga clic en “Examinar” y, a continuación, vaya a la ubicación del archivo.
- **Tipo de archivo:** Seleccione **Archivo** o **Script**.
- **Ejecutar inmediatamente:** Al seleccionar **Script**, aparece **Ejecutar inmediatamente**. Seleccione si quiere que el script se ejecute tan pronto como el archivo se cargue. Está **desactivado** de forma predeterminada.
- **Reemplazar expresiones de macros:** Seleccione si quiere reemplazar nombres de token de macro en un script por una propiedad de usuario o de dispositivo. Está **desactivado** de forma predeterminada.
- **Carpeta de destino:** En la lista, seleccione la ubicación en que almacenar el archivo cargado, o bien haga clic en **Agregar nuevo** 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%\

- **Nombre del archivo de destino.** Si quiere, puede dar aquí un nombre diferente al archivo en caso de que sea necesario cambiarlo antes de implementarlo en un dispositivo.
- **Copiar el archivo solo si es diferente.** 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”.
- **Archivo de solo lectura.** Seleccione si el archivo será de solo lectura. Está **desactivado** de forma predeterminada.
- **Archivo oculto.** Seleccione esta opción si no quiere que el archivo se muestre en la lista de archivos. Está **desactivado** de forma predeterminada.

Directiva de FileVault

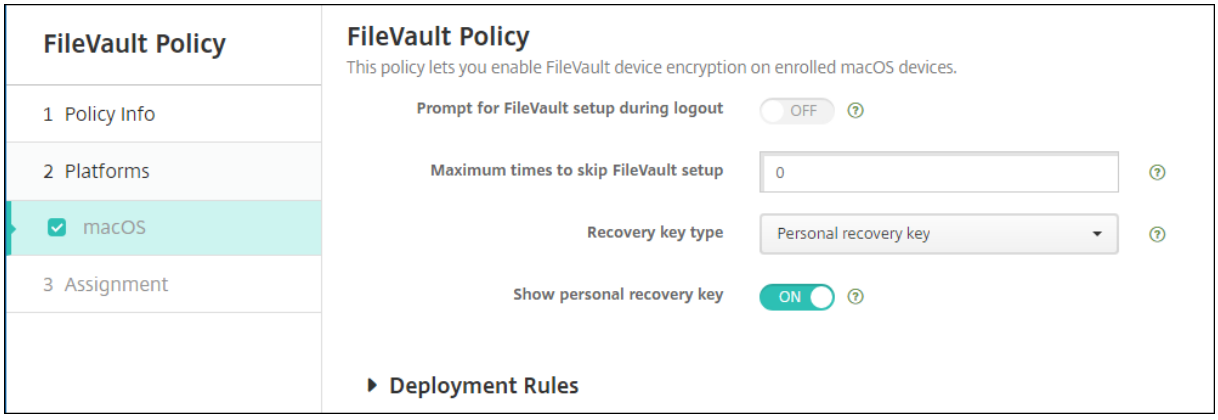
January 4, 2022

En macOS, la funcionalidad de cifrado de disco FileVault protege el volumen del sistema cifrando su contenido. Con FileVault habilitado en un dispositivo macOS, el usuario debe iniciar sesión con su contraseña de cuenta cada vez que se inicia el dispositivo. Si el usuario pierde la contraseña, una clave de recuperación le permite desbloquear el disco y restablecerla.

La directiva de dispositivo de XenMobile llamada FileVault permite al usuario de FileVault configurar pantallas y definir parámetros (como claves de recuperación). Para obtener más información acerca de FileVault, consulte el artículo de asistencia de Apple: https://support.apple.com.

Para agregar la directiva de FileVault, vaya a **Configurar > Directivas de dispositivo**.

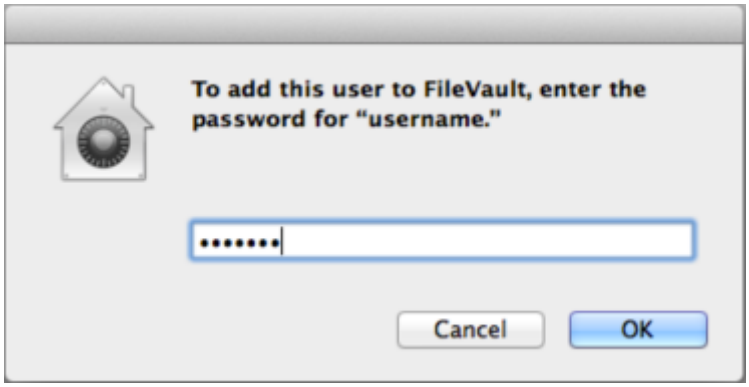
Parámetros de macOS



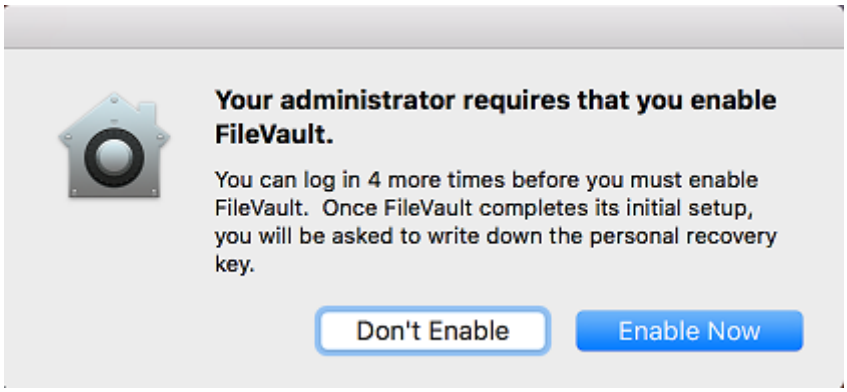
- **Solicitar la configuración de FileVault durante el cierre de sesión:** Si el valor es **Sí**, se pide al usuario que habilite FileVault una vez pasados los cierres de sesión indicados en la opción

Máximo de veces que se puede omitir la configuración de FileVault. Cuando el valor es **No**, no aparece la solicitud de contraseña de FileVault.

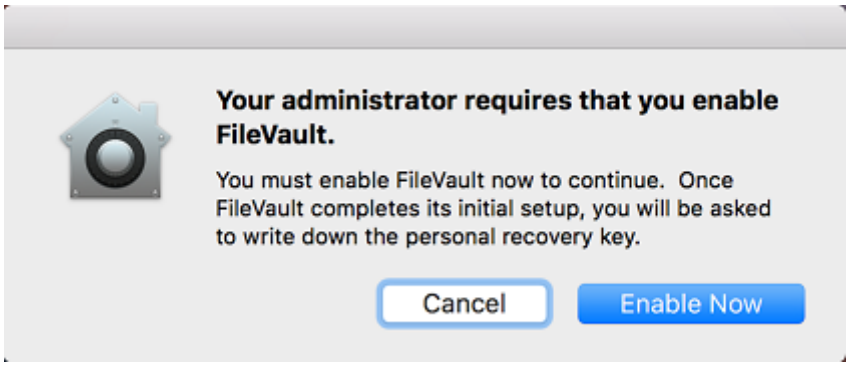
Después de implementar la directiva de FileVault con este parámetro activado, aparece la siguiente pantalla cuando un usuario cierra sesión en el dispositivo. La pantalla ofrece al usuario la opción de habilitar FileVault antes del cierre de sesión.

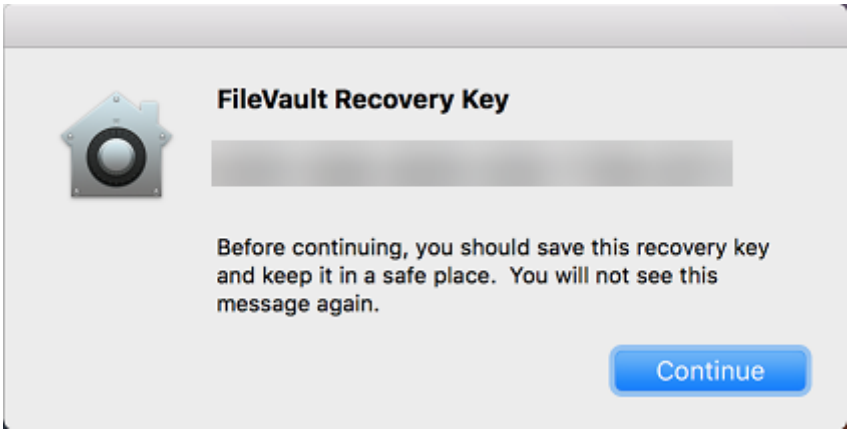


Si el valor de **Máximo de veces que se puede omitir la configuración de FileVault** no es 0, después de implementar la directiva FileVault con esta configuración desactivada, aparece la pantalla siguiente cuando el usuario inicia sesión.



Si el valor de **Máximo de veces que se puede omitir la configuración de FileVault** es 0 o el usuario ha omitido la configuración la cantidad máxima indicada de veces, aparece la siguiente pantalla.





Directiva de fuentes

January 4, 2022

En XenMobile, puede agregar una directiva para añadir fuentes de texto adicionales a dispositivos iOS y macOS. Las fuentes deben tener el formato TrueType (.ttf) u OpenType (.oft). No se admiten las colecciones de fuentes (.ttc u .otc).

Esta directiva solo se aplica a iOS 7.0 y versiones posteriores.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Nombre visible para el usuario:** Escriba el nombre que verán los usuarios en sus listas de fuentes.
- **Archivo de la fuente:** Seleccione el archivo de fuentes que se va a agregar a los dispositivos de los usuarios. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de macOS

- **Nombre visible para el usuario:** Escriba el nombre que verán los usuarios en sus listas de fuentes.
- **Archivo de la fuente:** Seleccione el archivo de fuentes que se va a agregar a los dispositivos de los usuarios. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Directiva de diseño de pantalla de inicio

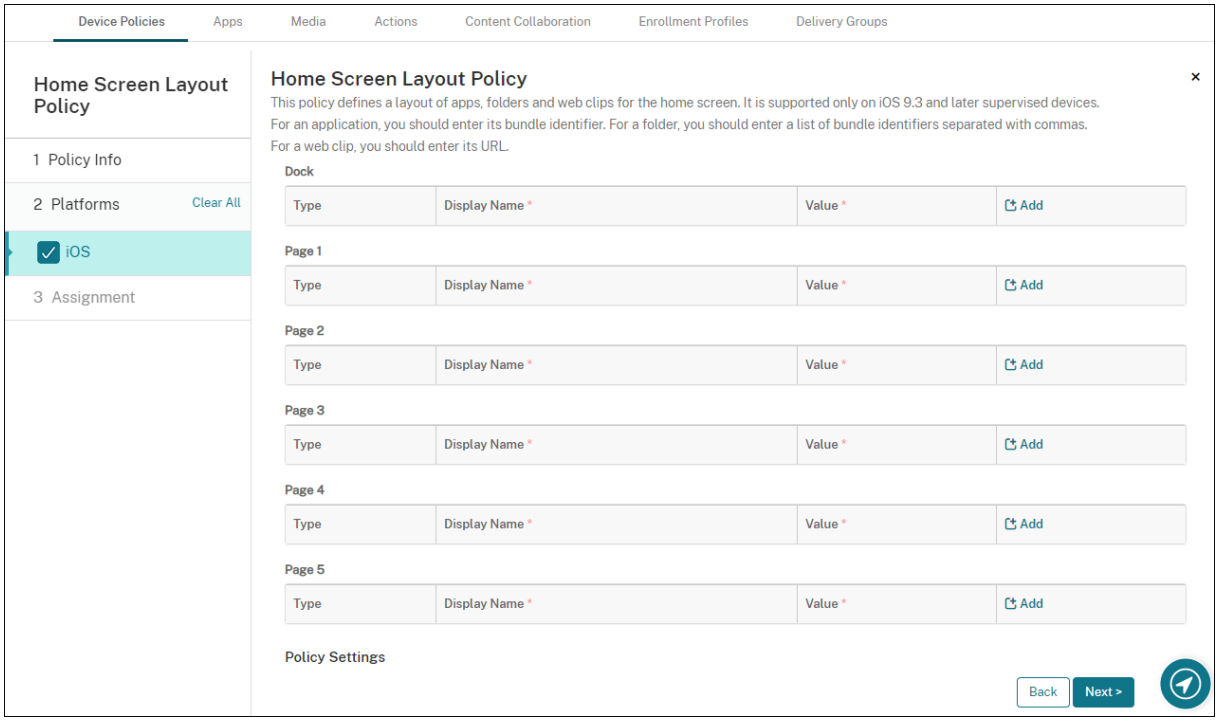
January 4, 2022

Puede especificar la distribución de las aplicaciones y las carpetas en la pantalla de inicio de iOS. La directiva de diseño de pantalla inicial es para dispositivos supervisados iOS 9.3 y versiones posteriores.

> **Importante:**
>
> La implementación de varias directivas de diseño de pantalla inicial en un dispositivo provoca un error de iOS en el dispositivo. Esta limitación se aplica tanto si la pantalla inicial se define a través de esta directiva de XenMobile o a través de Apple Configurator.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

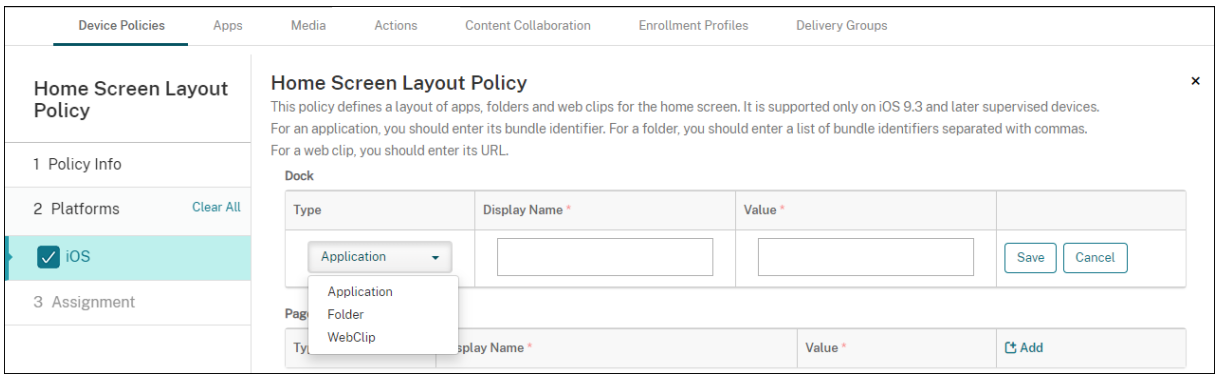
Parámetros de iOS



- Haga clic en **Agregar** para agregar cada una de las áreas de la pantalla que quiera configurar (como **Dock** o **Página 1**).
- **Tipo:** Elija **Aplicación**, **Carpeta** o **Clip web**.

  El parámetro **Uso restringido de aplicaciones > Permitir solo algunas aplicaciones** en la directiva de restricciones puede evitar que los clips web aparezcan correctamente en la pantalla de inicio. Para que los clips web aparezcan correctamente, realice una de las siguientes acciones:

  - Establezca **Uso restringido de aplicaciones** en **Permitir todas las aplicaciones** o en **No permitir algunas aplicaciones**.
  - Con **Uso restringido de aplicaciones** configurado en **Permitir solo algunas aplicaciones**, agregue una aplicación con el ID de paquete `com.apple.webapp` para permitir clips web.



- **Nombre simplificado:** El nombre de la aplicación o la carpeta que aparecerá en la pantalla de inicio.
- **Valor:** Para las aplicaciones, introduzca el ID de paquete. En caso de carpetas, introduzca una lista de identificadores de paquete, separados por comas. En caso de clips web, introduzca el ID del paquete `com.apple.webClip.managed` y configure la dirección URL del clip web en la directiva de clips web. Si existe más de un valor de clip web con la misma URL, el comportamiento no está definido en dispositivos iOS 11.3 y versiones posteriores.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible en iOS 9.3 y versiones posteriores.

Directiva de importación de perfiles de iOS y macOS

January 4, 2022

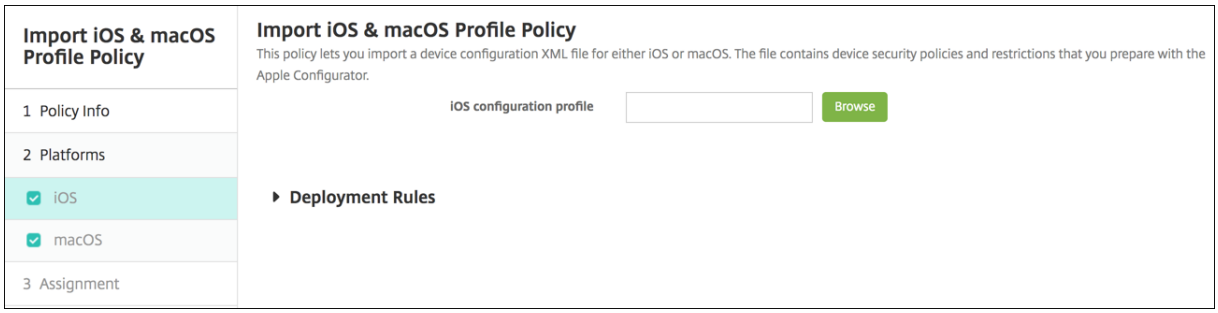
Puede importar en XenMobile archivos XML de configuración de dispositivos iOS y macOS. El archivo contiene las restricciones y las directivas seguridad de los dispositivos que se preparan con Apple Configurator.

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 Configu-

rator para crear un archivo de configuración, consulte el Soporte técnico de Apple Configurator.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS y macOS



- **Perfil de configuración de iOS** o **Perfil de configuración de macOS.** Seleccione el archivo de configuración que quiera importar. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.

Colocar un dispositivo iOS en modo supervisado mediante Apple Configurator

Para usar Apple Configurator, necesita un equipo de Apple con macOS 10.7.2 o una versión más reciente.

> **Importante:**
>
> Colocar un dispositivo en el modo supervisado instala 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 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) **Active** el indicador **Supervisar**. 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 **Más reciente** 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 **Preparar**.

Directiva de dispositivos de administración de Keyguard

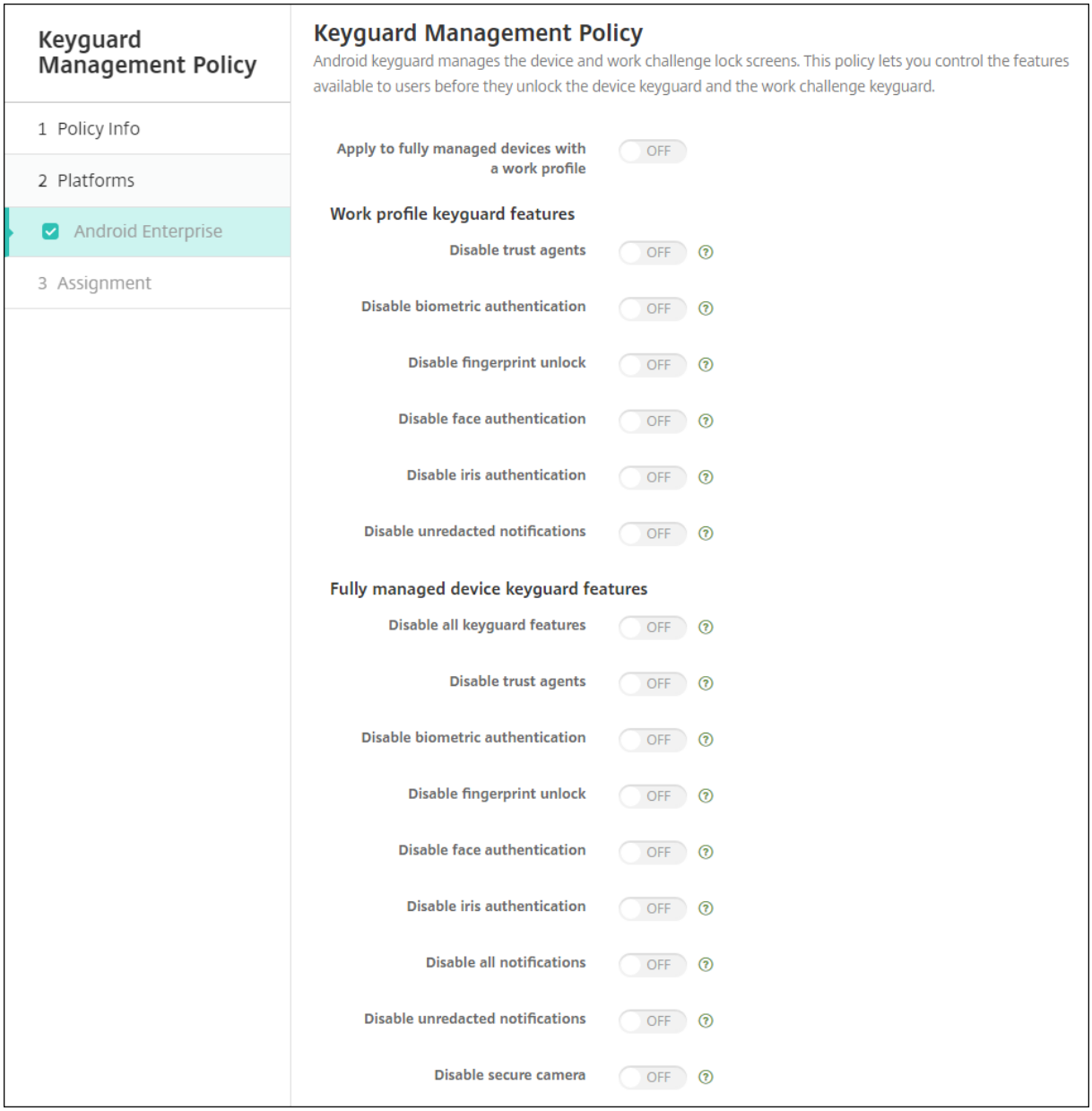
December 17, 2020

Android Keyguard administra las pantallas de bloqueo del dispositivo y de Work Challenge. Esta directiva le permite controlar funciones de Keyguard del perfil de trabajo y funciones de Keyguard avanzadas del dispositivo en Android Enterprise. Puede controlar:

- Administración de Keyguard en dispositivos de perfil de trabajo. Puede especificar las funciones disponibles para los usuarios antes de que desbloqueen el Keyguard del dispositivo y el Keyguard de Work Challenge. Por ejemplo, de forma predeterminada, los usuarios pueden usar desbloqueo mediante huella digital y ver notificaciones sin redactar en la pantalla de bloqueo.
- Administración de Keyguard en dispositivos dedicados y totalmente administrados. Puede especificar las funciones disponibles, como agentes de confianza y cámara segura, antes de que desbloqueen la pantalla de Keyguard. O bien, puede optar por desactivar todas las funciones de Keyguard.
- Administración de Keyguard en dispositivos totalmente administrados con perfiles de trabajo. Puede utilizar una directiva de administración de Keyguard para aplicar configuraciones independientes al dispositivo y al perfil de trabajo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Android Enterprise



- **Aplicar a dispositivos totalmente administrados con un perfil de trabajo:** Permite configurar los parámetros de la directiva de dispositivos de administración de Keyguard para dispositivos totalmente administrados con perfiles de trabajo.

  Si el valor es **Sí**, puede aplicar configuraciones independientes al dispositivo y al perfil de trabajo en dispositivos totalmente administrados con perfiles de trabajo.

  Si el valor es **No**, puede aplicar la configuración a dispositivos de perfil de trabajo o dispositivos totalmente administrados. Los parámetros que configure para los perfiles de trabajo solo se aplicarán a los dispositivos de perfil de trabajo. Los parámetros que configure para dispositivos

totalmente administrados solo se aplicarán a los dispositivos totalmente administrados.

Está **desactivado** de forma predeterminada.

- **Funciones de Keyguard del perfil de trabajo:** Controla si las siguientes funciones estarán disponibles antes de que un usuario desbloquee el Keyguard del perfil de trabajo (pantalla de bloqueo).
  - **Inhabilitar agentes de confianza:** Si el valor es **No**, los agentes de confianza pueden operar en pantallas de Keyguard seguras cuando se establece un desafío en el perfil de trabajo. Establézcalo en **Sí** para inhabilitar todos los agentes de confianza en el perfil de trabajo. Está **desactivado** de forma predeterminada.
  - **Inhabilitar autenticación biométrica:** Si el valor es **No**, la autenticación biométrica está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el perfil de trabajo. Establezca el valor en **Sí** para inhabilitar la autenticación biométrica en el perfil de trabajo. Esta configuración inhabilita el desbloqueo por huella dactilar, la autenticación facial y la autenticación del iris. Está **desactivado** de forma predeterminada. Para Android 9.0 y versiones posteriores.
  - **Inhabilitar desbloqueo mediante huella digital:** Si el valor es **Sí**, el desbloqueo mediante huella digital no está disponible en pantallas Keyguard seguras cuando se establece un desafío en el perfil de trabajo. Establézcalo en **No** para habilitar el desbloqueo mediante huella digital en el perfil de trabajo. Está **desactivado** de forma predeterminada.
  - **Inhabilitar autenticación facial:** Si el valor es **No**, la autenticación facial está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el perfil de trabajo. Establezca el valor en **Sí** para inhabilitar la autenticación facial en el perfil de trabajo. Está **desactivado** de forma predeterminada. Para Android 9.0 y versiones posteriores.
  - **Inhabilitar autenticación de iris:** Si el valor es **No**, la autenticación de iris está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el perfil de trabajo. Establezca el valor en **Sí** para inhabilitar la autenticación de iris en el perfil de trabajo. Está **desactivado** de forma predeterminada. Para Android 9.0 y versiones posteriores.
  - **Inhabilitar notificaciones sin redactar:** Si el valor es **No**, las notificaciones redactadas y sin redactar aparecen en las pantallas de Keyguard seguras. Establezca el valor en **Sí** para inhabilitar las notificaciones sin redactar y mostrar solo las notificaciones redactadas. Está **desactivado** de forma predeterminada.
- **Funciones de Keyguard del dispositivo totalmente administradas:** Controla si las siguientes funciones están disponibles antes de que un usuario desbloquee el Keyguard del dispositivo (pantalla de bloqueo). Estas funciones son aplicables a dispositivos totalmente administrados o dedicados.
  - **Inhabilitar todas las funciones de Keyguard:** Si el valor es **No**, todas las personalizaciones actuales y futuras de Keyguard estarán disponibles en las pantallas seguras de Keyguard. Establézcalo en **Sí** para desactivar todas las personalizaciones de Keyguard. Está

desactivado de forma predeterminada.

- **Inhabilitar agentes de confianza:** Si el valor es **No**, los agentes de confianza pueden operar en pantallas de Keyguard seguras. Establézcalo en **Sí** para inhabilitar los agentes de confianza. Está **desactivado** de forma predeterminada.
- **Inhabilitar autenticación biométrica:** Si el valor es **No**, la autenticación biométrica está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el dispositivo. Establezca el valor en **Sí** para inhabilitar la autenticación biométrica en el dispositivo. Así, se inhabilita el desbloqueo por huella dactilar, la autenticación facial y la autenticación del iris. Está **desactivado** de forma predeterminada. Para Android 9.0 y versiones posteriores.
- **Inhabilitar desbloqueo mediante huella digital:** Si el valor es **No**, el desbloqueo mediante huella digital está disponible en pantallas Keyguard seguras cuando se establece un desafío en el dispositivo. Establézcalo en **Sí** para inhabilitar el desbloqueo mediante huella digital en el dispositivo. Está **desactivado** de forma predeterminada.
- **Inhabilitar autenticación facial:** Si el valor es **No**, la autenticación facial está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el dispositivo. Establezca el valor en **Sí** para inhabilitar la autenticación facial en el dispositivo. Está **desactivado** de forma predeterminada. Para Android 9.0 y versiones posteriores.
- **Inhabilitar autenticación de iris:** Si el valor es **No**, la autenticación de iris está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el dispositivo. Establezca el valor en **Sí** para inhabilitar la autenticación de iris en el dispositivo. Está **desactivado** de forma predeterminada. Para Android 9.0 y versiones posteriores.
- **Inhabilitar todas las notificaciones:** Si el valor es **No**, todas las notificaciones aparecerán en las pantallas seguras de Keyguard. Establézcalo en **Sí** para mostrar todas las notificaciones. Está **desactivado** de forma predeterminada.
- **Inhabilitar notificaciones sin redactar:** Si el valor es **No**, las notificaciones redactadas y sin redactar aparecen en las pantallas de Keyguard seguras. Establezca el valor en **Sí** para inhabilitar las notificaciones sin redactar y mostrar solo las notificaciones redactadas. Está **desactivado** de forma predeterminada.
- **Inhabilitar cámara segura:** Si el valor es **No**, la cámara segura está disponible en las pantallas seguras de Keyguard. Establézcalo en **Sí** para inhabilitar la cámara segura. Está **desactivado** de forma predeterminada.

Directiva de quiosco

January 4, 2022

La directiva Quiosco permite restringir los dispositivos al modo quiosco porque limita las aplicaciones que se pueden ejecutar en ellos: XenMobile no controla qué parte del dispositivo se bloquea en modo

quiosco. El dispositivo administra la configuración del modo quiosco después de que se haya implementado la directiva.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

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 clave de licencia MDM de Samsung. Este paso le permite habilitar directivas en dispositivos Samsung SAFE.
2. Habilite Firebase Cloud Messaging para dispositivos Android como se describe en Firebase Cloud Messaging. Este paso permite que los dispositivos Android se conecten con XenMobile.
3. Agregue una directiva Quiosco como se describe en la sección siguiente.
4. Asigne esas tres directivas a los grupos de entrega correspondientes. Decida si quiere incluir otras directivas, como "Inventario de aplicaciones", en esos grupos de entrega.

   Para quitar los dispositivos del modo quiosco, cree una nueva directiva de quiosco que tenga el parámetro **Modo quiosco inhabilitado**. Actualice los grupos de entrega para quitar la directiva de quiosco que habilitaba el modo quiosco y agregue la directiva de quiosco que lo inhabilita.

Para agregar una directiva de quiosco

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.

Parámetros de Samsung SAFE

Puede especificar que solo se pueda usar una o varias aplicaciones específicas. Esta directiva es útil para los dispositivos de empresa diseñados para ejecutar solo un tipo o clase específicos de aplicaciones. Asimismo, esta directiva permite elegir imágenes personalizadas para la pantalla de inicio y fondos para la pantalla de bloqueo del dispositivo cuando el dispositivo está en modo quiosco.

- **Modo quiosco.** Haga clic en **Habilitar** o **Inhabilitar**. El valor predeterminado es **Habilitar**. Si hace clic en **Inhabilitar**, desaparecerán todas las opciones siguientes.
- **Paquete de inicio.** 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 usa un programa interno de inicio, escriba el nombre completo del paquete de aplicación de ese programa.

- **Número de teléfono para emergencias.** Escriba un número de teléfono opcional. Cualquier persona puede usar este número para ponerse en contacto con su empresa. Se aplica solo a MDM 4.0 y versiones posteriores.
- **Permitir barra de navegación.** Seleccione si permitir que los usuarios vean y usen la barra de navegación en el modo quiosco. Se aplica solo a MDM 4.0 y versiones posteriores. Está **activado** de forma predeterminada.
- **Permitir modo multiventana.** Seleccione si permitir que los usuarios usen varias ventanas en el modo quiosco. Se aplica solo a MDM 4.0 y versiones posteriores. Está **activado** de forma predeterminada.
- **Permitir barra de estado.** Seleccione si permitir que los usuarios vean la barra de estado en el modo quiosco. Se aplica solo a MDM 4.0 y versiones posteriores. Está **activado** de forma predeterminada.
- **Permitir barra de sistema.** Seleccione si permitir que los usuarios vean la barra del sistema en el modo quiosco. Está **activado** de forma predeterminada.
- **Permitir administrador de tareas.** Seleccione si permitir que los usuarios vean y usen el Administrador de tareas en el modo quiosco. Está **activado** de forma predeterminada.
- **Cambiar código SAFE común.** Este parámetro protege contra cambios por error en el campo de código de acceso común SAFE. Cuando está **desactivado**, no se puede cambiar el campo del código SAFE común. Está **desactivado** de forma predeterminada.
- **Código SAFE común.** Si ha configurado una directiva general de código de acceso a todos los dispositivos Samsung SAFE, escriba el mismo código opcional de la directiva en este campo.
- **Fondos de pantalla**
  - **Definir un fondo para la pantalla de inicio.** Seleccione si utilizar una imagen personalizada para la pantalla de inicio en el modo quiosco. Está **desactivado** de forma predeterminada.
    - **Imagen de pantalla de inicio.** Cuando habilite **Definir un fondo para la pantalla de inicio**, deberá seleccionar un archivo de imagen. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.
  - **Definir un fondo para la pantalla de bloqueo.** Seleccione si utilizar una imagen personalizada para la pantalla de bloqueo durante el modo quiosco. Está **desactivado** de forma predeterminada. Se aplica solo a MDM 4.0 y versiones posteriores.
    - **Imagen de bloqueo.** Cuando habilite **Definir un fondo para la pantalla de bloqueo**, deberá seleccionar un archivo de imagen. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.
- **Aplicaciones.** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada aplicación al modo quiosco:
  - **Aplicación nueva que agregar:** 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 **Guardar** para agregar la aplicación, o bien haga clic en **Cancelar** para no agregarla.

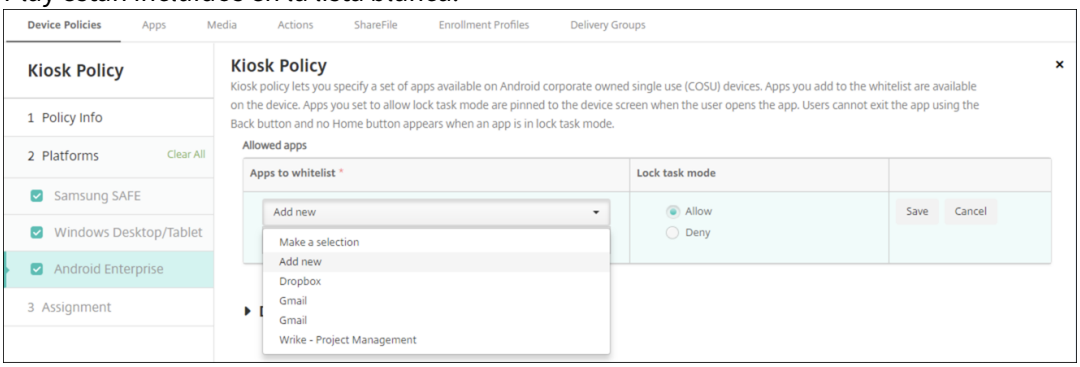
Parámetros de Android Enterprise

Para dispositivos Android Enterprise dedicados, que también se conocen como dispositivos de uso único y propiedad de la empresa (COSU), puede incluir aplicaciones en la lista de permitidos y establecer el modo de bloqueo de tarea. De forma predeterminada, los servicios Secure Hub y Google Play están en la lista de permitidos.

Para permitir una aplicación, haga clic en **Agregar**. Puedes permitir varias aplicaciones. Para obtener más información, consulte Android Enterprise.

> **Nota:**
>
> La consola de XenMobile Server contiene los términos “lista negra” y “lista blanca”. Estamos cambiando esos términos en una próxima versión a “lista de bloqueados” y “lista de permitidos”.

- **Aplicaciones para la lista blanca:** Indique el nombre del paquete de la aplicación que quiere incluir en la lista blanca o seleccione la aplicación en la lista.
  - Haga clic en **Agregar nuevo** para introducir el nombre del paquete de la aplicación aprobada que se mostrará en la lista.
  - Seleccione la aplicación existente de la lista. La lista muestra las aplicaciones cargadas en XenMobile Server. De forma predeterminada, los servicios de Secure Hub y Google Play están incluidos en la lista blanca.



- **Modo de bloqueo de tarea:** Seleccione **Permitir** para que la aplicación quede anclada en la pantalla del dispositivo cuando el usuario la abra. Elija **Denegar** para que la aplicación no quede anclada. De forma predeterminada, se permiten los servicios Secure Hub y Google Play. El valor predeterminado es **Allow**.

Cuando una aplicación se encuentra en el modo de bloqueo de tarea, esa aplicación queda anclada a la pantalla del dispositivo cuando el usuario la abre. No aparece el botón Inicio y el botón Atrás está desactivado. El usuario sale de la aplicación mediante una acción programada en la aplicación, como cerrar sesión.

Directiva de configuración del Launcher

September 19, 2021

Citrix Launcher permite personalizar la experiencia de usuario en los dispositivos Android implementados por XenMobile. Citrix Launcher y la directiva de dispositivo "Configuración de Launcher" no son compatibles con Android Enterprise.

Puede agregar una directiva de configuración de Launcher para controlar esas funciones de Citrix Launcher:

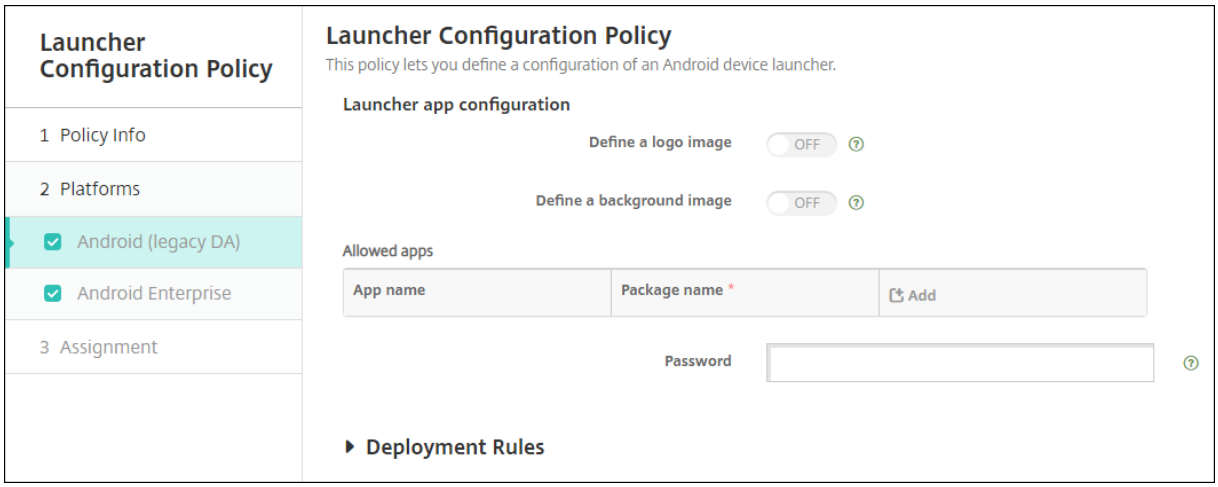
- Administre los dispositivos Android, de manera que los usuarios solo puedan acceder a las aplicaciones que especifique.
- Si lo prefiere, puede especificar una imagen de logo personalizada como icono de Citrix Launcher, así como una imagen de fondo para Citrix Launcher.
- Especifique una contraseña 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 Wi-Fi, 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).

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Android (AD heredado) y Android Enterprise



- **Definir una imagen de logotipo:** Seleccione si utilizar una imagen personalizada como logotipo para el icono de Citrix Launcher. Está **desactivado** de forma predeterminada.
- **Imagen de logotipo:** Cuando habilite **Definir una imagen de logotipo**, deberá seleccionar un archivo de imagen. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo. Los tipos de archivo admitidos son: PNG, JPG, JPEG y GIF.
- **Definir una imagen de fondo:** Seleccione si utilizar una imagen personalizada como imagen de fondo de Citrix Launcher. Está **desactivado** de forma predeterminada.
- **Imagen de fondo:** Cuando habilite **Definir una imagen de fondo**, deberá seleccionar un archivo de imagen. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo. Los tipos de archivo admitidos son: PNG, JPG, JPEG y GIF.
- **Aplicaciones permitidas:** Haga clic en **Agregar** y lleve a cabo lo siguiente para permitir cada aplicación en Citrix Launcher:
  - **Aplicación nueva que agregar:** 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 **Guardar** para agregar la aplicación, o bien haga clic en **Cancelar** para no agregarla.
- **Contraseña:** La contraseña que el usuario debe introducir para salir de Citrix Launcher.

Directiva de LDAP

January 4, 2022

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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Descripción de la cuenta.** Indique una descripción opcional de la cuenta.
- **Nombre de usuario de la cuenta.** Si quiere, escriba un nombre de usuario.
- **Contraseña de la cuenta.** Escriba una contraseña opcional. Use este campo solo con perfiles cifrados.
- **Nombre de host de LDAP.** Escriba el nombre de host del servidor LDAP. Este campo es obligatorio.

- **Usar SSL.** Seleccione si utilizar una capa de sockets seguros (SSL) en la conexión al servidor LDAP. Está **activado** de forma predeterminada.
- **Parámetros de búsqueda.** 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 **Agregar** y lleve a cabo lo siguiente:
  - **Descripción.** Introduzca una descripción de la opción de búsqueda. Este campo es obligatorio.
  - **Ámbito.** Seleccione **Base**, **Un nivel** o **Subárbol** 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 Búsqueda base.
    - El nivel **Un nivel** busca en el nodo Base y en un nivel por debajo de él.
    - El nivel **Subárbol** busca en el nodo Base y en todos sus elementos secundarios, independientemente de la cantidad de niveles de profundidad.
  - **Base de búsqueda.** 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 **Guardar** para agregar la opción de búsqueda, o bien haga clic en **Cancelar** para descartarla.
  - Repita estos pasos para cada opción de búsqueda que quiera agregar.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de macOS

- **Descripción de la cuenta.** Indique una descripción opcional de la cuenta.
- **Nombre de usuario de la cuenta.** Si quiere, escriba un nombre de usuario.
- **Contraseña de la cuenta.** Escriba una contraseña opcional. Use este campo solo con perfiles cifrados.
- **Nombre de host de LDAP.** Escriba el nombre de host del servidor LDAP. Este campo es obligatorio.
- **Usar SSL.** Seleccione si utilizar una capa de sockets seguros (SSL) en la conexión al servidor LDAP. Está **activado** de forma predeterminada.
- **Parámetros de búsqueda.** 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 **Agregar** y lleve a cabo lo siguiente:

- **Descripción.** Introduzca una descripción de la opción de búsqueda. Este campo es obligatorio.
- **Ámbito.** Seleccione **Base**, **Un nivel** o **Subárbol** 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 Búsqueda base.
  - El nivel **Un nivel** busca en el nodo Base y en un nivel por debajo de él.
  - El nivel **Subárbol** busca en el nodo Base y en todos sus elementos secundarios, independientemente de la cantidad de niveles de profundidad.
- **Base de búsqueda.** 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 **Guardar** para agregar la opción de búsqueda, o bien haga clic en **Cancelar** para descartarla.
- Repita estos pasos para cada opción de búsqueda que quiera agregar.

- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Directiva de localización geográfica

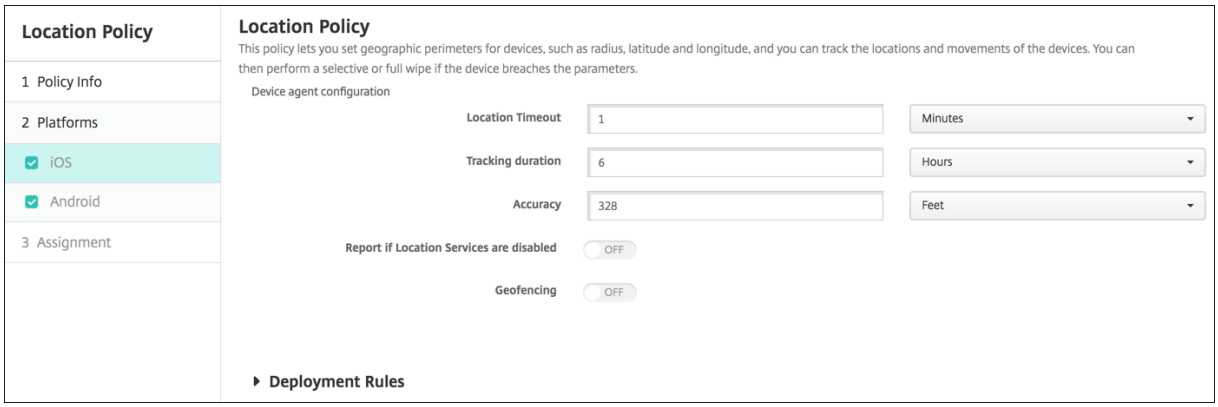
January 4, 2022

En XenMobile, puede crear directivas de localización geográfica para aplicar límites geográficos. Cuando los usuarios abandonen el perímetro definido, también llamado *geocerca*, XenMobile puede realizar determinadas acciones. Por ejemplo, puede configurar la directiva para emitir un mensaje de advertencia para los usuarios cuando estos abandonen el perímetro definido. También puede configurar la directiva para borrar datos empresariales de los usuarios cuando estos abandonen

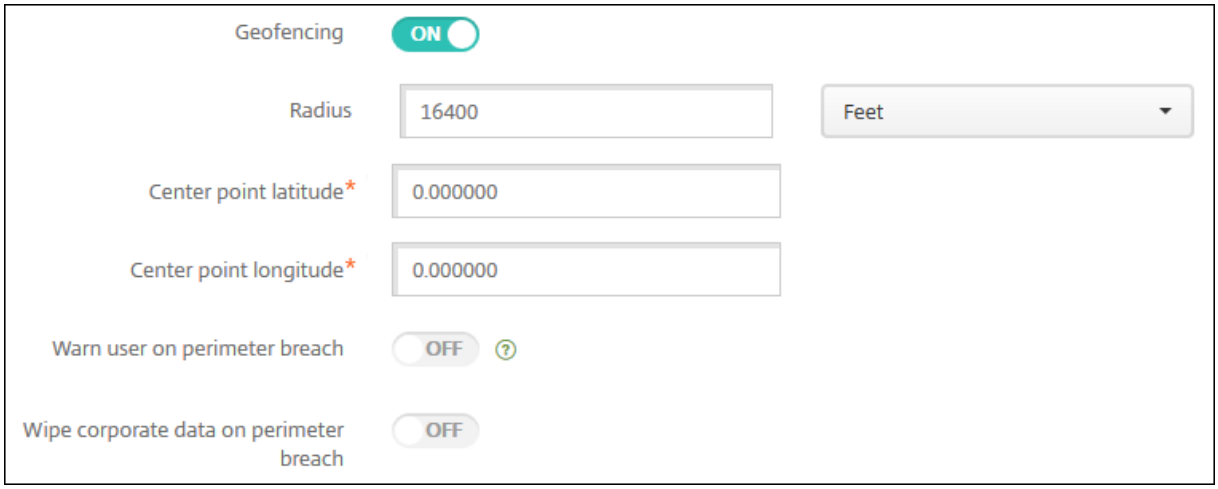
un perímetro, inmediatamente o pasado un período. Para obtener información acerca de las acciones de seguridad (como el seguimiento y la localización de un dispositivo), consulte Acciones de seguridad.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS



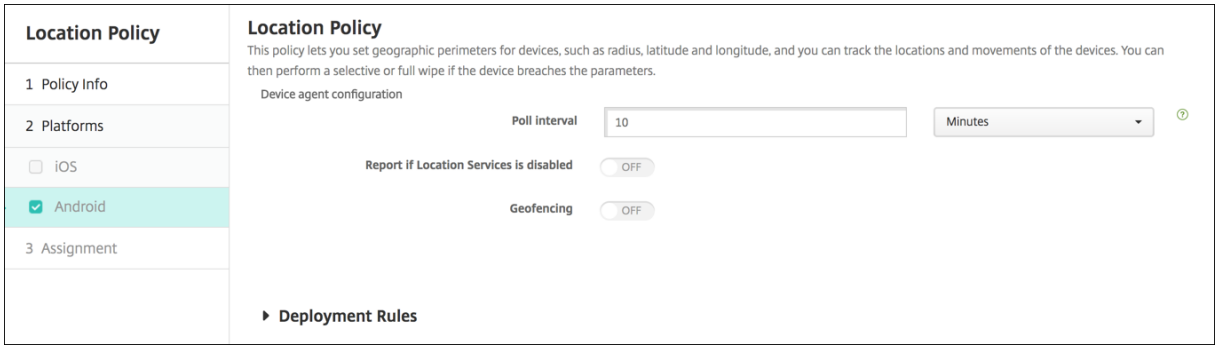
- **Tiempo de espera de la localización.** Escriba un número y, en la lista, haga clic en **Segundos** o **Minutos** para definir la frecuencia con que XenMobile intenta fijar la ubicación del dispositivo. Los valores válidos varían entre 60 y 900 segundos o entre 1 y 15 minutos. El valor predeterminado es 1 minuto.
- **Duración del seguimiento.** Escriba un número y, en la lista, haga clic en **Horas** o **Minutos** 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 6 horas.
- **Precisión.** Escriba un número y, en la lista, haga clic en **Metros**, **Pies** o **Yardas**, 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.
- **Notificar si los servicios de localización están inhabilitados.** Seleccione esta opción si el dispositivo debe enviar un informe a XenMobile cuando el GPS esté inhabilitado. Está **desactivado** de forma predeterminada.
- **Geocerca**



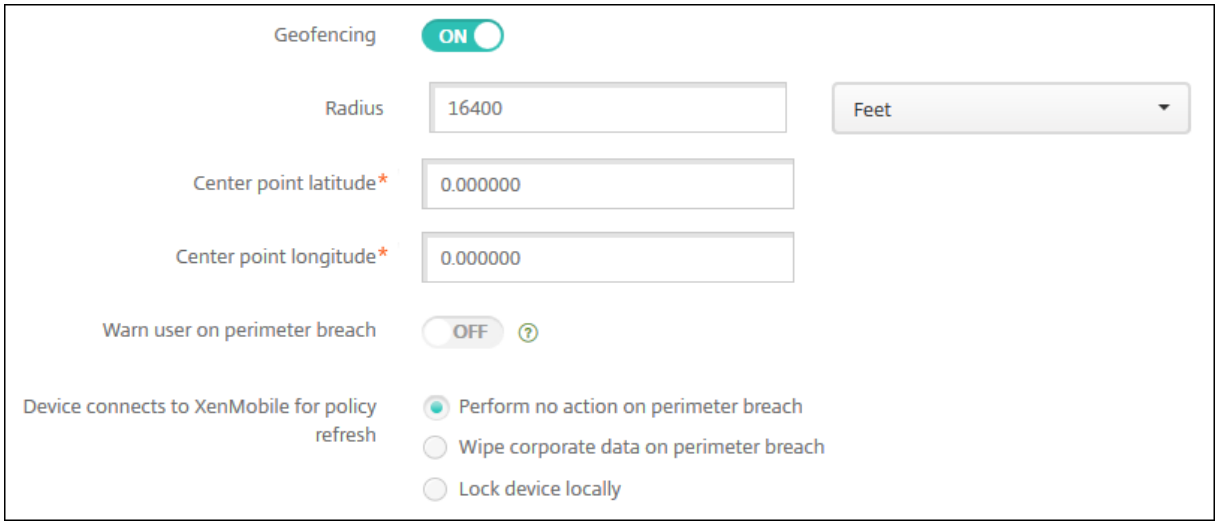
Al habilitar Geocercas, configure estos parámetros:

- **Radio.** 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
- **Latitud del punto central:** Escriba una latitud (por ejemplo, 37.787454) para definir la latitud del punto central de la geocerca.
- **Longitud del punto central:** Escriba una longitud (por ejemplo, 122.402952) para definir la longitud del punto central de la geocerca.
- **Advertir al usuario cuando salga del perímetro:** Seleccione si emitir un mensaje de advertencia cuando los usuarios abandonen el perímetro definido. Está **desactivado** de forma predeterminada. No se requiere conexión alguna a XenMobile para mostrar el mensaje de advertencia.
- **Borrar datos de empresa si sale del perímetro.** Seleccione si borrar los datos de los dispositivos de los usuarios cuando estos abandonen el perímetro. Está **desactivado** de forma predeterminada. Si habilita esta opción, aparecerá el campo **Demora del borrado local**.
  - Escriba un número y haga clic en **Segundos** o **Minutos** para establecer el tiempo de demora antes de eliminar los datos de empresa que contengan los dispositivos de los usuarios. Este parámetro 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.

Parámetros de Android



- **Intervalo de sondeo.** Escriba un número y, en la lista, haga clic en **Minutos**, **Horas** o **Días** para definir la frecuencia con que XenMobile intentará fijar la ubicación del dispositivo. Los valores válidos varían entre 1 y 1440 minutos o entre 1 y 24 horas, o bien se puede indicar cualquier cantidad de días. El valor predeterminado es 10 minutos. Si este valor es menor de 10 minutos, puede afectar de forma negativa a la duración de la batería del dispositivo.
- **Notificar si los servicios de localización están inhabilitados.** Seleccione esta opción si el dispositivo debe enviar un informe a XenMobile cuando el GPS esté inhabilitado. Está **desactivado** de forma predeterminada.
- **Geocerca**



Al habilitar Geocercas, configure estos parámetros:

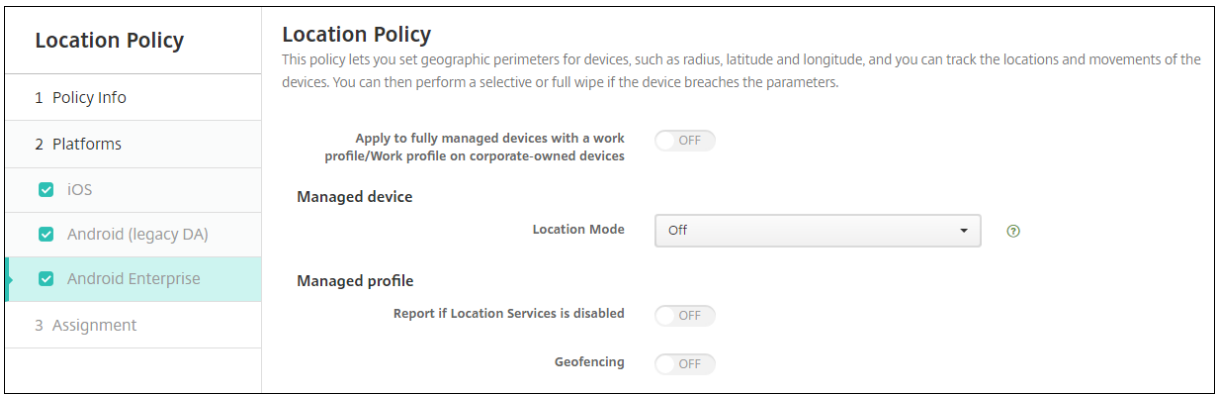
- **Radio.** Escriba un número y, en la lista, haga clic en las unidades que se van a utilizar para medir el radio. El valor predeterminado es de 16 400 pies. Los valores válidos para el radio del perímetro son:
  - De 164 a 164 000 pies
  - De 1 a 50 kilómetros
  - De 50 a 50 000 metros
  - De 54 a 54 680 yardas

  - De 1 a 31 millas
- **Latitud del punto central:** Escriba una latitud (por ejemplo, 37.787454) para definir la latitud del punto central de la geocerca.
- **Longitud del punto central:** Escriba una longitud (por ejemplo, 122.402952) para definir la longitud del punto central de la geocerca.
- **Advertir al usuario cuando salga del perímetro:** Seleccione si emitir un mensaje de advertencia cuando los usuarios abandonen el perímetro definido. Está **desactivado** de forma predeterminada. No se requiere conexión alguna a XenMobile para mostrar el mensaje de advertencia.
- **El dispositivo se conecta a XenMobile para actualizar directivas.** Seleccione una de las opciones siguientes para el momento en que los usuarios abandonen el perímetro:
  - **No realizar ninguna acción si sale del perímetro.** No hacer nada. Este es el valor predeterminado.
  - **Borrar datos de empresa si sale del perímetro.** Borrar datos empresariales del dispositivo una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparecerá el campo **Demora del borrado local**.
    * Escriba un número y haga clic en "Segundos" o "Minutos" para establecer el tiempo de demora antes de eliminar los datos de empresa que contengan los dispositivos de los usuarios. Este parámetro 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.
  - **Demora del bloqueo.** Bloquear los dispositivos de los usuarios una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparecerá el campo **Demora del bloqueo**.
    * Escriba un número y, en la lista, haga clic en "Segundos" o "Minutos" para establecer el tiempo de demora antes de bloquear los dispositivos de los usuarios. Este parámetro 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.

Parámetros de Android Enterprise

Para que el seguimiento de ubicación de Android funcione, asegúrese de que se cumplen los siguientes requisitos:

- Android 8.5 o una versión posterior
- El parámetro Permitir compartir ubicaciones está habilitado en la directiva Restricciones para Android Enterprise
- Programación de conexiones (se recomienda Firebase Cloud Messaging)



Aplicar a dispositivos totalmente administrados con un perfil de trabajo

Para dispositivos totalmente administrados con perfiles de trabajo, solo está disponible el parámetro de modo de ubicación.

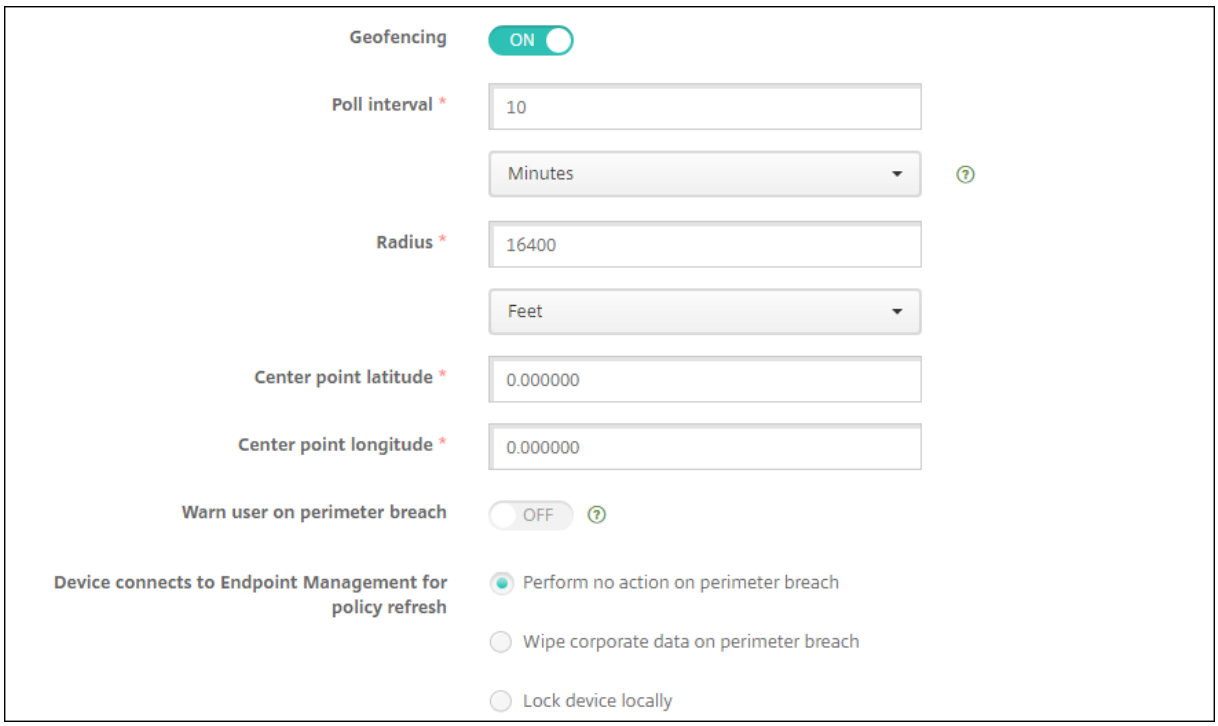
- **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa:** Le permite configurar el modo de ubicación para dispositivos totalmente administrados con perfiles de trabajo. Cuando este parámetro está activado, configure los parámetros del modo de ubicación del perfil de trabajo:
  - **Notificar si los servicios de localización están inhabilitados:** Seleccione esta opción si quiere que el dispositivo envíe un informe a XenMobile Server cuando el usuario desactive el GPS. Está **desactivado** de forma predeterminada.
  - **Geocerca:** Consulte los parámetros del apartado Dispositivo administrado en este artículo.

Cuando **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa** está desactivado, los parámetros se aplican al dispositivo administrado y al perfil de trabajo, como se muestra en las secciones siguientes. Está **desactivado** de forma predeterminada.

Dispositivo administrado

- **Modo de ubicación:** Especifique el grado de detección de la localización que se va a habilitar. Puede utilizar la acción de seguridad Localizar solamente cuando el modo de ubicación esté establecido en Alta precisión o Ahorro de batería. El valor predeterminado es Alta precisión.
  - **Alta precisión:** Permite todos los métodos de detección de la ubicación, incluidos GPS, redes y otros sensores.
  - **Solo sensores:** Habilita solo GPS y otros sensores.
  - **Ahorro de batería:** Habilita solo el proveedor de la ubicación de red.
  - **Desactivado:** Inhabilita la detección de la ubicación.

- **Geocerca:**



Al habilitar **Geocercas**, configure estos parámetros:

- **Intervalo de sondeo:** Escriba un número y, a continuación, haga clic en **Minutos**, **Horas** o **Días** para definir la frecuencia con que XenMobile Server intentará fijar la ubicación del dispositivo. Los valores válidos varían entre 1 y 1440 minutos o entre 1 y 24 horas, o bien se puede indicar cualquier cantidad de días. El valor predeterminado es **10 minutos**. Si este valor es menos de 10 minutos, puede afectar de forma negativa a la duración de la batería del dispositivo.
- **Radio:** Escriba un número y haga clic en las unidades que se van a utilizar para medir el radio. El valor predeterminado es **16400 pies** (**5000 metros**). 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
- **Latitud del punto central:** Escriba una latitud (por ejemplo, 37.787454) para definir la latitud del punto central de la geocerca. Para buscar el valor, vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Proteger** y, a continuación, haga clic en **Localizar**. Después de localizar el dispositivo, XenMobile Server indica la ubicación del dispositivo en la página **Detalles del dispositivo > General**, en la sección **Seguridad**.
- **Longitud del punto central:** Escriba una longitud (por ejemplo, 122.402952) para definir la

longitud del punto central de la geocerca.

- **Advertir al usuario cuando salga del perímetro:** Seleccione si emitir un mensaje de advertencia cuando los usuarios abandonen el perímetro definido. Está **desactivado** de forma predeterminada. No se requiere conexión alguna a XenMobile Server para mostrar el mensaje de advertencia.
- **El dispositivo se conecta a XenMobile Server para actualizar directivas:** Seleccione una de las opciones siguientes para el momento en que los usuarios abandonen el perímetro:
  - **No realizar ninguna acción si sale del perímetro.** No hacer nada. Este es el valor predeterminado.
  - **Borrar datos de empresa si sale del perímetro.** Borrar datos empresariales del dispositivo una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparecerá el campo **Demora del borrado local**.
    - Escriba un número y haga clic en **Segundos** o **Minutos** para establecer el tiempo de demora antes de eliminar los datos de empresa que contengan los dispositivos de los usuarios. Esta demora ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que XenMobile Server borre sus dispositivos de manera selectiva. El valor predeterminado es de **0** segundos.
  - **Bloquear dispositivo localmente:** Bloquear los dispositivos de los usuarios una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparecerá el campo **Demora del bloqueo**.
    - Escriba un número y haga clic en **Segundos** o **Minutos** para establecer el tiempo de demora antes de bloquear los dispositivos de los usuarios. Esta demora ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que XenMobile Server bloquee sus dispositivos. El valor predeterminado es de **0** segundos.

Perfil administrado

- **Notificar si los servicios de localización están inhabilitados:** Seleccione esta opción si quiere que el dispositivo envíe un informe a XenMobile Server cuando el usuario desactive el GPS. Está **desactivado** de forma predeterminada.
- **Geocerca:** Consulte los parámetros del apartado Dispositivo administrado en este artículo.

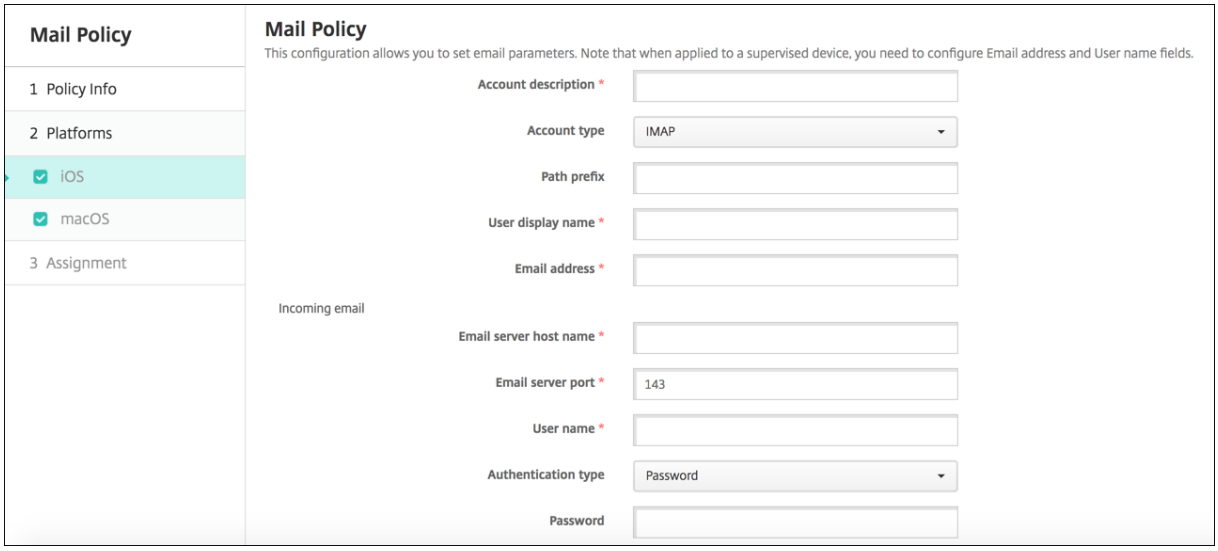
Directiva de correo

January 4, 2022

En XenMobile, puede agregar una directiva de dispositivo para configurar una cuenta de correo electrónico en dispositivos iOS o macOS.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS y macOS



- **Descripción de la cuenta.** Indique una descripción de la cuenta. Esta descripción aparece en las aplicaciones Correo y Ajustes. Este campo es obligatorio.
- **Tipo de cuenta.** Elija **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 **Prefijo de ruta**.
- **Prefijo de ruta.** Escriba **Bandeja de entrada** o introduzca el prefijo de la ruta de su cuenta de correo electrónico IMAP. Este campo es obligatorio.
- **Nombre simplificado de usuario.** Escriba el nombre de usuario completo que se va a usar para los mensajes, entre otros. Este campo es obligatorio.
- **Correo electrónico.** Escriba la dirección de correo electrónico completa de la cuenta. Este campo es obligatorio.
- **Configuración de correos electrónicos entrantes**
  - **Nombre de host del servidor de correo.** Escriba el nombre del host o la dirección IP del servidor de correo entrante. Este campo es obligatorio.
  - **Puerto del servidor de correo.** Escriba el número de puerto del servidor de correo entrante. El valor predeterminado es **143**. Este campo es obligatorio.
  - **Nombre de usuario.** Escriba el nombre de usuario de la cuenta de correo electrónico. Este nombre suele ser el mismo que la dirección de correo electrónico hasta el carácter @. Este campo es obligatorio.
  - **Tipo de autenticación.** En la lista, haga clic en el tipo de autenticación que se va a usar. El valor predeterminado es **Contraseña**. Si se selecciona **Ninguno**, desaparece el campo **Contraseña**.

  - **Contraseña.** Si quiere, escriba una contraseña para el servidor de correo entrante.
  - **Usar SSL.** Seleccione esta opción si el servidor de correo entrante utiliza la autenticación de capa de sockets seguros (SSL). Está **desactivado** de forma predeterminada.
- **Configuración de correos electrónicos salientes**
  - **Nombre de host del servidor de correo.** Escriba el nombre de host o la dirección IP del servidor de correos salientes. Este campo es obligatorio.
  - **Puerto del servidor de correo.** Escriba el número de puerto del servidor de correo saliente. Si no indica ningún número de puerto, se utiliza el puerto predeterminado para el protocolo especificado.
  - **Nombre de usuario.** Escriba el nombre de usuario de la cuenta de correo electrónico. Este nombre suele ser el mismo que la dirección de correo electrónico hasta el carácter @. Este campo es obligatorio.
  - **Tipo de autenticación.** Elija el método de autenticación que se va a utilizar. El valor predeterminado es **Contraseña**.
  - **Contraseña.** Si quiere, escriba una contraseña para el servidor de correo saliente.
  - **La contraseña de salida es la misma que la de entrada.** Seleccione si las contraseñas de correo entrante y saliente son iguales. El valor predeterminado es **No**, lo que significa que las contraseñas son diferentes.
  - **Usar SSL.** Seleccione esta opción si el servidor de correo saliente utiliza la autenticación de capa de sockets seguros (SSL). Está **desactivado** de forma predeterminada.
- **Directiva**
  - **Autorizar el movimiento de correo entre cuentas.** Seleccione si permitir a los usuarios transferir correos electrónicos de esta cuenta a otra cuenta, reenviarlos y responder a ellos desde otra cuenta. Está **desactivado** de forma predeterminada.
  - **Enviar correo electrónico solo desde aplicación de correo.** Seleccione esta opción para obligar a los usuarios a utilizar la aplicación de correo de iOS para enviar correos electrónicos.
  - **Inhabilitar sincronización de correo reciente.** Seleccione esta opción si quiere evitar que los usuarios sincronicen direcciones recientes. Está **desactivado** de forma predeterminada. Esta opción solo se aplica a iOS 6.0 y versiones posteriores.
  - **Permitir Mail Drop.** Seleccione si permitir Apple Mail Drop en dispositivos que ejecutan iOS 9.2 y versiones posteriores. Está **desactivado** de forma predeterminada.
  - **Habilitar firma S/MIME:** Seleccione si esta cuenta admite la firma S/MIME. Está **activado** de forma predeterminada. Si se **activa**, aparecen los siguientes campos.
    * **Credencial de identidad para firma.** Seleccione la credencial de firma que se va a usar.
    * **Firma S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden activar y desactivar la firma S/MIME en la configuración de sus dispositivos. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones poste-

riores.
    * **UUID de certificado de firma S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden seleccionar, en la configuración de sus dispositivos, la credencial de firma que se va a usar. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.
  – **Habilitar cifrado S/MIME:** Seleccione si esta cuenta admite el cifrado S/MIME. Está **desactivado** de forma predeterminada. Si se **activa**, aparecen los siguientes campos.
    * **Credencial de identidad para cifrado.** Seleccione la credencial de cifrado que se va a usar.
    * **Habilitar cambio de opción S/MIME para cada mensaje:** Cuando se **activa**, los usuarios ven una opción para activar o desactivar el cifrado S/MIME para cada mensaje que escriban. Está **desactivado** de forma predeterminada.
    * **Cifrado S/MIME predeterminado reemplazable por el usuario:** Si se **activa**, los usuarios pueden, en la configuración de sus dispositivos, seleccionar si S/MIME está activado de forma predeterminada. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.
    * **UUID de certificado de cifrado S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden activar y desactivar el cifrado S/MIME y la identidad del cifrado S/MIME en la configuración de sus dispositivos. Está **desactivado** de forma predeterminada. Esta opción se aplica a iOS 12.0 y versiones posteriores.
- **Configuraciones de directivas**
  – **Quitar directiva:** Para quitar la directiva más adelante, puede **seleccionar una fecha** u optar por una **demora hasta la eliminación (en horas)** .
  – **Permitir que el usuario elimine la directiva:** Permite que los usuarios eliminen la directiva de correo **Siempre**, solo con un **Código de acceso requerido** o **Nunca**.
  – **Ámbito del perfil:** Solo para macOS, elija si la directiva se aplica en el nivel de **usuario** o en todo el **sistema**.

Directiva de dominios administrados

January 4, 2022

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 cómo los usuarios abren documentos, datos adjuntos y archivos descargados del explorador web en dispositivos supervisados iOS 8 y versiones posteriores. Para dispositivos supervisados iOS 9.3 y versiones posteriores, puede

especificar las direcciones URL desde las que los usuarios pueden guardar contraseñas en Safari.

Si quiere conocer los pasos necesarios para colocar un dispositivo iOS en modo supervisado, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.

Cuando un usuario envía un correo electrónico a un destinatario cuyo dominio no consta en la lista de dominios administrados de correo electrónico, el mensaje se marca en el dispositivo del usuario para avisarle de que envía un mensaje a una persona fuera del dominio empresarial.

Para elementos como documentos, datos adjuntos o descargas: Cuando un usuario intente abrir un elemento con Safari desde un dominio que no conste en la lista de dominios web administrados, la aplicación empresarial 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 empresarial. Deberá usar una aplicación personal no administrada.

Para dispositivos supervisados, incluso si no especifica dominios de rellenado automático de contraseñas en Safari, si el dispositivo está configurado como multiusuario efímero, los usuarios no pueden guardar contraseñas. Sin embargo, si el dispositivo no está configurado como multiusuario efímero, los usuarios pueden guardar todas las contraseñas.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

Para especificar dominios:

Formato	Descripción
`example.com`	Toda ruta incluida en `example.com` se trata como administrada, pero no `site.example.com/`.
`foo.example.com`	Toda ruta incluida en `foo.example.com` se trata como administrada, pero no `example.com/` ni `bar.example.com/`.
`\*.example.com`	Toda ruta incluida en `foo.example.com` o `bar.example.com` se trata como administrada, pero no `example.com/`.
`example.com/sub`	Tanto `example.com/sub` como toda ruta que incluya se trata como administrada, pero no `example.com/`.

Formato	Descripción
`foo.example.com/sub`	Toda ruta incluida en `foo.example.com/sub` se trata como administrada, pero no `example.com`, `example.com/sub`, `foo.example.com/` ni `bar.example.com/sub`.
`\*.example.com/sub`	Toda ruta incluida en `foo.example.com/sub` o `bar.example.com/sub` se trata como administrada, pero no `example.com` ni `foo.example.com/`.

Reglas:

- Las “www” iniciales y las barras diagonales finales de las direcciones URL se omiten cuando se comparan los dominios.
- Si una entrada contiene un número de puerto, solo se consideran administradas las direcciones que especifican ese número de puerto. De lo contrario, solo se consideran administrados los puertos estándar (el puerto 80 para HTTP y el puerto 443 para HTTPS). Por ejemplo, el patrón `*.example.com:8080` coincide con `https://site.example.com:8080/page.html`, pero no `https://site.example.com/page.html`, mientras que el patrón `*.example.com` coincide con `https://site.example.com/page.html` y `https://site.example.com/page.html`, pero no `https://site.example.com:8080/page.html`.
- Las definiciones de dominios web administrados de Safari son acumulativas. Los modelos definidos por todas las cargas útiles de dominios web administrados de Safari se usan para coincidir con una solicitud de URL.

Parámetros:

- **Dominios administrados**
  - **Dominios de correo electrónico no marcados:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir en la lista cada dominio de correo electrónico:
    - **Dominio de correo electrónico administrado:** Escriba el dominio de correo electrónico.
    - Haga clic en **Guardar** para guardar el dominio del correo electrónico, o bien haga clic en **Cancelar** para no guardarlo.
  - **Dominios web Safari administrados:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir en la lista cada dominio web:
    - **Dominio web administrado:** Escriba el dominio web.
    - Haga clic en **Guardar** para guardar el dominio web, o bien haga clic en **Cancelar** para no guardarlo.

  - **Dominios de relleno automático de contraseña en Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir en la lista cada dominio de relleno automático:
    * **Dominio de relleno automático de contraseña en Safari:** Escriba el dominio de relleno automático.
    * Haga clic en **Guardar** para guardar el dominio de relleno automático, o bien haga clic en **Cancelar** para descartarlo.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva de opciones de MDM

January 4, 2022

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.

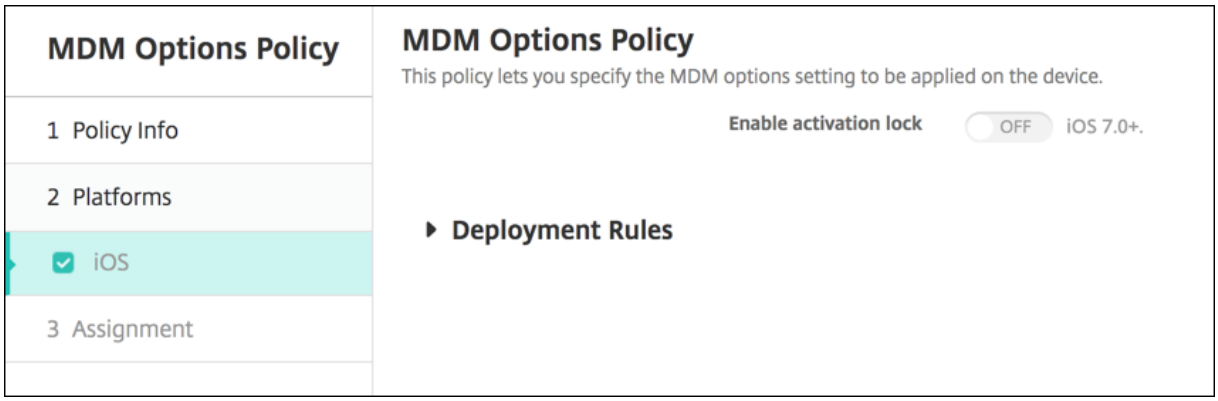
El bloqueo de activación es una función de Buscar mi iPhone o iPad que evita la reactivación de un dispositivo supervisado que se haya perdido o haya sido robado. El bloqueo de activación requiere el ID de Apple del usuario y la contraseña para poder desactivar Buscar mi iPhone o iPad, borrar el dispositivo o volver a activarlo. Para los dispositivos propiedad de la organización, es necesario omitir un bloqueo de activación para, por ejemplo, restablecer o reasignar dispositivos.

Para habilitar el bloqueo de activación, debe configurar e implementar la directiva de opciones MDM de XenMobile. A continuación, puede administrar un dispositivo desde la consola de XenMobile sin las credenciales de Apple del usuario. Para omitir el requisito de credenciales de Apple en un bloqueo de activación, debe emitir la acción de seguridad “Omisión del bloqueo de activación” desde la consola de XenMobile.

Por ejemplo, si un usuario devuelve un teléfono perdido o si usted quiere configurar uno antes o después de un borrado completo, cuando el teléfono le solicite las credenciales de la cuenta de iTunes, puede omitir ese paso emitiendo la acción de seguridad “Omisión del bloqueo de activación” desde la consola de XenMobile.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS



- **Habilitar bloqueo de activación:** Seleccione si quiere habilitar la función Bloqueo de activación en los dispositivos en los que se implementará esta directiva. Está **desactivado** de forma predeterminada.

Después de habilitar el bloqueo de activación por haber implementado la directiva de opciones de MDM, la acción de seguridad **Omisión del bloqueo de activación** aparece cuando seleccione esos dispositivos en la página **Administrar > Dispositivos** y haga clic en **Seguridad**. Una omisión del bloqueo de activación permite quitar el bloqueo de activación en dispositivos supervisados antes de la activación del dispositivo sin saber el ID de Apple ni la contraseña de los usuarios de los dispositivos. Puede enviar una omisión del bloqueo de activación a un dispositivo antes o después de un borrado completo. Para obtener información, consulte Omitir un bloqueo de activación de iOS en el artículo "Acciones de seguridad".

Directiva de información de la organización

January 3, 2020

En XenMobile, puede agregar una directiva de dispositivo 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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Nombre:** Escriba el nombre de la organización que ejecuta XenMobile.
- **Dirección:** Escriba la dirección de la organización.
- **Teléfono:** Escriba el número de teléfono de asistencia de la organización.
- **Correo:** Escriba la dirección de correo electrónico de asistencia.
- **Actividad de la organización:** Escriba una palabra o frase que describa los servicios que administra esa organización.

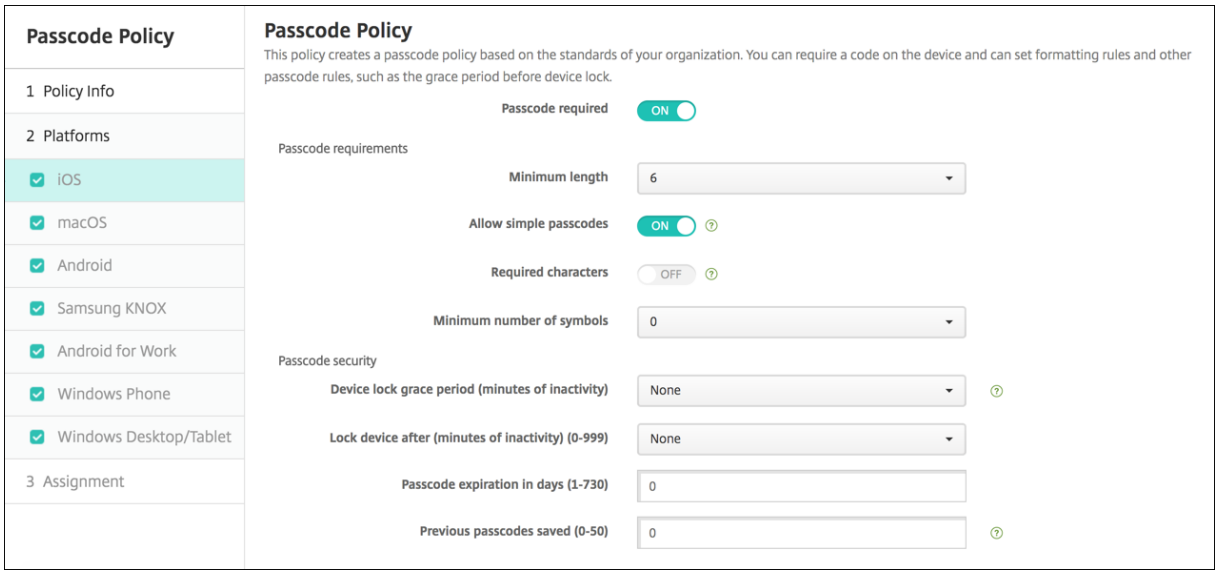
Directiva de código de acceso

January 4, 2022

En XenMobile, puede crear una directiva de código 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, macOS, Android, Samsung Knox, Android Enterprise, Windows Phone y escritorios/tabletas Windows. Cada plataforma requiere un conjunto diferente de valores, que se describen en este artículo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

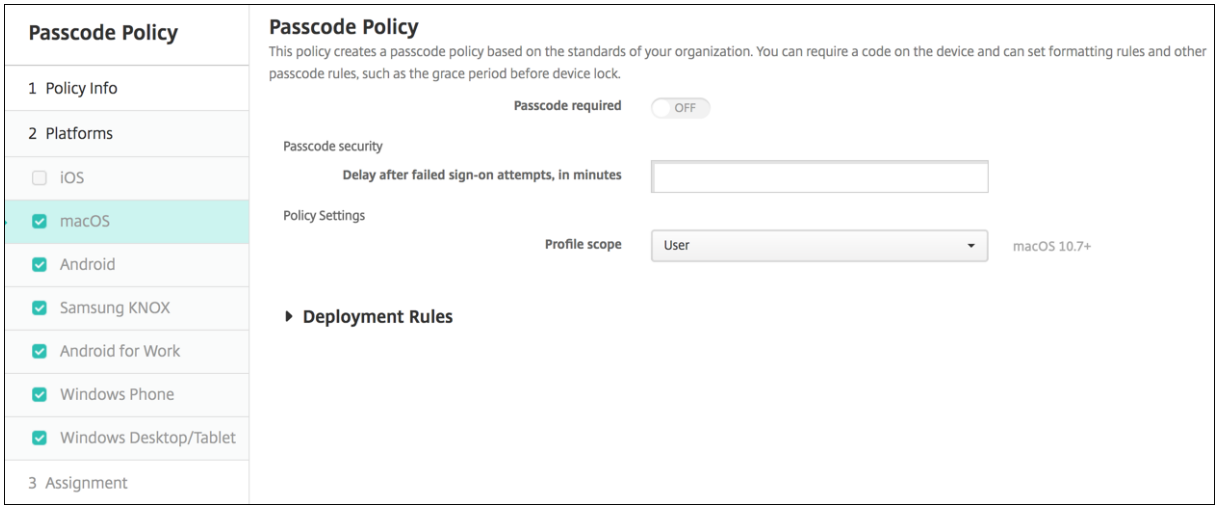


- **Requerir código de acceso.** Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de código de acceso para dispositivos

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 código de acceso**
  - **Longitud mínima:** En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
  - **Permitir códigos de acceso sencillos:** Seleccione si permitir códigos de acceso simples. Los códigos de acceso simples constan de conjuntos de caracteres secuenciales o repetidos. Está **activado** de forma predeterminada.
  - **Caracteres requeridos:** Seleccione si se debe requerir que los códigos de acceso contengan al menos una letra. Está **desactivado** de forma predeterminada.
  - **Cantidad mínima de símbolos:** En la lista, haga clic en la cantidad de símbolos que debe contener el código de acceso. El valor predeterminado es **0**.
- **Seguridad del código de acceso**
  - **Período de gracia de bloqueo del dispositivo (minutos de inactividad):** En la lista, haga clic en el período de tiempo que debe transcurrir antes de que los usuarios deban introducir un código de acceso para desbloquear un dispositivo bloqueado. El valor predeterminado es **Ninguno**.
  - **Bloquear dispositivo después de (minutos de inactividad):** En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es Ninguna.
  - **Caducidad del código de acceso en días (1-730):** Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
  - **Contraseñas anteriores guardadas (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.
  - **Cantidad máxima de intentos de inicio de sesión fallidos:** En la lista, haga clic en la cantidad de veces que un usuario puede fallar al intentar iniciar sesión antes de que se borre completamente el contenido del dispositivo. El valor predeterminado es **No definido**.

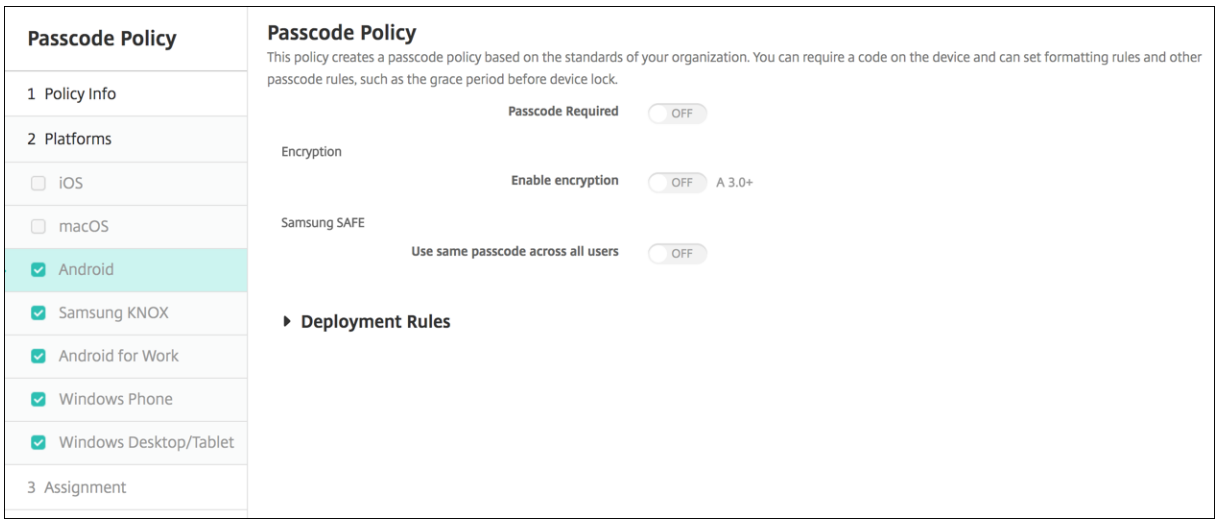
Parámetros de macOS



- **Requerir código de acceso.** Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de código 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 **Requerir código de acceso**, junto a **Demora posterior a intentos de inicio de sesión fallidos (minutos)**, escriba la cantidad de minutos de espera antes de permitir que los usuarios vuelvan a introducir sus códigos de acceso.
- Si habilita **Requerir código de acceso**, configure los siguientes parámetros:
- **Requisitos de código de acceso**
  - **Longitud mínima:** En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
  - **Permitir códigos de acceso sencillos:** Seleccione si permitir códigos de acceso simples. Los códigos de acceso simples constan de conjuntos de caracteres secuenciales o repetidos. Está **activado** de forma predeterminada.
  - **Caracteres requeridos:** Seleccione si se debe requerir que los códigos de acceso contengan al menos una letra. Está **desactivado** de forma predeterminada.
  - **Cantidad mínima de símbolos:** En la lista, haga clic en la cantidad de símbolos que debe contener el código de acceso. El valor predeterminado es **0**.
- **Seguridad del código de acceso**
  - **Período de gracia de bloqueo del dispositivo (minutos de inactividad):** En la lista, haga clic en el período de tiempo que debe transcurrir antes de que los usuarios deban introducir un código de acceso para desbloquear un dispositivo bloqueado. El valor predeterminado es **Ninguno**.
  - **Bloquear dispositivo después de (minutos de inactividad):** En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **Ninguno**.

  - **Caducidad del código de acceso en días (1-730):** Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
  - **Contraseñas anteriores guardadas (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.
  - **Cantidad máxima de intentos de inicio de sesión fallidos.** En la lista, haga clic en la cantidad de veces que un usuario puede fallar al intentar iniciar sesión antes de que se bloquee el dispositivo. El valor predeterminado es **No definido**.
  - **Demora posterior a intentos de inicio de sesión fallidos (minutos).** Escriba la cantidad de minutos de espera antes de permitir que un usuario vuelva a escribir un código de acceso.
  - **Forzar el restablecimiento del código de acceso:** La próxima vez que un usuario se autentique, este deberá restablecer su código de acceso.
- **Configuraciones de directivas**
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Parámetros de Android



> **Nota:**
>
> El valor predeterminado para Android es **No**.

- **Requerir código de acceso.** Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de código 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 código de acceso**
  - **Longitud mínima:** En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es 6.
  - **Reconocimiento biométrico:** Seleccione si habilitar el reconocimiento biométrico. Si habilita esta opción, se oculta el campo Caracteres requeridos. Está **desactivado** de forma predeterminada.
  - **Caracteres requeridos:** En la lista, haga clic en No hay restricciones, Números y letras, Solo números o Solo letras para configurar la composición de los códigos de acceso. El valor predeterminado es No hay restricciones.
  - **Reglas avanzadas.** Seleccione si aplicar reglas avanzadas de códigos de acceso. Esta opción está disponible para Android 3.0 y versiones posteriores. Está **desactivado** de forma predeterminada.
  - Si habilita **Reglas avanzadas**, 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:
    - **Símbolos:** La cantidad mínima de símbolos.
    - **Letras:** La cantidad mínima de letras.
    - **Letras minúsculas:** La cantidad mínima de minúsculas.
    - **Letras mayúsculas:** La cantidad mínima de mayúsculas.
    - **Números o símbolos:** La cantidad mínima de números o símbolos.
    - **Números:** La cantidad mínima de números.
- **Seguridad del código de acceso**
  - **Bloquear dispositivo después de (minutos de inactividad):** En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **Ninguno**.
  - **Caducidad del código de acceso en días (1-730):** Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
  - **Contraseñas anteriores guardadas (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.
  - **Cantidad máxima de intentos de inicio de sesión fallidos.** En la lista, haga clic en la cantidad de veces que un usuario puede fallar al intentar iniciar sesión antes de que se borre el contenido del dispositivo. El valor predeterminado es **No definido**.
- **Cifrado**
  - **Habilitar cifrado.** Seleccione si habilitar el cifrado. Esta opción está disponible para An-

droid 3.0 y versiones posteriores. La opción está disponible independientemente de la opción de configuración **Requerir código de acceso**.

Para cifrar los dispositivos, los usuarios deben empezar el proceso con la batería cargada y deben mantener el dispositivo enchufado durante el tiempo (poco más de una hora) 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 restablece a los valores de fábrica (proceso con el que se borrarán todos los datos hasta entonces almacenados en el dispositivo).

- **Samsung SAFE**

  > **Nota:**
  >
  > Como solución temporal para inhabilitar el reconocimiento facial o de iris en dispositivos Samsung SAFE, cree una directiva Restricciones para Samsung SAFE. En la directiva Restricciones, active **Inhabilitar aplicaciones** y agregue `com.samsung.android.bio.face.service` o `com.samsung.android.server.iris` a la tabla. A continuación, implemente la directiva Restricciones.

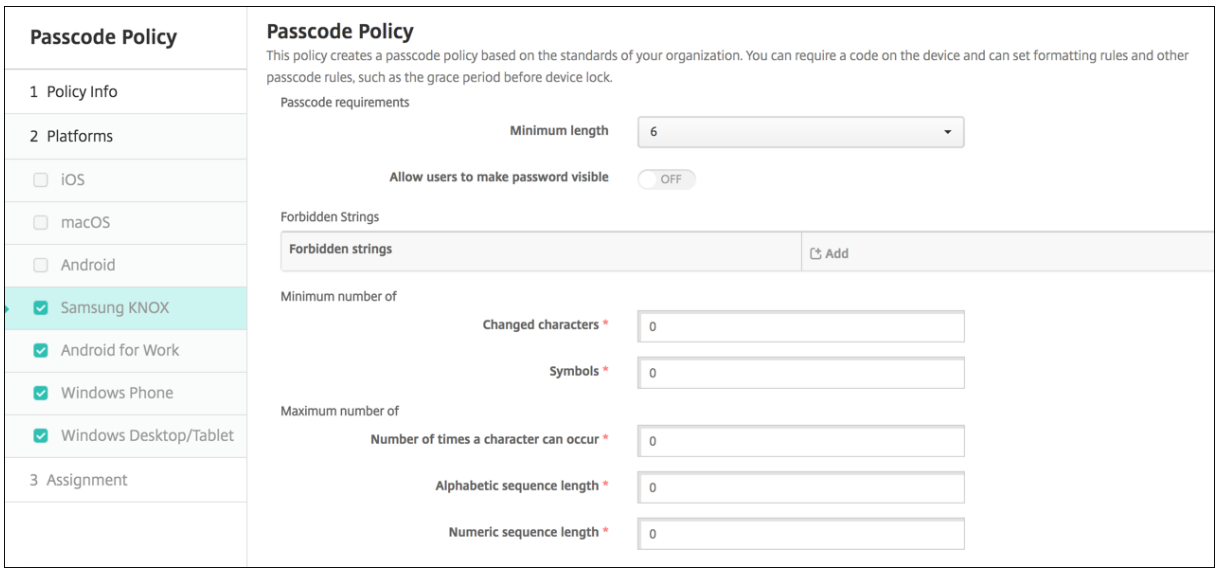
  - **Usar la misma contraseña para todos los usuarios:** Seleccione si utilizar el mismo código de acceso para todos los usuarios. Está **desactivado** de forma predeterminada. Esta opción solo se aplica a dispositivos Samsung SAFE y está disponible independientemente de la opción de configuración **Requerir código de acceso**.
  - Cuando habilite **Usar la misma contraseña para todos los usuarios**, escriba el código de acceso que utilizarán todos los usuarios en el campo **Código de acceso**.
  - Si habilita **Requerir código de acceso**, configure los siguientes parámetros de Samsung SAFE:
    - **Caracteres cambiados:** Escriba la cantidad de caracteres que los usuarios deben cambiar de su código de acceso anterior. El valor predeterminado es **0**.
    - **Cantidad de veces que puede aparecer un carácter:** Especifique la cantidad máxima de veces que se puede repetir un carácter en un código de acceso. El valor predeterminado es **0**.
    - **Longitud de la secuencia alfabética:** Escriba la longitud máxima de una secuencia alfabética en un código de acceso. El valor predeterminado es **0**.
    - **Longitud de la secuencia numérica:** Escriba la longitud máxima de una secuencia numérica en un código de acceso. El valor predeterminado es **0**.
    - **Permitir al usuario hacer visible la contraseña:** Seleccione si los usuarios pueden hacer visibles sus códigos de acceso. Está **activado** de forma predeterminada.
    - **Configurar la autenticación biométrica**. Seleccione si habilitar la autenticación biométrica. Está **desactivado** de forma predeterminada. Si la **activa**, puede configurar estas opciones:
      - **Permitir huella dactilar**. Seleccione la opción para permitir que los usuarios se

autentiquen por huella dactilar.

- **Permitir iris**. Seleccione la opción para permitir que los usuarios se autentiquen por el iris.

* **Cadenas prohibidas:** Cree cadenas prohibidas para evitar que los usuarios utilicen cadenas no seguras (fáciles de adivinar), como “contraseña”, “contra”, “bienvenida”, “123456” o “111111”, entre otras. Haga clic en **Agregar** y lleve a cabo lo siguiente para cada cadena que quiera denegar:
  - **Cadenas prohibidas:** Escriba la cadena que los usuarios no pueden usar.
  - Haga clic en **Guardar** para agregar la cadena, o bien haga clic en **Cancelar** para descartarla.

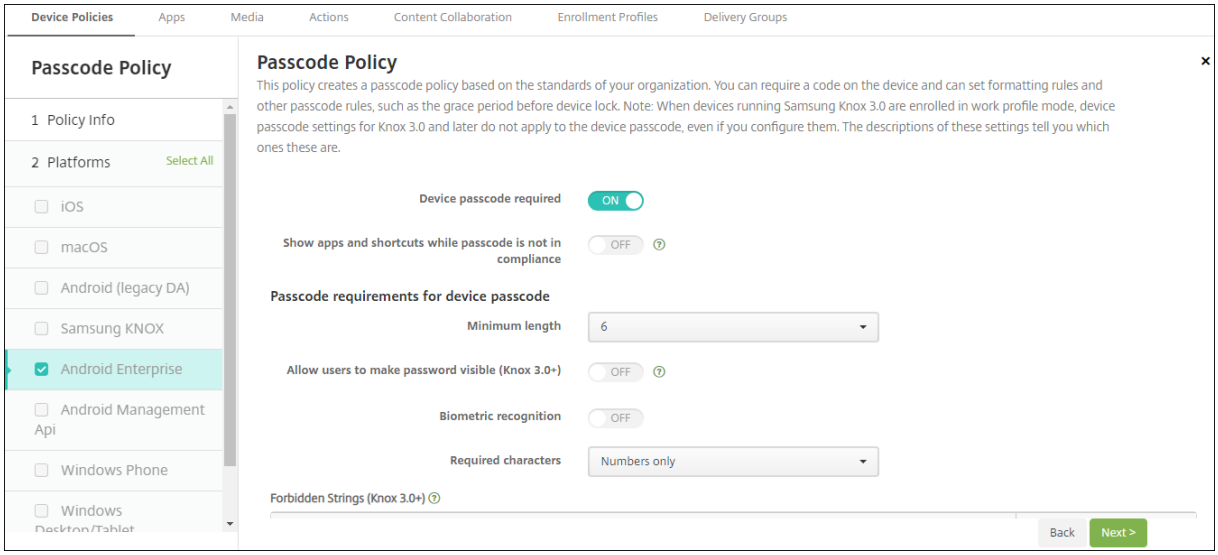
Parámetros de Samsung Knox



- **Requisitos de código de acceso**
  - **Longitud mínima:** En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
  - **Permitir al usuario hacer visible la contraseña:** Seleccione si los usuarios pueden hacer visibles sus contraseñas.
  - **Cadenas prohibidas:** Cree cadenas prohibidas para evitar que los usuarios utilicen cadenas no seguras (fáciles de adivinar), como “contraseña”, “contra”, “bienvenida”, “123456” o “111111”, entre otras. Haga clic en Agregar y lleve a cabo lo siguiente para cada cadena que quiera denegar:
    * **Cadenas prohibidas:** Escriba la cadena que los usuarios no pueden usar.
    * Haga clic en **Guardar** para agregar la cadena, o bien haga clic en **Cancelar** para descartarla.
- **Cantidad mínima de**

  - **Caracteres cambiados:** Escriba la cantidad de caracteres que los usuarios deben cambiar de su código de acceso anterior. El valor predeterminado es **0**.
  - **Símbolos:** Escriba la cantidad mínima de símbolos necesarios en un código de acceso. El valor predeterminado es **0**.
- **Cantidad máxima de**
  - **Cantidad de veces que puede aparecer un carácter:** Especifique la cantidad máxima de veces que se puede repetir un carácter en un código de acceso. El valor predeterminado es **0**.
  - **Longitud de la secuencia alfabética:** Escriba la longitud máxima de una secuencia alfabética en un código de acceso. El valor predeterminado es **0**.
  - **Longitud de la secuencia numérica:** Escriba la longitud máxima de una secuencia numérica en un código de acceso. El valor predeterminado es **0**.
- **Seguridad del código de acceso**
  - **Bloquear dispositivo después de (minutos de inactividad):** En la lista, haga clic en la cantidad de segundos que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **Ninguno**.
  - **Caducidad del código de acceso en días (1-730):** Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
  - **Contraseñas anteriores guardadas (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.
  - **Si se supera la cantidad de intentos de inicio de sesión fallidos, el dispositivo se bloquea:** En la lista, haga clic en la cantidad de veces que un usuario puede fallar al intentar iniciar sesión antes de que se bloquee el dispositivo. El valor predeterminado es **No definido**.
  - **Si se supera la cantidad de intentos de inicio de sesión fallidos, el dispositivo se borra:** 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 **No definido**.

Parámetros de Android Enterprise



Para dispositivos Android Enterprise, se puede requerir: un código de acceso para el dispositivo, una comprobación de seguridad para el perfil de trabajo de Android Enterprise o ambos.

Para dispositivos con Android 8.0 o una versión posterior y Samsung Knox 3.0 o una versión posterior, establezca los parámetros para Samsung Knox en la página **Android Enterprise**. Para dispositivos con versiones anteriores de Android o Samsung Knox, utilice la página **Samsung Knox**.

> **Nota:**
>
> Cuando los dispositivos con Samsung Knox 3.0 se inscriben como dispositivos de perfil de trabajo, los parámetros de código de acceso al dispositivo para Knox 3.0 y versiones posteriores no se aplican al código de acceso al dispositivo, incluso aunque los configure.

- **Código de acceso de dispositivo obligatorio:** Requiere un código de acceso en el dispositivo. Cuando esta opción esté **activada**, establezca las configuraciones de **Requisitos del código de acceso del dispositivo** y **Seguridad del código de acceso del dispositivo**. Está **desactivado** de forma predeterminada.
- **Mostrar aplicaciones y accesos directos mientras el código de acceso no cumpla los requisitos:** Cuando este parámetro está **activado**, las aplicaciones y los accesos directos del dispositivo no se ocultan, incluso cuando el código de acceso no cumple los requisitos. Cuando este parámetro está **desactivado**, las aplicaciones y los accesos directos se ocultan cuando el código de acceso no cumple los requisitos. Si se habilita este parámetro, Citrix recomienda crear una acción automatizada para marcar el dispositivo como no conforme cuando el código de acceso no cumpla los requisitos. Está **desactivado** de forma predeterminada.
- **Requisitos del código de acceso del dispositivo:**
  - **Longitud mínima:** Especifica la longitud mínima del código de acceso. El valor predeterminado es 6.

- **Permitir al usuario hacer visible la contraseña:** Para dispositivos con Samsung Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida. Solo para dispositivos totalmente administrados. Esta configuración no se aplica a los dispositivos inscritos como dispositivos de perfil de trabajo. Permite a los usuarios hacer visible la contraseña. Está **desactivado** de forma predeterminada.
- **Reconocimiento biométrico:** Permite el reconocimiento biométrico. Si esta opción está **activada**, se oculta el campo **Caracteres requeridos**. Está **desactivado** de forma predeterminada.
- **Caracteres requeridos:** Especifica los tipos de caracteres necesarios para los códigos de acceso. En la lista, elija **No hay restricciones**, **Números y letras**, **Solo números** o **Solo letras**. Use **No hay restricciones** solo para dispositivos con Android 7.0. Android 7.1 y las versiones posteriores no respetan la configuración **No hay restricciones**. El valor predeterminado es **Números y letras**.
- **Cadenas prohibidas:** Para dispositivos con Samsung Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida. Solo para dispositivos totalmente administrados. Esta configuración no se aplica a los dispositivos inscritos como dispositivos de perfil de trabajo. Especifica las cadenas que los usuarios no pueden usar como códigos de acceso. Puede crear cadenas prohibidas para impedir que los usuarios utilicen cadenas no seguras (fáciles de adivinar), como “contraseña”, “contra”, “bienvenida”, “123456” o “111111”, entre otras. Para cada cadena cuyo uso quiera impedir, haga clic en **Agregar**, escriba la cadena en sí, y haga clic en **Guardar** para agregar la cadena o haga clic en **Cancelar** para cancelar la operación.
- **Reglas avanzadas:** Aplica reglas avanzadas para los tipos de caracteres que pueden aparecer en los códigos de acceso. Cuando esta opción esté **activada**, establezca las configuraciones de **Cantidad mínima de** y **Cantidad máxima de**. Esta configuración no está disponible para dispositivos Android con versiones anteriores a Android 5.0. Está **desactivado** de forma predeterminada.
- **Cantidad mínima de:**
  * **Símbolos:** Especifica la cantidad mínima de símbolos. El valor predeterminado es **0**.
  * **Letras:** Especifica la cantidad mínima de letras. El valor predeterminado es **0**.
  * **Letras minúsculas:** Especifica la cantidad mínima de minúsculas. El valor predeterminado es **0**.
  * **Letras mayúsculas:** Especifica la cantidad mínima de mayúsculas. El valor predeterminado es **0**.
  * **Números o símbolos:** Especifica la cantidad mínima de números o símbolos. El valor predeterminado es **0**.
  * **Números:** Especifica la cantidad mínima de números. El valor predeterminado es **0**.
  * **Caracteres cambiados:** Para dispositivos con Samsung Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida. Solo para dispositivos

totalmente administrados. Esta configuración no se aplica a los dispositivos inscritos como dispositivos de perfil de trabajo. Especifica la cantidad de caracteres que los usuarios deben cambiar de su código de acceso anterior. El valor predeterminado es **0**.

- **Cantidad máxima de:** Para dispositivos con Samsung Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida. Solo para dispositivos totalmente administrados. Esta configuración no se aplica a los dispositivos inscritos como dispositivos de perfil de trabajo.
  - **Cantidad de veces que puede aparecer un carácter:** Especifica la cantidad máxima de veces que se puede repetir un carácter en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.
  - **Longitud de la secuencia alfabética:** Especifica la longitud máxima de una secuencia alfabética en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.
  - **Longitud de la secuencia numérica:** Especifica la longitud máxima de una secuencia numérica en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.

- **Seguridad del código de acceso del dispositivo:**
  - **Borrar dispositivo después (de los intentos fallidos de inicio de sesión):** Especifica la cantidad máxima de veces que un usuario puede fallar al intentar iniciar sesión antes de que el dispositivo se borre por completo. El valor predeterminado es **No definido**.
  - **Bloquear dispositivo después de (minutos de inactividad, entre 0 y 999):** Especifica los minutos que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **Ninguno**.
  - **Caducidad del código de acceso en días (1-730):** Especifica 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.
  - **Contraseñas anteriores guardadas (0-50):** Especifica la cantidad de contraseñas utilizadas que se guardan. 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.
  - **Bloquear dispositivo después (de los intentos fallidos de inicio de sesión):** Para dispositivos con Samsung Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida. Solo para dispositivos totalmente administrados. Esta configuración no se aplica a los dispositivos inscritos como dispositivos de perfil de trabajo. Especifica la cantidad máxima de veces que un usuario puede fallar al intentar iniciar sesión antes de que el dispositivo se bloquee. El valor predeterminado es **No definido**.
- **Desafío de seguridad de perfil de trabajo obligatorio:** Habilite esta opción para obligar a los usuarios a completar una comprobación de seguridad si quieren acceder a las aplicaciones que

se ejecutan en un perfil de trabajo de Android Enterprise. Para dispositivos con Android 7.0 y versiones posteriores. Cuando esta opción esté **activada**, establezca las configuraciones de **Requisitos del código de acceso para el desafío de seguridad del perfil de trabajo** y **Seguridad del código de acceso para el desafío de seguridad del perfil de trabajo**. Está **desactivado** de forma predeterminada.

- **Requisitos del código de acceso para el desafío de seguridad del perfil de trabajo:**
  - **Longitud mínima:** Especifica la longitud mínima del código de acceso. El valor predeterminado es 6.
  - **Permitir al usuario hacer visible la contraseña:** Para dispositivos con Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida. Permite a los usuarios hacer visible la contraseña. Está **desactivado** de forma predeterminada.
  - **Reconocimiento biométrico:** Permite el reconocimiento biométrico. Si esta opción está **activada**, se oculta el campo **Caracteres requeridos**. Está **desactivado** de forma predeterminada.
  - **Caracteres requeridos:** Especifica los tipos de caracteres necesarios para los códigos de acceso. En la lista, elija **No hay restricciones**, **Números y letras**, **Solo números** o **Solo letras**. Use **No hay restricciones** solo para dispositivos con Android 7.0. Android 7.1 y las versiones posteriores no respetan la configuración **No hay restricciones**. El valor predeterminado es **Números y letras**.
  - **Cadenas prohibidas:** Para dispositivos con Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida. Especifica las cadenas que los usuarios no pueden usar como códigos de acceso. Puede crear cadenas prohibidas para impedir que los usuarios utilicen cadenas no seguras (fáciles de adivinar), como “contraseña”, “contra”, “bienvenida”, “123456” o “111111”, entre otras. Para cada cadena cuyo uso quiera impedir, haga clic en **Agregar**, escriba la cadena en sí, y haga clic en **Guardar** para agregar la cadena o haga clic en **Cancelar** para cancelar la operación.
  - **Reglas avanzadas:** Aplica reglas avanzadas para los tipos de caracteres que pueden aparecer en los códigos de acceso. Cuando esta opción esté **activada**, establezca las configuraciones de **Cantidad mínima de** y **Cantidad máxima de**. Esta configuración no está disponible para dispositivos Android con versiones anteriores a Android 5.0. Está **desactivado** de forma predeterminada.
  - **Cantidad mínima de:**
    - **Símbolos:** Especifica la cantidad mínima de símbolos. El valor predeterminado es **0**.
    - **Letras:** Especifica la cantidad mínima de letras. El valor predeterminado es **0**.
    - **Letras minúsculas:** Especifica la cantidad mínima de minúsculas. El valor predeterminado es **0**.
    - **Letras mayúsculas:** Especifica la cantidad mínima de mayúsculas. El valor predeterminado es **0**.
    - **Números o símbolos:** Especifica la cantidad mínima de números o símbolos. El valor

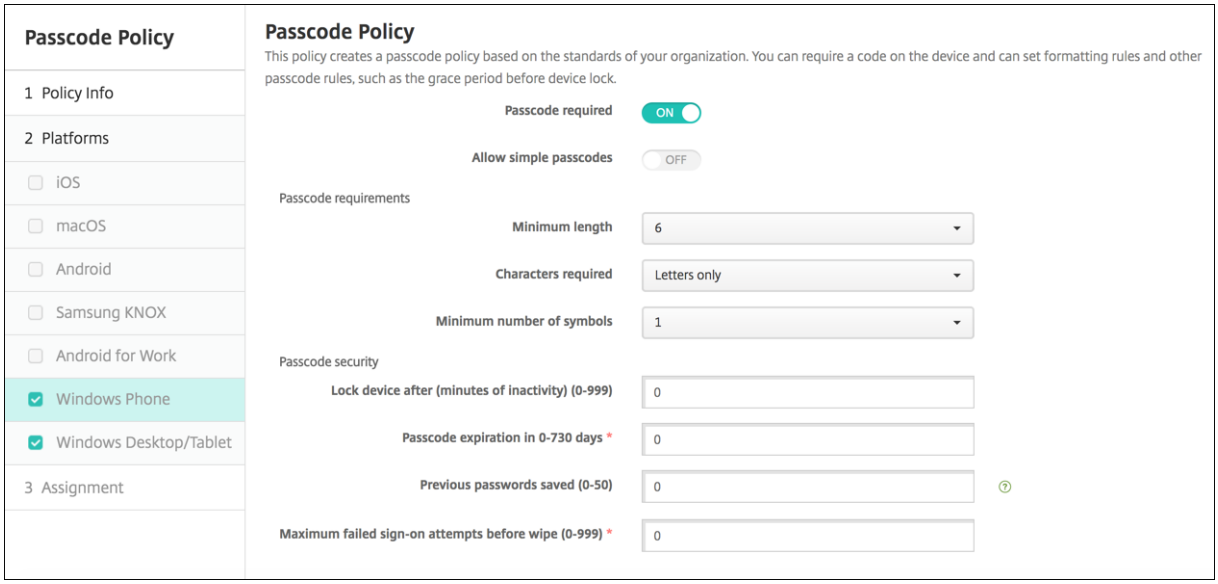
predeterminado es **0**.
    * **Números:** Especifica la cantidad mínima de números. El valor predeterminado es **0**.
    * **Caracteres cambiados:** Para dispositivos con Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida. Especifica la cantidad de caracteres que los usuarios deben cambiar de su código de acceso anterior. El valor predeterminado es **0**.
  - **Cantidad máxima de:** Para dispositivos con Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida.
    * **Cantidad de veces que puede aparecer un carácter:** Especifica la cantidad máxima de veces que se puede repetir un carácter en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.
    * **Longitud de la secuencia alfabética:** Especifica la longitud máxima de una secuencia alfabética en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.
    * **Longitud de la secuencia numérica:** Especifica la longitud máxima de una secuencia numérica en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.
  - **Enable unified passcode:** Si está **activado**, los usuarios utilizan un código de acceso para su dispositivo y perfil de trabajo. Si está **desactivado**:
    * Los usuarios deben utilizar códigos de acceso diferentes para su dispositivo y perfil de trabajo.
    * La opción **Use one lock** en el dispositivo, que los usuarios establecen si desean usar un código de acceso para su dispositivo y perfil de trabajo, está inhabilitada. El usuario no puede habilitarla.
    * Si el requisito de código de acceso para el desafío de seguridad del perfil de trabajo es más complejo que el código de acceso del dispositivo: A los usuarios con la opción **Use one lock** habilitada, se les pedirá que cambien sus códigos de acceso del perfil de trabajo.

    Está **desactivado** de forma predeterminada. Disponible a partir de Android 9.0.
- **Seguridad del código de acceso para el desafío de seguridad del perfil de trabajo**
  - **Borrar contenedor después (de los intentos fallidos de inicio de sesión):** Especifica la cantidad máxima de veces que un usuario puede fallar al intentar iniciar sesión antes de que el perfil de trabajo y sus datos se borren del dispositivo. Los usuarios deben reinicializar el perfil de trabajo después de que se produzca el borrado. El valor predeterminado es **No definido**.
  - **Bloquear contenedor después (minutos de inactividad):** Especifica los minutos que un dispositivo puede estar inactivo antes de bloquear el perfil de trabajo. El valor predeterminado es **Ninguno**.
  - **Caducidad del código de acceso en días (1-730):** Especifica 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.

- **Contraseñas anteriores guardadas (0-50):** Especifica la cantidad de contraseñas utilizadas que se guardan. 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.
- **Bloquear contenedor después (de los intentos fallidos de inicio de sesión):** Para dispositivos con Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia de Knox válida. Especifica la cantidad máxima de veces que un usuario puede fallar al intentar iniciar sesión antes de que el dispositivo se bloquee. El valor predeterminado es **No definido**.

Parámetros de Windows Phone



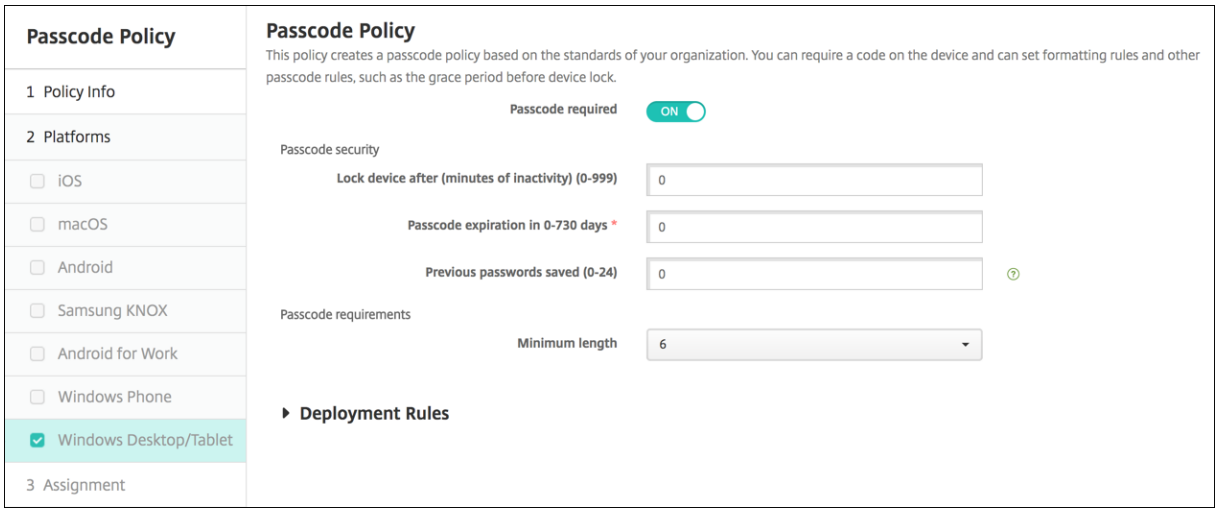
- **Requerir código de acceso:** Seleccione esta opción para requerir un código de acceso en los dispositivos Windows Phone. Está **activado** de forma predeterminada, lo que requiere un código de acceso. La página se contrae y las siguientes opciones desaparecen cuando se inhabilita esta opción de configuración.
- **Permitir códigos de acceso sencillos:** Seleccione si permitir códigos de acceso simples. Los códigos de acceso simples constan de conjuntos de caracteres secuenciales o repetidos. Está desactivado de forma predeterminada.
- **Requisitos de código de acceso**
  - **Longitud mínima:** En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
  - **Caracteres requeridos:** En la lista, haga clic en **Numéricos o alfanuméricos**, **Solo letras** o **Solo números** para definir la composición de los códigos de acceso. El valor predeter-

minado es **Solo letras**.

- **Cantidad mínima de símbolos:** En la lista, haga clic en la cantidad de símbolos que debe contener el código de acceso. El valor predeterminado es **1**.

- **Seguridad del código de acceso**
  - **Bloquear dispositivo después de (minutos de inactividad):** En la lista, haga clic en los minutos que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **0**.
  - **Caducidad del código de acceso en 0-730 días:** 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.
  - **Contraseñas anteriores guardadas (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.
  - **Cantidad máxima de intentos de inicio de sesión fallidos antes del borrado (0-999):** Introduzca cuántas veces puede un usuario fallar el inicio de sesión antes de que los datos de empresa se borren del dispositivo. El valor predeterminado es **0**.

Parámetros de escritorios y tabletas Windows



- **Prohibir inicio de sesión cómodo:** Seleccione si permitir que los usuarios accedan a sus dispositivos con contraseñas de imagen o inicios de sesión biométricos. Está **desactivado** de forma predeterminada.
- **Longitud mínima del código de acceso:** En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
- **Cantidad máxima de intentos con el código de acceso antes del borrado:** En la lista, haga clic en la cantidad de veces que un usuario puede fallar al intentar iniciar sesión hasta que los datos de empresa se borren del dispositivo. El valor predeterminado es **4**.

- **Caducidad del código de acceso (0-730 días):** 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.
- **Historial de códigos de acceso (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**.
- **Tiempo máximo de inactividad antes del bloqueo del dispositivo en minutos (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**.

Directiva de hotspot personal

January 3, 2020

Puede permitir que los usuarios se conecten a Internet aunque estén fuera del alcance de una red Wi-Fi, mediante la conexión de datos móviles a través de la función Compartir Internet de sus dispositivos iOS. Disponible en iOS 7.0 y versiones posteriores.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Inhabilitar hotspot personal:** Seleccione si quiere inhabilitar la función de hotspot personal (Compartir Internet) en los dispositivos de los usuarios. El valor predeterminado es **No**, lo que desactiva la función de hotspot personal de los dispositivos de los usuarios. Esta directiva no inhabilita la función. Los usuarios pueden seguir mediante la función de hotspot personal (Compartir Internet) en sus dispositivos. Sin embargo, cuando se implementa la directiva, dicha función se desactiva (no está activa de forma predeterminada).

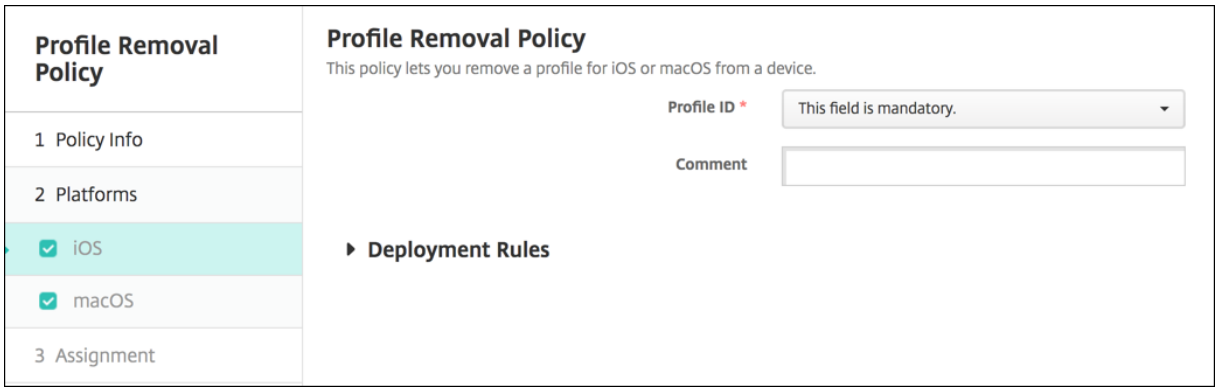
Directiva de eliminación de perfiles

January 3, 2020

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 macOS de los usuarios.

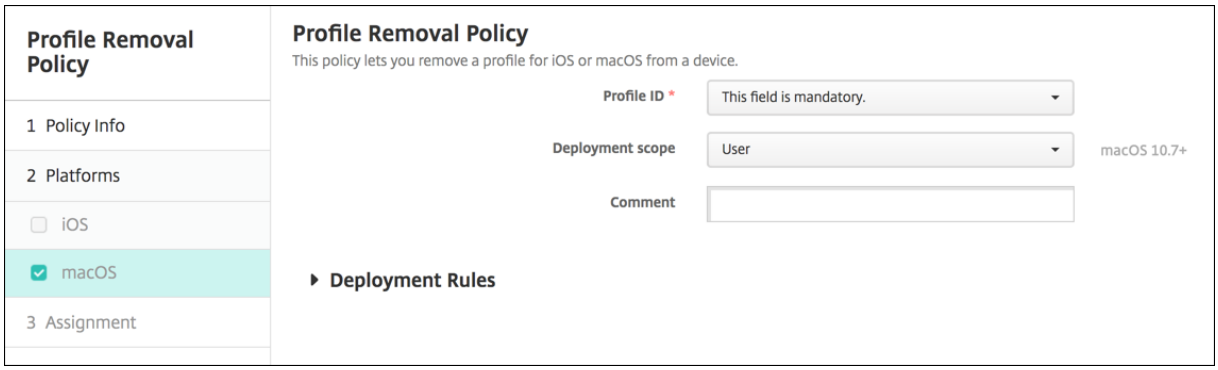
Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS



- **ID de perfil:** En la lista, haga clic en el ID del perfil de aplicación. Este campo es obligatorio.
- **Comentario:** Puede escribir un comentario opcional.

Parámetros de macOS



- **ID de perfil:** En la lista, haga clic en el ID del perfil de aplicación. Este campo es obligatorio.
- **Ámbito de implementación:** En la lista, haga clic en **Usuario** o **Sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.
- **Comentario:** Puede escribir un comentario opcional.

Directiva de perfil de datos

January 4, 2022

Por regla general, cuando se desarrolla y se firma con código una aplicación empresarial iOS, se incluye un perfil de datos de distribución empresarial, que requiere Apple para que la aplicación fun-

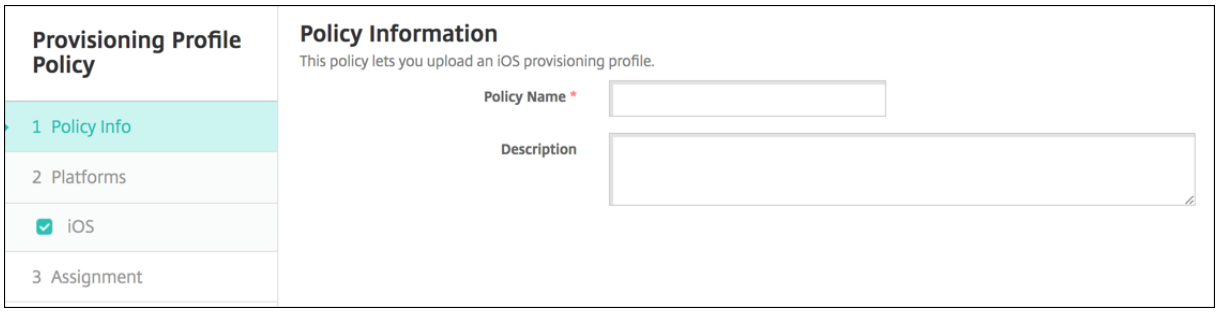
cione en dispositivos iOS. Si falta o ha caducado un perfil de datos, la aplicación se bloquea cuando un usuario toca en ella para abrirla.

El problema principal con los perfiles de datos 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 datos 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 datos a los usuarios o ponerlos en un portal web para que se puedan descargar e instalar desde allí. Estas soluciones funcionan, pero no son infalibles, puesto que los usuarios deben actuar siguiendo las instrucciones de un correo o visitar el portal Web para descargar e instalar el perfil en cuestión.

Si quiere que este proceso sea transparente para los usuarios, en XenMobile puede instalar y quitar perfiles de aprovisionamiento con directivas de dispositivo. Se quitan los perfiles que falten o hayan caducado y se instalan perfiles actualizados en los dispositivos de los usuarios, por lo que tocar una aplicación solo la abre para su uso.

Antes de crear una directiva de perfiles de datos, cree un archivo de perfil de datos. Para obtener más información, consulte el artículo de Apple sobre cómo crear un perfil de aprovisionamiento de desarrollo en el sitio para desarrolladores de Apple.

Parámetros de iOS



- **Perfil de datos de iOS:** Seleccione el archivo del perfil de datos que quiere importar. Para ello, haga clic en **Examinar** y vaya a la ubicación de ese archivo.

Directiva de eliminación de perfiles de datos

January 4, 2022

Puede eliminar perfiles de aprovisionamiento iOS con la ayuda de directivas de dispositivo. Para obtener más información acerca de los perfiles de aprovisionamiento, consulte Directiva de perfil de aprovisionamiento.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Perfil de datos de iOS:** En la lista, haga clic en el perfil de datos que quiere quitar.
- **Comentario:** Si lo prefiere, agregue un Comentario:

Directiva de proxy

January 4, 2022

En XenMobile, puede agregar una directiva de dispositivo 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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

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 o Implementar dispositivos mediante el Programa de implementación de Apple.

Establezca reglas de implementación para inscribir dispositivos antes de enviar la directiva de proxy a los dispositivos.

Parámetros de iOS

- **Configuración de proxy:** Haga clic en **Manual** o **Automática** para determinar cómo se configurará el proxy en los dispositivos de los usuarios.
  - Si hace clic en **Manual**, configure los siguientes parámetros:
    - **Nombre de host o dirección IP del servidor proxy:** Escriba el nombre de host o la dirección IP del servidor proxy. Este campo es obligatorio.
    - **Puerto del servidor proxy.** Escriba el número de puerto del servidor proxy. Este campo es obligatorio.
    - **Nombre de usuario:** Si quiere, escriba un nombre de usuario para la autenticación en el servidor proxy.

        * **Contraseña:** Si quiere, escriba una contraseña para la autenticación en el servidor proxy.
    - Si hace clic en **Automática**, configure los siguientes parámetros:
        * **URL del archivo PAC del proxy:** Escriba la dirección URL del archivo PAC que define la configuración de proxy.
        * **Permitir conexión directa si no se puede acceder al archivo PAC:** Seleccione si quiere permitir que los usuarios se conecten directamente al destino si no se puede acceder al archivo PAC. Está **activado** de forma predeterminada. Esta opción solo está disponible para iOS 7.0 y versiones posteriores.

- **Permitir omisión del proxy para acceder a redes cautivas:** Seleccione si permitir que el dispositivo omita el servidor proxy y pueda acceder a redes cautivas. Está **desactivado** de forma predeterminada.
- **Configuraciones de directivas**
    - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
        * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
        * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de Windows Mobile/CE

- **Red:** En la lista, haga clic en el tipo de red a utilizar. El valor predeterminado es **Oficina integrada**. Las opciones posibles son:
    - Oficina definida por el usuario
    - Internet definido por el usuario
    - Oficina integrada
    - Internet integrado
- **Red:** 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
- **Nombre de host o dirección IP del servidor proxy:** Escriba el nombre de host o la dirección IP del servidor proxy. Este campo es obligatorio.
- **Puerto del servidor proxy.** Escriba el número de puerto del servidor proxy. Este campo es obligatorio. El valor predeterminado es **80**.

- **Nombre de usuario:** Si quiere, escriba un nombre de usuario para la autenticación en el servidor proxy.
- **Contraseña:** Si quiere, escriba una contraseña para la autenticación en el servidor proxy.
- **Nombre de dominio:** Si quiere, escriba un nombre de dominio.
- **Habilitar:** Seleccione si habilitar el proxy. Está **activado** de forma predeterminada.

Directiva de Registro

January 3, 2020

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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Windows Mobile/CE

Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada clave de Registro o par clave/valor de Registro:

- **Ruta de clave de Registro:** 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.
- **Nombre de valor de Registro:** 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 un par clave/valor de Registro.
- **Tipo:** 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.
  - **Cadena:** Cualquier cadena.
  - **Cadena extendida:** Un valor de cadena que puede contener variables de entorno como, por ejemplo, %TEMP% o %USERPROFILE%.
  - **Binario:** Cualquier dato binario arbitrario.
- **Valor:** 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 **Guardar** para guardar la información de la clave de Registro, o bien haga clic en **Cancelar** para no guardarla.

Directiva de asistencia remota

January 4, 2022

> **Nota:**
>
> Para las implementaciones locales de XenMobile Server, la asistencia remota (Remote Support) permite que el personal de Help Desk tome el control remoto de los dispositivos móviles Windows CE y Android administrados. La transmisión de la pantalla solo se admite en dispositivos Samsung Knox.
>
> Remote Support no está disponible para implementaciones locales en clúster de XenMobile Server.
>
> Para obtener más información, consulte Opciones de asistencia y Remote Support.

En XenMobile, puede crear una directiva de asistencia remota (Remote Support) para poder acceder de forma remota a los dispositivos Windows y Android admitidos. Puede configurar dos tipos de asistencia:

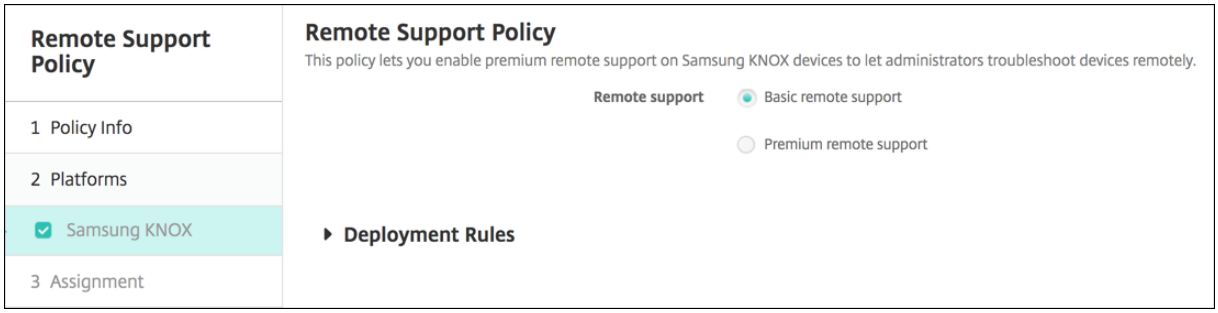
- **Básica**: Esta opción permite ver la información de diagnóstico referente al dispositivo, como la información del sistema, los procesos que se están ejecutando, el administrador de tareas (el uso de memoria y de CPU) o el contenido de las carpetas del software instalado, entre otros.
- **Premium**: Permite controlar de forma remota la pantalla del dispositivo:
  - controlar los colores (en la ventana principal o en la ventana aparte, flotante).
  - establecer una sesión de voz sobre IP (VoIP) entre el servicio de Help Desk y el usuario.
  - configurar parámetros.
  - establecer una sesión de chat entre servicio de Help Desk y el usuario.

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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Android y Windows CE



- **Asistencia remota.** Seleccione **Asistencia remota básica** o **Asistencia remota premium**. El valor predeterminado es **Asistencia remota básica**.

Directiva de restricciones

January 4, 2022

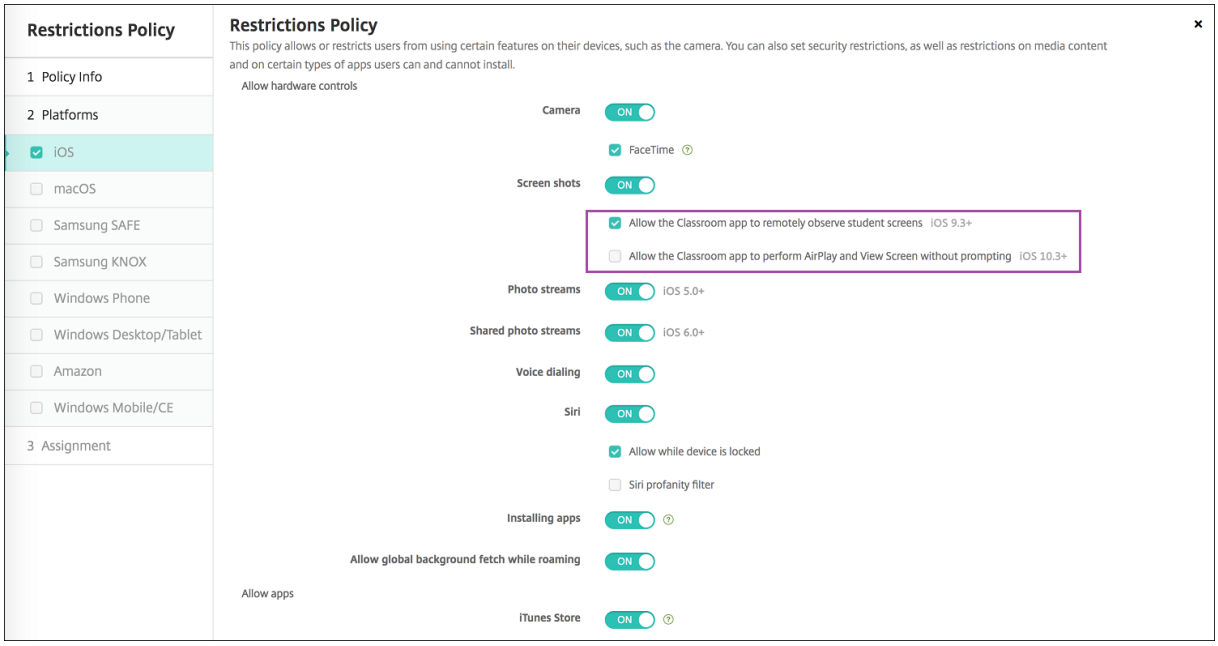
La directiva "Restricciones" permite o prohíbe a los usuarios utilizar funciones determinadas en sus dispositivos, como la cámara. También puede estipular restricciones de seguridad, de contenido multimedia y de tipos de aplicaciones que los usuarios puedan o no puedan instalar. El valor predeterminado de la mayoría de las opciones de restricción es **Activado** o *permite*. Las excepciones principales son la función "Seguridad: Forzar" de iOS y todas las funciones de tabletas Windows, que están **desactivadas** o establecidas en *restringe* de forma predeterminada.

Para Windows 10 RS2 Phone: después de implementar en el teléfono una directiva de XML personalizado o una directiva de restricciones que inhabilita Internet Explorer, el explorador web permanece habilitado. Para solucionar este problema, reinicie el teléfono. Este es un problema de terceros.

> **Sugerencia:**
>
> Si **activa** una opción, significa que el usuario puede realizar la operación o usar la función. Por ejemplo:
>
> **Cámara**. Si está **activada**, el usuario puede usar la cámara en su dispositivo. Si está **desactivada**, el usuario no puede usar la cámara en su dispositivo.
>
> **Capturas de pantalla**. Si está **activada**, el usuario puede realizar capturas de pantalla en su dispositivo. Si está **desactivada**, el usuario no puede realizar capturas de pantalla en su dispositivo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS



Algunas configuraciones de la directiva Restricciones para iOS solo se aplican a versiones concretas de iOS, como se indica aquí y en la página de la directiva Restricciones de la consola de XenMobile.

Pueden ser aplicables configuraciones de directiva de restricciones de iOS cuando el dispositivo está inscrito en modo de inscripción de usuario, en modo no supervisado (MDM completo) o en modo supervisado. En la tabla siguiente, se muestran los modos de inscripción disponibles para cada configuración de directiva de restricciones para iOS 13 y versiones posteriores.

Como se señala en la tabla, algunas configuraciones que anteriormente estaban disponibles en modo no supervisado y supervisado están disponibles solo en modo supervisado, a partir de iOS 13. Se aplican las siguientes reglas:

- Si un dispositivo supervisado posterior a iOS 13 se inscribe en XenMobile, se le aplica la configuración.
- Si un dispositivo no supervisado posterior a iOS 13 se inscribe en XenMobile, no se le aplica la configuración.
- Si un dispositivo iOS 12 (o anterior) ya inscrito en XenMobile se actualiza a iOS 13, no hay cambios. La configuración se aplica al dispositivo del mismo modo que antes de la actualización.

Para obtener información sobre cómo poner un dispositivo iOS en modo supervisado, consulte Para colocar un dispositivo iOS en modo supervisado mediante Apple Configurator.

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Permitir controles del hardware			
Cámara	No	Sí	Sí
FaceTime	No	No (novedad en iOS 13)	Sí
Capturas de pantalla	Sí	No	Sí
Permitir que la aplicación Aula observe remotamente las pantallas de los alumnos	No	No	Sí
Permitir que la aplicación Aula use AirPlay y Ver pantalla sin preguntar	No	No	Sí
Fotos en streaming	No	Sí	Sí
Permitir compartir fotos en streaming	No	Sí	Sí
Marcado por voz	No	Sí	Sí
Siri	Sí	Sí	Sí
Permitir durante bloqueo del dispositivo	Sí	Sí	Sí
Filtro de lenguaje explícito de Siri	No	No	Sí
Instalar aplicaciones	No	No (novedad en iOS 13)	Sí
Permitir obtención global en segundo plano durante la itinerancia	No	Sí	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Permitir aplicaciones			
iTunes Store	No	No (novedad en iOS 13)	Sí
Compras en la aplicación	No	Sí	Sí
Requerir contraseña de iTunes Store para todas las compras	No	Sí	Sí
Safari	No	No (novedad en iOS 13)	Sí
Autorrelleno	No	No (novedad en iOS 13)	Sí
Forzar advertencia de fraude	Sí	Sí	Sí
Habilitar JavaScript	No	Sí	Sí
Bloquear ventanas emergentes	No	Sí	Sí
Aceptar cookies	No	Sí	Sí
Red: Permite acciones de iCloud			
Datos y documentos de iCloud	No	No (novedad en iOS 13)	Sí
Copia de seguridad de iCloud	No	Sí	Sí
Llavero de fotos de iCloud	No	Sí	Sí
Fototeca iCloud	No	Sí	Sí
Seguridad: Forzar			
Copias de seguridad cifradas	Sí	Sí	Sí
Seguimiento de publicidad limitado	No	Sí	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Código de acceso para enlazar con AirPlay por primera vez	Sí	Sí	Sí
Apple Watch emparejado para usar detección de muñeca	Sí	Sí	Sí
Compartir documentos administrados con AirDrop	Sí	Sí	Sí
Seguridad: Permitir			
Aceptar certificados SSL que no son de confianza	No	Sí	Sí
Permitir actualización automática de parámetros de confianza de certificados	No	Sí	Sí
Documentos de aplicaciones administradas en aplicaciones no administradas	Sí	Sí	Sí
Las aplicaciones no administradas pueden leer contactos administrados	No	No	Sí
Las aplicaciones administradas pueden registrar contactos no administrados	No	No	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Documentos de aplicaciones no administradas en aplicaciones administradas	Sí	Sí	Sí
Envío de información de diagnóstico a Apple	Sí	Sí	Sí
Permitir Touch ID para desbloquear el dispositivo	No	Sí	Sí
Notificaciones de Passbook durante bloqueo de dispositivo	No	Sí	Sí
Handoff	No	Sí	Sí
Sincronización de iCloud para aplicaciones administradas	Sí	Sí	Sí
Copia de seguridad de libros de la empresa	Sí	Sí	Sí
Sincronización de notas y subrayados de libros de la empresa	Sí	Sí	Sí
Resultados de Internet en Spotlight	No	Sí	Sí
Confianza en aplicaciones de empresa	No	Sí	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Parámetros solo para dispositivos supervisados: Permitir			
Borrar todo el contenido y los parámetros	No	No	Sí
Configurar restricciones	No	No	Sí
Podcasts	No	No	Sí
Instalar perfiles de configuración	No	No	Sí
Modificación de huella digital	No	No	Sí
Instalar aplicaciones desde el dispositivo	No	No	Sí
Teclas de acceso rápido	No	No	Sí
Apple Watch emparejado	No	No	Sí
Modificación de código de acceso	No	No	Sí
Modificación de nombre de dispositivo	No	No	Sí
Modificación de fondo de pantalla	No	No	Sí
Descarga automática de aplicaciones	No	No	Sí
AirDrop	No	No	Sí
iMessage	No	No	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Contenido de Siri generado por el usuario	No	No	Sí
iBooks	No	No	Sí
Quitar aplicaciones	No	Sí	Sí
Game Center	No	No (novedad en iOS 13)	Sí
Añadir amigos	No	No	Sí
Juegos multijugador	No	No (novedad en iOS 13)	Sí
Modificar parámetros de cuenta	No	No	Sí
Modificar parámetros de datos móviles de las aplicaciones	No	No	Sí
Modificar parámetros de datos móviles de las aplicaciones	No	No	Sí
Permitir modificar parámetros de Buscar a mis amigos	No	No	Sí
Emparejar hosts que no tienen Configurator	No	No	Sí
Teclado predictivo	No	No	Sí
Teclado con corrección automática	No	No	Sí
Teclado con revisión ortográfica	No	No	Sí
Búsqueda de definiciones	No	No	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
ID único de paquete de la aplicación			
Noticias	No	No	Sí
Servicio Apple Music	No	No	Sí
iTunes Radio	No	No	Sí
Modificación de notificaciones	No	No	Sí
Uso de aplicaciones restringidas	No	No	Sí
Modificación de envío de diagnósticos	No	No	Sí
Modificación de Bluetooth	No	No	Sí
Permitir dictado	No	No	Sí
Unirse solo a redes Wi-Fi instaladas por una directiva de Wi-Fi	No	No	Sí
Permitir que la aplicación Aula use AirPlay y Ver pantalla sin preguntar	No	No	Sí
Permitir que la aplicación Aula bloquee una aplicación y bloquee el dispositivo sin preguntar	No	No	Sí
Unirse automáticamente a las clases de la aplicación Aula sin preguntar	No	No	Sí
Permitir AirPrint	No	No	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Permitir el almacenamiento de las credenciales de AirPrint en el Llavero	No	No	Sí
Permitir la detección de impresoras AirPrint mediante iBeacons	No	No	Sí
Permitir AirPrint solo en destinos con certificados de confianza	No	No	Sí
Agregar configuraciones VPN	No	No	Sí
Modificar parámetros de planes de datos móviles	No	No	Sí
Eliminar aplicaciones de sistema	No	No	Sí
Configurar nuevos dispositivos cercanos	No	No	Sí
Permitir modo restringido de USB	No	No	Sí
Forzar demora de actualizaciones de software	No	No	Sí
Demora forzosa para actualizaciones de software	No	No	Sí
Forzar permiso del aula para abandonar clases	No	No	Sí
Forzar fecha y hora automáticas	No	No	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Autorrelleno de contraseñas	No	No	Sí
Solicitud de contraseña a los contactos cercanos	No	No	Sí
Compartir contraseña	No	No	Sí
Seguridad: Mostrar en pantalla de bloqueo			
Centro de control	Sí	Sí	Sí
Notificación	Sí	Sí	Sí
Vista Hoy	Sí	Sí	Sí
Contenido multimedia: Permitir			
Música, podcasts y contenido de iTunes U explícito	No	No (novedad en iOS 13)	Sí
Contenido sexual explícito en iBooks	No	Sí	Sí
Región de calificación	No	Sí	Sí
Películas	No	Sí	Sí
Programas de TV	No	Sí	Sí
Aplicaciones	No	Sí	Sí

- **Permitir controles del hardware**
  - **Cámara:** Permite que los usuarios usen la cámara en sus dispositivos.
    - **FaceTime:** Permite que los usuarios usen FaceTime en sus dispositivos. Para dispositivos iOS supervisados.
  - **Capturas de pantalla:** Permite que los usuarios hagan capturas de pantalla en sus dispositivos.
    - **Permitir que la aplicación Aula observe remotamente las pantallas de los alumnos:** Si no se activa esta restricción, el profesor no puede usar la aplicación Aula para

observar de forma remota las pantallas de los alumnos. Está activado de forma predeterminada; así, un profesor puede utilizar la aplicación Aula para observar las pantallas de los alumnos. El parámetro **Permitir que la aplicación Aula use AirPlay y Ver pantalla sin preguntar** determina si los alumnos reciben una solicitud para conceder permiso al profesor. Para dispositivos iOS supervisados.

  * **Permitir que la aplicación Aula utilice AirPlay y ver la pantalla sin preguntar:** Si esta restricción está seleccionada, el profesor puede utilizar AirPlay y ver la pantalla en el dispositivo de un alumno sin solicitar permiso. Está desactivado de forma predeterminada. Para dispositivos iOS supervisados.

- **Fotos en streaming:** Permite que los usuarios usen MyPhotoStream para compartir fotos a través de iCloud con todos sus dispositivos iOS.
- **Permitir compartir fotos en streaming:** Permite que los usuarios usen iCloud Photo Sharing para compartir fotos con compañeros de trabajo, amigos y familiares.
- **Marcado por voz:** Habilita el marcado por voz en los dispositivos de los usuarios.
- **Siri:** Permite Siri a los usuarios.
  * **Permitir durante bloqueo del dispositivo:** Permite a los usuarios usar Siri mientras sus dispositivos están bloqueados.
  * **Filtro de lenguaje explícito de Siri.** Habilitar el filtro de lenguaje explícito de Siri. El valor predeterminado es la restricción de esta función, lo que significa que no se aplica ningún filtro de palabras malsonantes.
    Para obtener más información sobre la seguridad y Siri, consulte Directivas de Siri y dictado.
- **Instalación de aplicaciones:** Permite que los usuarios instalen aplicaciones. Para dispositivos iOS supervisados.
- **Permitir obtención global en segundo plano durante la itinerancia:** Permite que los dispositivos sincronicen automáticamente cuentas de correo electrónico con iCloud mientras el dispositivo está en itinerancia. Si está **desactivada**, no permite la obtención global de datos en segundo plano cuando un teléfono iOS está en itinerancia. Está **activado** de forma predeterminada.

- **Permitir aplicaciones**
  - **iTunes Store:** Permite que los usuarios accedan a la tienda iTunes. Para dispositivos iOS supervisados.
  - **Compras en la aplicación:** Permite que los usuarios hagan compras desde la aplicación.
    * **Requerir contraseña de iTunes para todas las compras:** Solicita una contraseña para las compras desde la aplicación. El valor predeterminado es la restricción de esta función, lo que significa que no se pide contraseña para realizar compras en la aplicación.
  - **Safari:** Permite que los usuarios accedan a Safari. Para dispositivos iOS supervisados.
    * **Autorrelleno:** Permite que los usuarios configuren el autorrelleno de nombres de

usuario y contraseñas en Safari.
    * **Forzar advertencia de fraude.** Si este parámetro está habilitado y los usuarios visitan un sitio web sospechoso de "phishing", Safari advierte a los usuarios. El valor predeterminado es la restricción de esta función, lo que significa que no se emite ninguna advertencia.
    * **Habilitar JavaScript:** Permite que JavaScript se ejecute en Safari.
    * **Bloquear elementos emergentes.** Bloquear los elementos emergentes cuando se visitan sitios web. El valor predeterminado es la restricción de esta función, lo que significa que no se bloquean los elementos emergentes.
  - **Aceptar cookies.** Defina el nivel al que se aceptan las cookies. En la lista, elija una opción para permitir o restringir las cookies. El valor predeterminado es **Siempre**, lo que permite que todos los sitios guarden cookies en Safari. Las demás opciones son: **Solo del sitio web actual**, **Nunca** y **Solo de sitios web visitados**.

- **Red: Permite acciones de iCloud**
  - **Datos y documentos de iCloud:** Permite que los usuarios sincronicen con iCloud los documentos y los datos. Para dispositivos iOS supervisados.
  - **Copia de seguridad de iCloud:** Permite que los usuarios guarden copias de seguridad de sus dispositivos en iCloud.
  - **Permitir llavero de iCloud:** Permite que los usuarios guarden sus nombres de usuario, contraseñas, información de redes Wi-Fi y datos de tarjeta de crédito en el Llavero de iCloud.
  - **Fototeca iCloud:** Permite que los usuarios accedan a su biblioteca de fotos de iCloud.

- **Seguridad: Forzar**

  El valor predeterminado es restringir las siguientes funciones, lo que significa que ninguna de las funciones de seguridad está habilitada.
  - **Copias de seguridad cifradas.** Forzar el cifrado de las copias de seguridad que se almacenarán en iCloud.
  - **Limitar seguimiento de anuncios:** Bloquear el seguimiento de anuncios segmentados.
  - **Código de acceso para enlazar con AirPlay por primera vez:** Requiere que los dispositivos de usuario con AirPlay habilitado se verifiquen con un código de uso único en pantalla para poder usar AirPlay.
  - **Apple Watch emparejado para usar detección de muñeca:** Requiere a un Apple Watch enlazado que use la **detección de muñeca**.
  - **Compartir documentos administrados con AirDrop:** Al **activar** esta opción, AirDrop aparece como un destino no administrado para colocar contenido.

- **Seguridad: Permitir**
  - **Aceptar certificados SSL que no son de confianza:** Permite que los usuarios acepten

certificados SSL que no son de confianza cuando visitan sitios web.

- **Permitir actualización automática de parámetros de confianza de certificados:** Permite la actualización automática de los certificados de confianza.
- **Documentos de aplicaciones administradas en aplicaciones no administradas:** Permite que los usuarios muevan datos desde aplicaciones administradas (corporativas) a aplicaciones no administradas (personales).
- **Documentos de aplicaciones no administradas en aplicaciones administradas:** Permite que los usuarios muevan datos desde aplicaciones no administradas (personales) a aplicaciones administradas (corporativas).
- **Envío de información de diagnóstico a Apple:** Permite el envío a Apple de datos anónimos de diagnóstico sobre los dispositivos de los usuarios.
- **Permitir Touch ID para desbloquear el dispositivo:** Permite que los usuarios usen sus huellas dactilares para desbloquear sus dispositivos.
- **Notificaciones de Passbook con dispositivo bloqueado:** Permite que las notificaciones de Passbook aparezcan en la pantalla de bloqueo.
- **Handoff:** Permite que los usuarios transfieran actividades desde un dispositivo iOS a otro dispositivo iOS cercano.
- **Sincronización de iCloud para aplicaciones administradas:** Permite que los usuarios sincronicen con iCloud las aplicaciones administradas.
- **Copia de seguridad de libros de la empresa:** Permite que se guarden copias de seguridad de los libros de la empresa en iCloud.
- **Sincronización de notas y subrayados de libros de la empresa:** Permite la sincronización con iCloud de las notas y los resaltados agregados por los usuarios a los libros de la empresa.
- **Confianza en aplicaciones de empresa:** Permite la confianza en las aplicaciones de empresa. Las aplicaciones de empresa son aquellas aplicaciones personalizadas para su organización. Pueden crearse de forma interna o pueden desarrollarse y adquirirse de un proveedor externo. Para obtener más información, consulte Instalar apps de empresa personalizadas en iOS.
- **Resultados de Internet en Spotlight:** Permite que Spotlight muestre los resultados de búsquedas encontrados en Internet y los encontrados en el dispositivo.
- **Las aplicaciones no administradas pueden leer contactos administrados:** Opcional. Solo disponible si **Documentos de aplicaciones administradas en aplicaciones no administradas** está desactivado. Si esta directiva está habilitada, las aplicaciones no administradas pueden leer datos de los contactos de las cuentas administradas. Está **desactivado** de forma predeterminada. Disponible a partir de iOS 12.
- **Las aplicaciones administradas pueden registrar contactos no administrados:** Opcional. Si está habilitado, se permite que las aplicaciones administradas agreguen contactos a los contactos de cuentas no administradas. Si **Documentos de aplicaciones ad-**

ministradas en aplicaciones no administradas está habilitado, esta restricción no tiene efecto. Está **desactivado** de forma predeterminada. Disponible a partir de iOS 12.

- **Parámetros solo para dispositivos supervisados: Permitir**

  Estos parámetros solo se aplican a dispositivos supervisados. 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.

  - **Borrar todo el contenido y los parámetros:** Permite que los usuarios borren todo el contenido y los parámetros de sus dispositivos.
  - **Configuración de restricciones:** Permite que los usuarios configuren controles parentales en sus dispositivos.
  - **Podcasts:** Permite que los usuarios descarguen y sincronicen podcasts.
  - **Instalación de perfiles de configuración:** Permite que los usuarios instalen un perfil de configuración distinto del implementado.
  - **Modificación de huella digital:** Permite que los usuarios cambien o eliminen su huella dactilar de Touch ID.
  - **Instalar aplicaciones desde el dispositivo:** Permite que los usuarios instalen aplicaciones. Al inhabilitar este parámetro, los usuarios finales no pueden instalar nuevas aplicaciones. El App Store está inhabilitado y su icono se quita de la pantalla de inicio.
  - **Teclas de acceso rápido:** Permite que los usuarios creen métodos de teclado abreviados y personalizados para palabras o frases que usan con frecuencia.
  - **Apple Watch emparejado:** Permite que los usuarios enlacen un Apple Watch a un dispositivo supervisado.
  - **Modificación de código de acceso:** Permite que los usuarios cambien el código de acceso en un dispositivo supervisado.
  - **Modificación de nombre de dispositivo:** Permite que los usuarios cambien el nombre de su dispositivo.
  - **Modificar de fondo de pantalla:** Permite que los usuarios cambien el fondo de pantalla en sus dispositivos.
  - **Descarga automática de aplicaciones:** Permite descargar aplicaciones.
  - **AirDrop:** Permite que los usuarios compartan fotos, vídeos, sitios web y ubicaciones, entre otros, con dispositivos iOS cercanos.
  - **iMessage:** Permite que los usuarios envíen mensajes de texto por Wi-Fi con iMessage.

- **Contenido de Siri generado por el usuario:** Permite que Siri haga consultas de contenido generado por usuarios desde la web. Los llamados consumidores y periodistas no tradicionales generan el contenido generado por el usuario. Por ejemplo, el contenido de Twitter o Facebook se considera como contenido generado por el usuario.
- **iBooks:** Permite que los usuarios usen la aplicación iBooks.
- **Eliminar aplicaciones:** Permite que los usuarios quiten aplicaciones de sus dispositivos.
- **Game Center:** Permite que los usuarios jueguen en línea a través de Game Center en sus dispositivos.
  - **Agregar amigos:** Permite que los usuarios envíen notificaciones a amigos para participar en un juego.
  - **Juegos multijugador:** Permite que los usuarios inicien juegos multijugador en sus dispositivos.
- **Modificar parámetros de cuenta:** Permite que los usuarios modifiquen los ajustes de cuenta de su dispositivo.
- **Permitir modificar parámetros de datos móviles de las aplicaciones:** Permite que los usuarios modifiquen el modo en que las aplicaciones usan los datos móviles.
- **Permitir modificar parámetros de Buscar a mis amigos:** Permite que los usuarios cambien los parámetros de Buscar a mis amigos.
- **Emparejamiento con hosts que no tienen Configurator:** Permite al administrador controlar con qué dispositivos puede emparejarse el dispositivo de un usuario. Si se inhabilita este parámetro, se impide el emparejamiento excepto con el host supervisor que ejecuta Apple Configurator. Si no se ha configurado ningún certificado de host supervisor, todo el emparejamiento estará inhabilitado.
- **Teclado predictivo:** Permite que los usuarios usen el teclado predictivo para sugerir palabras mientras teclean en sus dispositivos. Inhabilite esta opción en situaciones tales como la administración de textos estándar donde no quiere que los usuarios tengan acceso a sugerencias de palabras.
- **Teclado con corrección automática:** Permite que los usuarios usen la corrección automática del teclado en sus dispositivos. Inhabilite esta opción en situaciones tales como la administración de textos estándar donde no quiere que los usuarios tengan acceso a la corrección automática.
- **Teclado con revisión ortográfica:** Permite que los usuarios usen la revisión ortográfica mientras teclean en sus dispositivos. Inhabilite esta opción en situaciones tales como la administración de textos estándar donde no quiere que los usuarios tengan acceso a la revisión ortográfica.

- **Búsqueda de definiciones:** Permite que los usuarios usen la búsqueda de definiciones mientras teclean en sus dispositivos. Inhabilite esta opción en situaciones tales como la administración de textos estándar donde no quiere que los usuarios tengan acceso a la búsqueda de definiciones mientras teclean.
- **ID único de paquete de la aplicación.** Cree una lista de las aplicaciones a las que se permite conservar el control sobre el dispositivo e impedir la interacción con otras aplicaciones o funciones.
  Para agregar una aplicación, haga clic en **Agregar**, escriba un **Nombre de aplicación** y haga clic en **Guardar**. Repita este proceso para cada aplicación que quiera agregar.
- **News:** Permite que los usuarios usen la aplicación News.
- **Servicio Apple Music:** Permite que los usuarios usen el servicio Apple Music. Si no quiere permitir el uso del servicio Apple Music, la aplicación Música se ejecuta en el modo clásico.
- **iTunes Radio:** Permite que los usuarios usen iTunes Radio.
- **Modificación de notificaciones:** Permite que los usuarios modifiquen los parámetros de notificación.
- **Uso de aplicaciones restringidas:** Permite que los usuarios usen todas las aplicaciones, o bien usen o no usen las aplicaciones en función de los ID de paquete que proporcione. Se aplica solo a los dispositivos supervisados. Si selecciona **Permitir solo algunas aplicaciones**, agregue una aplicación con el ID de paquete `com.apple.webapp` para permitir clips web.

  > **Nota:**
  >
  > A partir de iOS 11, Apple introdujo cambios en las directivas que están disponibles para las restricciones a aplicaciones. Apple ya no permite eliminar el acceso a la aplicación Ajustes y a la aplicación Teléfono al restringir el paquete de aplicaciones iOS correspondiente.

  Después de configurar la directiva de restricciones para bloquear algunas aplicaciones y, a continuación, implementar la directiva: Si quiere permitir más adelante algunas o todas esas aplicaciones, cambiar y volver a implementar la directiva de restricciones no cambia esas restricciones. En este caso, iOS no aplica los cambios en el perfil de iOS. Para proceder, use la directiva de eliminación de perfiles para eliminar el perfil de iOS y, a continuación, implemente la directiva de restricciones actualizada.

  Si quiere cambiar este parámetro a **Permitir solo algunas aplicaciones**, antes de implementar esta directiva, indique a los usuarios de los dispositivos inscritos mediante el Programa de implementación de Apple que inicien sesión en sus cuentas de Apple desde el asistente de configuración. De lo contrario, los usuarios podrían tener que inhabilitar la

autenticación de dos factores en sus dispositivos para poder iniciar sesión en sus cuentas de Apple y acceder a las aplicaciones permitidas.

- **Modificación de envío de diagnósticos:** Permite que los usuarios modifiquen los parámetros de envío de información de diagnóstico y análisis de aplicaciones en el panel **Ajustes > Diagnóstico y uso**.
- **Modificación de Bluetooth:** Permite que los usuarios modifiquen los parámetros de Bluetooth.
- **Permitir dictado:** Solo en dispositivos supervisados. Cuando esta restricción está **desactivada**, no se permite la entrada de comandos de dictado ni de voz a texto. Está **activado** de forma predeterminada.
- **Unirse solo a redes Wi-Fi instaladas por una directiva de Wi-Fi:** Opcional. Solo dispositivos supervisados. Cuando esta restricción se **activa**, el dispositivo solo puede conectarse a aquellas redes Wi-Fi que se hayan configurado a través de un perfil de configuración. Está **desactivado** de forma predeterminada.
- **Permitir que la aplicación Aula utilice AirPlay y ver la pantalla sin preguntar:** Si esta restricción está seleccionada, el profesor puede utilizar AirPlay y ver la pantalla en el dispositivo de un alumno sin solicitar permiso. Está desactivado de forma predeterminada. Para dispositivos iOS supervisados.
- **Permitir que la aplicación Aula bloquee una aplicación y bloquee el dispositivo sin preguntar:** Si esta restricción está **activada** (Sí), la aplicación Aula bloquea automáticamente los dispositivos de usuario de una aplicación y bloquea el dispositivo sin avisar a los usuarios. Está **desactivado** de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Unirse automáticamente a las clases de la aplicación Aula sin preguntar:** Si esta restricción está **activada** (Sí), la aplicación Aula unirá automáticamente los usuarios a las clases sin avisar a los primeros. Está **desactivado** de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Permitir AirPrint:** Si esta restricción está **desactivada**, los usuarios no podrán imprimir con AirPrint. Está **activado** de forma predeterminada. Cuando esta restricción se **activa**, aparecen estas restricciones adicionales. Para dispositivos supervisados con iOS 11 (versión mínima).
  - **Permitir el almacenamiento de las credenciales de AirPrint en el Llavero:** Si esta restricción no está seleccionada, el nombre de usuario y la contraseña de AirPrint no se almacenan en el Llavero. Está activado de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
  - **Permitir la detección de impresoras AirPrint mediante iBeacons:** Si esta restricción no está seleccionada, la detección de impresoras AirPrint mediante iBeacons

está desactivada. Desactivar la detección impide que balizas falsas de AirPrint por Bluetooth se adjudiquen tráfico de red. Está activado de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).

  * **Permitir AirPrint solo en destinos con certificados de confianza:** Si se selecciona esta restricción, los usuarios pueden utilizar AirPrint para imprimir solamente en destinos con certificados de confianza. Está desactivado de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).

- **Agregar configuraciones VPN:** Si esta restricción está **desactivada** (No), los usuarios no podrán crear configuraciones VPN. Está **activado** de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Modificar parámetros de planes de datos móviles:** Si esta restricción está **desactivada** (No), los usuarios no podrán modificar los parámetros de planes de datos móviles. Está **activado** de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Eliminar aplicaciones del sistema:** Si esta restricción está **desactivada** (No), los usuarios no podrán quitar aplicaciones del sistema que haya presentes en su dispositivo. Está **activado** de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Configurar nuevos dispositivos cercanos:** Si esta restricción está desactivada, los usuarios no podrán configurar nuevos dispositivos cercanos. Está activado de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Permitir modo restringido de USB:** Si está **desactivado** (No), el dispositivo siempre se puede conectar a accesorios USB mientras esté bloqueado. De forma predeterminada, está **activado**. Disponible solamente para dispositivos supervisados iOS 11.3 y versiones posteriores.
- **Forzar demora de actualizaciones de software:** Si está **activado**, retrasa el momento en que el usuario ve las actualizaciones de software. Con esta restricción activada, el usuario no ve una actualización de software hasta que transcurra la cantidad especificada de días después de la fecha de publicación de la actualización. Está **desactivado** de forma predeterminada. Disponible solamente para dispositivos supervisados iOS 11.3 y versiones posteriores.
- **Demora forzosa para actualizaciones de software (días):** Permite especificar una cantidad de días para retrasar una actualización de software en el dispositivo. La demora máxima es **90** días. El valor predeterminado es **30** días. Disponible solamente para dispositivos supervisados iOS 11.3 y versiones posteriores.
- **Forzar permiso del aula para abandonar clases:** Si está **activado** (Sí), un alumno matriculado en un curso no gestionado con Aula debe solicitar el permiso del profesor cuando

intenta abandonar la clase. Está **desactivado** de forma predeterminada. Disponible solamente para dispositivos supervisados iOS 11.3 y versiones posteriores.

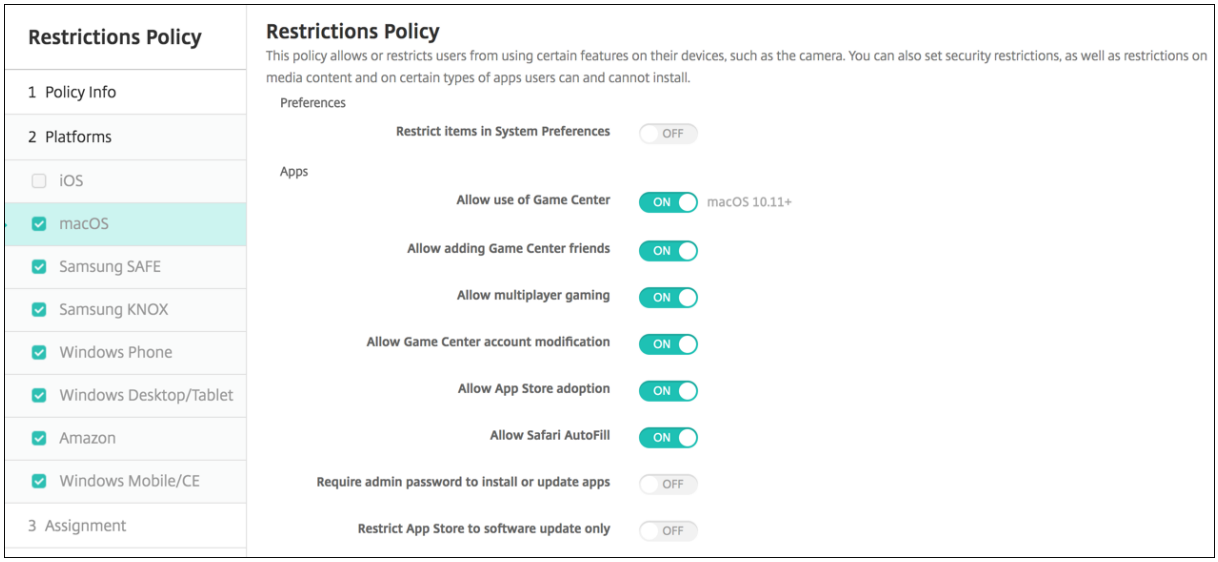
- **Forzar fecha y hora automáticas:** Permite configurar automáticamente la fecha y la hora en los dispositivos supervisados. Si está **activado**, los usuarios de los dispositivos no pueden desactivar **Establecer automáticamente** en **General > Fecha y hora**. La zona horaria en el dispositivo se actualiza solo cuando el dispositivo puede determinar su ubicación. Es decir, cuando un dispositivo tiene una conexión móvil o una conexión Wi-Fi con los servicios de ubicación habilitados. Está **desactivado** de forma predeterminada. Disponible solamente para dispositivos supervisados iOS 12 y versiones posteriores.
- **Autorrelleno de contraseñas:** Opcional. Si está inhabilitado, los usuarios no pueden usar las funciones de autorrelleno de contraseñas o sugerencias de contraseñas seguras. De forma predeterminada, está **activado**. Disponible a partir de iOS 12.
- **Solicitud de contraseña a los contactos cercanos:** Opcional. Si está inhabilitado, los dispositivos de los usuarios no solicitan contraseñas de los dispositivos cercanos. De forma predeterminada, está **activado**. Disponible a partir de iOS 12.
- **Compartir contraseña:** Opcional. Si está inhabilitado, los usuarios no pueden compartir sus contraseñas mediante la función de contraseñas de AirDrop. De forma predeterminada, está **activado**. Disponible a partir de iOS 12.

- **Seguridad: Mostrar en pantalla de bloqueo**
  - **Centro de control:** Permite el acceso al Centro de control en la pantalla de bloqueo. El Centro de control facilita a los usuarios la modificación de las funciones Modo Avión, Wi-Fi, Bluetooth, No molestar y Bloquear rotación.
  - **Notificación:** Permite notificaciones en la pantalla de bloqueo.
  - **Vista Hoy:** Permite la vista Hoy, que agrupa información diversa, como el tiempo y los eventos del calendario para el día en curso en la pantalla de bloqueo.
- **Contenido multimedia: Permitir**
  - **Música, podcasts y contenido de iTunes U explícito:** Permite material explícito en los dispositivos de los usuarios.
  - **Contenido sexual explícito en iBooks:** Permite la descarga de material explícito desde iBooks.
  - **Región de calificación:** Defina la región desde donde se obtienen las calificaciones de control parental. En la lista, haga clic en un país para establecer la región de las clasificaciones. El valor predeterminado es **Estados Unidos**.
  - **Películas:** Establezca si se permiten películas en los dispositivos de los usuarios. Si permite las películas, puede configurar también un nivel de clasificación de estas. En la lista, haga clic en una opción para permitir o restringir las películas en el dispositivo. El valor predeterminado es “Permitir todas las películas”.

- **Programas de TV:** Defina si se permiten programas de TV en los dispositivos de los usuarios. Si permite los programas de TV, puede configurar también un nivel de clasificación de estos. En la lista, haga clic en una opción para permitir o restringir los programas de TV en el dispositivo. El valor predeterminado es “Permitir todos los programas de TV”.
- **Aplicaciones:** Defina si se permiten aplicaciones en los dispositivos de los usuarios. Si permite aplicaciones, puede configurar también un nivel de clasificación de estas. En la lista, haga clic en una opción para permitir o restringir las aplicaciones en el dispositivo. El valor predeterminado es “Permitir todas las aplicaciones”.

- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible en iOS 9.3 y versiones posteriores.

Parámetros de macOS



- **Preferencias**
  - **Restringir elementos de Preferencias del Sistema:** Permita o restrinja el acceso de los usuarios a Preferencias del Sistema. Está **desactivado** de forma predeterminada, lo que concede a los usuarios acceso completo a las preferencias del sistema. Si esta opción se

habilita, defina las siguientes opciones de configuración:

* **Panel de Preferencias del Sistema:** Elija si las opciones que seleccione se habilitarán o inhabilitarán. Todas las opciones están **activadas** de forma predeterminada.
  - Usuarios y grupos
  - General
  - Accesibilidad
  - App Store
  - Actualización de software
  - Bluetooth
  - CD y DVD
  - Fecha y hora
  - Escritorio y protector de pantalla
  - Pantallas
  - Dock
  - Ahorro de energía
  - Extensiones
  - FibreChannel
  - iCloud
  - Ink
  - Cuentas de Internet
  - Teclado
  - Idioma y texto
  - Mission Control
  - Puntero
  - Red
  - Notificaciones
  - Control parental
  - Impresoras y escáneres
  - Perfiles
  - Seguridad y privacidad
  - Compartir
  - Sonido
  - Dictado y voz
  - Spotlight
  - Disco de arranque
  - Time Machine
  - Trackpad
  - Xsan

- **Aplicaciones**

- **Permitir el uso de Game Center:** Permite que los usuarios jueguen en línea a través de Game Center en sus dispositivos. Está **activado** de forma predeterminada.
- **Permitir agregar amigos de Game Center:** Permite que los usuarios envíen notificaciones a amigos para participar en un juego. Está **activado** de forma predeterminada.
- **Permitir juegos multijugador:** Permite que los usuarios inicien juegos multijugador. Está **activado** de forma predeterminada.
- **Permitir modificar cuenta de Game Center:** Permite que los usuarios modifiquen la configuración de sus cuentas de Game Center. Está **activado** de forma predeterminada.
- **Permitir adopción de App Store:** Permite o restringir que el App Store de Apple adopte aplicaciones ya existentes en OS X. Está **activado** de forma predeterminada.
- **Permitir autorrelleno en Safari:** Permite que Safari rellene automáticamente campos en sitios web con contraseñas, direcciones y demás información básica que haya almacenado. Está **activado** de forma predeterminada.
- **Requerir contraseña de administrador para instalar o actualizar aplicaciones:** Requiere una contraseña de administrador para instalar o actualizar aplicaciones. Está **desactivado** de forma predeterminada, lo que significa que no se requiere contraseña de administrador.
- **Restringir App Store a actualizaciones de software solamente:** Restringe el App Store a solo actualizaciones, lo que inhabilita todas las fichas del App Store de Apple salvo las actualizaciones (Updates). Está **desactivado** de forma predeterminada, lo que permite el acceso total al App Store.
- **Restringir las aplicaciones que se puede abrir:** Restringe o permite las aplicaciones que puedan utilizar los usuarios. Está desactivado de forma predeterminada, lo que permite el uso de todas las aplicaciones. Si activa esta opción, defina los siguientes parámetros:
  - **Aplicaciones permitidas:** Haga clic en **Agregar**, escriba el nombre y el ID de paquete de una aplicación cuyo inicio esté permitido y, a continuación, haga clic en **Guardar**. Repita este paso para cada aplicación cuyo inicio esté permitido.
  - **Carpetas no permitidas:** Haga clic en **Agregar**, escriba la ruta de la carpeta a la que quiera restringir el acceso de los usuarios (por ejemplo, /Aplicaciones/Utilidades) y, a continuación, haga clic en **Guardar**. Repita este paso para cada carpeta a la que no quiera que accedan los usuarios.
  - **Carpetas permitidas:** Haga clic en **Agregar**, escriba la ruta de la carpeta a la que quiera permitir el acceso por parte de los usuarios y, a continuación, haga clic en **Guardar**. Repita este paso para cada carpeta a la que quiera que los usuarios puedan acceder.

- **Widgets**
  - **Permitir solo la ejecución de estos widgets del panel de mandos:** Permite o restringe los widgets del panel de mandos, como el Reloj internacional o la Calculadora, que los usuarios pueden ejecutar. Está **desactivado** de forma predeterminada, lo que permite

a los usuarios ejecutar todos los widgets. Si activa esta opción, defina el siguiente parámetro:

* **Widgets permitidos:** Haga clic en **Agregar**, escriba el nombre y el ID de un widget que se pueda ejecutar y, a continuación, haga clic en **Guardar**. Repita este paso para cada widget que quiera ejecutar en el panel de mandos.

- **Medios**
  - **Permitir AirDrop:** Permite que los usuarios compartan fotos, vídeos, sitios web, ubicaciones y otros objetos con dispositivos iOS cercanos.
- **Compartir**
  - **Habilitar automáticamente nuevos servicios de uso compartido:** Seleccione si el uso compartido de los servicios se habilita automáticamente.
  - **Correo:** Seleccione si permitir un buzón compartido.
  - **Facebook:** Seleccione si permitir una cuenta compartida de Facebook.
  - **Servicios de vídeo: Flickr, Vimeo, Tudou y Youku:** Seleccione si permitir servicios de vídeos compartidos.
  - **Agregar a Aperture:** Seleccione si habilitar la capacidad de compartir elementos agregados a Aperture.
  - **Sina Weibo:** Seleccione si permitir una cuenta compartida de microblogs en Sina Weibo.
  - **Twitter:** Seleccione si permitir una cuenta compartida de Twitter.
  - **Mensajes:** Seleccione si permitir el acceso compartido a los mensajes.
  - **Agregar a iPhoto:** Seleccione si permitir la capacidad compartida de agregar contenido a iPhoto.
  - **Agregar a la lista de lectura:** Seleccione si permitir la capacidad compartida de agregar contenido a la lista de lectura.
  - **AirDrop:** Seleccione si permitir una cuenta compartida de AirDrop.
- **Funcionalidad**
  - **Bloquear imagen de escritorio:** Seleccione si los usuarios pueden cambiar la imagen de sus escritorios. Está **desactivado** de forma predeterminada, lo que significa que los usuarios pueden cambiar la imagen del escritorio.
  - **Permitir el uso de la cámara:** Seleccione si los usuarios pueden usar la cámara en sus Mac. Está **desactivado** de forma predeterminada, con lo que los usuarios no pueden utilizar la cámara.
  - **Permitir Apple Music:** Permite a los usuarios usar el servicio Apple Music (a partir de macOS 10.12). Si no quiere permitir el uso del servicio Apple Music, la aplicación Música se ejecuta en el modo clásico. Se aplica solo a los dispositivos supervisados. Está **activado** de forma predeterminada.
  - **Permitir sugerencias de Spotlight:** Seleccione si los usuarios pueden usar sugerencias de Spotlight en las búsquedas de sus equipos Mac y para proporcionar sugerencias de Spotlight procedentes de Internet, iTunes y el App Store. Está **desactivado** de forma pre-

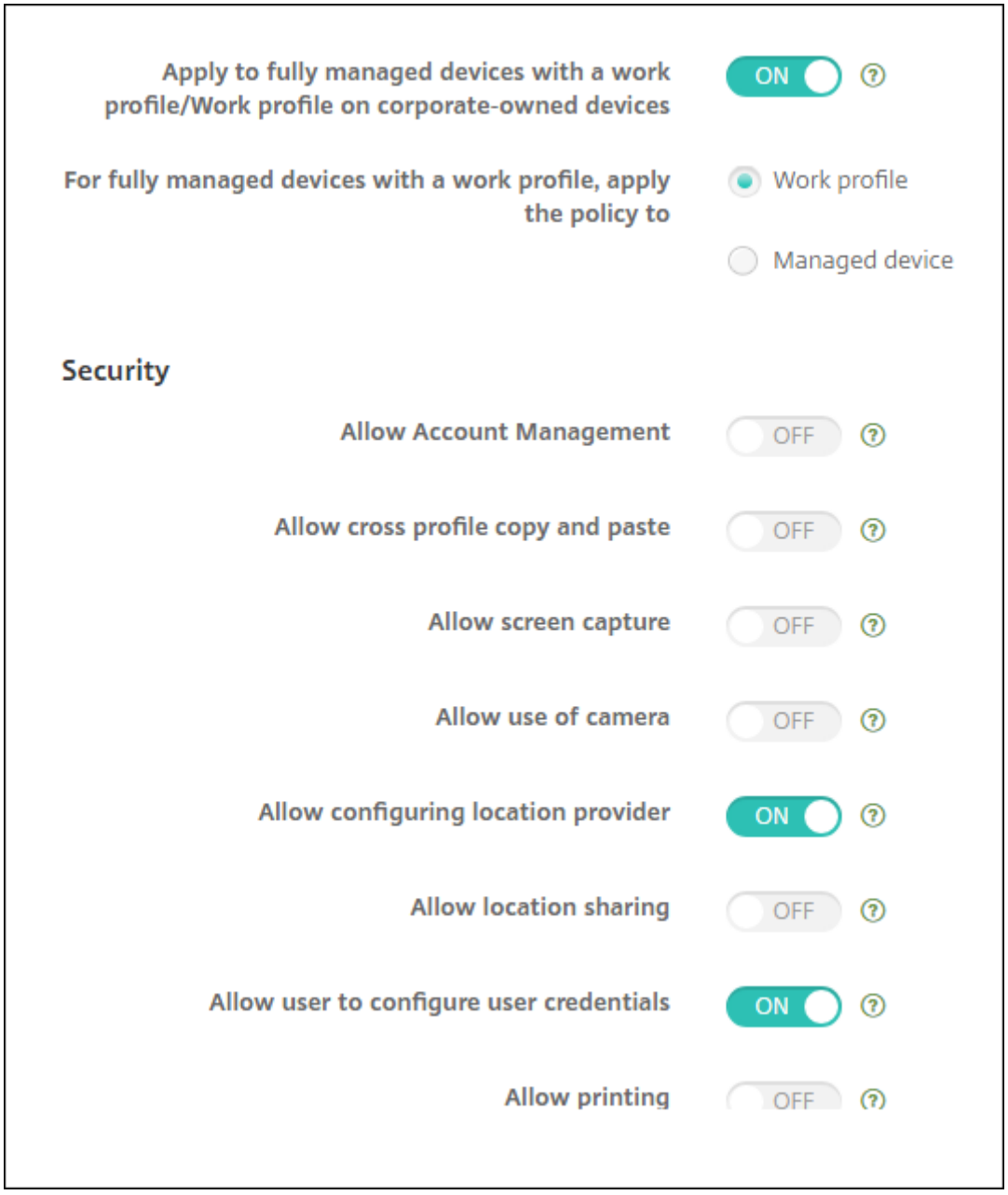
determinada, lo que impide que los usuarios utilicen sugerencias de Spotlight.
- **Permitir búsquedas:** Seleccione si los usuarios pueden buscar la definición de palabras con el menú contextual o el menú de búsqueda de Spotlight. Está desactivado de forma predeterminada, lo que impide que los usuarios utilicen Buscar en sus equipos Mac.
- **Permitir el uso de la contraseña de iCloud para cuentas locales:** Seleccione si los usuarios pueden usar su ID de Apple y su contraseña de iCloud para iniciar sesión en su Mac. Si se habilita esta directiva, los usuarios usarán solo un ID y una contraseña para *todas* las pantallas de inicio de sesión de sus Mac. Está **activado** de forma predeterminada, lo que permite a los usuarios utilizar su ID de Apple y su contraseña de iCloud para acceder a su Mac.
- **Permitir datos y documentos de iCloud:** Seleccione si quiere permitir que los usuarios accedan a documentos y datos almacenados en iCloud desde sus equipos Mac. Este parámetro está **desactivado** de forma predeterminada, lo que impide a los usuarios utilizar documentos y datos de iCloud en su Mac.
  * **Permitir escritorio y documentos de iCloud** (a partir de macOS 10.12.4): El valor predeterminado está seleccionado.
- **Permitir sincronización de llavero de iCloud:** Permite la sincronización del llavero de iCloud (a partir de macOS 10.12). Está **activado** de forma predeterminada.
- **Permitir Correo de iCloud:** Permite que los usuarios utilicen Correo de iCloud (a partir de macOS 10.12). Está **activado** de forma predeterminada.
- **Permitir Contactos de iCloud:** Permite que los usuarios utilicen Contactos de iCloud (a partir de macOS 10.12). Está **activado** de forma predeterminada.
- **Permitir Calendarios de iCloud:** Permite que los usuarios utilicen Calendarios de iCloud (a partir de macOS 10.12). Está **activado** de forma predeterminada.
- **Permitir Recordatorios de iCloud:** Permite que los usuarios utilicen Recordatorios de iCloud (a partir de macOS 10.12). Está **activado** de forma predeterminada.
- **Permitir Favoritos de iCloud:** Permite que los usuarios sincronicen Favoritos de iCloud (a partir de macOS 10.12). Está **activado** de forma predeterminada.
- **Permitir Notas de iCloud:** Permite que los usuarios utilicen Notas de iCloud (a partir de macOS 10.12). Está **activado** de forma predeterminada.
- **Permitir fotos de iCloud:** Si **desactiva** este parámetro, cualquier foto que no se haya descargado totalmente desde la biblioteca de fotos de iCloud se eliminará del almacenamiento local del dispositivo (a partir de macOS 10.12). Está **activado** de forma predeterminada.
- **Permitir desbloqueo automático.** Para obtener información acerca de esta opción y Apple Watch, consulte https://www.imore.com/auto-unlock (macOS 10.12 y versiones posteriores). Está **activado** de forma predeterminada.
- **Permitir Touch ID para desbloquear el Mac** (a partir de macOS 10.12.4): Está **activado** de forma predeterminada.

- **Forzar demora de actualizaciones de software:** Si está **activado**, retrasa el momento en que el usuario ve las actualizaciones de software. Los usuarios no ven una actualización de software hasta que transcurra la cantidad especificada de días después de la fecha de publicación de la actualización. Está **desactivado** de forma predeterminada. Disponible solo para dispositivos supervisados que ejecutan macOS 10.13.4 y versiones posteriores.
- **Demora forzosa para actualizaciones de software (días):** Permite especificar una cantidad de días para retrasar una actualización de software en el dispositivo. El valor máximo es 90 días. El valor predeterminado es **30**. Disponible solo para dispositivos supervisados que ejecutan macOS 10.13.4 y versiones posteriores.
- **Autorrelleno de contraseñas:** Opcional. Si está inhabilitado, los usuarios no pueden usar las funciones de autorrelleno de contraseñas o sugerencias de contraseñas seguras. De forma predeterminada, está **activado**. Disponible a partir de macOS 10.14.
- **Solicitud de contraseña a los contactos cercanos:** Opcional. Si está inhabilitado, los dispositivos de los usuarios no solicitan contraseñas de los dispositivos cercanos. De forma predeterminada, está **activado**. Disponible a partir de macOS 10.14.
- **Compartir contraseña:** Opcional. Si está inhabilitado, los usuarios no pueden compartir sus contraseñas mediante la función de contraseñas de AirDrop. De forma predeterminada, está **activado**. Disponible a partir de macOS 10.14.

Parámetros de Android

- **Cámara:** Permite que los usuarios usen la cámara en sus dispositivos. Si está **desactivado**, se inhabilita la cámara. Está **activado** de forma predeterminada.

Parámetros de Android Enterprise



Cuando un dispositivo Android nuevo o restablecido a los valores de fábrica se inscribe en el modo de perfil de trabajo, los dispositivos con Android 8.0-10.x se inscriben como dispositivos totalmente administrados con un perfil de trabajo. Los dispositivos con Android 11 o una versión posterior se inscriben como un perfil de trabajo en dispositivos propiedad de la empresa. La directiva de restricciones puede aplicarse tanto al perfil de trabajo del dispositivo como al dispositivo administrado.

En los dispositivos inscritos en el modo de perfil de trabajo en dispositivos propiedad de la empresa, estas restricciones solo están disponibles para el perfil de trabajo:

- Permitir servicio de copia de seguridad
- Habilitar aplicaciones del sistema
- Impedir que Keyguard bloquee el dispositivo
- Permitir el uso de la barra de estado
- Mantener encendida la pantalla del dispositivo
- Permitir al usuario controlar los parámetros de la aplicación
- Permitir que el usuario configure las credenciales de usuario
- Permitir configuración VPN
- Permitir almacenamiento USB masivo
- Permitir restablecimiento de valores de fábrica
- Permitir la desinstalación de aplicaciones
- Permitir aplicaciones que no son de Google Play
- Permitir copiar y pegar contenido entre perfiles
- Habilitar verificación de la aplicación
- Permitir administración de cuentas
- Permitir impresión
- Permitir NFC
- Permitir incorporación de usuarios

De forma predeterminada, los parámetros de **depuración por USB y fuentes desconocidas** están inhabilitados en un dispositivo cuando se inscribe en Android Enterprise en el modo de perfil de trabajo.

Para dispositivos con Android 8.0-10.x y Samsung Knox 3.0 o una versión posterior, establezca las configuraciones para Samsung Knox y Samsung SAFE en la página **Android Enterprise**. Para dispositivos con versiones anteriores de Android o Samsung Knox, utilice las páginas **Samsung Knox** y **Samsung SAFE**.

Las restricciones de Samsung no se aplican a los dispositivos inscritos en el modo de perfil de trabajo en dispositivos propiedad de la empresa. Use Knox Service Plugin (KSP) para aplicar restricciones de Samsung a estos dispositivos. Para obtener más información, consulte la documentación de Samsung.

Se recomienda usar Samsung Knox 3.4 o una versión posterior para aprovechar las funciones de administración más recientes de Samsung Knox.

- **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa:** Permite configurar los parámetros de la directiva de restricciones para dispositivos totalmente administrados con perfiles de trabajo. Si esta configuración está **activada**, seleccione una de estas configuraciones:
  - **Perfil de trabajo:** Las configuraciones de restricciones que defina se aplicarán únicamente al perfil de trabajo del dispositivo.

- **Dispositivo administrado:** Los parámetros de restricciones que configure se aplicarán únicamente al dispositivo.

Si está **desactivada**, las configuraciones de credenciales que indique se aplicarán al dispositivo, con la excepción de aquellas que se aplican explícitamente al perfil de trabajo. Está **desactivado** de forma predeterminada.

Cuando **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa** está desactivado, configure estos parámetros:

- **Seguridad**
  - **Permitir administración de cuentas:** Permite que se agreguen cuentas a perfiles de trabajo y dispositivos administrados. Está **desactivado** de forma predeterminada.
  - **Permitir copiar y pegar contenido entre perfiles:** Si está **activado**, los usuarios pueden copiar y pegar contenido entre aplicaciones del perfil de Android Enterprise y aplicaciones del área personal. Está **desactivado** de forma predeterminada.
  - **Permitir capturas de pantalla:** Permite a los usuarios grabar o tomar una captura de la pantalla del dispositivo. Está **desactivado** de forma predeterminada.
  - **Permitir el uso de la cámara:** Permite a los usuarios tomar fotos y hacer vídeos con la cámara del dispositivo. Está **desactivado** de forma predeterminada.
  - **Permitir configuración VPN:** Permite a los usuarios crear configuraciones VPN. Para dispositivos de perfil de trabajo con Android 6 y versiones posteriores y para dispositivos totalmente administrados. De forma predeterminada, está **activado**.
  - **Permitir servicio de copia de seguridad:** Permite que los usuarios hagan copias de seguridad de los datos de aplicaciones y datos del sistema presentes en sus dispositivos. De forma predeterminada, está **activado**.
  - **Permitir NFC:** Permite que los usuarios envíen páginas web, fotos, vídeos y otro contenido desde sus dispositivos a otro dispositivo a través de NFC. Para MDM 4.0 y versiones posteriores. De forma predeterminada, está **activado**.
  - **Permitir configuración de proveedor de ubicación:** Permite a los usuarios activar el GPS en sus dispositivos. Para la API 28 de Android y versiones posteriores. De forma predeterminada, está **activado**.
  - **Permitir compartir ubicaciones:** En el caso de perfiles administrados, el propietario del dispositivo puede modificar esta configuración. Está **desactivado** de forma predeterminada.

    > **Sugerencia:**
    >
    > En XenMobile, puede crear directivas de localización geográfica para aplicar límites

> geográficos. Consulte Directiva de ubicación.

- **Permitir que el usuario configure las credenciales de usuario:** Especifique si los usuarios pueden configurar credenciales en el almacén de claves administrado. De forma predeterminada, está **activado**.
- **Permitir impresión:** Si está **activado**, la configuración permite a los usuarios imprimir contenido en cualquier impresora accesible desde el dispositivo del usuario. Está **desactivado** de forma predeterminada. Disponible a partir de Android 9.
- **Permitir depuración por USB:** De forma predeterminada, está **desactivado**.

- **Aplicaciones**
  - **Habilitar aplicaciones del sistema:** Permite a los usuarios ejecutar aplicaciones de dispositivos preinstaladas. Está **desactivado** de forma predeterminada. Para habilitar aplicaciones concretas, haga clic en **Agregar** en la tabla **Lista de aplicaciones del sistema**.
    - **Lista de aplicaciones del sistema:** Una lista de las aplicaciones del sistema que quiera habilitar en el dispositivo. **Active** la configuración **Habilitar aplicaciones del sistema** y agregue el nombre del paquete de la aplicación. Para buscar el nombre del paquete de una aplicación del sistema, puede usar Android Debug Bridge (`adb`) para llamar al comando del administrador de paquetes de Android (`pm`). Por ejemplo, `adb shell "pm list packages -f name"`, donde "name" forma parte del nombre del paquete. Para obtener más información, consulte https://developer.android.com/studio/command-line/adb. En dispositivos Android Enterprise, puede restringir los permisos de las aplicaciones mediante la directiva Permisos de aplicaciones Android Enterprise.
  - **Inhabilitar aplicaciones:** Bloquea la ejecución de una lista especificada de aplicaciones en dispositivos. Está **desactivado** de forma predeterminada. Para inhabilitar una aplicación instalada, **active** la configuración y haga clic en **Agregar** en la tabla **Lista de aplicaciones**.
    - **Lista de aplicaciones:** Una lista de las aplicaciones que quiera bloquear. **Active** el parámetro **Inhabilitar aplicaciones** y agregue la aplicación. Escriba el nombre del paquete de la aplicación. Cambiar e implementar una lista de aplicaciones sobrescribe la lista anterior de las aplicaciones. Por ejemplo: Si inhabilita com.ejemplo1 y com.ejemplo2 y, más adelante, cambia la lista a com.ejemplo1 y com.ejemplo3, XenMobile habilita com.ejemplo.2.
  - **Habilitar verificación de la aplicación.** Permite al sistema operativo examinar aplicaciones para detectar comportamiento malintencionado. De forma predeterminada, está **activado**.
  - **Habilitar aplicaciones de Google:** Permite que los usuarios descarguen aplicaciones desde Servicios de Google para Móviles en el dispositivo. De forma predeterminada, está **activado**.

  - **Permitir aplicaciones que no son de Google Play:** Permite la instalación de aplicaciones desde tiendas que no sean Google Play. Está **desactivado** de forma predeterminada.
  - **Permitir al usuario controlar los parámetros de la aplicación:** Permite a los usuarios desinstalar aplicaciones, inhabilitarlas, borrar la memoria caché y los datos, forzar la detención de cualquier aplicación y borrar los valores predeterminados. Los usuarios realizan estas acciones desde la aplicación Configuración. De forma predeterminada, está **desactivado**.
  - **Permitir la desinstalación de aplicaciones:** Permite a los usuarios desinstalar aplicaciones desde Google Play Store administrado. Está **desactivado** de forma predeterminada. Para mostrar este parámetro, habilite la propiedad de servidor `afw.restriction.policy.v2`. Para obtener información sobre propiedades de servidor, consulte Propiedades de servidor.

- **Perfil de trabajo BYOD**

  - **Permitir widgets de la aplicación de perfil de trabajo en la pantalla de inicio:** Si se **activa**, los usuarios pueden colocar widgets de la aplicación de perfil de trabajo en la pantalla de inicio del dispositivo. Si esta configuración está **desactivada**, los usuarios no pueden colocar widgets de la aplicación de perfil de trabajo en la pantalla de inicio del dispositivo. Está **desactivado** de forma predeterminada.
    * **Aplicaciones con widgets permitidos:** Una lista de las aplicaciones que quiere permitir en la pantalla de inicio. **Active** la configuración **Permite widgets de la aplicación de perfil de trabajo en la pantalla de inicio** y agregue la aplicación. Haga clic en **Agregar** y seleccione, de la lista, la aplicación cuyos widgets quiere permitir en la pantalla de inicio. Haga clic en **Guardar**. Repita este proceso para permitir más widgets de aplicación.
  - **Permitir contactos del perfil de trabajo en los contactos del dispositivo:** Muestra los contactos del perfil de Android Enterprise administrado en el perfil principal para las llamadas entrantes (Android 7.0 y versiones posteriores). Está **desactivado** de forma predeterminada.

- **Solo dispositivo totalmente administrado**

  - **Permitir incorporación de usuarios:** Permite a los usuarios agregar nuevos usuarios a un dispositivo. De forma predeterminada, está **activado**.
  - **Permitir itinerancia de datos:** Permite que los usuarios usen su conexión de datos móviles durante la itinerancia. Está desactivado de forma predeterminada, lo que inhabilita la itinerancia en los dispositivos de los usuarios. Está **desactivado** de forma predeterminada.
  - **Permitir SMS:** Permite a los usuarios enviar y recibir mensajes SMS. Está **desactivado** de forma predeterminada.
  - **Permitir el uso de la barra de estado:** Si se **activa**, esta configuración habilita la barra de

estado en dispositivos administrados y dispositivos dedicados (también conocidos como dispositivos COSU). Esta configuración inhabilita las notificaciones, los parámetros rápidos y otras capas de pantalla que permiten salir del modo de pantalla completa. Los usuarios pueden ir a la configuración del sistema y ver las notificaciones. Para Android 6.0 y posterior. Está **desactivado** de forma predeterminada.

- **Permitir Bluetooth:** Permite a los usuarios usar Bluetooth. De forma predeterminada, está **activado**.
  - **Permitir la opción Compartir Bluetooth:** Si no está activado, los usuarios no pueden establecer la opción Compartir Bluetooth saliente en sus dispositivos. Está activado de forma predeterminada. Para mostrar este parámetro, habilite la propiedad de servidor `afw.restriction.policy.v2`. Para obtener información sobre propiedades de servidor, consulte Propiedades de servidor.
- **Permitir configuración de fecha y hora:** Permite a los usuarios cambiar la fecha y la hora en sus dispositivos. De forma predeterminada, está **activado**.
- **Restablecer valores de fábrica:** Permite que los usuarios restablezcan sus dispositivos a los valores de fábrica. De forma predeterminada, está **activado**.
- **Mantener encendida la pantalla del dispositivo:** Si se **activa**, la pantalla del dispositivo permanece encendida mientras el dispositivo está conectado. Está **desactivado** de forma predeterminada.
- **Permitir almacenamiento USB masivo:** Permite la transferencia de archivos de datos de gran tamaño entre los dispositivos de los usuarios y un equipo a través de una conexión USB. De forma predeterminada, está **activado**.
- **Permitir micrófono:** Permite que los usuarios usen el micrófono en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir anclaje a red:** Permite a los usuarios configurar zonas hotspot portátiles y anclar datos. Está **desactivado** de forma predeterminada.
- **Impedir que Keyguard bloquee el dispositivo:** Si se **activa**, esta configuración desactiva Keyguard en la pantalla de bloqueo en dispositivos administrados y dispositivos dedicados (también conocidos como dispositivos COSU). Está **desactivado** de forma predeterminada.
- **Permitir cambios de Wi-Fi:** Si está **activado**, los usuarios pueden activar o desactivar redes Wi-Fi y conectarse a ellas. De forma predeterminada, está **activado**.
- **Permitir transferencia de archivos:** Permite transferencias de archivos a través de USB. Está **desactivado** de forma predeterminada.

- **Samsung**
  - **Habilitar almacén de claves TIMA:** El almacén de claves TIMA ofrece almacenamiento seguro de claves basado en TrustZone para las claves simétricas. Los pares de claves de RSA y los certificados se enrutan al proveedor de almacenamiento de claves predeterminado para su almacenamiento. Está **desactivado** de forma predeterminada.

- **Permitir uso compartido de lista:** Permite que los usuarios compartan contenido entre las aplicaciones en la lista de Compartir a través de. De forma predeterminada, está **activado**.
- **Habilitar registros de auditoría:** Permite la creación de registros de auditoría de eventos para el análisis forense de un dispositivo. Está **desactivado** de forma predeterminada.

• **Samsung: Solo dispositivo totalmente administrado**

- **Habilitar verificación de arranque seguro ODE:** Permite usar la verificación ODE de arranque de confianza para establecer una cadena de confianza desde el cargador de arranque hasta la imagen del sistema. De forma predeterminada, está **activado**.
- **Permitir solo llamadas de emergencia:** Permite a los usuarios habilitar el modo Solo llamadas de emergencia en sus dispositivos. Está **desactivado** de forma predeterminada.
- **Permitir recuperación de firmware:** Permite que los usuarios recuperen el firmware en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir cifrado rápido:** Permite el cifrado únicamente del espacio de memoria utilizado. Este cifrado es diferente del cifrado de disco completo, que cifra todos los datos. Estos datos incluyen parámetros, datos de aplicaciones, archivos y aplicaciones descargados, archivos multimedia y más. De forma predeterminada, está **activado**.
- **Modo Common Criteria:** Coloca el dispositivo en el modo Common Criteria. La configuración de Common Criteria impone procesos estrictos de seguridad. De forma predeterminada, está **activado**.
- **Habilitar pancarta de arranque:** Muestra una mensaje o pancarta sobre el uso del sistema aprobado por el DoD cuando los dispositivos de los usuarios se reinician. Está **desactivado** de forma predeterminada.
- **Permitir cambios en los parámetros:** Permite que los usuarios cambien parámetros en sus dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Habilitar el uso de datos en segundo plano:** Permite que las aplicaciones sincronicen datos en segundo plano en dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Permitir portapapeles:** Permite que los usuarios copien datos al portapapeles de sus dispositivos.
  * **Permitir el uso compartido del portapapeles:** Permite que los usuarios compartan el contenido del portapapeles entre sus dispositivos y un equipo (MDM 4.0 y versiones posteriores).
- **Permitir tecla Inicio:** Permite que los usuarios usen la tecla **Inicio** en sus dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Permitir ubicaciones falsas:** Permite que los usuarios indiquen una ubicación de GPS falsa. Para dispositivos totalmente administrados. Está **desactivado** de forma predeterminada.
- **NFC:** Permite que los usuarios usen la transmisión de datos en proximidad o NFC (Near

Field Communication) en sus dispositivos totalmente administrados (MDM 3.0 y versiones posteriores). De forma predeterminada, está **activado**.

- **Permitir apagado:** Permite que los usuarios apaguen sus dispositivos totalmente administrados (MDM 3.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir Wi-Fi Direct:** Permite a los usuarios conectarse directamente a otro dispositivo a través de su conexión Wi-Fi. De forma predeterminada, está **activado**. Si está **activado**, debe habilitar la configuración **Permitir cambios de Wi-Fi**.
- **Permitir tarjetas SD:** Permite que los usuarios usen tarjetas SD, si están disponibles, en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir almacenamiento de hosts de USB:** Permite que los dispositivos de los usuarios actúen como host de USB cuando un dispositivo USB se conecta a ellos. Los dispositivos de los usuarios suministran energía al dispositivo USB. De forma predeterminada, está **activado**.
- **Permitir marcador por voz:** Permite que los usuarios usen el marcador por voz en sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir S Beam:** Permite que los usuarios compartan contenido con otras personas a través de NFC y Wi-Fi Direct (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir S Voice:** Permite que los usuarios usen el asistente personal inteligente y el explorador de conocimientos en sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir anclaje a red USB:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión USB. Está **desactivado** de forma predeterminada. Si está **activado**, la opción **Permitir anclaje a red** también debe estar **activada**.
- **Permitir anclaje a red Bluetooth:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión Bluetooth. Está **desactivado** de forma predeterminada. Si está **activado**, la opción **Permitir anclaje a red** también debe estar **activada**.
  - **Permitir la opción Compartir Bluetooth:** Si no está activado, los usuarios no pueden establecer la opción Compartir Bluetooth saliente en sus dispositivos. Está activado de forma predeterminada. Para mostrar este parámetro, habilite la propiedad de servidor `afw.restriction.policy.v2`. Para obtener información sobre propiedades de servidor, consulte Propiedades de servidor.
- **Permitir anclaje a red Wi-Fi:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión Wi-Fi. Está **desactivado** de forma predeterminada. Si está **activado**, la opción **Permitir anclaje a red** también debe estar **activada**.
- **Permitir MMS entrantes:** Permite que los usuarios reciban mensajes MMS. Está **desacti-**

vado de forma predeterminada. Si está **activado**, debe activar la configuración **Permitir SMS**.

- **Permitir MMS salientes:** Permite que los usuarios envíen mensajes MMS. Está **desactivado** de forma predeterminada. Si está **activado**, debe activar la configuración **Permitir SMS**.
- **Permitir SMS entrantes:** Permite que los usuarios reciban mensajes SMS. Está **desactivado** de forma predeterminada. Si está **activado**, debe activar la configuración **Permitir SMS**.
- **Permitir SMS salientes:** Permite que los usuarios envíen mensajes SMS. Está **desactivado** de forma predeterminada. Si está **activado**, debe activar la configuración **Permitir SMS**.
- **Configurar redes móviles:** Permite a los usuarios utilizar su conexión de datos móviles. Está **desactivado** de forma predeterminada.
- **Límite diario (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada día. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
- **Límite semanal (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada semana. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
- **Límite mensual (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada mes. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
- **Permitir solo conexiones VPN seguras:** Permite que los usuarios usen solamente conexiones seguras (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir grabación de audio:** Permite que los usuarios graben sonido con sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**. Si está **activado**, debe activar la configuración **Permitir micrófono**.
- **Permitir grabación de vídeo:** Permite que los usuarios graben vídeo con sus dispositivos (MDM 4.0 y versiones posteriores). Está **desactivado** de forma predeterminada. Si está **activado**, debe activar la configuración **Permitir el uso de la cámara**.
- **Permitir mensajes push en itinerancia:** Permite a los usuarios utilizar datos móviles para enviar mensajes push. Está **desactivado** de forma predeterminada. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.
- **Permitir sincronización automática en itinerancia:** Permite a los usuarios utilizar datos móviles para la sincronización. Está **desactivado** de forma predeterminada. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.
- **Permitir llamadas de voz en itinerancia:** Permite a los usuarios utilizar datos móviles para llamadas de voz. Está **desactivado** de forma predeterminada. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.

- **Samsung: Contenedor Knox/Dispositivo totalmente administrado**
  - **Habilitar comprobación de revocación:** Habilita la comprobación de certificados revocados. Está **desactivado** de forma predeterminada.
- **Samsung: Solo contenedor Knox**
  - **Mover aplicaciones al contenedor:** Permite que los usuarios muevan aplicaciones entre el contenedor Knox y el área personal de sus dispositivos. De forma predeterminada, está **activado**.
  - **Aplicar autenticación de varios factores:** Los usuarios deben utilizar una huella digital y otro método de autenticación, como una contraseña o un PIN, para abrir sus dispositivos. De forma predeterminada, está **activado**.
  - **Aplicar autenticación para contenedor:** Utilice un método de autenticación diferente del método utilizado para desbloquear el dispositivo y, así, abrir el contenedor Knox. De forma predeterminada, está **activado**.
  - **Habilitar teclado seguro:** Obliga a los usuarios a usar un teclado seguro dentro del contenedor Knox. De forma predeterminada, está **activado**.
- **Samsung: DeX**
  - **Habilitar Samsung DeX:** Permite que los dispositivos con Knox compatibles funcionen en el modo Samsung DeX. Requiere Samsung Knox 3.1 (versión mínima). De forma predeterminada, está **activado**. Para obtener información sobre los requisitos de dispositivos Samsung DeX y la configuración de Samsung DeX, consulte la documentación para desarrolladores de Samsung.
    * **Permitir Ethernet solo en modo DeX:** Habilita el uso de Ethernet en el modo Samsung DeX. Los datos móviles, Wi-Fi y de anclaje a red (Wi-Fi, Bluetooth y USB) están restringidos en el modo DeX. De forma predeterminada, ningún elemento está seleccionado.
    * **Cargar imagen del logo de DeX:** Seleccione esta configuración para especificar la imagen PNG que se usará como icono para Samsung DeX.
    * **Tiempo de espera de la pantalla DeX (segundos):** Especifique la cantidad de tiempo de inactividad, en segundos, después del cual la pantalla DeX se apaga. Para inhabilitar el tiempo de espera, escriba **0**. El valor predeterminado es **1200** segundos (20 minutos).
    * **Agregar acceso directo a la aplicación en Samsung DeX:** Especifique un nombre de paquete de aplicación para agregar un acceso directo de la aplicación a DeX. Para buscar el nombre del paquete de una aplicación, vaya a Google Play y seleccione la aplicación. La URL incluye el nombre del paquete: `https://play.google.com/store/apps/details?id=<package.name><!--NeedCopy-->`.
    * **Quitar acceso directo a la aplicación en Samsung DeX:** Especifique un nombre de paquete de aplicación para eliminar un acceso directo que hubiera en DeX. Vaya a

Google Play para buscar nombres de paquetes de aplicación.

* **Paquetes de aplicaciones que inhabilitar en Samsung DeX:** Especifique una lista separada por comas de los paquetes de aplicación que quiere bloquear en el modo Samsung DeX. Por ejemplo: `"com.android.chrome", "com.google.android.gm"<!--NeedCopy-->`.

Si **Aplicar a dispositivos totalmente administrados con un perfil de trabajo** está activado y **Para dispositivos totalmente administrados con perfil de trabajo, la directiva se aplica a** está establecido en **Perfil de trabajo**, configure estos parámetros:

- **Seguridad**
  - **Permitir administración de cuentas:** Permite que se agreguen cuentas a perfiles de trabajo y dispositivos administrados. Está **desactivado** de forma predeterminada.
  - **Permitir copiar y pegar contenido entre perfiles:** Si está **activado**, los usuarios pueden copiar y pegar contenido entre aplicaciones del perfil de Android Enterprise y aplicaciones del área personal. Está **desactivado** de forma predeterminada.
  - **Permitir capturas de pantalla:** Permite a los usuarios grabar o tomar una captura de la pantalla del dispositivo. Está **desactivado** de forma predeterminada.
  - **Permitir el uso de la cámara:** Permite a los usuarios tomar fotos y hacer vídeos con la cámara del dispositivo. Está **desactivado** de forma predeterminada.
  - **Permitir configuración de proveedor de ubicación:** Permite a los usuarios activar el GPS en sus dispositivos. Para la API 28 de Android y versiones posteriores. De forma predeterminada, está **activado**.
  - **Permitir compartir ubicaciones:** En el caso de perfiles administrados, el propietario del dispositivo puede modificar esta configuración. Está **desactivado** de forma predeterminada.

    > **Sugerencia:**
    >
    > En XenMobile, puede crear directivas de localización geográfica para aplicar límites geográficos. Consulte Directiva de ubicación.

  - **Permitir que el usuario configure las credenciales de usuario:** Especifique si los usuarios pueden configurar credenciales en el almacén de claves administrado. De forma predeterminada, está **activado**.
  - **Permitir impresión:** Si está **activado**, la configuración permite a los usuarios imprimir contenido en cualquier impresora accesible desde el dispositivo del usuario. Está **desactivado** de forma predeterminada. Disponible a partir de Android 9.
- **Aplicaciones**

- **Habilitar aplicaciones del sistema:** Permite a los usuarios ejecutar aplicaciones de dispositivos preinstaladas. Está **desactivado** de forma predeterminada. Para habilitar aplicaciones concretas, haga clic en **Agregar** en la tabla **Lista de aplicaciones del sistema**.
  * **Lista de aplicaciones del sistema:** Una lista de las aplicaciones del sistema que quiera habilitar en el dispositivo. **Active** la configuración **Habilitar aplicaciones del sistema** y agregue el nombre del paquete de la aplicación. Para buscar el nombre del paquete de una aplicación del sistema, puede usar Android Debug Bridge (`adb`) para llamar al comando del administrador de paquetes de Android (`pm`). Por ejemplo, `adb shell "pm list packages -f name"`, donde "name" forma parte del nombre del paquete. Para obtener más información, consulte https://developer.android.com/studio/command-line/adb. En dispositivos Android Enterprise, puede restringir los permisos de las aplicaciones mediante la directiva Permisos de aplicaciones Android Enterprise.
- **Inhabilitar aplicaciones:** Bloquea la ejecución de una lista especificada de aplicaciones en dispositivos. Está **desactivado** de forma predeterminada. Para inhabilitar una aplicación instalada, **active** la configuración y haga clic en **Agregar** en la tabla **Lista de aplicaciones**.
  * **Lista de aplicaciones:** Una lista de las aplicaciones que quiera bloquear. **Active** el parámetro **Inhabilitar aplicaciones** y agregue la aplicación. Escriba el nombre del paquete de la aplicación. Cambiar e implementar una lista de aplicaciones sobrescribe la lista anterior de las aplicaciones. Por ejemplo: Si inhabilita com.ejemplo1 y com.ejemplo2 y, más adelante, cambia la lista a com.ejemplo1 y com.ejemplo3, XenMobile habilita com.ejemplo.2.
- **Habilitar verificación de la aplicación.** Permite al sistema operativo examinar aplicaciones para detectar comportamiento malintencionado. De forma predeterminada, está **activado**.
- **Habilitar aplicaciones de Google:** Permite que los usuarios descarguen aplicaciones desde Servicios de Google para Móviles en el dispositivo. De forma predeterminada, está **activado**.
- **Permitir aplicaciones que no son de Google Play:** Permite la instalación de aplicaciones desde tiendas que no sean Google Play. Está **desactivado** de forma predeterminada.
- **Permitir al usuario controlar los parámetros de la aplicación:** Permite a los usuarios desinstalar aplicaciones, inhabilitarlas, borrar la memoria caché y los datos, forzar la detención de cualquier aplicación y borrar los valores predeterminados. Los usuarios realizan estas acciones desde la aplicación Configuración. De forma predeterminada, está **desactivado**.
- **Permitir la desinstalación de aplicaciones:** Permite a los usuarios desinstalar aplicaciones desde Google Play Store administrado. Está **desactivado** de forma predeterminada. Para mostrar este parámetro, habilite la propiedad de servidor `afw`.

`restriction.policy.v2`. Para obtener información sobre propiedades de servidor, consulte Propiedades de servidor.

- **Perfil de trabajo BYOD**
  - **Permitir widgets de la aplicación de perfil de trabajo en la pantalla de inicio:** Si se **activa**, los usuarios pueden colocar widgets de la aplicación de perfil de trabajo en la pantalla de inicio del dispositivo. Si esta configuración está **desactivada**, los usuarios no pueden colocar widgets de la aplicación de perfil de trabajo en la pantalla de inicio del dispositivo. Está **desactivado** de forma predeterminada.
    - **Aplicaciones con widgets permitidos:** Una lista de las aplicaciones que quiere permitir en la pantalla de inicio. **Active** la configuración **Permite widgets de la aplicación de perfil de trabajo en la pantalla de inicio** y agregue la aplicación. Haga clic en **Agregar** y seleccione, de la lista, la aplicación cuyos widgets quiere permitir en la pantalla de inicio. Haga clic en **Guardar**. Repita este proceso para permitir más widgets de aplicación.
  - **Permitir contactos del perfil de trabajo en los contactos del dispositivo:** Muestra los contactos del perfil de Android Enterprise administrado en el perfil principal para las llamadas entrantes (Android 7.0 y versiones posteriores). Está **desactivado** de forma predeterminada.
- **Samsung**
  - **Habilitar almacén de claves TIMA:** El almacén de claves TIMA ofrece almacenamiento seguro de claves basado en TrustZone para las claves simétricas. Los pares de claves de RSA y los certificados se enrutan al proveedor de almacenamiento de claves predeterminado para su almacenamiento. Está **desactivado** de forma predeterminada.
  - **Permitir uso compartido de lista:** Permite que los usuarios compartan contenido entre las aplicaciones en la lista de Compartir a través de. De forma predeterminada, está **activado**.
  - **Habilitar registros de auditoría:** Permite la creación de registros de auditoría de eventos para el análisis forense de un dispositivo. Está **desactivado** de forma predeterminada.
- **Samsung: Contenedor Knox/Dispositivo totalmente administrado**
  - **Habilitar comprobación de revocación:** Habilita la comprobación de certificados revocados. Está **desactivado** de forma predeterminada.
- **Samsung: Solo contenedor Knox**
  - **Mover aplicaciones al contenedor:** Permite que los usuarios muevan aplicaciones entre el contenedor Knox y el área personal de sus dispositivos. De forma predeterminada, está **activado**.
  - **Aplicar autenticación de varios factores:** Los usuarios deben utilizar una huella digital y otro método de autenticación, como una contraseña o un PIN, para abrir sus dispositivos.

De forma predeterminada, está **activado**.
- **Aplicar autenticación para contenedor:** Utilice un método de autenticación diferente del método utilizado para desbloquear el dispositivo y, así, abrir el contenedor Knox. De forma predeterminada, está **activado**.
- **Habilitar teclado seguro:** Obliga a los usuarios a usar un teclado seguro dentro del contenedor Knox. De forma predeterminada, está **activado**.

Si **Aplicar a dispositivos totalmente administrados con un perfil de trabajo** está activado y **Para dispositivos totalmente administrados con perfil de trabajo, la directiva se aplica a** está establecido en **Dispositivo administrado**, configure estos parámetros:

- **Seguridad**
  - **Permitir administración de cuentas:** Permite que se agreguen cuentas a perfiles de trabajo y dispositivos administrados. Está **desactivado** de forma predeterminada.
  - **Permitir copiar y pegar contenido entre perfiles:** Si está **activado**, los usuarios pueden copiar y pegar contenido entre aplicaciones del perfil de Android Enterprise y aplicaciones del área personal. Está **desactivado** de forma predeterminada.
  - **Permitir capturas de pantalla:** Permite a los usuarios grabar o tomar una captura de la pantalla del dispositivo. Está **desactivado** de forma predeterminada.
  - **Permitir el uso de la cámara:** Permite a los usuarios tomar fotos y hacer vídeos con la cámara del dispositivo. Está **desactivado** de forma predeterminada.
  - **Permitir configuración VPN:** Permite a los usuarios crear configuraciones VPN. Para dispositivos de perfil de trabajo con Android 6 y versiones posteriores y para dispositivos totalmente administrados. De forma predeterminada, está **activado**.
  - **Permitir servicio de copia de seguridad:** Permite que los usuarios hagan copias de seguridad de los datos de aplicaciones y datos del sistema presentes en sus dispositivos. De forma predeterminada, está **activado**.
  - **Permitir NFC:** Permite que los usuarios envíen páginas web, fotos, vídeos y otro contenido desde sus dispositivos a otro dispositivo a través de NFC. Para MDM 4.0 y versiones posteriores. De forma predeterminada, está **activado**.
  - **Permitir configuración de proveedor de ubicación:** Permite a los usuarios activar el GPS en sus dispositivos. Para la API 28 de Android y versiones posteriores. De forma predeterminada, está **activado**.
  - **Permitir compartir ubicaciones:** En el caso de perfiles administrados, el propietario del dispositivo puede modificar esta configuración. Está **desactivado** de forma predeterminada.

> **Sugerencia:**
>
> En XenMobile, puede crear directivas de localización geográfica para aplicar límites geográficos. Consulte Directiva de ubicación.

- **Permitir que el usuario configure las credenciales de usuario:** Especifique si los usuarios pueden configurar credenciales en el almacén de claves administrado. De forma predeterminada, está **activado**.
- **Permitir impresión:** Si está **activado**, la configuración permite a los usuarios imprimir contenido en cualquier impresora accesible desde el dispositivo del usuario. Está **desactivado** de forma predeterminada. Disponible a partir de Android 9.
- **Permitir depuración por USB:** De forma predeterminada, está **desactivado**.

- **Aplicaciones**
  - **Habilitar aplicaciones del sistema:** Permite a los usuarios ejecutar aplicaciones de dispositivos preinstaladas. Está **desactivado** de forma predeterminada. Para habilitar aplicaciones concretas, haga clic en **Agregar** en la tabla **Lista de aplicaciones del sistema**.
    - **Lista de aplicaciones del sistema:** Una lista de las aplicaciones del sistema que quiera habilitar en el dispositivo. **Active** la configuración **Habilitar aplicaciones del sistema** y agregue el nombre del paquete de la aplicación. Para buscar el nombre del paquete de una aplicación del sistema, puede usar Android Debug Bridge (`adb`) para llamar al comando del administrador de paquetes de Android (`pm`). Por ejemplo, `adb shell "pm list packages -f name"`, donde "name" forma parte del nombre del paquete. Para obtener más información, consulte https://developer.android.com/studio/command-line/adb. En dispositivos Android Enterprise, puede restringir los permisos de las aplicaciones mediante la directiva Permisos de aplicaciones Android Enterprise.
  - **Inhabilitar aplicaciones:** Bloquea la ejecución de una lista especificada de aplicaciones en dispositivos. Está **desactivado** de forma predeterminada. Para inhabilitar una aplicación instalada, **active** la configuración y haga clic en **Agregar** en la tabla **Lista de aplicaciones**.
    - **Lista de aplicaciones:** Una lista de las aplicaciones que quiera bloquear. **Active** el parámetro **Inhabilitar aplicaciones** y agregue la aplicación. Escriba el nombre del paquete de la aplicación. Cambiar e implementar una lista de aplicaciones sobrescribe la lista anterior de las aplicaciones. Por ejemplo: Si inhabilita com.ejemplo1 y com.ejemplo2 y, más adelante, cambia la lista a com.ejemplo1 y com.ejemplo3, XenMobile habilita com.ejemplo.2.
  - **Habilitar verificación de la aplicación.** Permite al sistema operativo examinar aplicaciones para detectar comportamiento malintencionado. De forma predeterminada, está **activado**.

  - **Habilitar aplicaciones de Google:** Permite que los usuarios descarguen aplicaciones desde Servicios de Google para Móviles en el dispositivo. De forma predeterminada, está **activado**.
  - **Permitir aplicaciones que no son de Google Play:** Permite la instalación de aplicaciones desde tiendas que no sean Google Play. Está **desactivado** de forma predeterminada.
  - **Permitir al usuario controlar los parámetros de la aplicación:** Permite a los usuarios desinstalar aplicaciones, inhabilitarlas, borrar la memoria caché y los datos, forzar la detención de cualquier aplicación y borrar los valores predeterminados. Los usuarios realizan estas acciones desde la aplicación Configuración. De forma predeterminada, está **desactivado**.
  - **Permitir la desinstalación de aplicaciones:** Permite a los usuarios desinstalar aplicaciones desde Google Play Store administrado. Está **desactivado** de forma predeterminada. Para mostrar este parámetro, habilite la propiedad de servidor `afw.restriction.policy.v2`. Para obtener información sobre propiedades de servidor, consulte Propiedades de servidor.

- **Solo dispositivo totalmente administrado**
  - **Permitir incorporación de usuarios:** Permite a los usuarios agregar nuevos usuarios a un dispositivo. De forma predeterminada, está **activado**.
  - **Permitir itinerancia de datos:** Permite que los usuarios usen su conexión de datos móviles durante la itinerancia. Está desactivado de forma predeterminada, lo que inhabilita la itinerancia en los dispositivos de los usuarios. Está **desactivado** de forma predeterminada.
  - **Permitir SMS:** Permite a los usuarios enviar y recibir mensajes SMS. Está **desactivado** de forma predeterminada.
  - **Permitir el uso de la barra de estado:** Si se **activa**, esta configuración habilita la barra de estado en dispositivos administrados y dispositivos dedicados (también conocidos como dispositivos COSU). Esta configuración inhabilita las notificaciones, los parámetros rápidos y otras capas de pantalla que permiten salir del modo de pantalla completa. Los usuarios pueden ir a la configuración del sistema y ver las notificaciones. Para Android 6.0 y posterior. Está **desactivado** de forma predeterminada.
  - **Permitir Bluetooth:** Permite a los usuarios usar Bluetooth. De forma predeterminada, está **activado**.
    * **Permitir la opción Compartir Bluetooth:** Si no está activado, los usuarios no pueden establecer la opción Compartir Bluetooth saliente en sus dispositivos. Está activado de forma predeterminada. Para mostrar este parámetro, habilite la propiedad de servidor `afw.restriction.policy.v2`. Para obtener información sobre propiedades de servidor, consulte Propiedades de servidor.
  - **Permitir configuración de fecha y hora:** Permite a los usuarios cambiar la fecha y la hora en sus dispositivos. De forma predeterminada, está **activado**.

- **Restablecer valores de fábrica:** Permite que los usuarios restablezcan sus dispositivos a los valores de fábrica. De forma predeterminada, está **activado**.
- **Mantener encendida la pantalla del dispositivo:** Si se **activa**, la pantalla del dispositivo permanece encendida mientras el dispositivo está conectado. Está **desactivado** de forma predeterminada.
- **Permitir almacenamiento USB masivo:** Permite la transferencia de archivos de datos de gran tamaño entre los dispositivos de los usuarios y un equipo a través de una conexión USB. De forma predeterminada, está **activado**.
- **Permitir micrófono:** Permite que los usuarios usen el micrófono en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir anclaje a red:** Permite a los usuarios configurar zonas hotspot portátiles y anclar datos. Está **desactivado** de forma predeterminada. Cuando esta configuración está activa, están disponibles estas opciones para los dispositivos Samsung:
- **Impedir que Keyguard bloquee el dispositivo:** Si se **activa**, esta configuración desactiva Keyguard en la pantalla de bloqueo en dispositivos administrados y dispositivos dedicados (también conocidos como dispositivos COSU). Está **desactivado** de forma predeterminada.
- **Permitir cambios de Wi-Fi:** Si está **activado**, los usuarios pueden activar o desactivar redes Wi-Fi y conectarse a ellas. De forma predeterminada, está **activado**.
- **Permitir transferencia de archivos:** Permite transferencias de archivos a través de USB. Está **desactivado** de forma predeterminada.

- **Samsung**
  - **Habilitar almacén de claves TIMA:** El almacén de claves TIMA ofrece almacenamiento seguro de claves basado en TrustZone para las claves simétricas. Los pares de claves de RSA y los certificados se enrutan al proveedor de almacenamiento de claves predeterminado para su almacenamiento. Está **desactivado** de forma predeterminada.
  - **Permitir uso compartido de lista:** Permite que los usuarios compartan contenido entre las aplicaciones en la lista de Compartir a través de. De forma predeterminada, está **activado**.
  - **Habilitar registros de auditoría:** Permite la creación de registros de auditoría de eventos para el análisis forense de un dispositivo. Está **desactivado** de forma predeterminada.
- **Samsung: Solo dispositivo totalmente administrado**
  - **Habilitar verificación de arranque seguro ODE:** Permite usar la verificación ODE de arranque de confianza para establecer una cadena de confianza desde el cargador de arranque hasta la imagen del sistema. De forma predeterminada, está **activado**.
  - **Permitir solo llamadas de emergencia:** Permite a los usuarios habilitar el modo Solo llamadas de emergencia en sus dispositivos. Está **desactivado** de forma predeterminada.
  - **Permitir recuperación de firmware:** Permite que los usuarios recuperen el firmware en

sus dispositivos. De forma predeterminada, está **activado**.

- **Permitir cifrado rápido:** Permite el cifrado únicamente del espacio de memoria utilizado. Este cifrado es diferente del cifrado de disco completo, que cifra todos los datos. Estos datos incluyen parámetros, datos de aplicaciones, archivos y aplicaciones descargados, archivos multimedia y más. De forma predeterminada, está **activado**.
- **Modo Common Criteria:** Coloca el dispositivo en el modo Common Criteria. La configuración de Common Criteria impone procesos estrictos de seguridad. De forma predeterminada, está **activado**.
- **Habilitar pancarta de arranque:** Muestra una mensaje o pancarta sobre el uso del sistema aprobado por el DoD cuando los dispositivos de los usuarios se reinician. Está **desactivado** de forma predeterminada.
- **Permitir cambios en los parámetros:** Permite que los usuarios cambien parámetros en sus dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Habilitar el uso de datos en segundo plano:** Permite que las aplicaciones sincronicen datos en segundo plano en dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Permitir portapapeles:** Permite que los usuarios copien datos al portapapeles de sus dispositivos. De forma predeterminada, está **activado**.
  * **Permitir el uso compartido del portapapeles:** Permite que los usuarios compartan el contenido del portapapeles entre sus dispositivos y un equipo (MDM 4.0 y versiones posteriores).
- **Permitir tecla Inicio:** Permite que los usuarios usen la tecla **Inicio** en sus dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Permitir ubicaciones falsas:** Permite que los usuarios indiquen una ubicación de GPS falsa. Para dispositivos totalmente administrados. Está **desactivado** de forma predeterminada.
- **NFC:** Permite que los usuarios usen la transmisión de datos en proximidad o NFC (Near Field Communication) en sus dispositivos totalmente administrados (MDM 3.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir apagado:** Permite que los usuarios apaguen sus dispositivos totalmente administrados (MDM 3.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir Wi-Fi Direct:** Permite a los usuarios conectarse directamente a otro dispositivo a través de su conexión Wi-Fi. De forma predeterminada, está **activado**. Si está **activado**, debe habilitar la configuración **Permitir cambios de Wi-Fi**.
- **Permitir tarjetas SD:** Permite que los usuarios usen tarjetas SD, si están disponibles, en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir almacenamiento de hosts de USB:** Permite que los dispositivos de los usuarios actúen como host de USB cuando un dispositivo USB se conecta a ellos. Los dispositivos de los usuarios suministran energía al dispositivo USB. De forma predeterminada, está

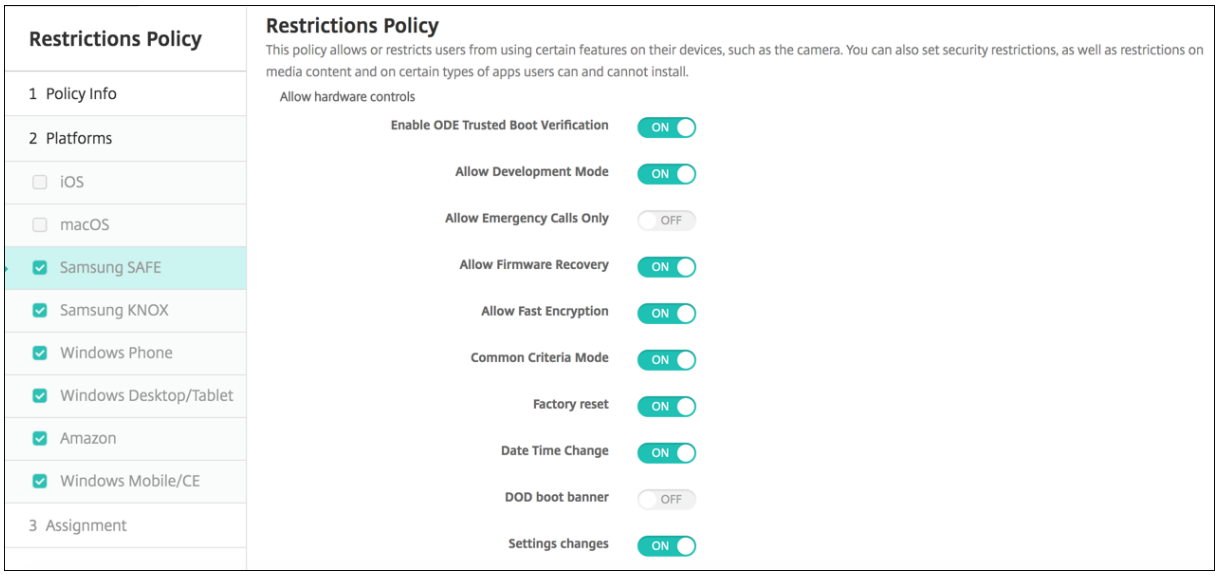
activado.

- **Permitir marcador por voz:** Permite que los usuarios usen el marcador por voz en sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir S Beam:** Permite que los usuarios compartan contenido con otras personas a través de NFC y Wi-Fi Direct (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir S Voice:** Permite que los usuarios usen el asistente personal inteligente y el explorador de conocimientos en sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir anclaje a red USB:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión USB. Está **desactivado** de forma predeterminada. Si está **activado**, la opción **Permitir anclaje a red** también debe estar **activada**.
- **Permitir anclaje a red Bluetooth:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión Bluetooth. Está **desactivado** de forma predeterminada. Si está **activado**, la opción **Permitir anclaje a red** también debe estar **activada**.
- **Permitir anclaje a red Wi-Fi:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión Wi-Fi. Está **desactivado** de forma predeterminada. Si está **activado**, la opción **Permitir anclaje a red** también debe estar **activada**.
- **Permitir MMS entrantes:** Permite que los usuarios reciban mensajes MMS. Está **desactivado** de forma predeterminada. Si está **activado**, debe activar la configuración **Permitir SMS**.
- **Permitir MMS salientes:** Permite que los usuarios envíen mensajes MMS. Está **desactivado** de forma predeterminada. Si está **activado**, debe activar la configuración **Permitir SMS**.
- **Permitir SMS entrantes:** Permite que los usuarios reciban mensajes SMS. Está **desactivado** de forma predeterminada. Si está **activado**, debe activar la configuración **Permitir SMS**.
- **Permitir SMS salientes:** Permite que los usuarios envíen mensajes SMS. Está **desactivado** de forma predeterminada. Si está **activado**, debe activar la configuración **Permitir SMS**.
- **Configurar redes móviles:** Permite a los usuarios utilizar su conexión de datos móviles. Está **desactivado** de forma predeterminada.
- **Límite diario (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada día. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
- **Límite semanal (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios

pueden usar cada semana. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
- **Límite mensual (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada mes. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
- **Permitir solo conexiones VPN seguras:** Permite que los usuarios usen solamente conexiones seguras (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir grabación de audio:** Permite que los usuarios graben sonido con sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**. Si está **activado**, debe activar la configuración **Permitir micrófono**.
- **Permitir grabación de vídeo:** Permite que los usuarios graben vídeo con sus dispositivos (MDM 4.0 y versiones posteriores). Está **desactivado** de forma predeterminada. Si está **activado**, debe activar la configuración **Permitir el uso de la cámara**.
- **Permitir mensajes push en itinerancia:** Permite a los usuarios utilizar datos móviles para enviar mensajes push. Está **desactivado** de forma predeterminada. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.
- **Permitir sincronización automática en itinerancia:** Permite a los usuarios utilizar datos móviles para la sincronización. Está **desactivado** de forma predeterminada. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.
- **Permitir llamadas de voz en itinerancia:** Permite a los usuarios utilizar datos móviles para llamadas de voz. Está **desactivado** de forma predeterminada. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.

- **Samsung: Contenedor Knox/Dispositivo totalmente administrado**
  - **Habilitar comprobación de revocación:** Habilita la comprobación de certificados revocados. Está **desactivado** de forma predeterminada.
- **Samsung: Solo contenedor Knox**
  - **Mover aplicaciones al contenedor:** Permite que los usuarios muevan aplicaciones entre el contenedor Knox y el área personal de sus dispositivos. De forma predeterminada, está **activado**.
  - **Aplicar autenticación de varios factores:** Los usuarios deben utilizar una huella digital y otro método de autenticación, como una contraseña o un PIN, para abrir sus dispositivos. De forma predeterminada, está **activado**.
  - **Aplicar autenticación para contenedor:** Utilice un método de autenticación diferente del método utilizado para desbloquear el dispositivo y, así, abrir el contenedor Knox. De forma predeterminada, está **activado**.
  - **Habilitar teclado seguro:** Obliga a los usuarios a usar un teclado seguro dentro del contenedor Knox. De forma predeterminada, está **activado**.

Parámetros de Samsung SAFE



Algunas opciones están disponibles únicamente en unas API de Mobile Device Management específicas de Samsung. Esas opciones están marcadas con la información de la versión correspondiente.

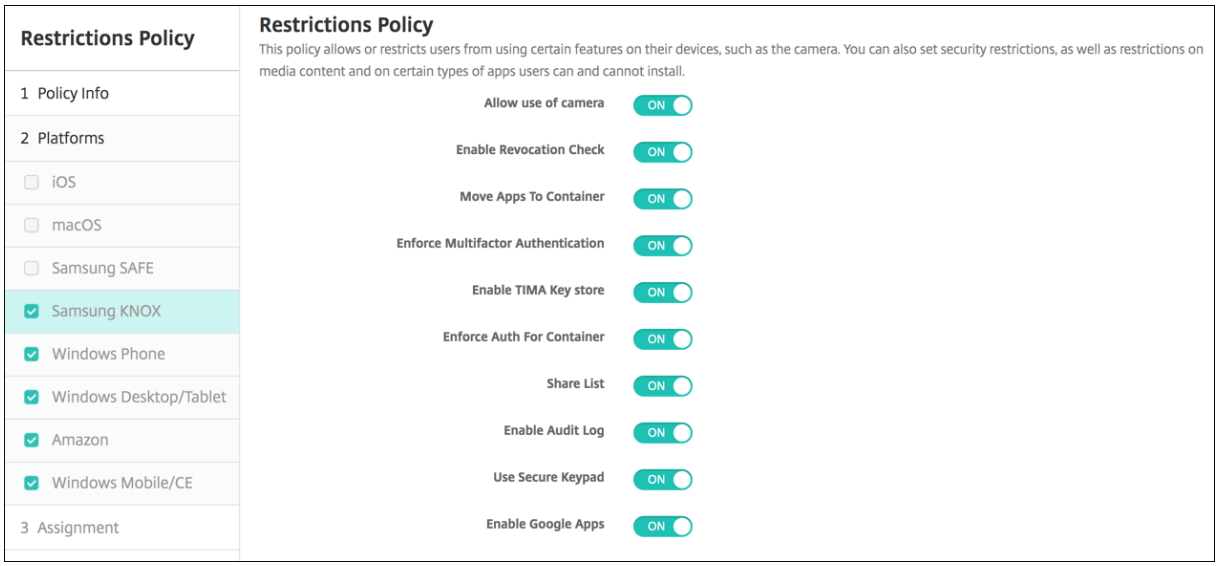
- **Permitir controles del hardware**
  - **Habilitar verificación de arranque seguro ODE.** Permite usar la verificación ODE de arranque de confianza para establecer una cadena de confianza desde el cargador de arranque hasta la imagen del sistema.
  - **Permitir modo de desarrollo:** Permite a los usuarios habilitar opciones de desarrollador en sus dispositivos.
  - **Permitir solo llamadas de emergencia:** Permite a los usuarios habilitar el modo Solo llamadas de emergencia en sus dispositivos.
  - **Permitir recuperación de firmware:** Permite que los usuarios recuperen el firmware en sus dispositivos.
  - **Permitir cifrado rápido:** Permite el cifrado únicamente del espacio de memoria utilizado. No es lo mismo que el cifrado de todo el disco, que cifra todos los datos, incluidos la configuración, los datos de aplicaciones, las aplicaciones y los archivos descargados y los archivos multimedia, entre otros.
  - **Modo Common Criteria**. Colocar el dispositivo en el modo de criterios comunes. La configuración de Common Criteria impone procesos estrictos de seguridad.
  - **Restablecer valores de fábrica:** Permite que los usuarios restablezcan sus dispositivos a los valores de fábrica.
  - **Cambio de fecha y hora:** Permite que los usuarios cambien la fecha y la hora en sus dispositivos.
  - **Pancarta de inicio del DoD:** Permite mostrar un mensaje o pancarta de notificación del uso del sistema aprobado por el DoD cuando los dispositivos de los usuarios se reinician.

  - **Cambios en los parámetros:** Permite que los usuarios cambien parámetros en sus dispositivos.
  - **Copia de seguridad:** Permite que los usuarios hagan copias de seguridad de los datos de aplicaciones y datos del sistema presentes en sus dispositivos.
  - **Actualización Over the Air:** Permite que los dispositivos de los usuarios reciban actualizaciones de software por conexión inalámbrica (MDM 3.0 y versiones posteriores).
  - **Datos en segundo plano:** Permite que las aplicaciones sincronicen datos en segundo plano.
  - **Cámara:** Permite que los usuarios usen la cámara en sus dispositivos.
  - **Portapapeles:** Permite que los usuarios copien datos al Portapapeles de sus dispositivos.
    * **Portapapeles compartido:** Permite que los usuarios compartan el contenido del Portapapeles entre sus dispositivos y un equipo (MDM 4.0 y versiones posteriores).
  - **Tecla Inicio:** Permite que los usuarios usen la tecla Inicio en sus dispositivos.
  - **Micrófono:** Permite que los usuarios usen el micrófono en sus dispositivos.
  - **Ubicaciones falsas:** Permite que los usuarios indiquen una ubicación de GPS falsa.
  - **NFC:** Permite que los usuarios usen la transmisión de datos en proximidad o NFC (Near Field Communication) en sus dispositivos (MDM 3.0 y versiones posteriores).
  - **Apagar:** Permite que los usuarios apaguen sus dispositivos (MDM 3.0 y versiones posteriores).
  - **Captura de pantalla:** Permite que los usuarios hagan capturas de pantalla en sus dispositivos.
  - **Tarjeta SD:** Permite que los usuarios usen una tarjeta SD, si está disponible, en sus dispositivos.
  - **Marcado por voz:** Permite que los usuarios usen el marcador por voz en sus dispositivos (MDM 4.0 y versiones posteriores).
  - **SBeam:** Permite que los usuarios compartan contenido con otras personas a través de NFC y Wi-Fi Direct (MDM 4.0 y versiones posteriores).
  - **SVoice:** Permite que los usuarios usen el asistente personal inteligente y el explorador de conocimientos en sus dispositivos (MDM 4.0 y versiones posteriores).
  - **Permitir varios usuarios:** Permite que varios usuarios usen un dispositivo (MDM 4.0 y versiones posteriores). Está **desactivado** de forma predeterminada.
- **Permitir aplicaciones**
  - **Explorador web:** Permite que los usuarios usen el explorador web.
  - **YouTube:** Permite que los usuarios accedan a YouTube.
  - **Google Play/Marketplace:** Permite que los usuarios accedan a Google Play y Google Apps Marketplace.
  - **Permitir aplicaciones que no son de Google Play:** Permite que los usuarios descarguen aplicaciones desde sitios que no sean Google Play y Google Apps Marketplace. Si se **activa**, un usuario puede usar la configuración de seguridad en su dispositivo para confiar en las

aplicaciones de fuentes desconocidas.
  - **Detener aplicaciones del sistema:** Permite que los usuarios inhabiliten las aplicaciones del sistema preinstaladas (MDM 4.0 y versiones posteriores).
  - **Inhabilitar aplicaciones.** Si se **activa**, bloquea la ejecución de una lista especificada de aplicaciones en dispositivos Samsung SAFE.
- **Red**
  - **MMS entrantes:** Permite que los usuarios reciban mensajes MMS.
  - **SMS entrantes:** Permite que los usuarios reciban mensajes SMS.
  - **MMS salientes:** Permite que los usuarios envíen mensajes MMS.
  - **SMS salientes:** Permite que los usuarios envíen mensajes SMS.
  - **Agregar perfiles VPN por parte del usuario:**
  - **Bluetooth:** Permite que los usuarios usen Bluetooth.
    - **Tethering.** Permitir que los usuarios compartan una conexión de datos móviles con otro dispositivo mediante la conexión Bluetooth.
  - **Wi-Fi:** Permite que los usuarios se conecten a redes inalámbricas.
    - **Tethering:** Permite que los usuarios compartan una conexión de datos móviles con otro dispositivo mediante la conexión Wi-Fi.
    - **Directo:** Permite que los usuarios se conecten directamente con otro dispositivo a través de su conexión Wi-Fi (MDM 4.0 y versiones posteriores).
    - **Cambio de estado:** Permite que las aplicaciones cambien el estado de la conectividad Wi-Fi.
    - **Cambios de directivas del usuario:** Permite que los usuarios cambien las directivas de red Wi-Fi. Si no se selecciona, los usuarios podrán cambiar solo el nombre de usuario y la contraseña de Wi-Fi. Si se selecciona, los usuarios podrán modificar todas las directivas de redes Wi-Fi.
  - **Tethering:** Permite que los usuarios compartan una conexión de datos móviles con otro dispositivo.
  - **Datos móviles:** Permite que los usuarios usen su conexión de móvil para datos.
  - **Permitir itinerancia:** Permite que los usuarios usen su conexión de datos móviles durante la itinerancia. Está desactivado de forma predeterminada, lo que inhabilita la itinerancia en los dispositivos de los usuarios.
  - **Solo conexiones seguras.** Permitir que los usuarios usen solamente conexiones seguras (MDM 4.0 y versiones posteriores).
  - **Android Beam:** Permite que los usuarios envíen páginas Web, fotos, vídeos y otro contenido desde sus dispositivos a otro dispositivo a través de NFC (MDM 4.0 y versiones posteriores).
  - **Grabación de audio.** Permitir que los usuarios graben sonido con sus dispositivos (MDM 4.0 y versiones posteriores).
  - **Grabación de vídeo:** Permite que los usuarios graben vídeo con sus dispositivos (MDM

4.0 y versiones posteriores).
  - **Servicios de localización:** Permite que los usuarios activen GPS en sus dispositivos.
  - **Límite diario (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada día. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
  - **Límite semanal (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada semana. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
  - **Límite mensual (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada mes. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
- **Permitir acciones de USB:** Permite la conexión de USB entre los dispositivos de los usuarios y un equipo.
  - **Depuración:** Permite la depuración por USB.
  - **Almacenamiento del host:** Permite que los dispositivos de los usuarios actúen como host de USB cuando un dispositivo USB se conecta a ellos. Los dispositivos de los usuarios suministran energía al dispositivo USB.
  - **Almacenamiento masivo:** Permite la transferencia de archivos de datos de gran tamaño entre los dispositivos de los usuarios y un equipo a través de una conexión USB.
  - **Reproductor multimedia Kies:** Permite que los usuarios usen la herramienta Samsung Kies para sincronizar archivos entre sus dispositivos y un equipo.
  - **Tethering:** Permite que los usuarios compartan una conexión de datos móviles con otro dispositivo por la conexión USB.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

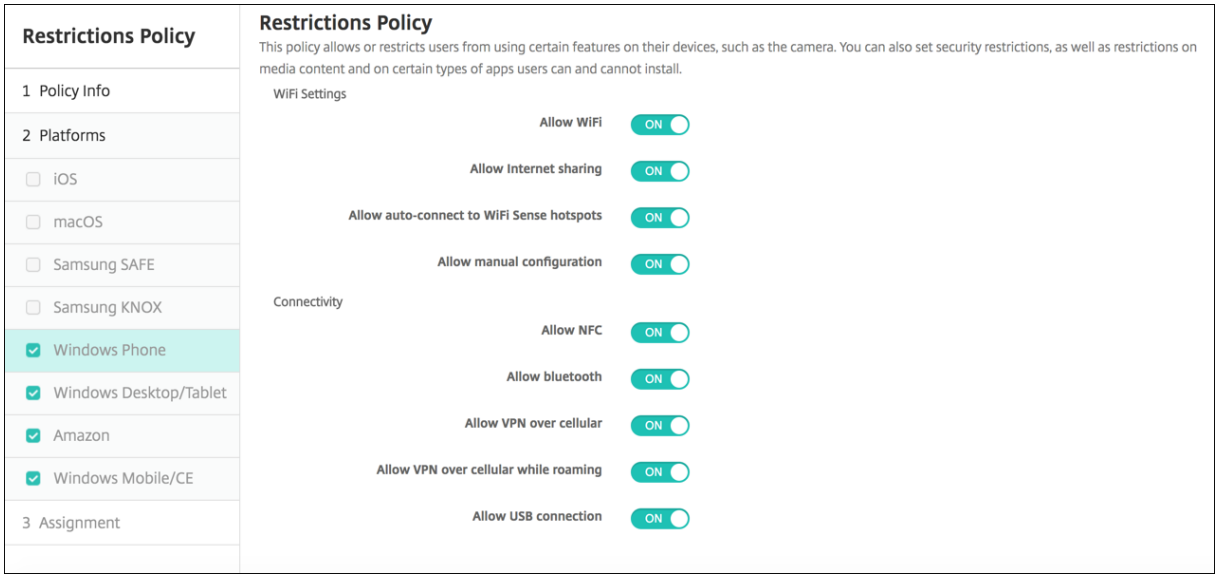
Parámetros de Samsung Knox



Estas opciones están disponibles únicamente en Samsung Knox Premium (Knox 2.0).

- **Permitir el uso de la cámara:** Permite que los usuarios usen la cámara en sus dispositivos.
- **Permitir comprobación de revocación.** Habilitar la comprobación de certificados revocados.
- **Mover aplicaciones al contenedor:** Permite que los usuarios muevan aplicaciones entre el contenedor Knox y el área personal de sus dispositivos.
- **Aplicar autenticación de varios factores.** Los usuarios deben usar una huella digital junto con otro método de autenticación (como un PIN o una contraseña) para desbloquear sus dispositivos.
- **Habilitar almacén de claves TIMA.** El almacén de claves TIMA ofrece almacenamiento seguro de claves basado en TrustZone para las claves simétricas. Los pares de claves de RSA y los certificados se enrutan al proveedor de almacenamiento de claves predeterminado para su almacenamiento.
- **Aplicar autenticación para contenedor.** Usar una autenticación aparte para abrir el contenedor Knox, distinta de la autenticación usada para dispositivo.
- **Compartir lista:** Permite que los usuarios compartan contenido entre las aplicaciones en la lista Share Via.
- **Habilitar registros de auditoría:** Permite la creación de registros de auditoría de eventos para el análisis forense de un dispositivo.
- **Usar teclado seguro.** Obligar a los usuarios a usar un teclado seguro dentro del contenedor Knox.
- **Habilitar Google Apps:** Permite que los usuarios descarguen aplicaciones desde Google Mobile Services en el contenedor Knox.
- **Autenticación de explorador con tarjetas inteligentes.** Habilitar la autenticación de exploradores en dispositivos que dispongan de un lector de tarjetas inteligentes.

Parámetros de Windows Phone y escritorios y tabletas Windows



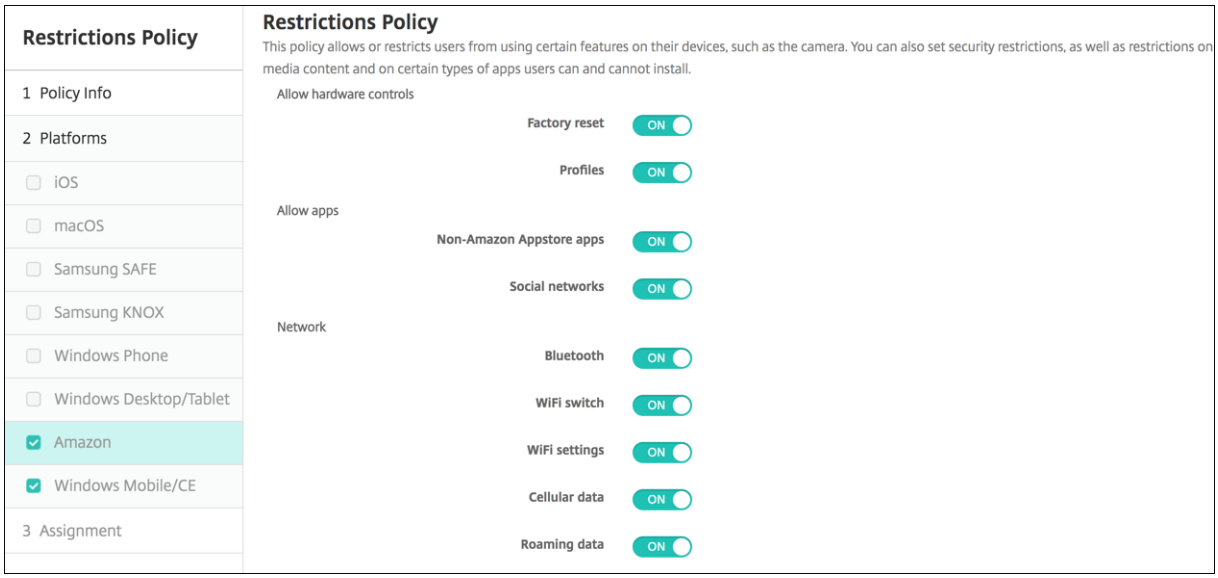
- **Parámetros de Wi-Fi**
  - **Permitir Wi-Fi:** Permite que un dispositivo se conecte a una red inalámbrica. Solo para Windows Phone.
  - **Permitir compartir Internet:** Permite que un dispositivo comparta su conexión de Internet con otros dispositivos convirtiéndolo en una zona hotspot de Wi-Fi.
  - **Permitir conexión automática con hotspots Wi-Fi Sense:** Permite que un dispositivo se conecte automáticamente a hotspots del Sensor Wi-Fi. Los servicios de ubicación deben estar habilitados para que funcione esta opción. Para obtener más información acerca del Sensor Wi-Fi, consulte las Preguntas más frecuentes sobre el Sensor Wi-Fi de Windows Phone.
  - **Permitir configuración manual:** Permite que los usuarios configuren manualmente las conexiones Wi-Fi. Solo para Windows Phone.
- **Conectividad**
  - **Permitir NFC:** Permite que el dispositivo se comunique con una etiqueta NFC (Near Field Communication) u otro dispositivo de transmisión habilitado para NFC. Solo para Windows Phone.
  - **Permitir Bluetooth:** Permite que el dispositivo se conecte a través de Bluetooth. Solo para Windows Phone.
  - **Permitir VPN por red móvil:** Permite que el dispositivo se conecte por VPN a una red de telefonía móvil.
  - **Permitir VPN por red móvil durante la itinerancia:** Permite que el dispositivo se conecte por VPN cuando el dispositivo se mueve entre redes de telefonía móvil.
  - **Permitir conexión USB:** Permite que un escritorio acceda al almacenamiento de un dispositivo a través de una conexión USB. Solo para Windows Phone.

  - **Permitir itinerancia de datos móviles:** Permite que los usuarios usen su conexión de datos móviles durante la itinerancia.
- **Cuentas**
  - **Permitir conexión con cuenta de Microsoft:** Permite que el dispositivo use una cuenta de Microsoft para servicios y autenticación de conexiones no relacionados con correo electrónico.
  - **Permitir correo electrónico que no es de Microsoft:** Permite que el usuario agregue cuentas de correo electrónico que no son de Microsoft.
- **Buscar:** Solo Windows Phone.
  - **Permitir que la búsqueda use la ubicación:** Permite que las búsquedas usen el servicio de ubicación del dispositivo.
  - **Filtrar contenido para adultos:** Permite el contenido para adultos. Está **desactivado** de forma predeterminada, lo que significa que el contenido para adultos no se filtra.
  - **Permitir que Bing Vision almacene imágenes:** Permite que Bing Vision guarde imágenes capturadas al realizar búsquedas con Bing Vision.
- **Sistema**
  - **Permitir tarjeta de almacenamiento:** Permite que el dispositivo use una tarjeta de almacenamiento.
  - **Telemetría:** En la lista, haga clic en una opción para permitir o impedir que el dispositivo envíe información de telemetría. El valor predeterminado es **Permitida**. Las demás opciones son: **No permitida** y **Permitida, excepto para solicitudes de datos secundarios**.
  - **Permitir servicios de localización:** Permite los servicios de localización geográfica.
  - **Permitir la versión Tech Preview de compilaciones internas:** Permite que los usuarios obtengan una versión Tech Preview de las compilaciones internas de Microsoft.
- **Cámara:** Solo escritorios o tabletas Windows.
  - **Permitir el uso de la cámara:** Permite que los usuarios usen la cámara del dispositivo.
- **Bluetooth:** Solo para escritorios o tabletas Windows.
  - **Permitir modo detectable:** Permite que los dispositivos Bluetooth encuentren el dispositivo local.
  - **Nombre del dispositivo local:** Un nombre para el dispositivo local.
- **Seguridad:** Solo para Windows Phone.
  - **Permitir instalación manual de certificado raíz:** Permite que los usuarios instalen manualmente un certificado raíz.
  - **Requerir cifrado del dispositivo:** Requiere el cifrado del dispositivo. Tenga en cuenta que después de habilitar el cifrado en un dispositivo, ya no se puede inhabilitar. Está **desactivado** de forma predeterminada.
  - **Permitir copiar y pegar:** Permite que los usuarios copien y peguen datos en sus dispositivos.
  - **Permitir capturas de pantalla:** Permite que los usuarios hagan capturas de pantalla en

sus dispositivos.
  - **Permitir grabación de voz:** Permite que los usuarios usen la grabación de voz en sus dispositivos.
  - **Permitir Guardar como para archivos de Office:** Permite que los usuarios guarden archivos de Office con la opción “Guardar como”.
  - **Permitir notificaciones del Centro de actividades:** Permite notificaciones del Centro de actividades en la pantalla de bloqueo del dispositivo.
  - **Permitir Cortana:** Permite que los usuarios accedan al asistente personal inteligente y explorador de conocimientos llamado Cortana.
  - **Permitir sincronizar parámetros del dispositivo:** Permite que los usuarios sincronicen parámetros entre dispositivos Windows Phone 8.1 durante la itinerancia.
- **Experiencia:** Solo para escritorios o tabletas Windows.
  - **Permitir Cortana:** Permite que los usuarios accedan al asistente personal inteligente y explorador de conocimientos llamado Cortana.
  - **Permitir detección de dispositivos:** Permite la detección de red del dispositivo.
  - **Permitir desinscripción manual de MDM:** Permite que los usuarios desinscriban manualmente sus dispositivos de XenMobile MDM.
  - **Permitir sincronizar parámetros del dispositivo:** Permite que los usuarios sincronicen parámetros entre dispositivos con Windows 10 o Windows 11 durante la itinerancia.
- **Encima de bloqueo:** Solo para escritorios o tabletas Windows.
  - **Permitir notificaciones toast:** Permite las notificaciones toast en la pantalla de bloqueo. Solo para escritorios o tabletas Windows.
- **Aplicaciones**
  - **Permitir acceso a la tienda:** Permite que los usuarios accedan a la Tienda Microsoft. Solo para Windows Phone.
  - **Permitir desbloqueo para desarrolladores:** Permite que los usuarios registren sus dispositivos en Microsoft y desarrollen o instalen aplicaciones que no están en la tienda de aplicaciones de Windows Phone. Solo para Windows Phone.
  - **Permitir acceso a explorador web:** Permite Internet Explorer en el dispositivo. Solo para Windows Phone.
  - **Permitir actualización automática de App Store:** Permite que las aplicaciones del App Store se actualicen automáticamente. Solo para escritorios o tabletas Windows.
- **Privacidad:** Solo para escritorios o tabletas Windows.
  - **Permitir personalización de la entrada:** Permite que se ejecute el servicio de personalización de entrada, lo que mejora las entradas predictivas (como lápiz y teclado táctil) según lo que escriba el usuario.
- **Configuración:** Solo para escritorios o tabletas Windows.
  - **Permitir reproducción automática:** Permite que los usuarios cambien los parámetros de la reproducción automática.

- **Permitir Sensor de datos:** Permite que los usuarios cambien los parámetros de Sensor de datos.
- **Permitir fecha y hora:** Permite que los usuarios cambien los parámetros de la fecha y la hora.
- **Permitir idioma:** Permite que los usuarios cambien los parámetros de idioma.
- **Permitir suspensión:** Permite que los usuarios cambien los parámetros de suspensión.
- **Permitir región:** Permite que los usuarios cambien los parámetros de región.
- **Permitir opciones de inicio de sesión:** Permite que los usuarios cambien los parámetros de inicio de sesión.
- **Permitir área de trabajo:** Permite que los usuarios cambien los parámetros del área de trabajo.
- **Permitir su cuenta:** Permite que los usuarios cambien los parámetros de cuenta.

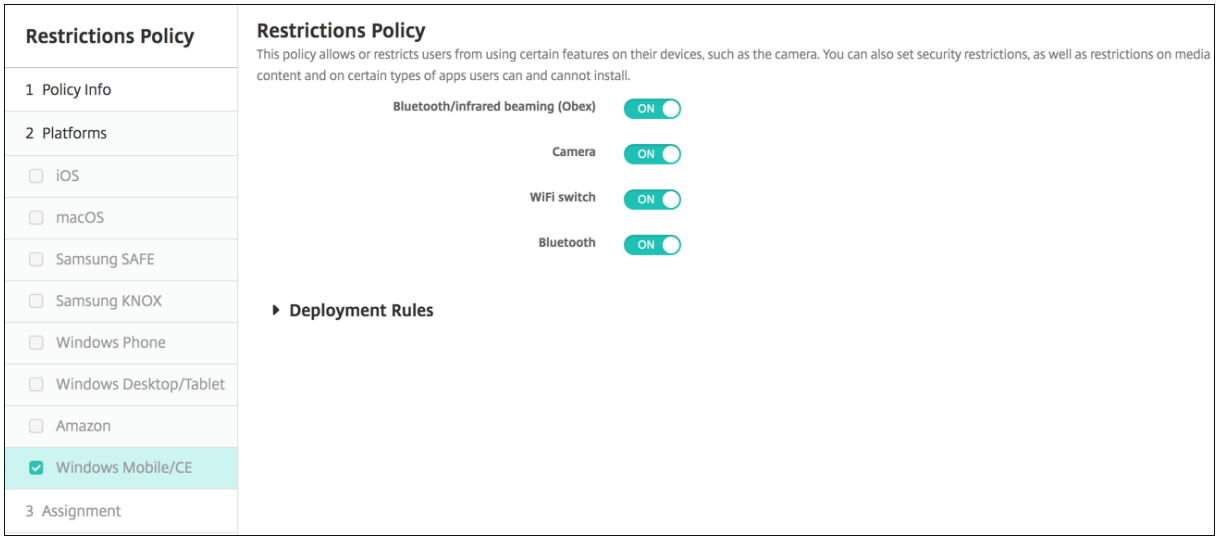
Parámetros de Amazon



- **Permitir controles del hardware**
  - **Restablecer valores de fábrica:** Permite que los usuarios restablezcan sus dispositivos a los valores de fábrica.
  - **Perfiles:** Permite que los usuarios cambien el perfil de hardware en sus dispositivos.
- **Permitir aplicaciones**
  - **Aplicaciones que no son de la Tienda Apps de Amazon:** Permite que los usuarios instalen en sus dispositivos aplicaciones que no provienen de la tienda Amazon Appstore.
  - **Redes sociales:** Permite que los usuarios accedan a redes sociales desde sus dispositivos.
- **Red**
  - **Bluetooth:** Permite que los usuarios usen Bluetooth.
  - **Conmutador Wi-Fi:** Permite que las aplicaciones cambien el estado de la conectividad

Wi-Fi.
  - **Parámetros de Wi-Fi:** Permite que los usuarios cambien los parámetros de las redes inalámbricas.
  - **Datos móviles:** Permite que los usuarios usen su conexión de móvil para datos.
  - **Datos de itinerancia:** Permite que los usuarios usen su conexión de datos móviles durante la itinerancia.
  - **Servicios de localización:** Permite que los usuarios usen GPS.
- **Acciones de USB:**
  - **Depuración:** Permite que los dispositivos de los usuarios se conecten mediante USB a un equipo para su depuración.

Parámetros de Windows Mobile/CE



- **Bluetooth/transmisión por infrarrojos (Obex).** Habilitar OBEX (OBject EXchange protocol) por conexión Bluetooth o infrarrojos para intercambiar datos entre dispositivos.
- **Cámara.** Habilitar la cámara en los dispositivos de los usuarios.
- **Conmutador Wi-Fi:** Permite que los usuarios cambien de redes inalámbricas.
- **Bluetooth:** Habilita Bluetooth en los dispositivos de los usuarios.
- **Cámara.** Habilitar la cámara en los dispositivos de los usuarios.
- **Conmutador Wi-Fi:** Permite que los usuarios cambien de redes inalámbricas.
- **Bluetooth:** Habilita Bluetooth en los dispositivos de los usuarios.

Directiva de itinerancia

January 4, 2022

En XenMobile, puede agregar una directiva de dispositivo 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 itinerancia de voz, la itinerancia de datos se inhabilita automáticamente. En el caso de iOS, esta directiva solo está disponible para iOS 5.0 y versiones posteriores.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Inhabilitar itinerancia de voz:** Seleccione si inhabilitar la itinerancia de voz. Si se inhabilita esta opción, la itinerancia de datos se inhabilita automáticamente. El valor predeterminado es **No**, lo que permite la itinerancia de voz.
- **Inhabilitar itinerancia de datos.** Seleccione si inhabilitar la itinerancia de datos. Esta opción solo está disponible cuando la itinerancia de voz está habilitada. El valor predeterminado es **No**, lo que permite la itinerancia de datos.

Parámetros de Windows Mobile/CE

- **Mientras el dispositivo está en itinerancia**
  - **Usar solo conexión a demanda.** 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.
  - **Bloquear todas las conexiones móviles excepto las administradas por XenMobile.** El dispositivo no enviará ni recibirá ningún dato, salvo el tráfico de datos declarado oficialmente en un túnel de aplicaciones XenMobile u otras tareas de administración de dispositivos que lleve a cabo XenMobile. Por ejemplo, esta opción inhabilita todas las conexiones a Internet a través del explorador web del dispositivo.
  - **Bloquear todas las conexiones móviles administradas por 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.
  - **Bloquear todas las conexiones móviles a XenMobile.** En este caso, hasta que el dispositivo se vuelva a conectar por USB, Wi-Fi o su operador predeterminado de telefonía móvil, no hay tráfico que transite entre el dispositivo y XenMobile.
- **Mientras el dispositivo está en itinerancia en el ámbito nacional**
  - **Ignorar itinerancia en el ámbito nacional:** No se bloquean datos mientras los usuarios se muevan en el ámbito nacional.

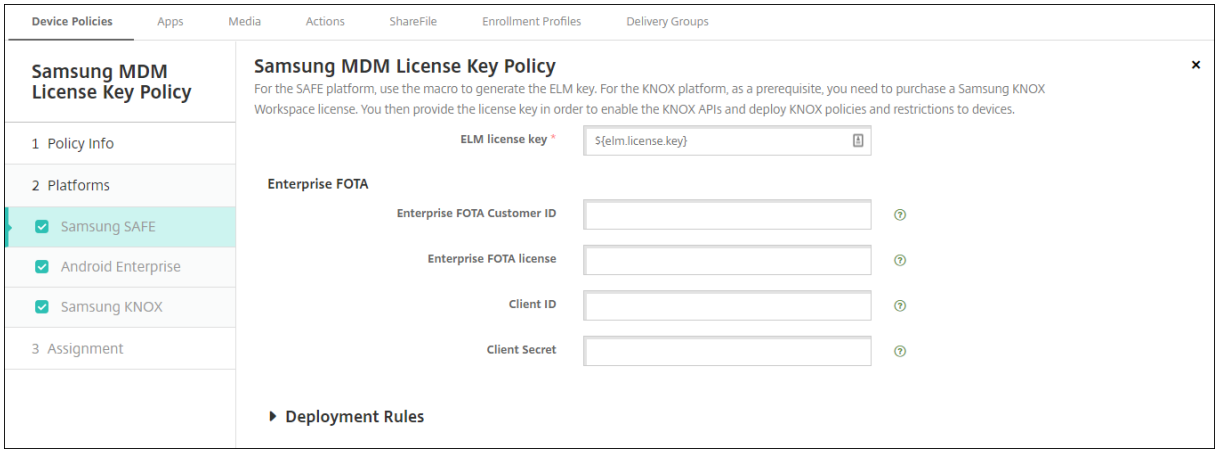
Directiva de clave de licencia MDM de Samsung

January 4, 2022

Permite indicar la clave integrada de Samsung Enterprise License Management (ELM) que debe implementar en un dispositivo para poder implementar después directivas y restricciones de SAFE. XenMobile también admite el servicio Enterprise Firmware-Over-The-Air (E-FOTA) de Samsung. XenMobile admite y extiende directivas de Samsung for Enterprise (SAFE) y Samsung Knox.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Samsung SAFE



- **Clave de licencia ELM.** XenMobile rellena previamente este campo con la macro que genera la clave de licencia ELM. Si el campo está en blanco, escriba esta macro: ${elm.license.key}

Configurar los parámetros de Samsung E-FOTA

Enterprise FOTA (E-FOTA) de Samsung permite determinar cuándo se actualizan los dispositivos y la versión de firmware que se va a usar. E-FOTA permite probar las actualizaciones antes de implementarlas. De esta manera, puede asegurarse de que las actualizaciones sean compatibles con las aplicaciones. Puede obligar los dispositivos a que se actualicen a la versión disponible más reciente del firmware, sin necesidad de interacción con el usuario.

Samsung admite E-FOTA para dispositivos Samsung Knox 2.7.1 (versión mínima) con firmware autorizado.

XenMobile admite la incorporación de dispositivos desde la consola de XenMobile a Knox E-FOTA One. Para obtener más información sobre cómo exportar una lista de dispositivos desde XenMobile, con-

sulte Exportar la tabla Dispositivos. Para obtener más información sobre cómo agregar dispositivos a Knox E-FOTA One, consulte la documentación de Samsung.

XenMobile no admite la solución Knox E-FOTA en MDM.

Para configurar una directiva de E-FOTA:

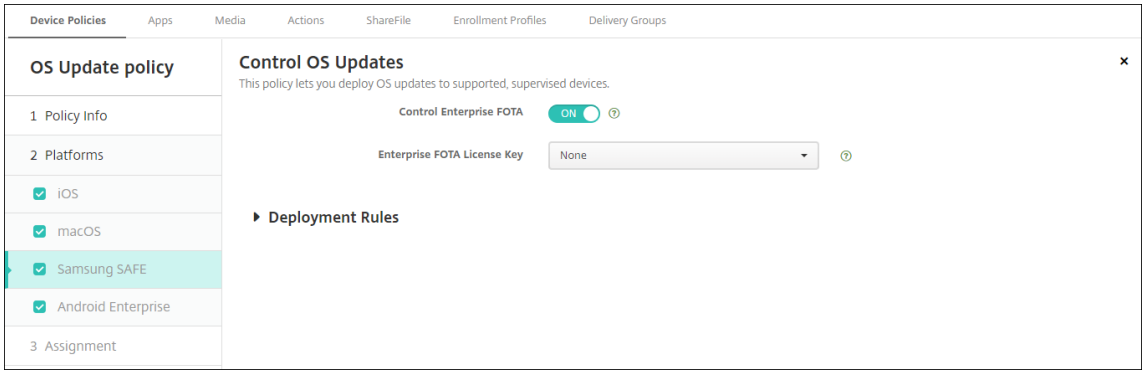
1. Cree una directiva “Clave de licencia para MDM de Samsung” con las claves y la información de licencia que haya recibido de Samsung. XenMobile Server valida y registra la información. Si XenMobile detecta un problema en E-FOTA, aparece un mensaje de error que así lo indica. Utilice el código facilitado para solucionar el problema. Para obtener más información, consulte Developer Guides.

   Escriba la **Clave de licencia ELM**. XenMobile rellena previamente este campo con la macro que genera la clave de licencia ELM. Si el campo está en blanco, escriba esta macro: ${elm.license.key}

   Escriba la siguiente información, proporcionada por Samsung cuando adquirió un paquete de E-FOTA:

   - **ID de cliente de Enterprise FOTA**
   - **Licencia de Enterprise FOTA**
   - **ID de cliente**
   - **Secreto del cliente**

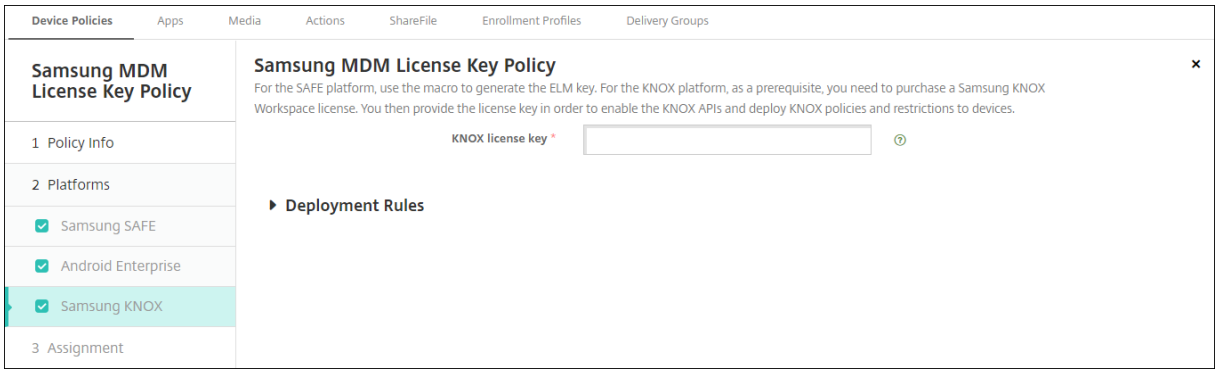
2. Si quiere, cree una directiva Control de actualizaciones de sistema operativo.



   - **Enterprise FOTA:** Elija **Sí** para este parámetro.
   - **Clave de licencia de Enterprise FOTA.** Seleccione el nombre de la directiva de clave de licencia MDM para Samsung que creó en el paso 1.

3. Implemente la directiva de control de actualizaciones de SO en Secure Hub.

Configuración de Android Enterprise y Samsung KNOX



- **Clave de licencia Knox:** Escriba la clave de licencia Knox que ha obtenido de Samsung.

Directiva de firewall para Samsung SAFE

July 10, 2020

Esta directiva permite configurar los parámetros del firewall para dispositivos Samsung. Escriba las direcciones IP, los puertos y los nombres de host que se van a permitir o bloquear. También puede configurar el proxy y las opciones de reenrutado de este.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Samsung SAFE

- **Permitir/denegar hosts.** Haga clic en **Agregar** y lleve a cabo lo siguiente para cada host al que quiera permitir o denegar el acceso:
  - **Nombre de host/intervalo IP.** El nombre de host o el intervalo de direcciones IP del sitio en cuestión.
  - **Puerto/intervalo de puertos.** El número de puerto o el intervalo de puertos.
  - **Filtro de reglas para permitir/denegar.** Seleccione **Lista blanca** para permitir el acceso al sitio o **Lista negra** para denegarlo.

    > **Nota:**
    > La consola de XenMobile Server contiene los términos “lista negra” y “lista blanca”. Estamos cambiando esos términos en una próxima versión a “lista de bloqueados” y “lista de permitidos”.
- **Configuración de enrutamiento.** Haga clic en **Agregar** y lleve a cabo lo siguiente para configurar cada proxy:

  - **Nombre de host/intervalo IP.** El nombre de host o el intervalo de direcciones IP para el reenrutado del proxy.
  - **Puerto/intervalo de puertos.** El número de puerto o el intervalo de puertos para el reenrutado del proxy.
  - **IP del proxy.** La dirección IP del proxy para el reenrutado.
  - **Puerto del proxy.** El puerto del proxy para el reenrutado.
- **Configuración de proxy**
  - **IP del proxy.** La dirección IP del servidor proxy.
  - **Puerto.** El puerto del servidor proxy.

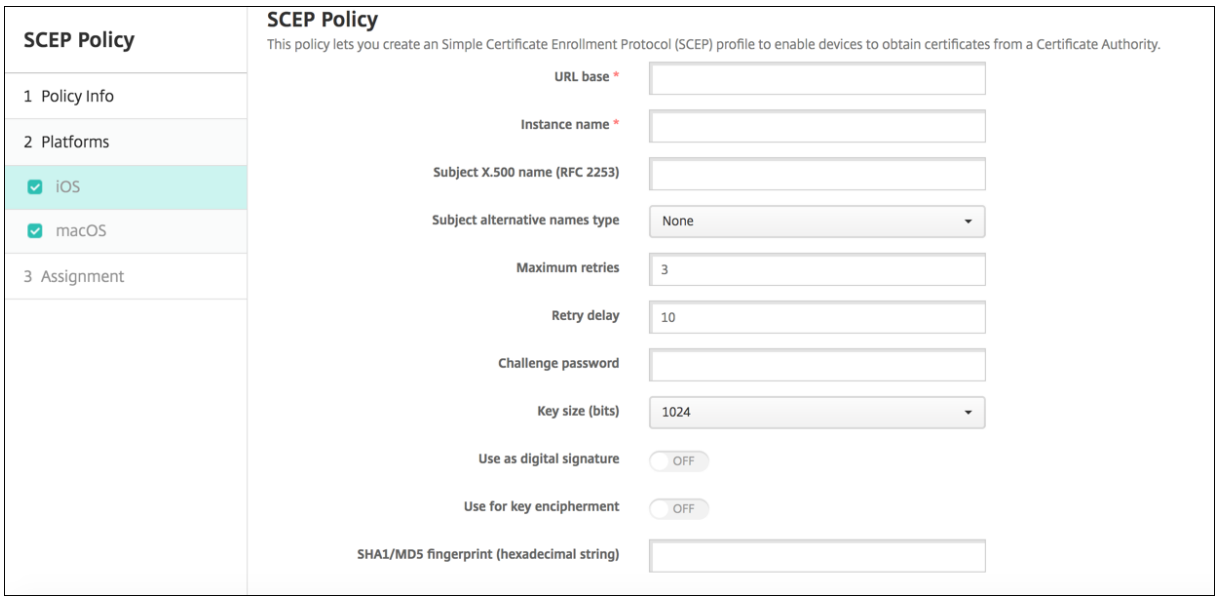
Directiva de SCEP

January 4, 2022

Esta directiva permite configurar dispositivos iOS y macOS 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 PKI.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

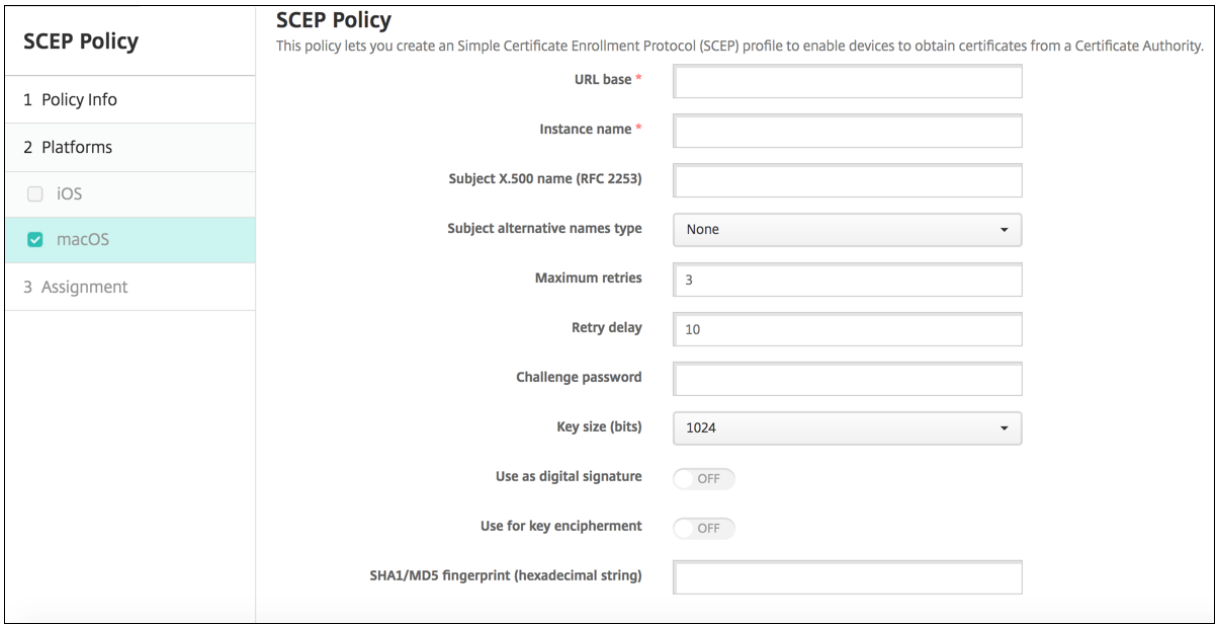
Parámetros de iOS



- **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.
- **Nombre de la instancia.** 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.
- **Nombre de sujeto X.500 (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).
- **Tipo de nombres alternativos del sujeto.** 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 **Ninguno**, **Nombre RFC 822**, **Nombre DNS** o **URI**.
- **Máximo de reintentos.** Escriba la cantidad de veces que un dispositivo vuelve a intentar conectarse cuando el servidor SCEP envía la respuesta PENDIENTE. El valor predeterminado es **3**.
- **Demora entre reintentos.** Escriba la cantidad de segundos que deben transcurrir entre los reintentos. El primer reintento se produce sin retraso. El valor predeterminado es **10**.
- **Verificar contraseña.** Escriba un secreto previamente compartido.
- **Tamaño de la clave (bits):** Seleccione **2048** o un valor superior para el tamaño de la clave en bits.
- **Usar como firma digital.** 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.
- **Usar para cifrado de claves.** 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.

- **Huella digital SHA1/MD5 (cadena hexadecimal).** 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**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de macOS



- **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.
- **Nombre de la instancia.** 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.

- **Nombre de sujeto X.500 (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).
- **Tipo de nombres alternativos del sujeto.** 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 **Ninguno**, **Nombre RFC 822**, **Nombre DNS** o **URI**.
- **Máximo de reintentos.** Escriba la cantidad de veces que un dispositivo vuelve a intentar conectarse cuando el servidor SCEP envía la respuesta PENDIENTE. El valor predeterminado es **3**.
- **Demora entre reintentos.** Escriba la cantidad de segundos que deben transcurrir entre los reintentos. El primer reintento se produce sin retraso. El valor predeterminado es **10**.
- **Verificar contraseña.** Escriba un secreto previamente compartido.
- **Tamaño de la clave (bits):** Seleccione **2048** o un valor superior para el tamaño de la clave en bits.
- **Usar como firma digital.** 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.
- **Usar para cifrado de claves.** 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.
- **Huella digital SHA1/MD5 (cadena hexadecimal).** 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**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.

    * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

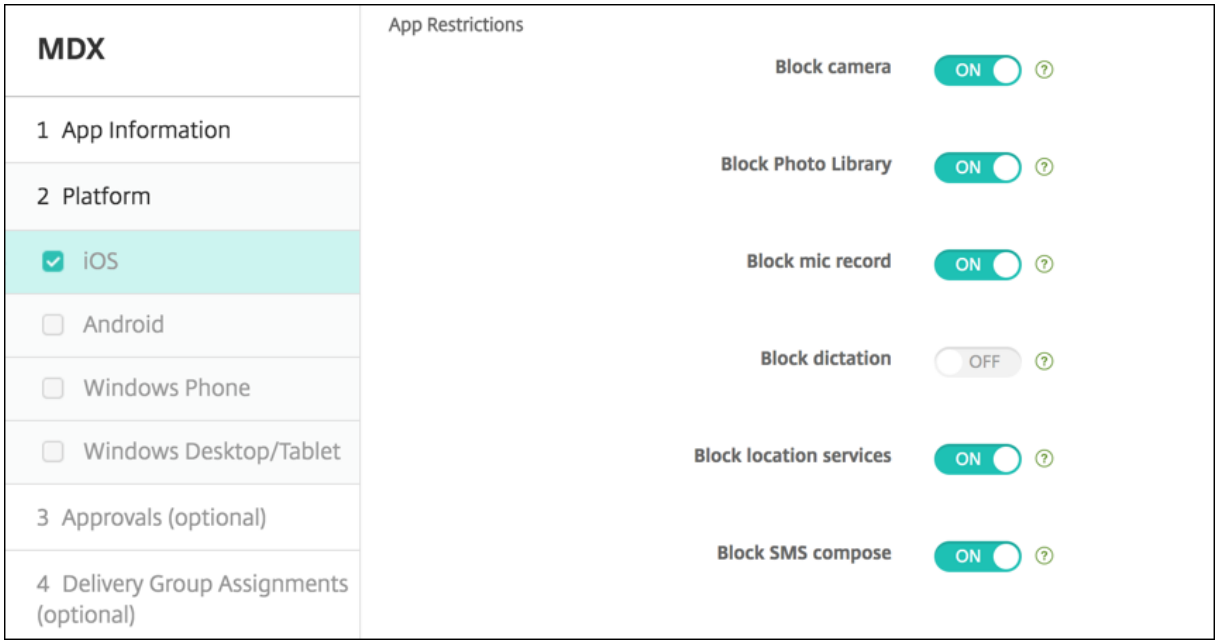
Directivas de Siri y dictado

January 4, 2022

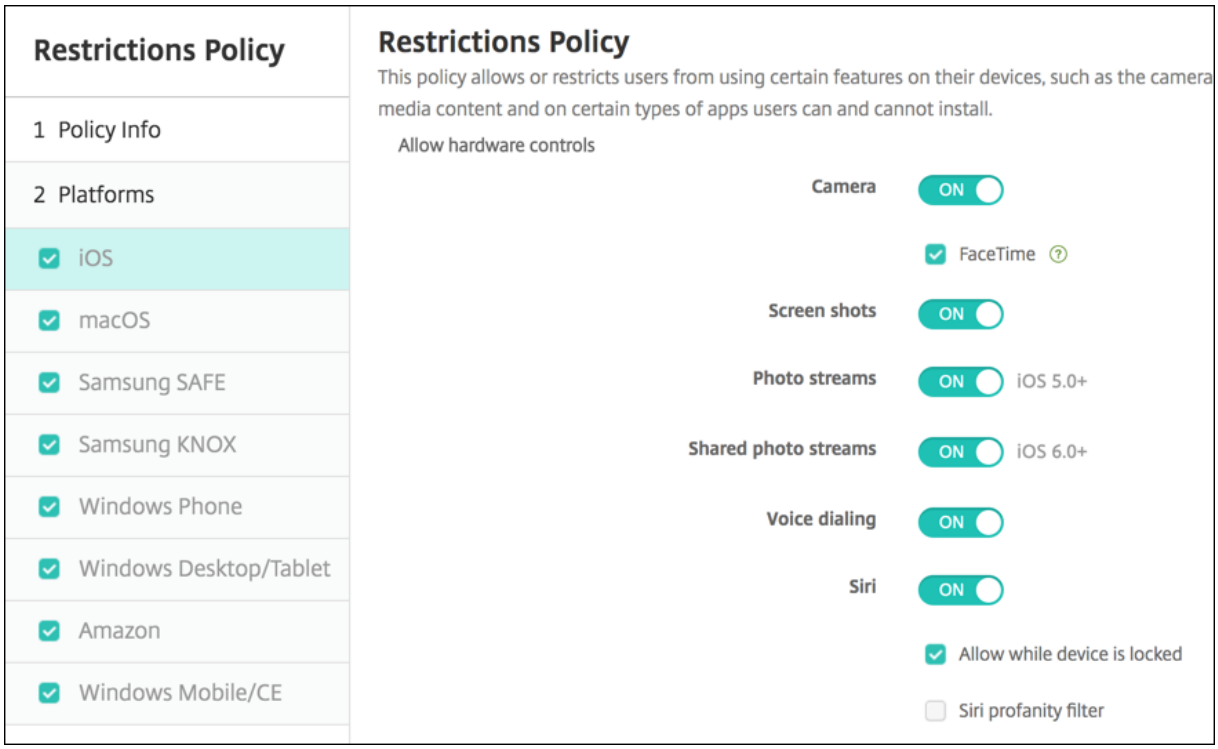
Cuando los usuarios preguntan algo a Siri o dictan texto en dispositivos iOS administrados, Apple recopila los datos de voz con el fin de mejorar Siri. Los datos de voz pasan a través de los servicios de nube de Apple, y por lo tanto existen fuera del contenedor seguro de XenMobile. El texto resultado del dictado, sin embargo, queda dentro del contenedor.

XenMobile 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 **Bloquear dictado** para cada aplicación tiene el valor **Sí** (activado) de forma predeterminada, lo que inhabilita el micrófono del dispositivo. Configúrela con el valor **No** si quiere permitir el dictado. La directiva se encuentra en la consola de XenMobile, en **Configurar > Aplicaciones**. Seleccione la aplicación, haga clic en **Modificar** y, a continuación, haga clic en **iOS**.



En las implementaciones MDM (administración de dispositivos móviles), también puede inhabilitar Siri desde la directiva de Siri, en **Configurar > Directivas de dispositivo**. El uso de Siri está permitido de manera predeterminada.



Hay algunas cuestiones a tener en cuenta a la hora de decidir si se permiten Siri y el dictado:

- De acuerdo con la información que Apple ha hecho pública, Apple guarda datos de clips de voz y Siri por un máximo de dos años. Se asigna un número aleatorio a los datos, para representar

al usuario, y los archivos de voz se asocian con dicho número. Para obtener más información, consulte este artículo de Wired: Apple reveals how long Siri keeps your data.
- Puede consultar la directiva de privacidad de Apple yendo a **Ajustes > General > Teclados** en cualquier dispositivo iOS, y tocando el enlace bajo **Habilitar dictado**.

Directiva de cuenta SSO

January 4, 2022

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.

Esta directiva se aplica solamente a iOS 7.0 y versiones posteriores.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Nombre de cuenta.** Escriba el nombre de la cuenta SSO de Kerberos que aparece en los dispositivos de los usuarios. Este campo es obligatorio.
- **Nombre principal de Kerberos.** Escriba el nombre de la entidad de seguridad asignada a Kerberos. Este campo es obligatorio.
- **Credencial de identidad (credencial PKI o de almacén de claves).** 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.
- **Territorio de Kerberos.** Escriba el territorio 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.
- **Direcciones URL permitidas.** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada URL que deba requerir el inicio Single Sign-On:
  - **URL permitida:** Introduzca una URL que deba requerir SSO 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 Single Sign-On con el token de Kerberos que se haya almacenado en caché

en el dispositivo después de un inicio de sesión Kerberos previo. La coincidencia debe ser exacta en la parte de host de la URL. Por ejemplo, `https://shopping.apple.com` es válido, pero `https://*.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 podría significar casi cualquier cosa, desde un desafío de contraseña estándar hasta un error HTTP si la URL solo está configurada para SSO mediante Kerberos.

- Haga clic en **Agregar** para agregar la URL, o bien haga clic en **Cancelar** para no agregarla.

- **Identificadores de aplicaciones.** Haga clic en **Agregar** y lleve a cabo lo siguiente para cada aplicación que pueda emplear este inicio de sesión:
  - **Identificador de aplicación.** 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 **Agregar** para agregar el identificador de aplicación, o bien haga clic en **Cancelar** para cancelar la operación.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva de cifrado de almacenamiento

January 21, 2021

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 y Windows Phone. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en este artículo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

Para dispositivos Samsung SAFE, antes de configurar esta directiva, compruebe que se cumplen los siguientes requisitos:

- Establezca la opción de bloqueo de pantalla en los dispositivos de los usuarios.
- Conecte los dispositivos de los usuarios y cárguelos al menos al 80 %.
- Compruebe que los dispositivos requieren una contraseña que contenga números y letras o símbolos.

Configurar parámetros de Samsung SAFE

- **Cifrar almacenamiento interno.** Seleccione si cifrar el almacenamiento interno en los dispositivos de los usuarios. Este almacenamiento incluye el almacenamiento interno y la memoria del dispositivo. Está **activado** de forma predeterminada.
- **Cifrar almacenamiento externo.** Seleccione si cifrar el almacenamiento externo en los dispositivos de los usuarios. Está **activado** de forma predeterminada.

Parámetros de Windows Phone

- **Requerir cifrado del dispositivo.** Seleccione esta opción para cifrar los dispositivos de los usuarios. Está **desactivado** de forma predeterminada.
- **Inhabilitar tarjeta de almacenamiento.** Seleccione esta opción para evitar que los usuarios utilicen tarjetas de almacenamiento en sus dispositivos. Está **desactivado** de forma predeterminada.

Directiva de tiendas

January 4, 2022

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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de plataforma

Para cada plataforma que quiera configurar, seleccione si aparecerá un clip Web de XenMobile Store en los dispositivos de los usuarios. Está **activado** de forma predeterminada.

Directiva de calendarios suscritos

January 4, 2022

En XenMobile, puede agregar una directiva de dispositivo para agregar un calendario suscrito a la lista de calendarios en los dispositivos iOS. La lista de los calendarios públicos a los que se puede suscribir está disponible en www.apple.com/downloads/macosx/calendars.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisito previo

Debe haberse suscrito a un calendario para poder agregarlo a la lista de calendarios suscritos en los dispositivos de los usuarios.

Parámetros de iOS

- **Descripción.** 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 `https://` a un archivo de iCalendar (.ics). Este campo es obligatorio.
- **Nombre de usuario.** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña.** Escriba una contraseña opcional de usuario.
- **Usar SSL.** Seleccione si utilizar una conexión de capa de sockets seguros (SSL) para el calendario. Está **desactivado** de forma predeterminada.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva de términos y condiciones

January 4, 2022

En XenMobile, puede crear directivas de términos y condiciones cuando quiera que los usuarios acepten aquellas directivas específicas de la empresa que rijan las conexiones a la red corporativa. Cuando los usuarios inscriban sus dispositivos con XenMobile, se les presentarán los términos y las condiciones, y deberán aceptarlos para llevar a cabo la inscripción. Si rechazan dichos términos y condiciones, se cancelará el proceso de inscripción.

Si la empresa tiene usuarios internacionales y quiere que acepten los términos y las condiciones en su idioma nativo, puede crear directivas distintas para los términos y las condiciones en diferentes idiomas. Debe suministrar un archivo para cada combinación de plataforma e idioma que quiera implementar. Para dispositivos Android y iOS, debe proporcionar archivos PDF. Para dispositivos Windows, debe suministrar archivos de texto (.txt) y los archivos de imagen correspondientes.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS y Android

- **Archivos a importar:** Seleccione el archivo de términos y condiciones a importar; para ello, haga clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.
- **Términos y condiciones predeterminados:** Seleccione si este archivo es el documento predeterminado para los usuarios que son miembros de varios grupos con términos y condiciones diferentes. Está **desactivado** de forma predeterminada.

Parámetros de Windows Phone y tabletas Windows

- **Archivos a importar:** Seleccione el archivo de términos y condiciones a importar; para ello, haga clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.
- **Imagen:** Para seleccionar el archivo de imagen a importar, haga clic en **Examinar** y vaya a la ubicación de ese archivo.
- **Términos y condiciones predeterminados:** Seleccione si este archivo es el documento predeterminado para los usuarios que son miembros de varios grupos con términos y condiciones diferentes. Está **desactivado** de forma predeterminada.

Directiva de VPN

January 4, 2022

La directiva “VPN” permite 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 VPN para las plataformas siguientes. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en este artículo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos para las redes VPN por aplicación

Puede configurar la función de VPN por aplicación para estas plataformas a través de directivas VPN:

- iOS
- macOS
- Android (AD heredado)
- Samsung SAFE
- Samsung Knox

Para configurar redes VPN para dispositivos Android Enterprise, cree una directiva Configuraciones administradas por Android Enterprise para la aplicación Citrix SSO. Consulte Configurar perfiles de VPN para Android Enterprise.

Las opciones de VPN por aplicación están disponibles para ciertos tipos de conexión. Esta tabla indica cuándo están disponibles las opciones de VPN por aplicación.

Platform	Tipo de conexión	Comentario
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO o SSL personalizado.	
macOS	Cisco AnyConnect, Juniper SSL, SSL F5, SonicWALL Mobile Connect, Ariba VIA o SSL personalizado.	
Android (AD heredado)	Citrix SSO	
Samsung SAFE	IPsec, SSL	Tipo de VPN establecido en **Genérico**
Samsung Knox	IPsec, SSL	Tipo de VPN establecido en **Genérico**

Para crear una VPN por aplicación en dispositivos iOS y Android (AD heredado) mediante la aplicación Citrix SSO, debe realizar otros pasos, además de la configuración de la directiva VPN. Además, debe comprobar que se cumplen estos requisitos previos:

- Dispositivo Citrix Gateway local
- Estas aplicaciones están instaladas en el dispositivo:
  - Citrix SSO
  - Citrix Secure Hub

He aquí un flujo de trabajo general para configurar una VPN por aplicación en dispositivos iOS y Android mediante la aplicación Citrix SSO:

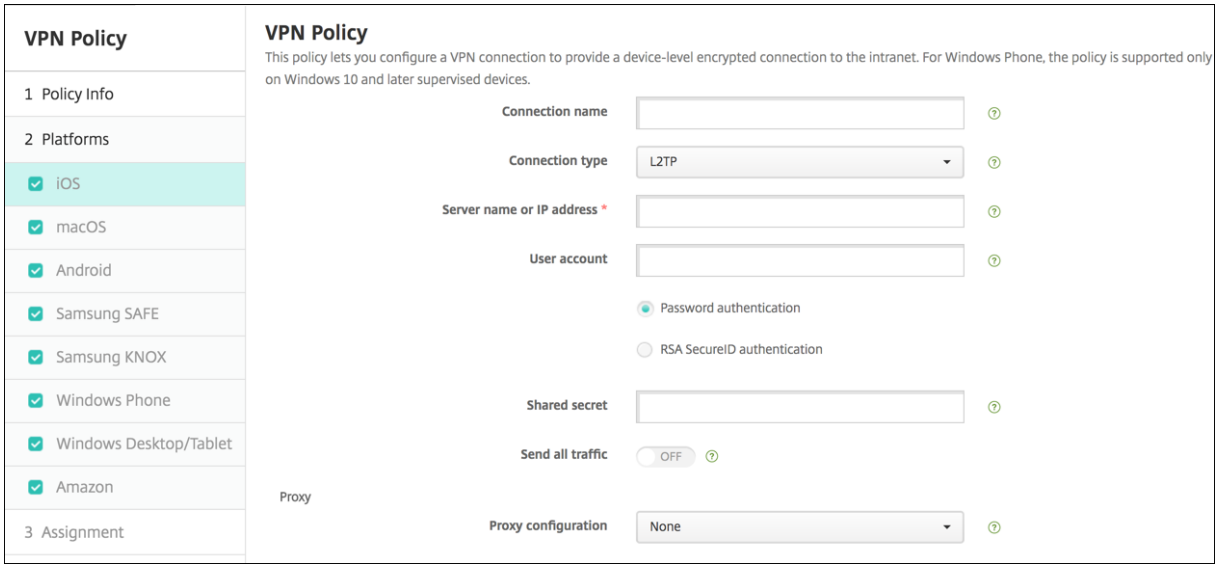
1. Configure una directiva de dispositivos VPN tal y como se describe en este artículo.
   - Para *iOS*, consulte Configurar el protocolo Citrix SSO para iOS. Después de configurar el protocolo de Citrix SSO para iOS a través de una directiva de dispositivos VPN, también debe crear una directiva de atributos de aplicación para asociar las aplicaciones a la directiva VPN por aplicación. Para obtener más información, consulte Configurar una VPN por aplicación.
     - Para el campo **Tipo de autenticación para la conexión**, si selecciona **Certificado**, primero debe configurar la autenticación por certificado para Endpoint Management. Consulte Autenticación con certificado de cliente o certificado y dominio.
   - Para *Android (AD heredado)*, consulte Configurar el protocolo Citrix SSO para Android.
     - Para el campo **Tipo de autenticación para la conexión**, si selecciona **Certificado** o **Contraseña y certificado**, primero debe configurar la autenticación por certificado para Endpoint Management. Consulte Autenticación con certificado de cliente o certificado y dominio.
2. Configure Citrix ADC para aceptar el tráfico de la VPN por aplicación. Para obtener información detallada, consulte Configuración de VPN completa en Citrix Gateway.

Parámetros de iOS

> **Con respecto a las actualizaciones de dispositivos a iOS 12**
>
> , tenga en cuenta que el tipo de conexión VPN de Citrix en la directiva de VPN para iOS no admite iOS 12. Lleve a cabo estos pasos para eliminar la directiva de VPN existente y crear otra directiva de VPN con el tipo de conexión Citrix SSO:
>
> 1. Elimine su directiva de VPN para iOS.
> 2. Agregue una directiva de VPN para iOS. Configuraciones importantes:
>   - **Connection type** = **Citrix SSO**
>   - **Enable per-app VPN** = **On**

- **Provider type** = **Packet tunnel**

3. Agregue una directiva de atributos de aplicaciones para iOS. En **Identificador de VPN por aplicación**, elija **iOS_VPN**.



- **Nombre de la conexión:** Escriba un nombre para la conexión.
- **Tipo de conexión:** En la lista, seleccione 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 Legacy AnyConnect.** Este tipo de conexión requiere que el cliente VPN de Cisco Legacy AnyConnect esté instalado en el dispositivo del usuario. Cisco ha empezado a retirar progresivamente el cliente Cisco Legacy AnyConnect, basado en un framework de VPN que se ha retirado. Para obtener más información, consulte este artículo de asistencia: https://support.citrix.com/article/CTX227708.
    Para utilizar el cliente actual de Cisco AnyConnect, use el **Tipo de conexión** llamado **SSL personalizado**. Para conocer la configuración requerida, consulte “Configurar el protocolo SSL personalizado” en esta sección.
  - **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 (solo iOS).** Intercambio de claves por red versión 2 solo para iOS.
  - **AlwaysOn IKEv2:** Acceso permanente mediante IKEv2.
  - **Configuración dual de AlwaysOn IKEv2:** Acceso permanente mediante la configuración

dual de IKEv2.
- **Citrix SSO:** Cliente de Citrix SSO para iOS 12 y versiones posteriores.
- **SSL personalizado:** Capa de sockets seguros (SSL) personalizada. Se requiere este tipo de conexión para el cliente Cisco AnyConnect que tiene un ID de paquete **com.cisco.anyconnect**. Indique el **Nombre de conexión** llamado **Cisco AnyConnect**. También puede implementar la directiva de VPN y habilitar un filtro de Control de acceso a red (NAC) para dispositivos iOS. El filtro NAC bloquea una conexión VPN para dispositivos que tienen instaladas aplicaciones no conformes. La configuración requiere configuraciones específicas para la directiva de VPN de iOS, como se describe en la siguiente sección de iOS. Para obtener más información sobre otras configuraciones necesarias para habilitar el filtro NAC, consulte Control de acceso a red.

En las siguientes secciones se ofrecen las opciones de configuración para cada uno de los tipos de conexión mencionados.

Configurar el protocolo L2TP para iOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación por contraseña** o **Autenticación con RSA SecureID**.
- **Secreto compartido:** Escriba la clave de secreto compartido de IPsec.
- **Enviar todo el tráfico:** Seleccione si enviar todo el tráfico por la red privada virtual (VPN). Está **desactivado** de forma predeterminada.

Configurar el protocolo PPTP para iOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación por contraseña** o **Autenticación con RSA SecureID**.
- **Nivel de cifrado.** En la lista, seleccione un nivel de cifrado. El valor predeterminado es **Ninguno**.
  - **Ninguno:** No se usa ningún cifrado.
  - **Automático:** Se usa el nivel más alto de cifrado que admite el servidor.
  - **Máximo (128 bits):** Se usa siempre el cifrado de 128 bits.
- **Enviar todo el tráfico:** Seleccione si enviar todo el tráfico por la red privada virtual (VPN). Está **desactivado** de forma predeterminada.

Configurar el protocolo IPsec para iOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.

- **Tipo de autenticación para la conexión:** En la lista, seleccione **Secreto compartido** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Secreto compartido**.
- Si ha seleccionado **Secreto compartido**, configure los siguientes parámetros:
  - **Nombre del grupo:** Escriba un nombre de grupo opcional.
  - **Secreto compartido:** Escriba una clave opcional de secreto compartido.
  - **Usar autenticación híbrida:** Seleccione si utilizar la autenticación híbrida. Con la autenticación híbrida, el servidor se autentica primero en el cliente, y, a continuación, se autentica en el servidor. Está **desactivado** de forma predeterminada.
  - **Pedir contraseña:** Seleccione si solicitar a los usuarios sus contraseñas cuando se conectan a la red. Está **desactivado** de forma predeterminada.
- Si habilita **Certificado**, defina las siguientes configuraciones:
  - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
  - **Pedir PIN al conectar:** Seleccione esta opción para obligar a los usuarios a introducir su PIN cuando se conecten a la red. Está **desactivado** de forma predeterminada.
  - **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada.
- **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. Está **desactivado** de forma predeterminada.
- **Dominios de Safari:** Haga clic en **Agregar** para agregar un nombre de dominio de Safari.

Configurar el protocolo Cisco Legacy AnyConnect para iOS

Para realizar la transición del cliente Cisco Legacy AnyConnect al nuevo cliente Cisco AnyConnect, use el protocolo “SSL personalizado”.

- **Identificador de paquete de proveedor.** Para el cliente Legacy AnyConnect, el ID de paquete es com.cisco.anyconnect.gui.
- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Grupo:** Escriba un nombre de grupo opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.

  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, defina las siguientes configuraciones:
    * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.
    * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, defina las siguientes configuraciones:
  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. Está **desactivado** de forma predeterminada.
  - **Tipo de proveedor:** Seleccione si la VPN por aplicación se ofrece como **proxy de aplicación** o como **túnel de paquete**. El valor predeterminado es **Proxy de aplicación**.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
    * **Dominio:** Escriba el dominio que se va a agregar.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo Juniper SSL para iOS

- **Identificador de paquetes de proveedor:** Si el perfil de su VPN por aplicación contiene el identificador de paquetes de una aplicación con varios proveedores de VPN del mismo tipo, especifique el proveedor que quiere utilizar aquí.
- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Territorio:** Escriba un nombre opcional para el territorio Kerberos.
- **Rol:** Escriba un nombre opcional para el rol.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.

  - Si habilita **Certificado**, defina las siguientes configuraciones:
    * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.
    * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, defina las siguientes configuraciones:
  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. Está **desactivado** de forma predeterminada.
  - **Tipo de proveedor:** Seleccione si la VPN por aplicación se ofrece como **proxy de aplicación** o como **túnel de paquete**. El valor predeterminado es **Proxy de aplicación**.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
    * **Dominio:** Escriba el dominio que se va a agregar.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo F5 SSL para iOS

- **Identificador de paquetes de proveedor:** Si el perfil de su VPN por aplicación contiene el identificador de paquetes de una aplicación con varios proveedores de VPN del mismo tipo, especifique el proveedor que quiere utilizar aquí.
- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, defina las siguientes configuraciones:
    * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se

conectan a la red. Está **desactivado** de forma predeterminada.
    * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, defina las siguientes configuraciones:
  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
  - **Tipo de proveedor:** Seleccione si la VPN por aplicación se ofrece como **proxy de aplicación** o como **túnel de paquete**. El valor predeterminado es **Proxy de aplicación**.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
    * **Dominio:** Escriba el dominio que se va a agregar.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo SonicWALL para iOS

- **Identificador de paquetes de proveedor:** Si el perfil de su VPN por aplicación contiene el identificador de paquetes de una aplicación con varios proveedores de VPN del mismo tipo, especifique el proveedor que quiere utilizar aquí.
- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Dominio o grupo de inicio de sesión:** Escriba un dominio o grupo opcional de inicio de sesión.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, defina las siguientes configuraciones:
    * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.
    * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción

Habilitar VPN a demanda está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.

- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, configure los siguientes parámetros:
  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
  - **Tipo de proveedor:** Seleccione si la VPN por aplicación se ofrece como **proxy de aplicación** o como **túnel de paquete**. El valor predeterminado es **Proxy de aplicación**.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
    * **Dominio:** Escriba el dominio que se va a agregar.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo Ariba VIA para iOS

- **Identificador de paquetes de proveedor:** Si el perfil de su VPN por aplicación contiene el identificador de paquetes de una aplicación con varios proveedores de VPN del mismo tipo, especifique el proveedor que quiere utilizar aquí.
- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, defina las siguientes configuraciones:
    * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.
    * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, defina las siguientes configuraciones:

  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
    * **Dominio:** Escriba el dominio que se va a agregar.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar protocolos IKEv2 para iOS

Esta sección incluye parámetros utilizados para los protocolos IKEv2, AlwaysOn IKEv2 y AlwaysOn IKEv2 Dual Configuration. Para el protocolo de configuración dual AlwaysOn IKEv2, configure todos estos parámetros tanto para redes móviles como para redes Wi-Fi.

- **Permitir que el usuario inhabilite la conexión automática:** Para protocolos AlwaysOn. Seleccione si permitir a los usuarios que desactiven la conexión automática a la red en sus dispositivos. Está **desactivado** de forma predeterminada.
- **Nombre de host o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Identificador local:** El FQDN o la dirección IP del cliente IKEv2. Este campo es obligatorio.
- **Identificador remoto:** El FQDN o la dirección IP del servidor VPN. Este campo es obligatorio.
- **Autenticación del dispositivo:** Seleccione **Secreto compartido**, **Certificado** o **Certificado de dispositivo basado en la identidad del dispositivo** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Secreto compartido**.
  - Si elige **Secreto compartido**, escriba una clave opcional de secreto compartido.
  - Si elige **Certificado**, elija la **Credencial de identidad** que quiere utilizar. El valor predeterminado es **Ninguno**.
  - Si elige **Certificado de dispositivo basado en la identidad del dispositivo**, seleccione el **Tipo de identidad del dispositivo** que quiere utilizar. El valor predeterminado es **IMEI**. Para utilizar esta opción, importe certificados en bloque con la API de REST. Consulte Cargar en bloque certificados en dispositivos iOS con la API de REST. Solo está disponible si selecciona **Always On IKEv2**.
- **Autenticación extendida habilitada:** Seleccione si habilitar el Protocolo de autenticación extensible (EAP). Si lo **activa**, escriba la **Cuenta de usuario** y la **Contraseña de autenticación**.
- **Intervalo DPD (Dead Peer Detection):** Seleccione la frecuencia con que un nodo establece contacto con otro del mismo nivel con el fin de garantizar que este permanece contactable. El valor predeterminado es **Ninguno**. Las opciones son:

  - **Ninguno:** Inhabilita la opción Dead Peer Detection (detección de actividad en un nodo del mismo nivel).
  - **Bajo:** Establece contacto con un nodo del mismo nivel cada 30 minutos.
  - **Medio:** Establece contacto con un nodo del mismo nivel cada 10 minutos.
  - **Alto:** Establece contacto con un nodo del mismo nivel cada minuto.
- **Inhabilitar movilidad y multihoming:** Seleccione si inhabilitar esta función.
- **Utilizar atributos de subred interna IPv4/IPv6:** Seleccione si habilitar esta función.
- **Inhabilitar redirecciones:** Seleccione si inhabilitar las redirecciones.
- **Habilitar NAT Keep-Alive mientras el dispositivo está en modo de suspensión:** Para los protocolos AlwaysOn. Los paquetes Keep-Alive mantienen las asignaciones NAT para las conexiones IKEv2. El chip envía esos paquetes regularmente cuando el dispositivo está activado. Si este parámetro está activado, el chip envía paquetes Keep-Alive incluso aunque el dispositivo esté en modo de suspensión. El intervalo predeterminado es de 20 segundos por Wi-Fi y 110 segundos por red móvil. Puede cambiar el intervalo con el parámetro Intervalo de NAT Keep-Alive.
- **Intervalo de NAT Keep-Alive (segundos):** El valor predeterminado es de 20 segundos.
- **Habilitar PFS (Perfect Forward Secrecy):** Seleccione si habilitar esta función.
- **Direcciones IP de servidores DNS.** Opcional. Una lista de cadenas de direcciones IP pertenecientes a servidores DNS. Estas direcciones IP pueden incluir una mezcla de direcciones IPv4 e IPv6. Haga clic en **Agregar** para escribir una dirección.
- **Nombre de dominio.** Opcional. El dominio principal del túnel.
- **Dominios de búsqueda.** Opcional. Una lista de dominios que se utiliza para calificar totalmente los nombres de host de etiqueta única.
- **Agregar dominios complementarios a la lista de resolución:** Opcional. Determina si agregar la lista de dominios suplementarios de correspondencia a la lista de dominios de búsqueda para la resolución. De forma predeterminada, está **activado**.
- **Dominios suplementarios de correspondencia.** Opcional. Una lista de los dominios que se utilizan para determinar qué consultas DNS van a usar los parámetros de resolución DNS que contienen las direcciones de servidor DNS. Esta clave crea una configuración de DNS dividido donde solo los hosts de dominios determinados van a resolverse mediante la resolución DNS del túnel. Los hosts que no consten en uno de los dominios de esta lista se resuelven con la resolución predeterminada del sistema.

Si este parámetro contiene una cadena vacía, esa cadena se utilizará como el dominio predeterminado. Así es como una configuración de túnel dividido puede dirigir todas las consultas DNS a los

servidores DNS de las redes VPN antes de dirigirlas a los servidores DNS principales. Si el túnel VPN es la ruta predeterminada de la red, los servidores DNS de la lista pasan a ser la resolución predeterminada. En ese caso, se ignora la lista de los dominios complementarios de correspondencia.

- **Parámetros de IKE SA** y **Parámetros de Child SA**. Configure estos parámetros para cada opción de asociación de seguridad (SA):
  - **Algoritmo de cifrado:** En la lista, seleccione el algoritmo de cifrado IKE que se va a usar. El valor predeterminado es **3DES**.
  - **Algoritmo de integridad:** En la lista, seleccione el algoritmo de integridad que se va a usar. El valor predeterminado es **SHA1-96**.
  - **Grupo Diffie-Hellman:** En la lista, seleccione el número de grupo de Diffie Hellman. El valor predeterminado es **2**.
  - **Tiempo de vida de IKE (en minutos):** Escriba un número entero comprendido entre 10 y 1440 que represente la vigencia de la asociación de seguridad (intervalo de regeneración de claves). El valor predeterminado es **1440** minutos.
- **Excepciones de servicios.** Para los protocolos AlwaysOn. Las excepciones de servicios son aquellos servicios del sistema que se eximen de la VPN de AlwaysOn. Configure estos parámetros de excepciones de servicios:
  - **Correo de voz:** En la lista, seleccione cómo gestionar la excepción del correo de voz. El valor predeterminado es **Permitir tráfico a través de túnel**.
  - **AirPrint:** En la lista, seleccione cómo gestionar la excepción de AirPrint. El valor predeterminado es **Permitir tráfico a través de túnel**.
  - **Permitir tráfico desde hojas Web cautivas fuera del túnel VPN**. Seleccione si permitir que los usuarios se conecten a puntos de acceso a Internet (hotspots) públicos que se encuentren fuera del túnel VPN. Está **desactivado** de forma predeterminada.
  - **Permitir tráfico desde todas las aplicaciones de redes cautivas fuera del túnel VPN:** Seleccione si permitir todas las aplicaciones provenientes de hotspots que se encuentren fuera del túnel VPN. Está **desactivado** de forma predeterminada.
  - **Identificadores de paquetes de aplicaciones de redes cautivas:** Para cada ID de paquete de aplicación de red de hotspot al que los usuarios tengan autorizado el acceso, haga clic en **Agregar** y escriba el **Identificador de paquete** de aplicación relativo a la red del hotspot. Haga clic en **Guardar** para guardar el identificador del paquete de aplicación.
- **VPN por aplicación**: Configure estos parámetros para los tipos de conexión IKEv2.
  - **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada.

  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. Está **desactivado** de forma predeterminada.
  - **Dominios de Safari:** Haga clic en **Agregar** para agregar un nombre de dominio de Safari.

- **Configuración de proxy.** Seleccione cómo se enruta la conexión VPN a través de un servidor proxy. El valor predeterminado es **Ninguno**.

Configurar el protocolo Citrix SSO para iOS

El cliente de Citrix SSO está disponible https://apps.apple.com/us/app/citrix-sso/id1333396910 en el Apple Store.

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, defina las siguientes configuraciones:
    * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.
    * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, configure los siguientes parámetros:
  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
  - **Tipo de proveedor:** Seleccione si la VPN por aplicación se ofrece como **proxy de aplicación** o como **túnel de paquete**. El valor predeterminado es **Proxy de aplicación**.
  - **Tipo de proveedor:** Establezca la configuración en **Túnel de paquete**.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:

        * **Dominio:** Escriba el dominio que se va a agregar.
        * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **XML personalizado:** Haga clic en **Agregar** y especifique los pares clave/valor para agregar cada parámetro XML personalizado. Los parámetros disponibles son:
  - **disableL3:** Inhabilita conexiones VPN a nivel del sistema. Permite únicamente conexiones VPN por aplicación. No se necesita ningún **Valor**.
  - **useragent:** Asocia, a esta directiva, las directivas de Citrix Gateway dirigidas a clientes con plug-in VPN. El **Valor** de esta clave se agrega automáticamente al plug-in VPN para las solicitudes iniciadas por el plug-in.

Configurar el protocolo SSL personalizado para iOS

Para realizar la transición del cliente Cisco Legacy AnyConnect al nuevo cliente Cisco AnyConnect:

1. Configure la directiva de VPN con el protocolo SSL personalizado. Implemente esa directiva en los dispositivos iOS.
2. Cargue el cliente Cisco AnyConnect desde https://apps.apple.com/us/app/cisco-anyconnect/id1135064690, agregue la aplicación a XenMobile y, a continuación, impleméntela en los dispositivos iOS.
3. Quite la directiva de VPN antigua que hubiera en los dispositivos iOS.

Parámetros:

- **Identificador de SSL personalizado (formato DNS inverso).** Establézcalo en el ID del paquete. Para el cliente Cisco AnyConnect, use **com.cisco.anyconnect**.
- **Identificador de paquete de proveedor.** Si la aplicación especificada en **Identificador de SSL personalizado** tiene varios proveedores VPN del mismo tipo (proxy de aplicación o túnel de paquetes), especifique este identificador de paquete. Para el cliente Cisco AnyConnect, use **com.cisco.anyconnect**.
- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, defina las siguientes configuraciones:
    * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.

        * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, configure los siguientes parámetros:
  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
  - **Tipo de proveedor.** El tipo de proveedor indica si este es un servicio proxy o un servicio VPN. Para el servicio VPN, elija **Túnel de paquete**. Para el servicio proxy, elija **Proxy de aplicación**. Para el cliente Cisco AnyConnect, elija **Túnel de paquete**.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
    * **Dominio:** Escriba el dominio que se va a agregar.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **XML personalizado:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada parámetro XML personalizado:
  - **Nombre del parámetro:** Escriba el nombre del parámetro que se va a agregar.
  - **Valor:** Escriba el valor asociado al **Nombre del parámetro**.
  - Haga clic en **Guardar** para guardar el parámetro, o bien haga clic en **Cancelar** para no guardarlo.

Configurar la directiva de VPN para admitir NAC

1. Se requiere el **Tipo de conexión** de **SSL personalizado** para configurar el filtro NAC.
2. Especifique **VPN** como **Nombre de conexión**.
3. En **Identificador de SSL personalizado**, escriba **com.citrix.NetScalerGateway.ios.app**
4. En **Identificador de paquete de proveedor**, escriba **com.citrix.NetScalerGateway.ios.app.vpnplugin**

Los valores de los pasos 3 y 4 se toman de la instalación requerida de Citrix SSO para el filtrado de NAC. No se configura una contraseña de autenticación. Para obtener más información sobre el uso de la función NAC, consulte Control de acceso a red.

Configurar opciones de Habilitar VPN a demanda para iOS

- **Dominio a demanda:** Por cada dominio y acción asociada que deben realizarse cuando los usuarios se conecten, pinche en **Agregar** y haga lo siguiente:

- **Dominio:** Escriba el dominio que se va a agregar.
- **Acción:** En la lista, seleccione en una de las posibles acciones:
  - **Establecer siempre:** El dominio siempre activa una conexión VPN.
  - **No establecer nunca:** El dominio no activa nunca una conexión VPN.
  - **Establecer si es necesario:** El dominio activa un intento de conexión VPN si falla la resolución de nombres de dominio. El error ocurre cuando el servidor DNS no puede resolver el dominio, redirige a un servidor diferente o agota el tiempo de espera.
  - Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **Reglas a demanda**
  - **Acción:** En la lista, seleccione la acción que se debe realizar. El valor predeterminado es **EvaluateConnection**. Las acciones posibles son:
    - **Permitir:** Al activarse, permite que la VPN a demanda se conecte.
    - **Conectar:** Inicia incondicionalmente una conexión VPN.
    - **Desconectar:** Quita la conexión VPN y no vuelve a conectarse a demanda mientras la regla se cumpla.
    - **EvaluateConnection:** Evalúa la matriz ActionParameters para cada conexión.
    - **Ignorar:** Deja activa cualquier conexión VPN existente, pero no vuelve a conectarse a demanda mientras la regla se cumpla.
  - **DNSDomainMatch:** Para agregar cada dominio que se va a cotejar con la lista de búsqueda de dominios de un dispositivo, haga clic en **Agregar** y lleve a cabo lo siguiente:
    - **Dominio DNS:** Escriba el nombre del dominio. Puede usar el prefijo comodín "*" para abarcar varios dominios. Por ejemplo: *.ejemplo.com abarca midominio.ejemplo.com, tudominio.ejemplo.com y sudominio.ejemplo.com.
    - Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
  - **DNSServerAddressMatch:** Para agregar cada dirección IP con la que puede coincidir cualquier servidor DNS indicado en la red, haga clic en **Agregar** y lleve a cabo lo siguiente:
    - **Dirección del servidor DNS:** Escriba la dirección del servidor DNS que quiere agregar. Puede usar el sufijo comodín "*" para abarcar varios servidores DNS. Por ejemplo: 17.* abarca cualquier servidor DNS incluido en la subred de clase A.
    - Haga clic en **Guardar** para guardar el servidor DNS, o bien haga clic en **Cancelar** para no guardarlo.
  - **InterfaceTypeMatch:** En la lista, seleccione el tipo de hardware de interfaz de red principal que se está utilizando. El valor predeterminado es **No especificado**. Los valores posibles son:
    - **No especificado:** Coincide con cualquier hardware de interfaz de red. Esta es la opción predeterminada.
    - **Ethernet:** Solo coincide con el hardware de interfaz de red Ethernet.

    * **Wi-Fi:** Solo coincide con el hardware de interfaz de red Wi-Fi.
    * **Móvil:** Solo coincide con el hardware de interfaz de red móvil.
- **SSIDMatch:** Haga clic en **Agregar** y haga lo siguiente para agregar cada SSID que se va a cotejar con la red actual.
    * **SSID:** Escriba el SSID que se va a agregar. Si no se trata de una red Wi-Fi, o bien si el SSID no aparece, el cotejo falla. Deje esta lista vacía para que abarque cualquier SSID.
    * Haga clic en **Guardar** para guardar el SSID, o bien haga clic en **Cancelar** para descartarlo.
- **URLStringProbe:** Escriba una URL a capturar. Si la URL se captura correctamente sin redirección, se cumple esta regla.
- **ActionParameters: Domains:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada dominio que va a comprobar EvaluateConnection:
    * **Dominio:** Escriba el dominio que se va a agregar.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **ActionParameters: DomainAction:** En la lista, seleccione el **comportamiento de la red VPN** correspondiente para los dominios especificados en **ActionParameters: Domains**. El valor predeterminado es **ConnectIfNeeded**. Las acciones posibles son:
    * **ConnectIfNeeded:** El dominio activa un intento de conexión VPN si falla la resolución de nombres de dominio. El error ocurre cuando el servidor DNS no puede resolver el dominio, redirige a un servidor diferente o agota el tiempo de espera.
    * **NeverConnect:** El dominio no activa nunca una conexión VPN.
- **Action Parameters: RequiredDNSServers:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada dirección IP del servidor DNS que se va a usar para resolver los dominios especificados:
    * **Servidor DNS:** Solo válido si **ActionParameters** : **DomainAction** es **ConnectIfNeeded**. Escriba el servidor DNS que se va a agregar. No es necesario que este servidor forme parte de la configuración de red actual del dispositivo. Si el servidor DNS no es accesible, se establece una conexión VPN. Este debe ser un servidor DNS interno o un servidor DNS externo de confianza.
    * Haga clic en **Save** para guardar el servidor DNS, o bien haga clic en **Cancel** para no guardarlo.
- **ActionParameters : RequiredURLStringProbe:** Si quiere, escriba una URL en formato HTTP o HTTPS (preferentemente este) para llevar a cabo un sondeo con la ayuda de una solicitud GET. Si el nombre de host de la URL no se puede resolver, o si el servidor es inaccesible o el servidor no responde, se establece una conexión VPN. Válido solamente si **ActionParameters**: **DomainAction** = **ConnectIfNeeded**.
- **OnDemandRules : XML content.** Escriba o copie y pegue las reglas a demanda de la configuración XML.

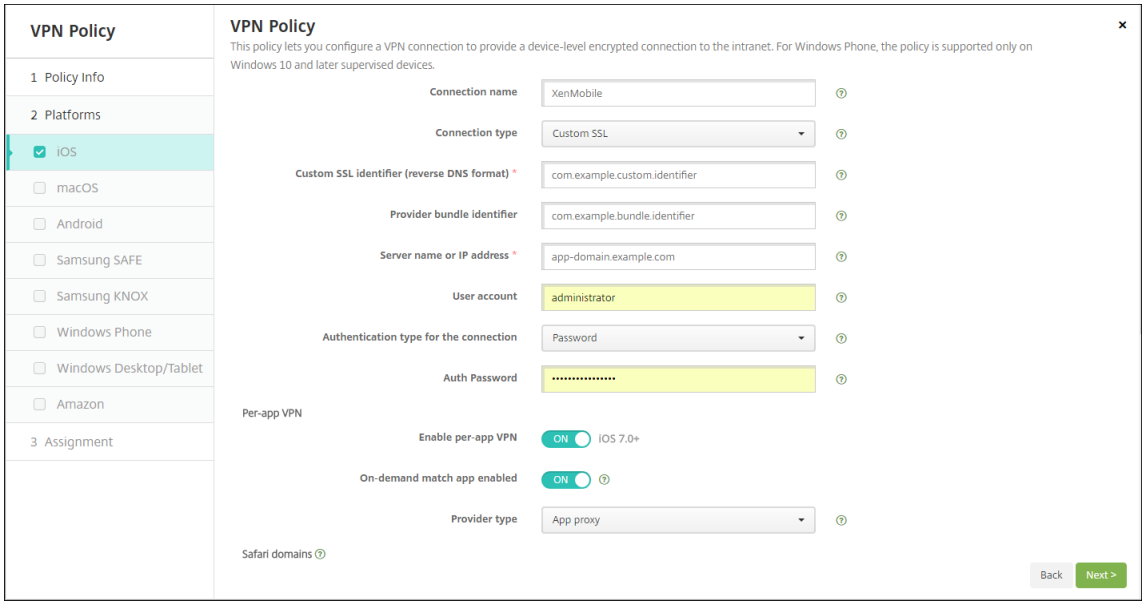
        * Haga clic en **Diccionario de comprobación** para validar la sintaxis del código XML. Puede ver el mensaje "XML válido" en verde debajo del cuadro de texto de **Contenido XML** si el XML es válido. Si no es válido, verá un mensaje de error en texto en naranja que describe el error.
- **Proxy**
  - **Configuración de proxy:** En la lista, seleccione cómo se redirige la conexión VPN a través de un servidor proxy. El valor predeterminado es **Ninguno**.
    * Si habilita **Manual**, configure los siguientes parámetros:
      · **Nombre de host o dirección IP del servidor proxy:** Escriba el nombre de host o la dirección IP del servidor proxy. Este campo es obligatorio.
      · **Puerto del servidor proxy.** Escriba el número de puerto del servidor proxy. Este campo es obligatorio.
      · **Nombre de usuario:** Escriba un nombre de usuario opcional para el servidor proxy.
      · **Contraseña:** Escriba una contraseña opcional de servidor proxy.
    * Si selecciona **Automático**, configure este parámetro:
      · **URL del servidor proxy:** Escriba la URL del servidor proxy. Este campo es obligatorio.
- **Configuraciones de directivas**
  - En **Configuraciones de directivas**, junto a **Quitar directiva**, haga clic en **Seleccionar fecha** o **Demora hasta la eliminación (en horas)**.
  - Si selecciona **Seleccionar fecha**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
  - En la lista Permite **al usuario quitar la directiva**, seleccione **Siempre**, **Requerir código de acceso** o **Nunca**.
  - Si selecciona **Requerir código de acceso**, junto a **Código de acceso para la eliminación**, introduzca la contraseña en cuestión.

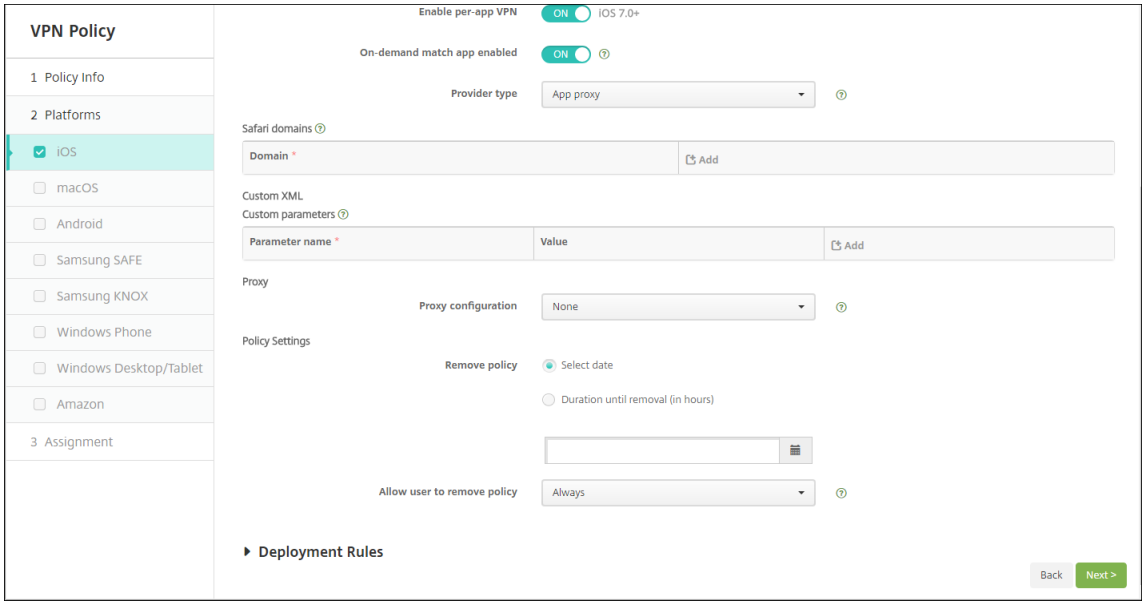
Configurar una VPN por aplicación

Las opciones de VPN por aplicación para iOS están disponibles para estos tipos de conexión: Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, Citrix SSO y SSL personalizado.

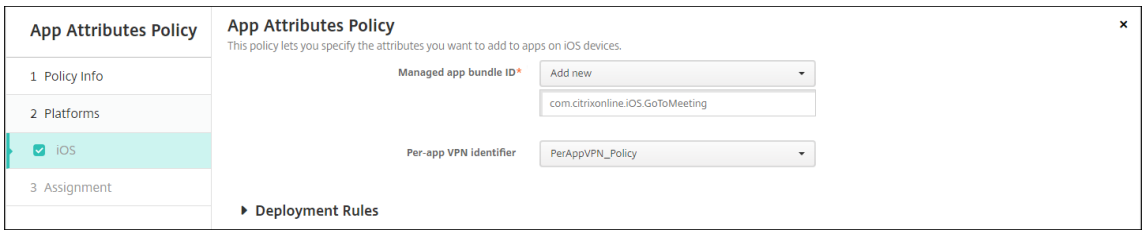
Para configurar una VPN por aplicación:

1. En **Configurar > Directivas de dispositivo**, cree una directiva de red VPN. Por ejemplo:



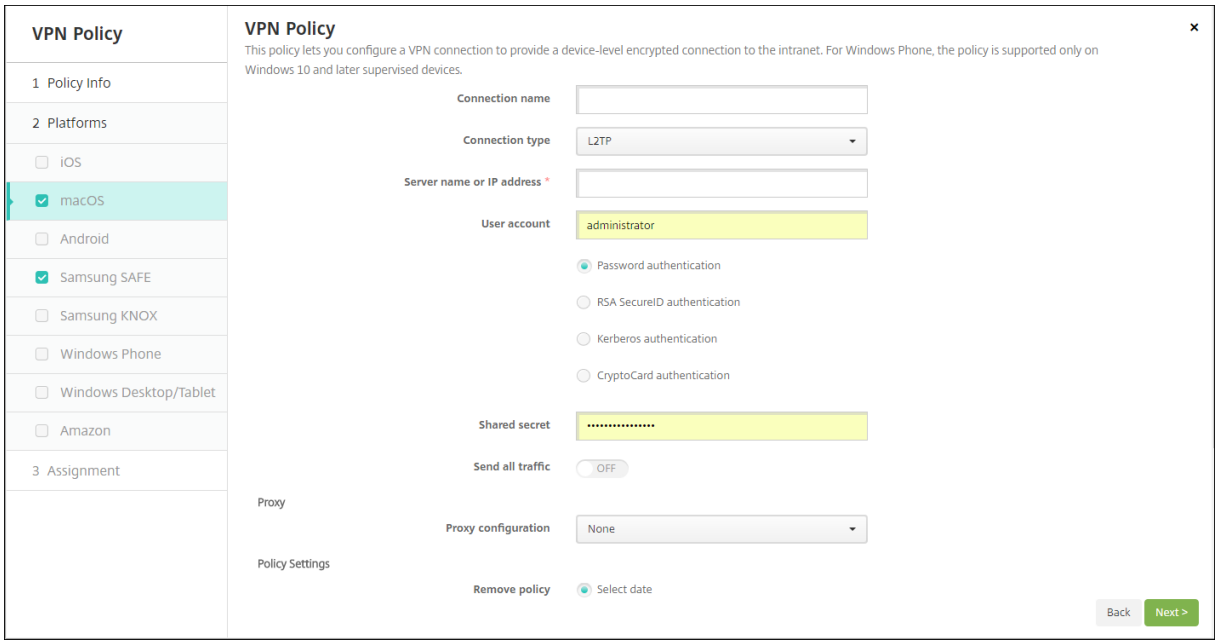


2. En **Configurar > Directivas de dispositivo**, cree una directiva de atributos de aplicaciones para asociar una aplicación a la directiva de VPN por aplicación. Para **Identificador de VPN por aplicación**, elija el nombre de la directiva de VPN creada en el paso 1. Para **ID de paquete de la aplicación administrada**, elija un ID de la lista de aplicaciones o introduzca el ID de paquete de aplicación (si implementa una directiva Inventario de aplicaciones en iOS, la lista contendrá aplicaciones).



- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de macOS



- **Nombre de la conexión:** Escriba un nombre para la conexión.
- **Tipo de conexión:** En la lista, seleccione 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 de Cisco AnyConnect.

  - **Juniper SSL:** Cliente SSL VPN de Juniper Networks.
  - **F5 SSL:** Cliente SSL VPN de F5 Networks.
  - **SonicWALL Mobile Connect:** Cliente VPN unificado de Dell para iOS.
  - **Ariba VIA:** Cliente de acceso virtual a Internet de Ariba Networks.
  - **Citrix VPN:** Cliente VPN de Citrix.
  - **SSL personalizado:** Capa de sockets seguros (SSL) personalizada.

En las siguientes secciones se ofrecen las opciones de configuración para cada uno de los tipos de conexión mencionados.

Configurar el protocolo L2TP para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación por contraseña**, **Autenticación con RSA SecureID**, **Autenticación Kerberos** o **Autenticación CryptoCard**. El valor predeterminado es **Autenticación por contraseña**.
- **Secreto compartido:** Escriba la clave de secreto compartido de IPsec.
- **Enviar todo el tráfico:** Seleccione si enviar todo el tráfico por la red privada virtual (VPN). Está **desactivado** de forma predeterminada.

Configurar el protocolo PPTP para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación por contraseña**, **Autenticación con RSA SecureID**, **Autenticación Kerberos** o **Autenticación CryptoCard**. El valor predeterminado es **Autenticación por contraseña**.
- **Nivel de cifrado.** Seleccione el nivel de cifrado pertinente. El valor predeterminado es **Ninguno**.
  - **Ninguno:** No se usa ningún cifrado.
  - **Automático:** Se usa el nivel más alto de cifrado que admite el servidor.
  - **Máximo (128 bits):** Se usa siempre el cifrado de 128 bits.
- **Enviar todo el tráfico:** Seleccione si enviar todo el tráfico por la red privada virtual (VPN). Está **desactivado** de forma predeterminada.

Configurar el protocolo IPsec para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.

- **Tipo de autenticación para la conexión:** En la lista, seleccione **Secreto compartido** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Secreto compartido**.
  - Si habilita la autenticación **Secreto compartido**, configure los siguientes parámetros:
    - **Nombre del grupo:** Escriba un nombre de grupo opcional.
    - **Secreto compartido:** Escriba una clave opcional de secreto compartido.
    - **Usar autenticación híbrida:** Seleccione si utilizar la autenticación híbrida. Con la autenticación híbrida, el servidor se autentica primero en el cliente, y, a continuación, se autentica en el servidor. Está **desactivado** de forma predeterminada.
    - **Pedir contraseña:** Seleccione si solicitar a los usuarios sus contraseñas cuando se conectan a la red. Está **desactivado** de forma predeterminada.
  - Si habilita la autenticación **Certificado**, configure los siguientes parámetros:
    - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    - **Pedir PIN al conectar:** Seleccione esta opción para obligar a los usuarios a introducir su PIN cuando se conecten a la red. Está **desactivado** de forma predeterminada.
    - **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.

Configurar el protocolo Cisco AnyConnect para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Grupo:** Escriba un nombre de grupo opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, defina las siguientes configuraciones:
    - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    - **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.
    - **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar

VPN a demanda.

- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, defina las siguientes configuraciones:
  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. Está **desactivado** de forma predeterminada.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
    - **Dominio:** Escriba el dominio que se va a agregar.
    - Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo Juniper SSL para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Territorio:** Escriba un nombre opcional para el territorio Kerberos.
- **Rol:** Escriba un nombre opcional para el rol.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, defina las siguientes configuraciones:
    - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    - **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.
    - **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, configure los siguientes parámetros:
  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. Está **desactivado** de forma

predeterminada.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
    * **Dominio:** Escriba el dominio que se va a agregar.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo F5 SSL para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, defina las siguientes configuraciones:
    * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.
    * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, defina las siguientes configuraciones:
  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. Está **desactivado** de forma predeterminada.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
    * **Dominio:** Escriba el dominio que se va a agregar.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo SonicWALL Mobile Connect para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Dominio o grupo de inicio de sesión:** Escriba un dominio o grupo opcional de inicio de sesión.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, defina las siguientes configuraciones:
    - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    - **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.
    - **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, defina las siguientes configuraciones:
  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. Está **desactivado** de forma predeterminada.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
    - **Dominio:** Escriba el dominio que se va a agregar.
    - Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo Ariba VIA para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.

  - Si habilita **Certificado**, defina las siguientes configuraciones:
    * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.
    * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, defina las siguientes configuraciones:
  - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. Está **desactivado** de forma predeterminada.
  - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
    * **Dominio:** Escriba el dominio que se va a agregar.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo SSL personalizado para macOS

- **Identificador de SSL personalizado (formato DNS inverso).** Escriba el identificador de SSL en formato DNS inverso. Este campo es obligatorio.
- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN. Este campo es obligatorio.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
  - **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, defina las siguientes configuraciones:
    * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
    * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. Está **desactivado** de forma predeterminada.

        * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. Está **desactivado** de forma predeterminada. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.
    - **VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Está **desactivado** de forma predeterminada. Si activa esta opción, defina las siguientes configuraciones:
        * **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
        * **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
            · **Dominio:** Escriba el dominio que se va a agregar.
            · Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **XML personalizado:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada parámetro XML personalizado:
    - **Nombre del parámetro:** Escriba el nombre del parámetro que se va a agregar.
    - **Valor:** Escriba el valor asociado al **Nombre del parámetro**.
    - Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar opciones de Habilitar VPN a demanda

- **Dominio a demanda:** Para agregar un dominio y la acción asociada que se realizará cuando los usuarios se conecten a él, haga clic en **Agregar** y lleve a cabo lo siguiente:
    - **Dominio:** Escriba el dominio que se va a agregar.
    - **Acción:** En la lista, seleccione en una de las posibles acciones:
        * **Establecer siempre:** El dominio siempre activa una conexión VPN.
        * **No establecer nunca:** El dominio no activa nunca una conexión VPN.
        * **Establecer si es necesario:** El dominio activa un intento de conexión VPN si falla la resolución de nombres de dominio. El error ocurre cuando el servidor DNS no puede resolver el dominio, redirige a un servidor diferente o agota el tiempo de espera.
    - Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **Reglas a demanda**
    - **Acción:** En la lista, seleccione la acción que se debe realizar. El valor predeterminado es **EvaluateConnection**. Las acciones posibles son:
        * **Permitir:** Al activarse, permite que la VPN a demanda se conecte.

    * **Conectar:** Inicia incondicionalmente una conexión VPN.
    * **Desconectar:** Quita la conexión VPN y no vuelve a conectarse a demanda mientras la regla se cumpla.
    * **EvaluateConnection:** Evalúa la matriz **ActionParameters** para cada conexión.
    * **Ignorar:** Deja activa cualquier conexión VPN existente, pero no vuelve a conectarse a demanda mientras la regla se cumpla.
- **DNSDomainMatch:** Para cada dominio incluido en la lista de búsqueda de dominios de un dispositivo de usuario que quiera agregar, haga clic en **Agregar** y lleve a cabo lo siguiente:
    * **Dominio DNS:** Escriba el nombre del dominio. Puede usar el prefijo comodín "*" para abarcar varios dominios. Por ejemplo: *.ejemplo.com abarca midominio.ejemplo.com, tudominio.ejemplo.com y sudominio.ejemplo.com.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **DNSServerAddressMatch:** Para agregar cada dirección IP con la que puede coincidir cualquier servidor DNS indicado en la red, haga clic en **Agregar** y lleve a cabo lo siguiente:
    * **Dirección del servidor DNS:** Escriba la dirección del servidor DNS que quiere agregar. Puede usar el sufijo comodín "*" para abarcar varios servidores DNS. Por ejemplo: 17.* abarca cualquier servidor DNS incluido en la subred de clase A.
    * Haga clic en **Guardar** para guardar el servidor DNS, o bien haga clic en **Cancelar** para no guardarlo.
- **InterfaceTypeMatch:** En la lista, haga clic en el tipo de hardware de interfaz de red principal que se está utilizando. El valor predeterminado es **No especificado**. Los valores posibles son:
    * **No especificado:** Coincide con cualquier hardware de interfaz de red. Esta es la opción predeterminada.
    * **Ethernet:** Solo coincide con el hardware de interfaz de red Ethernet.
    * **Wi-Fi:** Solo coincide con el hardware de interfaz de red Wi-Fi.
    * **Móvil:** Solo coincide con el hardware de interfaz de red móvil.
- **SSIDMatch:** Haga clic en **Agregar** y haga lo siguiente para agregar cada SSID que se va a cotejar con la red actual.
    * **SSID:** Escriba el SSID que se va a agregar. Si no se trata de una red Wi-Fi, o bien si el SSID no aparece, el cotejo falla. Deje esta lista vacía para que abarque cualquier SSID.
    * Haga clic en **Guardar** para guardar el SSID, o bien haga clic en **Cancelar** para descartarlo.
- **URLStringProbe:** Escriba una URL a capturar. Si la URL se captura correctamente sin redirección, se cumple esta regla.
- **ActionParameters: Domains:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada dominio que va a comprobar EvaluateConnection:
    * **Dominio:** Escriba el dominio que se va a agregar.

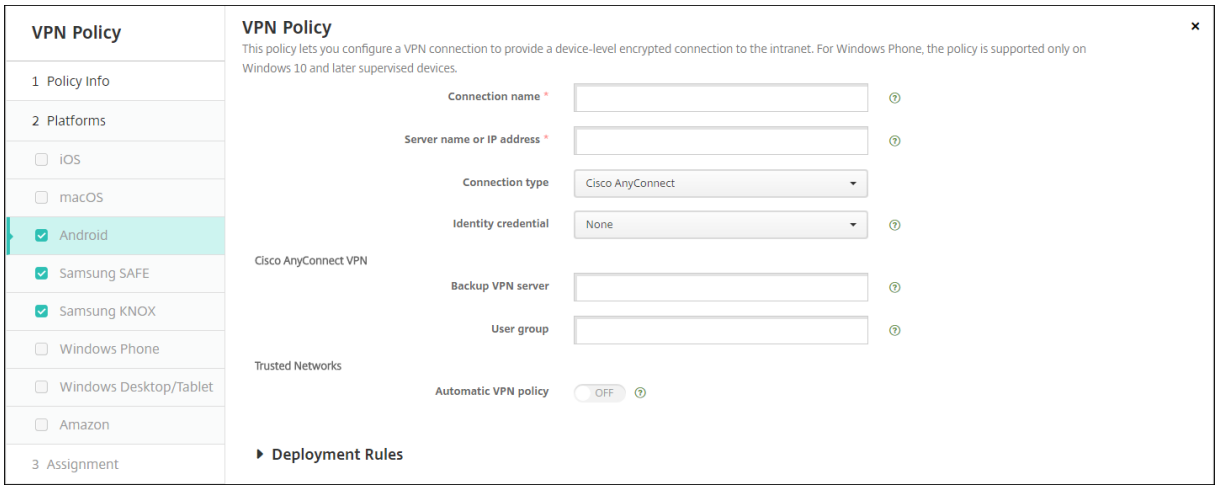
        * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
    - **ActionParameters: DomainAction:** En la lista, seleccione el **comportamiento de la red VPN** correspondiente para los dominios especificados en **ActionParameters: Domains**. El valor predeterminado es **ConnectIfNeeded**. Las acciones posibles son:
        * **ConnectIfNeeded:** El dominio activa un intento de conexión VPN si falla la resolución de nombres de dominio. El error ocurre cuando el servidor DNS no puede resolver el dominio, redirige a un servidor diferente o agota el tiempo de espera.
        * **NeverConnect:** El dominio no activa nunca una conexión VPN.
    - **Action Parameters: RequiredDNSServers:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada dirección IP del servidor DNS que se va a usar para resolver los dominios especificados:
        * **Servidor DNS:** Solo válido si **ActionParameters** : **DomainAction** es **ConnectIfNeeded**. Escriba el servidor DNS que se va a agregar. No es necesario que este servidor forme parte de la configuración de red actual del dispositivo. Si el servidor DNS no es accesible, se establece una conexión VPN. Este debe ser un servidor DNS interno o un servidor DNS externo de confianza.
        * Haga clic en **Save** para guardar el servidor DNS, o bien haga clic en **Cancel** para no guardarlo.
    - **ActionParameters : RequiredURLStringProbe:** Si quiere, escriba una URL en formato HTTP o HTTPS (preferentemente este) para llevar a cabo un sondeo con la ayuda de una solicitud GET. Si el nombre de host de la URL no se puede resolver, o si el servidor es inaccesible o el servidor no responde, se establece una conexión VPN. Válido solamente si **ActionParameters**: **DomainAction** = **ConnectIfNeeded**.
    - **OnDemandRules : XML content:** Escriba o copie y pegue las reglas a demanda de la configuración XML.
        * Haga clic en **Diccionario de comprobación** para validar la sintaxis del código XML. Puede ver el mensaje “XML válido” en verde debajo del cuadro de texto de **Contenido XML** si el XML es válido. Si no es válido, verá un mensaje de error en texto en naranja que describe el error.
- **Proxy**
    - **Configuración de proxy:** En la lista, seleccione cómo se redirige la conexión VPN a través de un servidor proxy. El valor predeterminado es **Ninguno**.
        * Si habilita **Manual**, configure los siguientes parámetros:
            · **Nombre de host o dirección IP del servidor proxy:** Escriba el nombre de host o la dirección IP del servidor proxy. Este campo es obligatorio.
            · **Puerto del servidor proxy.** Escriba el número de puerto del servidor proxy. Este campo es obligatorio.
            · **Nombre de usuario:** Escriba un nombre de usuario opcional para el servidor

proxy.

- **Contraseña:** Escriba una contraseña opcional de servidor proxy.

* Si selecciona **Automático**, configure este parámetro:
  - **URL del servidor proxy:** Escriba la URL del servidor proxy. Este campo es obligatorio.

Parámetros de Android



Configurar el protocolo VPN de Cisco AnyConnect para Android

- **Nombre de la conexión.** Escriba un nombre para la conexión VPN de Cisco AnyConnect. Este campo es obligatorio.
- **Nombre o dirección IP del servidor.** Escriba el nombre o la dirección IP del servidor VPN. Este campo es obligatorio.
- **Credencial de identidad:** En la lista, seleccione una credencial de identidad.
- **Servidor VPN de reserva:** Escriba la información del servidor VPN de reserva.
- **Grupo de usuarios.** Escriba la información del grupo de usuarios.
- **Redes de confianza**
  - **Directiva de VPN automática.** 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:
    * **Directiva de redes de confianza.** En la lista, seleccione la directiva pertinente. El valor predeterminado es **Desconectar**. Las opciones posibles son:
      - **Desconectar.** El cliente termina la conexión VPN en la red de confianza. Este es el valor predeterminado.
      - **Conectar.** El cliente inicia una conexión VPN en la red de confianza.
      - **No hacer nada:** El cliente no lleva a cabo ninguna acción.

        - **Pausa:** Cuando un usuario establece una sesión VPN fuera de la red de confianza y luego entra en una red configurada como “de confianza”, la sesión VPN se suspende. Cuando el usuario abandona esa red de confianza, la sesión se reanuda. Este parámetro elimina la necesidad de establecer una nueva sesión VPN después de abandonar una red de confianza.
    * **Directiva de redes no seguras:** En la lista, seleccione la directiva pertinente. El valor predeterminado es **Conectar**. Las opciones posibles son:
        - **Conectar.** El cliente inicia una conexión VPN en una red que no es de confianza.
        - **No hacer nada:** El cliente no lleva a cabo ninguna acción. Esta opción inhabilita la opción “VPN permanente”.
  - **Dominios de confianza.** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada sufijo de dominio que tenga la interfaz de red cuando el cliente se encuentra en la red de confianza:
    * **Dominio:** Escriba el dominio que se va a agregar.
    * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
  - **Servidores de confianza.** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada dirección de servidor que tenga la interfaz de red cuando el cliente se encuentra en la red de confianza:
    * **Servidores.** Escriba el servidor que se va a agregar.
    * Haga clic en **Guardar** para guardar el servidor, o bien haga clic en **Cancelar** para descartarlo.

Configurar el protocolo Citrix SSO para Android

- **Nombre de la conexión.** Escriba un nombre para la conexión VPN. Este campo es obligatorio.
- **Nombre o dirección IP del servidor:** Escriba el FQDN o la dirección IP de Citrix Gateway.
- **Tipo de autenticación para la conexión.** Elija un tipo de autenticación y complete cualquiera de los campos que aparecen para el tipo de conexión:
  - **Nombre de usuario** y **Contraseña**. Escriba las credenciales de la red VPN para los **tipos de autenticación** que sean **Contraseña** o **Contraseña y certificado**. Opcional. Si no proporciona las credenciales de VPN, la aplicación Citrix VPN solicitará un nombre de usuario y una contraseña.
  - **Credencial de identidad:** Aparece cuando los valores de los **Tipos de autenticación** son **Contraseña** o **Contraseña y certificado**. En la lista, seleccione una credencial de identidad.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Si no habilita VPN por aplicación, todo el tráfico pasará por el túnel VPN de Citrix. Si habilita VPN por

aplicación, especifique los siguientes parámetros. Está **desactivado** de forma predeterminada.

- **Lista blanca** o **Lista negra:** Si es **Lista blanca**, todas las aplicaciones permitidas pasarán a través del túnel de esta red VPN. Si es **Lista negra**, todas las aplicaciones excepto aquellas de la lista de bloqueados pasarán a través de esta red VPN.

  > **Nota:**
  >
  > La consola de XenMobile Server contiene los términos “lista negra” y “lista blanca”. Estamos cambiando esos términos en una próxima versión a “lista de bloqueados” y “lista de permitidos”.

- **Lista de aplicaciones:** Especifique las aplicaciones permitidas o bloqueadas. Haga clic en **Agregar** y, a continuación, escriba una lista separada por comas de nombres de paquetes de aplicación.

- **XML personalizado:** Haga clic en **Agregar** y, a continuación, escriba los parámetros personalizados. XenMobile admite estos parámetros para Citrix VPN:
  - **DisableUserProfiles:** Opcional. Para habilitar este parámetro, escriba **Sí** en **Valor**. Si está habilitado, XenMobile no muestra las conexiones VPN que haya agregado el usuario y este no puede agregar conexiones. Este parámetro es una restricción global y se aplica a todos los perfiles de red VPN.
  - **userAgent:** Un valor de cadena. Puede especificar una cadena personalizada de agente de usuario que se enviará en cada solicitud HTTP. La cadena del agente de usuario indicada se agrega al agente de usuario existente de Citrix VPN.

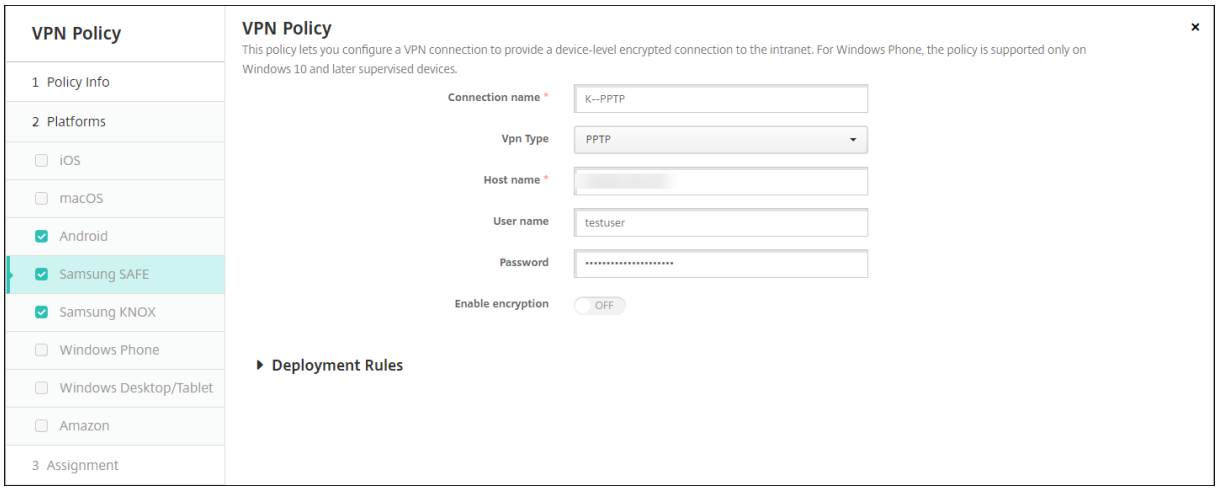
Configurar redes VPN para poder utilizar NAC

1. Utilice el **Tipo de conexión** llamado **SSL personalizado** para configurar el filtro NAC.
2. Especifique **VPN** como **Nombre de conexión**.
3. Para **XML personalizado**, haga clic en **Agregar** y lleve a cabo lo siguiente:
   - **Nombre del parámetro:** Escriba **XenMobileDeviceId**. Este campo es el ID de dispositivo que se utilizará para la comprobación de NAC basado en la inscripción de dispositivos en XenMobile. Si XenMobile inscribe y administra el dispositivo, se permite la conexión VPN. De lo contrario, la autenticación queda denegada al establecer la VPN.
   - **Valor:** Escriba **DeviceID_${device.id}**, que es el valor del parámetro **XenMobileDeviceId**.
   - Haga clic en **Guardar** para guardar el parámetro.

Configurar redes VPN para Android Enterprise

Para configurar redes VPN para dispositivos Android Enterprise, cree una directiva Configuraciones administradas por Android Enterprise para la aplicación Citrix SSO. Consulte Configurar perfiles de VPN para Android Enterprise.

Parámetros de Samsung SAFE



- **Nombre de la conexión:** Escriba un nombre para la conexión.
- **Tipo de VPN:** En la lista, seleccione el protocolo que se va a usar para esta conexión. El valor predeterminado es **L2TP con clave precompartida**. Las opciones posibles son:
  - **L2TP con clave precompartida.** Protocolo Layer 2 Tunneling Protocol con autenticación de clave previamente compartida. Este es el valor predeterminado.
  - **L2TP con certificado.** Protocolo Layer 2 Tunneling Protocol con certificado.
  - **PPTP:** Túnel punto a punto.
  - **Empresa.** La conexión VPN de su empresa. Se aplica a versiones SAFE anteriores a 2.0.
  - **Genérico.** Una conexión VPN genérica. Se aplica a SAFE 2.0 o versiones posteriores.

Configurar el protocolo L2TP con clave precompartida para Samsung SAFE

- **Nombre de host:** Escriba el nombre de host de la red privada virtual (VPN). Esta opción es obligatoria.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Clave precompartida.** Escriba la clave precompartida. Esta opción es obligatoria.

Configurar el protocolo L2TP con certificado para Samsung SAFE

- **Nombre de host:** Escriba el nombre de host de la red privada virtual (VPN). Esta opción es obligatoria.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.

Configurar el protocolo PPTP para Samsung SAFE

- **Nombre de host:** Escriba el nombre de host de la red privada virtual (VPN). Esta opción es obligatoria.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Habilitar cifrado:** Seleccione si permitir el cifrado de la conexión VPN.

Configurar el protocolo Empresa para Samsung SAFE

- **Nombre de host:** Escriba el nombre de host de la red privada virtual (VPN). Esta opción es obligatoria.
- **Habilitar servidor de reserva:** Seleccione si habilitar un servidor VPN de reserva. Si se habilita esta opción, en **Servidor VPN de reserva**, escriba el nombre de dominio completo (FQDN) o la dirección IP del servidor VPN de reserva.
- **Habilitar autenticación de usuarios:** Seleccione si requerir la autenticación de los usuarios. Si activa esta opción, defina los siguientes parámetros:
  - **Nombre de usuario:** Escriba un nombre de usuario.
  - **Contraseña:** Escriba la contraseña de usuario.
- **Nombre del grupo:** Escriba un nombre de grupo opcional.
- **Método de autenticación:** En la lista, seleccione el método de autenticación que se va a usar. Las opciones posibles son:
  - **Certificado:** Se usa la autenticación por certificado. Este es el valor predeterminado. Si se selecciona, en la lista **Credencial de identidad**, elija la credencial que se usará. El valor predeterminado es **Ninguno**.
  - **Clave precompartida:** Se usa una clave previamente compartida. Si se selecciona, en el campo **Clave precompartida**, escriba la clave de secreto compartida.
  - **RSA híbrido:** Se usa la autenticación híbrida con certificados RSA.
  - **EAP MD5:** Autentica el protocolo EAP del mismo nivel en el servidor EAP, pero sin autenticación mutua.
  - **EAP MSCHAPv2:** Se usa el protocolo de autenticación por desafío mutuo Microsoft Challenge-Handshake para la autenticación mutua.
- **Certificado de CA:** En la lista, seleccione el certificado que se va a utilizar. El valor predeterminado es **Ninguno**.
- **Habilitar ruta predeterminada:** Seleccione si habilitar una ruta predeterminada al servidor VPN. Está **desactivado** de forma predeterminada.
- **Habilitar autenticación con tarjeta inteligente:** Seleccione si permitir que los usuarios se autentiquen mediante tarjetas inteligentes. Está **desactivado** de forma predeterminada.
- **Habilitar opción móvil:** Seleccione si habilitar la opción móvil. Está **desactivado** de forma predeterminada.

- **Valor del grupo Diffie-Hellman (nivel de clave):** En la lista, seleccione el nivel de seguridad que tendrá la clave que se va a usar. El valor predeterminado es 0.
- **Tipo de túnel dividido:** En la lista, seleccione el tipo de túnel dividido que se va a usar. El valor predeterminado es **Automático**. Las opciones posibles son:
  - **Automático.** El túnel dividido se utiliza automáticamente.
  - **Manual:** El túnel dividido se usa en la dirección IP y el puerto especificados en el servidor VPN.
  - **Inhabilitado:** No se utiliza el túnel dividido.
- **Tipo SuiteB:** En la lista, seleccione el nivel de cifrado Suite B de NSA que se usará. El valor predeterminado es **GCM-128**. Las opciones posibles son:
  - **GCM-128:** Se usa el cifrado AES-GCM de 128 bits.
  - **GCM-256:** Se usa el cifrado AES-GCM de 256 bits.
  - **GMAC-128:** Se usa el cifrado AES-GMAC de 128 bits.
  - **GMAC-256:** Se usa el cifrado AES-GMAC de 256 bits.
  - **Ninguno:** No se usa ningún cifrado.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Configurar el protocolo genérico para Samsung SAFE

- **Nombre de host:** Escriba el nombre de host de la red privada virtual (VPN). Esta opción es obligatoria.
- **Habilitar autenticación de usuarios:** Seleccione si requerir la autenticación de los usuarios. Si se habilita, en **Contraseña**, escriba la contraseña de usuario.
- **Nombre de usuario:** Escriba un nombre de usuario.
- **Nombre de paquete de agente VPN:** El nombre de paquete o el ID de la VPN instalada en el dispositivo; por ejemplo, Mocana o Pulse Secure.
- **Tipo de conexión VPN:** En la lista, seleccione **IPsec** o **SSL** para el tipo de conexión que se debe usar. El valor predeterminado es **IPsec**. En las secciones siguientes, se describen los parámetros de configuración para cada tipo de conexión.

Configurar el tipo de conexión IPsec para Samsung SAFE

- **Identidad:** Puede escribir un identificador opcional para esta configuración.
- **Tipo de ID de grupo IPsec:** En la lista, seleccione el tipo de ID de grupo IPsec que se va a usar. El valor predeterminado es **Predeterminado**. Las opciones posibles son:
  - **Predeterminado**
  - **Dirección IPv4**

  - **Nombre de dominio completo (FQDN)**
  - **Nombre de dominio completo (FQDN) de usuario**
  - **ID de clave IKE**
- **Versión de IKE:** En la lista, seleccione la versión de Intercambio de claves por red que se va a usar. El valor predeterminado es **IKEv1**.
- **Método de autenticación:** En la lista, seleccione el método de autenticación que se va a usar. El valor predeterminado es **Certificado**. Las opciones posibles son:
  - **Certificado:** Se usa la autenticación por certificado. Si se selecciona, en la lista **Credencial de identidad**, elija la credencial que se usará. El valor predeterminado es **Ninguno**.
  - **Clave precompartida:** Se usa una clave previamente compartida. Si se selecciona, en el campo **Clave precompartida**, escriba la clave de secreto compartida.
  - **RSA híbrido:** Se usa la autenticación híbrida con certificados RSA.
  - **EAP MD5:** Autentica el protocolo EAP del mismo nivel en el servidor EAP, pero sin autenticación mutua.
  - **EAP MSCHAPv2:** Se usa el protocolo de autenticación por desafío mutuo Microsoft Challenge-Handshake para la autenticación mutua.
  - **Autenticación basada en CAC:** Se usa una tarjeta de acceso común (CAC) para la autenticación.
- **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
- **Certificado de CA:** En la lista, seleccione el certificado que se va a utilizar.
- **Habilitar DPD (Dead Peer Detection):** Seleccione si establecer contacto con un nodo del mismo nivel para comprobar que permanece activo. Está **desactivado** de forma predeterminada.
- **Habilitar ruta predeterminada:** Seleccione si habilitar una ruta predeterminada al servidor VPN.
- **Habilitar opción móvil:** Seleccione si habilitar la opción móvil.
- **Tiempo de vida de IKE (en minutos):** Escriba la cantidad de minutos que debe transcurrir antes de restablecer la conexión VPN. El valor predeterminado es 1440 minutos (24 horas).
- **Tiempo de vida de IPsec (en minutos):** Escriba la cantidad de minutos que debe transcurrir antes de restablecer la conexión VPN. El valor predeterminado es 1440 minutos (24 horas).
- **Valor del grupo Diffie-Hellman (nivel de clave):** En la lista, seleccione el nivel de seguridad que tendrá la clave que se va a usar. El valor predeterminado es **0**.
- **Modo de intercambio de clave IKE Phase 1:** Seleccione **Principal** o **Agresivo** para el modo de negociación de la fase 1 de IKE. El valor predeterminado es **Principal**.
  - **Principal:** No se expone información a posibles atacantes durante la negociación, pero es más lento que el modo **Agresivo**.
  - **Agresivo:** Se expone parte de la información (por ejemplo, la identidad de los negociantes) a posibles atacantes durante la negociación, pero es más rápido que el modo

Principal.

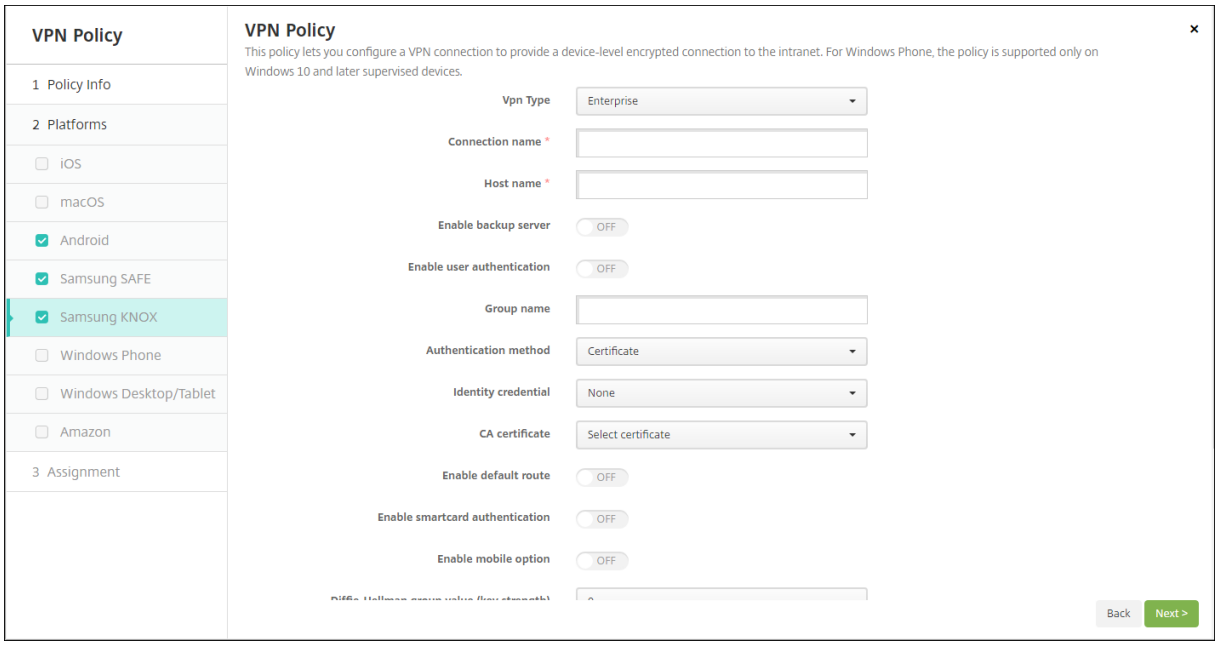
- **Valor de PFS (Perfect Forward Secrecy):** Seleccione si utilizar PFS para requerir un nuevo intercambio de claves y renegociar una conexión.
- **Tipo de túnel dividido:** En la lista, seleccione el tipo de túnel dividido que se va a usar. Las opciones posibles son:
  - **Automático:** El túnel dividido se utiliza automáticamente.
  - **Manual:** El túnel dividido se usa en la dirección IP y el puerto especificados en el servidor VPN.
  - **Inhabilitado:** No se utiliza el túnel dividido.
- **Algoritmo de cifrado IPsec:** Una configuración de red VPN que usa el protocolo IPsec.
- **Algoritmo de cifrado IKE:** Una configuración de red VPN que usa el protocolo IPsec.
- **Algoritmo de integridad IKE:** Una configuración de red VPN que usa el protocolo IPsec.
- **Proveedor:** Un perfil personal para agentes genéricos que se comunican con la API de Knox.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.
- **VPN por aplicación:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada VPN por aplicación:
  - **VPN por aplicación:** La configuración de red VPN que usa la aplicación para comunicarse.
  - Haga clic en **Guardar** para guardar la red VPN por aplicación, o bien haga clic en **Cancelar** para no guardarla.

Configurar el tipo de conexión SSL para Samsung SAFE

- **Método de autenticación:** En la lista, seleccione el método de autenticación que se va a usar. El valor predeterminado es **No aplicable**. Las opciones posibles son:
  - **No aplicable**
  - **Certificado:** Se usa la autenticación por certificado. Si se selecciona, en la lista **Credencial de identidad**, elija la credencial que se usará. El valor predeterminado es **Ninguno**.
  - **Autenticación basada en CAC:** Se usa una tarjeta de acceso común (CAC) para la autenticación.
- **Certificado de CA:** En la lista, seleccione el certificado que se va a utilizar.
- **Habilitar ruta predeterminada:** Seleccione si habilitar una ruta predeterminada al servidor VPN.
- **Habilitar opción móvil:** Seleccione si habilitar la opción móvil.
- **Tipo de túnel dividido:** En la lista, seleccione el tipo de túnel dividido que se va a usar. Las opciones posibles son:
  - **Automático:** El túnel dividido se utiliza automáticamente.
  - **Manual:** El túnel dividido se usa en la dirección IP y el puerto especificados en el servidor

VPN.
  - **Inhabilitado:** No se utiliza el túnel dividido.
- **Algoritmo SSL:** Escriba el algoritmo SSL que se va a utilizar para la negociación entre cliente y servidor.
- **Proveedor:** Un perfil personal para agentes genéricos que se comunican con la API de Knox.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.
- **VPN por aplicación:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada VPN por aplicación:
  - **VPN por aplicación:** La configuración de red VPN que usa la aplicación para comunicarse.
  - Haga clic en **Guardar** para guardar la red VPN por aplicación, o bien haga clic en **Cancelar** para no guardarla.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Parámetros de Samsung Knox



La directiva para Samsung Knox solo se aplica dentro del contenedor Samsung Knox.

- **Tipo de VPN:** En la lista, seleccione el tipo de conexión VPN que quiere configurar. La conexión puede ser **Empresa** (aplicable a las versiones de Knox anteriores a 2.0) o **Genérico** (aplicable a las versiones de Knox 2.0 o posteriores). El valor predeterminado es **Empresa**.

En las siguientes secciones se ofrecen las opciones de configuración para cada uno de los tipos de conexión mencionados.

Configurar el protocolo Empresa para Samsung Knox

- **Nombre de la conexión:** Escriba un nombre para la conexión. Este campo es obligatorio.
- **Nombre de host:** Escriba el nombre de host de la red privada virtual (VPN). Esta opción es obligatoria.
- **Habilitar servidor de reserva:** Seleccione si habilitar un servidor VPN de reserva. Si se habilita esta opción, en **Servidor VPN de reserva**, escriba el nombre de dominio completo (FQDN) o la dirección IP del servidor VPN de reserva.
- **Habilitar autenticación de usuarios:** Seleccione si requerir la autenticación de los usuarios. Si activa esta opción, defina los siguientes parámetros:
  - **Nombre de usuario:** Escriba un nombre de usuario.
  - **Contraseña:** Escriba la contraseña de usuario.
- **Nombre del grupo:** Escriba un nombre de grupo opcional.
- **Método de autenticación:** En la lista, seleccione el método de autenticación que se va a usar. Las opciones posibles son:

  - **Certificado:** Se usa la autenticación por certificado. Para la autenticación por certificado, seleccione también la credencial que se usará en la lista **Credencial de identidad**.
  - **Clave precompartida:** Se usa una clave previamente compartida. Si se selecciona, en el campo **Clave precompartida**, escriba la clave de secreto compartida.
  - **RSA híbrido:** Se usa la autenticación híbrida con certificados RSA.
  - **EAP MD5:** Autentica el protocolo EAP del mismo nivel en el servidor EAP, pero sin autenticación mutua.
  - **EAP MSCHAPv2:** Se usa el protocolo de autenticación por desafío mutuo Microsoft Challenge-Handshake para la autenticación mutua.
- **Certificado de CA:** En la lista, seleccione el certificado que se va a utilizar.
- **Habilitar ruta predeterminada:** Seleccione si habilitar una ruta predeterminada al servidor VPN.
- **Habilitar autenticación con tarjeta inteligente:** Seleccione si permitir que los usuarios se autentiquen mediante tarjetas inteligentes. Está **desactivado** de forma predeterminada.
- **Habilitar opción móvil:** Seleccione si habilitar la opción móvil.
- **Valor del grupo Diffie-Hellman (nivel de clave):** En la lista, seleccione el nivel de seguridad que tendrá la clave que se va a usar. El valor predeterminado es **0**.
- **Tipo de túnel dividido:** En la lista, seleccione el tipo de túnel dividido que se va a usar. Las opciones posibles son:
  - **Automático:** El túnel dividido se utiliza automáticamente.
  - **Manual:** El túnel dividido se usa en la dirección IP y el puerto especificados en el servidor VPN.
  - **Inhabilitado:** No se utiliza el túnel dividido.
- **Tipo SuiteB:** En la lista, seleccione el nivel de cifrado Suite B de NSA que se usará. Las opciones posibles son:
  - **GCM-128.** Se usa el cifrado AES-GCM de 128 bits. Este es el parámetro predeterminado.
  - **GCM-256:** Se usa el cifrado AES-GCM de 256 bits.
  - **GMAC-128:** Se usa el cifrado AES-GMAC de 128 bits.
  - **GMAC-256:** Se usa el cifrado AES-GMAC de 256 bits.
  - **Ninguno:** No se usa ningún cifrado.
- **Rutas de reenvío.** Haga clic en **Agregar** para agregar rutas de reenvío opcionales si el servidor VPN de la empresa es compatible con varias tablas de enrutamiento.

Configurar el protocolo Genérico para Samsung Knox

- **Nombre de la conexión:** Escriba un nombre para la conexión. Este campo es obligatorio.
- **Nombre de paquete de agente VPN:** El nombre de paquete o el ID de la VPN instalada en el dispositivo; por ejemplo, Mocana o Pulse Secure.
- **Nombre de host:** Escriba el nombre de host de la red privada virtual (VPN). Esta opción es obligatoria.

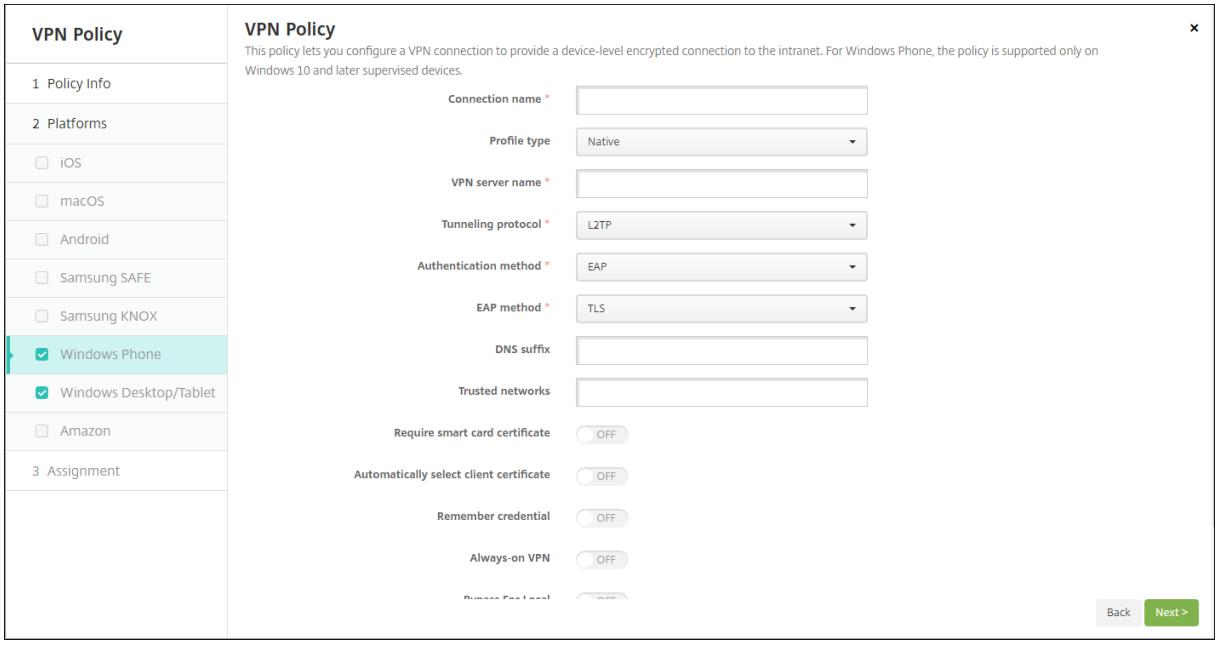
- **Habilitar autenticación de usuarios:** Seleccione si requerir la autenticación de los usuarios. Si activa esta opción, defina los siguientes parámetros:
  - **Nombre de usuario:** Escriba un nombre de usuario.
  - **Contraseña:** Escriba la contraseña de usuario.
- **Identidad:** Puede escribir un identificador opcional para esta configuración. Solo se aplica cuando el **Tipo de conexión VPN es IPSEC**.
- **Tipo de conexión VPN:** En la lista, seleccione **IPsec** o **SSL** para el tipo de conexión que se debe usar. El valor predeterminado es **IPsec**. En las secciones siguientes, se describen los parámetros de configuración para cada tipo de conexión.
- **Configurar la conexión IPsec**
  - **Tipo de ID de grupo IPsec:** En la lista, seleccione el tipo de ID de grupo IPsec que se va a usar. El valor predeterminado es **Predeterminado**. Las opciones posibles son:
    - **Predeterminado**
    - **Dirección IPv4**
    - **Nombre de dominio completo (FQDN)**
    - **Nombre de dominio completo (FQDN) de usuario**
    - **ID de clave IKE**
  - **Versión de IKE:** En la lista, seleccione la versión de Intercambio de claves por red que se va a usar. El valor predeterminado es **IKEv1**.
  - **Método de autenticación:** En la lista, seleccione el método de autenticación que se va a usar. El valor predeterminado es **Certificado**. Las opciones posibles son:
    - **Certificado:** Se usa la autenticación por certificado. Si se selecciona, en la lista **Credencial de identidad**, elija la credencial que se usará. El valor predeterminado es **Ninguno**.
    - **Clave precompartida:** Se usa una clave previamente compartida. Si se selecciona, en el campo **Clave precompartida**, escriba la clave de secreto compartida.
    - **RSA híbrido:** Se usa la autenticación híbrida con certificados RSA.
    - **EAP MD5:** Autentica el protocolo EAP del mismo nivel en el servidor EAP, pero sin autenticación mutua.
    - **EAP MSCHAPv2:** Se usa el protocolo de autenticación por desafío mutuo Microsoft Challenge-Handshake para la autenticación mutua.
    - **Autenticación basada en CAC:** Se usa una tarjeta de acceso común (CAC) para la autenticación.
  - **Certificado de CA:** En la lista, seleccione el certificado que se va a utilizar.
  - **Habilitar DPD (Dead Peer Detection):** Seleccione si establecer contacto con un nodo del mismo nivel para comprobar que permanece activo. Está **desactivado** de forma predeterminada.
  - **Habilitar ruta predeterminada:** Seleccione si habilitar una ruta predeterminada al servidor VPN.

- **Habilitar opción móvil:** Seleccione si habilitar la opción móvil.
- **Tiempo de vida de IKE (en minutos):** Escriba la cantidad de minutos que debe transcurrir antes de restablecer la conexión VPN. El valor predeterminado es 1440 minutos (24 horas).
- **Tiempo de vida de IPsec (en minutos):** Escriba la cantidad de minutos que debe transcurrir antes de restablecer la conexión VPN. El valor predeterminado es 1440 minutos (24 horas).
- **Valor del grupo Diffie-Hellman (nivel de clave):** En la lista, seleccione el nivel de seguridad que tendrá la clave que se va a usar. El valor predeterminado es **0**.
- **Modo de intercambio de clave IKE Phase 1:** Seleccione **Principal** o **Agresivo** para el modo de negociación de la fase 1 de IKE. El valor predeterminado es **Principal**.
  - **Principal:** No se expone información a posibles atacantes durante la negociación, pero es más lento que el modo **Agresivo**.
  - **Agresivo:** Se expone parte de la información (por ejemplo, la identidad de los negociantes) a posibles atacantes durante la negociación, pero es más rápido que el modo **Principal**.
- **Valor de PFS (Perfect Forward Secrecy):** Seleccione si utilizar PFS para requerir un nuevo intercambio de claves y renegociar una conexión.
- **Tipo de túnel dividido:** En la lista, seleccione el tipo de túnel dividido que se va a usar. Las opciones posibles son:
  - **Automático:** El túnel dividido se utiliza automáticamente.
  - **Manual:** El túnel dividido se usa en la dirección IP y el puerto especificados en el servidor VPN.
  - **Inhabilitado:** No se utiliza el túnel dividido.
- **Tipo SuiteB:** En la lista, seleccione el nivel de cifrado Suite B de NSA que se usará. El valor predeterminado es **GCM-128**. Las opciones posibles son:
  - **GCM-128:** Se usa el cifrado AES-GCM de 128 bits.
  - **GCM-256:** Se usa el cifrado AES-GCM de 256 bits.
  - **GMAC-128:** Se usa el cifrado AES-GMAC de 128 bits.
  - **GMAC-256:** Se usa el cifrado AES-GMAC de 256 bits.
  - **Ninguno:** No se usa ningún cifrado.
- **Algoritmo de cifrado IPsec:** Una configuración de red VPN que usa el protocolo IPsec.
- **Algoritmo de cifrado IKE:** Una configuración de red VPN que usa el protocolo IPsec.
- **Algoritmo de integridad IKE:** Una configuración de red VPN que usa el protocolo IPsec.
- **Knox:** Solo para configuraciones de Samsung Knox.
- **Proveedor:** Un perfil personal para agentes genéricos que se comunican con la API de Knox.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.

        * Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.
    - **VPN por aplicación:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada VPN por aplicación:
        * **VPN por aplicación:** La configuración de red VPN que usa la aplicación para comunicarse.
        * Haga clic en **Guardar** para guardar la red VPN por aplicación, o bien haga clic en **Cancelar** para no guardarla.
- **Configurar la conexión SSL**
    - **Método de autenticación:** En la lista, haga clic en el método de autenticación que se va a usar. Las opciones posibles son:
        * **No aplicable:** No se aplica ningún método de autenticación. Este es el valor predeterminado.
        * **Certificado:** Se usa la autenticación por certificado. Este es el valor predeterminado. Si se selecciona, en la lista Credencial de identidad, elija la credencial que se usará. El valor predeterminado es Ninguna.
        * **Autenticación basada en CAC:** Se usa una tarjeta de acceso común (CAC) para la autenticación.
    - **Certificado de CA:** En la lista, seleccione el certificado que se va a utilizar.
    - **Habilitar ruta predeterminada:** Seleccione si habilitar una ruta predeterminada al servidor VPN.
    - **Habilitar opción móvil:** Seleccione si habilitar la opción móvil.
    - **Tipo de túnel dividido:** En la lista, seleccione el tipo de túnel dividido que se va a usar. Las opciones posibles son:
        * **Automático:** El túnel dividido se utiliza automáticamente.
        * **Manual.** El túnel dividido se usa en la dirección IP y el puerto especificados.
        * **Inhabilitado:** No se utiliza el túnel dividido.
    - **Tipo SuiteB:** En la lista, seleccione el nivel de cifrado Suite B de NSA que se usará. El valor predeterminado es GCM-128. Las opciones posibles son:
        * **GCM-128:** Se usa el cifrado AES-GCM de 128 bits.
        * **GCM-256:** Se usa el cifrado AES-GCM de 256 bits.
        * **GMAC-128:** Se usa el cifrado AES-GMAC de 128 bits.
        * **GMAC-256:** Se usa el cifrado AES-GMAC de 256 bits.
        * **Ninguno:** No se usa ningún cifrado.
    - **Algoritmo SSL:** Escriba el algoritmo SSL que se va a utilizar para la negociación entre cliente y servidor.
    - **Knox:** Solo para configuraciones de Samsung Knox.
    - **Proveedor:** Un perfil personal para agentes genéricos que se comunican con la API de Knox.

- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
  * **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  * Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.
- **VPN por aplicación:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada VPN por aplicación:
  * **VPN por aplicación:** La configuración de red VPN que usa la aplicación para comunicarse.
  * Haga clic en **Guardar** para guardar la red VPN por aplicación, o bien haga clic en **Cancelar** para no guardarla.

Parámetros de Windows Phone



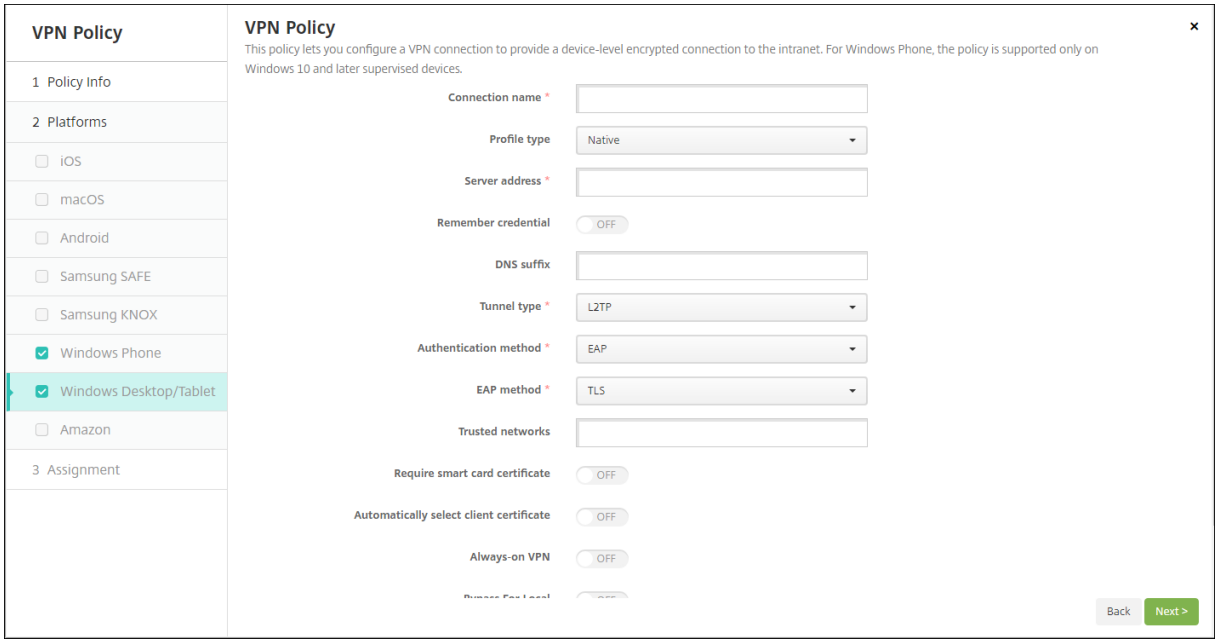
Esta configuración solo se admite en teléfonos supervisados con Windows 10 y versiones posteriores.

- **Nombre de la conexión:** Escriba el nombre de la conexión. Este campo es obligatorio.
- **Tipo de perfil:** En la lista, seleccione **Nativo** o **Plug-in**. El valor predeterminado es **Nativo**. En los siguientes apartados, se describe la configuración de cada una de las opciones.
- **Configuración de tipo de perfil nativo.** Esta configuración se aplica a la red VPN integrada en los teléfonos Windows de los usuarios.
  - **Nombre de servidor de VPN.** Escriba el nombre de dominio completo (FQDN) o la dirección IP del servidor VPN. Este campo es obligatorio.
  - **Protocolo de túnel.** En la lista, seleccione 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.
    - **Método de autenticación:** En la lista, seleccione 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:** Se usa el protocolo de autenticación por desafío mutuo de Microsoft para la autenticación mutua. Esta opción no está disponible cuando se selecciona IKEv2 como tipo de túnel. Al elegir MSCHAPv2, aparece la opción **Usar credenciales de Windows automáticamente**. Está **desactivado** de forma predeterminada.
    - **Método de EAP:** En la lista, seleccione el método de 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).
    - **Sufijo DNS:** Escriba el sufijo DNS.
    - **Redes de confianza:** 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.
    - **Requerir certificado de tarjeta inteligente:** Seleccione si se debe requerir un certificado de tarjeta inteligente. Está desactivado de forma predeterminada.
    - **Seleccionar automáticamente el certificado del cliente:** Seleccione si elegir automáticamente el certificado de cliente para la autenticación. Está desactivado de forma predeterminada. Esta opción no está disponible si se habilita la opción Requerir certificado de tarjeta inteligente.
    - **Recordar credencial:** Seleccione si almacenar la credencial en la memoria caché. Está desactivado de forma predeterminada. Cuando está habilitada, las credenciales se almacenan en caché siempre que sea posible.
    - **VPN permanente:** Seleccione si la red VPN siempre está activada. Está desactivado de forma predeterminada. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario se desconecta manualmente.
    - **Omitir para direcciones locales:** Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor proxy.
- **Configuración del tipo de protocolo del plug-in:** Estos parámetros se aplican a plug-ins VPN obtenidos de la Tienda Windows e instalados en los dispositivos de los usuarios.
    - **Dirección del servidor:** Escriba la URL, el nombre de host o la dirección IP del servidor VPN.

- **ID de aplicación de cliente:** Escriba el nombre de familia del paquete que tenga el plug-in VPN.
- **XML de perfil de plug-in.** Seleccione el perfil personalizado de plug-in VPN que se va a usar. Para ello, haga clic en **Examinar** 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.
- **Sufijo DNS:** Escriba el sufijo DNS.
- **Redes de confianza:** 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.
- **Recordar credencial:** Seleccione si almacenar la credencial en la memoria caché. Está desactivado de forma predeterminada. Cuando está habilitada, las credenciales se almacenan en caché siempre que sea posible.
- **VPN permanente:** Seleccione si la red VPN siempre está activada. Está desactivado de forma predeterminada. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario se desconecta manualmente.
- **Omitir para direcciones locales:** Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor proxy.

Parámetros de escritorios y tabletas Windows



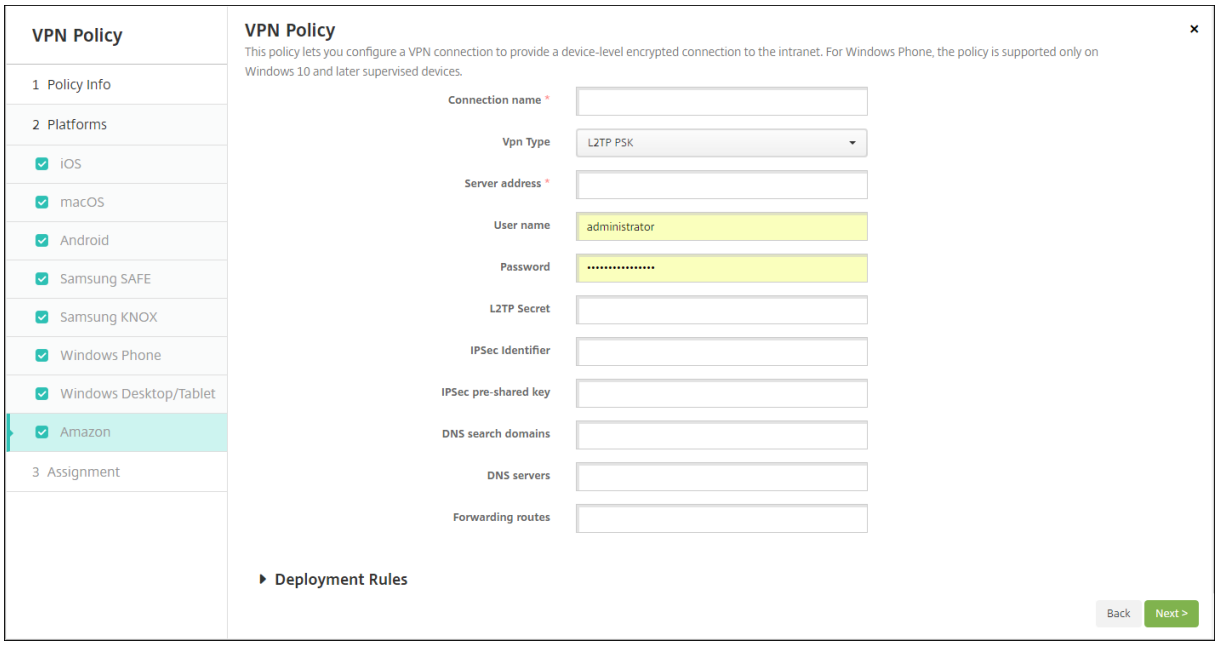
- **Nombre de la conexión:** Escriba el nombre de la conexión. Este campo es obligatorio.
- **Tipo de perfil:** En la lista, seleccione **Nativo** o **Plug-in**. El valor predeterminado es **Nativo**.
- **Configuración de tipo de perfil nativo.** Estos parámetros se aplican a la red VPN integrada en

los dispositivos Windows de los usuarios.

- **Dirección de servidor:** Escriba el nombre de dominio completo o la dirección IP del servidor VPN. Este campo es obligatorio.
- **Recordar credencial:** Seleccione si almacenar la credencial en la memoria caché. Está **desactivado** de forma predeterminada. Cuando está habilitada, las credenciales se almacenan en caché siempre que sea posible.
- **Sufijo DNS:** Escriba el sufijo DNS.
- **Tipo de túnel.** En la lista, seleccione 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.
- **Método de autenticación:** En la lista, seleccione 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:** Se usa el protocolo de autenticación por desafío mutuo de Microsoft para la autenticación mutua. Esta opción no está disponible cuando se selecciona **IKEv2** como tipo de túnel.
- **Método de EAP:** En la lista, seleccione el método de 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).
- **Redes de confianza:** 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.
- **Requerir certificado de tarjeta inteligente:** Seleccione si se debe requerir un certificado de tarjeta inteligente. Está **desactivado** de forma predeterminada.
- **Seleccionar automáticamente el certificado del cliente:** Seleccione si elegir automáticamente el certificado de cliente para la autenticación. Está **desactivado** de forma predeterminada. Esta opción no está disponible si habilita **Requerir certificado de tarjeta inteligente**.
- **VPN permanente:** Seleccione si la red VPN siempre está activada. Está **desactivado** de forma predeterminada. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario se desconecta manualmente.
- **Omitir para direcciones locales:** Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor proxy.

- **Configuración de tipo de perfil del plug-in.** Estos parámetros se aplican a plug-ins VPN obtenidos de la Tienda Windows e instalados en los dispositivos de los usuarios.
  - **Dirección de servidor:** Escriba el nombre de dominio completo o la dirección IP del servidor VPN. Este campo es obligatorio.
  - **Recordar credencial:** Seleccione si almacenar la credencial en la memoria caché. Está **desactivado** de forma predeterminada. Cuando está habilitada, las credenciales se almacenan en caché siempre que sea posible.
  - **Sufijo DNS:** Escriba el sufijo DNS.
  - **ID de aplicación de cliente:** Escriba el nombre de familia del paquete que tenga el plug-in VPN.
  - **XML de perfil de plug-in.** Seleccione el perfil personalizado de plug-in VPN que se va a usar. Para ello, haga clic en **Examinar** 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.
  - **Redes de confianza:** 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.
  - **VPN permanente:** Seleccione si la red VPN siempre está activada. Está **desactivado** de forma predeterminada. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario se desconecta manualmente.
  - **Omitir para direcciones locales:** Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor proxy.

Parámetros de Amazon



- **Nombre de la conexión:** Escriba el nombre de la conexión.
- **Tipo de VPN.** Seleccione el tipo de conexión. Las opciones posibles son:
  - **L2TP PSK:** Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida. Este es el valor predeterminado.
  - **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 ofrecen las opciones de configuración para cada uno de los tipos de conexión mencionados.

Configurar L2TP PSK para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Secreto L2TP:** Escriba la clave de secreto compartida.
- **Identificador de IPSec:** Escriba el nombre de la conexión VPN que verán los usuarios en sus dispositivos cuando se conecten.
- **Clave precompartida de IPsec:** Escriba la clave secreta.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar para resolver los dominios especificados.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Configurar L2TP RSA para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Secreto L2TP:** Escriba la clave de secreto compartida.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar para resolver los dominios especificados.

- **Certificado de servidor:** En la lista, seleccione el certificado de servidor que se va a utilizar.
- **Certificado de CA:** En la lista, seleccione el certificado de CA que se va a utilizar.
- **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Configurar IPSEC XAUTH PSK para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Identificador de IPSec:** Escriba el nombre de la conexión VPN que verán los usuarios en sus dispositivos cuando se conecten.
- **Clave precompartida de IPsec:** Escriba la clave de secreto compartida.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar para resolver los dominios especificados.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Configurar IPSEC AUTH RSA para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar para resolver los dominios especificados.
- **Certificado de servidor:** En la lista, seleccione el certificado de servidor que se va a utilizar.
- **Certificado de CA:** En la lista, seleccione el certificado de CA que se va a utilizar.
- **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.

- Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Configurar IPSEC HYBRID RSA para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar para resolver los dominios especificados.
- **Certificado de servidor:** En la lista, seleccione el certificado de servidor que se va a utilizar.
- **Certificado de CA:** En la lista, seleccione el certificado de CA que se va a utilizar.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Configurar PPTP para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar para resolver los dominios especificados.
- **Cifrado PPP (MPPE).** Seleccione si habilitar el cifrado de datos con el Cifrado punto a punto de Microsoft (MPPE). Está **desactivado** de forma predeterminada.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Directiva de fondo de pantalla

August 16, 2021

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 solamente para dispositivos supervisados. Para usar fondos de pantalla diferentes en iPads y iPhones, debe crear varias directivas de fondo de escritorio y aplicarlas a los usuarios correspondientes.

En la siguiente tabla, se ofrece una lista de las dimensiones de imagen que recomienda Apple para dispositivos iOS.

iPhone

Dispositivo	Dimensiones de imagen en píxeles
iPhone 12 Pro Max	2778 x 1284
iPhone 12 y iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE de 2.ª generación	1334 x 750
iPhone 7 Plus, 8 Plus	2208 x 1242
iPhone 7, 8	1334 x 750
iPhone 8 Plus	1334 x 750
iPhone 8	1334 x 750

iPad

Dispositivo	Dimensiones de imagen en píxeles
iPad Pro (1.ª, 2.ª y 3.ª generación de 12,9 pulgadas)	2732 x 2048
iPad Pro (10,5 pulgadas)	2224 x 1668

Dispositivo	Dimensiones de imagen en píxeles
iPad Pro (9,7 pulgadas)	1536 x 2048
iPad Air, 2	2048 x 1536

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Aplicar a.** En la lista, seleccione **Pantalla de bloqueo**, **Pantalla de inicio (lista de iconos)** o **Pantallas de inicio y de bloqueo** para definir dónde aparecerá el fondo de pantalla.
- **Archivo de fondo de pantalla.** Seleccione el archivo del fondo de pantalla. Para ello, deberá hacer clic en **Examinar** y, a continuación, ir a la ubicación del archivo.

Directiva de filtro de contenido web

January 4, 2022

En XenMobile, puede agregar una directiva de dispositivo 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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Tipo de filtro.** En la lista, haga clic en **Integrado** o **Plug-in** y, a continuación, siga los procedimientos de la opción que elija. El valor predeterminado es **Integrado**.

Tipo de filtro integrado

- **Filtro de contenido web**

- **Filtro automático habilitado.** Seleccione si utilizar la función de filtro automático de Apple para analizar sitios web en busca de contenido inadecuado. Está **desactivado** de forma predeterminada.
- **Direcciones URL permitidas.** Esta lista se omite si la opción **Filtro automático habilitado** está **desactivada**. Si la opción **Filtro automático habilitado** está **activada**, los elementos de esta lista son siempre accesibles, independientemente de si el filtro automático permite el acceso. Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada URL a la lista de permitidos:
  * Escriba la URL del sitio web permitido. Debe agregar `http://` o `https://` antes de la dirección web.
  * Haga clic en **Guardar** para guardar el sitio web en la lista de permitidos, o bien haga clic en **Cancelar** para no guardarlo.
- **Direcciones URL en lista negra.** Los elementos de esta lista están siempre bloqueados. Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada URL a la lista de bloqueados:
  * Escriba la URL del sitio web que quiere bloquear. Debe agregar `http://` o `https://` antes de la dirección web.
  * Haga clic en **Guardar** para guardar el sitio web en la lista de bloqueados, o bien haga clic en **Cancelar** para cancelar la operación.

    > **Nota:**
    > La consola de XenMobile Server contiene los términos “lista negra” y “lista blanca”. Estamos cambiando esos términos en una próxima versión a “lista de bloqueados” y “lista de permitidos”.

- **Lista blanca de marcadores**
  - **Lista blanca de marcadores.** Especifica los sitios a los que pueden acceder los usuarios. Agregue las URL de los sitios web para permitir el acceso a ellos.
    * **URL.** La URL de cada sitio web al que los usuarios pueden acceder. Por ejemplo, para permitir el acceso a la tienda Secure Hub, agregue la URL de XenMobile Server a la lista **URL**. Debe agregar `http://` o `https://` antes de la dirección web. Este campo es obligatorio.
    * **Carpeta de marcadores.** Escriba un nombre opcional para la carpeta de marcadores. Si este campo se deja en blanco, el marcador se agrega al directorio predeterminado de marcadores.
    * **Título.** Escriba un título descriptivo para el sitio web. Por ejemplo, introduzca “Google” para la dirección URL `https://google.com`.
    * Haga clic en **Guardar** para guardar el sitio web en la lista de permitidos, o bien haga clic en **Cancelar** para no guardarlo.

Tipo de filtro plug-in

- **Nombre del filtro.** Escriba un nombre único para el filtro.
- **Identificador.** Escriba el ID de paquete del plugin que proporciona el servicio de filtrado.
- **Dirección del servicio.** Escriba una dirección de servidor opcional. Los formatos válidos son la URL, la dirección IP o el nombre de host.
- **Nombre de usuario.** Escriba un nombre de usuario opcional para el servicio.
- **Contraseña.** Escriba una contraseña opcional para el servicio.
- **Certificado.** En la lista, haga clic en el certificado de identidad opcional que se va a usar para autenticar al usuario en el servicio. El valor predeterminado es **Ninguno**.
- **Filtrar tráfico de WebKit.** Seleccione si se debe filtrar el tráfico WebKit.
- **Filtrar tráfico de socket.** Seleccione si filtrar el tráfico de sockets.
- **Datos personalizados.** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada clave personalizada al filtro Web:
  - **Clave.** Escriba la clave personalizada.
  - **Valor.** Escriba un valor para la clave personalizada.
  - Haga clic en **Guardar** para guardar la clave personalizada, o bien haga clic en **Cancelar** para cancelar la operación.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva de clip web

January 4, 2022

Puede colocar accesos directos, o clips web, para que los sitios web aparezcan junto a las aplicaciones en los dispositivos de los usuarios. Puede especificar sus propios iconos para representar los clips web en dispositivos iOS, iPadOS, macOS y Android. Las tabletas Windows solo requieren una etiqueta y una URL. Para dispositivos iOS e iPadOS, configure la directiva de diseño de pantalla de inicio para organizar los clips web que cree. Si restringe el acceso a aplicaciones en iOS, asegúrese de configurar la directiva de restricciones para permitir clips web. Para obtener información sobre la configuración de estas directivas, consulte Directiva de diseño de pantalla inicio y Directiva de restricciones.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener

más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Etiqueta:** 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 `https://server`.
- **Eliminable:** Seleccione si los usuarios pueden quitar el clip web. Está **desactivado** de forma predeterminada.
- **Icono a actualizar:** Seleccione el icono que se utilizará para el clip web. Para ello, haga clic en **Examinar** para ir a la ubicación del archivo.
- **Icono precompuesto:** Seleccione si habrá efectos que se aplicarán al icono (como esquinas redondeadas, sombra paralela y brillo de reflejos, entre otros). El valor predeterminado es **No**, con lo que se agregan efectos.
- **Pantalla completa:** Seleccione si la página web enlazada se abre en modo de pantalla completa. Está **desactivado** de forma predeterminada.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de macOS

- **Etiqueta:** 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 `https://server`.
- **Icono a actualizar:** Seleccione el icono que se utilizará para el clip web. Para ello, haga clic en Examinar para ir a la ubicación del archivo.

Parámetros de Android

- **Regla:** Seleccione si esta directiva agrega o quita clips web. El valor predeterminado es **Agregar**.

- **Etiqueta:** Escriba la etiqueta que aparecerá con el clip web.
- **URL:** Escriba la URL asociada al clip web.
- **Definir un icono:** Seleccione si quiere usar un archivo de icono. Está **desactivado** de forma predeterminada.
- **Archivo del icono:** Si **activa** el parámetro **Definir un icono**, deberá seleccionar el archivo de icono que se va a usar. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Parámetros de escritorios y tabletas Windows

- **Nombre:** Escriba la etiqueta que aparecerá con el clip web.
- **URL:** Escriba la URL asociada al clip web.

Directiva Wi-Fi

January 4, 2022

Puede crear o modificar las directivas de Wi-Fi desde la página **Configurar > Directivas de dispositivo** de la consola de XenMobile. Las directivas de Wi-Fi permiten administrar cómo los usuarios conectan sus dispositivos a redes Wi-Fi definiendo los siguientes elementos:

- Tipos y nombres de red
- Directivas de autenticación y seguridad
- Uso de servidor proxy
- Otros datos relacionados con redes Wi-Fi

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

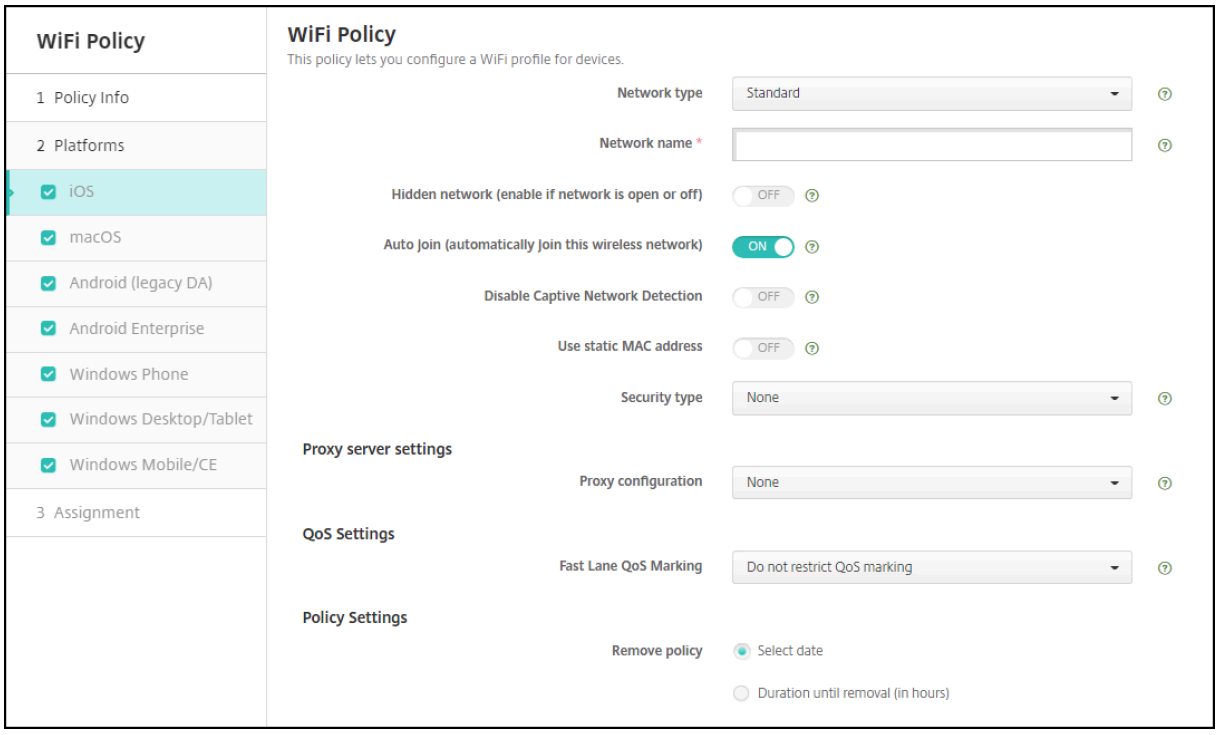
Requisitos previos

Antes de crear una directiva, lleve a cabo estos pasos:

- Cree los grupos de entrega que va a utilizar.
- Averigüe el nombre y el tipo de red.
- Averigüe los métodos de autenticación o los tipos de seguridad que va a utilizar.
- Averigüe cualquier información del servidor proxy que pueda necesitar.
- Instalar los certificados de CA necesarios.
- Obtenga todas las claves compartidas necesarias.
- Cree una entidad PKI para la autenticación por certificado.
- Configure proveedores de credenciales.

Para obtener más información, consulte Autenticación y sus apartados.

Parámetros de iOS



- **Tipo de red:** En la lista, haga clic en **Estándar**, **Hotspot antiguo** o **Hotspot 2.0** para establecer el tipo de red que quiere usar.
- **Nombre de la red:** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo. No se aplica a **Hotspot 2.0**.

- **Red oculta (habilitar si la red está abierta o inactiva):** Elija si la red está oculta o no.
- **Unirse automáticamente (a esta red inalámbrica).** Seleccione si se conecta a la red automáticamente o no. Si un dispositivo iOS ya está conectado a otra red, no se unirá a esta. El usuario debe desconectarse de la red anterior antes de que el dispositivo se pueda conectar automáticamente. Está **activado** de forma predeterminada.
- **Usar dirección MAC estática:** Las direcciones MAC son identificadores únicos que un dispositivo transmite dentro de una red. Para aumentar la privacidad, los dispositivos iOS e iPadOS pueden usar una dirección MAC diferente cada vez que se conectan a una red. Si está **activado**, el dispositivo utiliza siempre la misma dirección MAC cuando se conecta a esta red. Si está **desactivado**, el dispositivo utiliza una dirección MAC diferente cada vez que se conecta a esta red. Está **desactivado** de forma predeterminada.
- **Tipo de seguridad.** En la lista, haga clic en el tipo de seguridad que quiere usar. No se aplica a **Hotspot 2.0**.
  - Ninguna. No requiere ninguna configuración adicional.
  - WEP
  - WPA o WPA2 Personal
  - Cualquiera (Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise: El uso de WPA-2 Enterprise requiere configurar el protocolo SCEP (Simple Certificate Enrollment Protocol). Así, XenMobile puede enviar el certificado a los dispositivos para autenticarse en el servidor Wi-Fi. Para configurar SCEP, vaya a la página Distribución en **Parámetros > Proveedores de credenciales**. Para obtener más información, consulte Proveedores de credenciales.
  - Cualquiera (Enterprise)

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

Parámetros de iOS para WPA, WPA Personal, Cualquiera (Personal)

Contraseña: Si quiere, escriba una contraseña. Si deja este campo en blanco, los usuarios pueden recibir un aviso para introducir la contraseña al iniciar sesión.

Parámetros de iOS para WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Cualquiera (Enterprise)

Al seleccionar estos parámetros, aparecen después de **Parámetros del servidor proxy**.

- **Protocolos, tipos de EAP aceptados:** Habilite los tipos de EAP que quiera admitir y, a continuación, configure los parámetros asociados. Está **desactivado** de forma predeterminada para cada uno de los tipos de EAP disponibles.

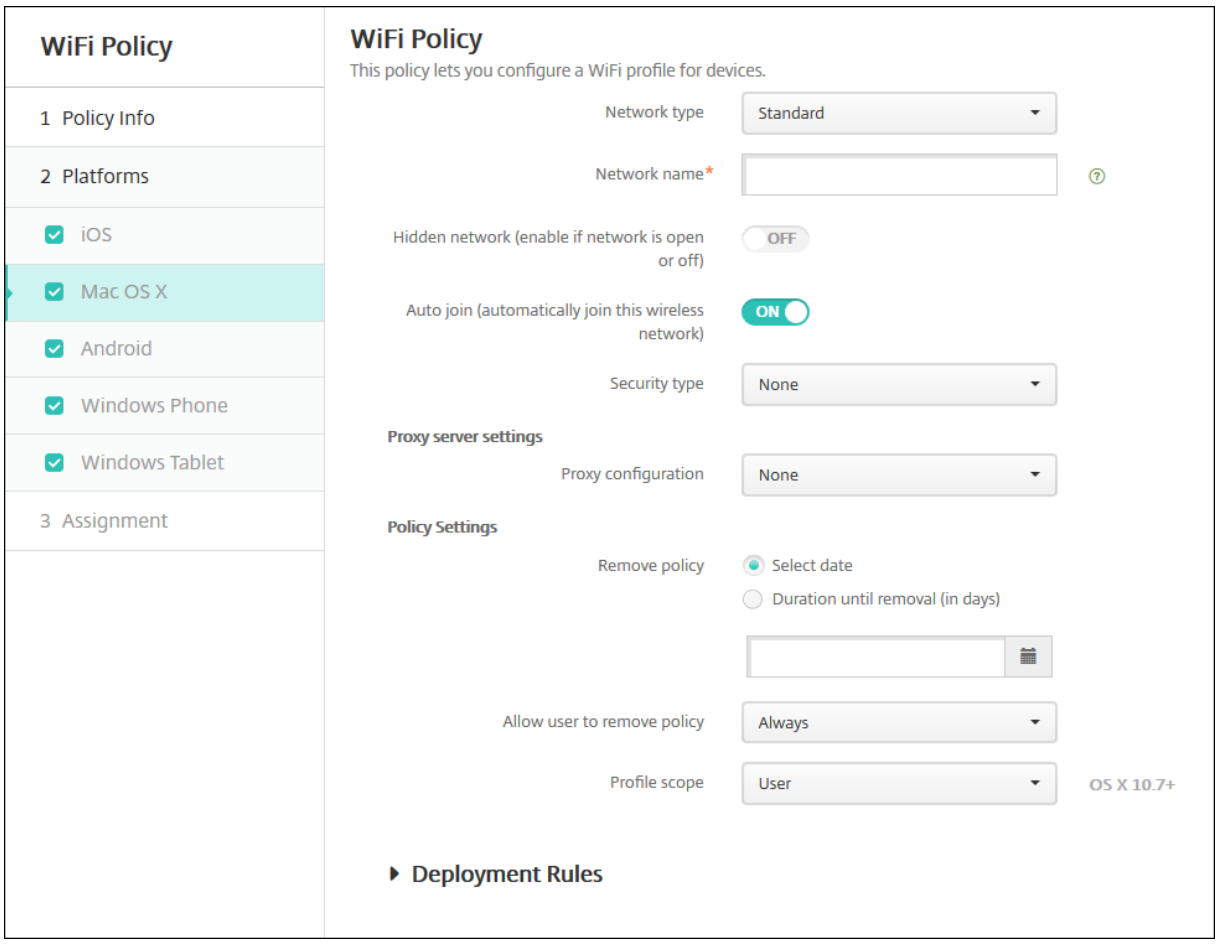
- **Autenticación interna (TTLS).** *Solo es necesario cuando se habilita TTLS*. En la lista, seleccione el método de autenticación interna que quiere usar. Las opciones son: **PAP**, **CHAP**, **MSCHAP** o **MSCHAPv2**. El valor predeterminado es **MSCHAPv2**.
- **Protocolos, EAP-FAST:** Seleccione si quiere usar las credenciales de acceso protegido (PAC).
  - Si selecciona **Usar PAC**, elija si quiere usar unas credenciales PAC de aprovisionamiento.
    - Si selecciona **Aprovisionar PAC**, elija si quiere permitir un protocolo anónimo de enlace TLS entre el cliente del usuario final y XenMobile.
      - **Aprovisionar PAC anónimamente**
- **Autenticación:**
  - **Nombre de usuario:** Escriba un nombre de usuario.
  - **Contraseña por conexión.** Seleccione si quiere requerir una contraseña cada vez que los usuarios inicien sesión.
  - **Contraseña:** Si quiere, escriba una contraseña. Si deja este campo en blanco, los usuarios pueden recibir un aviso para introducir la contraseña al iniciar sesión.
  - **Credencial de identidad (PKI o almacén de claves).** En la lista, haga clic en el tipo de credencial de identidad. El valor predeterminado es **Ninguno**.
  - **Identidad externa:** Opción *requerida solamente cuando se habilita* **PEAP**, **TTLS** *o* **EAP-FAST**. Escriba el nombre de usuario que será visible externamente. Puede aumentar la seguridad si escribe un término genérico como "anónimo" para que no pueda verse el nombre del usuario.
  - **Requerir certificado TLS.** Elija si quiere requerir un certificado TLS.
- **Confianza**
  - **Certificados de confianza.** Para agregar cada certificado de confianza, haga clic en **Agregar** y haga lo siguiente:
    - **Aplicación.** En la lista, elija la aplicación que quiere agregar.
    - Haga clic en **Guardar** para guardar el certificado, o bien en **Cancelar** para cancelar la operación.
  - **Nombres de certificado de servidor de confianza.** Para agregar cada nombre común de los certificados de confianza del servidor, haga clic en **Agregar** y haga lo siguiente:
    - **Certificado.** Escriba el nombre del certificado de servidor. Puede usar comodines para especificar el nombre, como wpa.*.ejemplo.com.
    - Haga clic en **Guardar** para guardar el nombre del certificado, o bien en **Cancelar** para cancelar la operación.
- **Permitir excepciones en la confianza.** Elija si quiere que el cuadro de diálogo de confianza en el certificado aparezca en los dispositivos de los usuarios cuando un certificado no sea de confianza. Está **activado** de forma predeterminada.
- **Parámetros del servidor proxy**
  - **Configuración de proxy.** En la lista, elija **Ninguno**, **Manual** o **Automático** 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 **Ninguno**, que no requiere ninguna configuración adicional.

- Si selecciona **Manual**, configure los siguientes parámetros:
  - **Dirección IP / nombre de host.** Escriba el nombre de host o la dirección IP del servidor proxy.
  - **Puerto.** Escriba el número de puerto del servidor proxy.
  - **Nombre de usuario:** Si quiere, escriba un nombre de usuario para la autenticación en el servidor proxy.
  - **Contraseña:** Si quiere, escriba una contraseña para la autenticación en el servidor proxy.
- Si hace clic en **Automático**, configure los siguientes parámetros:
  - **URL del servidor:** Escriba la dirección URL del archivo PAC que define la configuración de proxy.
  - **Permitir conexión directa si no se puede acceder al archivo PAC:** Elija si permitir que los usuarios se conecten directamente al destino si no se puede acceder al archivo PAC. Está **activado** de forma predeterminada. Esta opción solo está disponible para iOS 7.0 y versiones posteriores.

- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de macOS



- **Tipo de red:** En la lista, haga clic en **Estándar**, **Hotspot antiguo** o **Hotspot 2.0** para establecer el tipo de red que quiere usar.
- **Nombre de la red:** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo. No se aplica a **Hotspot 2.0**.
- **Red oculta (habilitar si la red está abierta o inactiva):** Elija si la red está oculta o no.
- **Unirse automáticamente (a esta red inalámbrica).** Seleccione si se conecta a la red automáticamente o no. Si un dispositivo ya está conectado a otra red, no se unirá a esta. El usuario debe desconectarse de la red anterior antes de que el dispositivo se pueda conectar automáticamente. Está **activado** de forma predeterminada.
- **Tipo de seguridad.** En la lista, haga clic en el tipo de seguridad que quiere usar. No se aplica a **Hotspot 2.0**.
  - Ninguna. No requiere ninguna configuración adicional.
  - WEP
  - WPA o WPA2 Personal
  - Cualquiera (Personal)
  - WEP Enterprise

  - WPA o WPA2 Enterprise
  - Cualquiera (Enterprise)

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

Parámetros de macOS para WPA, WPA Personal, WPA 2 Personal, Cualquiera (Personal)

- **Contraseña:** Si quiere, escriba una contraseña. Si deja este campo en blanco, los usuarios pueden recibir un aviso para introducir la contraseña al iniciar sesión.

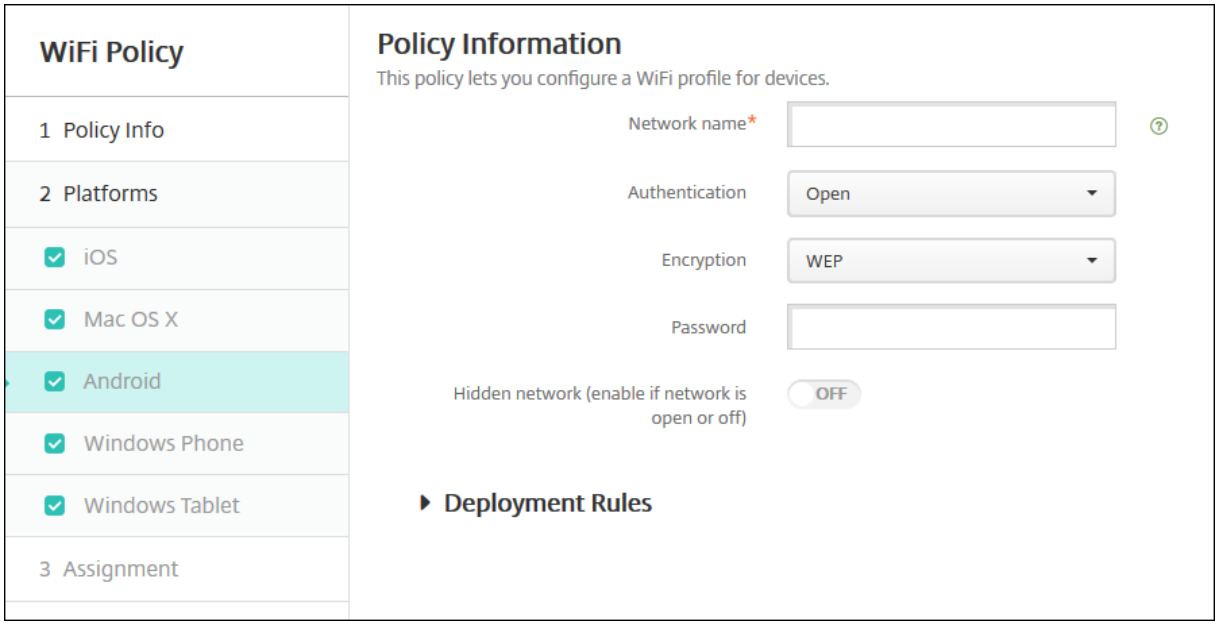
Parámetros de macOS para WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Cualquiera (Enterprise)

Al seleccionar estos parámetros, aparecen después de **Parámetros del servidor proxy**.

- **Protocolos, tipos de EAP aceptados:** Habilite los tipos de EAP que quiera admitir y, a continuación, configure los parámetros asociados. Está **desactivado** de forma predeterminada para cada uno de los tipos de EAP disponibles.
- **Autenticación interna (TTLS).** *Solo es necesario cuando se habilita TTLS*. En la lista, seleccione el método de autenticación interna que quiere usar. Las opciones son: **PAP**, **CHAP**, **MSCHAP** o **MSCHAPv2**. El valor predeterminado es **MSCHAPv2**.
- **Protocolos, EAP-FAST:** Seleccione si quiere usar las credenciales de acceso protegido (PAC).
  - Si selecciona **Usar PAC**, elija si quiere usar unas credenciales PAC de aprovisionamiento.
    - Si selecciona **Aprovisionar PAC**, elija si quiere permitir un protocolo anónimo de enlace TLS entre el cliente del usuario final y XenMobile.
      - **Aprovisionar PAC anónimamente**
- **Autenticación:**
  - **Nombre de usuario:** Escriba un nombre de usuario.
  - **Contraseña por conexión.** Seleccione si quiere requerir una contraseña cada vez que los usuarios inicien sesión.
  - **Contraseña:** Si quiere, escriba una contraseña. Si deja este campo en blanco, los usuarios pueden recibir un aviso para introducir la contraseña al iniciar sesión.
  - **Credencial de identidad (PKI o almacén de claves).** En la lista, haga clic en el tipo de credencial de identidad. El valor predeterminado es **Ninguno**.
  - **Identidad externa:** Opción *requerida solamente cuando se habilita* **PEAP**, **TTLS** *o* **EAP-FAST**. Escriba el nombre de usuario que será visible externamente. Puede aumentar la seguridad si escribe un término genérico como “anónimo” para que no pueda verse el nombre del usuario.
  - **Requerir certificado TLS.** Elija si quiere requerir un certificado TLS.
- **Confianza**

  - **Certificados de confianza.** Para agregar cada certificado de confianza, haga clic en **Agregar** y haga lo siguiente:
    * **Aplicación.** En la lista, elija la aplicación que quiere agregar.
    * Haga clic en **Guardar** para guardar el certificado, o bien en **Cancelar** para cancelar la operación.
  - **Nombres de certificado de servidor de confianza.** Para agregar cada nombre común de los certificados de confianza del servidor, haga clic en **Agregar** y haga lo siguiente:
    * **Certificado.** Escriba el nombre del certificado de servidor que quiere agregar. Puede usar comodines para especificar el nombre, como wpa.*.ejemplo.com.
    * Haga clic en **Guardar** para guardar el nombre del certificado, o bien en **Cancelar** para cancelar la operación.
- **Permitir excepciones en la confianza.** Elija si quiere que el cuadro de diálogo de confianza en el certificado aparezca en los dispositivos de los usuarios cuando un certificado no sea de confianza. Está **activado** de forma predeterminada.
- **Usar como configuración de ventana de inicio de sesión.** Elija si utilizar las mismas credenciales especificadas en la ventana de inicio de sesión para autenticar al usuario.
- **Parámetros del servidor proxy**
  - **Configuración de proxy.** En la lista, elija **Ninguno**, **Manual** o **Automático** 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 **Ninguno**, que no requiere ninguna configuración adicional.
  - Si selecciona **Manual**, configure los siguientes parámetros:
    * **Dirección IP / nombre de host.** Escriba el nombre de host o la dirección IP del servidor proxy.
    * **Puerto.** Escriba el número de puerto del servidor proxy.
    * **Nombre de usuario:** Si quiere, escriba un nombre de usuario para la autenticación en el servidor proxy.
    * **Contraseña:** Si quiere, escriba una contraseña para la autenticación en el servidor proxy.
  - Si hace clic en **Automático**, configure los siguientes parámetros:
    * **URL del servidor:** Escriba la dirección URL del archivo PAC que define la configuración de proxy.
    * **Permitir conexión directa si no se puede acceder al archivo PAC:** Elija si permitir que los usuarios se conecten directamente al destino si no se puede acceder al archivo PAC. Está **activado** de forma predeterminada. Esta opción solo está disponible para iOS 7.0 y versiones posteriores.

Parámetros de Android



- **Nombre de la red:** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **Autenticación:** En la lista, elija 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.

Parámetros de Android para red abierta y compartida

- **Cifrado:** En la lista, elija **Inhabilitado** o **WEP**. El valor predeterminado es **WEP**.
- **Contraseña:** Si quiere, escriba una contraseña.

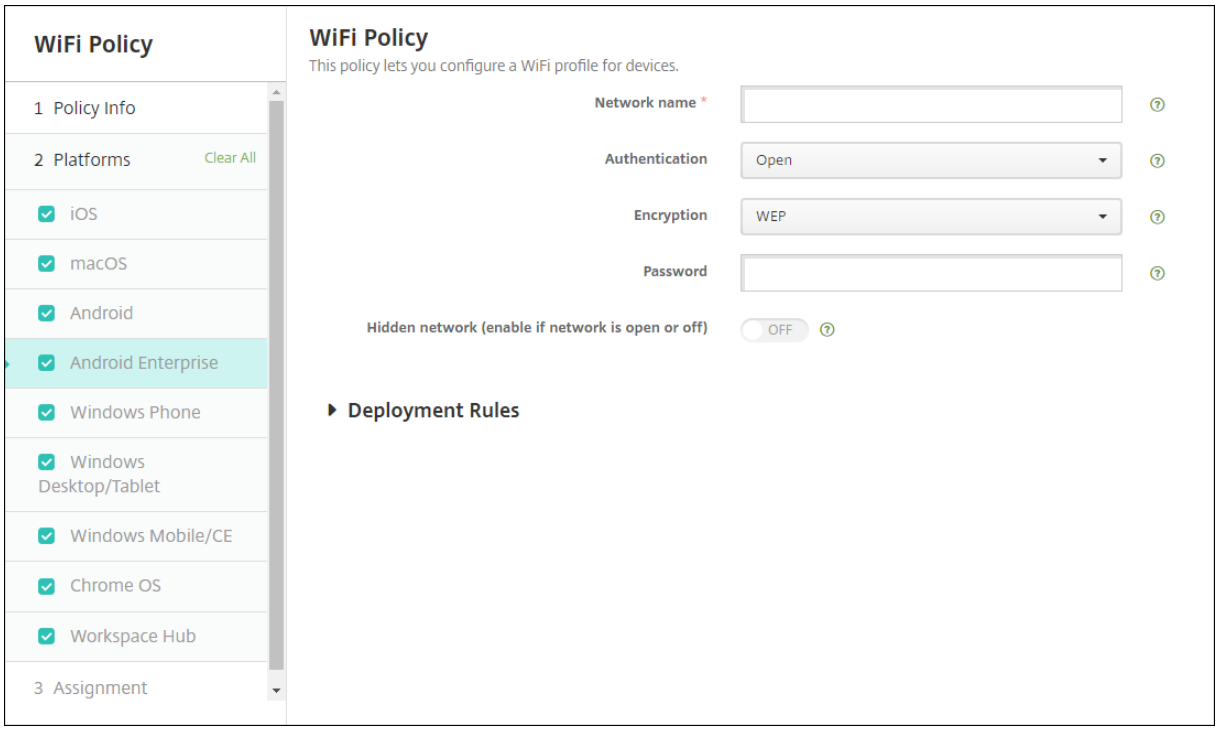
Parámetros de Android para WPA, WPA-PSK, WPA2, WPA2-PSK

- **Cifrado:** En la lista, elija **TKIP** o **AES**. El valor predeterminado es **TKIP**.
- **Contraseña:** Si quiere, escriba una contraseña.

Parámetros de Android para 802.1x

- **Tipo de EAP:** En la lista, elija **PEAP**, **TLS** o **TTLS**. El valor predeterminado es **PEAP**.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Autenticación fase 2:** En la lista, elija **Ninguna**, **PAP**, **MSCHAP**, **MSCHAPPv2** o **GTC**. El valor predeterminado es **PAP**.
- **Identidad:** Escriba el nombre de usuario y el dominio opcionales.
- **Anónimo:** Escriba el nombre de usuario opcional que será visible externamente. Puede aumentar la seguridad si escribe un término genérico como “anónimo” para que no pueda verse el nombre del usuario.
- **Certificado de CA:** En la lista, elija el certificado que se va a utilizar.
- **Credencial de identidad:** En la lista, elija la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
- **Red oculta (habilitar si la red está abierta o inactiva):** Elija si la red está oculta o no.

Parámetros de Android Enterprise



- **Nombre de la red:** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **Autenticación:** En la lista, elija 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.

Parámetros de Android para red abierta y compartida

- **Cifrado:** En la lista, elija **Inhabilitado** o **WEP**. El valor predeterminado es **WEP**.
- **Contraseña:** Si quiere, escriba una contraseña.

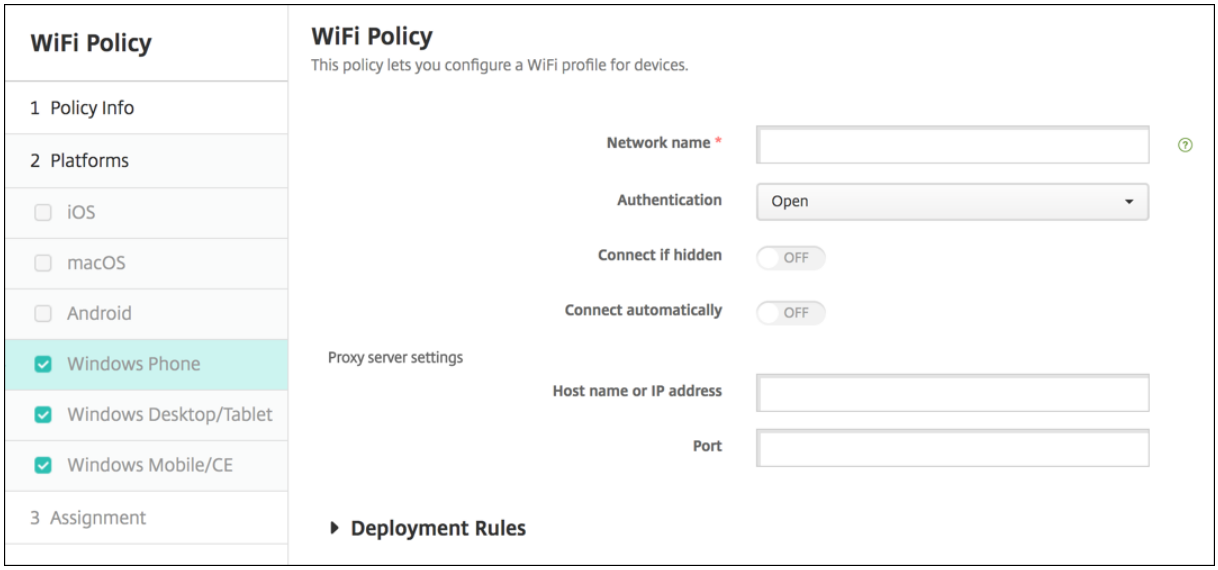
Parámetros de Android para WPA, WPA-PSK, WPA2, WPA2-PSK

- **Cifrado:** En la lista, elija TKIP o AES. El valor predeterminado es TKIP.
- **Contraseña:** Si quiere, escriba una contraseña.

Parámetros de Android para 802.1x

- **Tipo de EAP:** En la lista, elija **PEAP**, **TLS** o **TTLS**. El valor predeterminado es **PEAP**.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Autenticación fase 2:** En la lista, elija **Ninguna**, **PAP**, **MSCHAP**, **MSCHAPPv2** o **GTC**. El valor predeterminado es **PAP**.
- **Identidad:** Escriba el nombre de usuario y el dominio opcionales.
- **Anónimo:** Escriba el nombre de usuario opcional que será visible externamente. Puede aumentar la seguridad si escribe un término genérico como “anónimo” para que no pueda verse el nombre del usuario.
- **Certificado de CA:** En la lista, elija el certificado que se va a utilizar.
- **Credencial de identidad:** En la lista, elija la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
- **Red oculta (habilitar si la red está abierta o inactiva):** Elija si la red está oculta o no.

Parámetros de Windows Phone



- **Nombre de la red:** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **Autenticación:** En la lista, elija el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
  - Abierta
  - WPA Personal
  - WPA2 Personal
  - WPA-2 Enterprise: El uso de WPA-2 Enterprise requiere configurar SCEP. La configuración de SCEP permite a XenMobile enviar el certificado a los dispositivos para autenticarse en el servidor Wi-Fi. Para configurar SCEP, vaya a la página **Distribución** en **Parámetros > Proveedores de credenciales**. 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.

Parámetros de Windows Phone para red abierta

- **Conectar si está oculta:** Elija si establecer conexión cuando la red esté oculta.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.

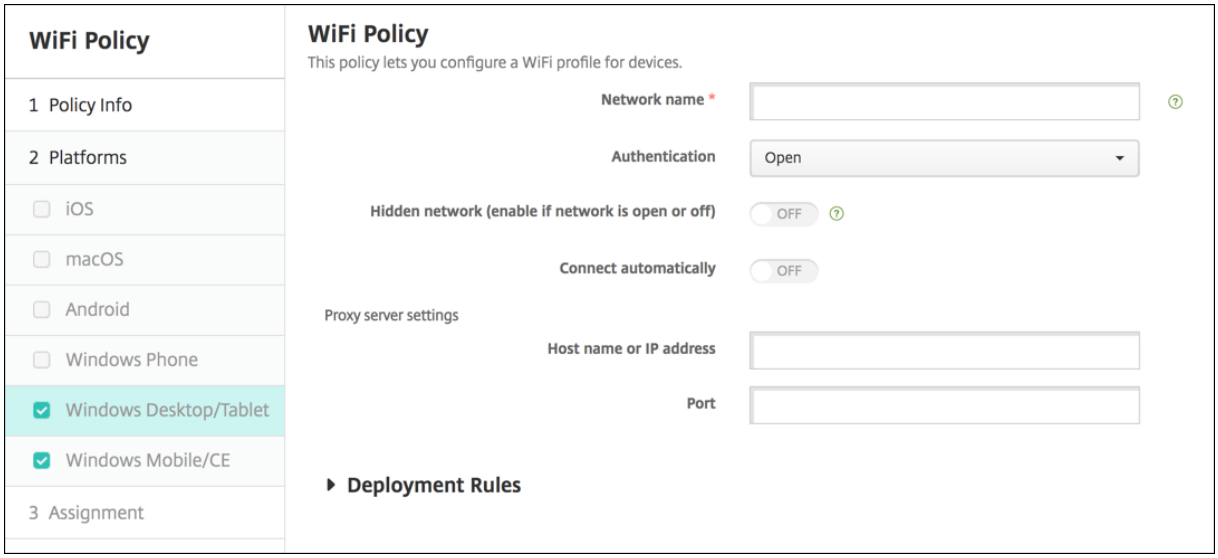
Parámetros de Windows Phone para WPA Personal, WPA-2 Personal

- **Cifrado:** En la lista, elija **AES** o **TKIP** para establecer el tipo de cifrado. El valor predeterminado es **AES**.
- **Conectar si está oculta:** Elija si establecer conexión cuando la red esté oculta.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.

Parámetros de Windows Phone para WPA-2 Enterprise

- **Cifrado:** En la lista, elija **AES** o **TKIP** para establecer el tipo de cifrado. El valor predeterminado es **AES**.
- **Tipo de EAP:** En la lista, elija **PEAP-MSCHAPv2** o **TLS** para establecer el tipo de EAP. El valor predeterminado es **PEAP-MSCHAPv2**.
- **Conectar si está oculta:** Elija si establecer conexión cuando la red esté oculta.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.
- **Enviar certificado mediante SCEP:** Elija si quiere insertar el certificado en los dispositivos de los usuarios mediante el Protocolo de inscripción de certificados simple (SCEP).
- **Proveedor de credenciales para SCEP:** En la lista, seleccione el proveedor de credenciales del protocolo SCEP. El valor predeterminado es **Ninguno**.
- **Parámetros del servidor proxy**
  - **Nombre de host o dirección IP:** Escriba el nombre o la dirección IP del servidor proxy.
  - **Puerto:** Escriba el número de puerto del servidor proxy.
- **Configuraciones de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
    - **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Parámetros de Windows 10 y Windows 11



- **Autenticación:** En la lista, haga clic en el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
  - Abierta
  - WPA Personal
  - WPA2 Personal
  - WPA Enterprise
  - WPA-2 Enterprise: El uso de WPA-2 Enterprise requiere configurar SCEP. La configuración de SCEP permite a XenMobile enviar el certificado a los dispositivos para autenticarse en el servidor Wi-Fi. Para configurar SCEP, vaya a la página **Distribución** en **Parámetros > Proveedores de credenciales**. 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.

Parámetros abiertos de Windows 10 y Windows 11

- **Red oculta (habilitar si la red está abierta o inactiva):** Elija si la red está oculta o no.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.

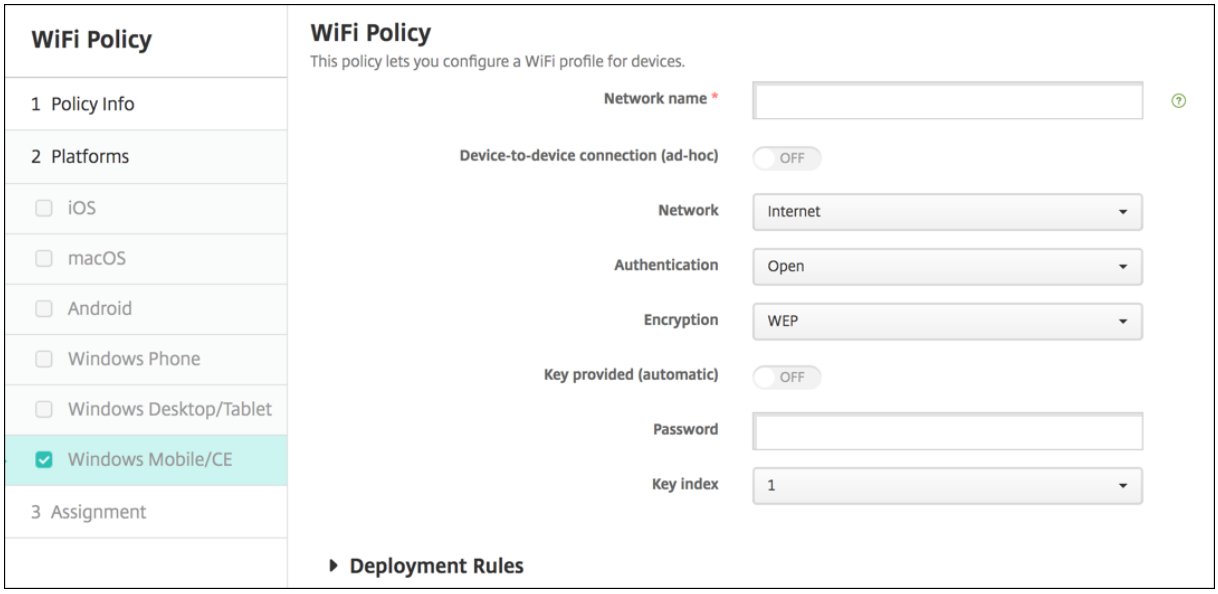
Parámetros de WPA Personal y WPA-2 Personal para Windows 10 y Windows 11

- **Cifrado:** En la lista, elija **AES** o **TKIP** para establecer el tipo de cifrado. El valor predeterminado es **AES**.
- **Red oculta (habilitar si la red está abierta o inactiva):** Elija si la red está oculta o no.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.

Parámetros de WPA-2 Enterprise para Windows 10 y Windows 11

- **Cifrado:** En la lista, elija **AES** o **TKIP** para establecer el tipo de cifrado. El valor predeterminado es **AES**.
- **Tipo de EAP:** En la lista, elija **PEAP-MSCHAPv2** o **TLS** para establecer el tipo de EAP. El valor predeterminado es **PEAP-MSCHAPv2**.
- **Conectar si está oculta:** Elija si la red está oculta.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.
- **Enviar certificado mediante SCEP:** Elija si quiere insertar el certificado en los dispositivos de los usuarios mediante el Protocolo de inscripción de certificados simple (SCEP).
- **Proveedor de credenciales para SCEP:** En la lista, seleccione el proveedor de credenciales del protocolo SCEP. El valor predeterminado es **Ninguno**.

Parámetros de Windows Mobile/CE



- **Nombre de la red:** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **Conexión de dispositivo a dispositivo (ad-hoc):** Permite que dos dispositivos se conecten directamente. Está **desactivado** de forma predeterminada.
- **Red:** Elija si el dispositivo está conectado a un origen de Internet externo o a una red de intranet de la oficina.
- **Autenticación:** En la lista, elija el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
  - Abierta
  - WPA Personal
  - WPA2 Personal
  - WPA-2 Enterprise

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

Parámetros de Windows Mobile/CE para red abierta

- **Red oculta (habilitar si la red está abierta o inactiva):** Elija si la red está oculta o no.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.

Parámetros de Windows Mobile/CE para WPA Personal, WPA-2 Personal

- **Cifrado:** En la lista, elija **AES** o **TKIP** para establecer el tipo de cifrado. El valor predeterminado es **AES**.
- **Red oculta (habilitar si la red está abierta o inactiva):** Elija si la red está oculta o no.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.

Parámetros de Windows Mobile/CE para WPA-2 Enterprise

- **Cifrado:** En la lista, elija **AES** o **TKIP** para establecer el tipo de cifrado. El valor predeterminado es **AES**.
- **Tipo de EAP:** En la lista, elija **PEAP-MSCHAPv2** o **TLS** para establecer el tipo de EAP. El valor predeterminado es **PEAP-MSCHAPv2**.
- **Conectar si está oculta:** Elija si la red está oculta.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.
- **Enviar certificado mediante SCEP:** Elija si quiere insertar el certificado en los dispositivos de los usuarios mediante el protocolo de inscripción de certificados simple (SCEP).
- **Proveedor de credenciales para SCEP:** En la lista, seleccione el proveedor de credenciales del protocolo SCEP. El valor predeterminado es **Ninguno**.
- **Clave suministrada (automática):** Seleccione si la clave se proporciona automáticamente. Está **desactivado** de forma predeterminada.
- **Contraseña:** Introduzca aquí la contraseña.
- **Índice de la clave:** Elija el índice de la clave. Las opciones disponibles son: **1**, **2**, **3** y **4**.

Directiva de certificado de Windows CE

January 4, 2022

En XenMobile, puede crear una directiva de dispositivo para crear y entregar certificados de Windows Mobile/CE provenientes de una infraestructura de clave pública externa a los dispositivos de los usuar-

ios. Para obtener más información acerca de los certificados y las entidades de infraestructura PKI, consulte Certificados.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Windows CE

- **Proveedor de credenciales:** En la lista, haga clic en el proveedor de credenciales. El valor predeterminado es **Ninguno**.
- **Contraseña del PKCS#12 generado:** Escriba la contraseña utilizada para cifrar la credencial.
- **Carpeta de destino:** En la lista, haga clic en la carpeta de destino de la credencial o haga clic en **Agregar** para agregar una carpeta que aún no esté en la lista. Las opciones predeterminadas son:
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Nombre del archivo de destino:** Escriba el nombre del archivo de la credencial.

Directiva de Windows Information Protection

January 4, 2022

Windows Information Protection (WIP), anteriormente conocida como Enterprise Data Protection (EDP), es una tecnología de Windows que ofrece protección frente a la filtración potencial de datos de empresa. La filtración de datos se puede producir por compartir datos de empresa con aplicaciones protegidas que no sean de empresa, compartir datos entre las aplicaciones o fuera de la red de la empresa. Para obtener más información, consulte Protect your enterprise data using Windows Information Protection (WIP).

En XenMobile, puede crear una directiva de dispositivo para especificar las aplicaciones que requieren Windows Information Protection al nivel de exigencia que necesite. La directiva Windows Information Protection es para teléfonos, tabletas y escritorios supervisados con Windows 10 o Windows 11.

XenMobile incluye algunas aplicaciones comunes y puede agregar otras. Puede especificar un nivel de aplicación de la directiva que afecte a la experiencia de usuario. Por ejemplo, puede:

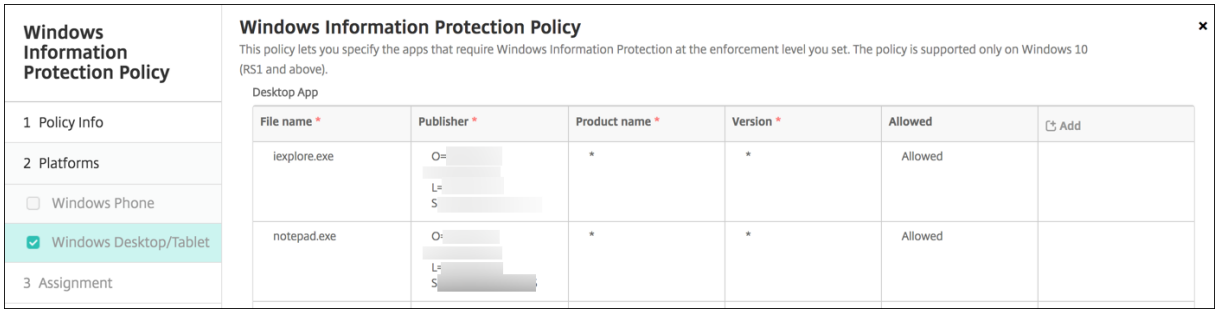
- Bloquear toda forma inadecuada de compartir datos.

- Advertir sobre formas inadecuadas de compartir datos y permitir que los usuarios anulen la directiva.
- Ejecutar WIP de forma silenciosa al iniciar sesión y permitir formas inadecuadas de compartir datos.

Para excluir aplicaciones de Windows Information Protection, defina las aplicaciones en archivos XML de Microsoft AppLocker y, a continuación, importe esos archivos en XenMobile.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Windows 10 y Windows 11



- **Aplicación de escritorio** (escritorios con Windows 10 o Windows 11), **aplicación de almacén** (teléfonos con Windows 10 y tabletas con Windows 10 o Windows 11): XenMobile incluye algunas aplicaciones comunes, como se muestra en el ejemplo anterior. Puede modificar o quitar las aplicaciones según sea necesario.

  Para agregar otras aplicaciones: En la tabla **Aplicación de escritorio** o **Aplicación de tienda**, haga clic en **Agregar** e indique la información de la aplicación.

  Las aplicaciones **Permitidas** pueden leer, crear y actualizar los datos de empresa. Las aplicaciones **Denegadas** no pueden acceder a los datos de empresa. Las aplicaciones **Exentas** pueden leer los datos de empresa, pero no pueden crear ni modificar los datos.

  - **XML de AppLocker:** Microsoft proporciona una lista de las aplicaciones Microsoft que presentan problemas conocidos de compatibilidad con WIP. Para excluir esas aplicaciones de WIP, haga clic en **Examinar** para cargar la lista. XenMobile combina el archivo XML cargado de AppLocker con las aplicaciones de escritorio y tienda en la directiva enviada al dispositivo. Para obtener más información, consulte Recommended deny list for Windows Information Protection.
  - **Nivel de exigencia:** Seleccione una opción para especificar cómo quiere que Windows Information Protection proteja y administre el uso compartido de datos. Está **desactivado** de forma predeterminada.

    * **0-No.** La protección WIP está inhabilitada y no protege ni audita los datos.
    * **1-Silencioso:** La protección WIP se ejecuta de forma silenciosa, registra toda forma inadecuada de compartir datos y no bloquea nada. Puede acceder a los registros desde Informes CSP.
    * **2-Reemplazar:** La protección WIP advierte a los usuarios sobre una forma potencialmente no segura de compartir datos. Los usuarios pueden anular las advertencias y compartir los datos. Este modo registra las acciones, incluidas las anulaciones del usuario, en el registro de auditoría.
    * **3-Bloquear:** La protección WIP impide que los usuarios compartan datos de manera potencialmente no segura.

- **Nombres de dominio protegidos:** Los dominios que la empresa usa para la identidad de los usuarios. Esta lista de dominios de identidad administrados, junto con el dominio principal, conforman la identidad de su empresa administradora. El primer dominio de la lista es la identidad de empresa principal utilizada en la interfaz de usuario de Windows. Utilice la barra vertical (|) para separar los elementos de la lista. Por ejemplo: `domain1.com | domain2.com`
- **Certificado de recuperación de datos:** Haga clic en **Examinar** y, a continuación, seleccione el certificado de recuperación que se usará para recuperar datos provenientes de archivos cifrados. Este certificado es el mismo que el certificado del agente de recuperación de datos (DRA) para el sistema de archivos de cifrado (EFS), que solo se entrega a través de MDM en lugar de la directiva de grupo. Si un certificado de recuperación no está disponible, créelo. Para obtener más información, consulte “Crear un certificado de recuperación de datos” en esta sección.
- **Nombres de dominio de red:** Una lista de dominios que incluye los dominios límite de la empresa. WIP protege todo el tráfico a los dominios completos en esta lista. Este parámetro, junto con el parámetro **Intervalo IP**, detecta si un dispositivo de punto final de la red es personal o empresarial en las redes privadas. Utilice comas para separar los elementos de la lista. Por ejemplo: corp.ejemplo.com,region.ejemplo.com
- **Intervalo IP:** Una lista de los intervalos de IPv4 e IPv6 de la empresa que definen los equipos incluidos en la red empresarial. WIP considera estas ubicaciones como un destino seguro para compartir datos empresariales. Utilice comas para separar los elementos de la lista. Por ejemplo:

  `10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff`
- **La lista de intervalos IP es autoritativa:** Para impedir que Windows detecte automáticamente los intervalos de IP, **active** este parámetro. Está **desactivado** de forma predeterminada.

- **Servidores proxy:** Una lista de los servidores proxy que puede usar la empresa para recursos empresariales. Este parámetro es necesario si usa a un proxy en la red. Sin un servidor proxy, los recursos de la empresa podrían no estar disponibles cuando un cliente esté detrás de un proxy. Por ejemplo, es posible que los recursos no estén disponibles en ciertos puntos de acceso Wi-Fi de hoteles y restaurantes. Utilice comas para separar los elementos de la lista. Por ejemplo:

  ```
  proxy.example.com:80;157.54.11.118:443
  ```

- **Servidores proxy internos.** Una lista de los servidores proxy por los que pasan los dispositivos para conectarse a los recursos en la nube. El uso de este tipo de servidor indica que los recursos de la nube a los que se conecta son recursos empresariales. No incluya en esta lista ningún servidor del parámetro **Servidores proxy**, que se utilizan para el tráfico no protegido por WIP. Utilice comas para separar los elementos de la lista. Por ejemplo:

  ```
  example.internalproxy1.com;10.147.80.50
  ```

- **Recursos de nube:** Una lista de recursos de la nube que protege WIP. Para dirigir el tráfico de cada recurso en la nube, también puede especificar un servidor proxy en la lista **Servidores proxy**. Todo el tráfico enrutado a través de **Servidores proxy** se trata como tráfico de empresa. Utilice comas para separar los elementos de la lista. Por ejemplo:

  ```
  domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.
  domain2.com
  ```

- **Definir requisito de protección bajo bloqueo:** Solo para Windows 10 Phone. Si el parámetro está **activado**, también se requiere la directiva Código de acceso. De lo contrario, falla la implementación de la directiva Windows Information Protection. Además, si esta directiva está **activada**, aparecerá el parámetro **Requerir protección durante bloqueo**. Está **desactivado** de forma predeterminada.

- **Requerir protección durante bloqueo:** Solo para Windows 10 Phone. Especifica si se deben cifrar los datos de empresa mediante una clave protegida por un PIN de empleado en un dispositivo bloqueado. Las aplicaciones no pueden leer datos de empresa en un dispositivo bloqueado. Está **activado** de forma predeterminada.

- **Revocar certificado WIP al desinscribir:** Especifica si se deben revocar las claves de cifrado local del dispositivo de usuario cuando se desinscriba de Windows Information Protection. Después de revocar las claves de cifrado, un usuario no puede acceder a los datos de empresa cifrados. Si está **desactivado**, las claves no se revocan y el usuario sigue teniendo acceso a los archivos protegidos después de desinscribirse. Está **activado** de forma predeterminada.

- **Mostrar iconos de superposición:** Especifica si se debe superponer el icono de Windows Information Protection sobre los archivos de empresa en Explorer y en los iconos de aplicaciones solo empresariales en el menú Inicio. Está **desactivado** de forma predeterminada.

Crear un certificado de recuperación de datos

Se requiere un certificado de recuperación de datos para habilitar la directiva **Windows Information Protection**.

1. En la máquina con la consola de XenMobile, abra un símbolo del sistema y vaya a una carpeta (que no sea Windows\System32) donde quiera crear el certificado.
2. Ejecute el comando:

   ```
   cipher /r:ESFDRA
   ```

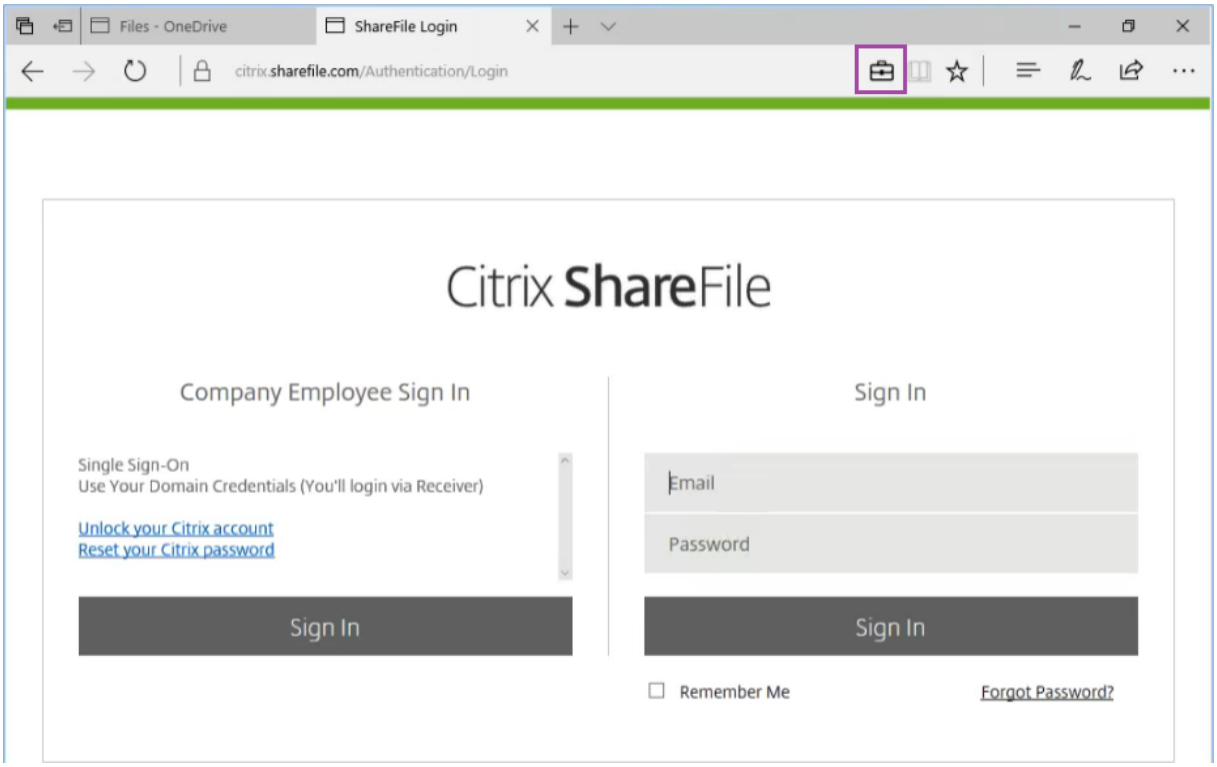
3. Cuando se le solicite, introduzca una contraseña para proteger el archivo de clave privada.

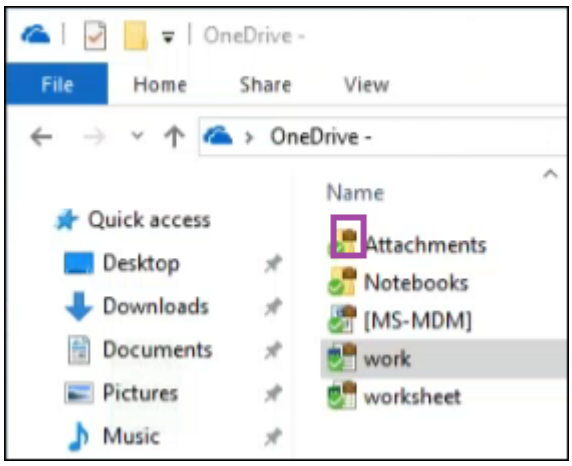
   El comando de cifrado crea un archivo .cer y .pfx.

4. En la consola de XenMobile, vaya a **Parámetros > Certificados** e importe el archivo CER, que se aplica a tabletas con Windows 10 y Windows 11 y a teléfonos con Windows 10.

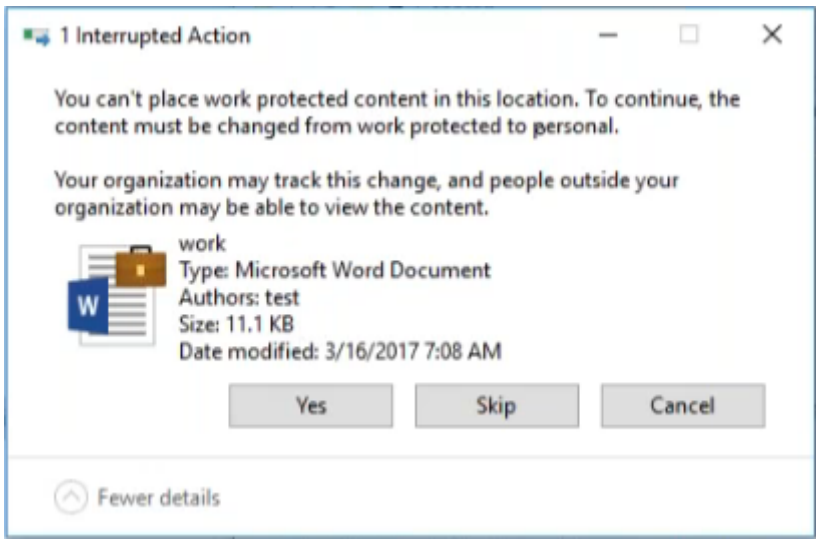
Experiencia de usuario

Cuando Windows Information Protection está en vigor, las aplicaciones y los archivos incluyen un icono:





Si un usuario intenta copiar o guardar un archivo protegido en una ubicación no protegida, aparece la siguiente notificación, dependiendo del nivel de exigencia configurado.



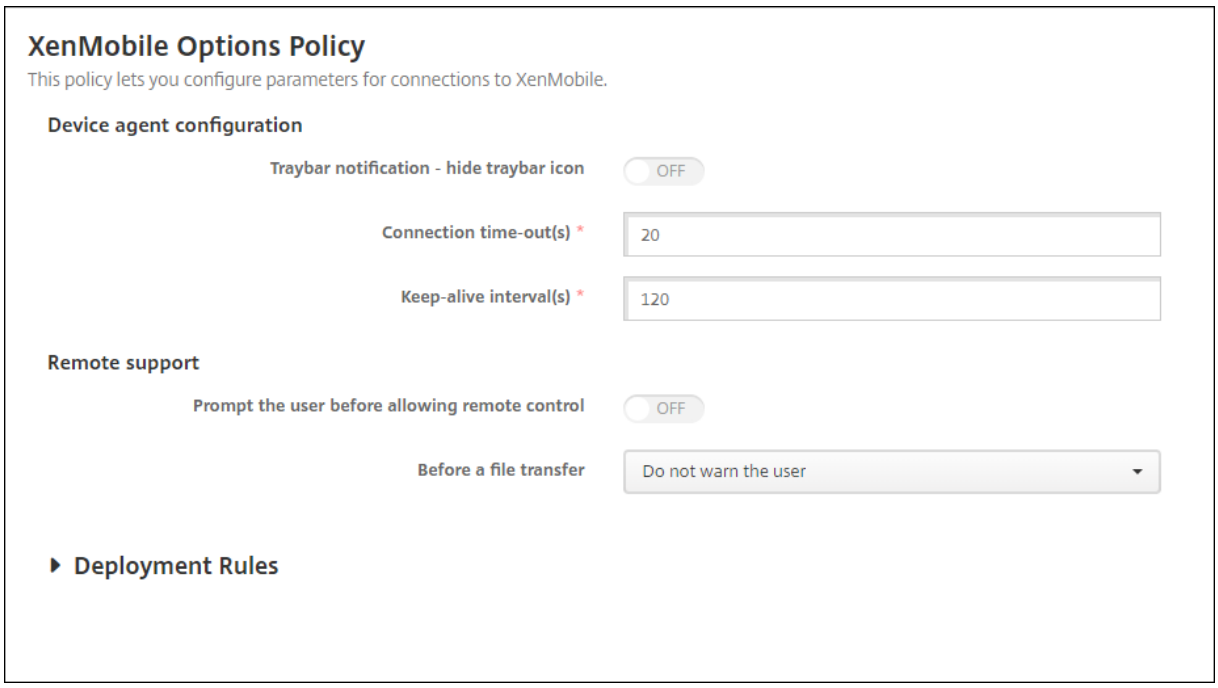
Directiva de opciones de XenMobile

January 4, 2022

Puede agregar una directiva “Opciones de XenMobile” para configurar el comportamiento de Secure Hub al conectarse a XenMobile desde dispositivos Android y Windows Mobile/CE.

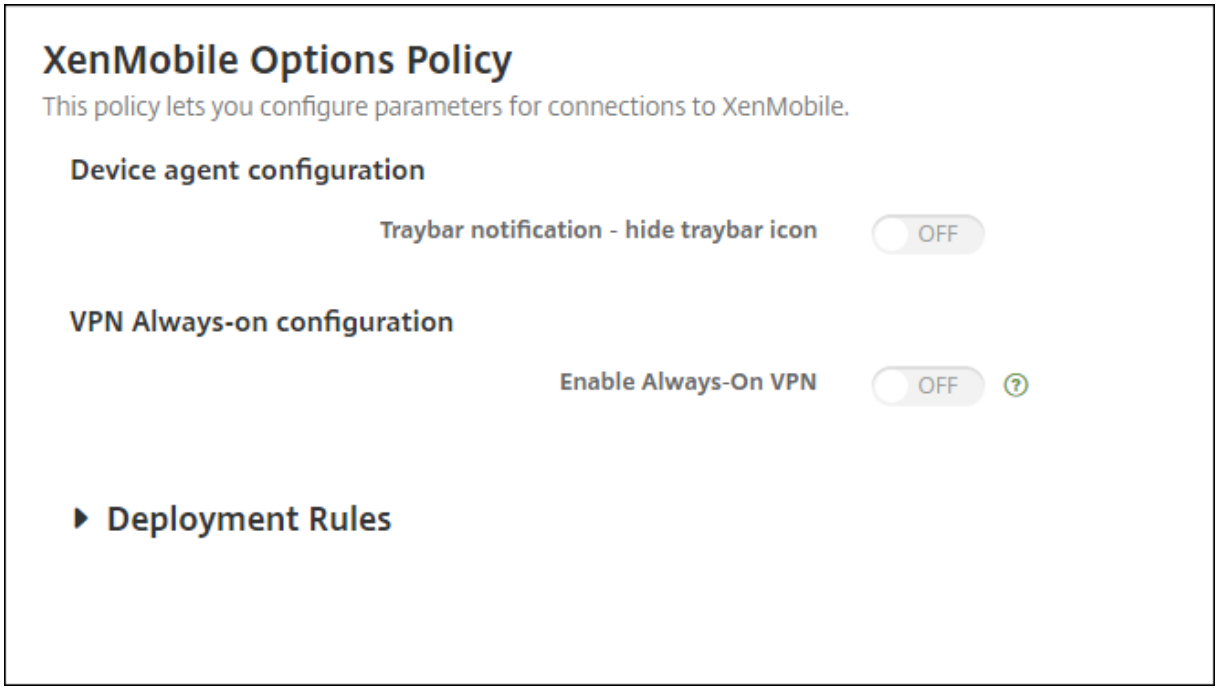
Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de Android



- **Bandeja de notificaciones: ocultar icono:** Seleccione si el icono de la barra de la bandeja será visible o no. Está **desactivado** de forma predeterminada.
- **Tiempos de espera de conexión:** 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.
- **Intervalos de Keep-Alive:** Escriba la cantidad de tiempo en segundos para mantener una conexión abierta. El valor predeterminado es de 120 segundos.
- **Preguntar al usuario antes de permitir el control remoto:** Seleccione si pedir confirmación al usuario antes de permitir el control por asistencia remota. Está **desactivado** de forma predeterminada.
- **Antes de una transferencia de archivos:** 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: **No advertir al usuario**, **Advertir al usuario** y **Pedir permiso al usuario**. El valor predeterminado es **No advertir al usuario**.

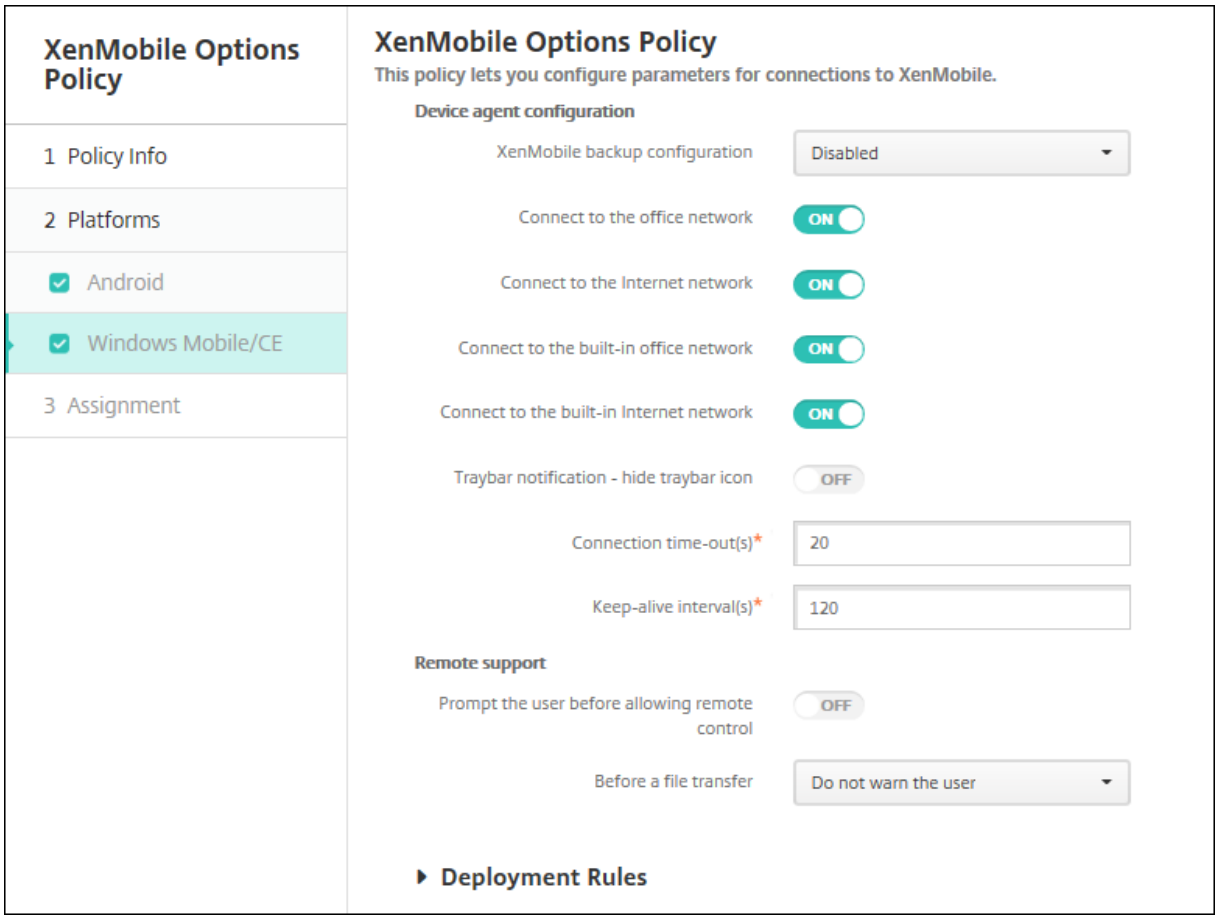
Parámetros de Android Enterprise



Compatible a partir de la versión 7 de Android.

- **Bandeja de notificaciones: ocultar icono:** Seleccione si el icono de la barra de la bandeja será visible o no. Está **desactivado** de forma predeterminada.
- **Habilitar VPN permanente.** Seleccione si la VPN permanente está habilitada. Cuando esta configuración está **activada**, el servicio de VPN se inicia cuando el dispositivo se enciende y sigue ejecutándose mientras el dispositivo esté encendido. Está **desactivado** de forma predeterminada.
- **Paquete VPN.** Escriba el nombre del paquete de la aplicación VPN que utiliza el dispositivo. De forma predeterminada, el nombre del paquete de la aplicación Citrix SSO, **com.citrix.CitrixVPN**, se rellena automáticamente en este campo.

Parámetros de Windows Mobile/CE



- **Configuración del agente del dispositivo**
  - **Configuración de copia de seguridad de XenMobile:** En la lista, haga clic en una opción para la copia de seguridad de la configuración de XenMobile en los dispositivos de los usuarios. De forma predeterminada, está **inhabilitado**. Las opciones disponibles son:
    - Inhabilitado
    - En la primera conexión después de instalar XenMobile
    - En la primera conexión después del reinicio de cada dispositivo
  - **Conectar a la red de la oficina**
  - **Conectar a la red de Internet**
  - **Conectar a la red de la oficina integrada:** Cuando esta opción está **activada**, XenMobile detecta automáticamente la red.
  - **Conectar a la red de Internet integrado:** Cuando esta opción está **activada**, XenMobile detecta automáticamente la red.
  - **Bandeja de notificaciones: ocultar icono:** Seleccione si el icono de la barra de la bandeja será visible o no. Está **desactivado** de forma predeterminada.
  - **Tiempos de espera de conexión:** Escriba la cantidad de tiempo en segundos que una conexión puede estar inactiva antes de que se agote el tiempo de espera. El valor prede-

terminado es de 20 segundos.
  - **Intervalos de Keep-Alive:** Escriba la cantidad de tiempo en segundos para mantener una conexión abierta. El valor predeterminado es de 120 segundos.
- **Asistencia remota**
  - **Preguntar al usuario antes de permitir el control remoto:** Seleccione si pedir confirmación al usuario antes de permitir el control por asistencia remota. Está **desactivado** de forma predeterminada.
  - **Antes de una transferencia de archivos:** 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: **No advertir al usuario**, **Advertir al usuario** y **Pedir permiso al usuario**. El valor predeterminado es **No advertir al usuario**.

Directiva de desinstalación de XenMobile

January 4, 2022

En XenMobile, puede agregar una 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.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de los parámetros de Android y Windows Mobile/CE

- **Desinstalar XenMobile de los dispositivos:** Seleccione si quiere desinstalar XenMobile de todos los dispositivos en los que se implementará esta directiva. Está **desactivado** de forma predeterminada.

Agregar aplicaciones

January 4, 2022

Al agregar aplicaciones a XenMobile, estas se pueden gestionar vía la administración de aplicaciones móviles (MAM). XenMobile simplifica la entrega de aplicaciones, la gestión de licencias de software, la configuración y la administración del ciclo de vida de las aplicaciones.

Habilitar aplicaciones para MDX es una etapa importante en la preparación de la mayoría de los tipos de aplicaciones para su distribución a los dispositivos de los usuarios. Para ver una introducción a

MDX, consulte Acerca de MDX Toolkit y la Introducción al SDK de MAM.

- Citrix recomienda habilitar aplicaciones para MDX con la ayuda del SDK de MAM. Si no, puede seguir empaquetando aplicaciones para MDX hasta que el MDX Toolkit quede obsoleto y se retire. Consulte Elementos retirados.
- No puede utilizar MDX Toolkit para empaquetar aplicaciones móviles de productividad de Citrix. Obtenga los archivos MDX de las aplicaciones móviles de productividad desde las descargas de Citrix.

Al agregar aplicaciones a la consola de XenMobile, puede hacer lo siguiente:

- Configurar las opciones de las aplicaciones
- Opcionalmente, puede organizar las aplicaciones en categorías para organizarlas en Secure Hub
- Opcionalmente, puede definir flujos de trabajo para que se requiera aprobación antes de permitir a los usuarios acceder a una aplicación
- Implementar las aplicaciones a los usuarios

En este artículo, se describen los flujos de trabajo generales para agregar aplicaciones. Consulte los siguientes artículos para conocer datos concretos de cada plataforma:

- Distribuir aplicaciones de Android Enterprise
- Distribuir aplicaciones de Apple

Tipos y funciones de aplicaciones

En la tabla siguiente, se resumen los tipos de aplicaciones que se pueden implementar con XenMobile.

Tipo de aplicación	Fuentes	Notas	Consulte
MDX	Aplicaciones iOS y Android desarrolladas internamente para los usuarios. Aplicaciones móviles de productividad de Citrix.	Desarrolle aplicaciones iOS o Android con el SDK de MAM o empaquételas con MDX Toolkit. Para las aplicaciones móviles de productividad, descargue los archivos MDX de la tienda pública de descargas de Citrix. A continuación, agregue las aplicaciones a XenMobile.	Agregar una aplicación MDX
Tienda pública de aplicaciones	Aplicaciones gratuitas o de pago provenientes de tiendas públicas de aplicaciones, como Google Play o el App Store de Apple.	Cargue las aplicaciones, habilítelas para MDX y, a continuación, agréguelas a XenMobile.	Agregar una aplicación de la tienda pública de aplicaciones
Web y SaaS	La red interna (aplicaciones web) o una red pública (SaaS).	Citrix Workspace ofrece inicio de sesión único SSO móvil a aplicaciones SaaS nativas desde dispositivos iOS y Android inscritos en MDM. O bien, use conectores de aplicación SAML.	Agregar una aplicación web o SaaS

Tipo de aplicación	Fuentes	Notas	Consulte
Empresarial	Aplicaciones privadas, incluidas las aplicaciones Win32, que no están habilitadas para MDX. Aplicaciones privadas de Android Enterprise que están habilitadas para MDX. Las aplicaciones de empresa residen en ubicaciones de red de entrega de contenido o servidores de XenMobile.	Agregue las aplicaciones a XenMobile.	Agregar una aplicación de empresa
Enlace web	Direcciones web de Internet, direcciones web de intranet o aplicaciones web que no requieren inicio SSO.	Configure enlaces web en XenMobile.	Agregar un enlace web

Al planificar la distribución de aplicaciones, tenga en cuenta los siguiente:

- Acerca de las instalaciones silenciosas
- Acerca de aplicaciones obligatorias y opcionales
- Acerca de las categorías de aplicaciones
- Habilitar aplicaciones de Microsoft 365
- Aplicar flujos de trabajo
- Personalizar la marca en el almacén de aplicaciones y Citrix Secure Hub

Acerca de las instalaciones silenciosas

Citrix ofrece la instalación y la actualización de versiones de manera silenciosa de aplicaciones iOS, Android Enterprise y Samsung. La instalación silenciosa significa que no se pide a los usuarios que instalen las aplicaciones que usted implementa en el dispositivo. Las aplicaciones se instalan automáticamente en segundo plano.

Requisitos previos para implementar la instalación silenciosa:

- Para iOS, coloque el dispositivo iOS administrado en modo supervisado. Para obtener más información, consulte Directiva de importación de perfiles de iOS y macOS.
- Para Android Enterprise, las aplicaciones se instalan en el perfil de trabajo de Android del dispositivo. Para obtener más información, consulte Android Enterprise.
- Para dispositivos Samsung, habilite Samsung Knox en el dispositivo.

  Para ello, configure la directiva de clave de licencia MDM de Samsung para que genere claves de licencia ELM y Knox de Samsung. Para obtener más información, consulte Directivas de claves de licencia para la administración de dispositivos móviles (MDM) Samsung.

Acerca de aplicaciones obligatorias y opcionales

Cuando se agregan aplicaciones a un grupo de entrega, se puede elegir si serán opcionales u obligatorias. Citrix recomienda implementar aplicaciones con la opción **Requerido**.

- Las aplicaciones necesarias se instalan silenciosamente en los dispositivos del usuario, lo que minimiza la interacción con ellas. Tener esta función habilitada también permite que las aplicaciones se actualicen automáticamente.
- Las aplicaciones opcionales permiten a los usuarios elegir qué aplicaciones instalar, pero los usuarios deben iniciar la instalación manualmente a través de Secure Hub.

Para las aplicaciones marcadas como obligatorias, los usuarios reciben inmediatamente actualizaciones en situaciones como estas:

- Se carga una nueva aplicación y se marca como obligatoria.
- Se marca una aplicación existente como obligatoria.
- Un usuario elimina una aplicación obligatoria.
- Hay una actualización de Secure Hub disponible.

Requisitos para la implementación forzosa de las aplicaciones obligatorias

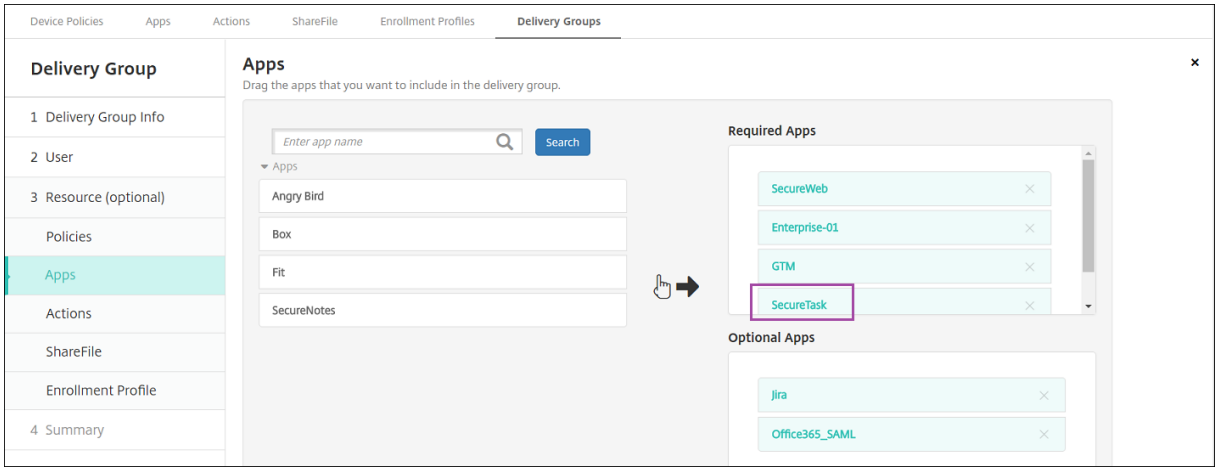
- XenMobile Server 10.6 (versión mínima)
- Secure Hub 10.5.15 para iOS y 10.5.20 para Android (versiones mínimas)
- SDK de MAM o MDX Toolkit 10.6 (versión mínima)
- Propiedad personalizada de servidor: force.server.push.required.apps

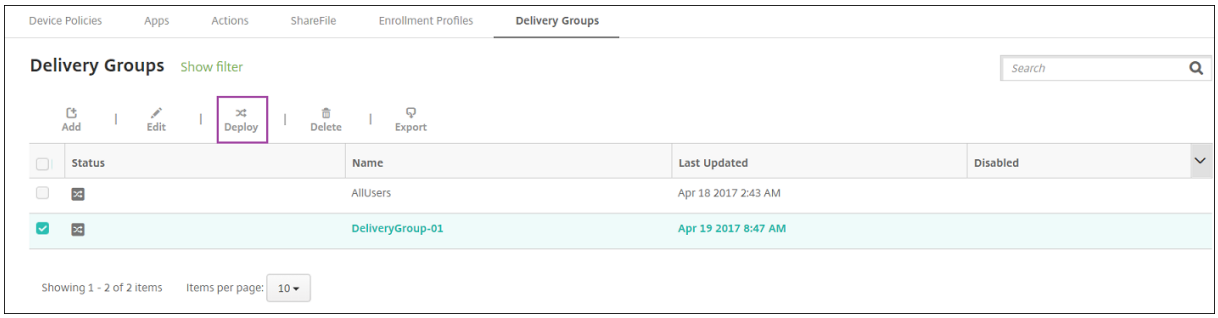
  La implementación forzosa de aplicaciones obligatorias está inhabilitada de forma predeterminada. Para habilitar la función, cree una propiedad de servidor de clave personalizada. Establezca **Clave** y **Nombre simplificado** con **force.server.push.required.apps** y establezca el **Valor** en **true**.

- Después de actualizar XenMobile Server y Secure Hub: los usuarios que tengan dispositivos inscritos deberán cerrar la sesión y, a continuación, iniciarla una vez en Secure Hub para obtener las actualizaciones de la implementación de aplicaciones obligatorias.

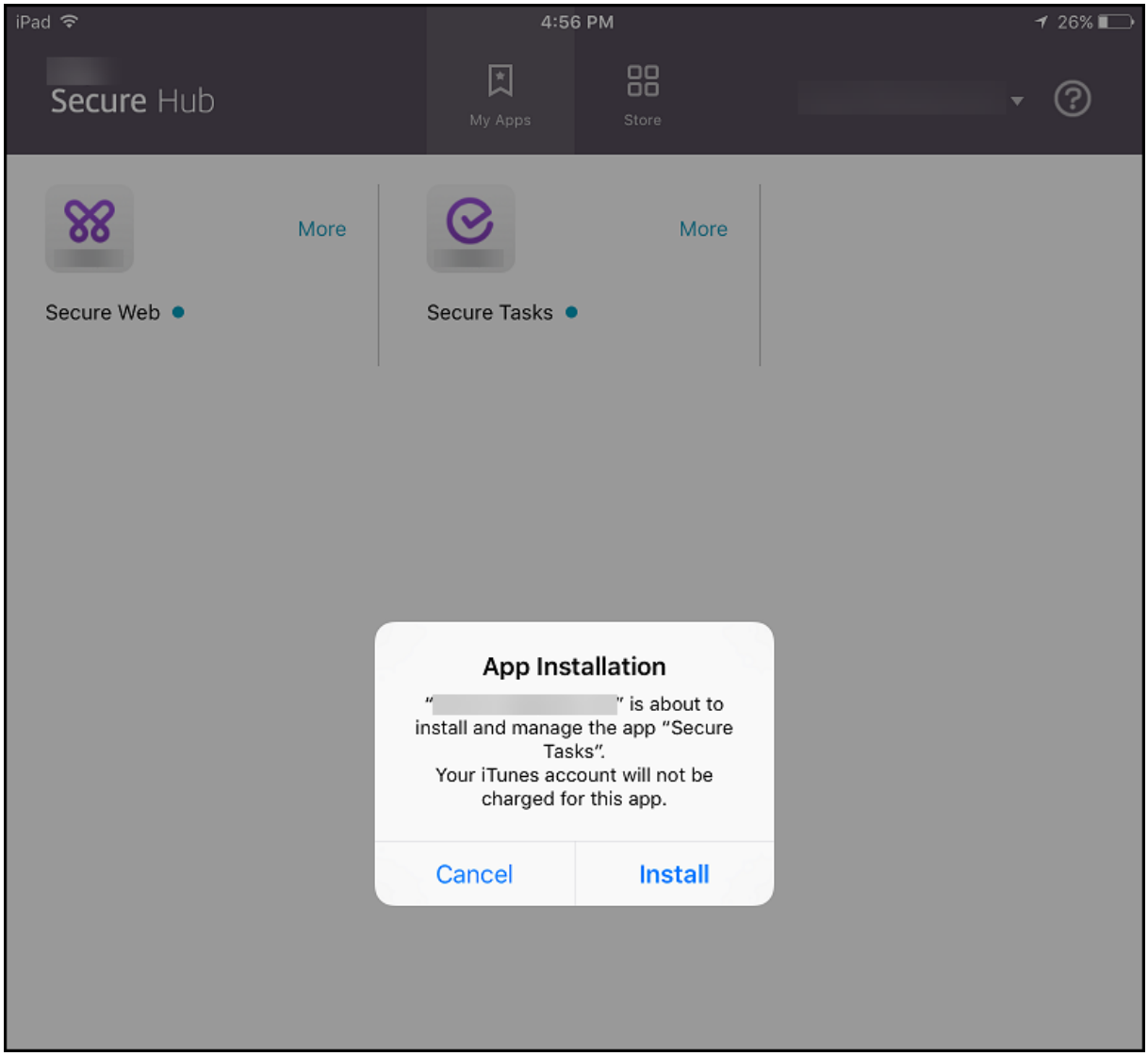
Ejemplos

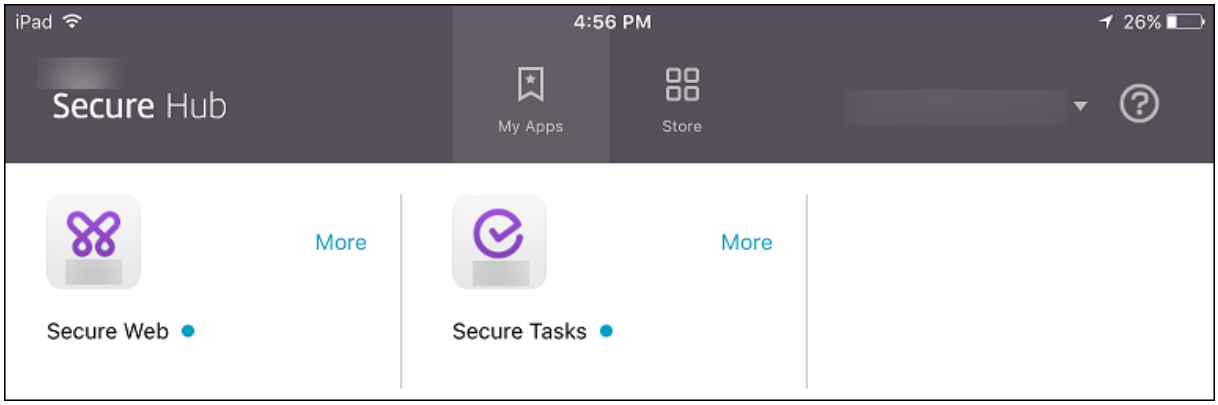
En los siguientes ejemplos, se muestra la secuencia de agregar la aplicación llamada Secure Tasks a un grupo de entrega y, a continuación, implementar ese grupo de entrega.





Una vez implementada la aplicación de ejemplo (Secure Tasks) en el dispositivo del usuario, Secure Hub pide al usuario que instale la aplicación.





Importante:

Las aplicaciones obligatorias habilitadas con MDX, incluidas las aplicaciones de empresa y las aplicaciones de tiendas públicas, se actualizan de versión de inmediato. La actualización se

> produce incluso si configura una directiva MDX para un periodo de gracia de actualización de la aplicación y el usuario elige actualizar la aplicación más tarde.

Flujo de trabajo en iOS para aplicaciones obligatorias de empresa y tienda pública

1. Implemente la aplicación de XenMobile Apps durante la inscripción inicial. La aplicación obligatoria se instala en el dispositivo.
2. Actualice la aplicación en la consola de XenMobile.
3. Utilice la consola de XenMobile para implementar las aplicaciones obligatorias.
4. Se actualiza la aplicación en la pantalla de inicio. Y, para las aplicaciones de tiendas públicas, la actualización de versión se inicia automáticamente. No se solicita la actualización a los usuarios.
5. Los usuarios abren la aplicación desde la pantalla de inicio. Las aplicaciones se actualizan de versión inmediatamente, aunque establezca un período de gracia de actualización y el usuario toque actualizar la aplicación más tarde

Flujo de trabajo en Android para aplicaciones obligatorias de empresa

1. Implemente la aplicación de XenMobile Apps durante la inscripción inicial. La aplicación obligatoria se instala en el dispositivo.
2. Utilice la consola de XenMobile para implementar las aplicaciones obligatorias.
3. Se actualiza la versión de la aplicación. (los dispositivos Nexus solicitan instalar las actualizaciones, mientras que los dispositivos Samsung realizan una instalación silenciosa).
4. Los usuarios abren la aplicación desde la pantalla de inicio. Las aplicaciones se actualizan de versión inmediatamente, aunque establezca un período de gracia de actualización y el usuario toque actualizar la aplicación más tarde (los dispositivos Samsung llevan a cabo una instalación silenciosa).

Flujo de trabajo en Android para aplicaciones obligatorias de tienda pública

1. Implemente la aplicación de XenMobile Apps durante la inscripción inicial. La aplicación obligatoria se instala en el dispositivo.
2. Actualice la aplicación en la consola de XenMobile.
3. Utilice la consola de XenMobile para implementar las aplicaciones obligatorias. O bien, abra la tienda de Secure Hub en el dispositivo. Aparece el icono de actualización en el almacén.
4. La actualización de versión comienza automáticamente. (Los dispositivos Nexus piden a los usuarios que instalen la actualización.)
5. Abra la aplicación desde la pantalla de inicio. Se actualiza la versión de la aplicación. No se pide el período de gracia a los usuarios (los dispositivos Samsung llevan a cabo una instalación silenciosa).

Desinstalar una aplicación cuando está configurada como obligatoria

Puede permitir que los usuarios desinstalen una aplicación configurada como obligatoria. Para ello, vaya a **Configurar > Grupos de entrega** y mueva la aplicación de **Aplicaciones obligatorias** a **Aplicaciones opcionales**.

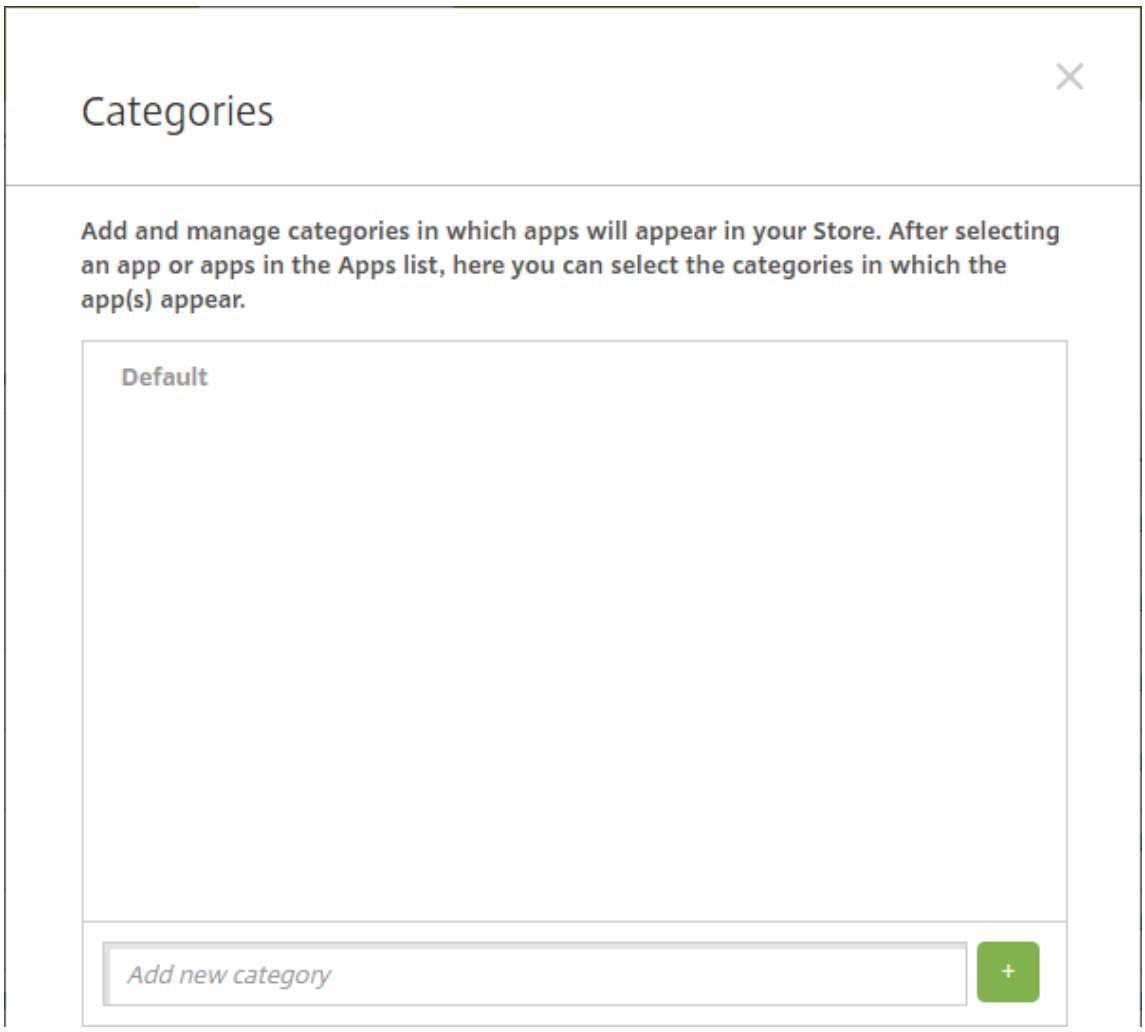
Recomendado: Use un grupo de entrega específico para cambiar temporalmente una aplicación a opcional, de modo que usuarios concretos puedan desinstalarla. Entonces, puede cambiar una aplicación obligatoria a opcional, implementarla en ese grupo de entrega y desinstalarla de esos dispositivos. Después de eso, si quiere que en las inscripciones futuras de ese grupo de entrega se requiera la aplicación, puede volver a establecerla como obligatoria.

Acerca de las categorías de aplicaciones

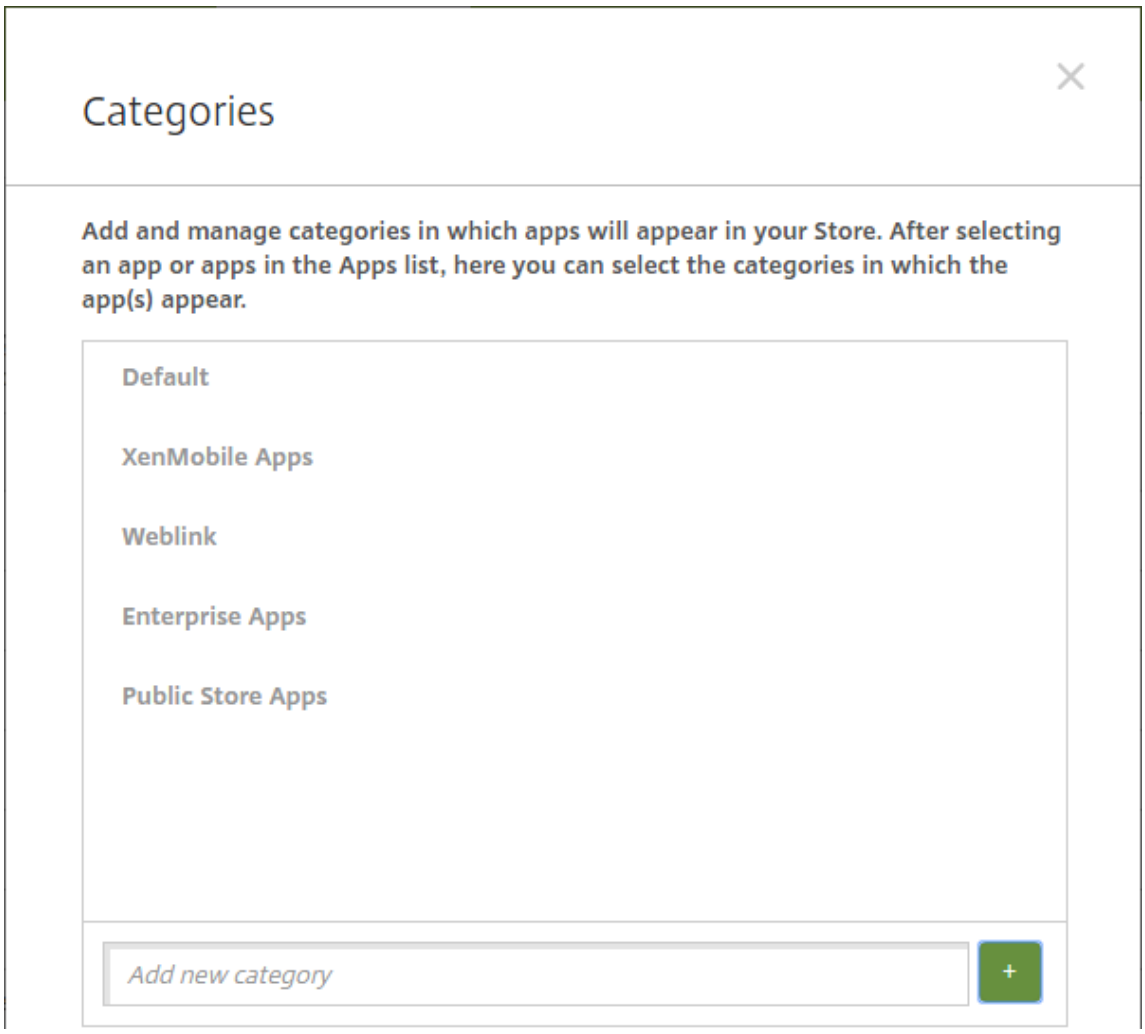
Cuando los usuarios inician sesión en Secure Hub, reciben una lista de las aplicaciones, los enlaces web y las tiendas que haya configurado en XenMobile. Puede usar categorías de aplicaciones para que los usuarios accedan solo a determinadas aplicaciones, tiendas o enlaces web. Por ejemplo, puede crear 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.

Al configurar o modificar una aplicación, un enlace web o un almacén, puede agregarla a una o varias de las categorías configuradas.

1. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones > Categoría**. Aparecerá el cuadro de diálogo **Categorías**.



2. Para agregar cada categoría, lleve a cabo lo siguiente:
   - Escriba el nombre de la categoría que quiere agregar en el campo **Agregar nueva categoría**, situado en la parte inferior del cuadro de diálogo. Por ejemplo, puede escribir “Aplicaciones de empresa” para crear una categoría que contenga 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 cuadro de diálogo **Categorías**.



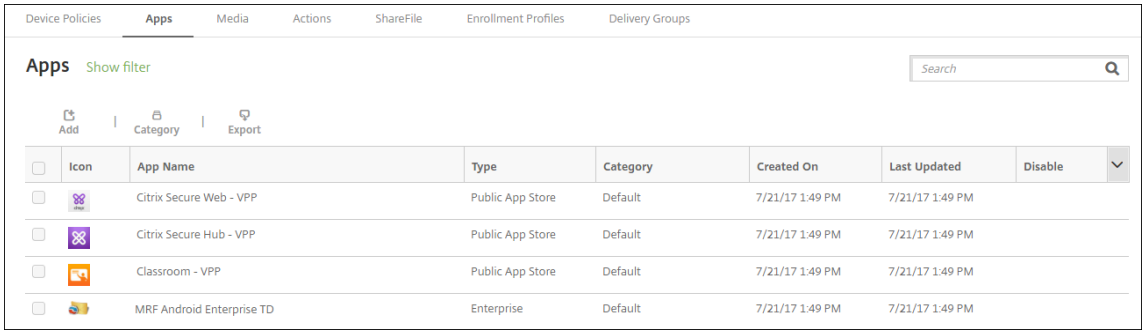
3. Cuando haya terminado de agregar categorías, cierre el cuadro de diálogo **Categorías**.
4. En la página **Aplicaciones**, puede colocar una aplicación existente en una categoría nueva.
    - Seleccione la aplicación que quiera categorizar.
    - Haga clic en **Edit**. Aparecerá la página **Información de la aplicación**.
    - En la lista **Categoría de la aplicación**, aplique la nueva categoría marcando la casilla de la categoría en cuestión. Desmarque las casillas de aquellas categorías existentes que no quiera aplicar a la aplicación.
    - Haga clic en la ficha **Asignaciones de grupo de entrega** o haga clic en **Siguiente** en las páginas restantes de la configuración de la aplicación.
    - Haga clic en **Guardar** en la página **Asignaciones de grupo de entrega** para aplicar la nueva categoría. La nueva categoría se aplicará a la aplicación y aparecerá en la tabla **Aplicaciones**.

Agregar una aplicación MDX

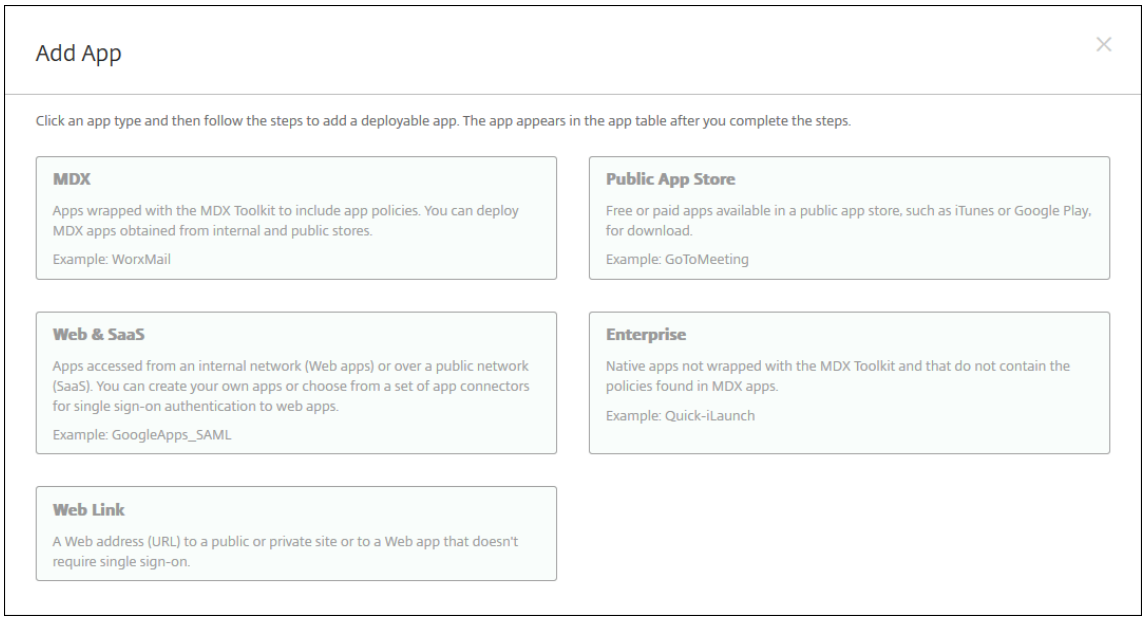
Tras recibir un archivo MDX para una aplicación iOS o Android, puede cargar la aplicación en XenMobile. Después de cargar la aplicación, puede definir sus datos y configuraciones de directiva. Para obtener más información sobre las directivas de aplicaciones que están disponibles para cada tipo de plataforma de dispositivos, consulte:

- Introducción al SDK de MAM
- Vista general de las directivas MDX

1. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones**. Aparecerá la página **Aplicaciones**.



2. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



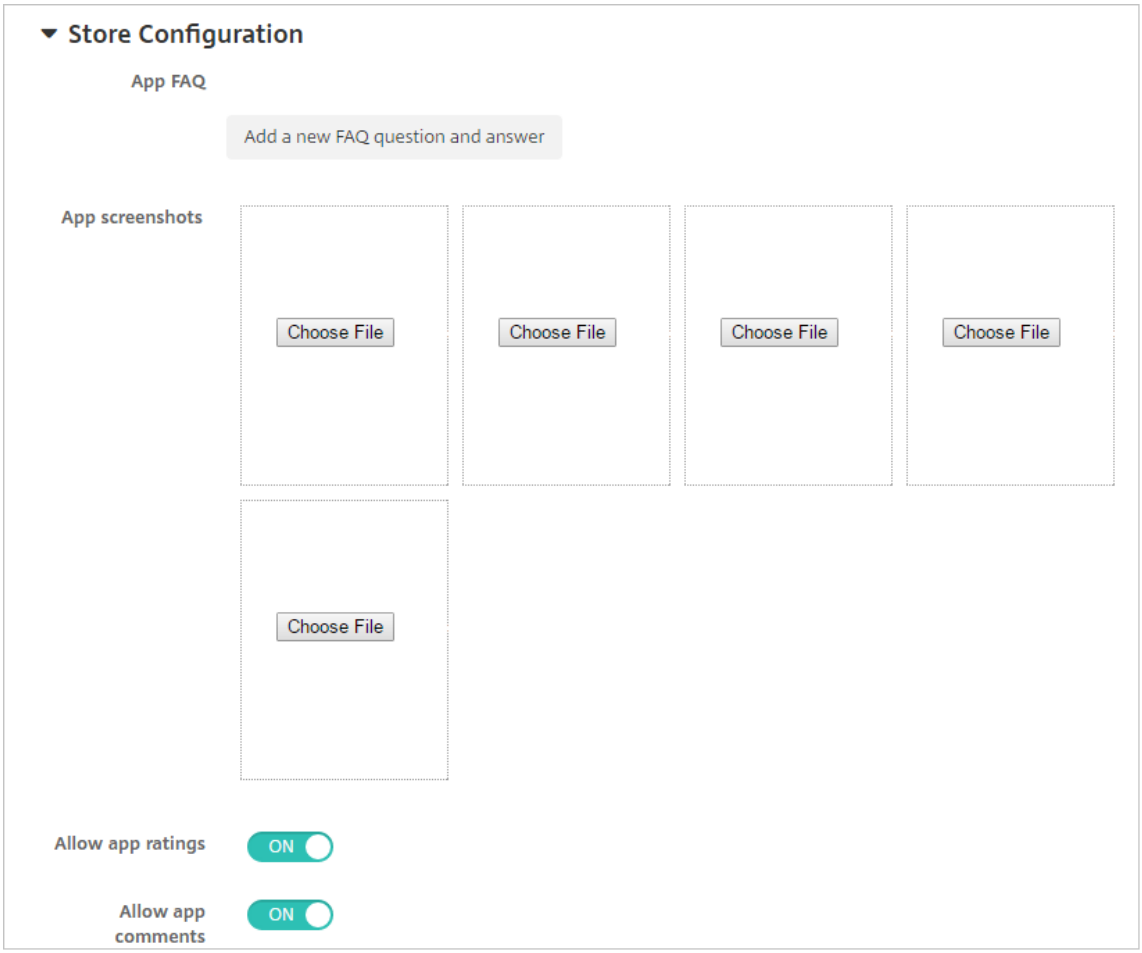
3. Haga clic en **MDX**. Aparecerá la página **Información de la aplicación** MDX.
4. En el panel **Información de la aplicación**, escriba la información siguiente:
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.

- **Descripción:** Escriba, si quiere, una descripción de la aplicación.
- **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.

5. Haga clic en **Siguiente**. Aparecerá la página de las **plataformas de la aplicación**.
6. En **Plataformas**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.
7. Para seleccionar un archivo MDX para cargarlo, haga clic en **Cargar** y vaya a la ubicación del archivo.
8. En la página **Detalles de la aplicación**, configure lo siguiente:
   - **Nombre de archivo:** Escriba el nombre del archivo asociado a la aplicación.
   - **Descripción de la aplicación:** Escriba una descripción de la aplicación.
   - **Versión de la aplicación:** Si quiere, escriba el número de versión de la aplicación.
   - **ID del paquete:** Escriba el ID del paquete de la aplicación, obtenido de Google Play Store administrado.
   - **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
   - **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
   - **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
   - **Quitar aplicación si se quita el perfil MDM:** Seleccione si quiere quitar la aplicación de un dispositivo iOS cuando se quite el perfil de MDM. Está **activado** de forma predeterminada.
   - **Impedir copia de seguridad de datos de la aplicación:** Seleccione si impedir que los usuarios realicen copias de seguridad de los datos de la aplicación en dispositivos iOS. Está **activado** de forma predeterminada.
   - **Seguimiento del producto:** Especifique qué tipo de seguimiento de producto quiere enviar a los dispositivos iOS. Si tiene un seguimiento diseñado para prueba, puede seleccionarlo y asignárselo a sus usuarios. El valor predeterminado es **Producción**.
   - **Forzar administración de la aplicación:** Si se instala una aplicación como no administrada, seleccione si solicitar a los usuarios permiso para administrarla en dispositivos iOS no supervisados. Está **activado** de forma predeterminada.
   - **Aplicación implementada mediante las compras por volumen:** Seleccione si quiere implementar la aplicación a través de las compras por volumen de Apple. Si está **activado**, se implementa una versión MDX de la aplicación y se utiliza las compras por volumen para implementar la aplicación, Secure Hub muestra solo la instancia de compras por volumen. Está **desactivado** de forma predeterminada.
9. Configure las **directivas MDX**. Las directivas MDX varían según la plataforma. Además, estas

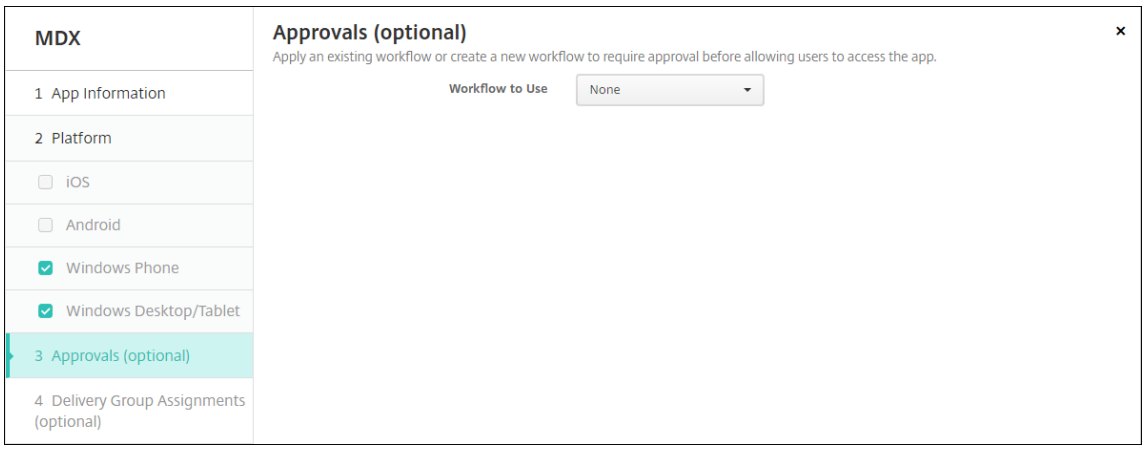
directivas incluyen opciones para tales áreas de directiva como autenticación, seguridad de los dispositivos y restricciones a aplicaciones. En la consola, se ofrece información descriptiva sobre cada una de las directivas.

10. Configurar las reglas de implementación. Para obtener información, consulte Reglas de implementación.
11. Expanda **Configuración del almacén**.



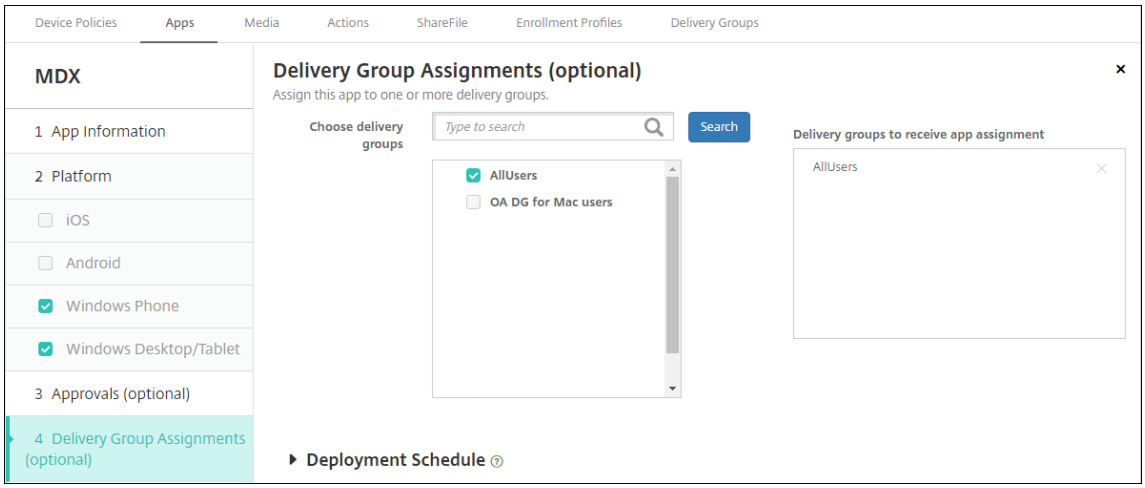
- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

12. Haga clic en **Siguiente**. Aparecerá la página **Aprobaciones**.



Para utilizar flujos de trabajo que requieran aprobación antes de permitir que los usuarios accedan a la aplicación, consulte Aplicar flujos de trabajo. Si no quiere configurar flujos de trabajo de aprobación, vaya directamente al paso siguiente.

13. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.



14. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione un grupo o varios de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.

15. Expanda **Programación de implementación** y, a continuación, configure estos parámetros:

    - **Implementar:** Elija si quiere implementar la aplicación en los dispositivos. Está **activado** de forma predeterminada.
    - **Programación de implementación:** Elija si quiere implementar la aplicación **Ahora** o **Más tarde**. Si selecciona **Más tarde**, configure una fecha y hora para implementar la aplicación. El valor predeterminado es **Ahora**.
    - **Condición de implementación:** Seleccione **En cada conexión** para implementar la aplicación cada vez que se conecte el dispositivo. Elija **Solo cuando haya fallado la implementación anterior** para implementar la aplicación cuando el dispositivo no haya

recibido previamente la aplicación. El valor predeterminado es **En cada conexión**.

La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

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 **Implementar para conexiones permanentes**.

16. Haga clic en **Guardar**.

Agregar una aplicación de la tienda pública de aplicaciones

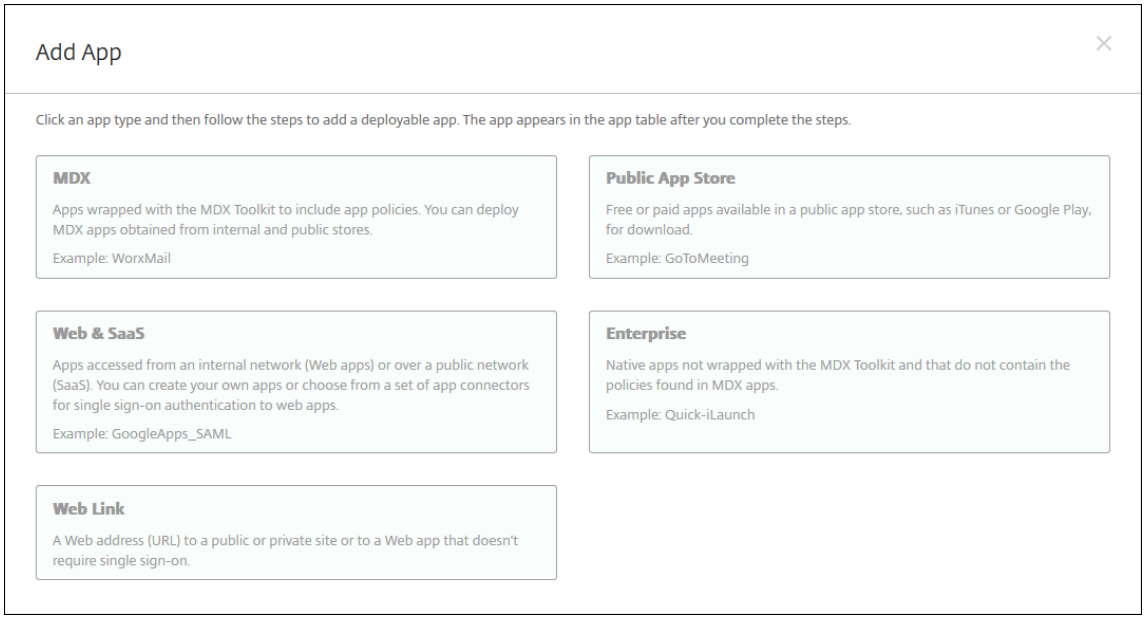
Se pueden agregar a XenMobile tanto aplicaciones gratuitas como de pago, que estén disponibles en una tienda pública de aplicaciones, como App Store de Apple o Google Play.

Puede configurar ciertos parámetros para obtener los nombres y las descripciones de las aplicaciones desde Apple App Store. Cuando obtiene la información de la aplicación, facilitada desde la tienda, XenMobile sobrescribe el nombre y la descripción existentes. Configure manualmente la información de la aplicación de Google Play Store.

Cuando agrega una aplicación de pago proveniente de una tienda pública a Android Enterprise, 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. El plan de compra en bloque de Android Enterprise simplifica el proceso de encontrar, comprar y distribuir aplicaciones y otros datos en masa para una organización.

Configure información sobre la aplicación y elija las plataformas en las que entregarla:

1. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones > Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



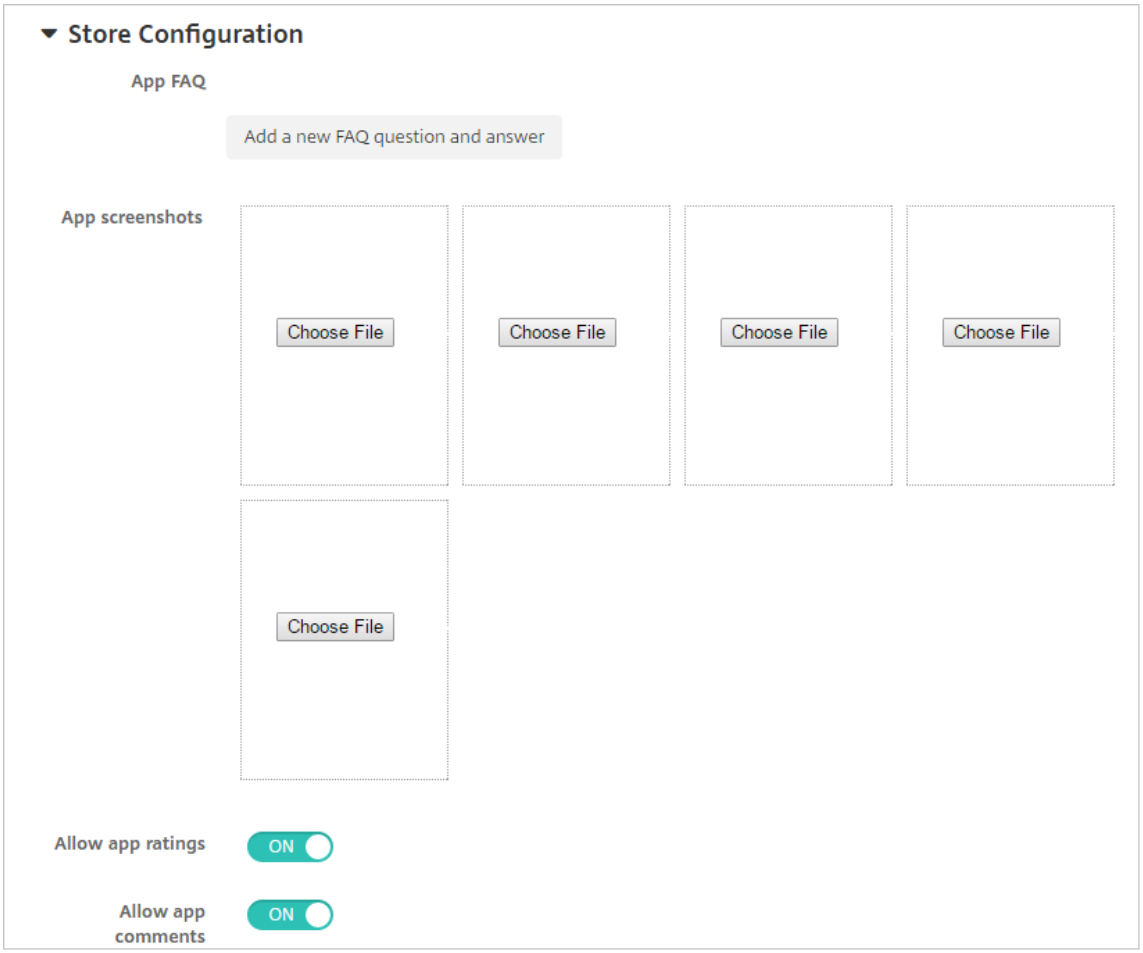
2. Haga clic en **Tienda pública de aplicaciones**. Aparecerá la página **Información de la aplicación**.
3. En el panel **Información de la aplicación**, escriba la información siguiente:
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.
   - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
   - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.
4. Haga clic en **Siguiente**. Aparecerá la página de las **plataformas de la aplicación**.
5. En **Plataformas**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.

A continuación, configure los parámetros de la aplicación para cada plataforma. Consulte:

- Configurar parámetros de aplicación para aplicaciones de Google Play
- Aplicaciones administradas de la tienda de aplicaciones
- Configurar parámetros de aplicación para aplicaciones iOS

Cuando termine de configurar los parámetros de una plataforma, defina las reglas de implementación de esa plataforma y los parámetros de tienda de aplicaciones.

1. Configurar las reglas de implementación. Para obtener información, consulte Reglas de implementación.
2. Expanda **Configuración del almacén**.



- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

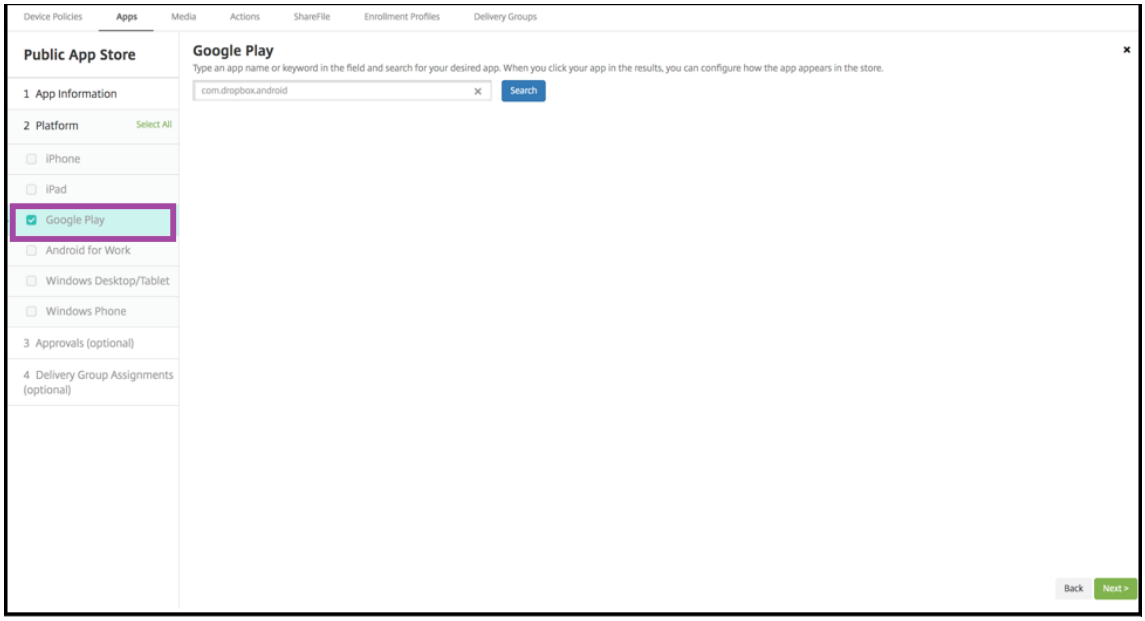
Configurar parámetros de aplicación para aplicaciones de Google Play

> **Nota:**
>
> Para que todas las aplicaciones de Google Play Store sean accesibles desde Google Play administrado, utilice la propiedad de servidor **Acceder a todas las aplicaciones en Google Play Store** de XenMobile. Consulte Propiedades de servidor. Al establecer esta propiedad en **true**, se permiten las aplicaciones de la tienda pública de Google Play para todos los usuarios de Android

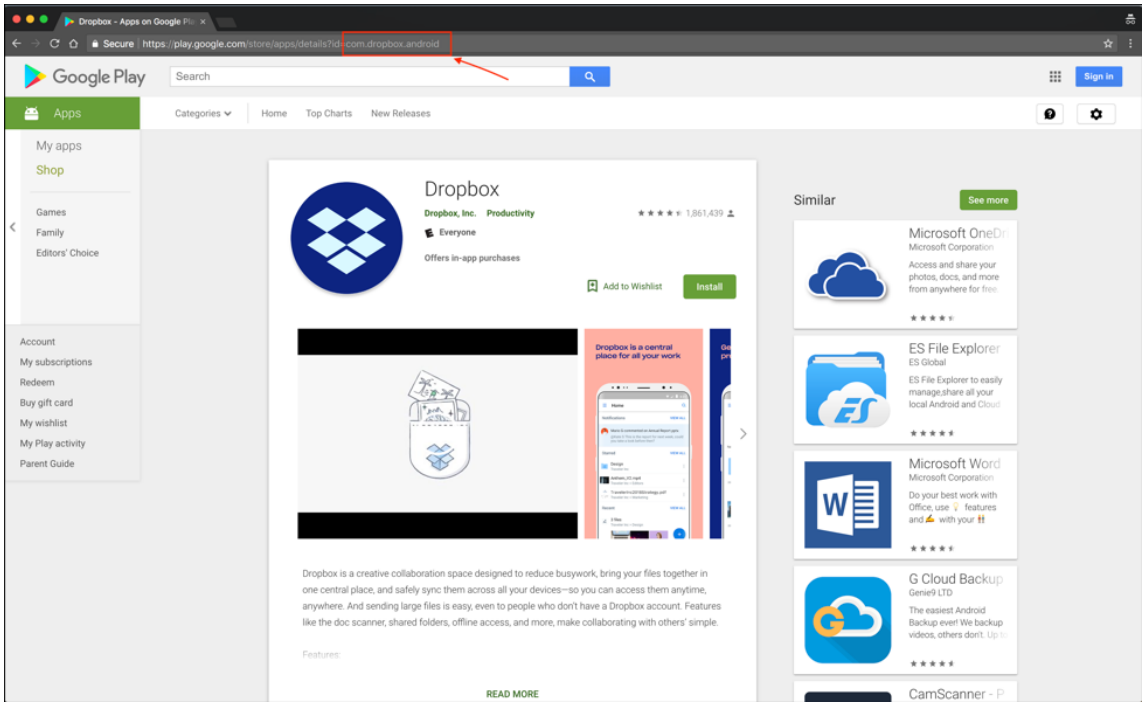
> Enterprise. A continuación, puede usar la directiva Restricciones para controlar el acceso a estas aplicaciones.

La configuración de las aplicaciones de Google Play Store requiere pasos diferentes a los de otras plataformas. Debe configurar manualmente la información de la aplicación de Google Play Store.

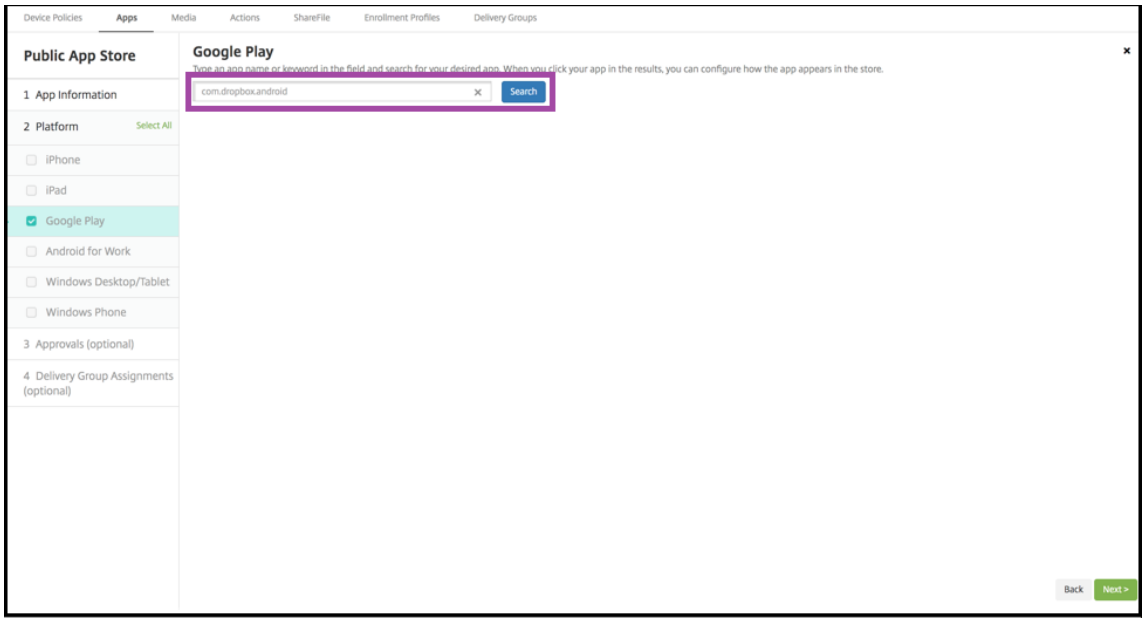
1. Compruebe que **Google Play** esté marcado en **Plataformas**.



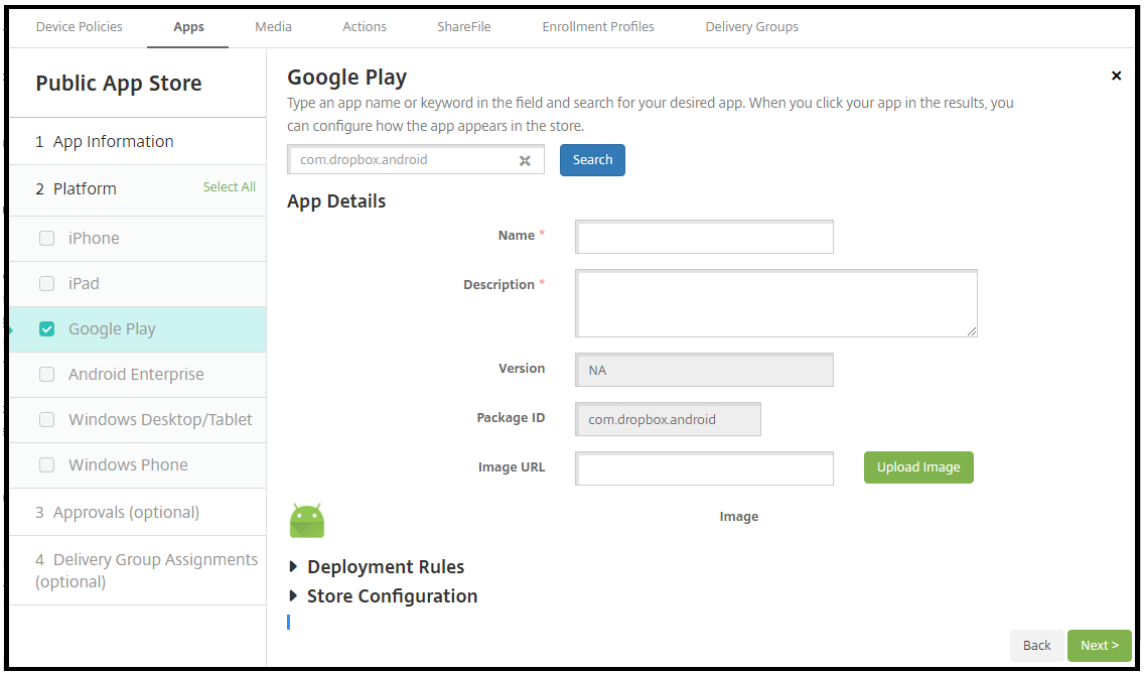
2. Vaya a Google Play Store. Desde Google Play Store, copie el ID del paquete. El ID está en la URL de la aplicación.



3. Al agregar una aplicación de tienda pública en la consola de XenMobile Server, pegue el ID del paquete en la barra de búsqueda. Haga clic en **Search**.



4. Si el ID del paquete es válido, aparece una interfaz de usuario que le permite introducir los detalles de la aplicación.



5. Puede configurar la URL de la imagen para que aparezca con la aplicación en el almacén. Para usar la imagen de Google Play Store:

   a) Vaya a Google Play Store. Haga clic con el botón secundario en la imagen de la aplicación y copie la dirección de la imagen.

b) Pegue la dirección de la imagen en el campo **URL de imagen**.

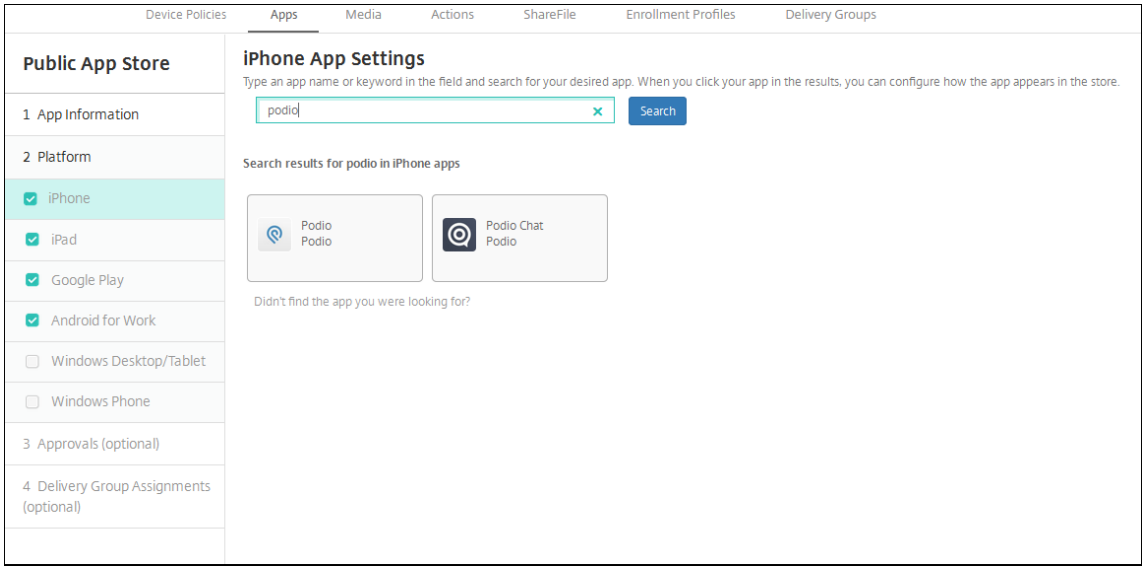
c) Haga clic en **Cargar imagen**. La imagen aparece junto a **Imagen**.

Si no configura ninguna imagen, aparecerá la imagen genérica de Android con la aplicación.

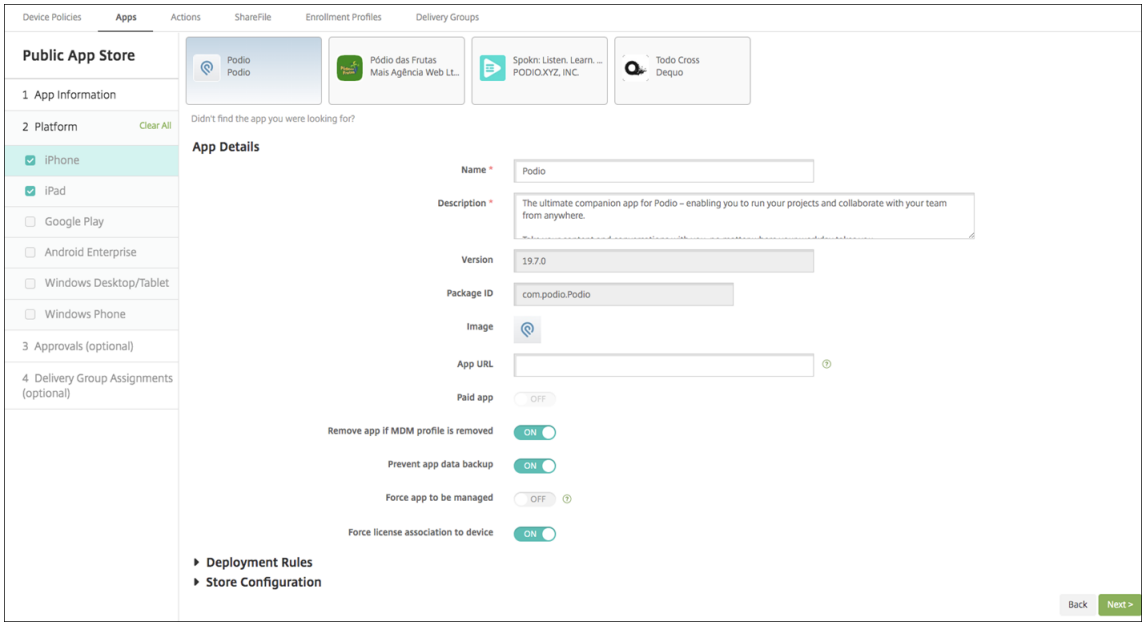
Configurar parámetros de aplicación para aplicaciones iOS

1. Introduzca el nombre de la aplicación en el cuadro de búsqueda y haga clic en **Buscar**. Aparecerán las aplicaciones que coincidan con los criterios de búsqueda. Aparecerán las aplicaciones que coincidan con los criterios de búsqueda.

   En la siguiente imagen, se muestran los resultados de la búsqueda **podio** en aplicaciones de un teléfono iPhone.



2. Haga clic en la aplicación que quiera agregar.
3. Los campos **Detalles de la aplicación** aparecen rellenos con información relativa a la aplicación seleccionada (incluido el nombre, la descripción, el número de versión y la imagen asociada).

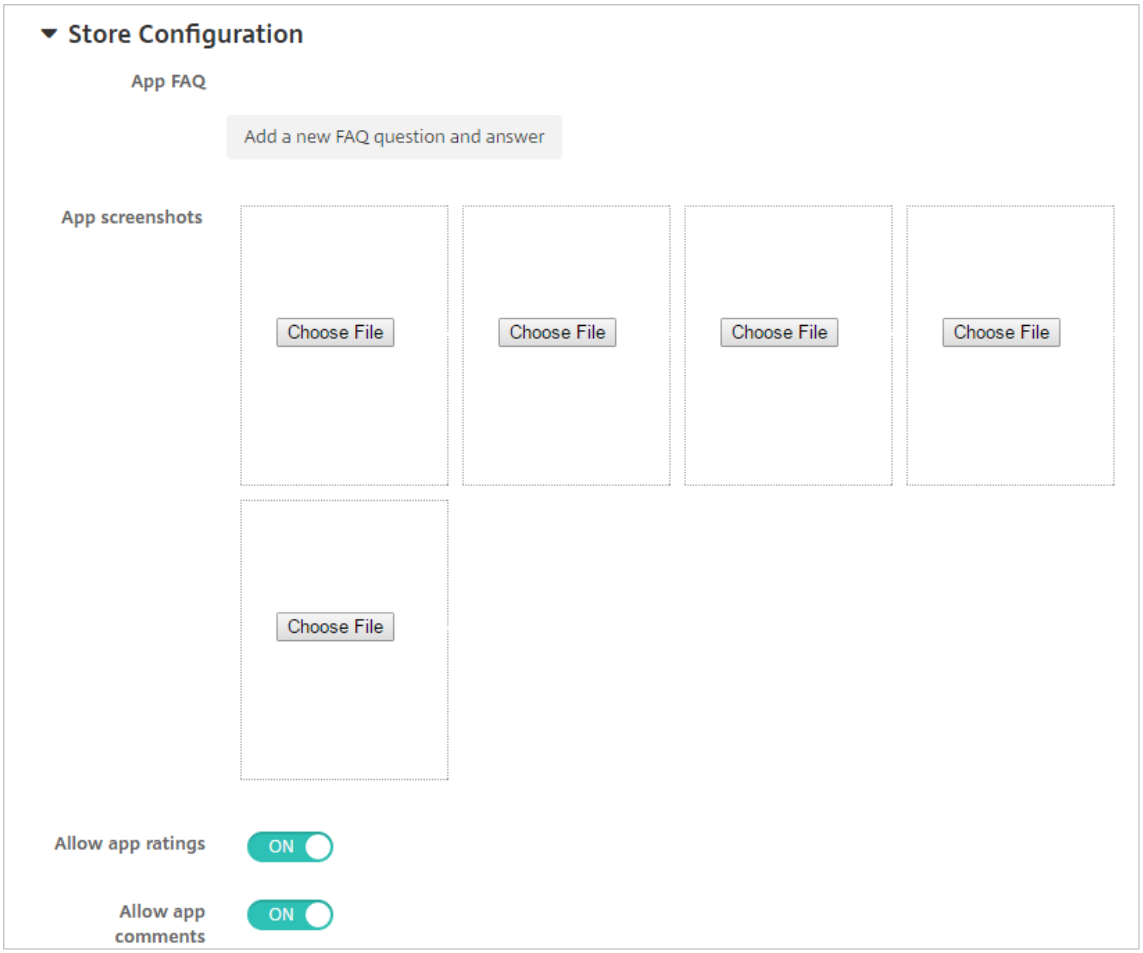


4. Configure estos parámetros:

   - Si fuera necesario, cambie el nombre y la descripción de la aplicación.
   - **Aplicación de pago:** Este campo está preconfigurado y no se puede cambiar.
   - **Quitar aplicación si se quita el perfil MDM:** Seleccione si quiere quitar la aplicación cuando se quite el perfil de MDM. De forma predeterminada, está **activado**.
   - **Impedir copia de seguridad de datos de la aplicación:** Seleccione si quiere impedir que la aplicación realice copias de seguridad de los datos. De forma predeterminada, está **activado**.
   - **Seguimiento del producto:** Especifique qué tipo de seguimiento de producto quiere enviar a los dispositivos de usuario. Si tiene un seguimiento diseñado para prueba, puede seleccionarlo y asignárselo a sus usuarios. El valor predeterminado es **Producción**.
   - **Forzar administración de la aplicación:** Si se instala una aplicación no administrada, seleccione si solicitar a los usuarios permiso para administrarla en dispositivos no supervisados. Está **desactivado** de forma predeterminada. Disponible en iOS 9.0 y versiones posteriores.
   - **Forzar asociación de licencia con el dispositivo:** 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.

5. Configurar las reglas de implementación. Para obtener información, consulte Reglas de implementación.

6. Expanda **Configuración del almacén**.



- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

7. Para iPhone o iPad, expanda **Compras por volumen**.

   a) Si desea habilitar XenMobile para aplicar una licencia de compras por volumen a la aplicación, en la lista **Licencia de compras por volumen**, haga clic en **Cargar un archivo de licencia de compras por volumen**.

   b) En el cuadro de diálogo que aparece, importe la licencia.

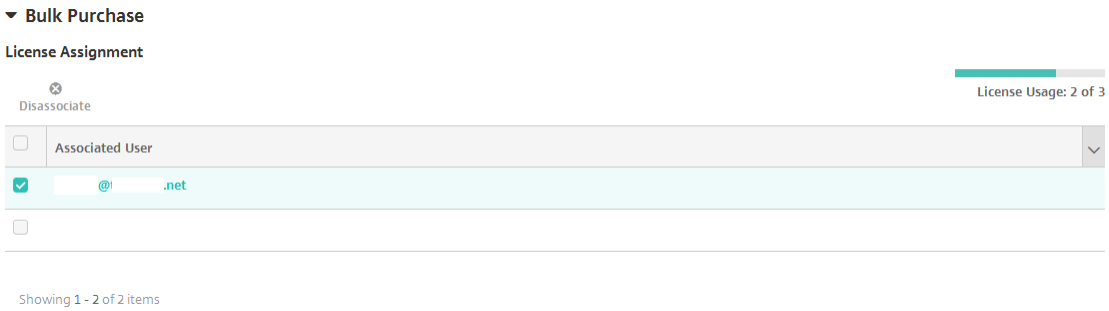
      La tabla “Asignación de licencias” muestra la cantidad de licencias de la aplicación que están en uso, frente al total de las licencias disponibles.

Puede desvincular las licencias de compras por volumen de un usuario en particular. Si lo hace, finaliza las asignaciones y libera licencias.

8. Para Android Enterprise, expanda la sección **Compra en bloque**.

   La tabla “Asignación de licencias” muestra la cantidad de licencias de la aplicación que están en uso, frente al total de las licencias disponibles.

   Puede seleccionar un usuario y hacer clic en **Desasociar** 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.



9. Después de completar los parámetros de **Compras por volumen** o **Compra en bloque**, haga clic en **Siguiente**. Aparecerá la página **Aprobaciones**.

   Para utilizar flujos de trabajo que requieran aprobación antes de permitir que los usuarios accedan a la aplicación, consulte Aplicar flujos de trabajo. Si no necesita flujos de trabajo de aprobación, vaya al siguiente paso.

10. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.

11. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione un grupo o varios de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.

12. Expanda **Programación de implementación** y, a continuación, configure estos parámetros:

    - **Implementar:** Elija si quiere implementar la aplicación en los dispositivos. Está **activado** de forma predeterminada.
    - **Programación de implementación:** Elija si quiere implementar la aplicación **Ahora** o **Más tarde**. Si selecciona **Más tarde**, configure una fecha y hora para implementar la aplicación. El valor predeterminado es **Ahora**.
    - **Condición de implementación:** Seleccione **En cada conexión** para implementar la aplicación cada vez que se conecte el dispositivo. Elija **Solo cuando haya fallado la implementación anterior** para implementar la aplicación cuando el dispositivo no haya recibido previamente la aplicación. El valor predeterminado es **En cada conexión**.

    La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave

de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

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 **Implementar para conexiones permanentes**.

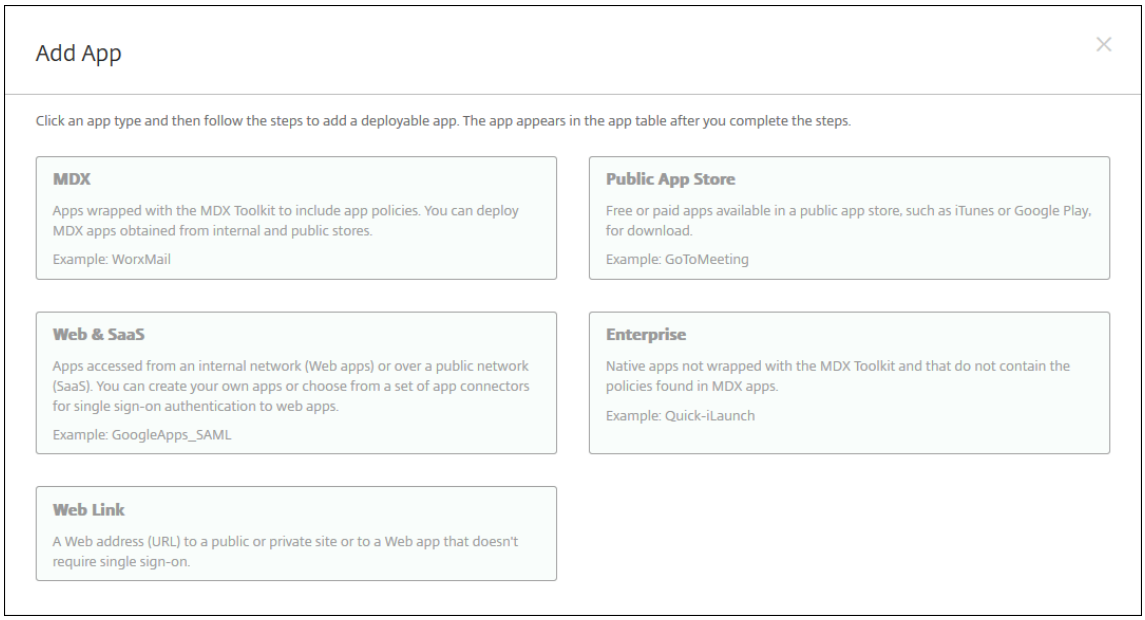
13. Haga clic en **Guardar**.

Agregar una aplicación web o SaaS

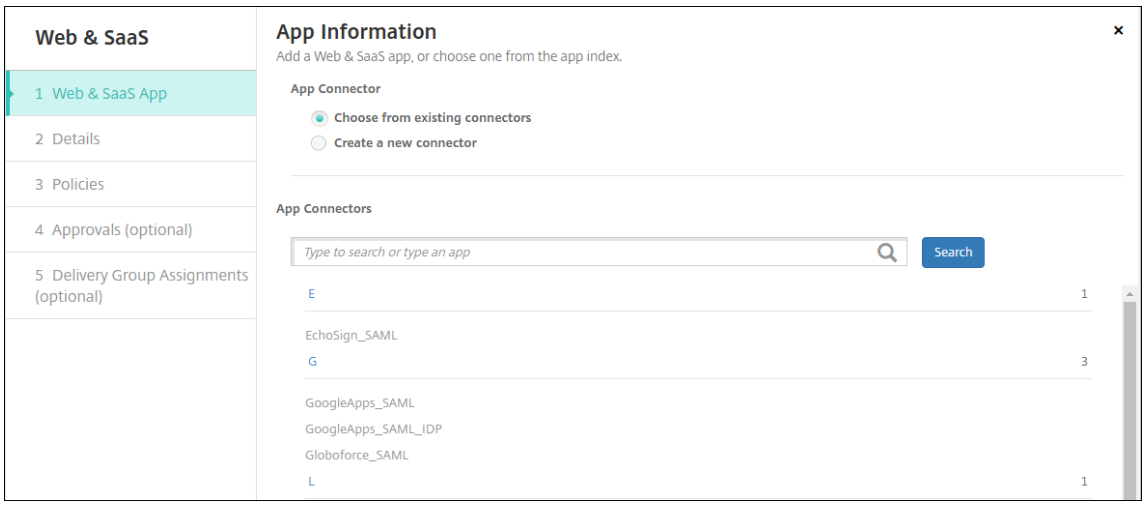
Con la consola de XenMobile, es posible ofrecer Single Sign-On (SSO) a los usuarios, para sus aplicaciones móviles, de empresa, web y SaaS. Puede habilitar aplicaciones para SSO. Para ello, debe utilizar plantillas de conectores de aplicaciones. Para obtener una lista de los tipos de conectores disponibles en XenMobile, consulte Tipos de conectores de aplicaciones. También puede crear su propio conector en XenMobile cuando agregue una aplicación web o SaaS.

Si una aplicación solo está disponible para SSO, tras guardar los parámetros anteriores, la aplicación aparece en la ficha **Aplicaciones** de la consola de XenMobile.

1. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones > Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



2. Haga clic en **Web y SaaS**. Aparecerá la página **Información de la aplicación**.



3. Configure un conector de aplicación nuevo o existente, como se muestra a continuación.

Para configurar un conector de aplicación existente

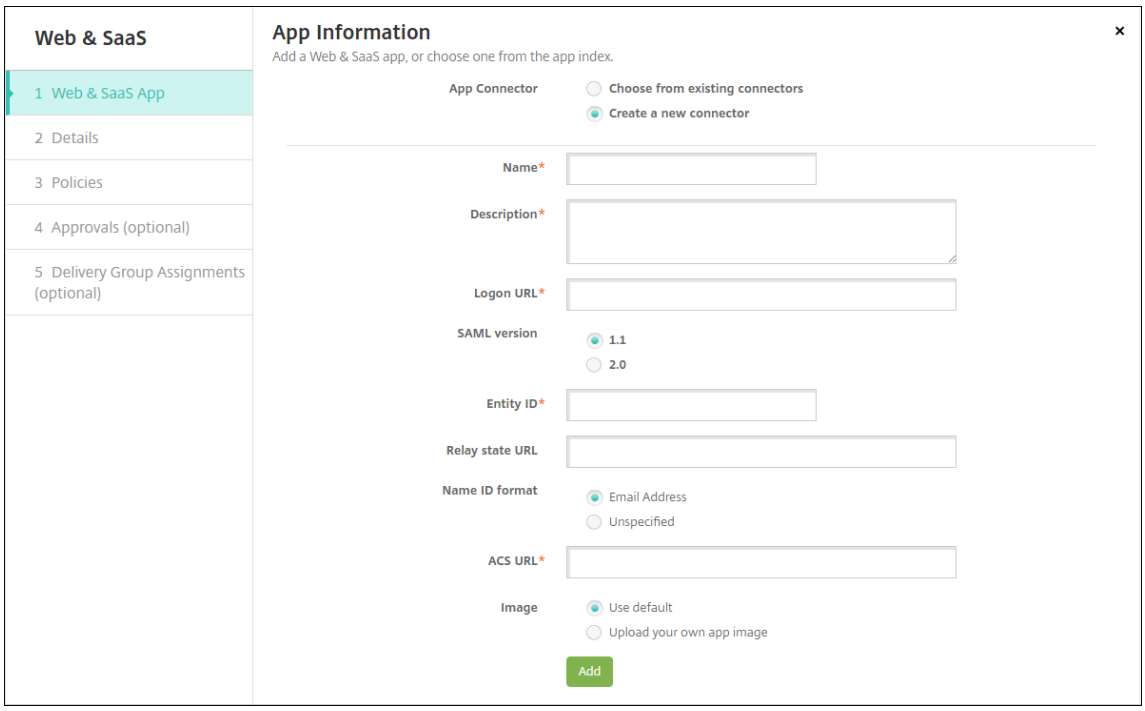
1. En la página **Información de la aplicación**, la opción **Elegir entre los conectores existentes** ya está seleccionada, como se muestra anteriormente. En la lista **Conectores de aplicación**, haga clic en el conector que quiera usar. Aparecerá la información del conector de aplicación.
2. Configure estos parámetros:
   - **Nombre de la aplicación:** Acepte el nombre que ya aparece o escriba uno nuevo.
   - **Descripción de la aplicación:** 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.
   - **Nombre de dominio:** Si corresponde, escriba el nombre de dominio de la aplicación. Este campo es obligatorio.
   - **Aplicación alojada en la red interna:** 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 Citrix Gateway. Si **activa** esta opción, se agrega la palabra clave VPN a la aplicación y se permite a los usuarios conectarse a través de Citrix Gateway. Está **desactivado** de forma predeterminada.
   - **Categoría de la aplicación:** En la lista, si quiere, haga clic en una categoría que se va a aplicar a la aplicación.
   - **Aprovisionamiento de cuentas de usuario:** 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 **Aprovisionamiento de cuentas de usuario**, configure los siguientes parámetros:

- **Cuenta de servicio**
  - **Nombre de usuario:** Escriba el nombre del administrador de la aplicación. Este campo es obligatorio.
  - **Contraseña:** Escriba la contraseña del administrador de la aplicación. Este campo es obligatorio.
- **Cuenta de usuario**
  - **Cuando finalizan los derechos del usuario:** En la lista, haga clic en la acción que se debe realizar cuando los usuarios ya no pueden acceder a la aplicación. La opción predeterminada es **Inhabilitar la cuenta**.
- **Regla de nombre de usuario**
  - Para agregar cada regla de nombre de usuario, haga lo siguiente:
    - **Atributos del usuario:** En la lista, haga clic en el atributo de usuario que quiere agregar a la regla.
    - **Longitud (caracteres):** 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 **Todo**.
    - **Regla:** Cada atributo de usuario que agregue se adjunta automáticamente a la regla de nombre de usuario.

- **Requisito de contraseña**
  - **Longitud:** Escriba la longitud mínima de la contraseña de usuario. El valor predeterminado es **8**.
- **Caducidad de contraseña**
  - **Validez (días):** Escriba la cantidad de días durante los que la contraseña será válida. Cualquier valor entre **0 y 90** es válido. El valor predeterminado es 90.
  - **Restablecer automáticamente la contraseña cuando caduque:** Seleccione si quiere restablecer la contraseña automáticamente cuando esta caduque. Está **desactivado** de forma predeterminada. 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

1. En la página **Información de la aplicación**, seleccione **Crear un nuevo conector**. Aparecerán los campos de información del conector de aplicaciones.

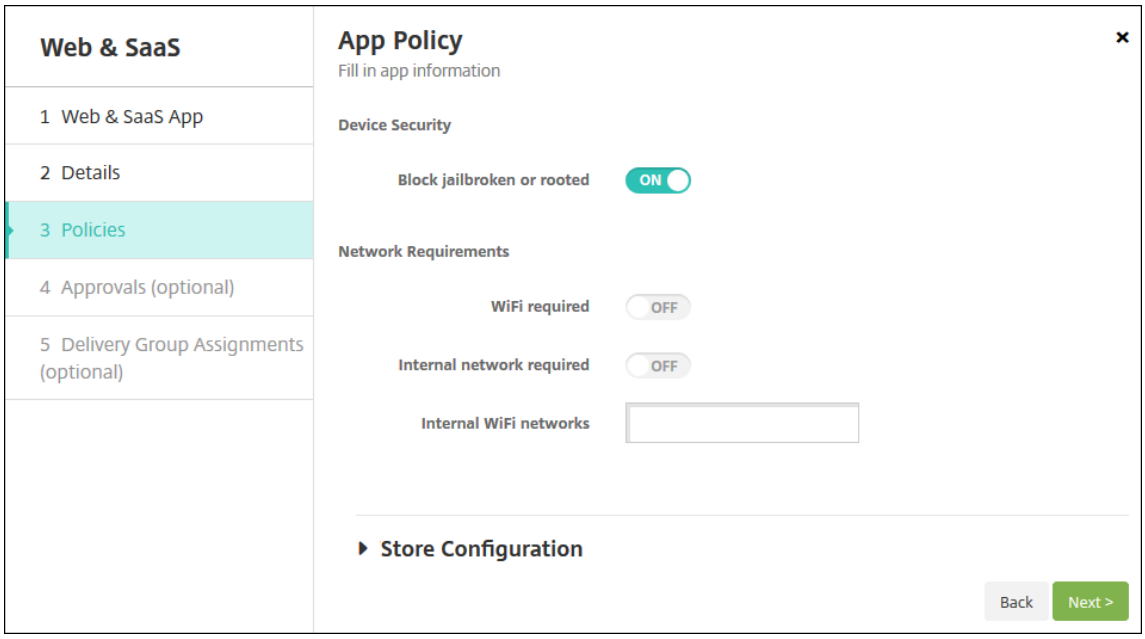


2. Configure estos parámetros:

   - **Nombre:** Escriba un nombre para el conector. Este campo es obligatorio.
   - **Descripción:** Escriba una descripción para el conector. Este campo es obligatorio.
   - **URL de inicio de sesión:** 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, que puede ser `https://www.example.com/logon`. Este campo es obligatorio.
   - **Versión SAML:** Seleccione **1.1** o **2.0**. El valor predeterminado es **1.1**.
   - **ID de entidad:** Escriba la identidad de la aplicación SAML.
   - **URL de estado del relé:** Escriba la dirección web de la aplicación SAML. Esta es la URL de respuesta de la aplicación.
   - **Formato de ID de nombre:** Seleccione **Correo electrónico** o **No especificado**. El valor predeterminado es **Correo electrónico**.
   - **URL de ACS:** 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).
   - **Imagen:** Seleccione si usar la imagen predeterminada de Citrix o cargar su propia imagen de la aplicación. El valor predeterminado es “Usar predeterminada”.
     - Si quiere cargar su propia imagen, haga clic en **Examinar**, vaya a la ubicación del archivo y selecciónelo. El archivo debe ser PNG. No se puede cargar archivos JPEG o GIF. Cuando se agrega un gráfico personalizado, no se puede modificar más tarde.

3. Cuando haya terminado, haga clic en **Agregar**. Aparecerá la página **Detalles**.

4. Haga clic en **Siguiente**. Aparecerá la página **Directiva de aplicación**.

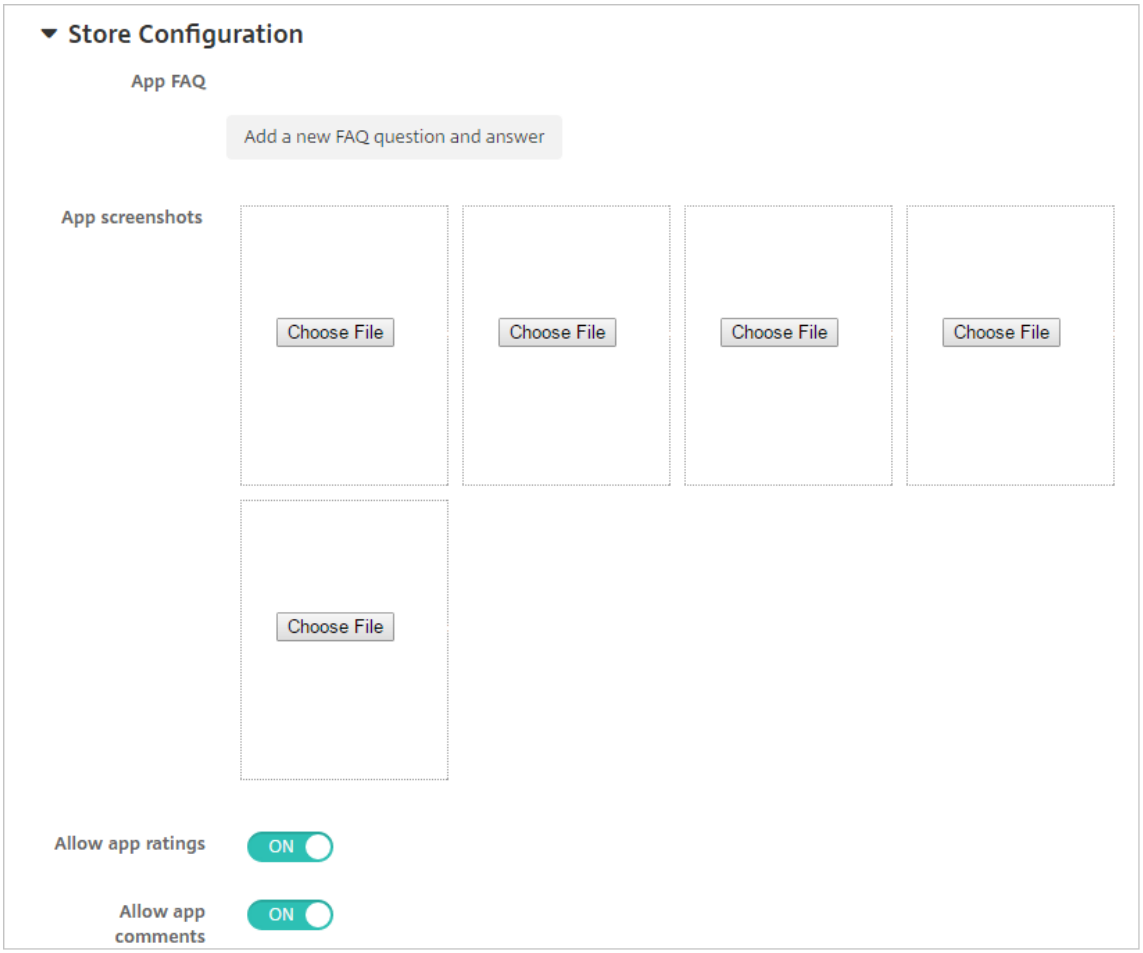


5. Configure estos parámetros:

   - **Seguridad del dispositivo**
   - **Bloquear si está liberado por jailbreak o rooting:** Seleccione si impedir que los dispositivos liberados por jailbreak o por rooting accedan a la aplicación. De forma predeterminada está **activado**.
   - **Requisitos de la red**
   - **Se requiere Wi-Fi:** Seleccione si se necesita una conexión Wi-Fi para ejecutar la aplicación. De forma predeterminada está **desactivado**.
   - **Se requiere red interna:** Seleccione si se necesita una red interna para ejecutar la aplicación. De forma predeterminada está **desactivado**.
   - **Redes Wi-Fi internas:** Si habilitó la opción **Se requiere Wi-Fi**, escriba las redes inalámbricas internas que se van a usar.

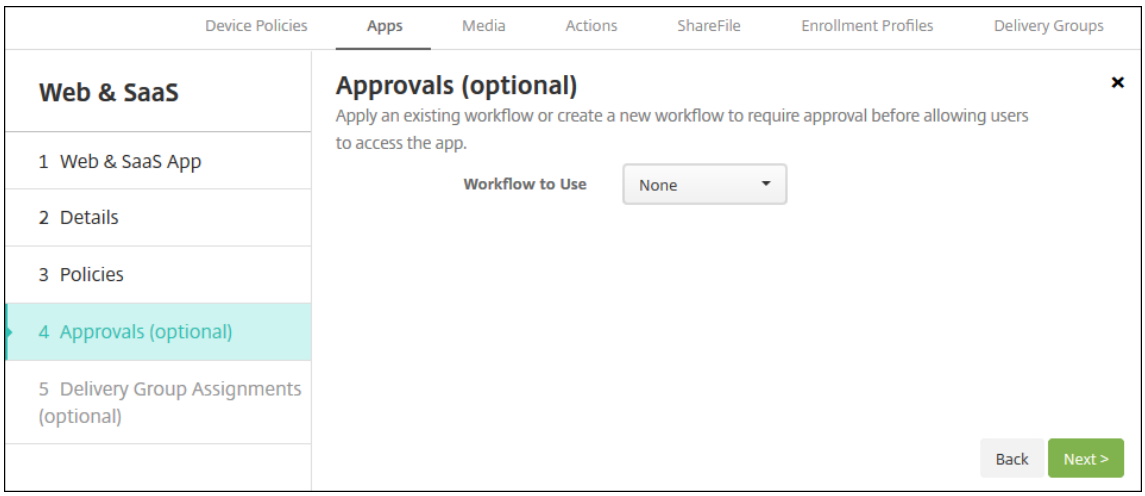
6. Configurar las reglas de implementación. Para obtener información, consulte Reglas de implementación.

7. Expanda **Configuración del almacén**.



- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

8. Haga clic en **Siguiente**. Aparecerá la página **Aprobaciones**.



Para utilizar flujos de trabajo que requieran aprobación antes de permitir que los usuarios accedan a la aplicación, consulte Aplicar flujos de trabajo.

9. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.
10. Junto a **Elegir grupos de entrega**, escriba para buscar un grupo de entrega o seleccione un grupo o varios. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.
11. Expanda **Programación de implementación** y, a continuación, configure estos parámetros:
    - **Implementar:** Elija si quiere implementar la aplicación en los dispositivos. Está **activado** de forma predeterminada.
    - **Programación de implementación:** Elija si quiere implementar la aplicación **Ahora** o **Más tarde**. Si selecciona **Más tarde**, configure una fecha y hora para implementar la aplicación. El valor predeterminado es **Ahora**.
    - **Condición de implementación:** Seleccione **En cada conexión** para implementar la aplicación cada vez que se conecte el dispositivo. Elija **Solo cuando haya fallado la implementación anterior** para implementar la aplicación cuando el dispositivo no haya recibido previamente la aplicación. El valor predeterminado es **En cada conexión**.

    La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

    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 **Implementar para conexiones permanentes**.
12. Haga clic en **Guardar**.

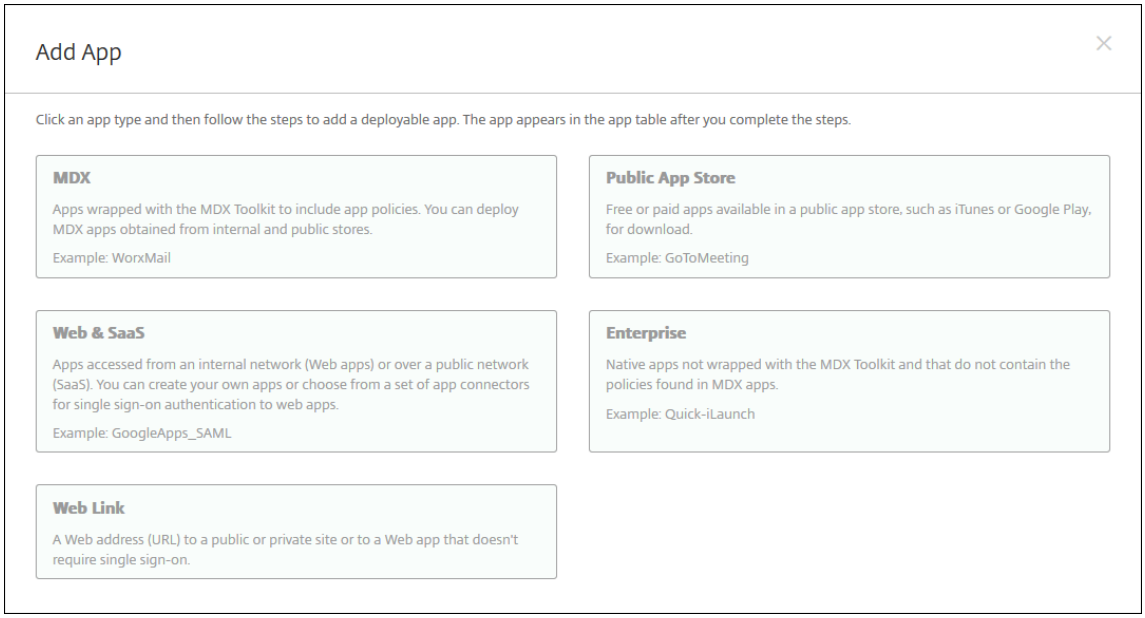
Agregar una aplicación de empresa

Las aplicaciones empresariales de XenMobile representan aplicaciones nativas que no están preparadas con el SDK de MAM o MDX Toolkit. Esas aplicaciones no contienen las directivas asociadas a las 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 Enterprise (archivo APK)
- Consulte también Aplicaciones privadas habilitadas para MDX.

No se admite la opción de agregar aplicaciones descargadas desde Google Play como aplicaciones de empresa. En vez de ello, agregue las aplicaciones de Google Play Store como aplicaciones provenientes del tienda pública de aplicaciones. Consulte Agregar una aplicación de la tienda pública de aplicaciones.

1. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones > Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



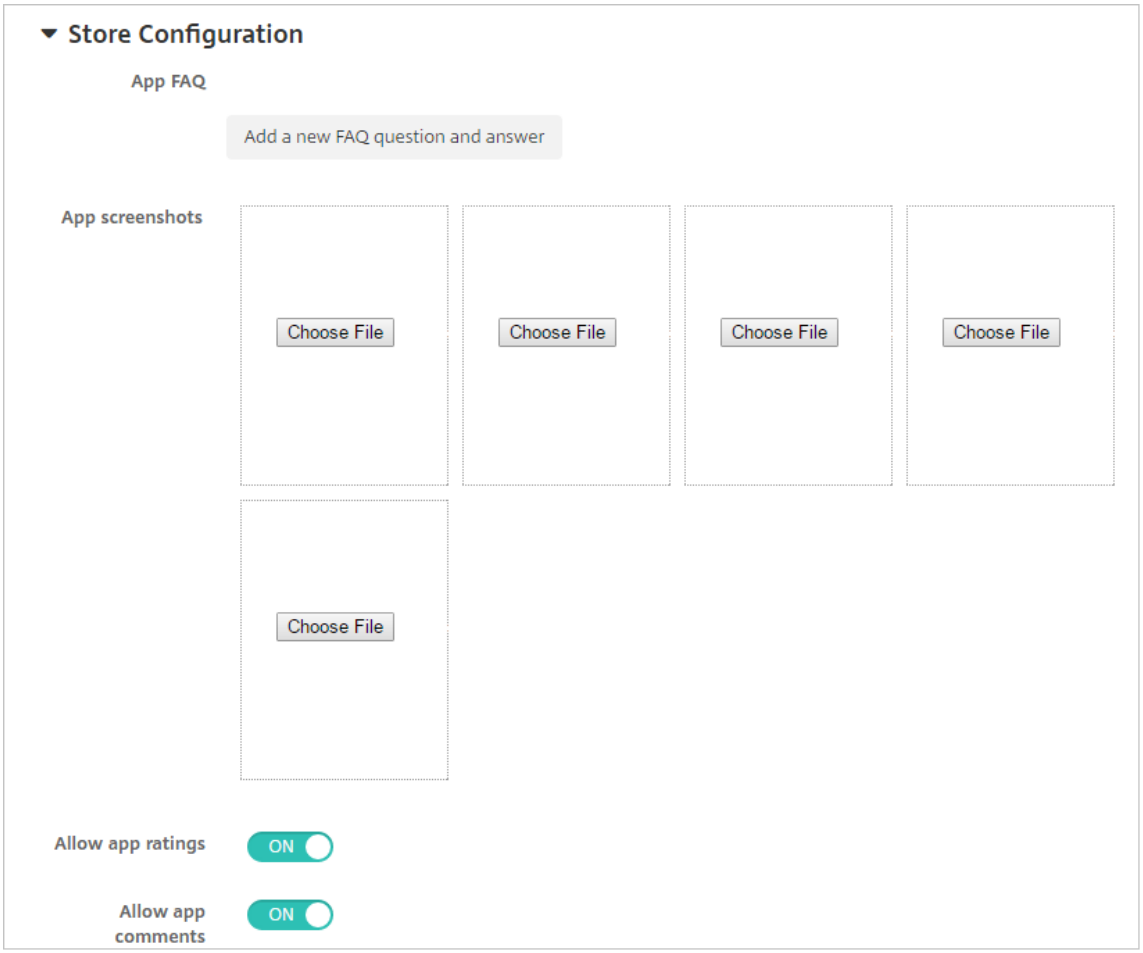
2. Haga clic en **Empresa**. Aparecerá la página **Información de la aplicación**.
3. En el panel **Información de la aplicación**, escriba la información siguiente:
    - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en "Nombre de la aplicación", en la tabla "Aplicaciones".
    - **Descripción:** Escriba, si quiere, una descripción de la aplicación.

- **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.

4. Haga clic en **Siguiente**. Aparecerá la página de las **plataformas de la aplicación**.
5. En **Plataformas**, seleccione las plataformas que quiera agregar. Si solo va a configurar una plataforma, desmarque las demás.
6. Elija un archivo que cargar correspondiente a la plataforma seleccionada. Para ello, haga clic en **Cargar** y vaya a la ubicación del archivo.
7. Haga clic en **Siguiente**. Aparecerá la página de información referente a la aplicación para la plataforma pertinente.
8. Configure los parámetros para el tipo de plataforma, como:

   - **Nombre de archivo:** Si quiere, escriba un nuevo nombre para la aplicación.
   - **Descripción de la aplicación:** Si quiere, indique una nueva descripción de la aplicación.
   - **Versión de la aplicación:** Este campo no se puede cambiar.
   - **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
   - **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
   - **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
   - **ID del paquete:** Identificador único de la aplicación.
   - **Quitar aplicación si se quita el perfil MDM:** Seleccione si quiere quitar la aplicación de un dispositivo cuando se quite el perfil de MDM. Está **activado** de forma predeterminada.
   - **Impedir copia de seguridad de datos de la aplicación:** Seleccione si quiere impedir que la aplicación realice copias de seguridad de los datos. Está **activado** de forma predeterminada.
   - **Forzar administración de la aplicación:** Si instala una aplicación no administrada, seleccione **Sí** para solicitar a los usuarios de dispositivos no supervisados permiso para administrarla. Si el usuario acepta la solicitud, la aplicación se administrará.

9. Configurar las reglas de implementación. Para obtener información, consulte Reglas de implementación.
10. Expanda **Configuración del almacén**.



- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

11. Haga clic en **Siguiente**. Aparecerá la página **Aprobaciones**.

    Para utilizar flujos de trabajo que requieran aprobación antes de permitir que los usuarios accedan a la aplicación, consulte Aplicar flujos de trabajo. Si no necesita flujos de trabajo de aprobación, vaya al siguiente paso.

12. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.
13. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione un grupo o varios de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.

14. Expanda **Programación de implementación** y, a continuación, configure estos parámetros:

    - **Implementar:** Elija si quiere implementar la aplicación en los dispositivos. Está **activado** de forma predeterminada.
    - **Programación de implementación:** Elija si quiere implementar la aplicación **Ahora** o **Más tarde**. Si selecciona **Más tarde**, configure una fecha y hora para implementar la aplicación. El valor predeterminado es **Ahora**.
    - **Condición de implementación:** Seleccione **En cada conexión** para implementar la aplicación cada vez que se conecte el dispositivo. Elija **Solo cuando haya fallado la implementación anterior** para implementar la aplicación cuando el dispositivo no haya recibido previamente la aplicación. El valor predeterminado es **En cada conexión**.

    La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

    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 **Implementar para conexiones permanentes**.

15. Haga clic en **Guardar**.

Agregar un enlace web

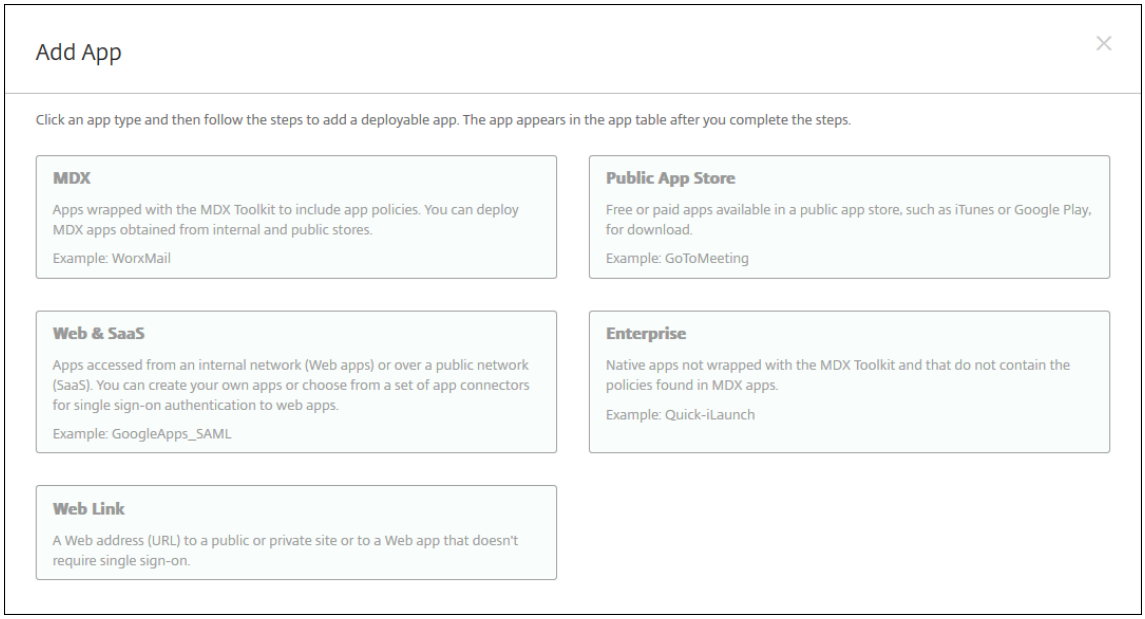
Un enlace web es una dirección web a un sitio de Internet o de intranet. Un enlace web también puede apuntar a una aplicación web que no requiere autenticación SSO. Una vez configurado el enlace web, este aparece como un icono en el almacén de aplicaciones. Cuando los usuarios inician sesión en Secure Hub, el enlace aparece con la lista de aplicaciones y escritorios disponibles.

Puede configurar enlaces web desde la ficha **Apps** de la consola de XenMobile. Una vez configurado el enlace web, aparece como un icono de enlace en la lista de la tabla **Aplicaciones**. Cuando los usuarios inician sesión en Secure Hub, el enlace aparece con la lista de aplicaciones y escritorios disponibles.

Para agregar el enlace, debe proporcionar la siguiente información:

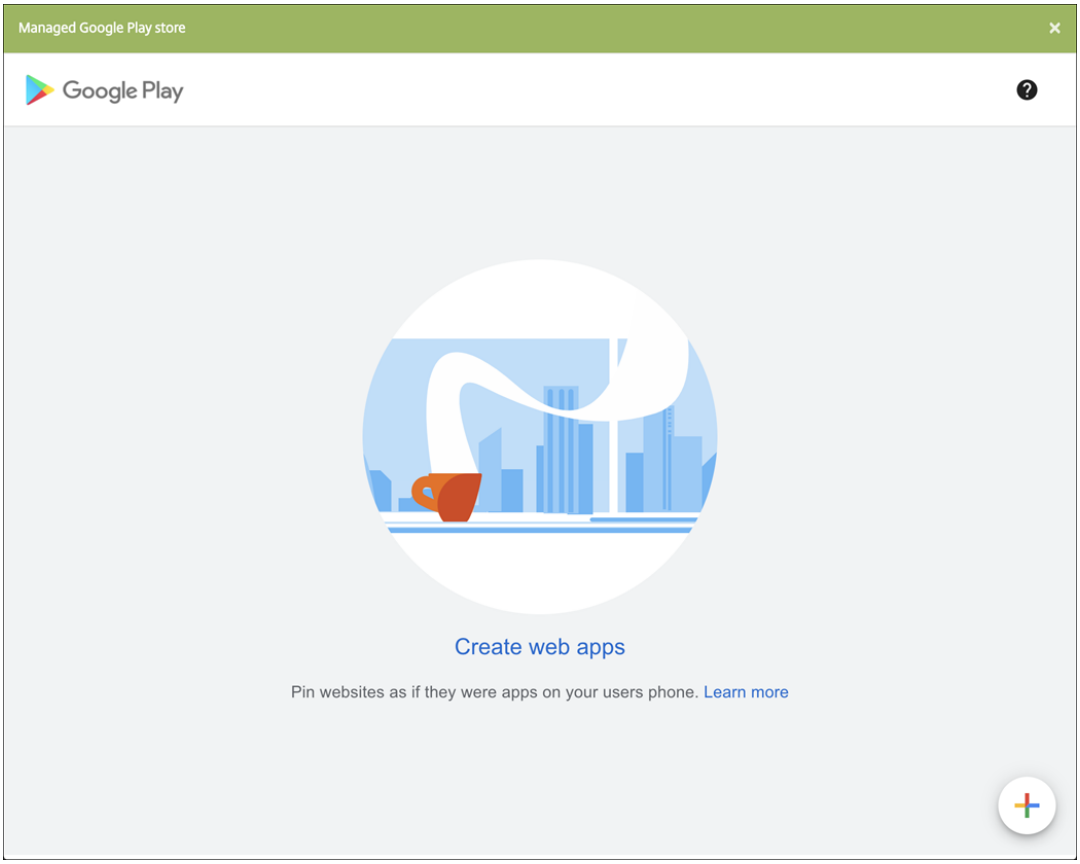
- Nombre del enlace
- Descripción del enlace
- Dirección web (URL)
- Categoría
- Rol
- Imagen en formato PNG (optativo)

1. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones > Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



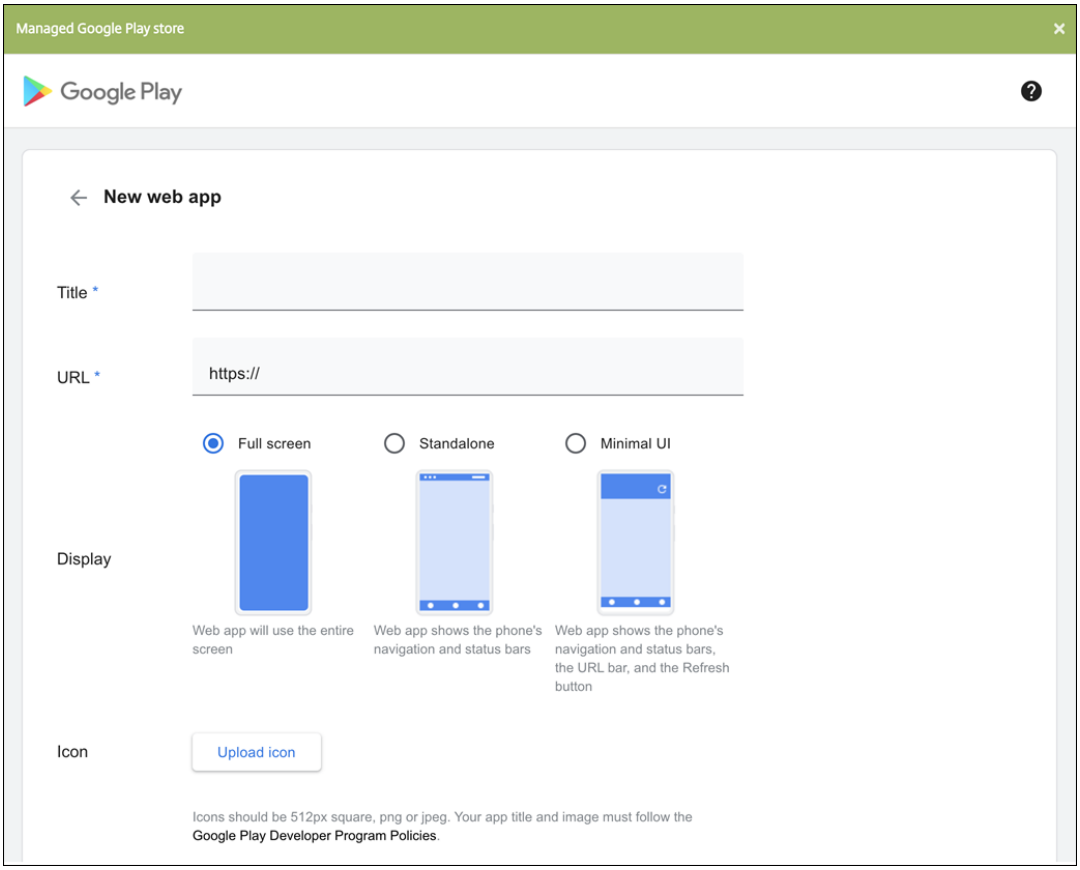
2. Haga clic en **Enlace web**. Aparecerá la página **Información de la aplicación**.
3. En el panel **Información de la aplicación**, escriba la información siguiente:

   Nombre: Escriba un nombre descriptivo para la aplicación. Este nombre figurará en “Nombre de la aplicación”, en la tabla “Aplicaciones”.
   Descripción: Escriba, si quiere, una descripción de la aplicación.
   Categoría de la aplicación: En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.
4. Haga clic en **Siguiente**. Aparecerá la página de las **plataformas de la aplicación**.
5. En **Plataformas**, seleccione **Otras plataformas** para agregar una aplicación web para iOS y Android (AD heredado), o seleccione **Android Enterprise**. Desmarque la casilla que no quiera agregar.
   - Si selecciona **Otras plataformas**, vaya al siguiente paso para configurar los parámetros.
   - Si selecciona **Android Enterprise**, haga clic en el botón **Cargar** para abrir Google Play Store administrado. No es necesario registrarse con una cuenta de desarrollador para publicar una aplicación web. Haga clic en el icono **Más** situado en la esquina inferior derecha para continuar.



Configure estos parámetros:

- **Título:** Escriba el nombre de la aplicación web.
- **URL:** Indique la dirección web de la aplicación.
- **Pantalla:** Indique cómo mostrar la aplicación web en los dispositivos de usuario. Las opciones disponibles son: **Pantalla completa**, **Independiente** e **Interfaz de usuario mínima**.
- **Icono:** Cargue su propia imagen para representar la aplicación web.



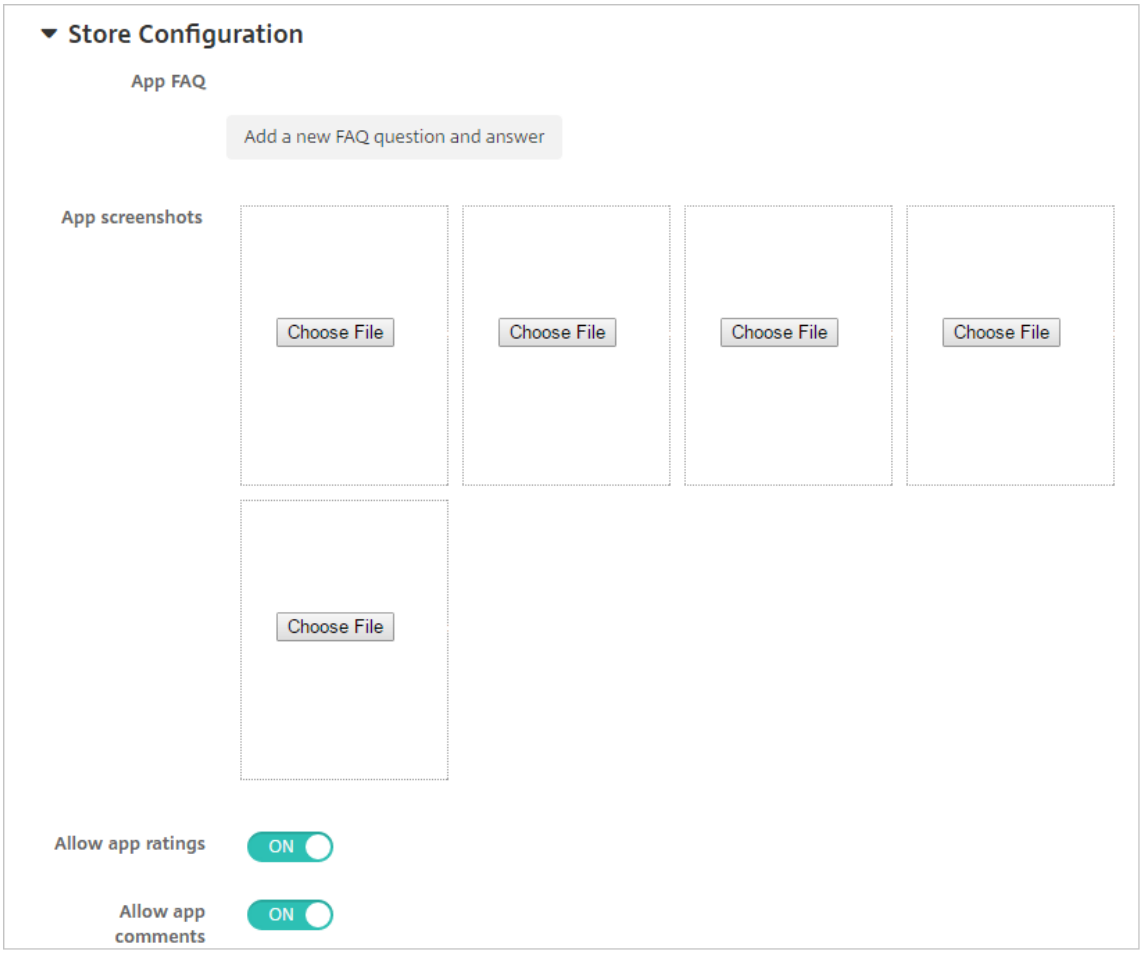
Cuando haya terminado, haga clic en **Crear**. La aplicación web puede tardar hasta 10 minutos en publicarse.

6. Para plataformas que no sean Android Enterprise, configure estas opciones:

   - **Nombre de la aplicación:** Acepte el nombre que ya aparece o escriba uno nuevo.
   - **Descripción de la aplicación:** 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.
   - **Aplicación alojada en la red interna:** 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 Citrix Gateway. Si **activa** esta opción, se agrega la palabra clave VPN a la aplicación y se permite a los usuarios conectarse a través de Citrix Gateway. Está **desactivado** de forma predeterminada.
   - **Categoría de la aplicación:** En la lista, si quiere, haga clic en una categoría que se va a aplicar a la aplicación.
   - **Imagen:** Seleccione si usar la imagen predeterminada de Citrix o cargar su propia imagen de la aplicación. El valor predeterminado es “Usar predeterminada”.
     - Si quiere cargar su propia imagen, haga clic en **Examinar**, vaya a la ubicación del

archivo y selecciónelo. El archivo debe ser PNG. No se puede cargar archivos JPEG o GIF. Cuando se agrega un gráfico personalizado, no se puede modificar más tarde.

7. Configurar las reglas de implementación. Para obtener información, consulte Reglas de implementación.
8. Expanda **Configuración del almacén**.



- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

9. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.
10. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione un grupo o varios de la lista. Los grupos que seleccione aparecerán en la lista

Grupos de entrega a recibir asignaciones de aplicaciones.

11. Expanda **Programación de implementación** y, a continuación, configure estos parámetros:

    - **Implementar:** Elija si quiere implementar la aplicación en los dispositivos. Está **activado** de forma predeterminada.
    - **Programación de implementación:** Elija si quiere implementar la aplicación **Ahora** o **Más tarde**. Si selecciona **Más tarde**, configure una fecha y hora para implementar la aplicación. El valor predeterminado es **Ahora**.
    - **Condición de implementación:** Seleccione **En cada conexión** para implementar la aplicación cada vez que se conecte el dispositivo. Elija **Solo cuando haya fallado la implementación anterior** para implementar la aplicación cuando el dispositivo no haya recibido previamente la aplicación. El valor predeterminado es **En cada conexión**.

    La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

    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 **Implementar para conexiones permanentes**.

12. Haga clic en **Guardar**.

Habilitar aplicaciones de Microsoft 365

Puede abrir el contenedor MDX para permitir a Secure Mail, Secure Web y Citrix Files que transfieran documentos y datos a las aplicaciones de Microsoft Office 365. Para obtener más información, consulte Permitir la interacción segura con aplicaciones Office 365.

Aplicar flujos de trabajo

Configure estos parámetros para asignar o crear un flujo de trabajo:

- **Flujo de trabajo para usar:** En la lista, haga clic en un flujo de trabajo existente o haga clic en **Crear un flujo de trabajo**. El valor predeterminado es **Ninguno**.

  Si selecciona **Crear un flujo de trabajo** configure los siguientes parámetros:

  - **Nombre:** Escriba un nombre único para el flujo de trabajo.
  - **Descripción:** Si quiere, escriba una descripción del flujo de trabajo.
  - **Plantillas de correo electrónico de aprobación:** En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar al flujo de trabajo. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.

- **Niveles de aprobación administrativa:** En la lista, seleccione la cantidad de niveles de aprobación administrativa necesarios para este flujo de trabajo. El valor predeterminado es 1 nivel. Las opciones posibles son:
  - No se necesita
  - 1 nivel
  - 2 niveles
  - 3 niveles
- **Seleccionar dominio de Active Directory:** En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
- **Buscar aprobadores adicionales requeridos:** Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Buscar**. Los nombres se originan en Active Directory.
- Cuando el nombre aparezca en el campo, marque la casilla situada al lado. El nombre y la dirección de correo electrónico aparecen en la lista **Aprobadores adicionales requeridos seleccionados**.

  Para quitar a una persona de la lista **Aprobadores adicionales requeridos seleccionados**, realice una de las siguientes acciones:
  - Haga clic en **Buscar** 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 **Buscar** para limitar los resultados de la búsqueda.
  - Las personas de la lista **Aprobadores adicionales requeridos seleccionados** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla situada junto a cada nombre que quiera quitar.

Personalizar la marca en el almacén de aplicaciones y Citrix Secure Hub

Puede definir el modo en que las aplicaciones aparecen en el almacén y agregar un logotipo para personalizar Secure Hub y el almacén de aplicaciones. Las funciones de personalización de marca están disponibles para dispositivos iOS y Android.

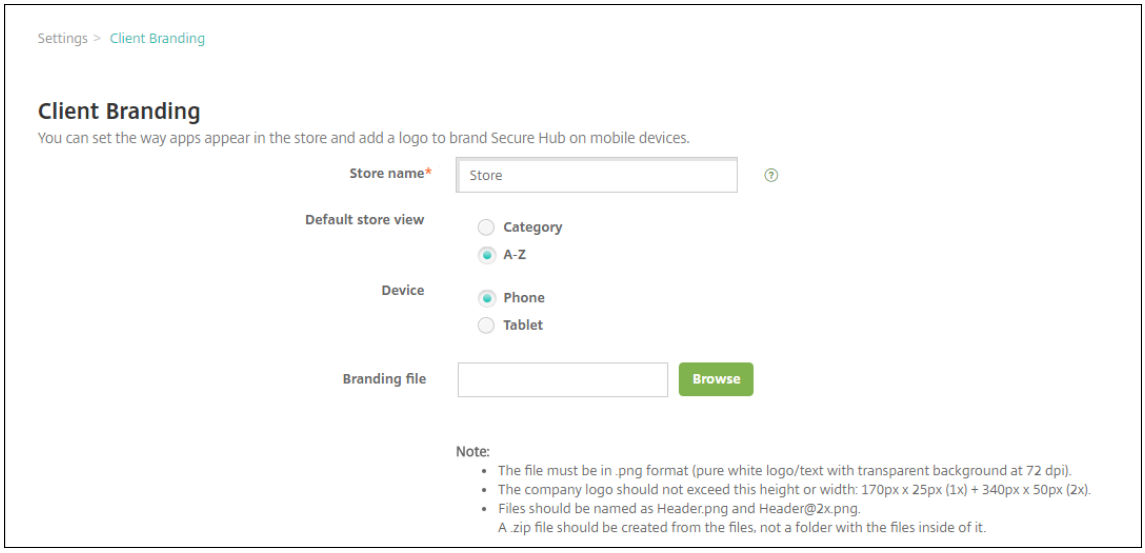
Antes de comenzar, compruebe que la imagen de personalización de marca está preparada y se puede acceder a ella.

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 Encabezado.png o Encabezado@2x.png.
- Cree un archivo ZIP con los archivos, no una carpeta con los archivos en ella.

1. En la consola de XenMobile Server, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Cliente**, haga clic en **Personalización de marca del cliente**. Aparecerá la página **Personalización de marca del cliente**.



Configure los siguientes parámetros:

- **Nombre del almacén:** El nombre de almacén 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 del almacén. Por lo general, no es necesario cambiar el nombre predeterminado.

  > **Importante:**
  >
  > El nombre del almacén solo puede contener caracteres alfanuméricos.

- **Vista predeterminada de almacén:** Seleccione **Categoría** o **A-Z**. El valor predeterminado es **A-Z**.
- **Opción de dispositivo:** Seleccione **Teléfono** o **Tableta**. El valor predeterminado es **Teléfono**.
- **Archivo de marca:** Seleccione un archivo o un ZIP con las imágenes que se van a usar para la personalización de marca. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.

3. Haga clic en **Guardar**.

Tipos de conectores de aplicaciones

April 1, 2020

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 un nuevo conector a XenMobile al agregar una aplicación web o SaaS.

En la tabla también se indica si el conector admite el uso de administración de cuentas de usuario, que permite crear cuentas nuevas automáticamente o con un flujo de trabajo.

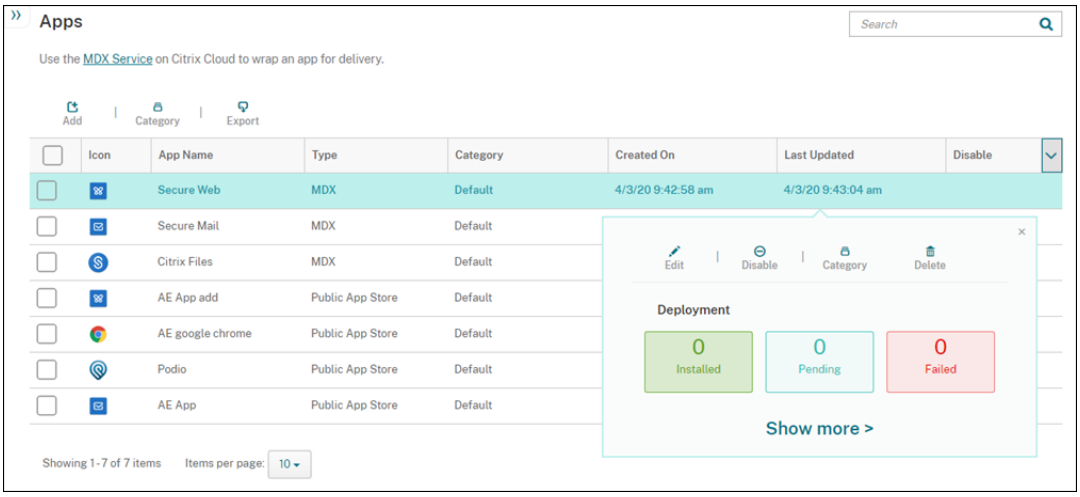
Nombre del conector	SSO SAML	Admite la administración de cuentas de usuario
EchoSign_SAML	S	S
Globoforce_SAML		**Nota:** Al utilizar este conector, debe habilitar la opción User Management for Provisioning para una correcta integración con el inicio de sesión SSO.
GoogleApps_SAML	S	S
GoogleApps_SAML_IDP	S	S
Lynda_SAML	S	S
Office365_SAML	S	S
Salesforce_SAML	S	S
Salesforce_SAML_SP	S	S
SandBox_SAML	S	
SuccessFactors_SAML	S	
ShareFile_SAML	S	
ShareFile_SAML_SP	S	
WebEx_SAML_SP	S	S

Actualizar la versión de aplicaciones MDX o de empresa

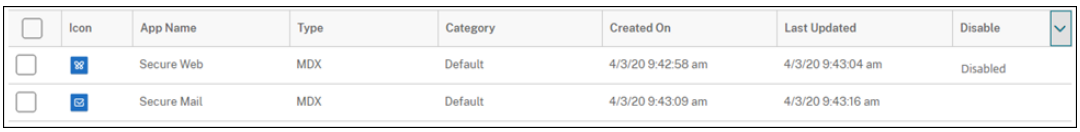
January 4, 2022

En XenMobile, para actualizar la versión de una aplicación MDX o de empresa, inhabilítela en la consola de XenMobile y, luego, cargue la nueva versión de esta. No necesita inhabilitar aplicaciones de almacén público como Citrix Secure Mail.

1. En la consola de XenMobile, haga clic en **Configurar > Aplicaciones**. Aparecerá la página **Aplicaciones**.
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:
   a) Para actualizar una aplicación, en la tabla **Aplicaciones**, marque la casilla situada junto a dicha aplicación o haga clic en la línea que la contiene.
   b) Haga clic en **Inhabilitar** en el menú que aparecerá.



   c) Haga clic en **Inhabilitar** en el cuadro de diálogo de confirmación. Aparecerá la etiqueta *Inhabilitada* en la columna **Inhabilitar** de la aplicación.



> **Nota:**
>
> 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, es posible que los usuarios que soliciten descargar la aplicación al mismo tiempo que usted carga la nueva versión tengan problemas.

3. Para actualizar una aplicación, en la tabla **Aplicaciones**, marque la casilla situada junto a dicha aplicación o haga clic en la línea que la contiene.

4. Haga clic en **Modificar** en el menú que aparecerá. Aparecerá la página **Información de la aplicación**, con las plataformas que ha elegido para la aplicación seleccionada.
5. Configure estos parámetros:
   - **Nombre:** Si quiere, puede cambiar el nombre de la aplicación.
   - **Descripción:** Si quiere, puede cambiar la descripción de la aplicación.
   - **Categoría de la aplicación:** 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:
   a) Elija el archivo de sustitución que quiera cargar. Para ello, haga clic en **Cargar** y vaya a la ubicación del archivo. La aplicación se cargará en XenMobile.

      Si va a cargar una aplicación para Android Enterprise, aparecerá una ventana de Google Play administrado. Cargue la nueva versión de la aplicación aquí. Para obtener más información detallada, consulte Distribuir aplicaciones de Android Enterprise.

   b) Si quiere, puede cambiar los datos de la aplicación y la configuración de directiva para la plataforma.

   c) También puede configurar reglas de implementación y XenMobile Store. Para obtener más información, consulte “Agregar una aplicación MDX” en Agregar aplicaciones.
7. Haga clic en **Guardar**. Aparecerá la página **Aplicaciones**.
8. Si ha inhabilitado la aplicación en el paso 2, haga lo siguiente:
   a) En la ficha **Aplicaciones**, haga clic para seleccionar la aplicación actualizada y, en el menú que aparece, haga clic en **Habilitar**.
   b) En el cuadro de confirmación que aparece, haga clic en **Habilitar**. Ahora, los usuarios podrán acceder a la aplicación y recibir una notificación que les pedirá actualizar la versión de la aplicación.

Citrix Launcher

January 4, 2022

Sustitución de Citrix Launcher

Citrix eliminará Citrix Launcher de la tienda de aplicaciones en agosto de 2020. Para reemplazar a Citrix Launcher, puede usar funciones que ya están disponibles.

Para aprovisionar dispositivos como quioscos (dispositivos dedicados):

1. Agregue un rol del control de acceso basado en roles (RBAC) que permita a los administradores de XenMobile inscribir dispositivos dedicados en su implementación de XenMobile. Consulte Aprovisionar dispositivos Android Enterprise dedicados.
2. Cree un perfil de inscripción con el **tipo de inscripción** llamado **Totalmente administrado/Perfil de trabajo**. Consulte Para crear un perfil de inscripción.
3. Cree una directiva de quiosco para configurar una aplicación que se anclará a la pantalla del dispositivo. Para ello, habilite la configuración **Modo de bloqueo de tarea**. Consulte Parámetros de Android Enterprise.

Acerca de Citrix Launcher

Citrix Launcher permite personalizar la experiencia de usuario en los dispositivos Android implementados por XenMobile. Android 4.0.3 es la versión mínima de Android que se admite para que Secure Hub administre Citrix Launcher. Citrix Launcher y la directiva de dispositivo "Configuración de Launcher" no son compatibles con Android Enterprise.

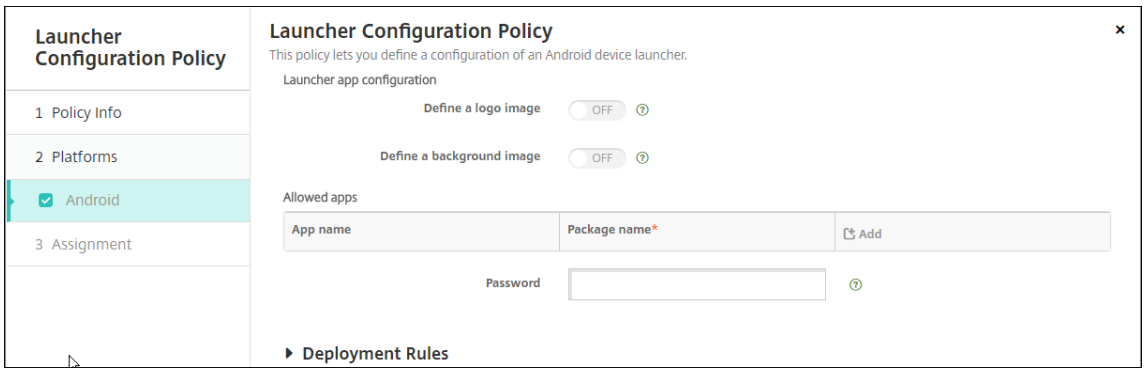
Puede agregar la directiva **Configuración de Launcher** para controlar esas funciones de Citrix Launcher:

- Administre los dispositivos Android, de manera que los usuarios solo puedan acceder a las aplicaciones que especifique.
- Si lo prefiere, puede especificar una imagen de logo personalizada como icono de Citrix Launcher, así como una imagen de fondo para Citrix Launcher.
- Especifique una contraseña que los usuarios deban introducir para salir de Launcher.

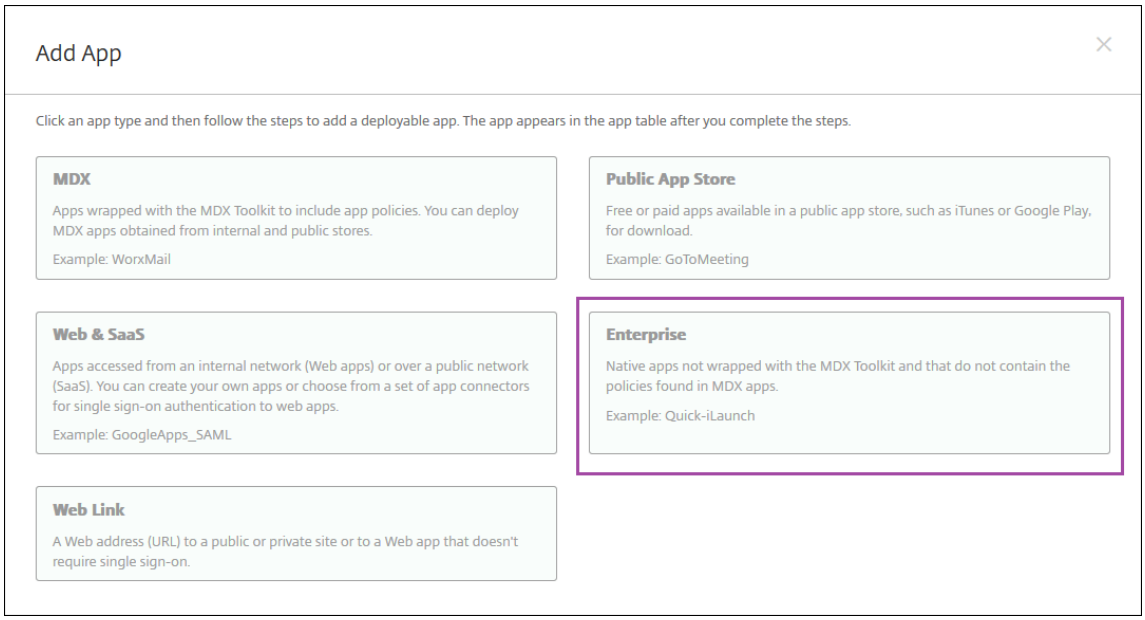
Si bien Citrix Launcher permite aplicar restricciones a nivel de dispositivo, también concede a los usuarios acceso integrado a las configuraciones de los dispositivos (como los parámetros de Wi-Fi, Bluetooth y los parámetros de códigos de acceso). Citrix Launcher no está diseñado como una capa de seguridad adicional situada sobre la capa que la plataforma del dispositivo ya proporciona.

Para proporcionar Citrix Launcher a dispositivos Android, siga estos pasos generales.

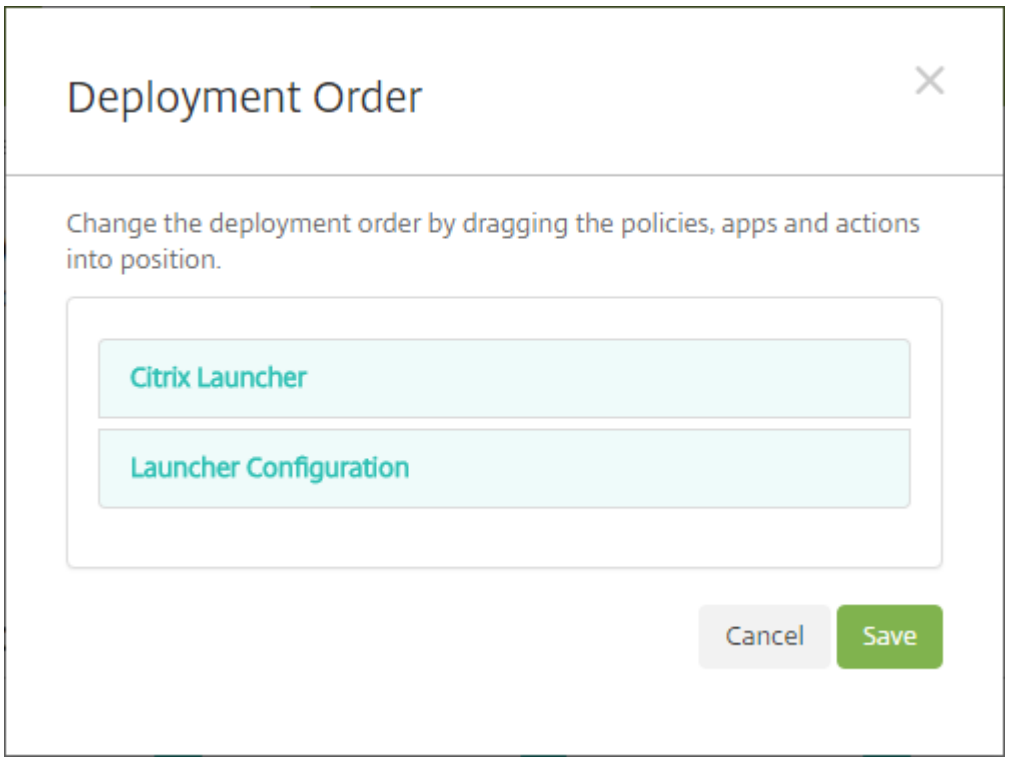
1. Para descargar la aplicación Citrix Launcher, vaya a https://www.citrix.com/downloads. Busque **Citrix Launcher**. El nombre del archivo es CitrixLauncher.apk. El archivo está listo para cargarlo en XenMobile y no requiere empaquetado.
2. Agregue la directiva de dispositivo: **Directiva de configuración del Launcher**. Vaya a **Configurar > Directivas de dispositivo**, haga clic en **Agregar** y, en el cuadro de diálogo **Agregar nueva directiva**, empiece a teclear **Launcher**. Para obtener más información, consulte Directiva de configuración del Launcher.



3. Agregue la aplicación Citrix Launcher a XenMobile como una aplicación de empresa. En **Configurar > Aplicaciones**, haga clic en **Agregar** y, a continuación, haga clic en **Empresa**. Para obtener información más detallada, consulte Agregar una aplicación de empresa.



4. Cree un grupo de entrega de Citrix Launcher con la siguiente configuración en **Configurar > Grupos de entrega**.
   - En la página **Directivas**, agregue **Directiva de configuración del Launcher**.
   - En la página **Aplicaciones**, arrastre **Citrix Launcher** a **Aplicaciones obligatorias**.
   - En la página **Resumen**, haga clic en **Orden de implementación** y compruebe que la aplicación **Citrix Launcher** precede a la directiva **Configuración del Launcher**.



Para obtener más información, consulte Implementar recursos.

Compras por volumen de Apple

January 4, 2022

Puede administrar las licencias de las aplicaciones iOS mediante las compras por volumen de Apple. La solución de compras por volumen simplifica el proceso de búsqueda, compra y distribución de aplicaciones (y otros datos) de forma masiva en una organización.

Con compra por volumen, puede usar XenMobile para distribuir aplicaciones de tienda pública.

- La compra por volumen no se admite para la inscripción en MAM. Debe inscribir dispositivos de compra por volumen en MDM o MDM+MAM.
- Las compras por volumen no se admiten para las aplicaciones móviles de productividad Citrix.
- Aunque puede distribuir las aplicaciones de tienda pública de XenMobile con compra por volumen, la implementación no es óptima. Se requieren mejoras a XenMobile y la tienda Secure Hub para abordar las limitaciones.
- Para ver una lista de los problemas conocidos a la hora de distribuir las aplicaciones de la tienda pública de XenMobile mediante las compras por volumen, consulte este artículo en Knowledge Center de Citrix.

Con la compra por volumen, puede distribuir las aplicaciones correspondientes directamente a los dispositivos. O bien, puede asignar contenido a los usuarios mediante códigos de canje. En XenMobile, puede configurar parámetros específicos de compra por volumen de iOS.

Periódicamente, XenMobile vuelve a importar licencias de compras por volumen desde Apple para que estas reflejen todos los cambios. Estos cambios incluyen la eliminación manual de una aplicación importada de la compra por volumen. De forma predeterminada, XenMobile actualiza el punto de referencia para las licencias de compra por volumen cada 1440 minutos (24 horas), como mínimo. Puede cambiar el intervalo del punto de referencia de compras por volumen a través de la propiedad de servidor `VPP.baseline`. Consulte Propiedades de servidor.

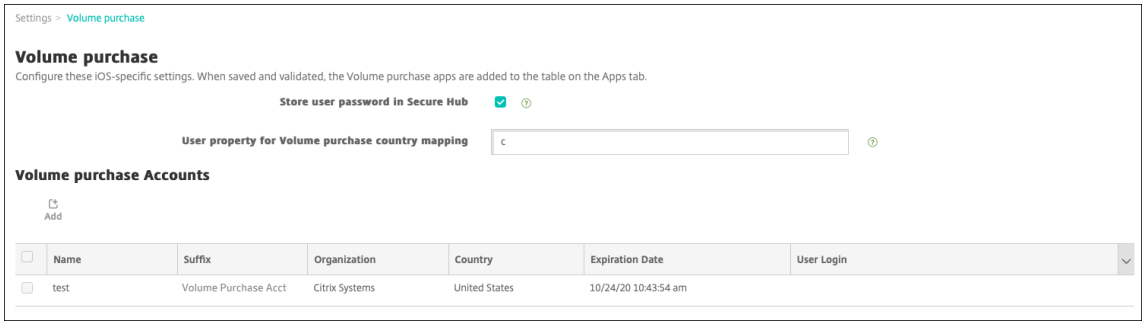
La configuración de **actualización automática de aplicaciones** también se basa en la propiedad de servidor `VPP.baseline`, y las aplicaciones se actualizan en la misma programación establecida en esa propiedad.

En este artículo, se describe exhaustivamente el uso de compra por volumen con licencias administradas, lo que permite utilizar XenMobile para distribuir aplicaciones. Si utiliza códigos de canje y quiere cambiar a una distribución administrada, consulte el documento de asistencia de Apple Migración de códigos de canje a distribución gestionada con las compras por volumen.

Para obtener información sobre las compras por volumen de iOS, consulte https://volume.itunes.apple.com/us/store. Para inscribirse en las compras por volumen, vaya a https://deploy.apple.com/qforms/open/register/index/avs. Para acceder a su tienda de compras por volumen en iTunes, vaya a https://volume.itunes.apple.com/?l=en.

Después de guardar estos parámetros de compras por volumen de iOS en XenMobile, las aplicaciones adquiridas aparecen en la página **Configurar > Aplicaciones** de la consola de XenMobile.

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Haga clic en **Compras por volumen**. Aparecerá la página de configuración de **Compras por volumen**.



3. Configure estos parámetros:

   - **Guardar contraseña del usuario en Secure Hub:** Seleccione si quiere almacenar de forma segura un nombre de usuario y la contraseña correspondiente en Secure Hub para

la autenticación en XenMobile. El valor predeterminado es almacenar los datos con este método seguro.

- **Propiedad de usuario para la asignación de país de las compras por volumen:** Escriba un código para que los usuarios puedan descargar aplicaciones de las tiendas de aplicaciones específicas de cada país.

XenMobile utiliza esta asignación para elegir la agrupación de propiedades de compra por volumen. Por ejemplo, si la propiedad del usuario es Estados Unidos, dicho usuario no puede descargar aplicaciones si el código de compra por volumen es para el Reino Unido. Póngase en contacto con el administrador de planes de compras por volumen para obtener más información acerca del código de asignación de país.

4. Para cada cuenta de compra por volumen que quiera agregar, haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar una cuenta de compras por volumen**.
5. Configure estos valores para cada cuenta que quiera agregar:

> **Nota:**
>
> Si utiliza Apple Configurator 1, debe cargar un archivo de licencias. Para ello, vaya a **Configurar > Aplicaciones**, vaya a la página de la plataforma y expanda **Compras por volumen**.

   - **Nombre:** Escriba el nombre de la cuenta de compras por volumen.
   - **Sufijo:** Escriba el sufijo que aparecerá en los nombres de las aplicaciones que se obtengan mediante la cuenta de compras por volumen. Por ejemplo, si introduce **VP**, la aplicación Secure Mail aparecerá en la lista de aplicaciones como **Secure Mail - VP**.
   - **Token de la empresa:** Copie y pegue el token de servicio de compra por volumen obtenido de Apple. Para obtener el token, en la página **Resumen de cuenta** del portal de compras por volumen de Apple, haga clic en el botón **Descargar** para generar y descargar el archivo de compra por volumen. Ese archivo contiene el token de servicio, además de otra información (como la caducidad y el código de país). Guarde el archivo en una ubicación segura.
   - **Inicio de sesión de usuario:** Escriba un nombre de administrador opcional de la cuenta de compra por volumen autorizada con la que se van a importar las aplicaciones B2B personalizadas.
   - **Contraseña de usuario:** Escriba la contraseña del administrador de la cuenta de compra por volumen.
   - **Actualización automática de aplicaciones:** Si está **activada**, las aplicaciones de compras por volumen se actualizan automáticamente cuando haya una actualización en la tienda de aplicaciones de Apple. Está **desactivado** de forma predeterminada.
6. Haga clic en **Guardar** para cerrar el cuadro de diálogo.
7. Haga clic en **Guardar** para guardar la configuración de compras por volumen.

Aparecerá un mensaje para informarle de que XenMobile agregará las aplicaciones a la lista de la página **Configurar > Aplicaciones**. En esa página, observe que los nombres de las aplicaciones extraídas de su cuenta de compra por volumen contienen el sufijo que proporcionó en la configuración anterior.

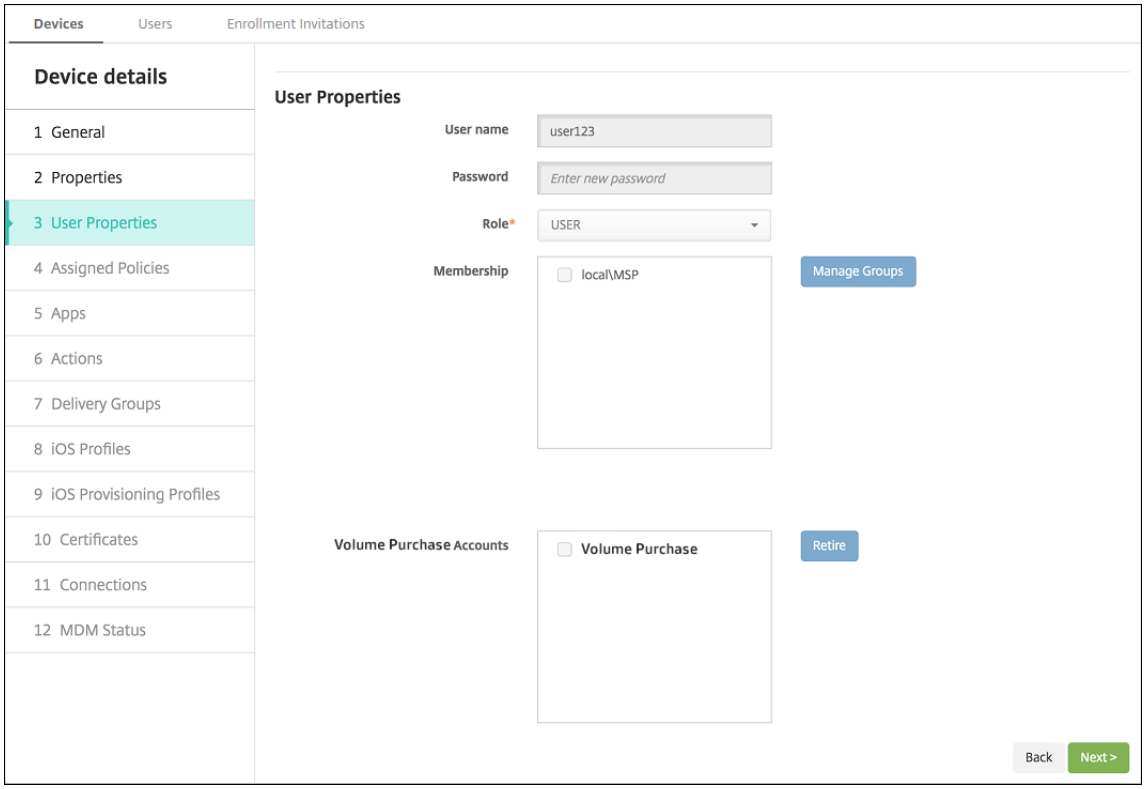
Ahora puede configurar la configuración de la aplicación de compra por volumen y, a continuación, ajustar la configuración de la directiva de grupo de entrega y dispositivo para las aplicaciones de compra por volumen. Después de completar esas configuraciones, los usuarios podrán inscribir sus dispositivos. Las siguientes notas contienen aspectos a tener en cuenta en dichos procesos.

- Al configurar los parámetros de la aplicación de compra por volumen (**Configurar > Aplicaciones**), habilite **Forzar asociación de licencia con el dispositivo**. Una de las ventajas de usar la compra por volumen de Apple y el programa de implementación con dispositivos supervisados es la capacidad de utilizar XenMobile para asignar la aplicación a nivel de dispositivo (en lugar de usuario). Por eso, no es necesario utilizar un dispositivo de ID de Apple. Además, los usuarios no reciben una invitación para participar en las compras por volumen de Apple. Asimismo, los usuarios pueden descargar las aplicaciones sin iniciar sesión en sus cuentas de iTunes.

  Para ver la información de compras por volumen de esa aplicación, expanda **Compras por volumen**. Observe que en la tabla **Claves de licencia de compras por volumen**, la licencia está asociada a un dispositivo. Si el usuario quita el token y lo importa de nuevo, aparecerá la palabra **Oculto** en lugar del número de serie, debido a las restricciones de privacidad de Apple.

  Para desvincular una licencia, haga clic en la fila de la licencia y en **Desasociar**.

  Si asocia licencias de compra por volumen a los usuarios, XenMobile integra a esos usuarios en la cuenta de compra por volumen y asocia sus ID de iTunes a la cuenta de compra por volumen. Ni la empresa ni el servidor de XenMobile ven nunca los ID de iTunes de los usuarios. Apple crea de forma transparente la asociación para mantener la privacidad de los usuarios. Puede retirar a un usuario de las compras por volumen de Apple para desasociar todas las licencias de la cuenta del usuario. Para retirar a un usuario, vaya a **Administrar > Dispositivos**.



- Cuando asigna una aplicación a un grupo de entrega, XenMobile la identifica de forma predeterminada como una aplicación opcional. Para que XenMobile implemente la aplicación en los dispositivos, vaya a **Configurar > Grupos de entrega**. En la página **Aplicaciones**, mueva la aplicación a la lista **Aplicaciones obligatorias**.
- Cuando hay una actualización disponible para una aplicación de tienda pública de aplicaciones y las compras por volumen envía esa aplicación a los dispositivos, esa aplicación se actualiza automáticamente en los dispositivos. Para enviar una actualización de Secure Hub, cuando se ha asignado a un dispositivo (no a un usuario), lleve a cabo lo siguiente. En **Configurar > Aplicaciones**, en la página de la plataforma, haga clic en **Comprobar actualizaciones** y aplique la actualización.

  XenMobile muestra una advertencia de caducidad de licencia cuando la compra por volumen de Apple ha caducado.

Virtual Apps and Desktops a través de Citrix Secure Hub

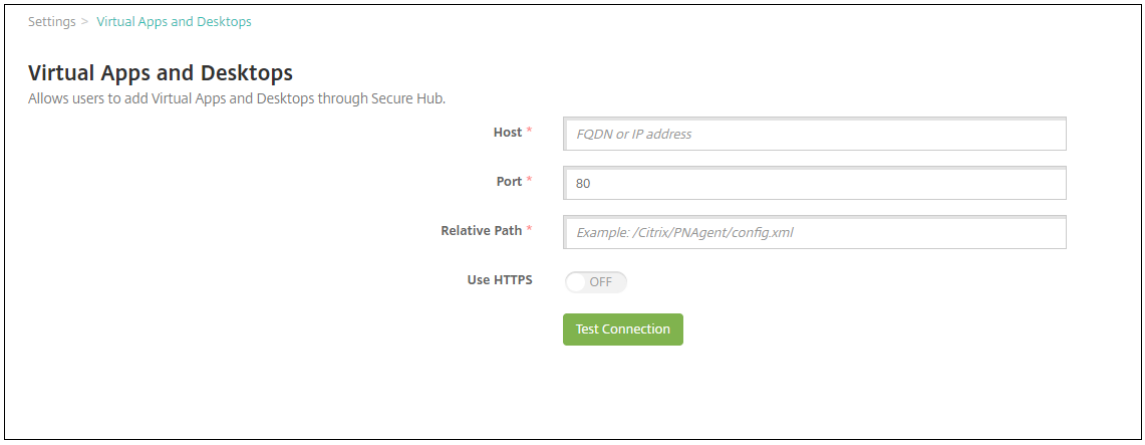
November 6, 2020

XenMobile puede recopilar aplicaciones desde Virtual Apps and Desktops y ponerlas a disposición de los usuarios de dispositivos móviles desde XenMobile Store. Los usuarios se suscriben a las apli-

caciones 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 **Parámetros**.
2. Haga clic en **Virtual Apps and Desktops**. Aparecerá la página **Virtual Apps and Desktops**.



3. Configure estos parámetros:
   - **Host:** Escriba el nombre de dominio completo (FQDN) o la dirección IP de StoreFront o del sitio de Interfaz Web.
   - **Puerto:** Escriba el número de puerto de StoreFront o del sitio de Interfaz Web. El valor predeterminado es 80.
   - **Ruta relativa:** Escriba la ruta. Por ejemplo, /Citrix/PNAgent/config.xml.
   - **Usar HTTPS:** Seleccione si habilitar la autenticación segura entre StoreFront o el sitio de Interfaz Web y el dispositivo cliente. Está **desactivado** de forma predeterminada.
4. Haga clic en **Probar conexión** para verificar que XenMobile puede conectarse al servidor Virtual Apps and Desktops especificado.
5. Haga clic en **Guardar**.

Usar Citrix Content Collaboration con XenMobile

January 4, 2022

XenMobile tiene dos opciones para integrarse en Citrix Content Collaboration: Citrix Files y los conectores de zonas de almacenamiento. La integración en Citrix Files o en conectores de zonas de alma-

cenamiento requiere XenMobile Enterprise Edition.

Citrix Files

Si dispone de XenMobile Enterprise Edition, puede configurar XenMobile para proporcionar acceso a su cuenta de Citrix Files. Esa configuración:

- Permite a los usuarios móviles acceder al conjunto completo de funcionalidades de Enterprise (como compartir archivos, sincronizarlos y utilizar conectores de zonas de almacenamiento).
- Puede ofrecer a Citrix Files la autenticación Single Sign-On para usuarios de las aplicaciones XenMobile y unas directivas completas de control de acceso.
- Proporciona la configuración de Citrix Files, la supervisión a nivel de servicio y la supervisión del uso de licencias a través de la consola de XenMobile.

Para obtener más información sobre cómo configurar XenMobile para Citrix Files, consulte SAML para Single Sign-On en Citrix Files.

Conectores de zonas de almacenamiento

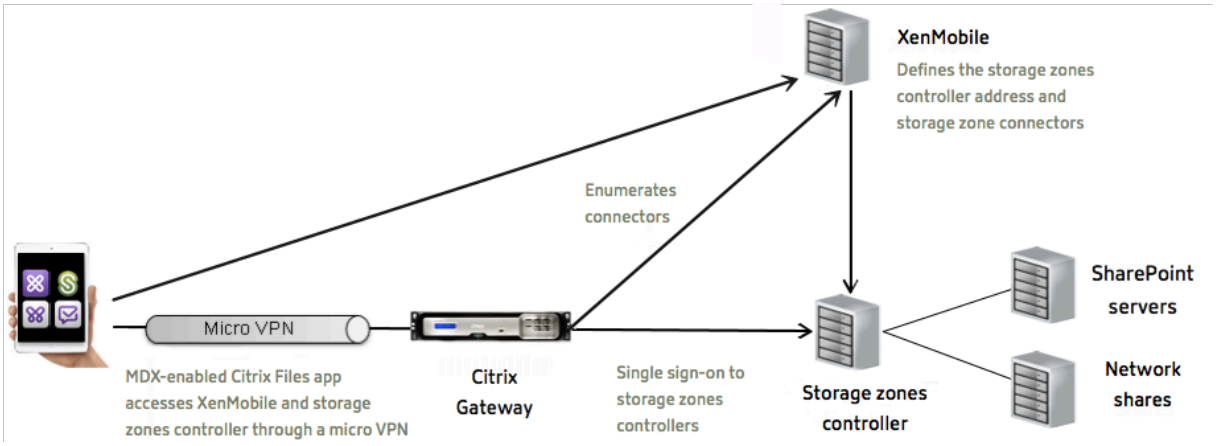
Puede configurar XenMobile para que solo ofrezca acceso a los conectores de zonas de almacenamiento que haya creado desde la consola de XenMobile. Esa configuración:

- Ofrece un acceso móvil seguro a los repositorios existentes de almacenamiento local (como sitios de SharePoint y recursos compartidos de red).
- No es necesario configurar un subdominio de Citrix Content Collaboration ni alojar datos de Citrix Files.
- Proporciona a los usuarios acceso móvil a los datos a través de las aplicaciones móviles de productividad de Citrix Files para iOS y Android. Los usuarios pueden modificar los documentos de Microsoft Office. Los usuarios también pueden ver en vista previa los archivos PDF de Adobe y hacer anotaciones en ellos desde dispositivos móviles.
- Cumple las restricciones de seguridad contra la filtración de datos de usuarios fuera de la red corporativa.
- Proporciona una configuración simple de conectores de zonas de almacenamiento desde la consola de XenMobile. Si más adelante decide usar la funcionalidad completa de Citrix Files con XenMobile, puede cambiar la configuración en la consola de XenMobile.
- Requiere XenMobile Enterprise Edition.

Para una integración de XenMobile solamente con conectores de zonas de almacenamiento:

- Citrix Content Collaboration utiliza su configuración de inicio de sesión único SSO en Citrix Gateway para autenticarse en conectores de zonas de almacenamiento.
- XenMobile no se autentica a través de SAML porque no se utiliza el plano de control de Citrix Files.

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



Requisitos

- Versiones mínimas de los componentes:
  - XenMobile Server 10.5 (instalación local)
  - ShareFile para iOS (MDX) 5.3
  - ShareFile para Android (MDX) 5.3
  - Controlador de zonas de almacenamiento 5.0
    Este artículo contiene instrucciones para configurar el controlador de zonas de almacenamiento 5.0
- Compruebe que el servidor que ejecutará el controlador de zonas de almacenamiento cumple los requisitos del sistema. Para conocer los requisitos, consulte Requisitos del sistema.

Los requisitos de las zonas de almacenamiento para datos de Citrix Files y para zonas de almacenamiento restringidas no se aplican cuando XenMobile se integra solamente en conectores de zonas de almacenamiento.

XenMobile no admite conectores para Documentum.

- Para ejecutar scripts de PowerShell:
  - Ejecute los scripts en la versión de 32 bits (x86) de PowerShell.

Tareas de instalación

Complete las siguientes tareas, en el orden presentado, para instalar y configurar un controlador de zonas de almacenamiento. Estos pasos son específicos de la integración de XenMobile con conectores de zonas de almacenamiento solamente. Algunos de estos artículos se encuentran en la documentación sobre los controladores de zonas de almacenamiento.

1. Configurar Citrix ADC para los controladores de zonas de almacenamiento

Puede usar Citrix ADC como un proxy DMZ para el controlador de zonas de almacenamiento.

2. Instalar un certificado SSL

   Un controlador de zonas de almacenamiento que aloja zonas estándares requiere un certificado SSL. Un controlador de zonas de almacenamiento que aloja zonas restringidas y usa una dirección interna no necesita ningún certificado SSL.

3. Preparar el servidor

   Se requiere la configuración de IIS y ASP.NET para los conectores de zonas de almacenamiento.

4. Instalar controlador de zonas de almacenamiento
5. Preparar un controlador de zonas de almacenamiento para que solo se pueda usar con conectores de zonas de almacenamiento
6. Especificar un servidor proxy para las zonas de almacenamiento

   La consola de los controladores de zonas de almacenamiento le permite especificar un servidor proxy para los controladores de zonas de almacenamiento. También puede especificar un servidor proxy mediante otros métodos.

7. Configurar el controlador de dominio de modo que confíe en el controlador de zonas de almacenamiento para la delegación

   Configure el controlador de dominio para admitir la autenticación NTLM o Kerberos en recursos compartidos de red o sitios de SharePoint.

8. Unir un controlador de zonas de almacenamiento secundario a una zona de almacenamiento

   Para configurar una zona de almacenamiento para alta disponibilidad, conecte al menos dos controladores de zonas de almacenamiento.

Instalar controlador de zonas de almacenamiento

1. Descargue e instale el software del controlador de zonas de almacenamiento:

   a) Vaya a https://www.citrix.com/downloads. Busque **ShareFile** y, a continuación, descargue el instalador más reciente del controlador de zonas de almacenamiento.

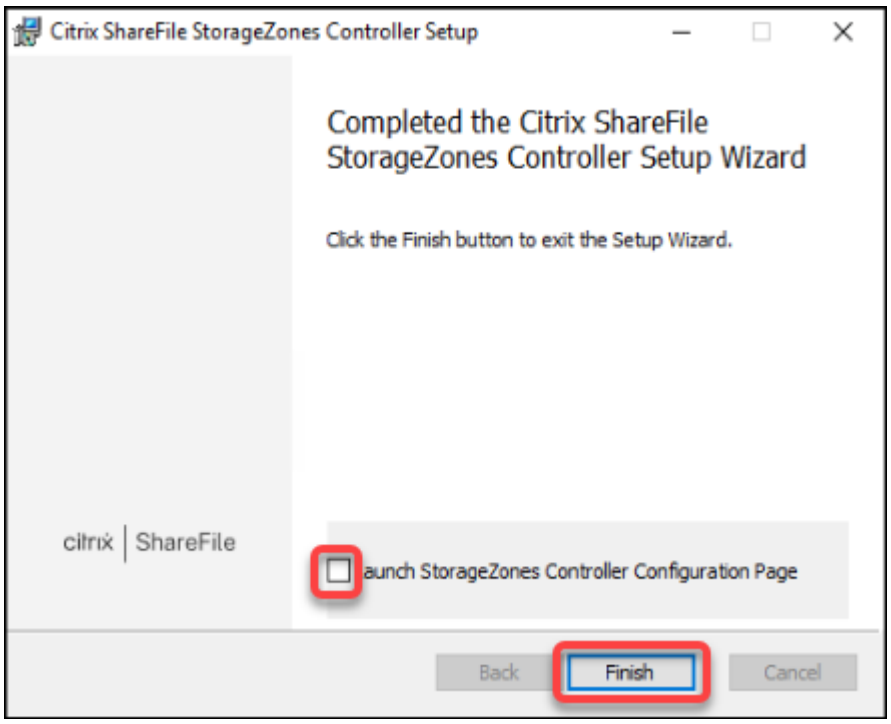
   b) Instalar el controlador de zonas de almacenamiento cambia el sitio web predeterminado en el servidor por la ruta de instalación del controlador. Habilite **Autenticación anónima** en el sitio web predeterminado.

2. En el servidor donde quiere instalar el controlador de zonas de almacenamiento, ejecute StorageCenter.msi.

   Se iniciará el asistente de instalación de controladores de zonas de almacenamiento.

3. Responda a estas indicaciones:

- En la página **Carpeta de destino**, si Internet Information Services (IIS) está instalado en la ubicación predeterminada, deje los valores predeterminados. Si no es así, vaya a la ubicación de instalación de IIS.
- Cuando finalice la instalación, desmarque la casilla para **Iniciar la página de configuración del controlador de zonas de almacenamiento** y, a continuación, haga clic en **Finalizar**.



4. Cuando se le solicite, reinicie el controlador de zonas de almacenamiento.
5. Para probar que la instalación se ha realizado correctamente, vaya a `https://localhost/`. Si la instalación se realiza correctamente, aparecerá el logotipo de Citrix Files.

   Si no aparece el logotipo de Citrix Files, borre la memoria caché del explorador web y vuelva a intentarlo.

   > **Importante:**
   >
   > Si va a clonar el controlador de zonas de almacenamiento, capture la imagen de disco antes de continuar con la configuración del controlador.

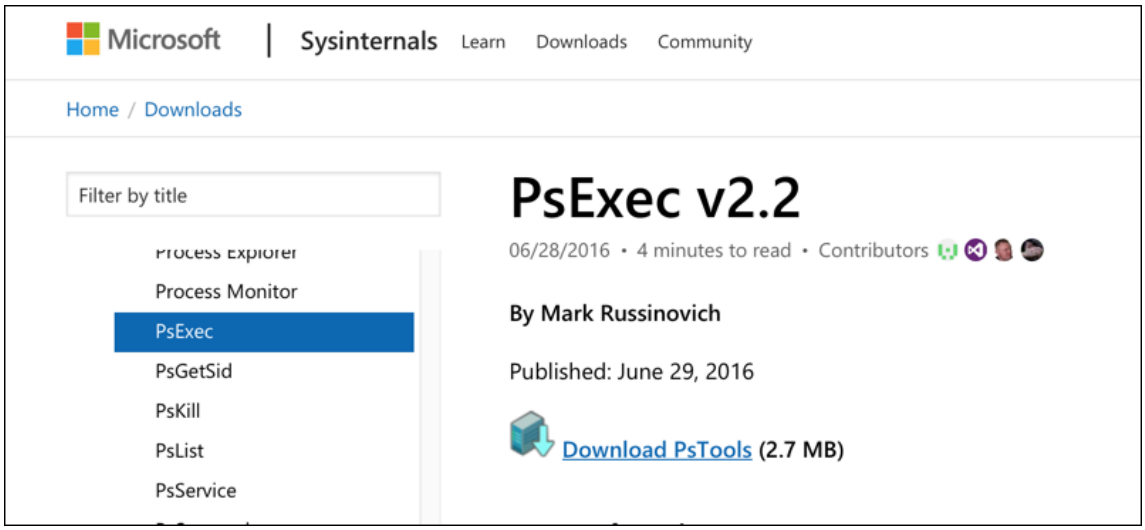
Preparar un controlador de zonas de almacenamiento para que solo se pueda usar con conectores de zonas de almacenamiento

Para una integración solo con conectores de zonas de almacenamiento, no es necesario usar la consola administrativa del controlador de zonas de almacenamiento. Esa interfaz requiere una cuenta de administrador de Citrix Files, que no es necesaria para esta solución. Por eso, puede ejecutar un

script de PowerShell para preparar el controlador de zonas de almacenamiento con el fin usarlo sin el plano de control de Citrix Files. El script lleva a cabo lo siguiente:

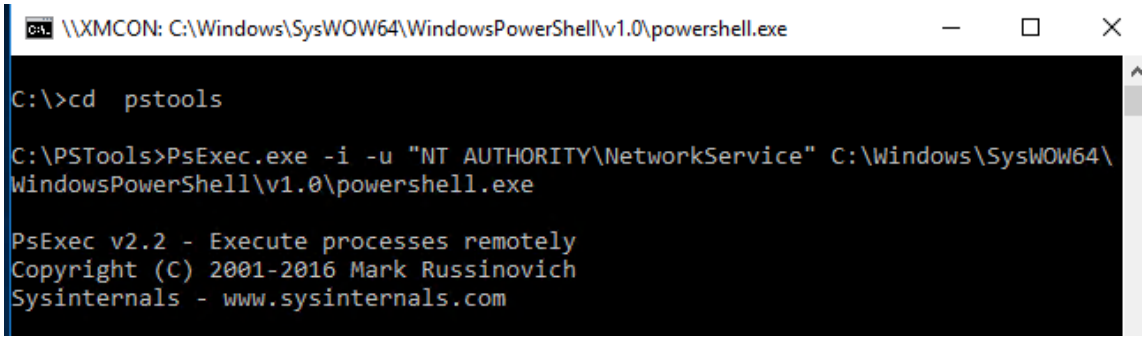
- Registra el controlador de zonas de almacenamiento actual como un controlador de zonas de almacenamiento principal. Más adelante puede unir al controlador principal controladores de zonas de almacenamiento secundarios.
- Crea una zona y establece la frase secreta para ella.

1. En el servidor del controlador de zonas de almacenamiento, descargue la herramienta PsExec. Para ello, vaya a Microsoft Windows Sysinternals y, a continuación, haga clic en **Descargar PsTools**. Extraiga la herramienta en la raíz de la unidad C:.

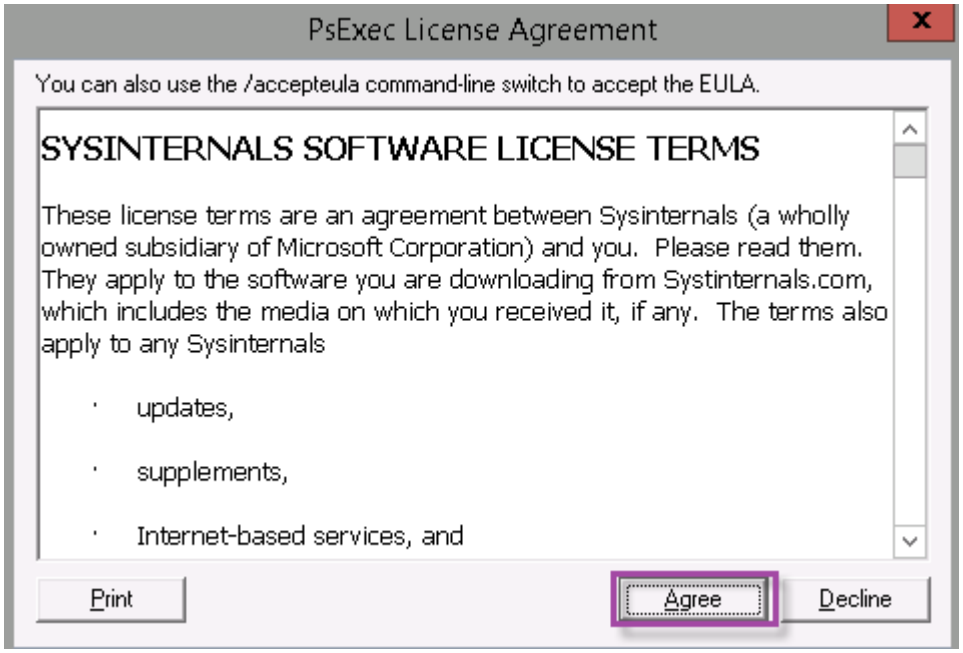


2. Ejecute la herramienta PsExec: Abra el símbolo del sistema como el usuario administrador y escriba lo siguiente:

```
cd c:\pstools
PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
<!--NeedCopy-->
```



3. Cuando se le pida, haga clic en **Agree** para ejecutar la herramienta Sysinternals.



Se abrirá una ventana de PowerShell.

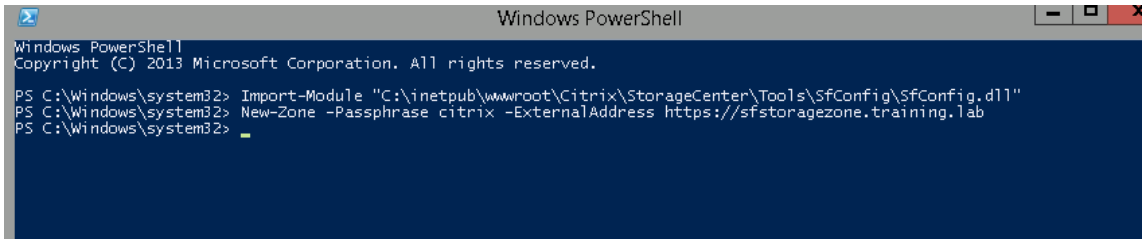
4. En la ventana de PowerShell, escriba lo siguiente:

```
Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\
   SfConfig\SfConfig.dll"
New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
   com
<!--NeedCopy-->
```

Donde:

Passphrase: Es la frase secreta que quiere asignar al sitio. Apúntela. No podrá recuperar la frase secreta desde el Controller. Si pierde la frase secreta, no puede volver a instalar el controlar de zonas de almacenamiento. Podrá unir más controladores de zonas de almacenamiento a la zona de almacenamiento o recuperar la zona de almacenamiento si el servidor falla.

ExternalAddress: Es el nombre de dominio completo externo del servidor del controlador de zonas de almacenamiento.



Ahora, el controlador de zonas de almacenamiento principal está listo.

Antes de iniciar sesión en XenMobile para crear conectores de zonas de almacenamiento, debe completar la configuración siguiente, si procede:

Especificar un servidor proxy para las zonas de almacenamiento

Configurar el controlador de dominio de modo que confíe en el controlador de zonas de almacenamiento para la delegación

Unir un controlador de zonas de almacenamiento secundario a una zona de almacenamiento

Para crear conectores de zonas de almacenamiento, consulte Definir conexiones de controladores de zonas de almacenamiento en XenMobile.

Unir un controlador de zonas de almacenamiento secundario a una zona de almacenamiento

Para configurar una zona de almacenamiento para alta disponibilidad, conecte al menos dos controladores de zonas de almacenamiento. Para unir un controlador de zonas de almacenamiento secundario a una zona, instale el controlador de zonas de almacenamiento en un segundo servidor. Luego, una ese Controller a la zona del Controller principal.

1. Abra una ventana de PowerShell en el servidor del controlador de zonas de almacenamiento que quiere unir al servidor principal.
2. En la ventana de PowerShell, escriba lo siguiente:

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
   ```

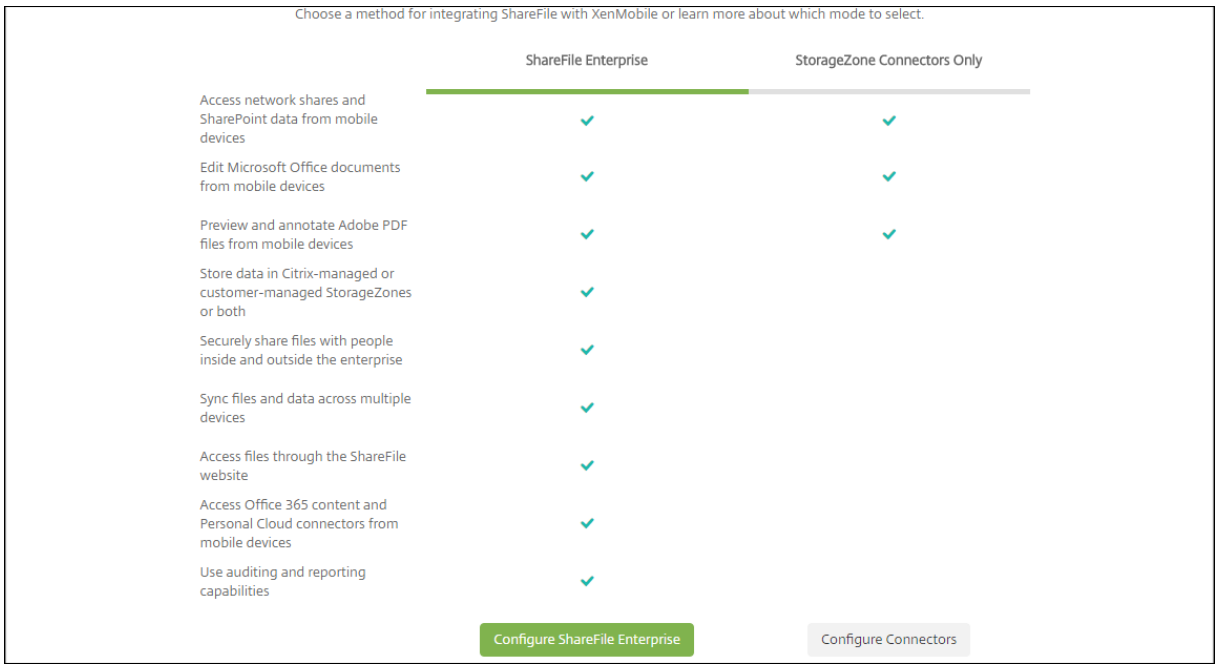
   Por ejemplo:

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

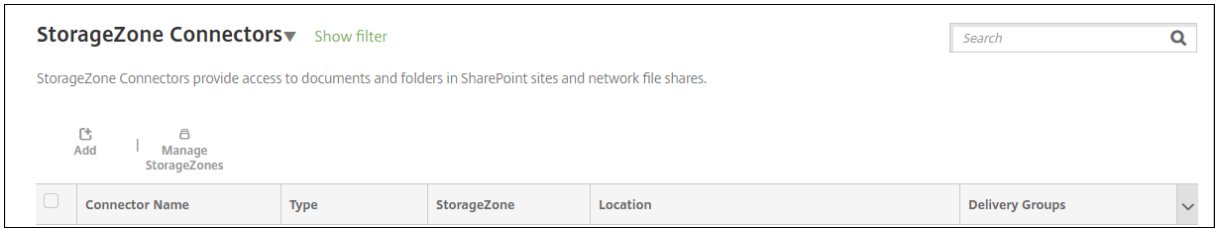
Definir conexiones de controladores de zonas de almacenamiento en XenMobile

Antes de agregar conectores de zonas de almacenamiento, configure la información de conexión de cada controlador de zonas de almacenamiento habilitado para conectores de zonas de almacenamiento. Los controladores de zonas de almacenamiento se pueden definir como se describe en esta sección, aunque también se pueden definir cuando se agregue un conector.

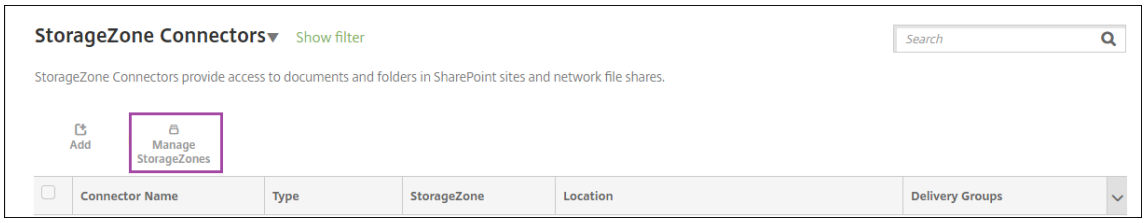
En su primera visita a la página **Configurar > ShareFile**, se resumen en la página las diferencias entre usar XenMobile para cuentas Enterprise y conectores de zonas de almacenamiento.



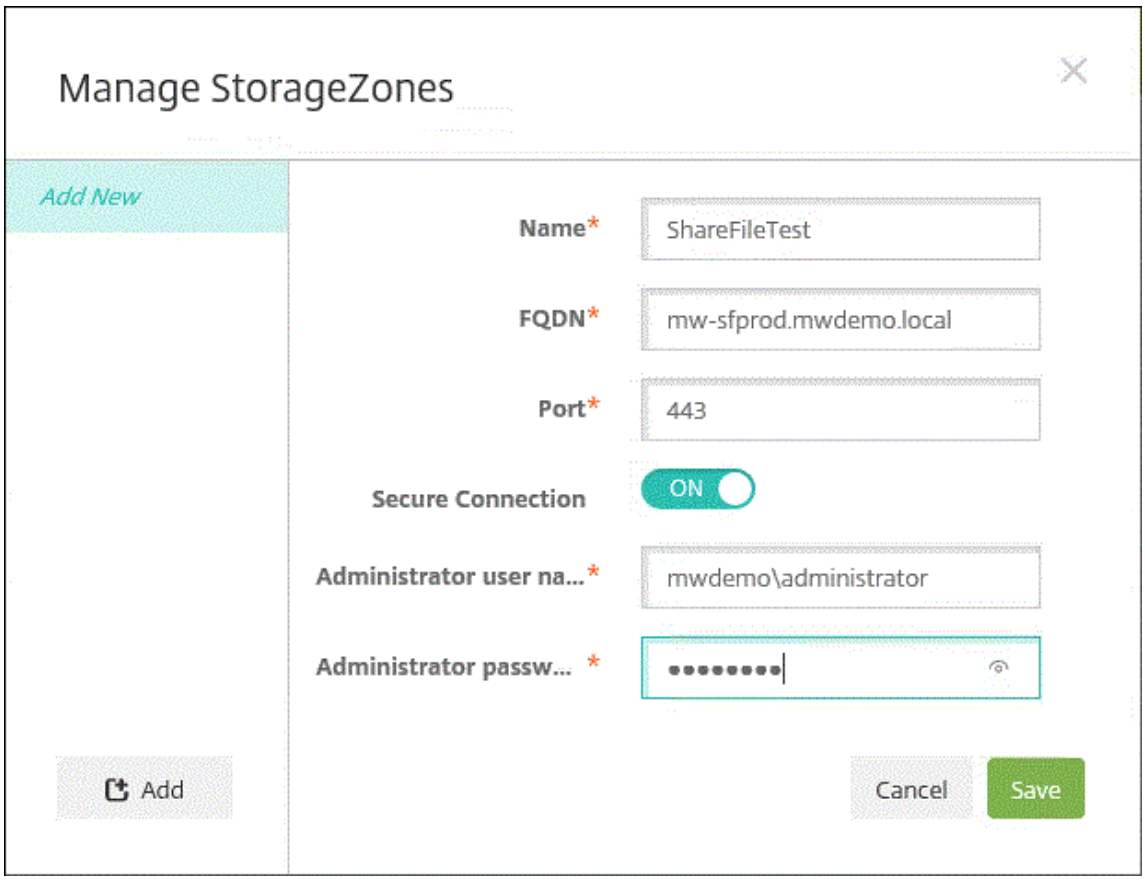
Haga clic en **Configurar conectores** para continuar con los pasos de configuración de este artículo.



1. En **Configurar > ShareFile**, haga clic en **Administrar StorageZones**.



2. En **Administrar StorageZones**, agregue la información de conexión.



- **Nombre:** Un nombre descriptivo para la StorageZone, que sirva para identificarla en XenMobile. No incluya espacios ni caracteres especiales en el nombre.
- **FQDN y puerto:** El nombre de dominio completo y el número de puerto de un controlador de zonas de almacenamiento al que se pueda acceder desde XenMobile Server.
- **Conexión segura:** Si usa SSL para las conexiones con el controlador de zonas de almacenamiento, use el parámetro predeterminado “Sí”. Si no utiliza SSL para las conexiones, desactive este parámetro.
- **Nombre de usuario del administrador** y **Contraseña del administrador:** El nombre de usuario de la cuenta del administrador del servicio (en el formato dominio\admin) y la contraseña. También puede utilizar una cuenta de usuario con permisos de lectura y escritura en los controladores de zonas de almacenamiento.

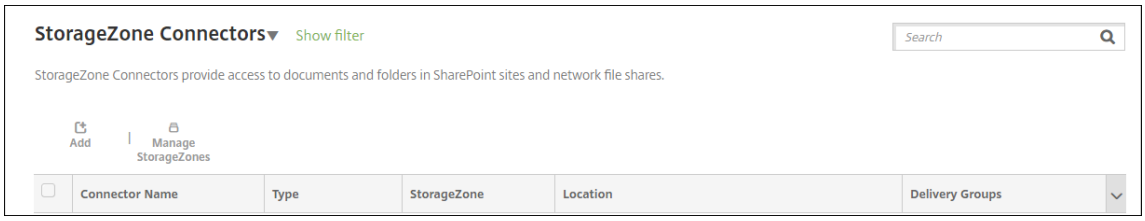
3. Haga clic en **Guardar**.
4. Para probar la conexión, compruebe que XenMobile Server puede establecer conexión con el nombre de dominio completo del controlador de zonas de almacenamiento en el puerto 443.
5. Para definir otra conexión del controlador de zonas de almacenamiento, haga clic en el botón **Agregar** en **Administrar StorageZones**.

   Para modificar o eliminar la información de una conexión del controlador de zonas de almacenamiento, seleccione el nombre de la conexión en **Administrar zonas de almacenamiento**.

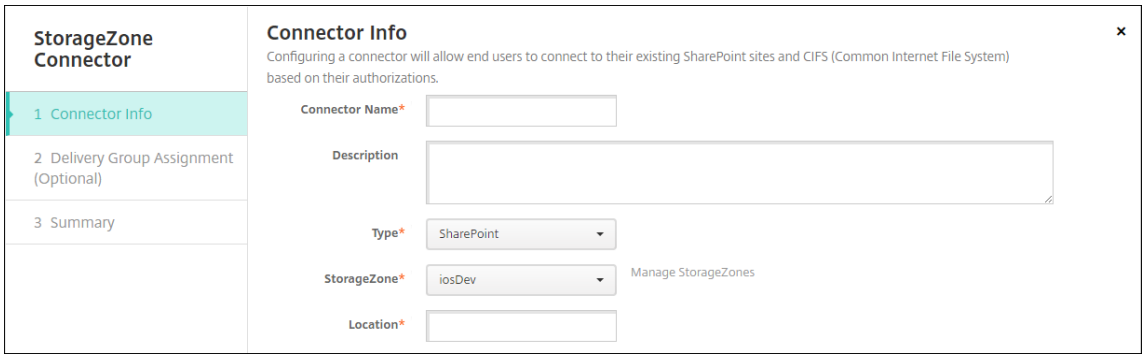
Haga clic en **Modificar** o **Eliminar**.

Agregar un conector de zonas de almacenamiento en XenMobile

1. Vaya a **Configurar > ShareFile** y, a continuación, haga clic en **Agregar**.

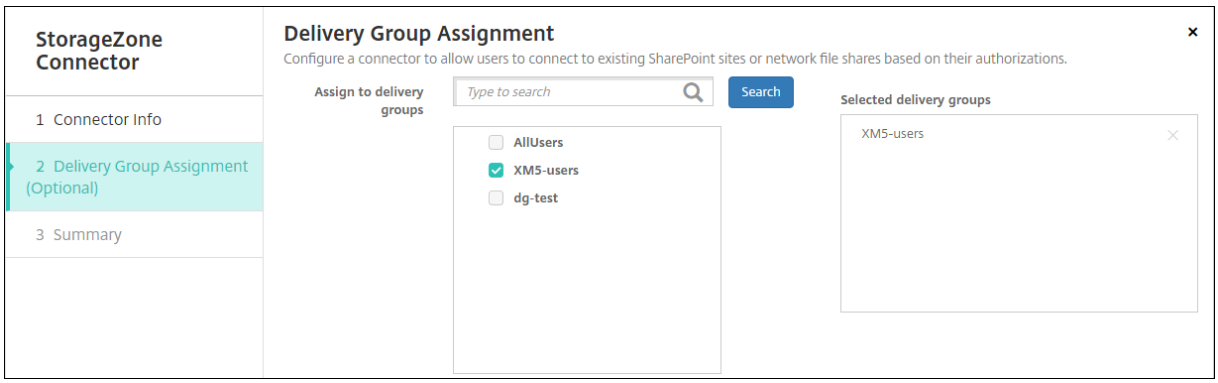


2. En la página **Información del conector**, configure los siguientes parámetros:



   - **Nombre de conector:** Un nombre que identifica el conector de zonas de almacenamiento en XenMobile.
   - **Descripción:** Notas opcionales sobre este conector.
   - **Tipo:** Elija **SharePoint** o **Red**.
   - **StorageZone:** Seleccione la zona de almacenamiento asociada al Connector. Si la zona de almacenamiento no aparece, haga clic en **Administrar StorageZones** para definir el controlador de zonas de almacenamiento.
   - **Ubicación:** Para SharePoint, especifique la URL del sitio en el nivel raíz de SharePoint, la colección del sitio o la biblioteca de documentos, en el formato `https://sharepoint.company.com`. Para un recurso compartido de red, especifique el nombre de dominio completo de la ruta Uniform Naming Convention (UNC) en el formato \\server\share.

3. En la página **Asignación de grupos de entrega**, puede asignar el conector a grupos de entrega. También puede asociar conectores a grupos de entrega desde **Configurar > Grupos de entrega**.



1. En la página **Resumen**, puede revisar las opciones que ha configurado. Para ajustar la configuración, haga clic en **Atrás**.
2. Haga clic en **Guardar** para guardar el conector.
3. Pruebe el conector:

    a) Cuando empaquete clientes de Citrix Files, lleve a cabo lo siguiente:

    - Establezca la directiva “Acceso de red” en **Túnel a la red interna**.

    En este modo de funcionamiento, el framework de XenMobile MDX intercepta todo el tráfico de red desde el cliente de Citrix Files. El tráfico se redirige a través de Citrix Gateway con una micro VPN específica de la aplicación.

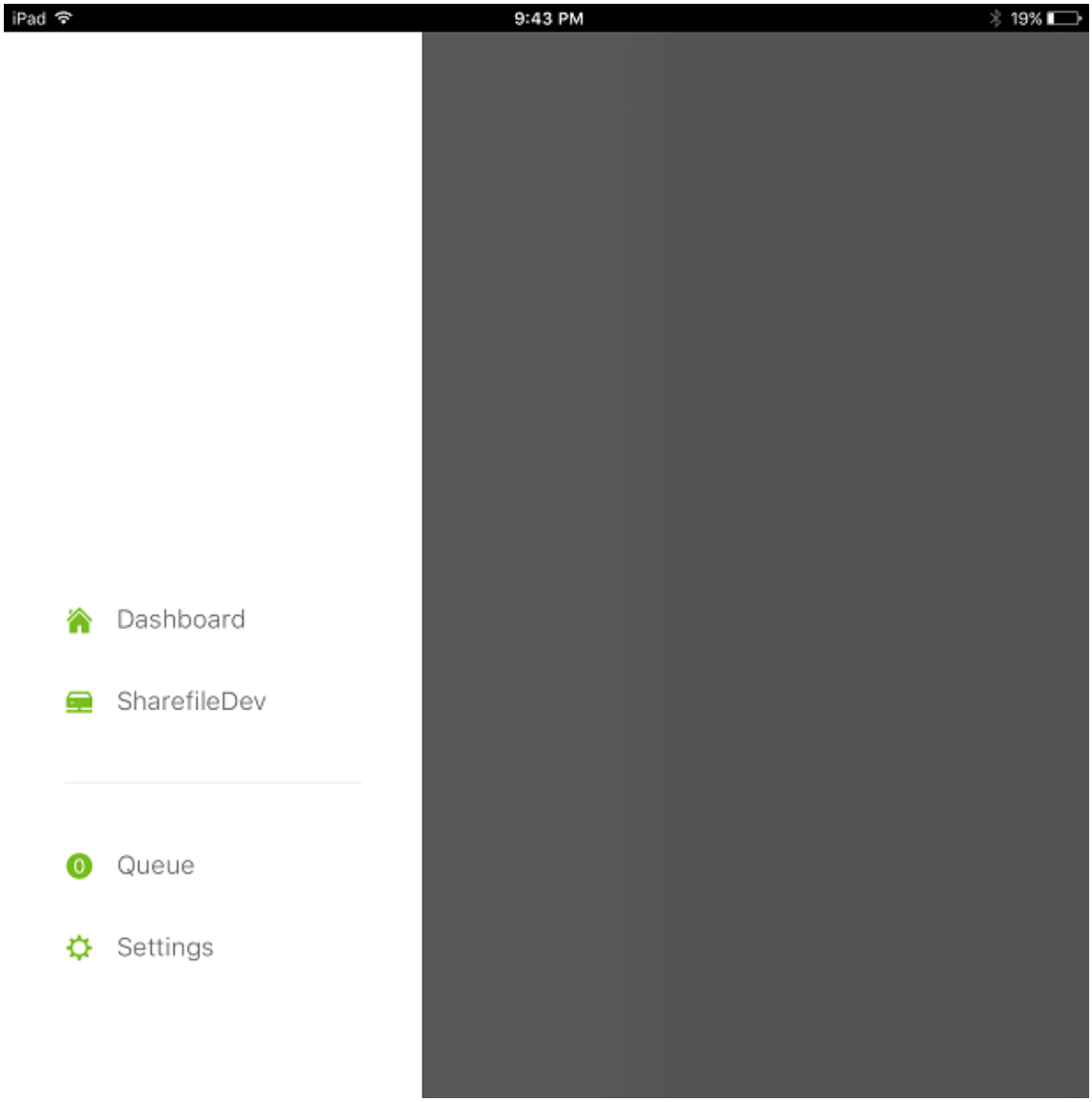
    - Establezca la directiva “Modo preferido de VPN” en **SSO web en túnel**.

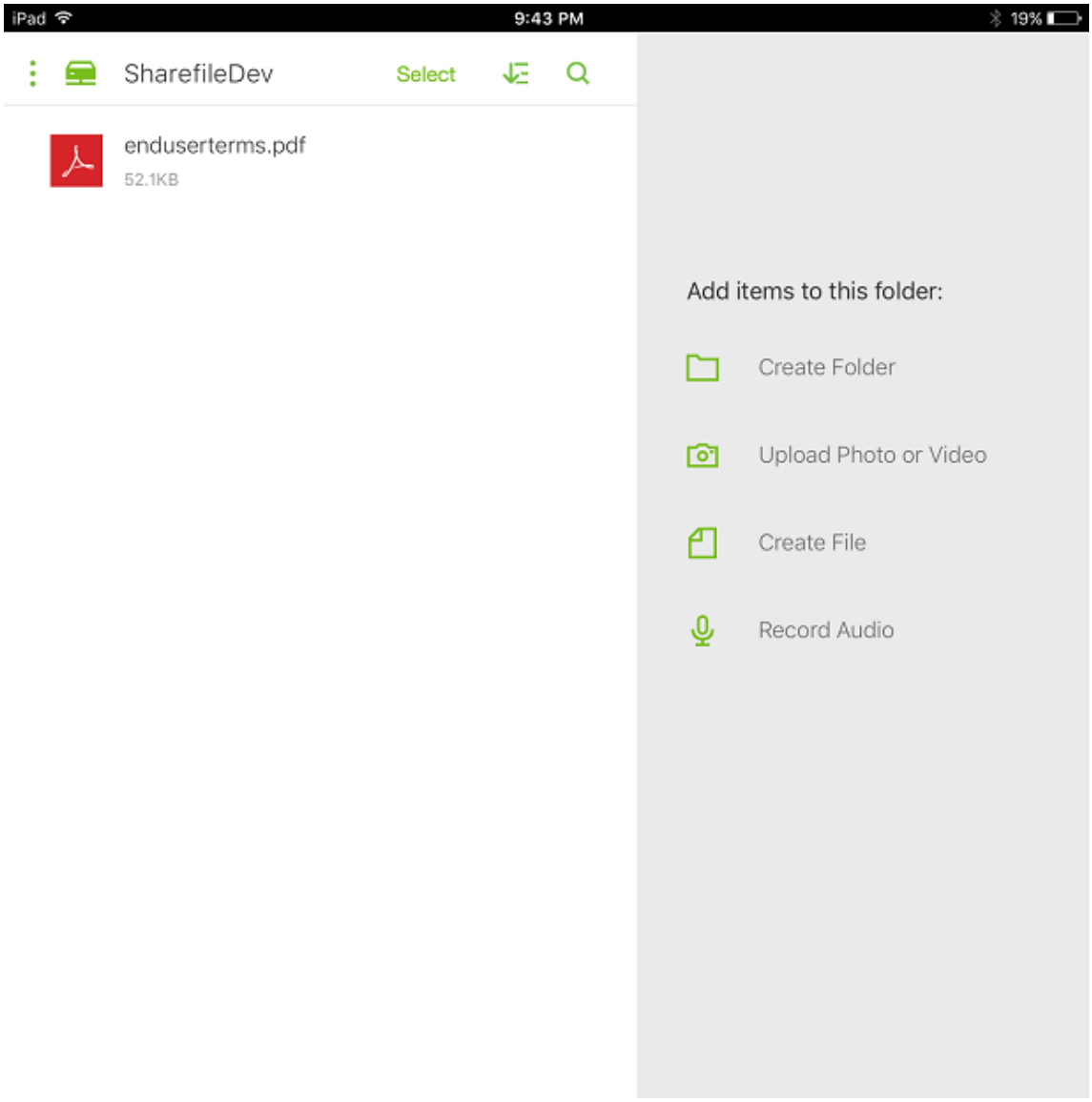
    En este modo de canalización por túnel, el framework MDX finaliza el tráfico SSL/HTTP desde una aplicación MDX. A continuación, MDX inicia conexiones nuevas con conexiones internas en nombre del usuario. Esta configuración de directiva permite que el marco de MDX detecte y responda a los desafíos de autenticación emitidos por servidores web.

    b) Agregue los clientes de Citrix Files a XenMobile. Para obtener información detallada, consulte Integrar y entregar clientes de Citrix Files para Endpoint Management.

    c) Desde un dispositivo admitido, compruebe el inicio Single Sign-On en Citrix Files y los conectores.

    En los siguientes ejemplos, SharefileDev es el nombre de un conector.

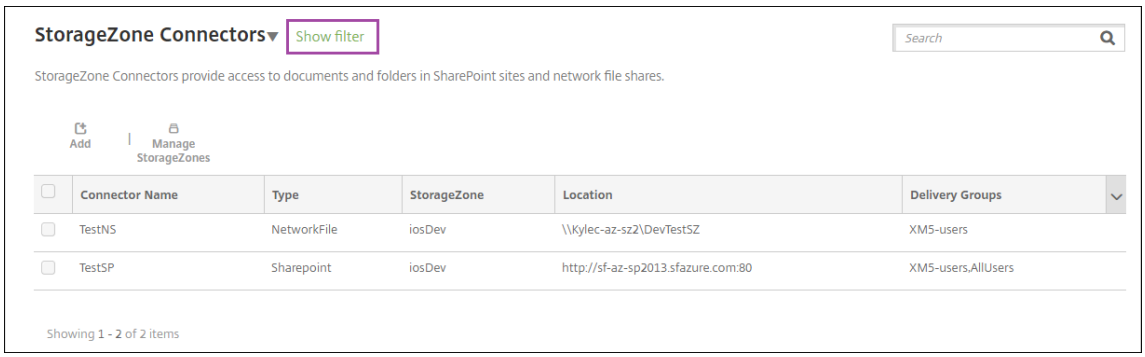




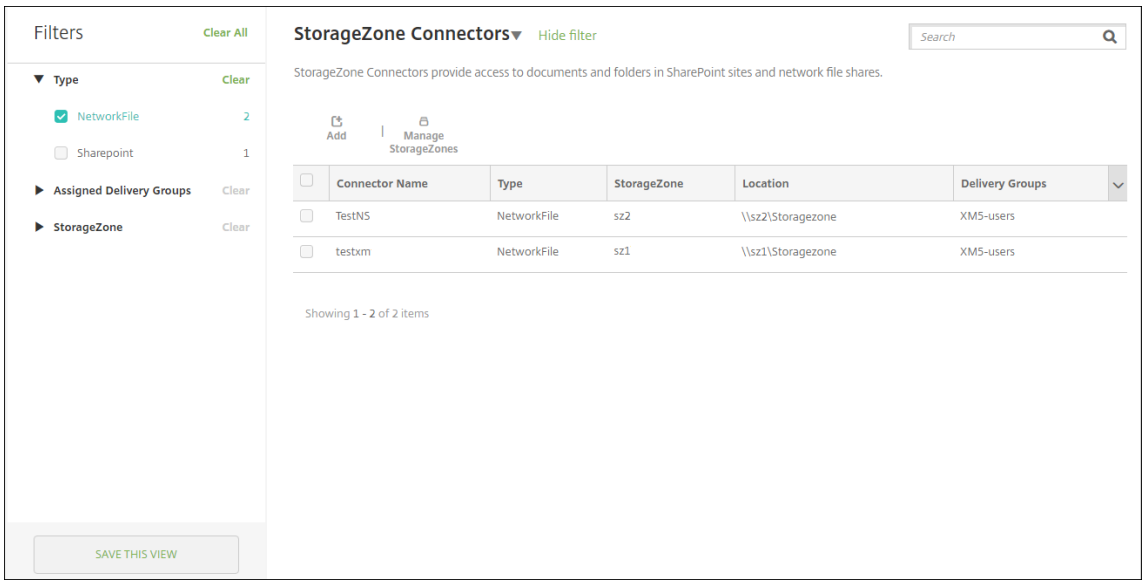
Filtrar la lista de conectores de zonas de almacenamiento

Puede filtrar la lista de conectores de zonas de almacenamiento por tipo de Connector, grupos de entrega asignados y zona de almacenamiento.

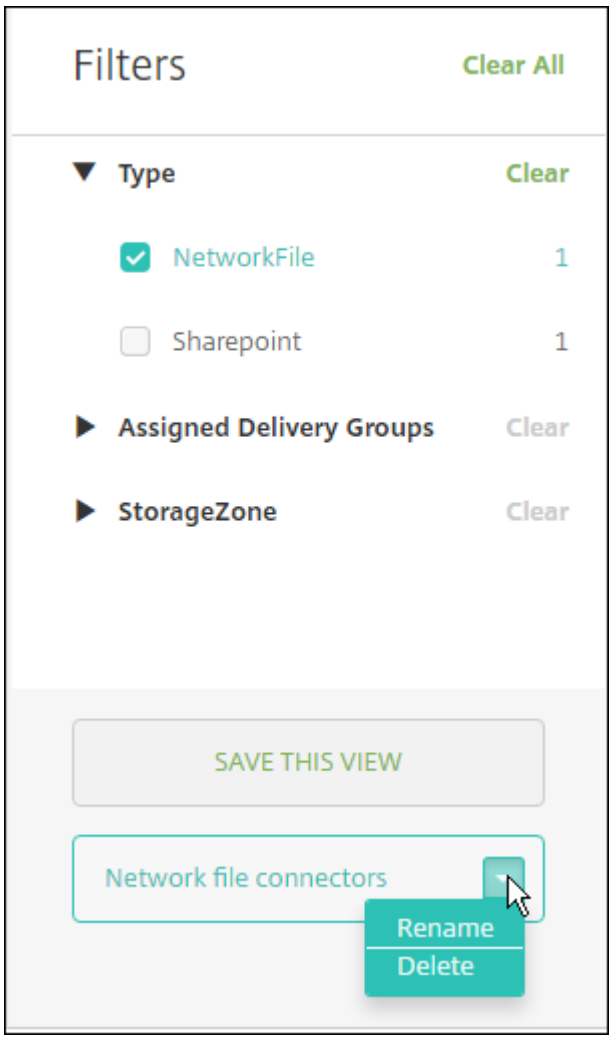
1. Vaya a **Configurar > ShareFile** y, a continuación, haga clic en **Mostrar filtro**.



2. Expanda los encabezados de los filtros para las selecciones necesarias. Para guardar un filtro, haga clic en **Guardar esta vista**, escriba el nombre del filtro y haga clic en **Guardar**.



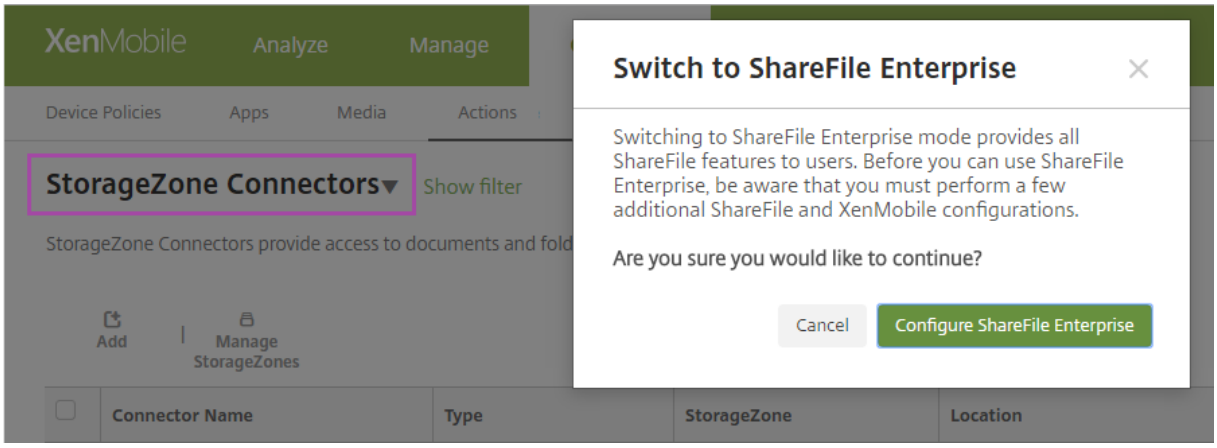
3. Para cambiar el nombre de un filtro o eliminarlo, haga clic en el icono de flecha situado junto al nombre del filtro.



Cambiar a Citrix Files

Después de integrar conectores de zonas de almacenamiento en XenMobile, puede cambiar al conjunto completo de funcionalidades de Enterprise. El conjunto de funcionalidades de Citrix Files requiere XenMobile Enterprise Edition. XenMobile conserva los parámetros existentes de integración de conectores de zonas de almacenamiento.

Vaya a **Configurar > ShareFile**, haga clic en el menú desplegable **Conectores StorageZone** y, a continuación, haga clic en **Configurar ShareFile Enterprise**.



Para obtener información sobre cómo configurar Citrix Files, consulte SAML para Single Sign-On en Citrix Files.

SmartAccess para aplicaciones HDX

January 4, 2022

Esta funcionalidad permite controlar el acceso a aplicaciones HDX en función de las propiedades del dispositivo, las propiedades de un usuario o las aplicaciones instaladas en un dispositivo. Puede usar esta función mediante acciones automatizadas que marcan el dispositivo como no conforme para denegarle el acceso a las aplicaciones. Las aplicaciones HDX utilizadas con esta función se configuran en Virtual Apps and Desktops mediante una directiva de SmartAccess que deniega el acceso a los dispositivos no conformes. XenMobile comunica el estado del dispositivo a StoreFront mediante una etiqueta firmada y cifrada. A continuación, StoreFront permite o deniega el acceso en función de la directiva del control de acceso de la aplicación.

Para usar esta función, su implementación requiere:

- Virtual Apps and Desktops 7.6
- StoreFront 3.7 o 3.8
- XenMobile Server configurado para agregar aplicaciones HDX desde un servidor de StoreFront
- XenMobile Server configurado con un certificado SAML que se utilizará para firmar y cifrar las etiquetas. El mismo certificado sin clave privada se carga en el servidor StoreFront.

Para empezar a usar esta funcionalidad:

- Configure el certificado de XenMobile Server para el almacén de StoreFront
- Configure al menos un grupo de entrega de Virtual Apps and Desktops con la directiva de SmartAccess requerida
- Establezca la acción automatizada en XenMobile

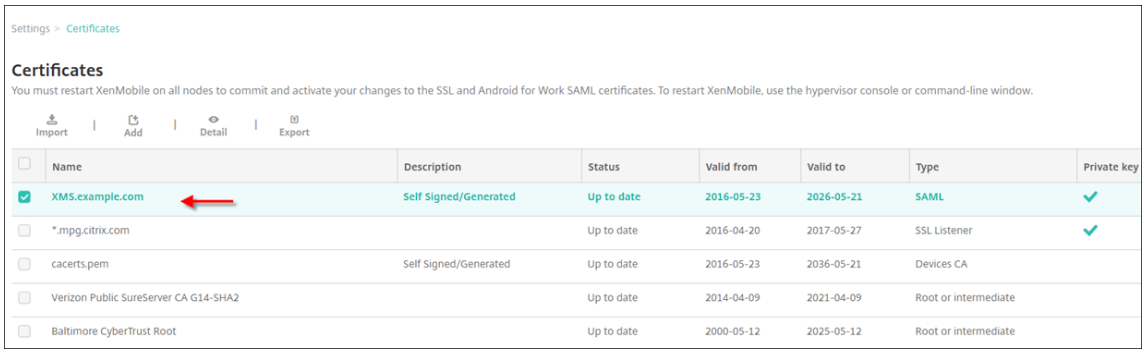
Exportar, configurar el certificado de XenMobile Server y cargarlo en el almacén de StoreFront

SmartAccess usa etiquetas cifradas y firmadas para la comunicación entre los servidores de XenMobile y StoreFront. Para habilitar esta comunicación, agregue el certificado de XenMobile Server al almacén de StoreFront.

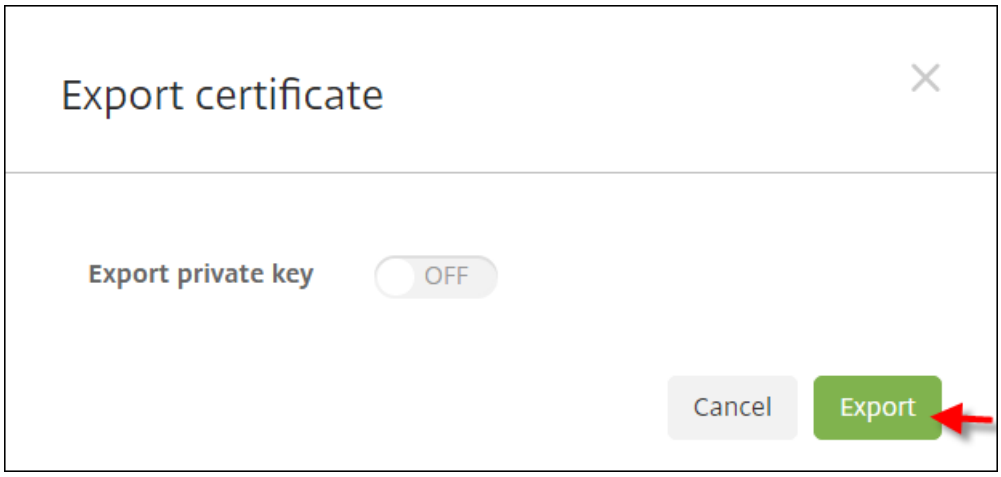
Para obtener más información sobre la integración de StoreFront y XenMobile cuando XenMobile tiende habilitada la autenticación basada en certificados y dominios, consulte los artículos de Knowledge Center.

Exportar el certificado SAML desde XenMobile Server

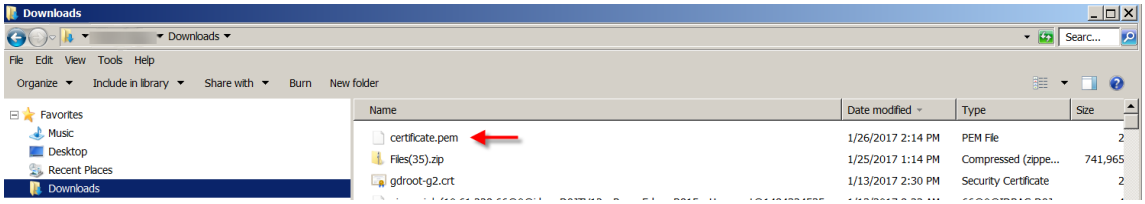
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**. Haga clic en **Certificados**.
2. Busque el certificado SAML para XenMobile Server.



3. Compruebe que **Exportar clave privada** está establecido en **No**. Haga clic en **Exportar** para exportar el certificado al directorio de descargas.

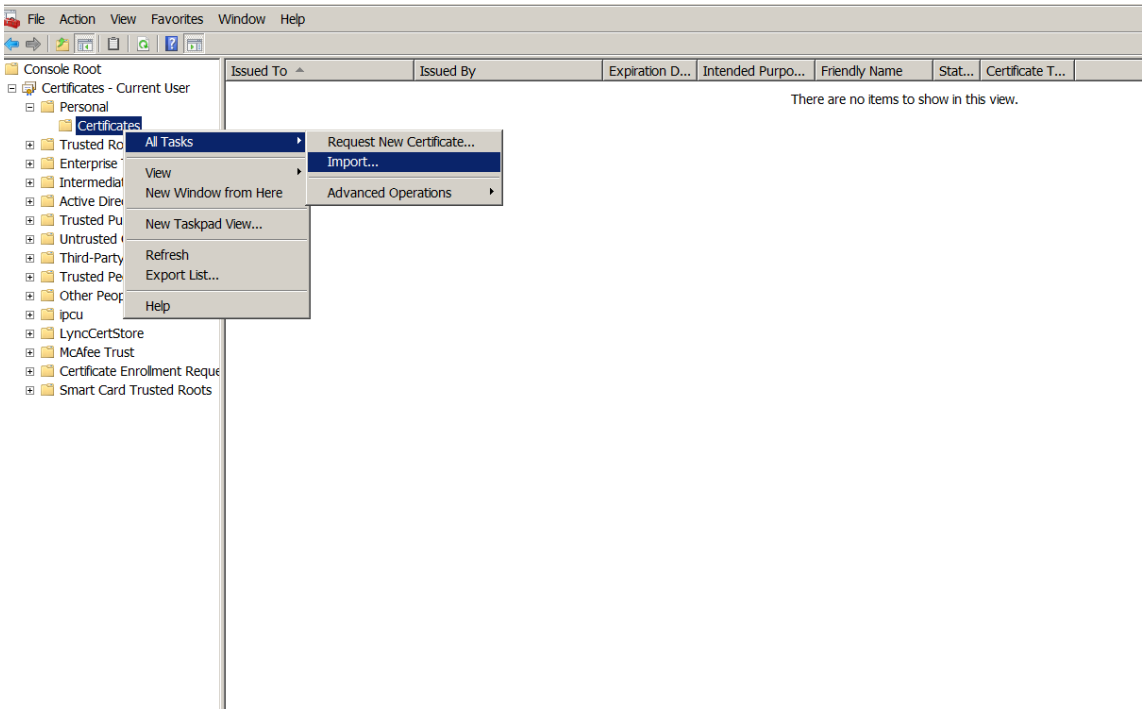


4. Busque el certificado en el directorio de descargas. El certificado raíz tiene el formato PEM.

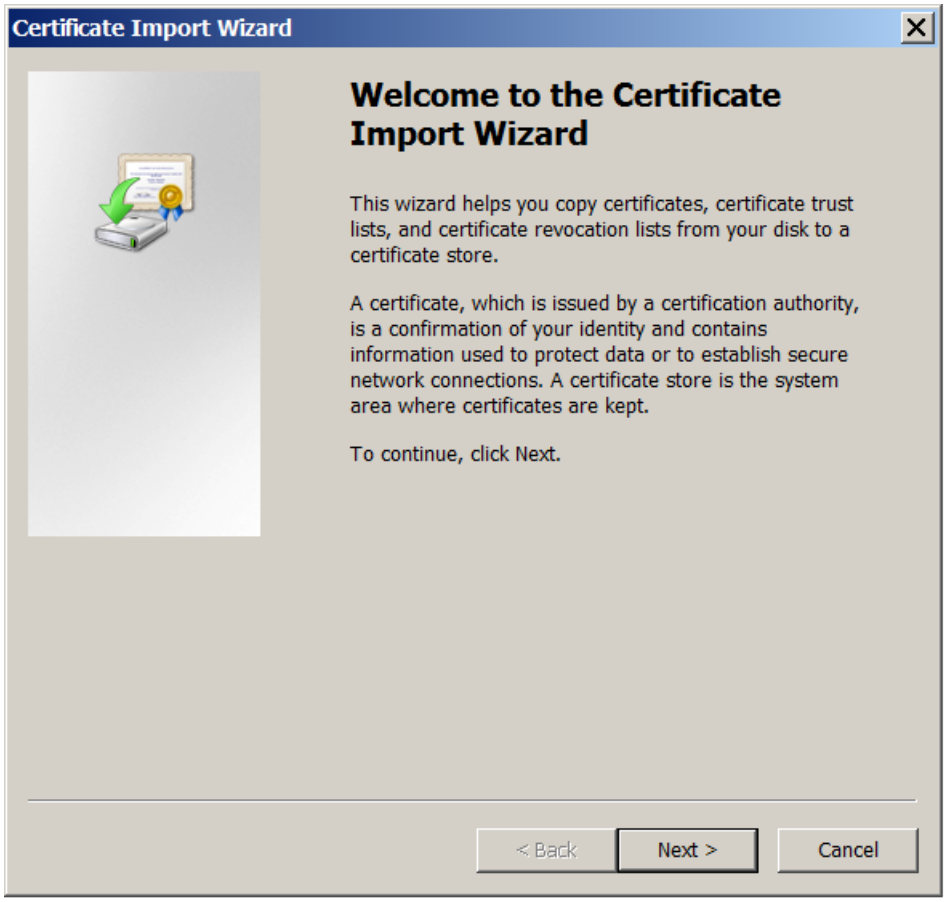


Convertir el certificado de PEM a CER

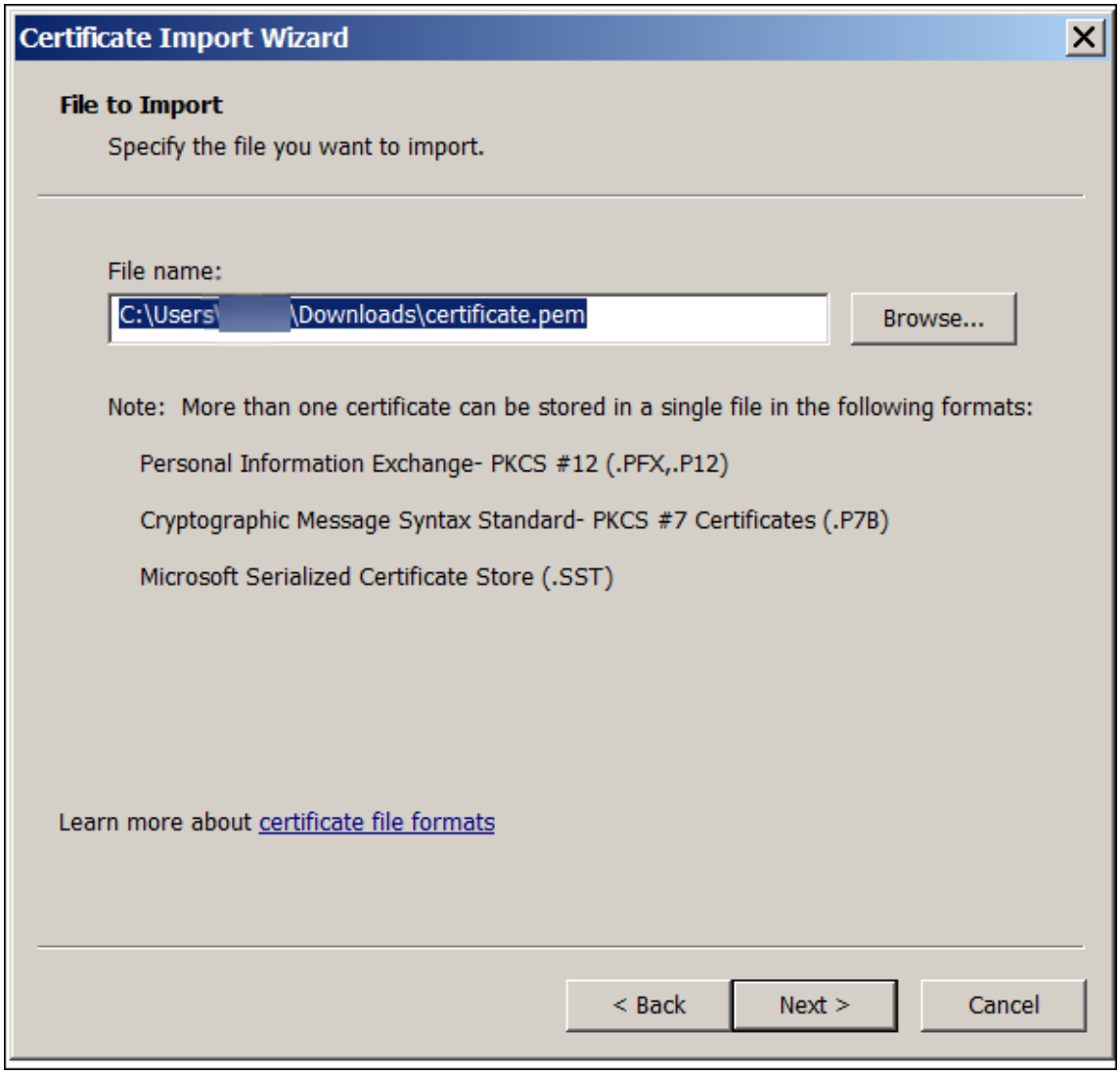
1. Abra Microsoft Management Console (MMC) y haga clic con el botón secundario en **Certificados > Todas las tareas > Importar**.



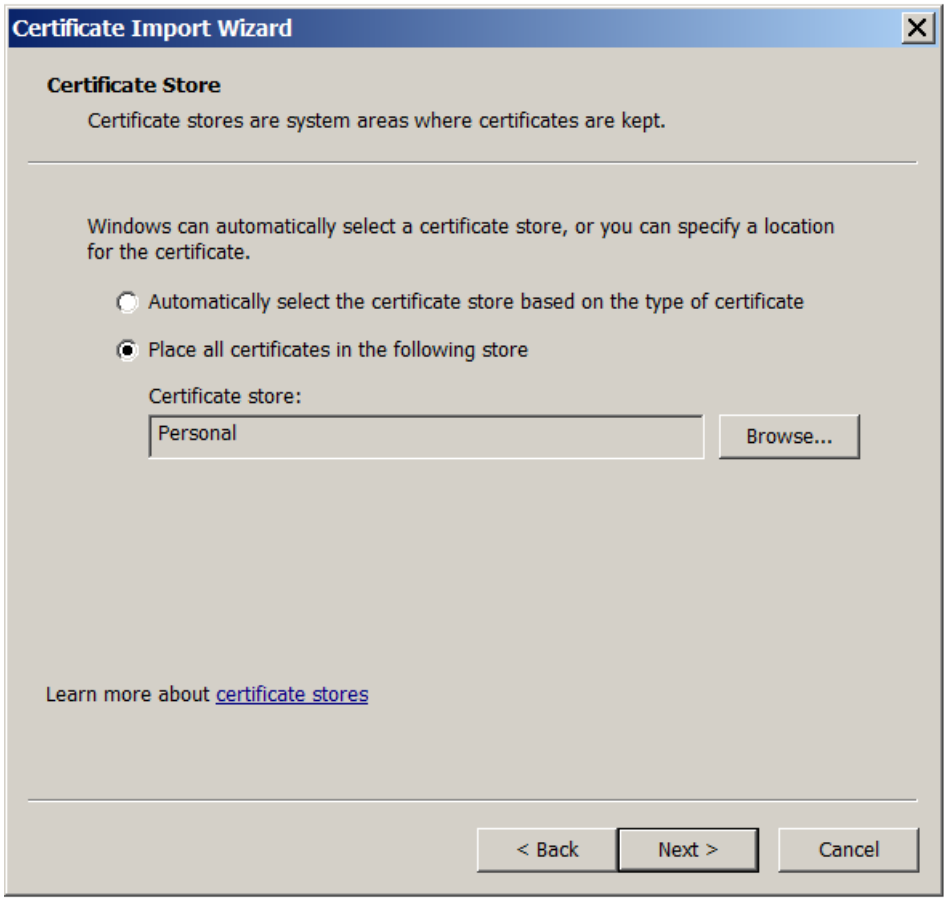
2. Cuando aparezca el asistente para la importación de certificados, haga clic en **Siguiente**.



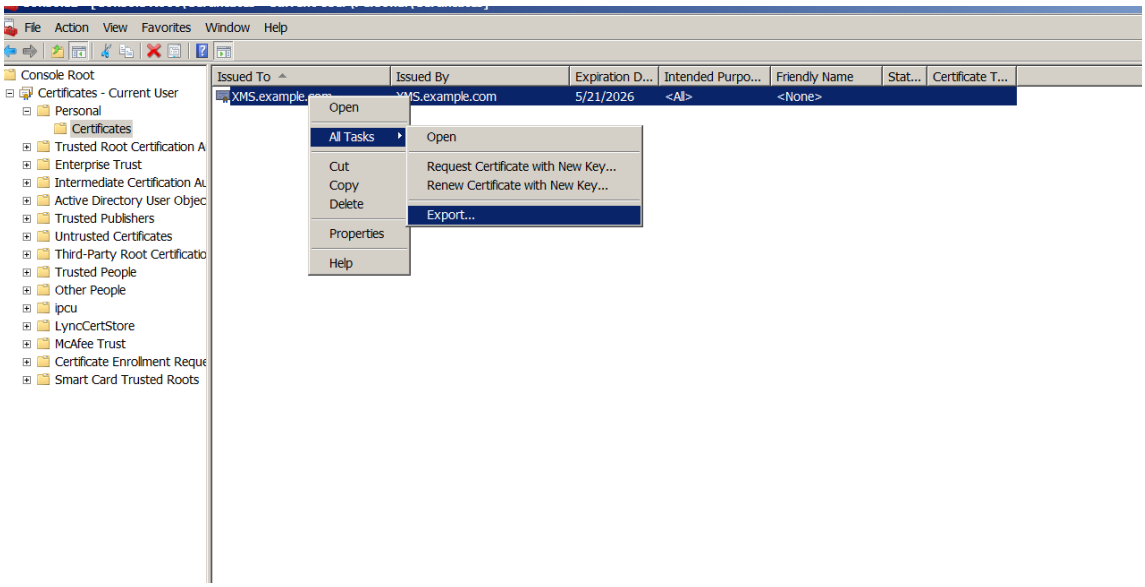
3. Vaya al certificado ubicado en el directorio de descargas.



4. Seleccione **Colocar todos los certificados en el siguiente almacén** y, a continuación, seleccione **Personal** como almacén de certificados. Haga clic en **Siguiente**.

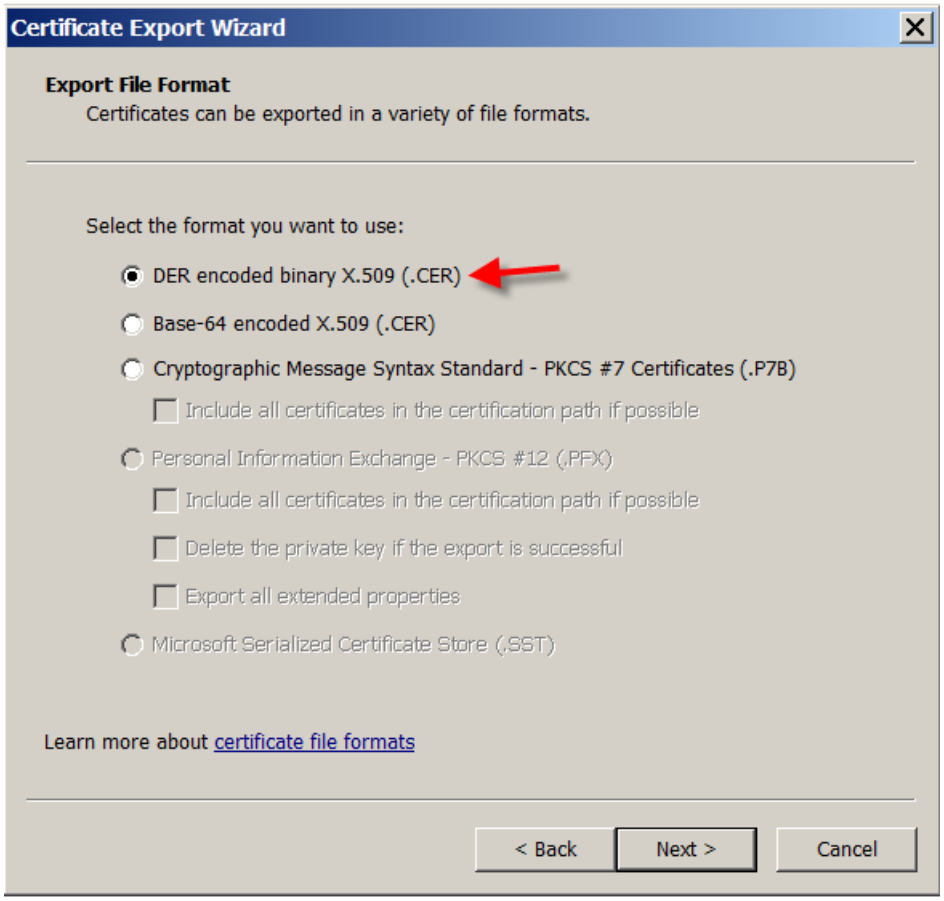


5. Revise los cambios y haga clic en **Finalizar**. Haga clic en **Aceptar** en la ventana de confirmación.
6. En la MMC, haga clic con el botón secundario en el certificado y seleccione **Todas las tareas > Exportar**.

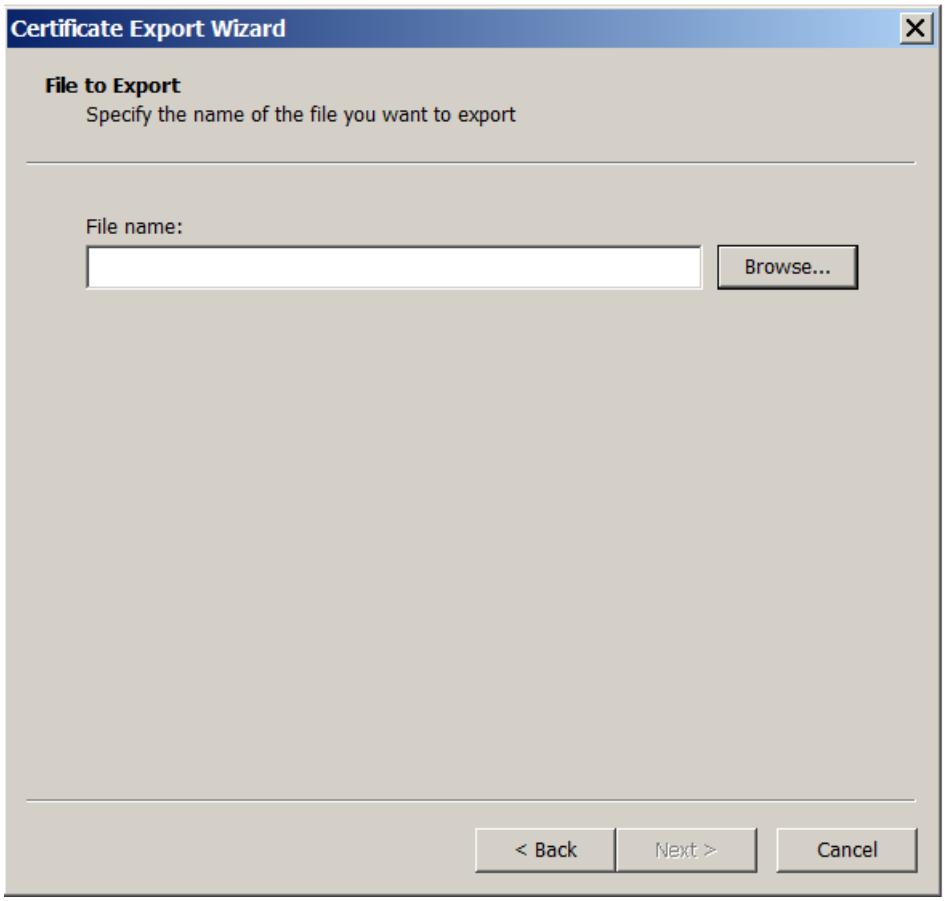


7. Cuando aparezca el asistente para la exportación de certificados, haga clic en **Siguiente**.

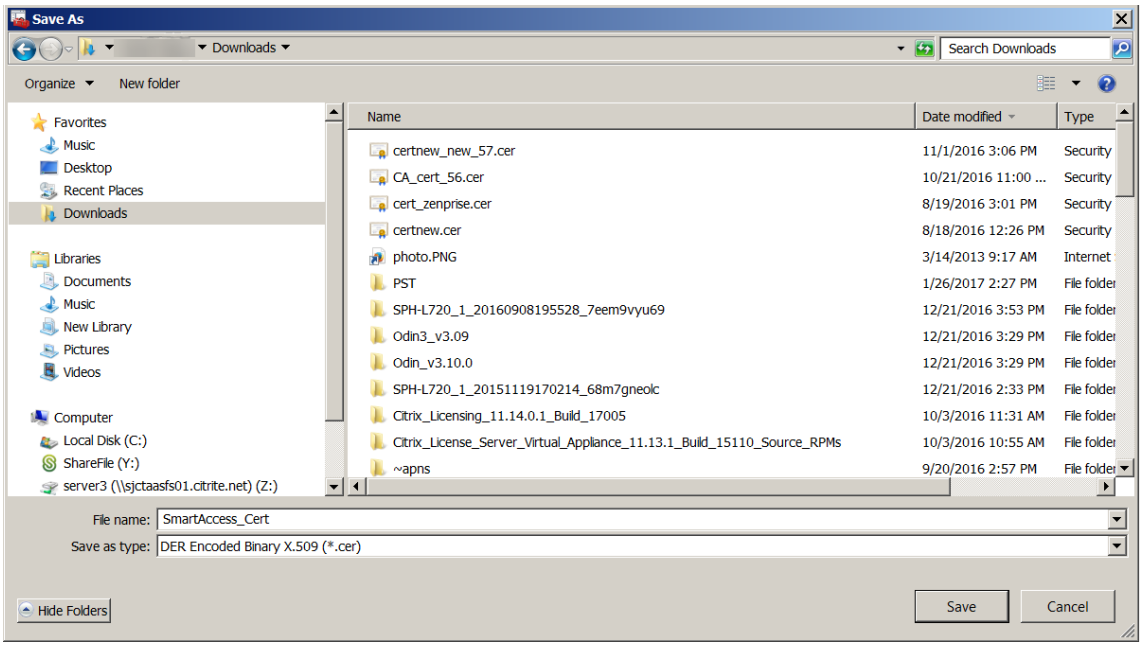
8. Seleccione el formato **DER binario codificado X.509 (.CER)**. Haga clic en **Siguiente**.



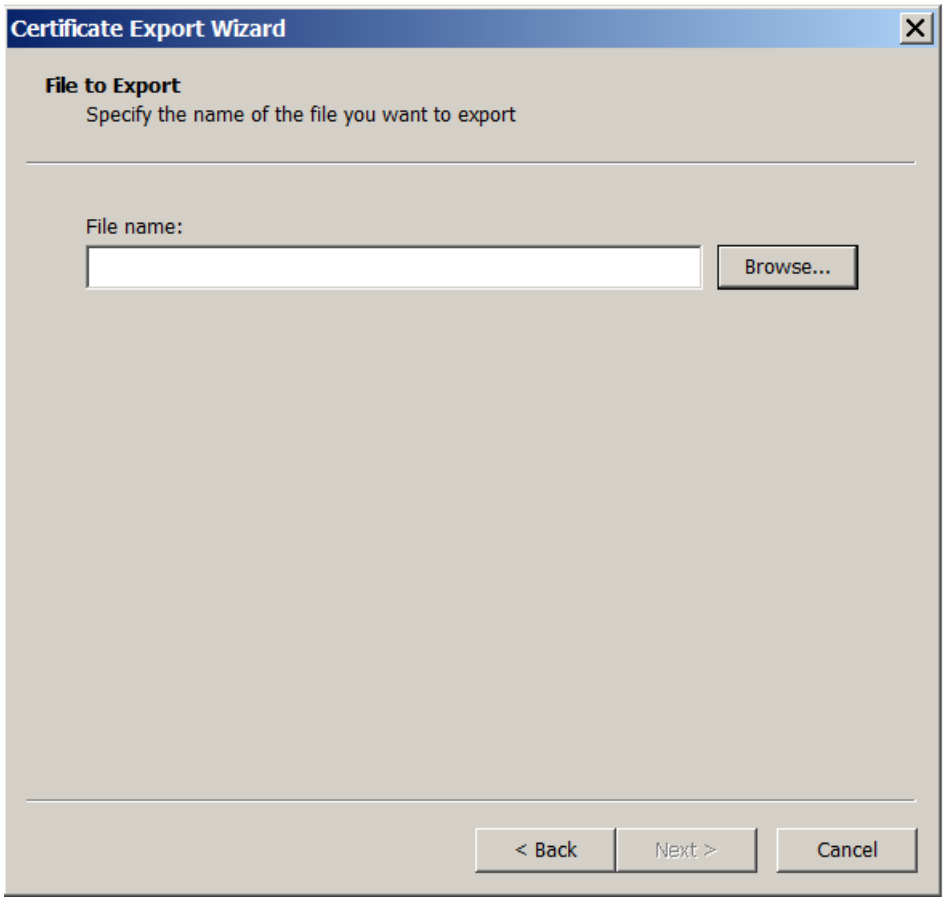
9. Vaya al certificado. Escriba un nombre para el certificado y haga clic en **Siguiente**.



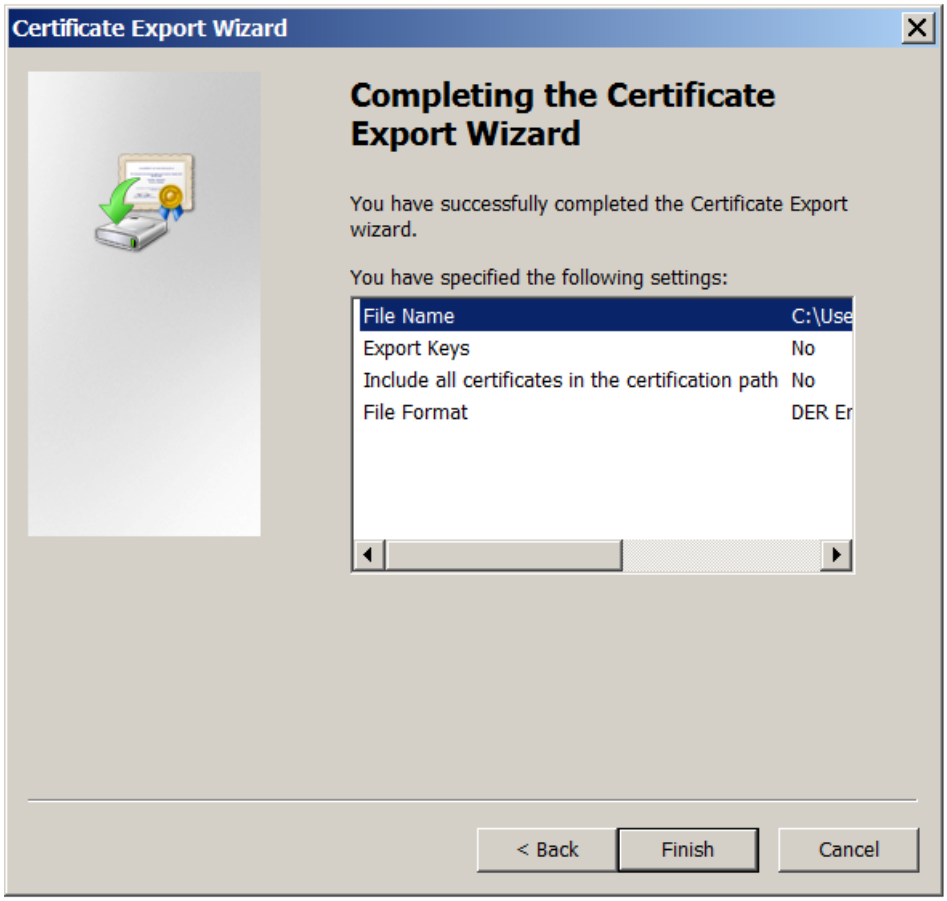
10. Guarde el certificado.



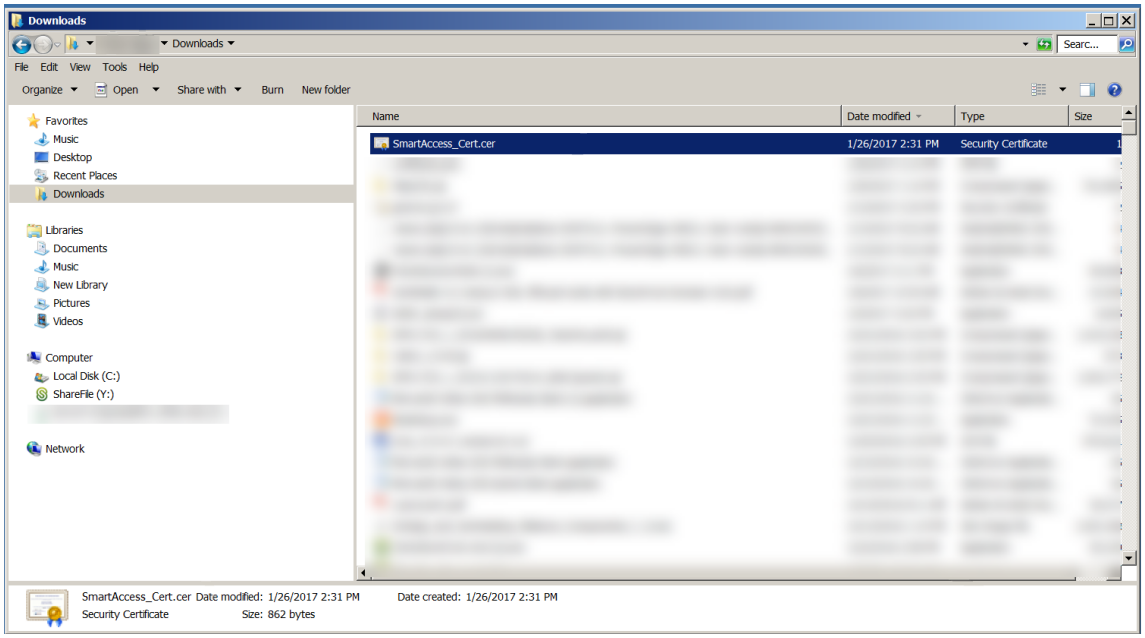
11. Vaya al certificado y haga clic en **Siguiente**.



12. Revise los cambios y haga clic en **Finalizar**. Haga clic en **Aceptar** en la ventana de confirmación.

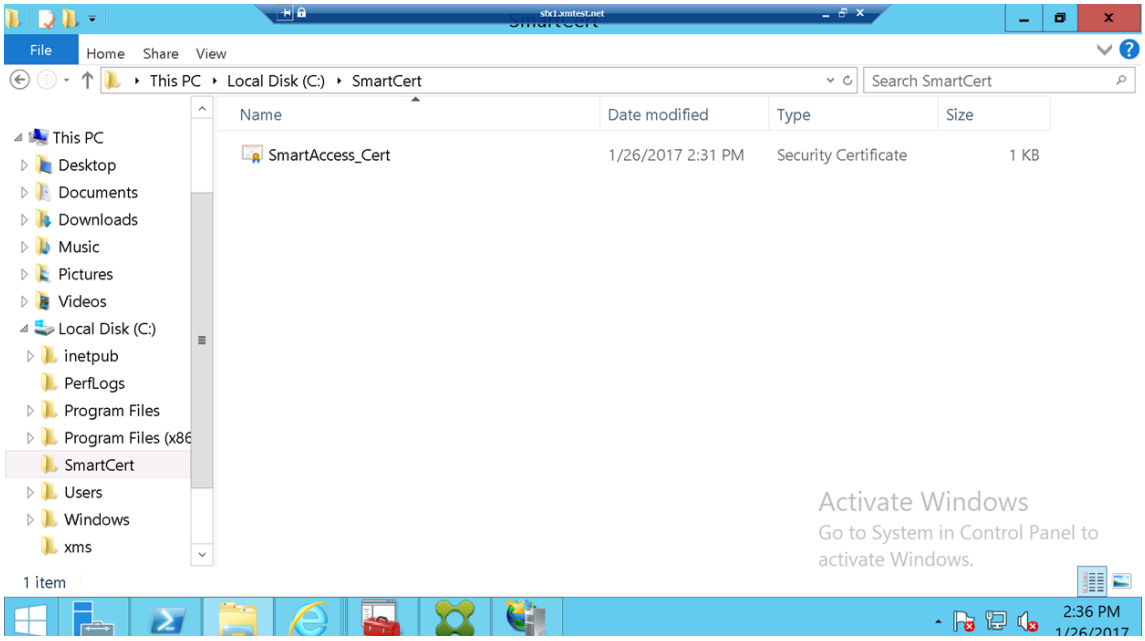


13. Busque el certificado en el directorio de descargas. Tenga en cuenta que el certificado está en formato CER.



Copiar el certificado al servidor de StoreFront

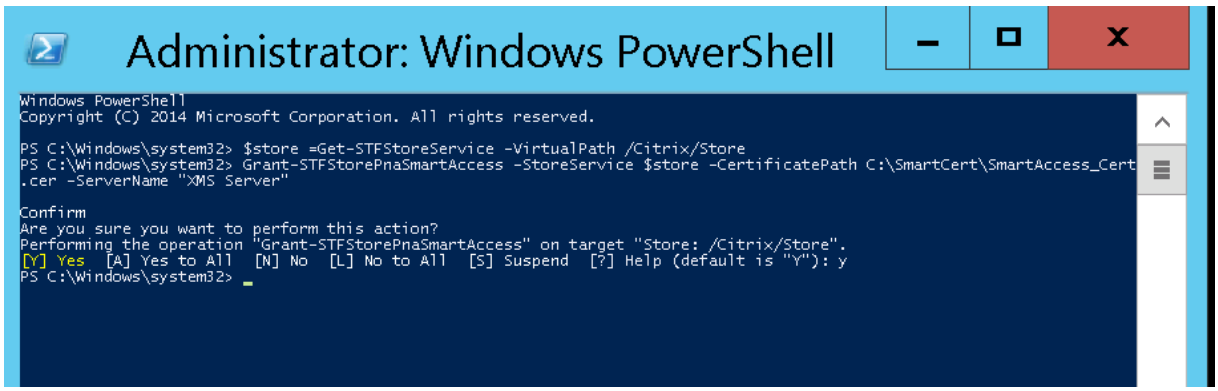
1. En el servidor de StoreFront, cree una carpeta llamada **SmartCert**.
2. Copie el certificado a la carpeta **SmartCert**.



Configurar el certificado en el almacén de StoreFront

En el servidor StoreFront, ejecute el siguiente comando de PowerShell para configurar el certificado de XenMobile Server convertido que se encuentra en el almacén:

```
1    Grant-STFStorePnaSmartAccess -StoreService $store -
        CertificatePath "C:\xms\xms.cer" -ServerName "XMS server"
2  <!--NeedCopy-->
```



Si ya hay certificados existentes en el almacén de StoreFront, ejecute este comando de PowerShell para revocarlos:


```
    Revoke-STFStorePnaSmartAccess  -StoreService $store  -All
<!--NeedCopy-->
```

También puede ejecutar cualquiera de estos comandos de PowerShell en el servidor de StoreFront para revocar los certificados existentes en el almacén de StoreFront:

- Revocar por nombre:

```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -ServerName  "
       My XM Server"
<!--NeedCopy-->
```

- Revocar por huella digital:

```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -
       CertificateThumbprint  "ReplaceWithThumbprint"
<!--NeedCopy-->
```

- Revocar por objeto de servidor:

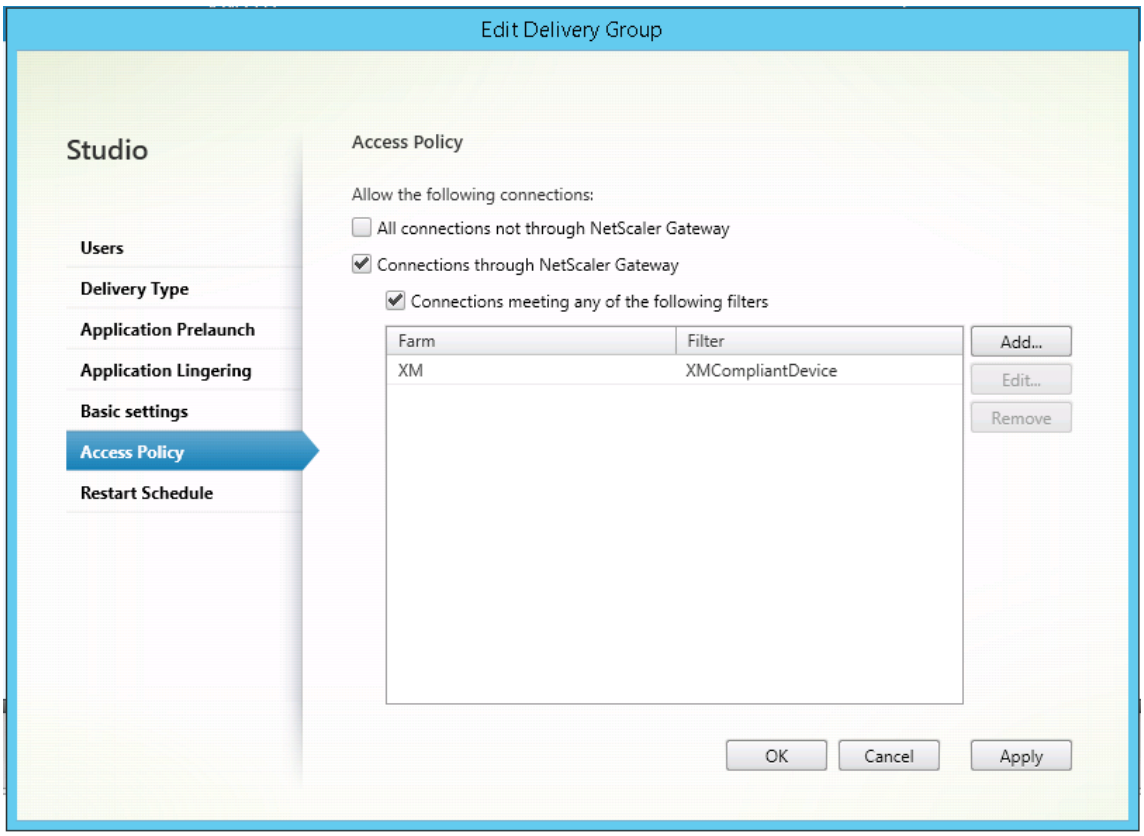
```
    $store = Get-STFStoreService  -VirtualPath /Citrix/Store

    $access = Get-STFStorePnaSmartAccess  -StoreService $store

    Revoke-STFStorePnaSmartAccess  -StoreService $store  -SmartAccess
       $access.AccessConditionsTrusts[0]
<!--NeedCopy-->
```

Configurar la directiva de SmartAccess para Virtual Apps and Desktops

Para agregar la directiva de SmartAccess requerida al grupo que entrega la aplicación HDX:

1. En el servidor de Virtual Apps and Desktops, abra Citrix Studio.
2. Seleccione **Grupos de entrega** en el panel de navegación de Studio.

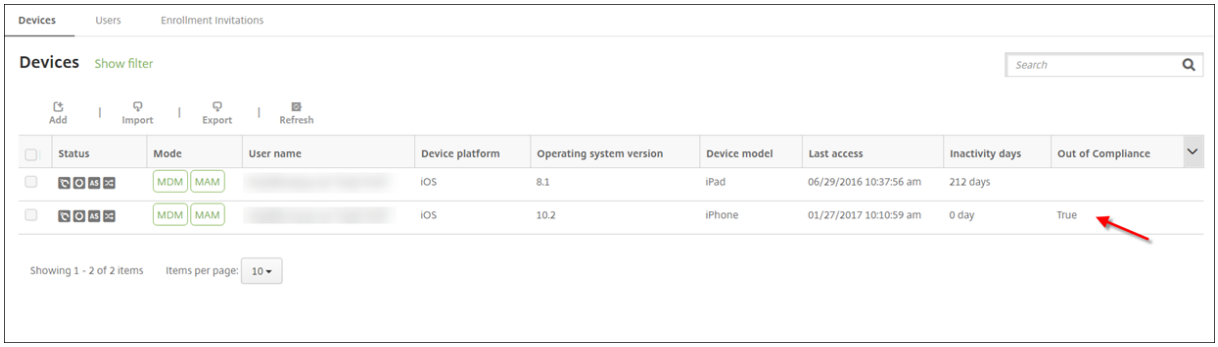
3. Seleccione el grupo que entrega la aplicación o aplicaciones a las que quiere controlar el acceso. Seleccione **Modificar grupo de entrega** en el panel **Acciones**.
4. En la página **Directiva de acceso**, seleccione **Conexiones a través de NetScaler Gateway** y **Conexiones que cumplan cualquiera de estos filtros**.
5. Haga clic en **Agregar**.
6. Agregue una directiva de acceso donde **Comunidad** es **XM** y **Filtro** es **XMCompliantDevice**.



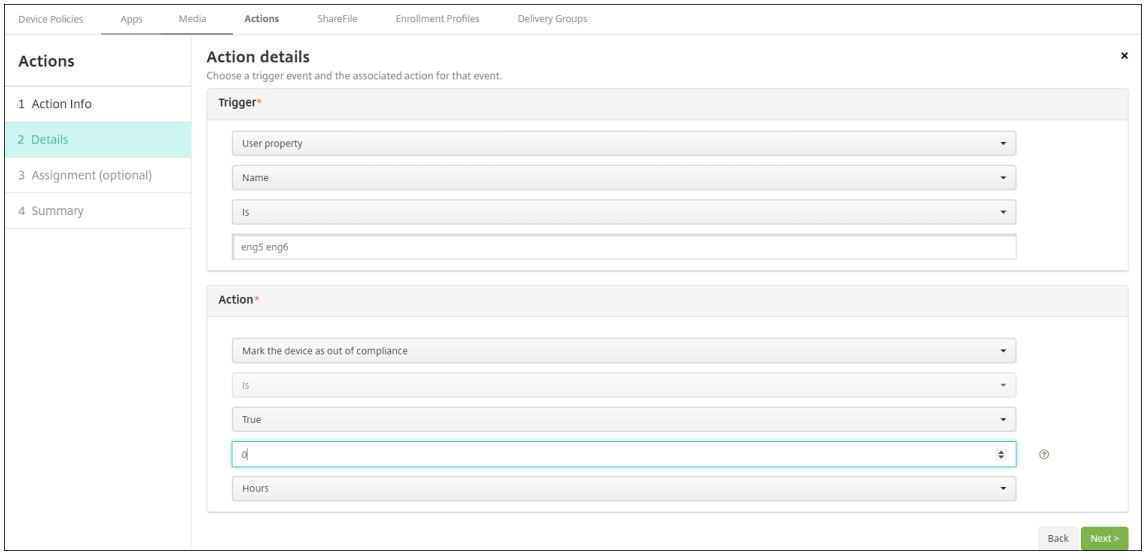
7. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Establecer acciones automatizadas en XenMobile

La directiva de SmartAccess que se estableció en el grupo de entrega para una aplicación HDX deniega el acceso a un dispositivo cuando el dispositivo no es conforme. Puede utilizar acciones automatizadas para marcar el dispositivo como no conforme.



1. En la consola de XenMobile, haga clic en **Configurar > Acciones**. Aparecerá la página **Acciones**.
2. Haga clic en **Agregar** para agregar una acción. Aparecerá la página **Información de la acción**.
3. En la página **Información de la acción**, escriba un nombre y una descripción para la acción.
4. Haga clic en **Siguiente**. Aparecerá la página **Detalles de la acción**. En el siguiente ejemplo, se crea un desencadenador que marca inmediatamente los dispositivos como no conformes si tienen el nombre de la propiedad de usuario **eng5** o **eng6**.



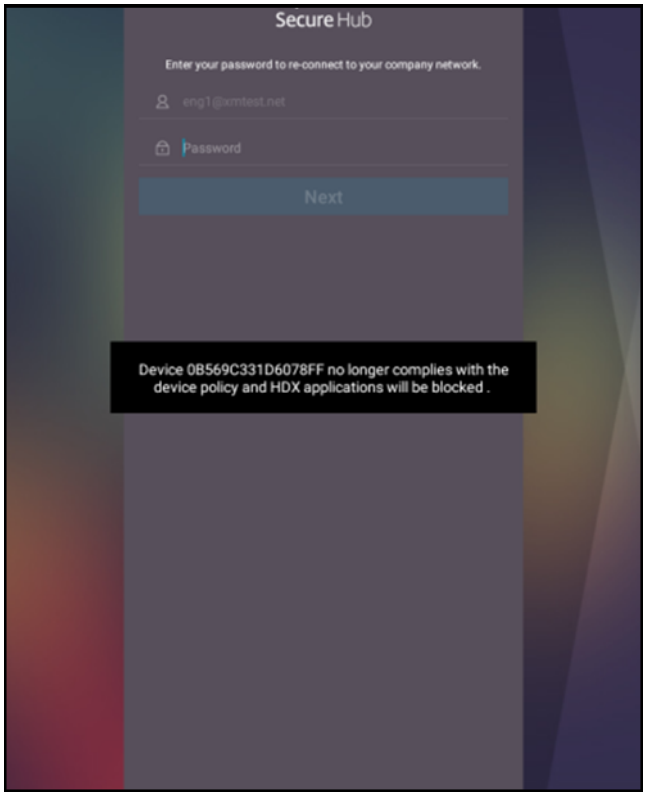
5. En la lista **Desencadenador**, elija **Propiedad de dispositivo**, **Propiedad de usuario** o **Nombre de la aplicación instalada**. SmartAccess no admite desencadenadores de eventos.
6. En la lista **Acción**:
   - Elija **Marcar dispositivo como No conforme**.
   - Elija **Es**.
   - Elija **Verdadero**.
   - Para que el dispositivo se marque como no conforme en cuanto se cumpla la condición del desencadenador, establezca el marco de tiempo en **0**.
7. Elija el grupo o grupos de entrega de XenMobile a los que aplicar esta acción.

8. Revise el resumen de la acción.
9. Haga clic en **Siguiente** y, a continuación, seleccione **Guardar**.

Cuando el dispositivo se marca como no conforme, las aplicaciones HDX ya no aparecen en el almacén Secure Hub. El usuario ya no está suscrito a las aplicaciones. No se envía ninguna notificación al dispositivo y nada en el almacén Secure Hub indica que las aplicaciones HDX estaban disponibles anteriormente.

Si quiere que se notifique a los usuarios cuando un dispositivo se marque como no conforme, cree una notificación y luego cree una acción automatizada para enviar esa notificación.

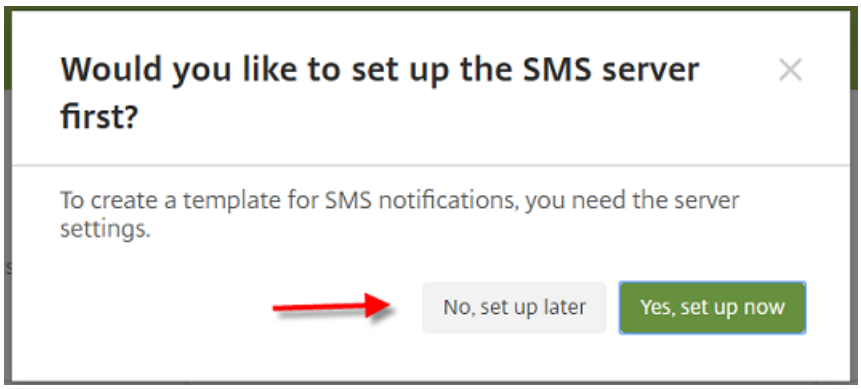
En este ejemplo se crea y se envía esta notificación cuando un dispositivo se marca como no conforme: "El número de serie o el número de teléfono del dispositivo ya no cumple la directiva de dispositivo y las aplicaciones HDX se bloquearán".



Crear la notificación que ven los usuarios cuando un dispositivo se marca como no conforme

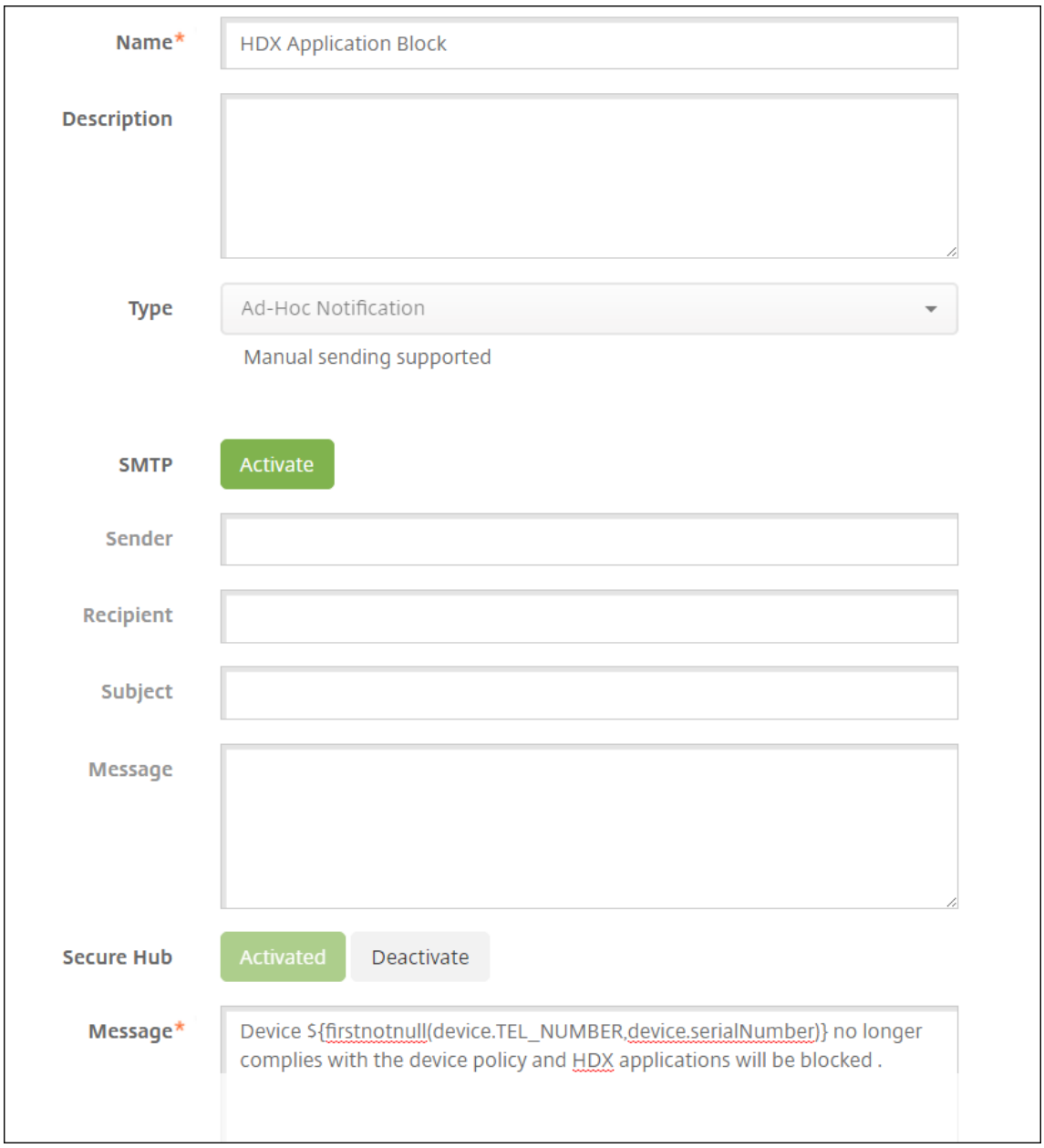
1. En la consola de XenMobile, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Parámetros**.
2. Haga clic en **Plantillas de notificaciones**. Aparecerá la página **Plantillas de notificaciones**.
3. Haga clic en **Agregar** para agregar una nueva plantilla de notificaciones en la página **Plantillas de notificaciones**.

4. Cuando se le solicite configurar primero el servidor SMS, haga clic en **No, lo configuraré más tarde**.



5. Configure estos parámetros:

   - **Nombre:** Bloqueo de aplicaciones HDX
   - **Descripción:** Notificación del agente cuando el dispositivo no es conforme
   - **Tipo:** Notificación ad hoc
   - **Secure Hub:** Activado
   - **Mensaje:** El dispositivo ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} ya no cumple la directiva de dispositivo y las aplicaciones HDX se bloquearán.



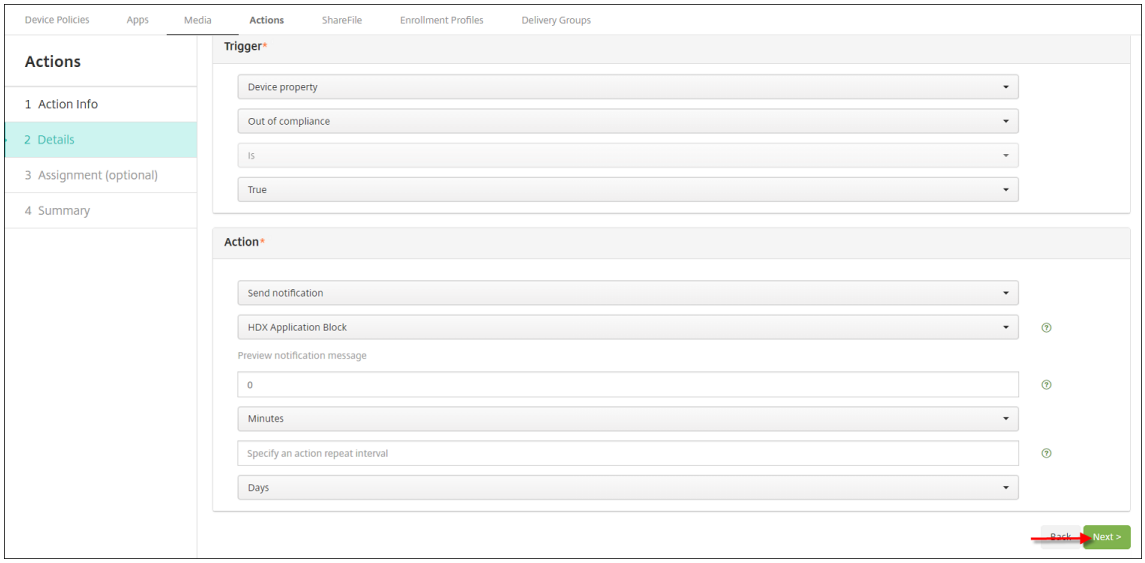
6. Haga clic en **Guardar**.

Crear la acción que envía la notificación cuando un dispositivo se marca como no conforme

1. En la consola de XenMobile, haga clic en **Configurar > Acciones**. Aparecerá la página **Acciones**.
2. Haga clic en **Agregar** para agregar una acción. Aparecerá la página **Información de la acción**.
3. En la página **Información de la acción**, escriba un nombre y una descripción para la acción:
   - **Nombre:** Notificación de HDX bloqueado

- **Descripción:** Notificación de HDX bloqueado porque el dispositivo no es conforme

4. Haga clic en **Siguiente**. Aparecerá la página **Detalles de la acción**.
5. En la lista **Desencadenador**:
   - Elija **Propiedad de dispositivo**.
   - Elija **No conforme**.
   - Elija **Es**.
   - Elija **Verdadero**.



6. En la lista **Acción**, especifique las acciones que se producen cuando se cumple el desencadenador:
   - Elija **Enviar notificación**.
   - Elija **Bloqueo de aplicaciones HDX, la notificación que ha creado**.
   - Elija **0**. Si este valor es 0, la notificación se enviará tan pronto como se cumpla la condición del desencadenador.
7. Elija el grupo o grupos de entrega de XenMobile a los que aplicar esta acción. En este ejemplo, se ha elegido **AllUsers**.
8. Revise el resumen de la acción.
9. Haga clic en **Siguiente** y, a continuación, seleccione **Guardar**.

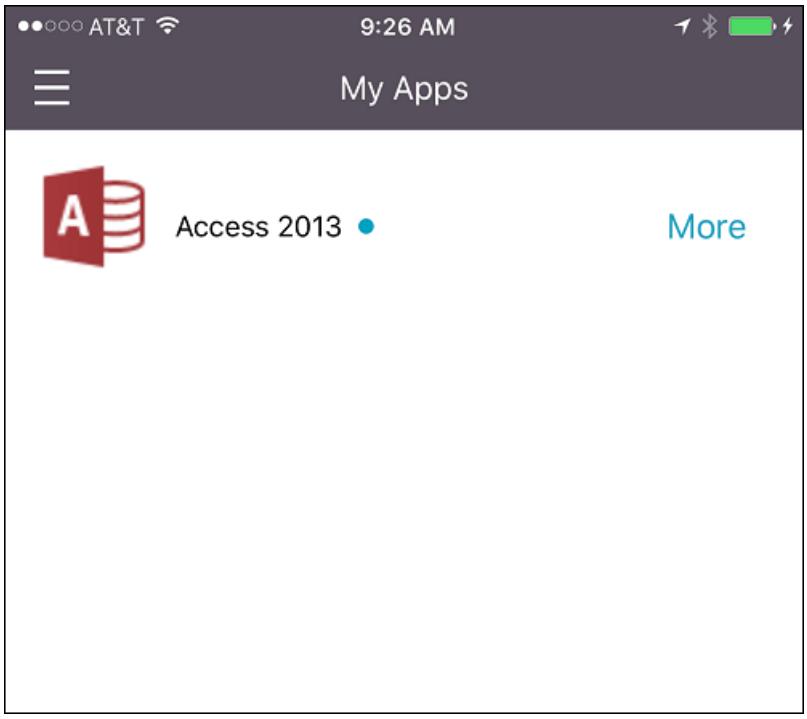
Para obtener información detallada acerca de la configuración de acciones automatizadas, consulte Acciones automatizadas.

Cómo los usuarios recuperan el acceso a las aplicaciones HDX

Los usuarios pueden volver a obtener el acceso a las aplicaciones HDX después de que el dispositivo vuelva a ser conforme:

1. En el dispositivo, vaya al almacén Secure Hub para actualizar las aplicaciones en el almacén.
2. Vaya a la aplicación y toque **Agregar** en la aplicación.

Una vez agregada la aplicación, aparece en “Mis aplicaciones” con un punto azul, porque es una aplicación recién instalada.



Agregar contenido multimedia

January 4, 2022

Puede agregar contenido multimedia a XenMobile para implementarlo en los dispositivos de usuario. Asimismo, puede utilizar XenMobile para implementar libros de Apple Books que obtiene a través de las compras por volumen de Apple.

Después de configurar una cuenta de compras por volumen en XenMobile, los libros gratuitos y adquiridos que posea aparecerán en **Configurar > Multimedia**. Los libros se configuran para la implementación en dispositivos iOS desde las páginas **Multimedia**. Para implementarlos, debe elegir grupos de entrega y especificar reglas de implementación.

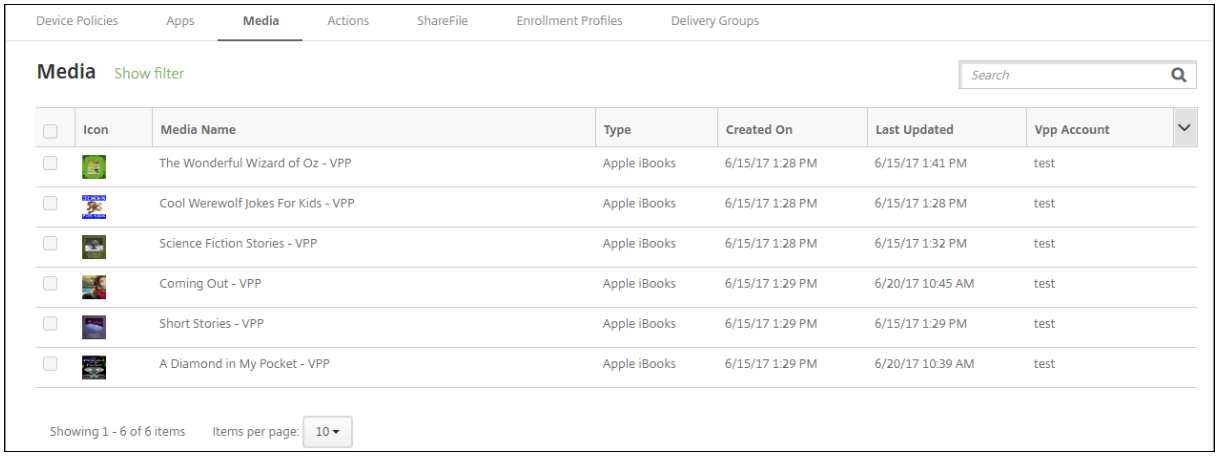
La primera vez que el usuario recibe un libro y acepta la licencia de compras por volumen, los libros implementados se instalan en el dispositivo. Los libros aparecen en la aplicación Apple Books. La licencia de un libro no se puede desasociar del usuario; tampoco se puede quitar el libro del dispositivo. XenMobile instala Books como aplicación obligatoria. Aunque un usuario elimine un libro instalado en el dispositivo, ese libro permanecerá en la aplicación Apple Books, listo para la descarga.

Requisitos previos

- Dispositivos iOS
- Configure las compras por volumen de Apple en XenMobile, tal y como se describe en Compras por volumen de Apple.

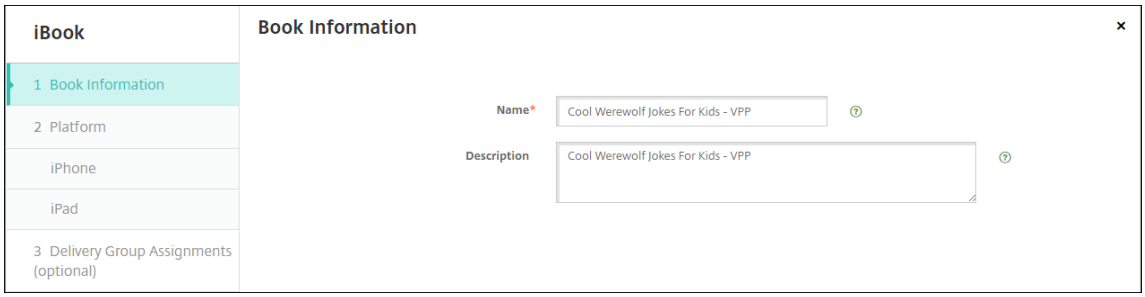
Configurar libros

Los libros de Apple Books obtenidos mediante las compras por volumen aparecen en la página **Configurar > Multimedia**.



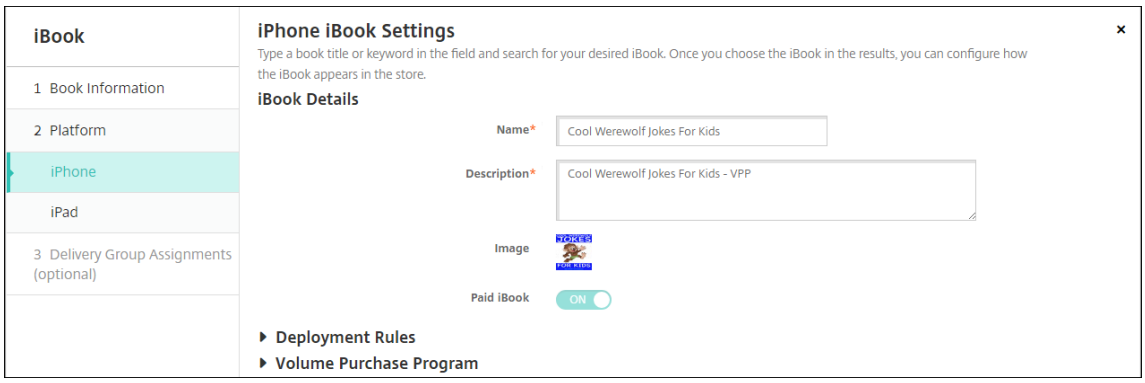
Para configurar un libro de Apple Books para la implementación

1. En **Configurar > Multimedia**, seleccione un libro y haga clic en **Modificar**. Aparecerá la página **Información del libro**.

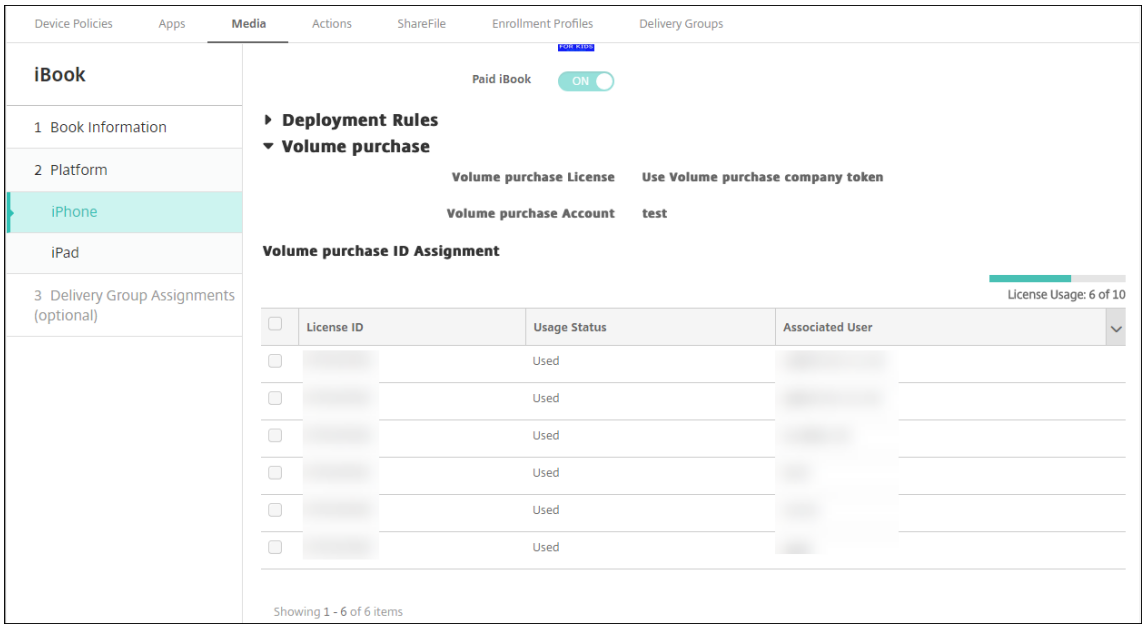


   El **Nombre** y la **Descripción** solo aparecen en los registros y la consola de XenMobile.

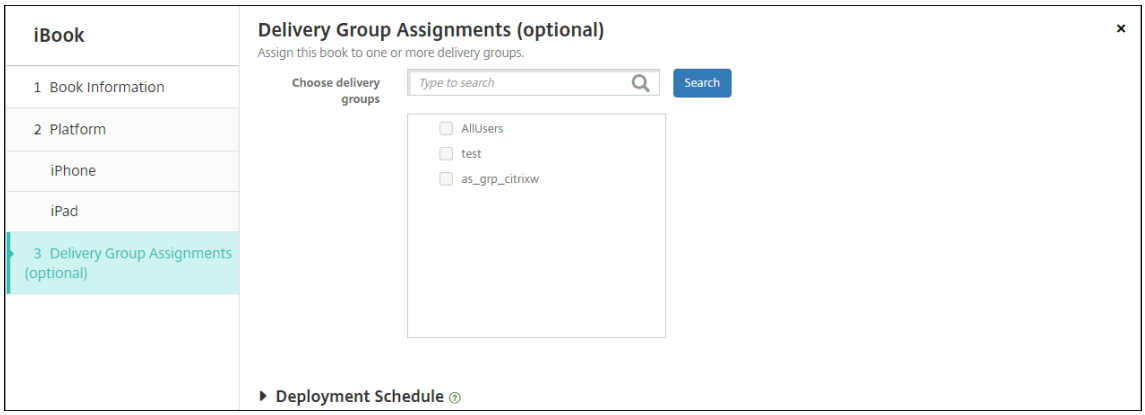
2. En las páginas **Parámetros de iBook para iPhone** y **Parámetros de iBook para iPad**, puede cambiar el nombre y la descripción del libro, aunque Citrix recomienda no cambiar estos parámetros. La imagen es para su información; este campo no se puede modificar. **iBook de pago** indica que el libro se ha adquirido a través de las compras por volumen de Apple.



También puede especificar reglas de implementación o ver la información de las compras por volumen.

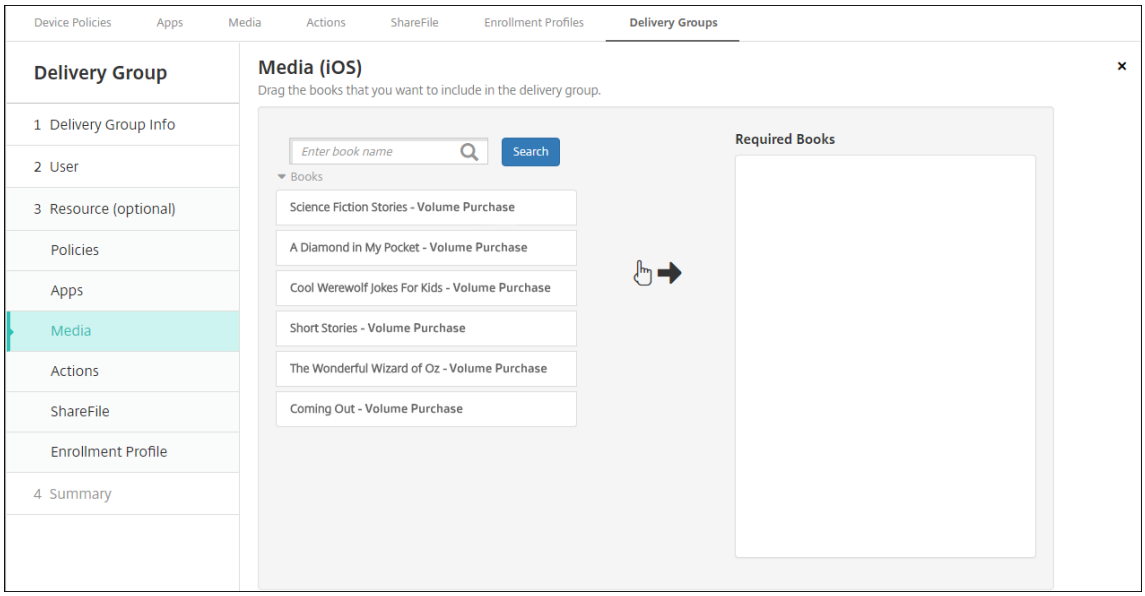


3. Si lo prefiere, asigne el libro a grupos de entrega y configure una programación de implementación.

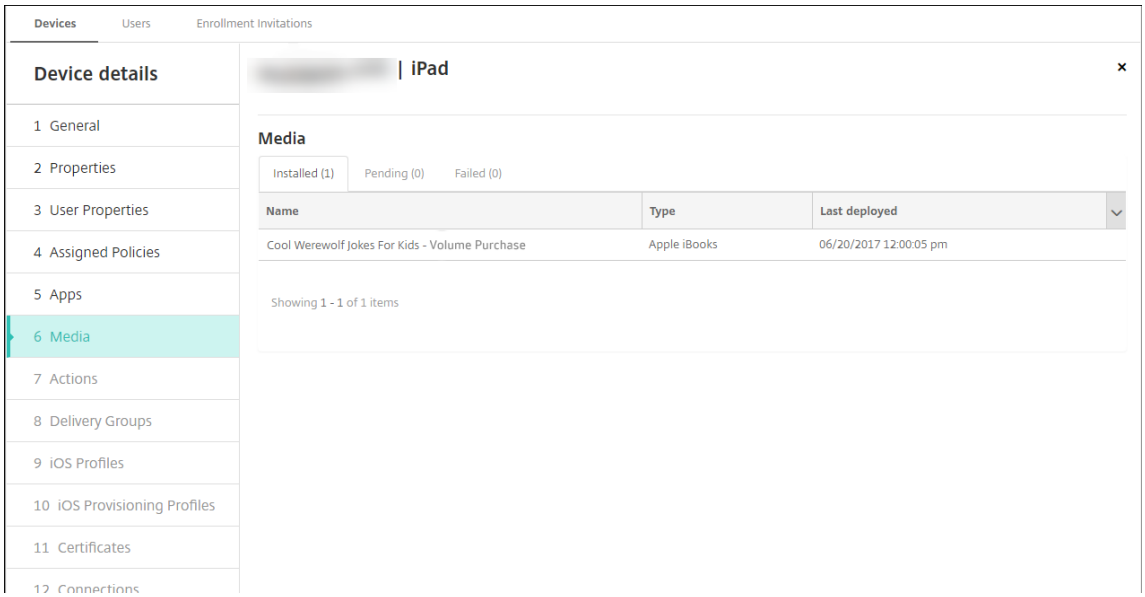


También puede asignar libros a grupos de entrega desde la ficha **Multimedia** de **Configurar >**

Grupos de entrega. XenMobile solo admite la implementación de libros obligatorios.

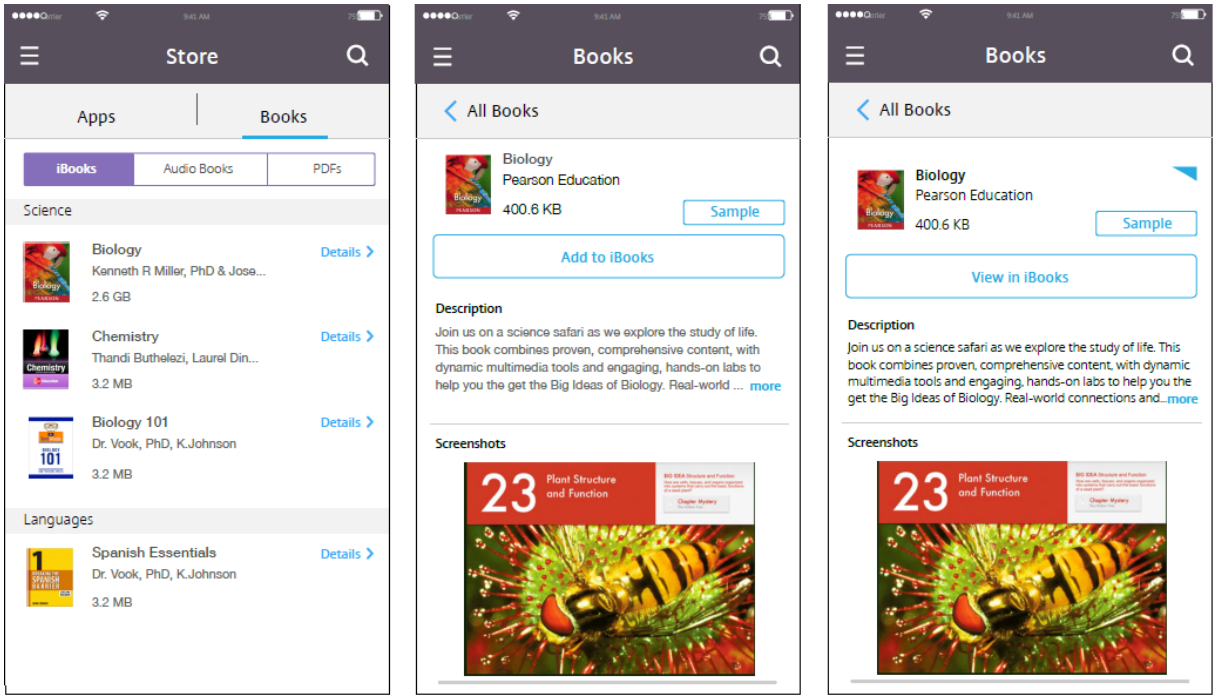


4. Puede ver el estado de la implementación desde la ficha **Multimedia** de **Administrar > Dispositivos**.



> **Nota:**
>
> En la página **Configurar > Multimedia**, si selecciona un libro y hace clic en **Eliminar**, XenMobile elimina ese libro de la lista. No obstante, la próxima vez que XenMobile se sincronice con las compras por volumen de Apple, el libro volverá a aparecer en la lista a menos que se haya quitado de las compras por volumen de Apple. Eliminar un libro de la lista no lo quita de los dispositivos.

Los libros aparecen en los dispositivos de usuario como se muestra en el siguiente ejemplo.



Implementar recursos

January 4, 2022

La configuración y la administración de dispositivos suelen implicar la creación de recursos (directivas, aplicaciones y contenido multimedia) y acciones en la consola de XenMobile y, posteriormente, su empaquetado por 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
- Cambiar el orden de la implementación de los recursos y las acciones en los grupos de entrega
- XenMobile determina el orden de implementación cuando un usuario está incluido en varios grupos de entrega que tienen directivas duplicadas o conflictivas.

Los grupos de entrega indican la categoría de usuarios en cuyos dispositivos se implementan las combinaciones de directivas, aplicaciones, contenido multimedia 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 en los dispositivos de todos los usuarios, o bien en los de un grupo más definido de ellos.

La implementación de recursos en un grupo de entrega implica enviar una notificación push a todos

los usuarios que tengan los dispositivos iOS y Windows admitidos. Los usuarios deben pertenecer al grupo de entrega para volver a conectarse a XenMobile. Puede volver a evaluar los dispositivos e implementar aplicaciones, directivas, contenido multimedia y acciones asignados a un grupo de entrega.

Para los usuarios con dispositivos Android: si ya están conectados, recibirán los recursos inmediatamente. De lo contrario, en función de cómo se haya configurado la directiva de programación, recibirán los recursos la próxima vez que se conecten.

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 aplica a los dispositivos de un grupo de entrega que tienen un perfil de inscripción configurado para la administración de dispositivos (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, a los recursos. Los recursos incluyen directivas, aplicaciones, acciones y 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.

Este es un resumen de los conceptos principales relacionados con el orden de implementación:

- **Orden de implementación:** La secuencia que sigue XenMobile para transferir los recursos (directivas, aplicaciones y contenido multimedia) y las acciones a un dispositivo. El orden de implementación de algunas directivas, tales como las de términos y condiciones e inventario de software, 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, el contenido multimedia 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 implementación:** XenMobile utiliza la programación de la implementación especificada para acciones, aplicaciones, contenido multimedia y directivas 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.

Esta tabla muestra los criterios de filtrado y control para los distintos tipos de objetos y recursos. Las reglas de implementación se basan en las propiedades del dispositivo.

Objeto/Recurso	Plataforma del dispositivo	Regla de implementación	Programación de la implementación	Usuario/Grupos
Directiva de dispositivo	S	S	S	-
Aplicación	S	S	S	-
Medios	S	S	S	-
Acción	-	S	S	-
Grupo de entrega	-	S	-	S

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 se configura de distinta forma en grupos de entrega diferentes asignados a un mismo usuario.

Cuando se da 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. Identifica todos los grupos de entrega de un usuario específico, en función de los filtros de usuario, grupos y reglas de implementación.
2. Crea una lista ordenada de todos los recursos (directivas, acciones, contenido multimedia y aplicaciones) en los grupos de entrega seleccionados. La lista se basa en los filtros de plataforma de dispositivo, reglas de implementación y programación de la implementación. El algoritmo para ordenarlos es el siguiente:
    a) Colocar los recursos de los grupos de entrega que tengan un orden de implementación definido por el usuario por delante de aquellos recursos de grupos de entrega que no lo tengan. La razón para hacer esto se describe después de los pasos.
    b) En caso de haber dos grupos de entrega en las mismas circunstancias, ordenar los recursos de los grupos de entrega por nombre de grupo. Por ejemplo, se colocan los recursos del

grupo de entrega A por delante de los del grupo de entrega B.

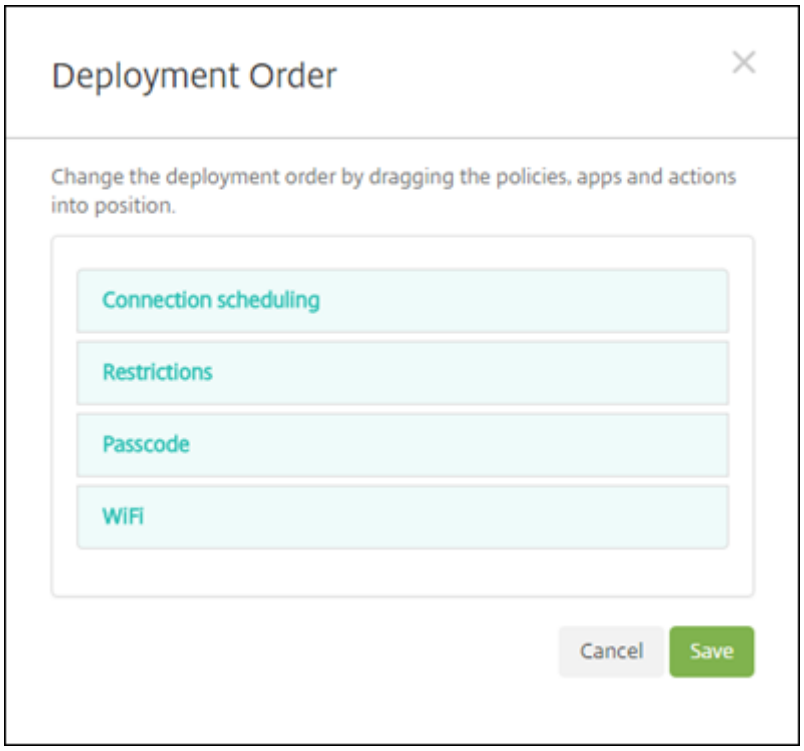
c) Durante el proceso de ordenamiento, se mantiene el orden de implementación especificado para los recursos de un grupo de entrega, si lo hubiera. Si no lo hay, los recursos del grupo de entrega se ordenan por nombre de recurso.

d) Si el mismo recurso aparece más de una vez, quitar el recurso duplicado.

Los recursos que tienen asociado un orden definido por el usuario se implementan antes que los recursos que no tienen un orden definido por el usuario. Un recurso puede existir en varios grupos de entrega asignados a un 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 de recursos **no especificado**. Contiene las directivas **Wi-Fi** y **Código de acceso**.
- Grupo de entrega, Gestores de cuentas 2: Con un orden de recursos **especificado**. Contiene las directivas **Programación de conexiones**, **Restricciones**, **Código de acceso** y **Wi-Fi**. En este caso, se quiere entregar la directiva **Código de acceso** antes que la directiva **Wi-Fi**.



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: **Wi-Fi**, **Código de acceso**, **Programación de conexiones** y **Restricciones**. XenMobile omitiría **Código**

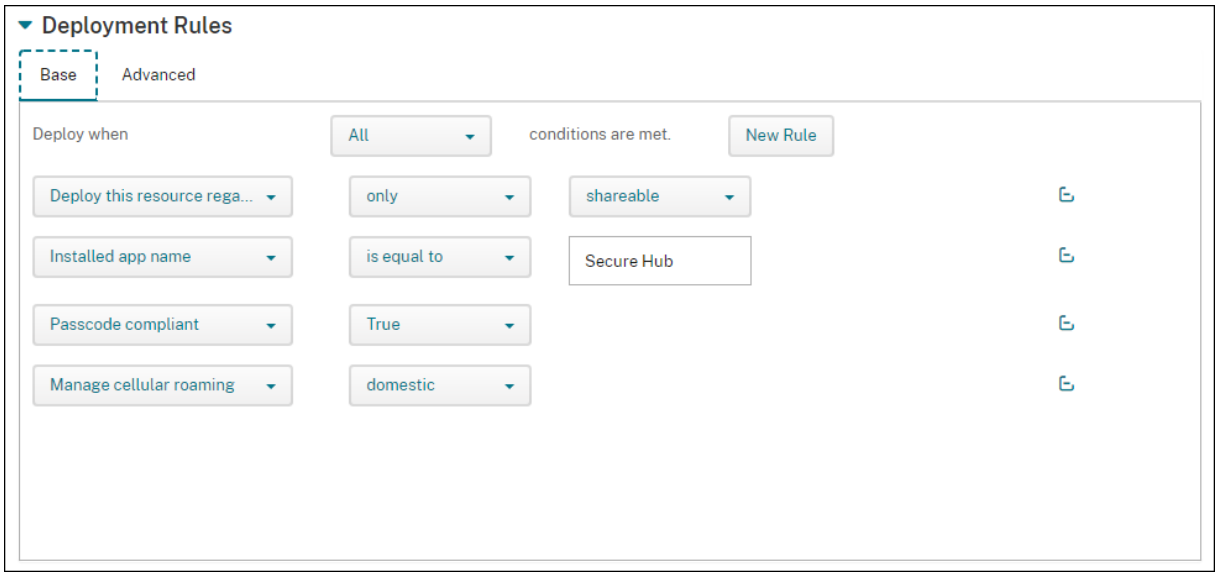
de acceso y **Wi-Fi**, por ser duplicados, del grupo de entrega Gestores de cuentas 2.

No obstante, el grupo Gestores de cuentas 2 tiene un orden de implementación especificado por el administrador. Por lo tanto, el algoritmo de cálculo coloca los recursos del grupo de entrega Gestores de cuentas 2 por encima de los recursos del otro grupo de entrega en la lista. Como resultado, XenMobile implementa las directivas en este orden: **Programación de conexiones**, **Restricciones**, **Código de acceso** y **Wi-Fi**. XenMobile omite las directivas **Wi-Fi** y **Código de acceso** 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.

Reglas de implementación

Configure las reglas de implementación para entregar los recursos solo cuando se cumplan ciertas condiciones. Puede configurar reglas de implementación básicas o avanzadas.

Cuando agregue una regla de implementación con el editor de reglas básicas, seleccione primero cuándo implementar el recurso.



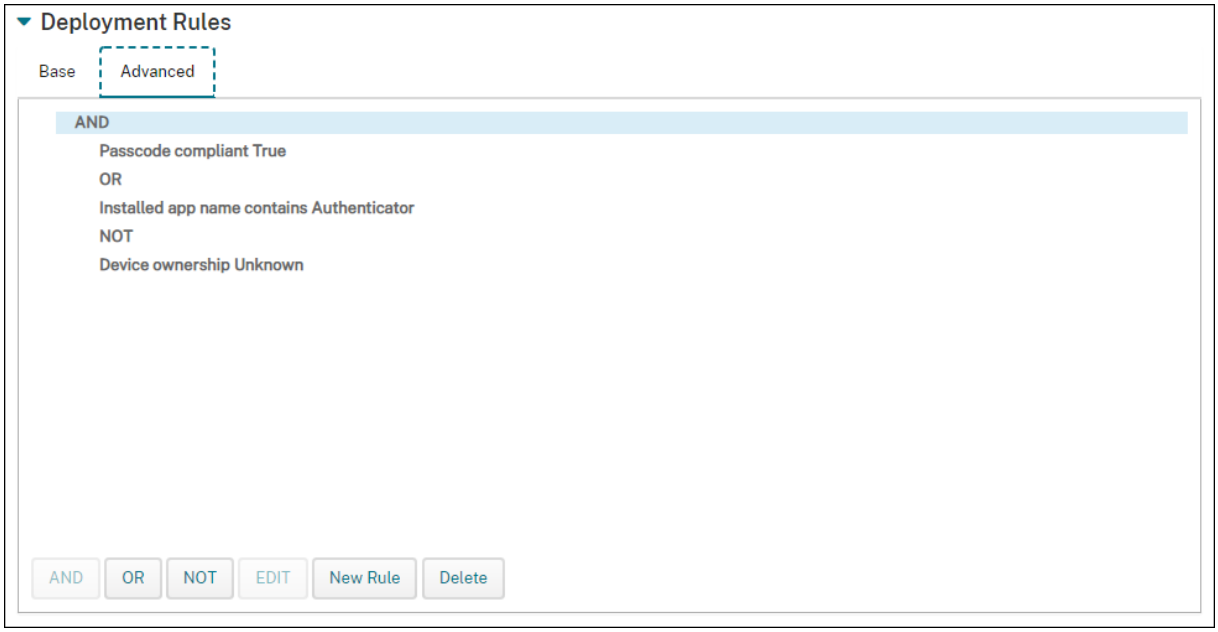
- **Todas:** Entregue el recurso cuando el usuario o dispositivo cumpla todas las condiciones que configure.
- **Cualquiera:** Entregue el recurso cuando el usuario o dispositivo cumpla al menos una de las condiciones que configure.

Haga clic en **Nueva regla** para agregar una condición. Las reglas varían en función del recurso que se está implementando y la plataforma para la que se configura el recurso. Existen varios tipos de reglas. Puede optar por implementar el recurso:

- Solo cuando se cumple la propiedad seleccionada o excepto cuando se cumple la propiedad seleccionada.

- Cuando la propiedad coincide exactamente con el texto que escribe, la propiedad contiene el texto que escribe o la propiedad no coincide con el texto que escribe.
- Cuando el dispositivo o el usuario cumplen con la propiedad seleccionada o no cumplen con la propiedad seleccionada.
- Cuando las propiedades del dispositivo o del usuario coinciden con la condición seleccionada de una lista predefinida.

Utilice el editor avanzado para crear reglas de implementación más complejas. Existen más reglas que seleccionar y es posible combinar diferentes operadores lógicos booleanos al crear una regla avanzada.



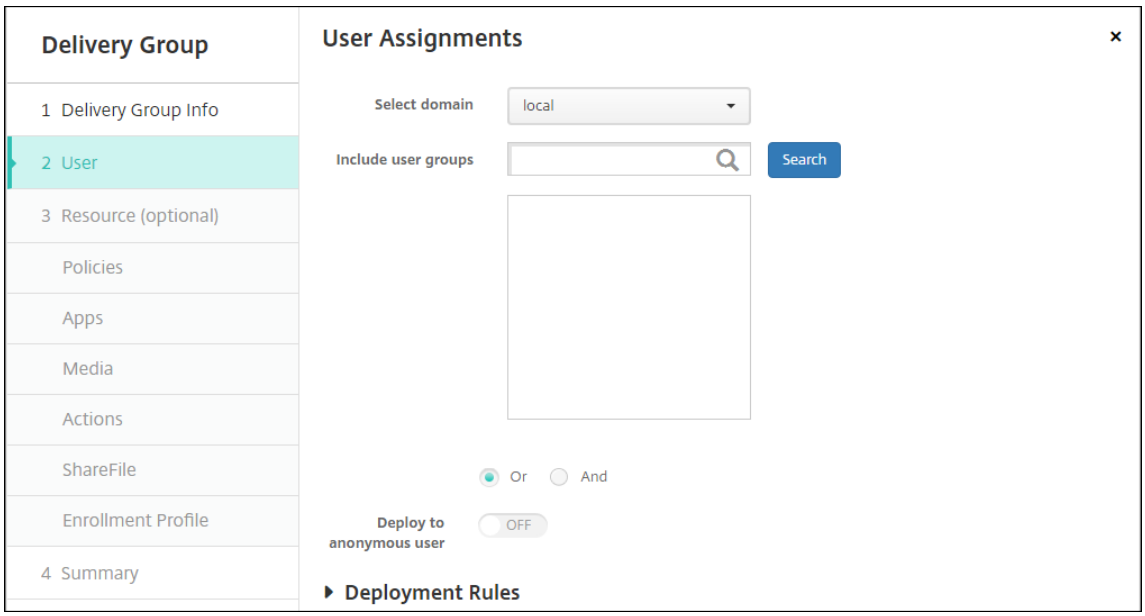
Para agregar un grupo de entrega

Citrix recomienda crear grupos de entrega antes de crear directivas de dispositivo y perfiles de inscripción.

1. En la consola, haga clic en **Configurar > Grupos de entrega**.
2. En la página **Grupos de entrega**, haga clic en **Agregar**.
3. En la página **Información del grupo de entrega**, escriba un nombre y una descripción para el grupo de entrega y, a continuación, haga clic en **Siguiente**.

   Si un usuario pertenece a varios grupos de entrega que tienen perfiles de inscripción diferentes, el nombre del grupo de entrega determina el perfil de inscripción utilizado. XenMobile selecciona el grupo de entrega que aparece en último lugar en una lista alfabética de grupos de entrega. Para obtener más información, consulte Perfiles de inscripción.

4. En la página **Asignaciones de usuarios**, especifique cómo administrar las asignaciones de usuario del grupo de entrega.



> **Importante:**
>
> No puede cambiar el parámetro **Administrar asignaciones de usuarios** una vez creado el grupo de usuarios.

- **Seleccionar dominio:** En la lista, seleccione el dominio del que se elegirá a los usuarios.
- **Incluir grupos de usuarios:** 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 **Grupos de usuarios seleccionados**.
  - Haga clic en **Buscar** 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 **Buscar** para limitar la lista de grupos de usuarios.

  Para quitar un grupo de usuarios de la lista **Grupos de usuarios seleccionados**, realice una de las siguientes acciones:

  - En la lista **Grupos de usuarios seleccionados**, haga clic en la **X** situada junto a cada uno de los grupos que quiera quitar.
  - Haga clic en **Buscar** 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 **Buscar** 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.
- **Implementar para usuario anónimo:** Seleccione si implementar recursos para usuarios sin autenticar del grupo de entrega. Los usuarios sin autenticar son aquellos que no han podido autenticarse pero a cuyos dispositivos se les ha permitido conectarse a XenMobile de todas formas.

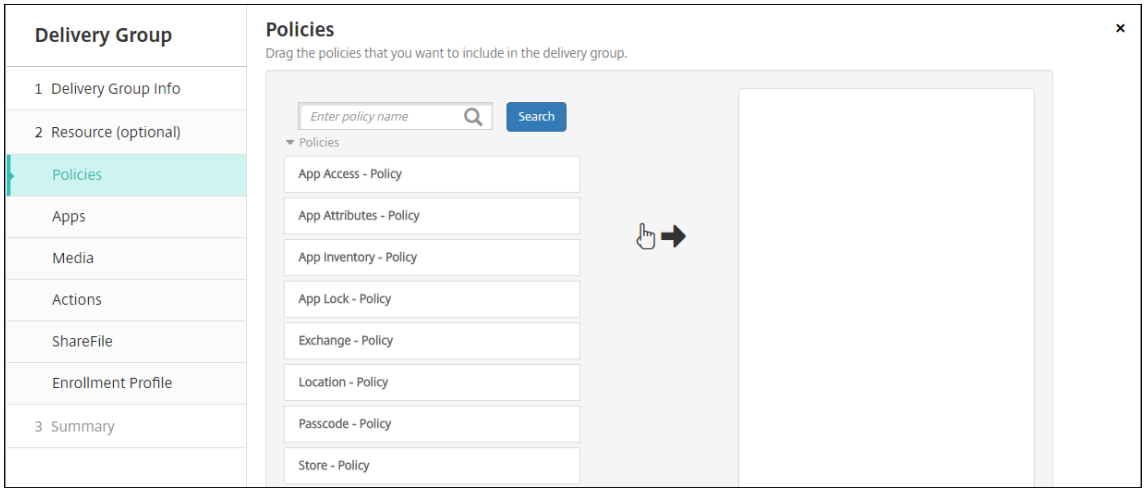
5. Configurar las reglas de implementación.
6. Haga clic en **Siguiente**. Aparecerá la página de recursos del **grupo de entrega**. Si quiere, aquí puede agregar directivas, aplicaciones o acciones al grupo de entrega. Para omitir este paso, en **Grupo de entrega**, haga clic en **Resumen** para ver un resumen de la configuración del grupo de entrega.

   Para omitir un recurso, en **Recurso (opcional)**, haga clic en el recurso que quiere agregar y siga los pasos de ese recurso.

Para agregar directivas

1. Lleve a cabo lo siguiente para agregar cada directiva:
   - Busque la directiva que quiera agregar en la lista de las directivas disponibles.
   - O bien, para limitar la cantidad de directivas de la lista, escriba el nombre completo o parcial de la directiva en el cuadro de búsqueda y, a continuación, haga clic en **Buscar**.
   - Haga clic en la directiva que quiera agregar y arrástrela al cuadro de la derecha.

   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 **Aplicaciones**.

Para agregar aplicaciones

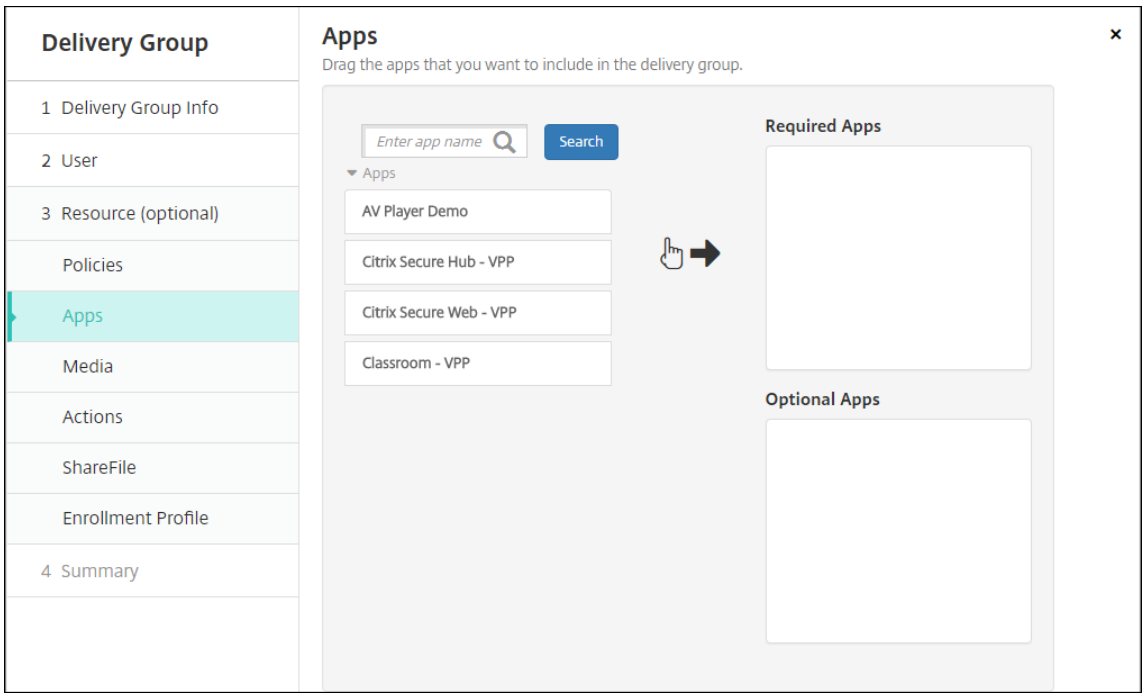
1. Lleve a cabo lo siguiente para agregar cada aplicación:

   - Busque la aplicación que quiera agregar en la lista de las aplicaciones disponibles.
   - O bien, para limitar la cantidad de aplicaciones de la lista, escriba el nombre completo o parcial de la aplicación en el cuadro de búsqueda y, a continuación, haga clic en **Buscar**.
   - Haga clic en la aplicación que quiera agregar y arrástrela al cuadro **Aplicaciones obligatorias** o al cuadro **Aplicaciones opcionales**.

   Para las aplicaciones marcadas como obligatorias, los usuarios reciben inmediatamente actualizaciones en situaciones como estas:

   - Se carga una nueva aplicación y se marca como obligatoria.
   - Se marca una aplicación existente como obligatoria.
   - Un usuario elimina una aplicación obligatoria.
   - Hay una actualización de Secure Hub disponible.

   Para obtener información acerca de la implementación forzosa de las aplicaciones obligatorias, incluido cómo habilitar la función, consulte Acerca de aplicaciones obligatorias y opcionales.

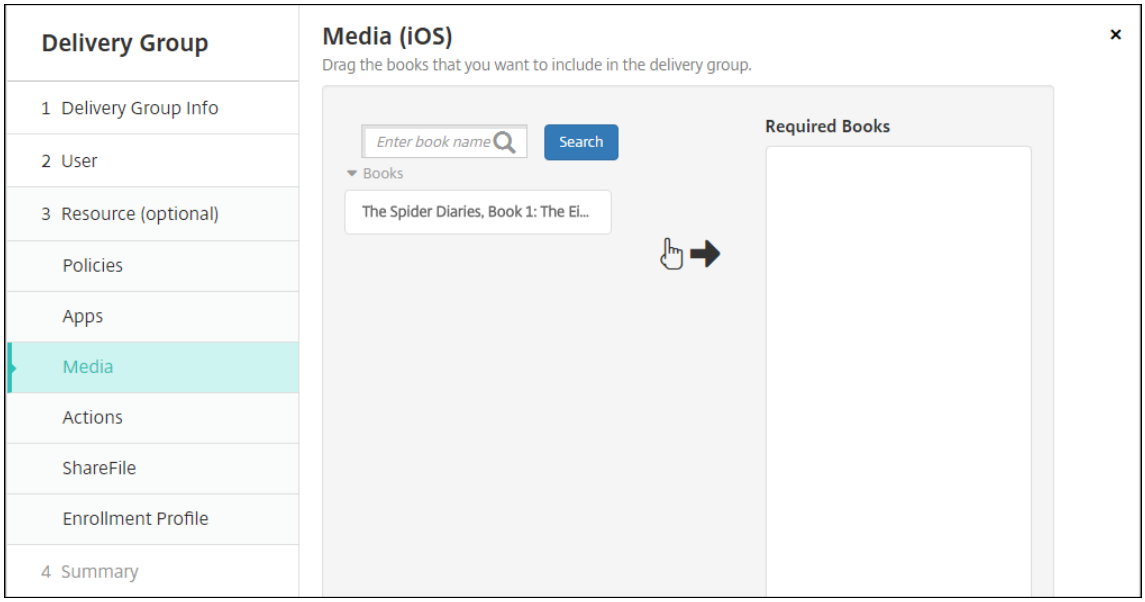


   Para quitar una aplicación, haga clic en la **X** situada junto al nombre de esa aplicación en el cuadro de la derecha.

2. Haga clic en **Siguiente**. Aparecerá la página **Multimedia**.

Para agregar contenido multimedia

1. Lleve a cabo lo siguiente para agregar cada libro:
   - Busque el libro que quiera agregar en la lista de los libros disponibles.
   - O bien, para limitar la cantidad de libros de la lista, escriba el nombre completo o parcial del libro en el cuadro de búsqueda y, a continuación, haga clic en **Buscar**.
   - Haga clic en el libro que quiere agregar y arrástrelo al cuadro **Libros obligatorios**.



   En caso de libros marcados como obligatorios, los usuarios reciben inmediatamente actualizaciones en situaciones tales como:
   - Se carga un nuevo libro y se marca como obligatorio.
   - Se marca un libro existente como obligatorio.
   - Un usuario elimina un libro obligatorio.
   - Hay una actualización de Secure Hub disponible.

   Para quitar un libro, haga clic en la **X** situada junto al nombre de ese libro en el cuadro de la derecha.

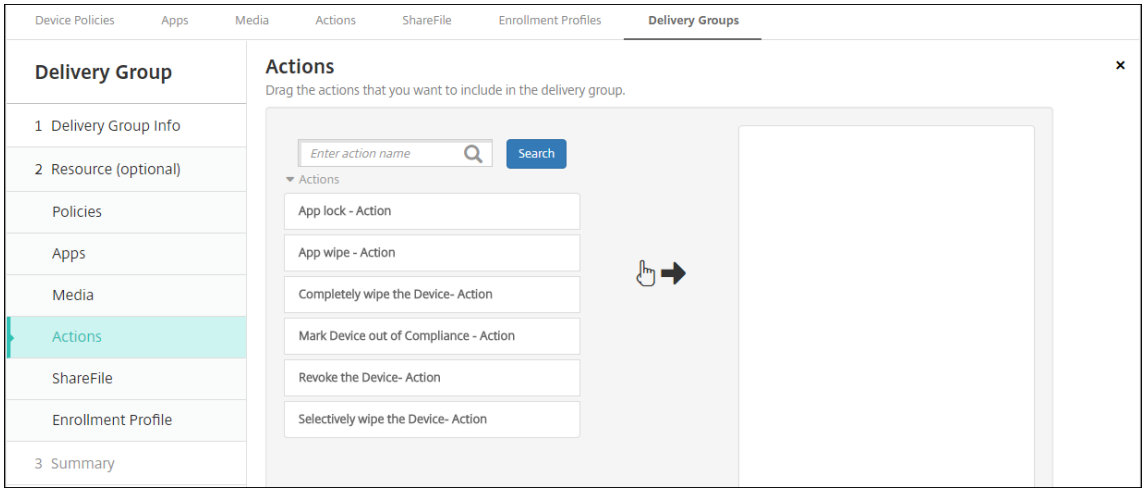
2. Haga clic en **Siguiente**. Aparecerá la página **Acciones**.

Para agregar acciones

1. Lleve a cabo lo siguiente para agregar cada acción:
   - Busque la acción que quiera agregar en la lista de las acciones disponibles.
   - O bien, para limitar la cantidad de acciones de la lista, escriba el nombre completo o parcial de la acción en el cuadro de búsqueda y, a continuación, haga clic en **Buscar**.

- Haga clic en la acción que quiera agregar y arrástrela al cuadro de la derecha.

Para quitar una acción, haga clic en la **X** situada junto al nombre de esa acción en el cuadro de la derecha.

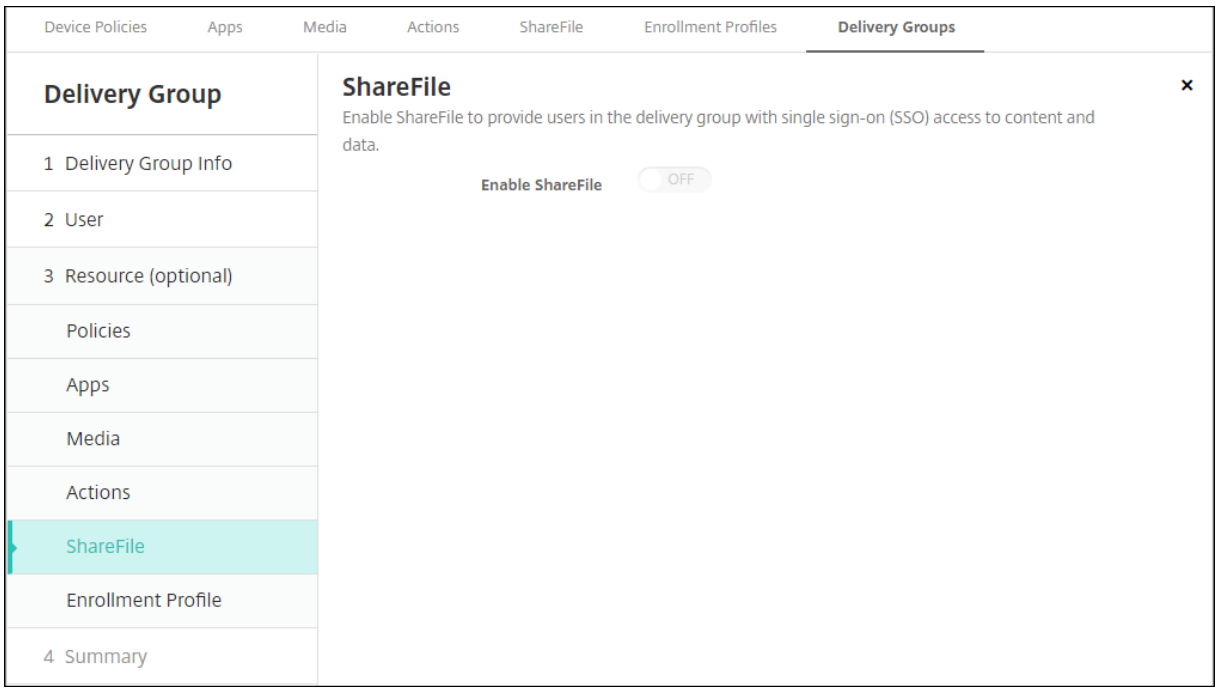


2. Haga clic en **Siguiente**. Aparecerá la página **ShareFile**.

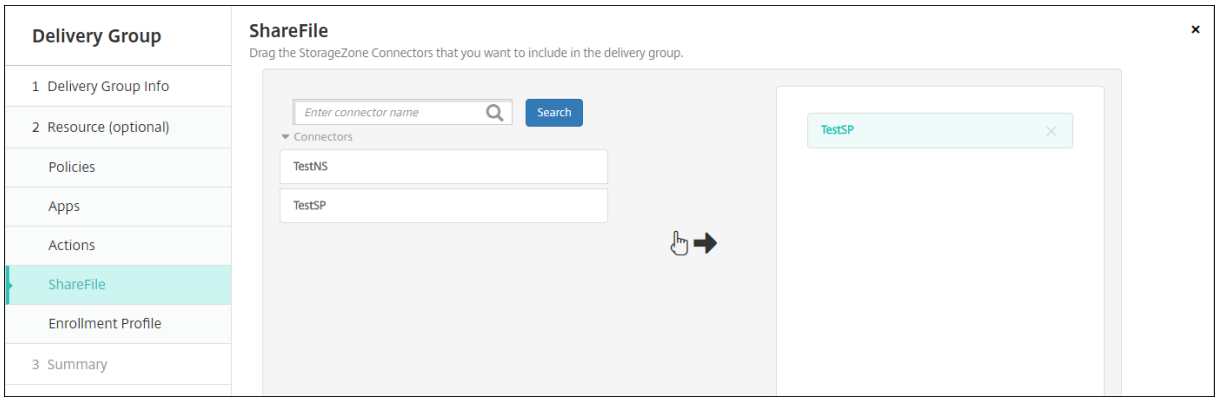
Para aplicar la configuración de Content Collaboration

La página Content Collaboration varía según si ha configurado XenMobile (**Configurar > Content ShareFile**) para cuentas Enterprise o para conectores de zonas de almacenamiento.

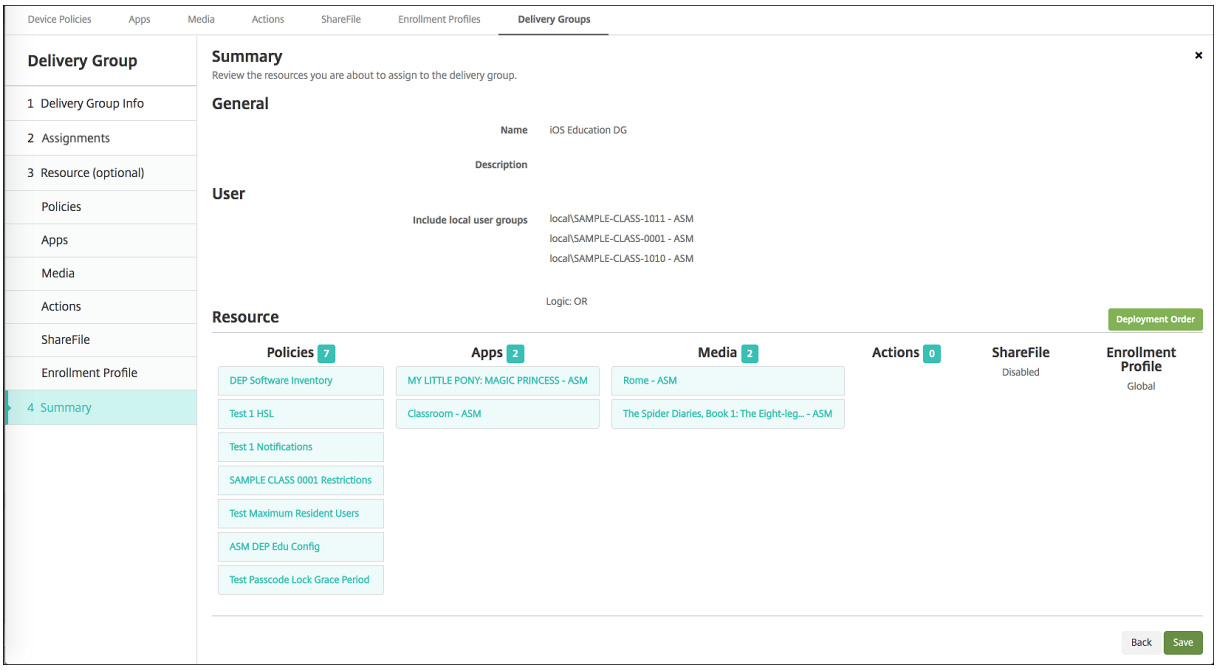
Si ha configurado cuentas Enterprise para usarlas con XenMobile, **active** el parámetro **Habilitar ShareFile** para conceder al grupo de entrega acceso Single Sign-On a los datos y contenido de Content Collaboration.



En cambio, si ha configurado conectores de zonas de almacenamiento para usarlos con XenMobile, seleccione los que se incluirán en el grupo de entrega.

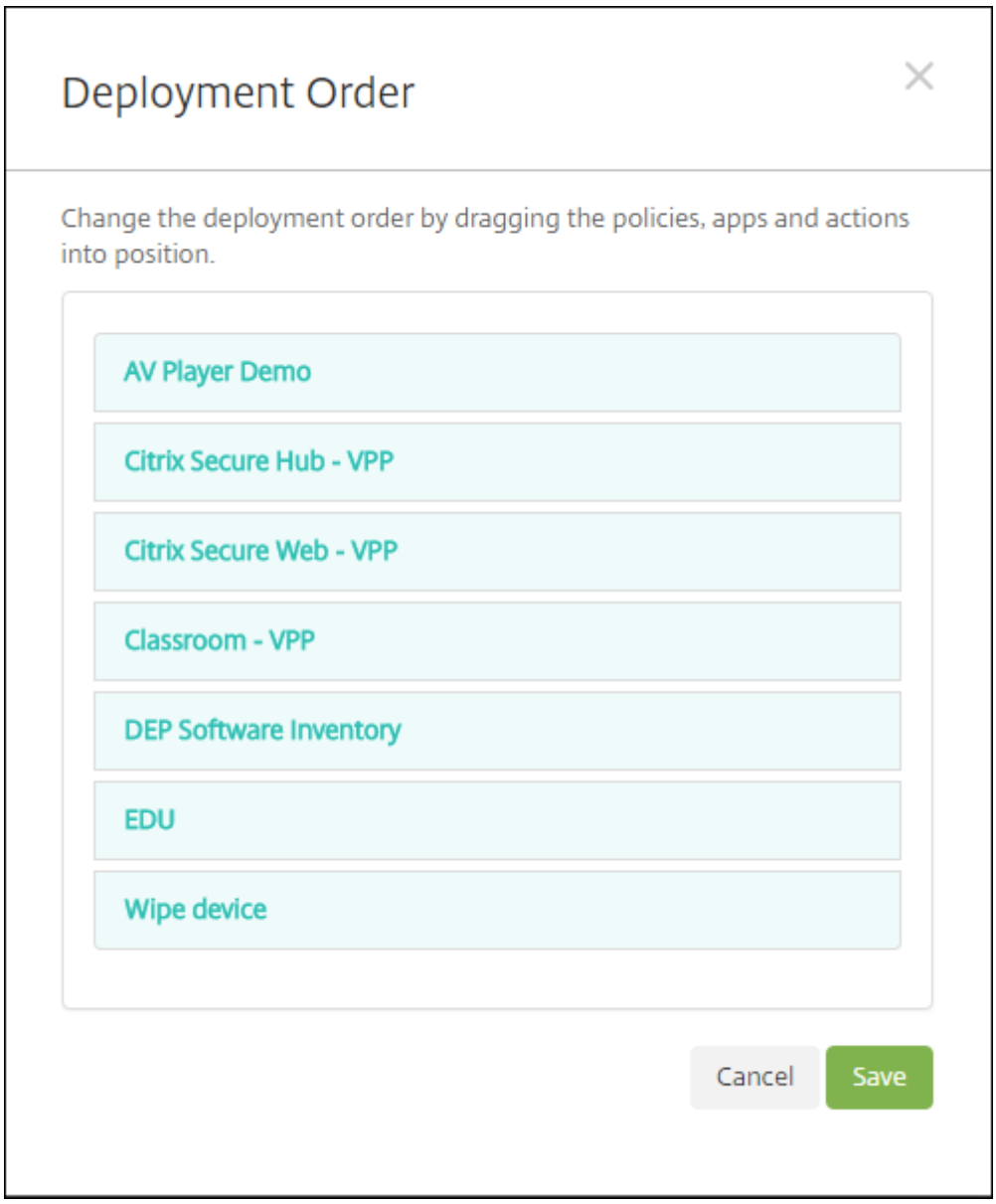


Para revisar las opciones configuradas y cambiar el orden de implementación



En la página **Resumen**, puede revisar las opciones que haya configurado para el grupo de entrega y cambiar el orden de implementación de los recursos. La página “Resumen” contiene los recursos por categoría. La página “Resumen” no refleja el orden de implementación.

1. Haga clic en **Atrás** para volver a las páginas anteriores y realizar los ajustes necesarios a la configuración.
2. Haga clic en **Orden de implementación** para ver el orden de implementación o para cambiarlo. Aparecerá el cuadro de diálogo **Orden de implementación**.



3. 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.
4. Haga clic en **Guardar** para guardar el orden de implementación.
5. Haga clic en **Guardar** para guardar el grupo de entrega.

Para modificar un grupo de entrega

No se puede cambiar el nombre de un grupo de entrega existente. Para actualizar otros parámetros: vaya a **Configurar > Grupos de entrega**, seleccione el grupo que quiera modificar y, a continuación, haga clic en **Modificar**.

Para habilitar e inhabilitar el grupo de entrega AllUsers

AllUsers es el único grupo de entrega que puede habilitar o inhabilitar.

Desde la página **Grupos de entrega**, para seleccionar el grupo de entrega AllUsers, marque la casilla situada junto al nombre **AllUsers** o haga clic en la línea que contiene AllUsers. A continuación, lleve a cabo una de las siguientes acciones:

- Haga clic en **Inhabilitar** para inhabilitar el grupo de entrega AllUsers. Este comando solo está disponible si AllUsers está habilitado (valor predeterminado). Una vez **inhabilitado**, aparecerá bajo el encabezado **Inhabilitado** en la tabla del grupo de entrega.
- Haga clic en **Habilitar** para habilitar el grupo de entrega AllUsers. Este comando solo está disponible si AllUsers está inhabilitado. Una vez **habilitado**, desaparecerá del encabezado **Inhabilitado** de la tabla del grupo de entrega.

Para implementar en grupos de entrega

La implementación en un grupo de entrega implica enviar una notificación push a todos los usuarios con dispositivos iOS, Windows Phone y tabletas Windows. Los usuarios deben pertenecer al grupo de entrega para volver a conectarse a XenMobile. De esta manera, puede volver a evaluar los dispositivos e implementar aplicaciones, directivas y acciones.

Para los usuarios con dispositivos de otras plataformas: si esos dispositivos ya están conectados a XenMobile, recibirán los recursos inmediatamente. De lo contrario, en función de cómo se haya configurado la directiva de programación, recibirán los recursos la próxima vez que se conecten.

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 “Inventario de aplicaciones” en los dispositivos de los usuarios.

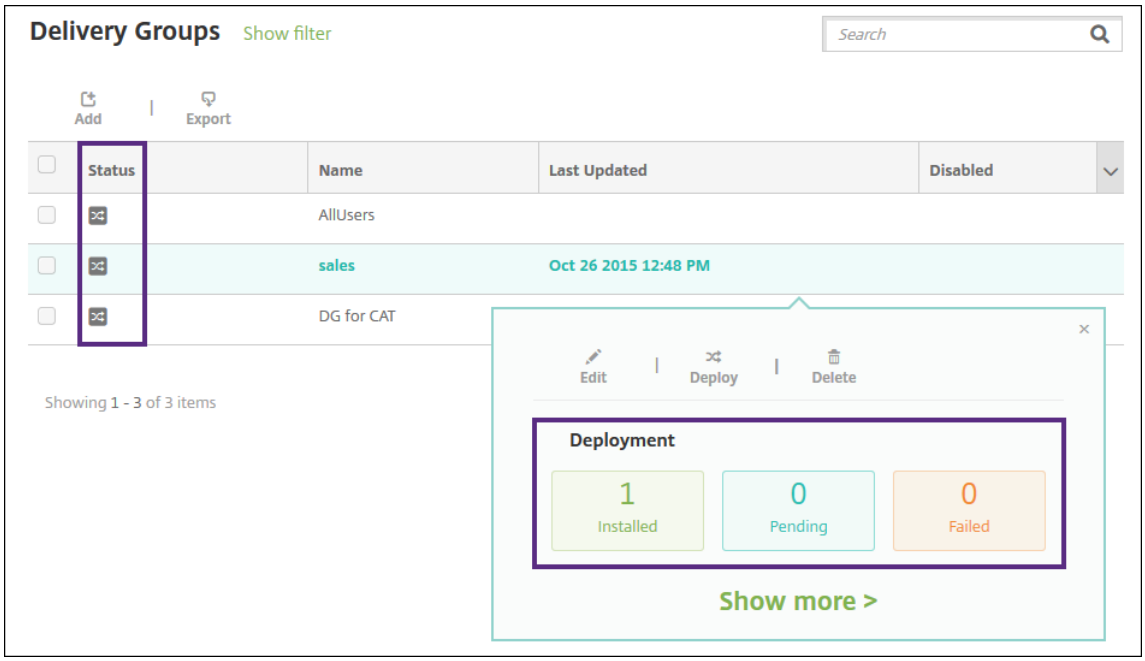
1. En la página **Grupos de entrega**, realice una de las siguientes acciones:
   - Para implementar recursos en más de un grupo de entrega a la vez, marque las casillas situadas junto a los grupos en los que quiere realizar la implementación.
   - Para implementar recursos en un solo grupo de entrega, marque la casilla que aparece junto a su nombre o haga clic en la línea que contiene su nombre.
2. Haga clic en **Implementar**.

   Según cómo seleccione el grupo de entrega, el comando **Implementar** aparecerá encima o a la derecha del grupo de entrega.

   Compruebe que los grupos en los que se van a implementar aplicaciones, directivas y acciones se encuentran en la lista y, a continuación, haga clic en **Implementar**. 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 **Grupos de entrega** de una de las siguientes maneras:

- Consulte el icono de implementación situado en el encabezado **Estado** del grupo de entrega. Este icono indica si ha habido algún error en la implementación.
- Haga clic en la línea que contiene el grupo de entrega para ver una etiqueta superpuesta donde se indica si la implementación **se ha instalado**, **está pendiente** o **ha fallado**.



Para eliminar grupos de entrega

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 **Grupos de entrega**, 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 **Eliminar**.

   Según cómo seleccione el grupo de entrega, el comando **Eliminar** aparecerá encima o a la derecha del grupo de entrega.

   > **Importante:**
   >
   > No puede deshacer una eliminación.

3. Haga clic en **Delete**.

Para exportar la tabla de grupos de entrega

1. Haga clic en el botón **Exportar** situado sobre la tabla **Grupos de entrega**. XenMobile extrae la información de la tabla **Grupos de entrega** y la convierte a un archivo CSV.
2. Abra o guarde el archivo CSV siguiendo los pasos habituales del explorador web que utilice. También puede cancelar la operación.

Macros

January 4, 2022

XenMobile ofrece macros para rellenar datos de propiedades de usuario o dispositivo en el campo de texto de los siguientes elementos:

- Directivas
- Notificaciones
- Plantillas de inscripción
- Acciones automatizadas
- Solicitudes de firma de certificado provenientes del proveedor de credenciales

XenMobile reemplaza una macro por los valores correspondientes al usuario o al sistema. Por ejemplo, puede rellenar de antemano el valor del buzón de correo perteneciente a un solo usuario en un perfil de Exchange entre miles de usuarios.

Sintaxis de macros

Una macro puede presentar el siguiente formato:

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)] }`

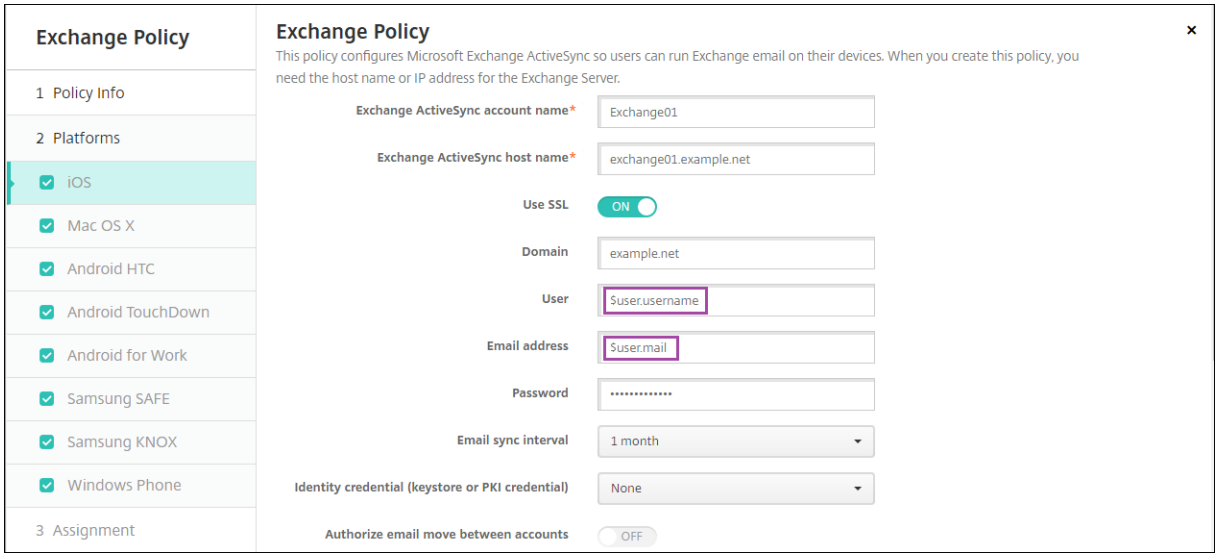
Incluya todos los elementos de sintaxis posteriores al signo de dólar ($) entre llaves ({ }).

- 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.

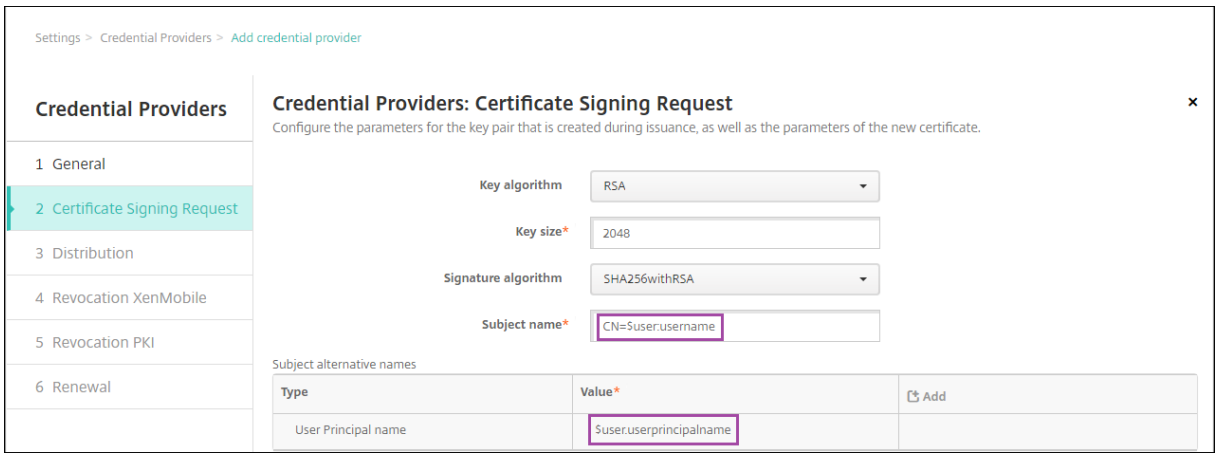
- Las propiedades del usuario tienen el formato `${ user.[PROPERTYNAME] (prefix="user.")}`.
- Las propiedades del dispositivo tienen el formato `${ device.[PROPERTYNAME] (prefix="device.")}`.
- Los nombres de propiedad distinguen mayúsculas de minúsculas.
- Una función puede ser una lista limitada o un enlace a una referencia externa que define las funciones. Esta macro para un mensaje de notificación incluye la función **firstnotnull**.

  El dispositivo `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` ha sido bloqueado…
- Para macros personalizadas (propiedades que usted define), el prefijo es `${ custom }`. Puede omitir el prefijo.

Este es el ejemplo de una macro frecuente, `${ user.username }`, que rellena el valor de nombre de usuario en el campo de texto de una directiva. Esta macro es útil para configurar perfiles de Exchange ActiveSync y otros perfiles utilizados por varios usuarios. En el siguiente ejemplo, se muestra cómo usar macros en una directiva de Exchange. La macro de **Usuario** es **`${ user.username }`**. La macro para **Dirección de correo electrónico** es **`${ user.mail }`**.

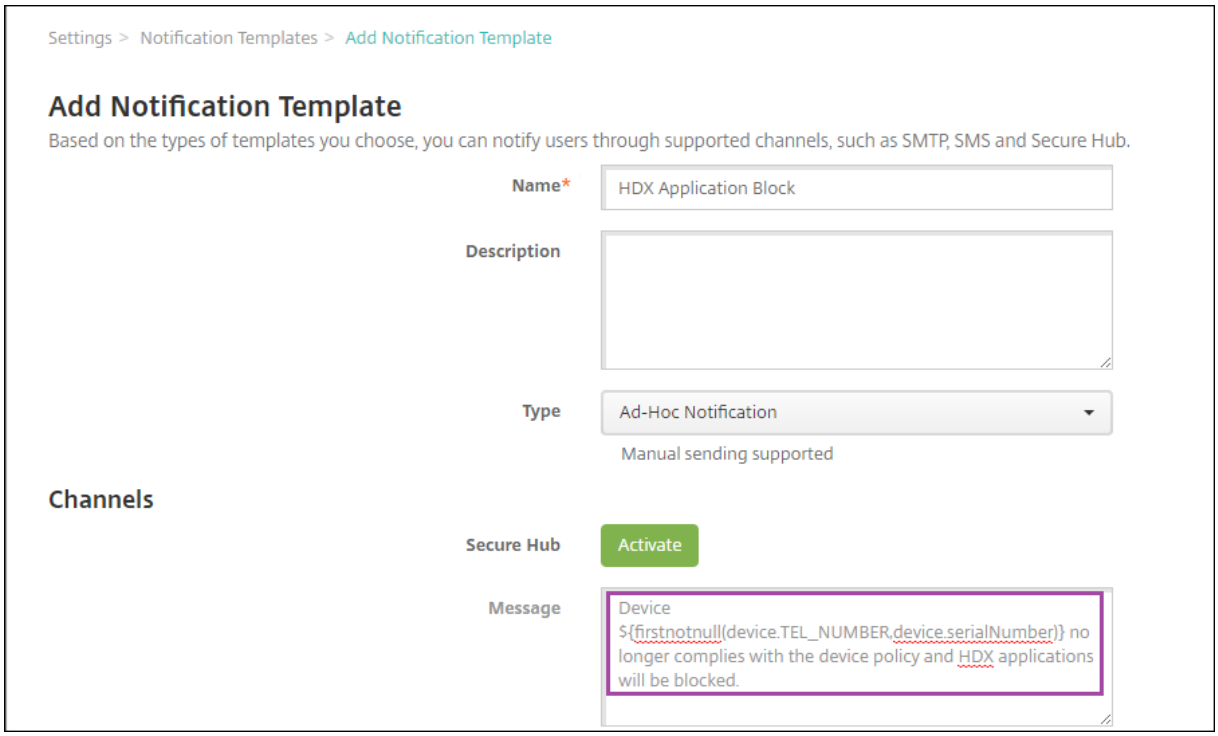


En el siguiente ejemplo, se muestra cómo usar macros en una solicitud de firma de certificado. La macro para el **nombre del sujeto** es **`CN=$user.username`**. La macro para el **valor** de un **nombre alternativo del sujeto** es **`$user.userprincipalname`**.



En el siguiente ejemplo, se muestra cómo usar macros en una plantilla de notificaciones. La plantilla de ejemplo define el mensaje enviado a un usuario cuando las aplicaciones HDX se bloquean debido a un dispositivo que no cumple las reglas. La macro para el **mensaje** es:

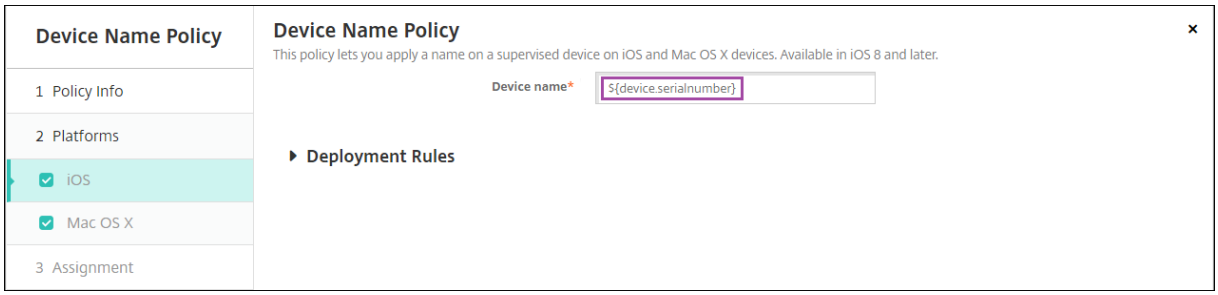
El dispositivo `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` ya no cumple la directiva de dispositivo. Las aplicaciones HDX se bloquearán.



Para obtener más ejemplos de macros utilizadas en las notificaciones, vaya a **Parámetros > Plantillas de notificaciones**, seleccione una plantilla predefinida y haga clic en **Modificar**.

En el siguiente ejemplo, se muestra una macro en la directiva de nombre de dispositivo. Escriba la macro, una combinación de ellas o una combinación de macros y texto para darle a cada dispositivo un nombre único. Por ejemplo, para establecer el número de serie de un dispositivo como su nom-

bre, puede utilizar `${ device.serialnumber }`. Use `${ device.serialnumber } ${ user.username }` para incluir el nombre de usuario en el nombre del dispositivo. La directiva de nombre de dispositivo funciona en dispositivos supervisados iOS y macOS.



Macros para plantillas de notificaciones predeterminadas

Puede utilizar estas macros en las plantillas de notificaciones predeterminadas:

- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`
- `${ enrollment.andriod.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`
- `${ enrollment.pin }`
- `${ enrollment.url }`
- `${ enrollment.urls }`
- `${ enrollment.ios.url }`
- `${ enrollment.macos.url }`
- `${ enrollment.android.url }`
- `${ enrollment.ios.platform }`
- `${ enrollment.macos.platform }`
- `${ enrollment.android.platform }`
- `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}`
- `${ firstnotnull(device.TEL_NUMBER,user.mobile)}`
- `${ outofcompliance.reason(smg_block)}`
- `${ outofcompliance.reason(whitelist_blacklist_apps_name)}`

> **Nota:**
>
> La consola de XenMobile Server contiene los términos “lista negra” y “lista blanca”. Estamos cambiando esos términos en una próxima versión a “lista de bloqueados” y “lista de permitidos”.

- `${ vpp.account }`
- `${ vpp.appname }`
- `${ vpp.url }`
- `${ zdmserver.hostPath } /enroll`

Macros para directivas específicas

En la directiva de nombre de dispositivo (para iOS y macOS), puede usar estas macros para **Nombre de dispositivo**:

- `${ device.serialnumber }`
- `${ user.username } @example.com`
- `${ device.serialnumber }`
- `${ device.serialnumber }`
- `${ user.username }`
- `${ enrollment.pin }`
- `${ user.dnsroot }`

En la directiva de clip web, puede utilizar esta macro para **URL**:

- `${ webeas-url }`

En la directiva de clave de licencia MDM de Samsung, puede utilizar esta macro para **Clave de licencia ELM**:

- `${ elm.license.key }`

Macros para obtener propiedades integradas de dispositivo

Nombre simplificado	Macros
ID de dispositivo	`$device.id`
GUID del dispositivo	`$device.uniqueid`
Número IMEI del dispositivo	`$device.imei`
Familia de SO	`$device.OSFamily`

Nombre simplificado	Macros
Número de serie	`$device.serialNumber`

Macros para todas las propiedades de dispositivo

En la lista siguiente, se indica el nombre simplificado, el elemento web y las macros.

¿Cuenta suspendida?

- GOOGLE_AW_DIRECTORY_SUSPENDED
- ${device.GOOGLE_AW_DIRECTORY_SUSPENDED

Código de omisión del bloqueo de activación

- ACTIVATION_LOCK_BYPASS_CODE
- ${device.ACTIVATION_LOCK_BYPASS_CODE

Bloqueo de activación habilitado

- ACTIVATION_LOCK_ENABLED
- ${device.ACTIVATION_LOCK_ENABLED

Cuenta de iTunes activa

- ACTIVE_ITUNES
- ${device.ACTIVE_ITUNES}

Dispositivo ActiveSync conocido por MSP

- AS_DEVICE_KNOWN_BY_ZMSP
- ${device.AS_DEVICE_KNOWN_BY_ZMSP

ID de ActiveSync

- EXCHANGE_ACTIVESYNC_ID
- ${device.EXCHANGE_ACTIVESYNC_ID

Administrador inhabilitado

- ADMIN_DISABLED
- ${device.ADMIN_DISABLED

¿Está AIK presente?

- WINDOWS_HAS_AIK_PRESENT
- ${device.WINDOWS_HAS_AIK_PRESENT

API MDM de Amazon disponible

- AMAZON_MDM

- ${device.AMAZON_MDM

ID de dispositivo Android Enterprise

- GOOGLE_AW_DEVICE_ID
- ${device.GOOGLE_AW_DEVICE_ID

¿Dispositivo habilitado para Android Enterprise?

- GOOGLE_AW_ENABLED_DEVICE
- ${device.GOOGLE_AW_ENABLED_DEVICE

Tipo de instalación de Android Enterprise

- GOOGLE_AW_INSTALL_TYPE
- ${device.GOOGLE_AW_INSTALL_TYPE

Estado de firma del antispyware

- ANTI_SPYWARE_SIGNATURE_STATUS
- ${device.ANTI_SPYWARE_SIGNATURE_STATUS

Estado del antispyware

- ANTI_SPYWARE_STATUS
- ${device.ANTI_SPYWARE_STATUS

Estado de firma del antivirus

- ANTI_VIRUS_SIGNATURE_STATUS
- ${device.ANTI_VIRUS_SIGNATURE_STATUS

Estado del antivirus

- ANTI_VIRUS_STATUS
- ${device.ANTI_VIRUS_STATUS

Código de omisión del bloqueo de activación ASM DEP

- DEP_ACTIVATION_LOCK_BYPASS_CODE
- ${device.DEP_ACTIVATION_LOCK_BYPASS_CODE

Clave de custodia ASM DEP

- DEP_ESCROW_KEY
- ${device.DEP_ESCROW_KEY

Etiqueta de inventario

- ASSET_TAG
- ${device.ASSET_TAG

Comprobar automáticamente las actualizaciones de software

- AutoCheckEnabled
- ${device.AutoCheckEnabled

Descargar automáticamente las actualizaciones de software en segundo plano

- BackgroundDownloadEnabled
- ${device.BackgroundDownloadEnabled

Instalar automáticamente las actualizaciones de aplicaciones

- AutomaticAppInstallationEnabled
- ${device.AutomaticAppInstallationEnabled

Instalar automáticamente las actualizaciones de SO

- AutomaticOSInstallationEnabled
- ${device.AutomaticOSInstallationEnabled

Instalar automáticamente las actualizaciones de seguridad

- AutomaticSecurityUpdatesEnabled
- ${device.AutomaticSecurityUpdatesEnabled

Estado de la actualización automática

- AUTOUPDATE_STATUS
- ${device.AUTOUPDATE_STATUS

RAM disponible

- MEMORY_AVAILABLE
- ${device.MEMORY_AVAILABLE

Actualizaciones de software disponibles

- AVAILABLE_OS_UPDATE_HUMAN_READABLE
- ${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE

Espacio de almacenamiento disponible

- FREEDISK
- ${device.FREEDISK

Batería de reserva

- BACKUP_BATTERY_PERCENT
- ${device.BACKUP_BATTERY_PERCENT

Versión de banda base de firmware

- MODEM_FIRMWARE_VERSION
- ${device.MODEM_FIRMWARE_VERSION

Carga de batería

- BATTERY_CHARGING_STATUS
- ${device.BATTERY_CHARGING_STATUS

Carga de batería

- BATTERY_CHARGING
- ${device.BATTERY_CHARGING

Batería restante

- BATTERY_ESTIMATED_CHARGE_REMAINING
- ${device.BATTERY_ESTIMATED_CHARGE_REMAINING

Tiempo de operación de la batería

- BATTERY_RUNTIME
- ${device.BATTERY_RUNTIME

Estado de la batería

- BATTERY_STATUS
- ${device.BATTERY_STATUS

Dispositivo BES conocido por MS

- BES_DEVICE_KNOWN_BY_ZMSP
- ${device.BES_DEVICE_KNOWN_BY_ZMSP

PIN de BES

- BES_PIN
- ${device.BES_PIN

ID del agente del servidor BES

- AGENT_ID
- ${device.AGENT_ID

Nombre del servidor BES

- BES_SERVER
- ${device.BES_SERVER

Versión del servidor BES

- BES_VERSION
- ${device.BES_VERSION

Información de BIOS

- BIOS_INFO

- ${device.BIOS_INFO

Estado de BitLocker

- WINDOWS_HAS_BIT_LOCKER_STATUS
- ${device.WINDOWS_HAS_BIT_LOCKER_STATUS

Dirección MAC de Bluetooth

- BLUETOOTH_MAC
- ${device.BLUETOOTH_MAC

¿Depuración de arranque habilitada?

- WINDOWS_HAS_BOOT_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED

BootManagerRevListVersion

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- ${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION

Código de operador

- CARRIER_CODE
- ${device.CARRIER_CODE

Versión de parámetros de operador

- CARRIER_SETTINGS_VERSION
- ${device.CARRIER_SETTINGS_VERSION

URL del catálogo

- CatalogURL
- ${device.CatalogURL

Móvil: Altitud

- GPS_ALTITUDE_FROM_CELLULAR
- ${device.GPS_ALTITUDE_FROM_CELLULAR

Móvil: Trayectoria

- GPS_COURSE_FROM_CELLULAR
- ${device.GPS_COURSE_FROM_CELLULAR

Móvil: Precisión horizontal

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR

Móvil: Latitud

- GPS_LATITUDE_FROM_CELLULAR
- ${device.GPS_LATITUDE_FROM_CELLULAR

Móvil: Longitud

- GPS_LONGITUDE_FROM_CELLULAR
- ${device.GPS_LONGITUDE_FROM_CELLULAR

Móvil: Velocidad

- GPS_SPEED_FROM_CELLULAR
- ${device.GPS_SPEED_FROM_CELLULAR

Tecnología del móvil

- CELLULAR_TECHNOLOGY
- ${device.CELLULAR_TECHNOLOGY

Móvil: Marca de hora

- GPS_TIMESTAMP_FROM_CELLULAR
- ${device.GPS_TIMESTAMP_FROM_CELLULAR

Móvil: Precisión vertical

- GPS_VERTICAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}

¿Cambiar contraseña en el siguiente inicio de sesión?

- GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN
- ${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

ID del dispositivo cliente

- CLIENT_DEVICE_ID
- ${device.CLIENT_DEVICE_ID

Copia de seguridad en nube habilitada

- CLOUD_BACKUP_ENABLED
- ${device.CLOUD_BACKUP_ENABLED

¿Integridad de código habilitada?

- WINDOWS_HAS_CODE_INTEGRITY_ENABLED
- ${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED

CodeIntegrityRevListVersion

- WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION
- ${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION

Color

- COLOR
- ${device.COLOR

Velocidad de reloj de CPU

- CPU_CLOCK_SPEED
- ${device.CPU_CLOCK_SPEED

Tipo de CPU

- CPU_TYPE
- ${device.CPU_TYPE}

Creado

- GOOGLE_AW_DIRECTORY_CREATION_TIME
- ${device.GOOGLE_AW_DIRECTORY_CREATION_TIME

Actualizaciones de software críticas

- AVAILABLE_OS_UPDATE_IS_CRITICAL
- ${device.AVAILABLE_OS_UPDATE_IS_CRITICAL

Red del operador actual

- CARRIER
- ${device.CARRIER

Código móvil de país actual

- CURRENT_MCC
- ${device.CURRENT_MCC

Código móvil de red actual

- CURRENT_MNC
- ${device.CURRENT_MNC

Itinerancia de datos permitida

- DATA_ROAMING_ENABLED
- ${device.DATA_ROAMING_ENABLED

Fecha de la última copia de seguridad en iCloud

- LAST_CLOUD_BACKUP_DATE
- ${device.LAST_CLOUD_BACKUP_DATE}

Catálogo predeterminado

- IsDefaultCatalog

- ${device.IsDefaultCatalog

Nombre de la cuenta DEP

- BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- ${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME

DEPPolicy

- WINDOWS_HAS_DEP_POLICY
- ${device.WINDOWS_HAS_DEP_POLICY

Perfil DEP asignado

- PROFILE_ASSIGN_TIME
- ${device.PROFILE_ASSIGN_TIME

Perfil DEP enviado

- PROFILE_PUSH_TIME
- ${device.PROFILE_PUSH_TIME

Perfil DEP quitado

- PROFILE_REMOVE_TIME
- ${device.PROFILE_REMOVE_TIME

Registrado en DEP por

- DEVICE_ASSIGNED_BY
- ${device.DEVICE_ASSIGNED_BY

Fecha de registro en DEP

- DEVICE_ASSIGNED_DATE
- ${device.DEVICE_ASSIGNED_DATE

Descripción

- DESCRIPCIÓN
- ${device.DESCRIPTION

Identificador de dispositivo

- Activesyncid
- ${device.activesyncid

Modelo del dispositivo

- SYSTEM_OEM
- ${device.SYSTEM_OEM

Nombre del dispositivo

- DEVICE_NAME
- ${device.DEVICE_NAME

Tipo de dispositivo

- DEVICE_TYPE
- ${device.DEVICE_TYPE

No Molestar activado

- DO_NOT_DISTURB
- ${device.DO_NOT_DISTURB

¿Controlador ELAM cargado?

- WINDOWS_HAS_ELAM_DRIVER_LOADED
- ${device.WINDOWS_HAS_ELAM_DRIVER_LOADED

Conformidad de cifrado

- ENCRYPTION_COMPLIANCE
- ${device.ENCRYPTION_COMPLIANCE

ENROLLMENT_KEY_GENERATION_DATE

- ENROLLMENT_KEY_GENERATION_DATE
- ${device.ENROLLMENT_KEY_GENERATION_DATE

ID de empresa

- ENTERPRISEID
- ${device.ENTERPRISEID

Almacenamiento externo 1: espacio disponible

- EXTERNAL_STORAGE1_FREE_SPACE
- ${device.EXTERNAL_STORAGE1_FREE_SPACE

Almacenamiento externo 1: nombre

- EXTERNAL_STORAGE1_NAME
- ${device.EXTERNAL_STORAGE1_NAME

Almacenamiento externo 1: espacio total

- EXTERNAL_STORAGE1_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE1_TOTAL_SPACE

Almacenamiento externo 2: espacio disponible

- EXTERNAL_STORAGE2_FREE_SPACE
- ${device.EXTERNAL_STORAGE2_FREE_SPACE

Almacenamiento externo 2: nombre

- EXTERNAL_STORAGE2_NAME
- ${device.EXTERNAL_STORAGE2_NAME

Almacenamiento externo 2: espacio total

- EXTERNAL_STORAGE2_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE2_TOTAL_SPACE

Almacenamiento externo cifrado

- EXTERNAL_ENCRYPTION
- ${device.EXTERNAL_ENCRYPTION

FileVault habilitado

- IS_FILEVAULT_ENABLED
- ${device.IS_FILEVAULT_ENABLED

Estado del firewall

- DEVICE_FIREWALL_STATUS
- ${device.DEVICE_FIREWALL_STATUS

Estado del firewall

- FIREWALL_STATUS
- ${device.FIREWALL_STATUS

Versión del firmware

- FIRMWARE_VERSION
- ${device.FIRMWARE_VERSION

Primera sincronización

- ZMSP_FIRST_SYNC
- ${device.ZMSP_FIRST_SYNC

Alias de Directorio Google

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- ${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS

Nombre de familia del Directorio Google

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- ${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME

Nombre del Directorio Google

- GOOGLE_AW_DIRECTORY_NAME

- ${device.GOOGLE_AW_DIRECTORY_NAME}

Correo electrónico principal de Directorio Google

- GOOGLE_AW_DIRECTORY_PRIMARY
- ${device.GOOGLE_AW_DIRECTORY_PRIMARY}

ID del usuario de Directorio Google

- GOOGLE_AW_DIRECTORY_USER_ID
- ${device.GOOGLE_AW_DIRECTORY_USER_ID}

GPS: Altitud

- GPS_ALTITUDE_FROM_GPS
- ${device.GPS_ALTITUDE_FROM_GPS

GPS: Trayectoria

- GPS_COURSE_FROM_GPS
- ${device.GPS_COURSE_FROM_GPS

GPS: Precisión horizontal

- GPS_HORIZONTAL_ACCURACY_FROM_GPS
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS

GPS: Latitud

- GPS_LATITUDE_FROM_GPS
- ${device.GPS_LATITUDE_FROM_GPS

GPS: Longitud

- GPS_LONGITUDE_FROM_GPS
- ${device.GPS_LONGITUDE_FROM_GPS

GPS: Velocidad

- GPS_SPEED_FROM_GPS
- ${device.GPS_SPEED_FROM_GPS

GPS: Marca de hora

- GPS_TIMESTAMP_FROM_GPS
- ${device.GPS_TIMESTAMP_FROM_GPS

GPS: Precisión vertical

- GPS_VERTICAL_ACCURACY_FROM_GPS
- ${device.GPS_VERTICAL_ACCURACY_FROM_GPS

ID de dispositivo de hardware

- HW_DEVICE_ID
- ${device.HW_DEVICE_ID

Capacidades de cifrado del hardware

- HARDWARE_ENCRYPTION_CAPS
- ${device.HARDWARE_ENCRYPTION_CAPS

HAS_CONTAINER

- HAS_CONTAINER
- ${device.HAS_CONTAINER

Hash de la cuenta de iTunes Store conectada actualmente

- ITUNES_STORE_ACCOUNT_HASH
- ${device.ITUNES_STORE_ACCOUNT_HASH

Red del operador local

- SIM_CARRIER_NETWORK
- ${device.SIM_CARRIER_NETWORK

Código móvil de país local

- SIM_MCC
- ${device.SIM_MCC

Código móvil de red local

- SIM_MNC
- ${device.SIM_MNC

ICCID

- ICCID
- ${device.ICCID

Identit

- AS_DEVICE_IDENTITY
- ${device.AS_DEVICE_IDENTITY

Número IMEI/MEID

- IMEI
- ${device.IMEI

IMSI

- SIM_ID
- ${device.SIM_ID

Almacenamiento interno cifrado

- LOCAL_ENCRYPTION
- ${device.LOCAL_ENCRYPTION

Localización de IP

- IP_LOCATION
- ${device.IP_LOCATION

Dirección IPv4

- IP_ADDRESSV4
- ${device.IP_ADDRESSV4

Dirección IPv6

- IP_ADDRESSV6
- ${device.IP_ADDRESSV6

IssuedAt

- WINDOWS_HAS_ISSUED_AT
- ${device.WINDOWS_HAS_ISSUED_AT

Liberado por jailbreak o rooting

- ROOT_ACCESS
- ${device.ROOT_ACCESS

¿Depuración de kernel habilitada?

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED

Modo quiosco

- IS_KIOSK
- ${device.IS_KIOSK

Última dirección IP conocida

- LAST_IP_ADDR
- ${device.LAST_IP_ADDR

Última actualización de directivas

- LAST_POLICY_UPDATE_TIME
- ${device.LAST_POLICY_UPDATE_TIME

Fecha del último examen

- PreviousScanDate

- ${device.PreviousScanDate

Resultado del último examen

- PreviousScanResult
- ${device.PreviousScanResult

Últimas actualizaciones de software programadas

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- ${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME

Último mensaje de fallo de actualizaciones de software programadas

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- ${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG

Último estado de las actualizaciones de software programadas

- AVAILABLE_OS_UPDATE_INSTALL_STATUS
- ${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS

Última sincronización

- ZMSP_LAST_SYNC
- ${device.ZMSP_LAST_SYNC

Servicio de localización habilitado

- DEVICE_LOCATOR
- ${device.DEVICE_LOCATOR

Dirección MAC

- MAC_ADDRESS
- ${device.MAC_ADDRESS

Conexión de red de la dirección MAC

- MAC_NETWORK_CONNECTION
- ${device.MAC_NETWORK_CONNECTION

Tipo de dirección MAC

- MAC_ADDRESS_TYPE
- ${device.MAC_ADDRESS_TYPE

Configuración de buzones de correo

- GOOGLE_AW_DIRECTORY_MAILBOX_SETUP
- ${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP

Batería principal

- MAIN_BATTERY_PERCENT
- ${device.MAIN_BATTERY_PERCENT

Modo perdido de MDM habilitado

- IS_MDM_LOST_MODE_ENABLED
- ${device.IS_MDM_LOST_MODE_ENABLED

MDX_SHARED_ENCRYPTION_KEY

- MDX_SHARED_ENCRYPTION_KEY
- ${device.MDX_SHARED_ENCRYPTION_KEY

MEID

- MEID
- ${device.MEID

Número de teléfono móvil

- TEL_NUMBER
- ${device.TEL_NUMBER

ID del modelo

- MODEL_ID
- ${device.MODEL_ID}

Número de modelo

- MODEL_NUMBER
- ${device.MODEL_NUMBER

Tipo de adaptador de red

- NETWORK_ADAPTER_TYPE
- ${device.NETWORK_ADAPTER_TYPE

Compilación del sistema operativo

- SYSTEM_OS_BUILD
- ${device.SYSTEM_OS_BUILD

Edición del sistema operativo

- OS_EDITION
- ${device.OS_EDITION

Idioma del sistema operativo (configuración regional)

- SYSTEM_LANGUAGE
- ${device.SYSTEM_LANGUAGE

Versión del sistema operativo

- SYSTEM_OS_VERSION
- ${device.SYSTEM_OS_VERSION

Dirección de la organización

- ORGANIZATION_ADDRESS
- ${device.ORGANIZATION_ADDRESS

Correo electrónico de la organización

- ORGANIZATION_EMAIL
- ${device.ORGANIZATION_EMAIL

Ámbito de la organización

- ORGANIZATION_MAGIC
- ${device.ORGANIZATION_MAGIC

Nombre de la organización

- ORGANIZATION_NAME
- ${device.ORGANIZATION_NAME

Número de teléfono de la organización

- ORGANIZATION_PHONE
- ${device.ORGANIZATION_PHONE

No conforme

- OUT_OF_COMPLIANCE
- ${device.OUT_OF_COMPLIANCE

Propietario

- CORPORATE_OWNED
- ${device.CORPORATE_OWNED

Código de acceso conforme

- PASSCODE_IS_COMPLIANT
- ${device.PASSCODE_IS_COMPLIANT

Código de acceso conforme con configuración

- PASSCODE_IS_COMPLIANT_WITH_CFG
- ${device.PASSCODE_IS_COMPLIANT_WITH_CFG

Código de acceso presente

- PASSCODE_PRESENT

- ${device.PASSCODE_PRESENT

PCR0

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0

Infracción de perímetro

- GPS_PERIMETER_BREACH
- ${device.GPS_PERIMETER_BREACH

Comprobación periódica

- PerformPeriodicCheck
- ${device.PerformPeriodicCheck

Personal Hotspot activado

- PERSONAL_HOTSPOT_ENABLED
- ${device.PERSONAL_HOTSPOT_ENABLED

Código PIN de la geocerca

- PIN_CODE_FOR_GEO_FENCE
- ${device.PIN_CODE_FOR_GEO_FENCE

Platform

- SYSTEM_PLATFORM
- ${device.SYSTEM_PLATFORM}

Nivel de API de la plataforma

- API_LEVEL
- ${device.API_LEVEL

Nombre de directiva

- POLICY_NAME
- ${device.POLICY_NAME

Número de teléfono principal

- IDENTITY1_PHONENUMBER
- ${device.IDENTITY1_PHONENUMBER

Operador de SIM principal

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY1_CARRIER_NETWORK_OPERATOR

ICCID de SIM principal

- IDENTITY1_ICCID
- ${device.IDENTITY1_ICCID

IMEI de la tarjeta SIM principal

- IDENTITY1_IMEI
- ${device.IDENTITY1_IMEI

IMSI de la tarjeta SIM principal

- IDENTITY1_IMSI
- ${device.IDENTITY1_IMSI

Itinerancia de la tarjeta SIM principal

- IDENTITY1_ROAMING
- ${device.IDENTITY1_ROAMING

Conformidad de la itinerancia de SIM principal

- IDENTITY1_ROAMING_COMPLIANCE
- ${device.IDENTITY1_ROAMING_COMPLIANCE

Nombre del producto

- PRODUCT_NAME
- ${device.PRODUCT_NAME

ID de dispositivo publicador

- PUBLISHER_DEVICE_ID
- ${device.PUBLISHER_DEVICE_ID

ResetCount

- WINDOWS_HAS_RESET_COUNT
- ${device.WINDOWS_HAS_RESET_COUNT

RestartCount

- WINDOWS_HAS_RESTART_COUNT
- ${device.WINDOWS_HAS_RESTART_COUNT

¿Modo seguro habilitado?

- WINDOWS_HAS_SAFE_MODE
- ${device.WINDOWS_HAS_SAFE_MODE

API de Samsung Knox disponible

- SAMSUNG_KNOX
- ${device.SAMSUNG_KNOX

Versión de API de Samsung Knox

- SAMSUNG_KNOX_VERSION
- ${device.SAMSUNG_KNOX_VERSION

Atestación de Samsung Knox

- SAMSUNG_KNOX_ATTESTED
- ${device.SAMSUNG_KNOX_ATTESTED

Fecha de actualización de atestación de Samsung Knox

- SAMSUNG_KNOX_ATT_UPDATED_TIME
- ${device.SAMSUNG_KNOX_ATT_UPDATED_TIME

API de Samsung SAFE disponible

- SAMSUNG_MDM
- ${device.SAMSUNG_MDM

Versión de API de Samsung SAFE

- SAMSUNG_MDM_VERSION
- ${device.SAMSUNG_MDM_VERSION

SBCPHash

- WINDOWS_HAS_SBCP_HASH
- ${device.WINDOWS_HAS_SBCP_HASH

Pantalla: altura

- SCREEN_HEIGHT
- ${device.SCREEN_HEIGHT

Pantalla: cantidad de colores

- SCREEN_NB_COLORS
- ${device.SCREEN_NB_COLORS

Pantalla: tamaño

- SCREEN_SIZE
- ${device.SCREEN_SIZE

Pantalla: anchura

- SCREEN_WIDTH
- ${device.SCREEN_WIDTH

Pantalla: resolución horizontal

- SCREEN_XDPI

- ${device.SCREEN_XDPI

Pantalla: resolución vertical

- SCREEN_YDPI
- ${device.SCREEN_YDPI

Número de teléfono secundario

- IDENTITY2_PHONENUMBER
- ${device.IDENTITY2_PHONENUMBER

Operador de SIM secundaria

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY2_CARRIER_NETWORK_OPERATOR

ICCID de SIM secundaria

- IDENTITY2_ICCID
- ${device.IDENTITY2_ICCID

IMEI de la tarjeta SIM secundaria

- IDENTITY2_IMEI
- ${device.IDENTITY2_IMEI

IMSI de la tarjeta SIM secundaria

- IDENTITY2_IMSI
- ${device.IDENTITY2_IMSI

Itinerancia de la tarjeta SIM secundaria

- IDENTITY2_ROAMING
- ${device.IDENTITY2_ROAMING

Conformidad de la itinerancia de SIM secundaria

- IDENTITY2_ROAMING_COMPLIANCE
- ${device.IDENTITY2_ROAMING_COMPLIANCE

¿Arranque seguro habilitado?

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- ${device.WINDOWS_HAS_SECURE_BOOT_ENABLED

Estado de Arranque seguro

- SECURE_BOOT_STATE
- ${device.SECURE_BOOT_STATE

Contenedor seguro habilitado

- DLP_ACTIVE
- ${device.DLP_ACTIVE

Nivel de revisión de seguridad

- SYSTEM_SECURITY_PATCH_LEVEL
- ${device.SYSTEM_SECURITY_PATCH_LEVEL

Número de serie

- SERIAL_NUMBER
- ${device.SERIAL_NUMBER

Capacidad para SMS

- IS_SMS_CAPABLE
- ${device.IS_SMS_CAPABLE

Supervisado

- SUPERVISED
- ${device.SUPERVISED

Motivo de suspensión

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON

Estado manipulado

- TAMPERED_STATUS
- ${device.TAMPERED_STATUS

Términos y condiciones

- TERMS_AND_CONDITIONS
- ${device.TERMS_AND_CONDITIONS

¿Contrato y términos aceptados?

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- ${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS

¿Firma de pruebas habilitada?

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- ${device.WINDOWS_HAS_TEST_SIGNING_ENABLED

Total de RAM

- MEMORY
- ${device.MEMORY

Total de espacio de almacenamiento

- TOTAL_DISK_SPACE
- ${device.TOTAL_DISK_SPACE

Versión de TPM

- TPM_VERSION
- ${device.TPM_VERSION

UDID

- UDID
- ${device.UDID}

Estado del control de cuentas de usuario

- UAC_STATUS
- ${device.UAC_STATUS

Agente de usuario

- USER_AGENT
- ${device.USER_AGENT

Definido por el usuario #1

- USER_DEFINED_1
- ${device.USER_DEFINED_1

Definido por el usuario #2

- USER_DEFINED_2
- ${device.USER_DEFINED_2

Definido por el usuario #3

- USER_DEFINED_3
- ${device.USER_DEFINED_3

Idioma del usuario (configuración regional)

- USER_LANGUAGE
- ${device.USER_LANGUAGE

Proveedor

- PROVEEDOR
- ${device.VENDOR

Capacidad para voz

- IS_VOICE_CAPABLE

- ${device.IS_VOICE_CAPABLE

Itinerancia de voz permitida

- VOICE_ROAMING_ENABLED
- ${device.VOICE_ROAMING_ENABLED

¿VSM habilitado?

- WINDOWS_HAS_VSM_ENABLED
- ${device.WINDOWS_HAS_VSM_ENABLED

Dirección MAC de Wi-Fi

- WIFI_MAC
- ${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY
- ${device.WINDOWS_ENROLLMENT_KEY

¿WinPE habilitado?

- WINDOWS_HAS_WINPE
- ${device.WINDOWS_HAS_WINPE

Estado de notificación WNS

- PROPERTY_WNS_PUSH_STATUS
- ${device.PROPERTY_WNS_PUSH_STATUS

URL de notificación WNS

- PROPERTY_WNS_PUSH_URL
- ${device.PROPERTY_WNS_PUSH_URL

Fecha de caducidad de URL de notificación WNS

- PROPERTY_WNS_PUSH_URL_EXPIRY
- ${device.PROPERTY_WNS_PUSH_URL_EXPIRY

ID del agente de XenMobile

- ENROLLMENT_AGENT_ID
- ${device.ENROLLMENT_AGENT_ID

Revisión del agente de XenMobile

- EW_REVISION
- ${device.EW_REVISION

Versión del agente de XenMobile

- EW_VERSION
- ${device.EW_VERSION

API de Zebra disponible

- ZEBRA_MDM
- ${device.ZEBRA_MDM

Versión de Zebra MXMF

- ZEBRA_MDM_VERSION
- ${device.ZEBRA_MDM_VERSION

Versión de la revisión de Zebra

- ZEBRA_PATCH_VERSION
- ${device.ZEBRA_PATCH_VERSION}

Macros para obtener propiedades integradas de usuario

Nombre simplificado	Macros
domainname (nombre de dominio; dominio predeterminado)	`${ user.domainname }`
loginname (nombre de usuario más el nombre de dominio)	`${ user.loginname }`
username (nombre de inicio de sesión menos el dominio, si existe alguno)	`${ user.username }`

Macros para todas las propiedades de usuario

Nombre simplificado	Elemento web	Macros
Intentos fallidos de inicio de sesión en Active Directory	badpwdcount	`${ user.badpwdcount }`
Correo electrónico de usuario de ActiveSync	asuseremail	`${ user.asuseremail }`
Origen de datos de ASM	asmpersonsource	`${ user.asmpersonsource }`
Nombre de la cuenta ASM DEP	asmdepaccount	`${ user.asmdepaccount }`

Nombre simplificado	Elemento web	Macros
ID de Apple administrado por ASM	asmpersonmanagedappleid	${ user.asmpersonmanagedappleid }
Tipo de código de acceso de ASM	asmpersonpasscodetype	${ user.asmpersonpasscodetype }
ID personal de ASM	asmpersonid	${ user.asmpersonid }
Estado personal de ASM	asmpersonstatus	${ user.asmpersonstatus }
Título personal de ASM	asmpersontitle	${ user.asmpersontitle }
ID personal único de ASM	asmpersonuniqueid	${ user.asmpersonuniqueid }
ID del sistema de origen de ASM	asmpersonsourcesystemid	${ user.asmpersonsourcesystemid }
Curso del estudiante de ASM	asmpersongrade	${ user.asmpersongrade }
Correo electrónico de usuario de BES	besuseremail	${ user.besuseremail }
Empresa	company	${ user.company }
Nombre de la empresa	companyname	${ user.companyname }
País	c	${ user.c }
Departamento	department	${ user.department }
Descripción	description	${ user.description }
Usuario inhabilitado	disableduser	${ user.disableduser }
Nombre simplificado	nombre simplificado	${ user.displayname }
Nombre distintivo	distinguishedname	${ user.distinguishedname }
Nombre del dominio	domainname	${ user.domainname }
Correo electrónico	mail	${ user.mail }
Nombre de pila	givenname	${ user.givenname }

Nombre simplificado	Elemento web	Macros
Dirección del domicilio	homestreetaddress	${ user.homestreetaddress }
Ciudad del domicilio	homecity	${ user.homecity }
País del domicilio	homecountry	${ user.homecountry }
Fax del domicilio	homefax	${ user.homefax }
Teléfono del domicilio	homephone	${ user.homephone }
Estado/región del domicilio	homestate	${ user.homestate }
Código postal del domicilio	homezip	${ user.homezip }
Teléfono IP	ipphone	${ user.ipphone }
Iniciales	middleinitial	${ user.middleinitial }
Segundo nombre	middlename	${ user.middlename }
Móvil	mobile	${ user.mobile }
Nombre	cn	${ user.cn }
Dirección de la oficina	physicaldeliveryofficename	${ user.physicaldeliveryofficename }
Ciudad de la oficina	l	${ user.l }
Fax de la oficina	facsimiletelephonenumber	${ user.facsimiletelephonenumber }
Estado/provincia de la oficina	st	${ user.st }
Calle de la oficina	officestreetaddress	${ user.officestreetaddress }
Teléfono de la oficina	telephonenumber	${ user.telephonenumber }
Código postal de la oficina	postalcode	${ user.postalcode }
Apartado de correos	postofficebox	${ user.postofficebox }
Buscapersonas	pager	${ user.pager }
ID de grupo principal	primarygroupid	${ user.primarygroupid }

Nombre simplificado	Elemento web	Macros
Cuenta SAM	samaccountname	`${ user.samaccountname }`
Calle	streetaddress	`${ user.streetaddress }`
Apellido	sn	`${ user.sn }`
Título	title	`${ user.title }`
Nombre de inicio de sesión del usuario	userprincipalname	`${ user.userprincipalname }`

Acciones automatizadas

January 4, 2022

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 crea una acción automatizada, los desencadenantes definidos para la acción determinan qué sucede en el dispositivo del usuario cuando este se conecta a XenMobile. Cuando un evento tiene lugar, usted puede enviar una notificación al usuario para que este corrija el problema antes de tomar medidas más terminantes.

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.

Las acciones de bloqueo y borrado de aplicaciones solo se pueden configurar en el modo de solo MAM.

> **Nota:**
>
> Para poder notificar a los usuarios, primero debe configurar servidores de notificaciones en los parámetros de XenMobile para SMTP y SMS, de modo que XenMobile pueda enviar los mensajes. Para obtener más información, consulte Notificaciones. Además, deberá configurar las plantillas de notificaciones que vaya a utilizar antes de continuar. Para obtener información detallada, consulte Crear y actualizar plantillas de notificaciones.

Acciones de ejemplo

Estos son algunos ejemplos del uso de acciones automatizadas:

Ejemplo 1

- Quiere detectar una aplicación que ha bloqueado previamente (por ejemplo, “Words with Friends”). Puede especificar un desencadenante que establezca el dispositivo del usuario como no conforme si se detecta la aplicación “Words with Friends”. La acción notifica a dicho usuario de que debe quitar la aplicación para que su dispositivo vuelva a la conformidad. También puede establecer un límite de tiempo de espera para que los usuarios realicen las acciones correctivas pertinentes. Después de ese límite de tiempo, se produce la acción definida (como borrar selectivamente el dispositivo).

Ejemplo 2

- Quiere verificar si los clientes están utilizando el firmware más reciente y bloquear el acceso a los recursos si los usuarios no tienen sus dispositivos actualizados. Puede especificar un desencadenante que establezca el dispositivo de usuario como no conforme cuando este no tenga la versión más reciente. Utilice las acciones automatizadas para bloquear recursos y notificar a los clientes.

Ejemplo tres

- Un dispositivo de usuario se establece en el estado no conforme y el usuario corrige el problema con el dispositivo. Puede configurar una directiva para implementar un paquete que restablezca el dispositivo al estado conforme.

Ejemplo cuatro

- Quiere marcar como no conformes los dispositivos de usuario que han estado inactivos durante un período de tiempo determinado. Puede crear una acción automatizada para dispositivos inactivos de la siguiente manera:

  1. En la consola de XenMobile, vaya a **Parámetros > Control de acceso de red** y, a continuación, seleccione **Dispositivos inactivos**. Para obtener información sobre el parámetro **Dispositivos inactivos**, consulte Control de acceso de red.
  2. Siga los pasos para agregar una acción, tal y como se describe en Agregar y administrar acciones. La única diferencia es que configura los parámetros siguientes en la página **Detalles de la acción**:
     - **Desencadenante**. Seleccione **Propiedad del dispositivo**, **No conforme** y **Verdadero**.
     - **Acción**. Seleccione **Enviar notificación** y, a continuación, una plantilla que haya creado con **Plantilla de notificación** en **Parámetros**. A continuación, establezca la demora en días, horas o minutos antes de realizar la acción. Establezca el intervalo

durante el que se repite la acción hasta que el usuario solucione el problema que ha provocado la activación del desencadenante.

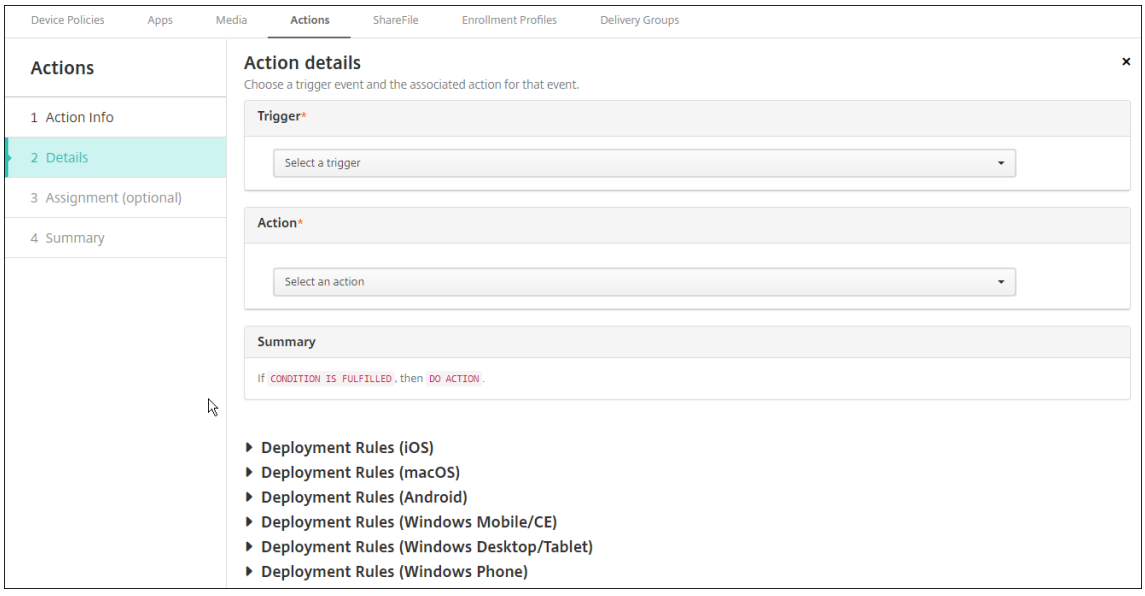
> **Sugerencia:**
>
> Para eliminar dispositivos inactivos en bloque, use la API pública para servicios REST. Obtenga, en primer lugar, el ID de dispositivo de los dispositivos inactivos que quiere eliminar y, a continuación, ejecute la API de eliminación para eliminarlos en bloque.

Agregar y administrar acciones

Para agregar, modificar y filtrar acciones automatizadas:

1. En la consola de XenMobile, haga clic en **Configurar > Acciones**. Aparecerá la página **Acciones**.
2. En la página **Acciones**, lleve a cabo alguna de estas acciones:
   - Haga clic en **Agregar** para agregar una acción.
   - Seleccione una acción existente para modificarla o eliminarla. Haga clic en la opción pertinente.
3. Aparecerá la página **Información de la acción**.
4. En la página **Información de la acción**, escriba o modifique la información siguiente:
   - **Nombre:** Escriba un nombre para identificar la acción. Este campo es obligatorio.
   - **Descripción:** Describa qué debe hacer la acción.
5. Haga clic en **Siguiente**. Aparecerá la página **Detalles de la acción**.

   En el siguiente ejemplo, se muestra cómo configurar un desencadenante de **eventos**. Si selecciona otro desencadenante, las opciones resultantes difieren de las mostradas aquí.



6. En la página **Detalles de la acción**, escriba o modifique la información siguiente:

   En la lista **Desencadenante**, haga clic en el tipo de desencadenante de eventos para esta acción. El significado de cada desencadenante es el siguiente:

   - **Evento:** Reacciona ante un evento determinado.
   - **Propiedad del dispositivo:** Consulta un atributo en un dispositivo administrado por MDM y, a continuación, reacciona ante él. Para obtener más información, consulte Valores y nombres de propiedades de dispositivo.
   - **Propiedad del usuario:** Reacciona ante un atributo de usuario, generalmente de Active Directory.
   - **Nombre de la aplicación instalada:** Reacciona ante una aplicación instalada. No se aplica al modo solo MAM. Requiere que la directiva "Inventario de aplicaciones" esté habilitada en el dispositivo. De forma predeterminada, la directiva "Inventario de aplicaciones" está habilitada en todas las plataformas. Para obtener más información, consulte Directiva de inventario de aplicaciones.

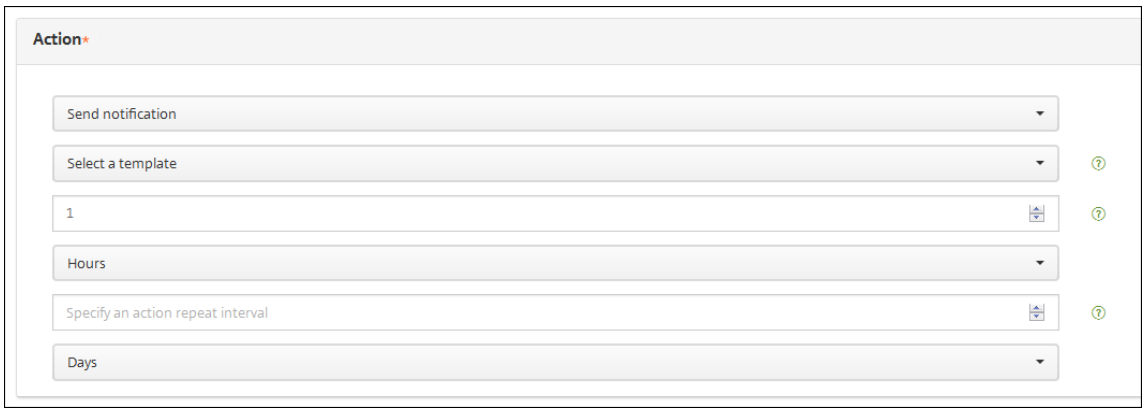
7. En la siguiente lista, haga clic en la respuesta del desencadenante.

8. En la lista **Acción**, haga clic en la acción que se debe realizar cuando se cumplan los criterios del desencadenante. A excepción de **Enviar notificación**, puede elegir un intervalo de tiempo en que los usuarios puedan resolver el problema que haya activado el desencadenante. Si el problema no se resuelve en ese período de tiempo, se llevará a cabo la acción seleccionada. Para ver la definición de las acciones, consulte Acciones de seguridad.

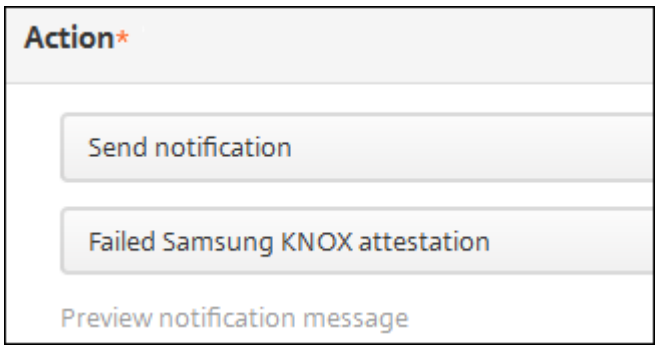
   Si elige **Enviar notificación**, use los siguientes pasos para enviar una acción de notificación.

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 en **Plantilla de notificación**, en **Parámetros**.

   Para poder notificar a los usuarios, primero debe configurar servidores de notificaciones en "Parámetros" para SMTP y SMS, de modo que XenMobile pueda enviar los mensajes; consulte Notificaciones. Además, deberá configurar las plantillas de notificaciones que vaya a utilizar antes de continuar. Para obtener más información acerca de la configuración de las plantillas de notificaciones, consulte Crear y actualizar plantillas de notificaciones.



Después de seleccionar la plantilla, puede obtener una vista previa de la notificación cuando hace clic en **Vista previa del mensaje de notificación**.



10. En los siguientes campos, configure la demora en días, horas o minutos antes de realizar la acción. Establezca el intervalo durante el que se repite la acción hasta que el usuario solucione el problema que ha provocado la activación del desencadenante.

11. En **Resumen**, verifique que la acción automatizada que ha creado es la acción esperada.

12. Después de configurar los datos de la acción, puede configurar las reglas de implementación para cada plataforma individualmente. Para ello, siga el paso 13 para cada plataforma seleccionada.

13. Configure las reglas de implementación. Para obtener más información sobre cómo configurar las reglas de implementación, consulte Implementar recursos.

    Para este ejemplo:

    - La propiedad del dispositivo debe ser **BYOD**.
    - El cifrado local del dispositivo debe ser **True**.
    - El dispositivo debe ser conforme con el código de acceso.
    - El código de país móvil del dispositivo no puede ser solo Andorra.

14. Tras configurar las reglas de implementación de las plataformas para la acción, haga clic en **Siguiente**. Aparecerá la página de **asignaciones de acciones**, en la que puede asignar la acción a un grupo o grupos de entrega. Este paso es opcional.

15. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione grupos de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.

16. Expanda Programación de implementación y, a continuación, configure estos parámetros:

    - Junto a **Implementar**, haga clic en **Sí** para programar la implementación, o bien, haga clic en **No** para cancelarla. De forma predeterminada, está **activado**. Si elige **No**, no habrá ninguna otra opción a configurar.
    - Junto a **Programación de implementación**, haga clic en **Ahora** o en **Más tarde**. La opción predeterminada es **Ahora**.
    - Si hace clic en **Más tarde**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
    - Junto a **Condición de implementación**, puede hacer clic en **En cada conexión** o en **Solo cuando haya fallado la implementación anterior**. La opción predeterminada es **En cada conexión**.
    - Junto a **Implementar para conexiones permanentes**, haga clic en **Sí** o **No**. Está **desactivado** de forma predeterminada.

      Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Parámetros > Propiedades de servidor**. La opción "Implementar para conexiones permanentes" 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 **Implementar para conexiones permanentes**, que no se aplicará para iOS.

17. Haga clic en **Siguiente**. Aparecerá la página **Resumen**, donde puede comprobar la configuración de la acción.

18. Haga clic en **Guardar** 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 desencadenantes 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 **Configurar > Acciones**.
2. En la página **Acciones**, haga clic en **Agregar**.
3. En la página **Información de la acción**, escriba un nombre para la acción y una descripción opcional.
4. En la página **Detalles de la acción**, seleccione el desencadenante pertinente.
5. En **Acción**, seleccione una acción.

   Para este paso, no olvide las siguientes condiciones:

   Si el tipo de desencadenante es **Evento**, pero el valor no es **Usuario de Active Directory inhabilitado**, las acciones **Borrado de aplicaciones** y **Bloqueo de aplicaciones** no aparecerán.

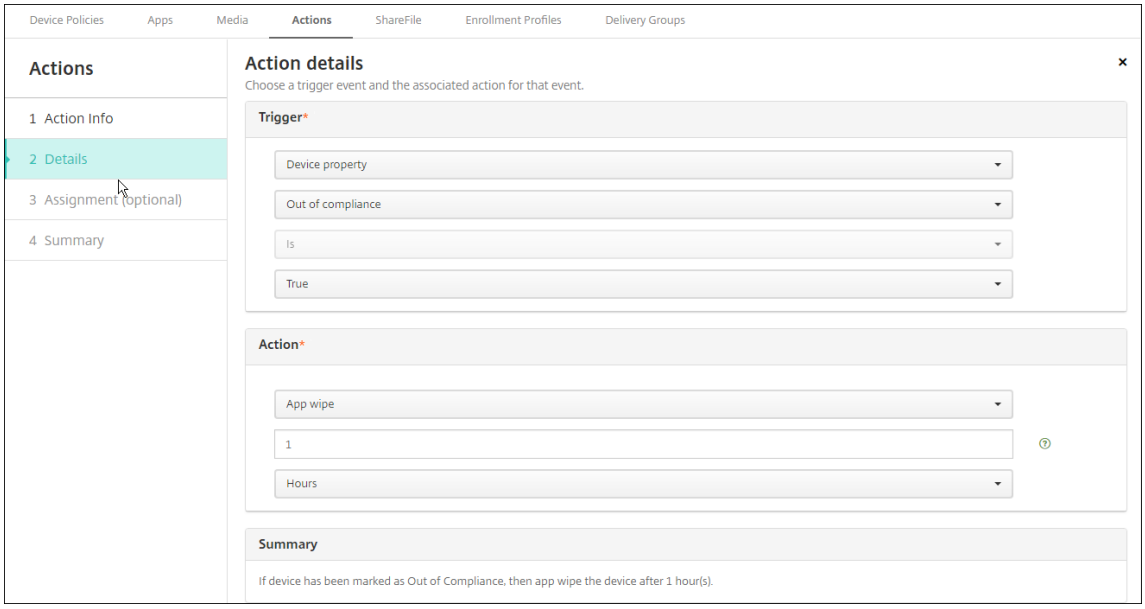
   Si el tipo de desencadenante es **Propiedad del dispositivo** y el valor es **Modo perdido de MDM habilitado**, aparecerán las siguientes acciones:

   - 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 intención de la demora es dar tiempo a los usuarios para solucionar el problema antes de que ocurra la acción. Para obtener más información sobre las acciones Borrado de aplicaciones y Bloqueo de aplicaciones, consulte Acciones de seguridad.

   > **Nota:**
   >
   > Si establece el desencadenante en **Evento**, 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.

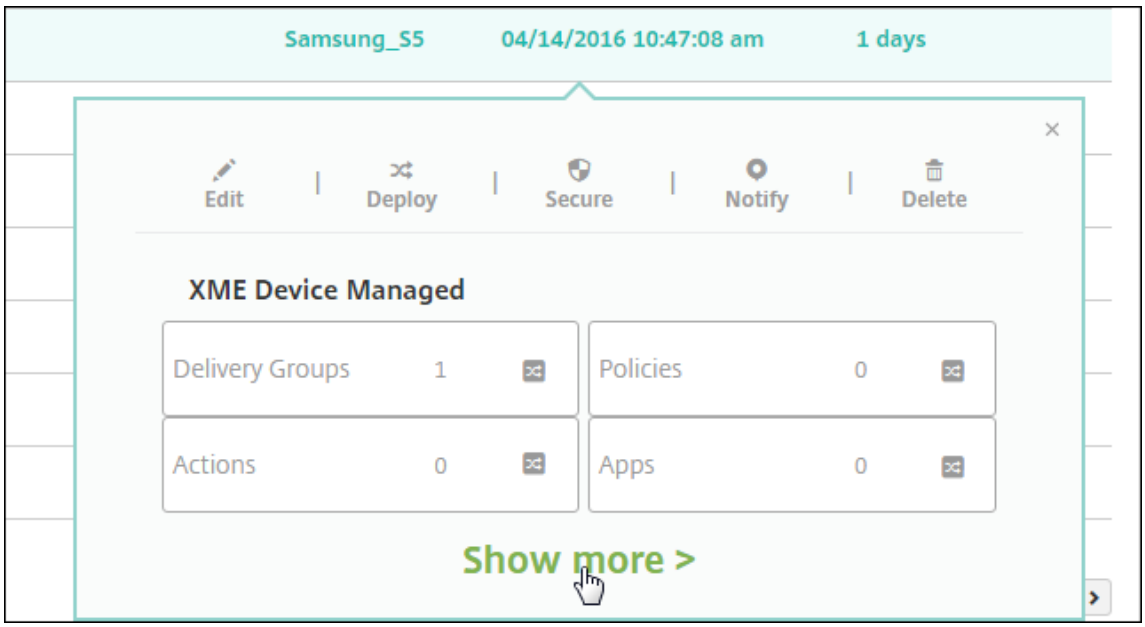
> También es posible que exista una demora de aproximadamente una hora antes de que la acción se lleve a cabo, para permitir que la base de datos de Active Directory se sincronice con XenMobile.



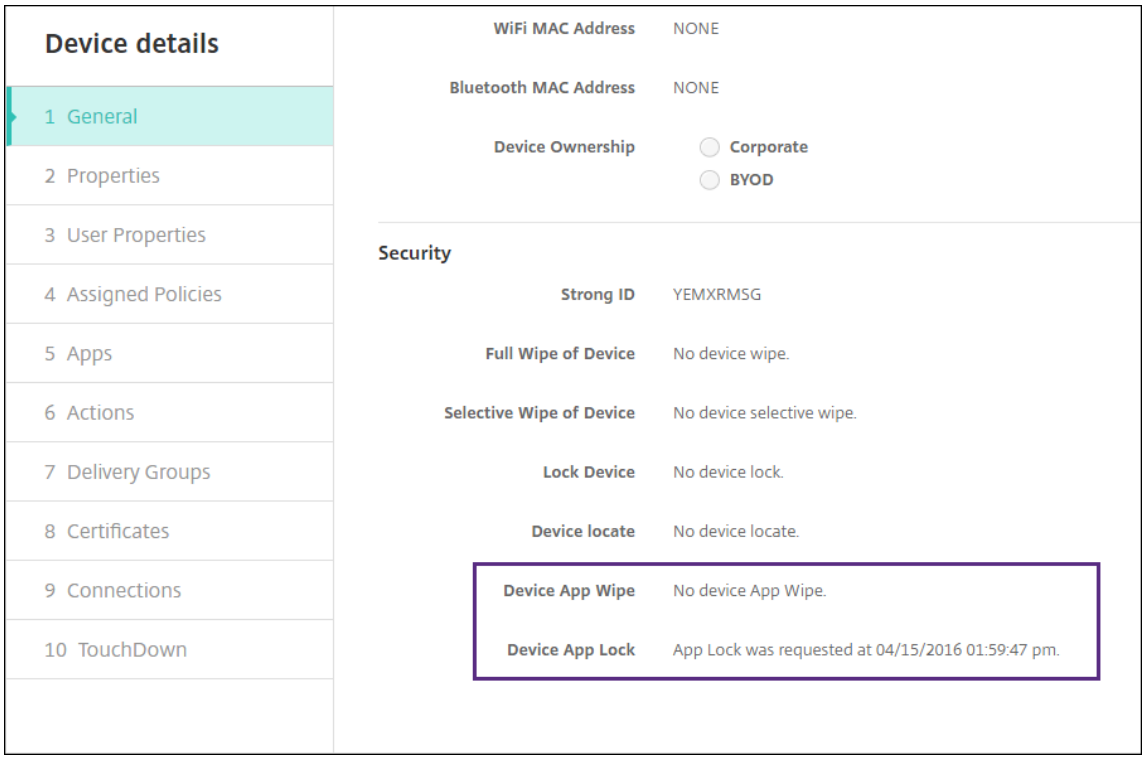
6. Configure las reglas de implementación y, a continuación, haga clic en **Siguiente**.
7. Configure las asignaciones de los grupos de entrega y una programación de la implementación. A continuación, haga clic en **Siguiente**.
8. Haga clic en **Guardar**.

Para comprobar el estado del bloqueo o borrado de las aplicaciones

1. Vaya a **Administrar > Dispositivos**, haga clic en un dispositivo y haga clic en **Mostrar más**.



2. Vaya a **Borrado de aplicaciones de dispositivo** y **Bloqueo de aplicaciones de dispositivo**.



Después de borrarse un dispositivo, se solicita al usuario que introduzca un código PIN. Si el usuario no consigue recordar el código, usted puede buscarlo en “Detalles del dispositivo”.

Supervisar y ofrecer asistencia

January 4, 2022

Puede utilizar el panel de mandos de XenMobile y la página “Asistencia” de XenMobile para supervisar y solucionar los problemas que presente su servidor de XenMobile Server. Use la página “Asistencia” de XenMobile para acceder a un repertorio de datos y herramientas relacionadas con la asistencia.

Para un servidor de XenMobile Server local, también puede realizar acciones desde la CLI de XenMobile. Para obtener información más detallada, consulte Opciones de la interfaz de línea de comandos.

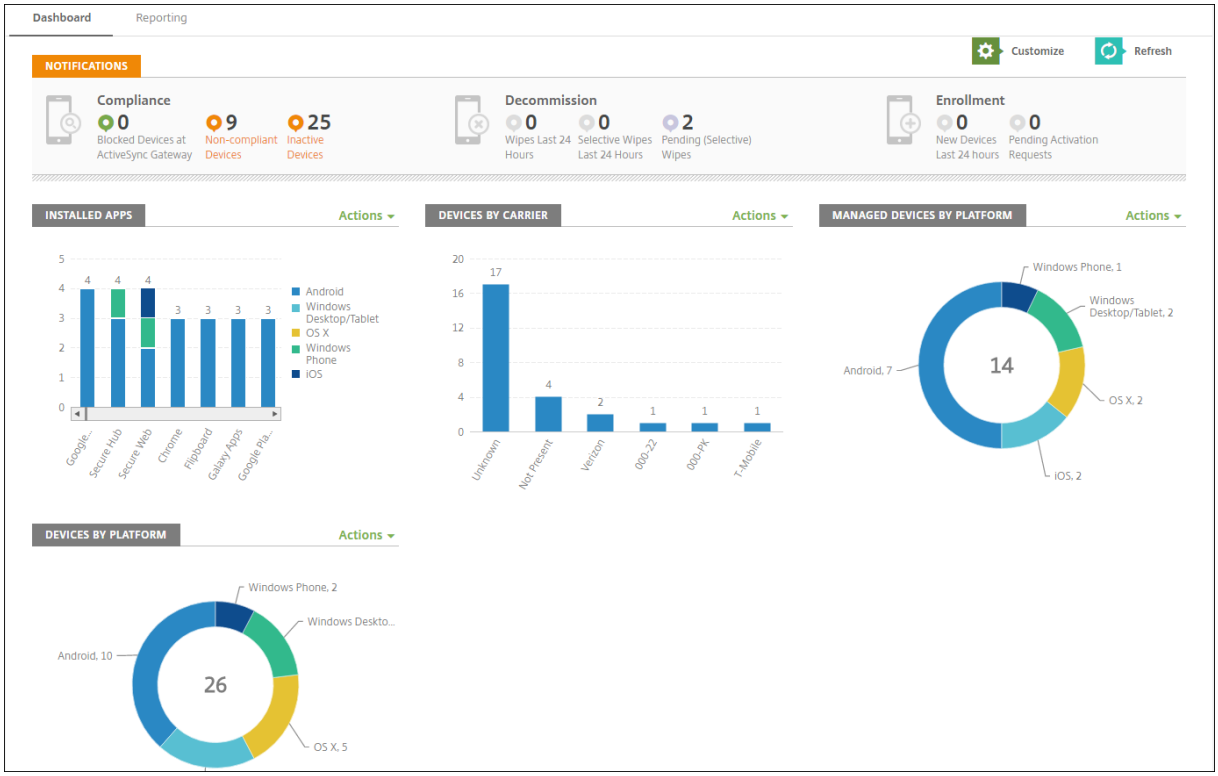
En la consola de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha.

Aparece la página Solución de problemas y asistencia.

Use la página **Asistencia** de XenMobile para:

- Acceder a datos de diagnóstico.
- Crear paquetes de asistencia (solo para instalaciones locales).
- Acceder a enlaces que llevan a la documentación de productos y al Knowledge Center de Citrix.
- Acceder a operaciones con registros.
- Utilizar las opciones de configuración avanzada.
- Acceder a un conjunto de herramientas y utilidades

Asimismo, puede ver toda la información de un vistazo desde su panel de mandos en la consola de XenMobile. En esta información, puede utilizar widgets para ver rápidamente los problemas y las operaciones correctas que se hayan producido.



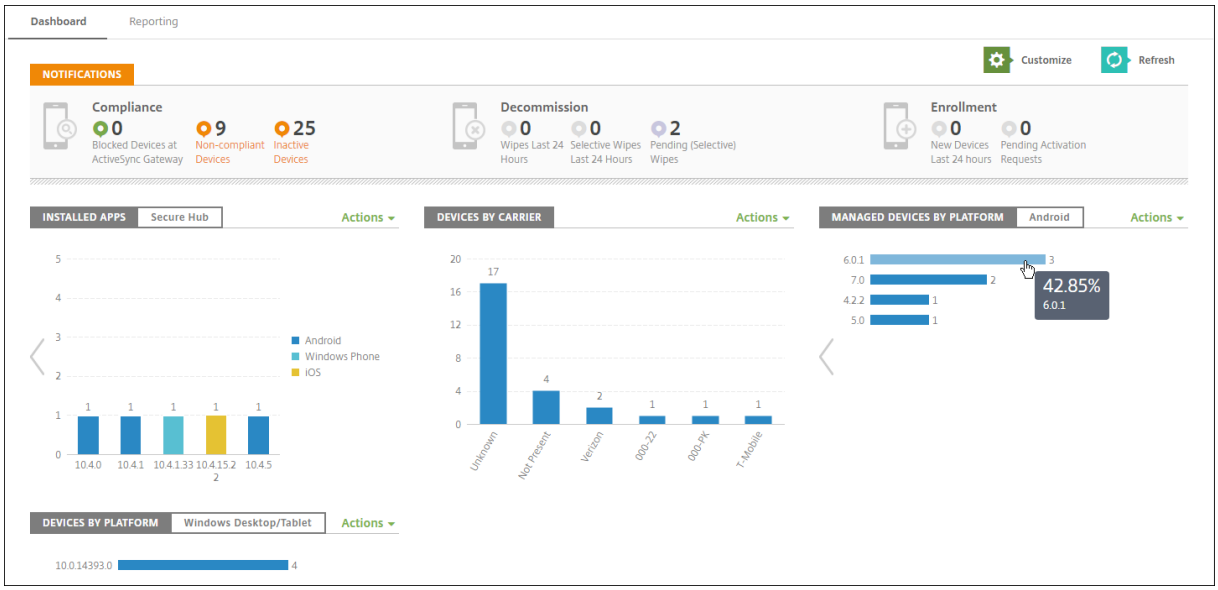
Por regla general, el panel de mandos es la pantalla que aparece al iniciar sesión por primera vez en la consola de XenMobile. Para acceder al panel de mandos desde cualquier otro sitio de la consola, haga clic en **Analizar**. Haga clic en **Personalizar** en el panel de mandos para modificar el diseño de la página y para modificar los widgets que aparecen.

- **Mis paneles de mandos:** Puede guardar hasta cuatro paneles de mandos diferentes. Puede seleccionar cada panel guardado para verlo y modificarlo por separado.
- **Estilo de diseño:** En esta fila, puede seleccionar la cantidad de widgets que aparecerán en el panel de mandos y cómo se etiquetarán.
- **Selección de widget:** Puede elegir qué información se mostrará en el panel de mandos.
  - **Notificaciones:** Marque la casilla situada encima de los números en la parte izquierda para agregar una barra de notificaciones encima de los widgets. Esta barra muestra la cantidad de dispositivos conformes, dispositivos inactivos, dispositivos borrados o dispositivos inscritos en las últimas 24 horas.
  - **Dispositivos por plataforma:** Muestra la cantidad de dispositivos administrados y no administrados por plataforma.
  - **Dispositivos por operador:** Muestra la cantidad de dispositivos administrados y no administrados por operador. Haga clic en cada barra para ver un desglose por plataforma.
  - **Dispositivos administrados por plataforma:** Muestra la cantidad de dispositivos administrados por plataforma.
  - **Dispositivos no administrados por plataforma:** Muestra la cantidad de dispositivos no administrados por plataforma. Los dispositivos que aparecen en este gráfico pueden tener

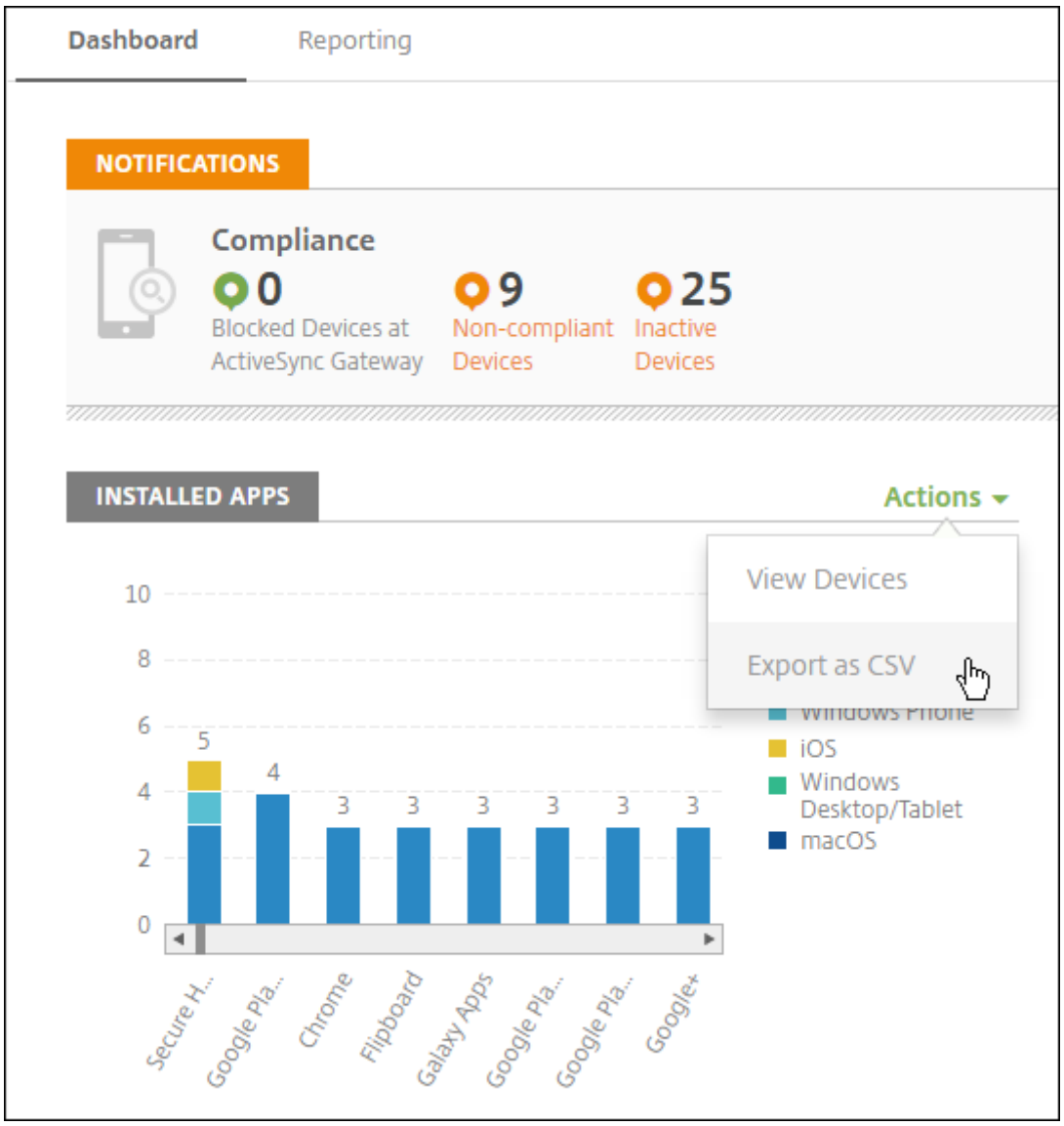
un agente instalado, pero se podrían haber borrado o revocado sus privilegios.

- **Dispositivos por estado de ActiveSync Gateway:** Muestra la cantidad de dispositivos agrupados por estado de ActiveSync Gateway. La información se muestra como estado Bloqueado, Permitido o Desconocido. Puede hacer clic en cada barra para desglosar los datos por plataforma.
- **Dispositivos por propietario:** Muestra la cantidad de dispositivos agrupados por propietario. La información se muestra como propiedad de la empresa, del empleado o de propietario desconocido.
- **Implementaciones fallidas de grupos de entrega:** Muestra la cantidad total de implementaciones fallidas desglosadas por paquete. Solo se muestran los paquetes de implementaciones con errores.
- **Dispositivos por motivo de bloqueo:** Muestra la cantidad de dispositivos bloqueados por ActiveSync.
- **Aplicaciones instaladas:** Escriba un nombre de aplicación para ver un gráfico de información de esta.
- **Uso de licencias de aplicaciones de compras por volumen:** Muestra estadísticas sobre el uso de licencias por parte de las aplicaciones de compras por volumen de Apple.

En cada widget, puede hacer clic en partes individuales para ampliar la información mostrada.



También puede exportar la información como archivo .csv. Para ello, haga clic en la lista desplegable **Acciones**.



Anonimato de datos en paquetes de asistencia

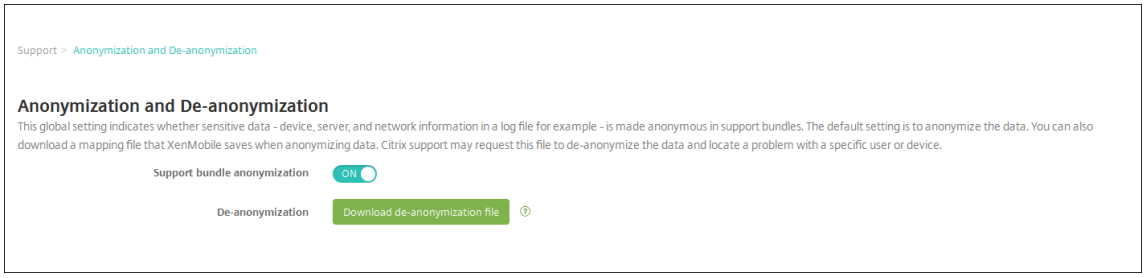
January 4, 2022

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 "Anonimización y reidentificación". 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 **Asistencia**.

2. En la página **Asistencia**, en **Avanzado**, haga clic en **Anonimización y reidentificación**. Aparecerá la página **Anonimización y reidentificación**.



3. En **Anonimización de paquetes de asistencia**, seleccione si los datos pasan a ser anónimos. De forma predeterminada, está **activado**.
4. Junto a **Reidentificación**, haga clic en **Descargar archivo de reidentificación** 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.

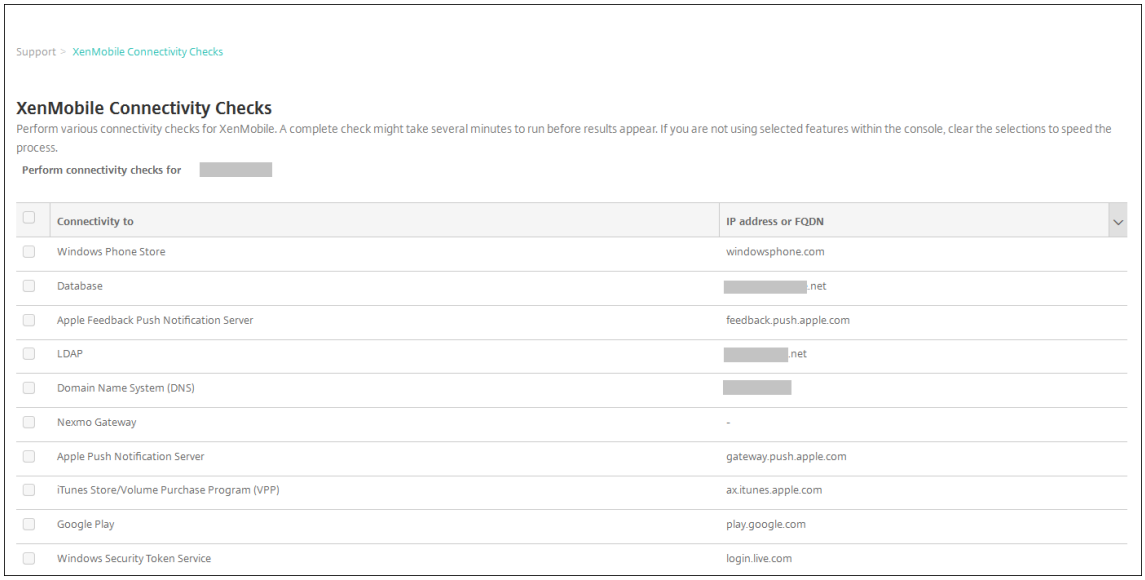
Comprobaciones de conectividad

November 6, 2020

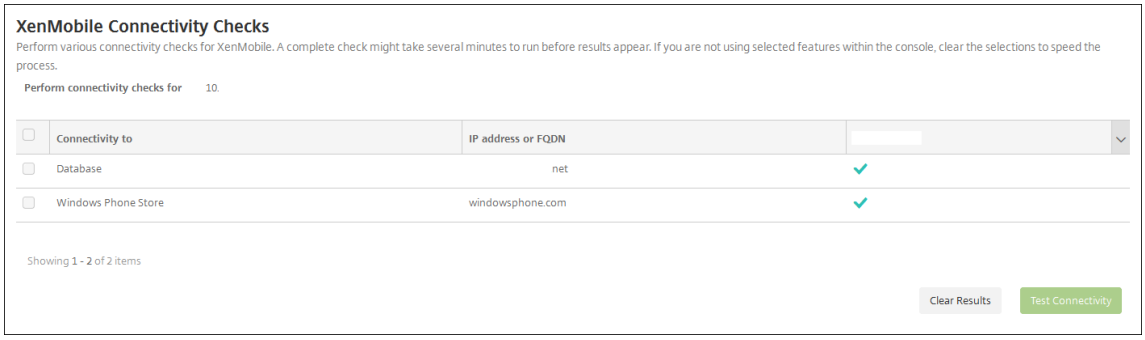
En la página **Asistencia** de XenMobile, puede comprobar la conexión de XenMobile con Citrix Gateway y con otros servidores y ubicaciones.

Comprobaciones de conectividad de XenMobile

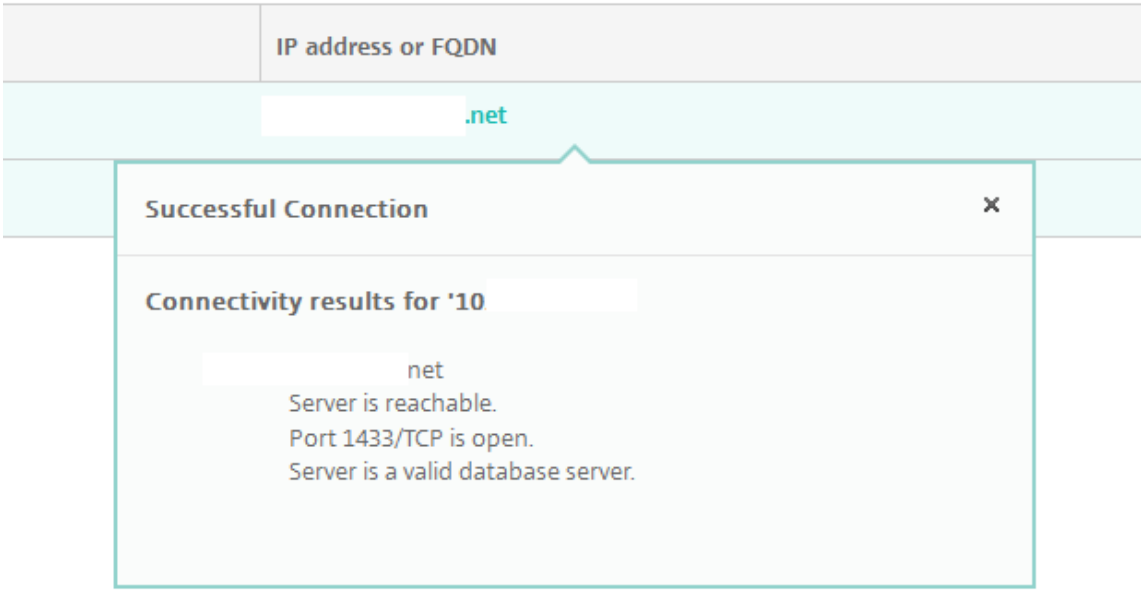
1. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha de la consola. Aparecerá la página **Asistencia**.
2. En **Diagnósticos**, haga clic en **Comprobaciones de conectividad de XenMobile**. Aparecerá la página **Comprobaciones de conectividad de XenMobile**. Si su entorno de XenMobile contiene nodos en clúster, se muestran todos los nodos.



3. Seleccione los servidores a incluir en la prueba de conectividad y, a continuación, haga clic en **Probar conectividad**. Aparecerá la página de resultados de pruebas.

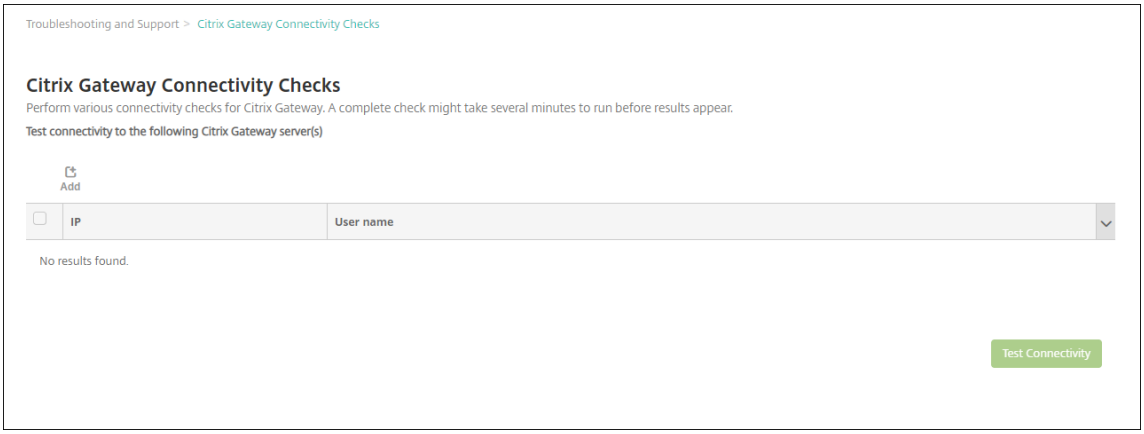


4. Seleccione un servidor de la tabla para ver los resultados detallados de dicho servidor.

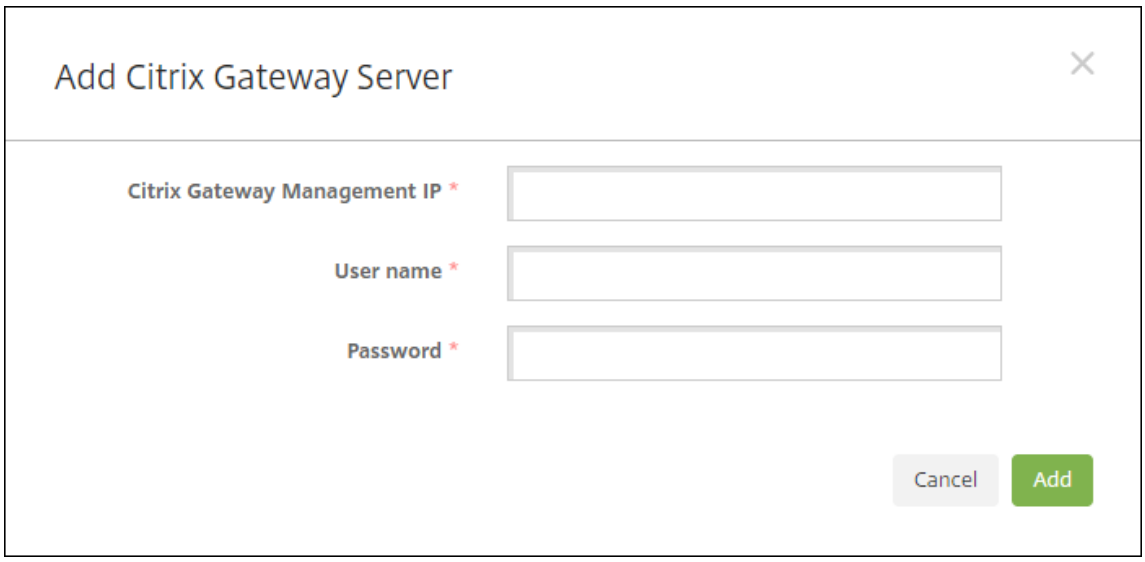


Comprobaciones de conectividad de Citrix Gateway

1. En la página **Asistencia**, en **Diagnósticos**, haga clic en **Comprobaciones de conectividad de Citrix Gateway**. Aparecerá la página **Comprobaciones de conectividad de Citrix Gateway**. La tabla está vacía si no ha agregado servidores de Citrix Gateway.



2. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar un servidor de Citrix Gateway**.



3. En **IP de administración de Citrix Gateway**, escriba la dirección IP de administración del servidor con Citrix Gateway que quiere probar.

   > **Nota:**
   >
   > Si está llevando a cabo la comprobación de conectividad de un servidor de Citrix Gateway que ya se ha agregado, se proporciona la dirección IP.

4. Escriba las credenciales de administrador de este servidor de Citrix Gateway.

   > **Nota:**
   >
   > Si está llevando a cabo la comprobación de conectividad de un servidor de Citrix Gateway que ya se ha agregado, se proporciona el nombre de usuario.

5. Haga clic en **Agregar**. El servidor de Citrix Gateway se agrega a la tabla que se encuentra en la página **Comprobaciones de conectividad de Citrix Gateway**.
6. Seleccione el servidor de Citrix Gateway y, a continuación, haga clic en **Probar conectividad**. Los resultados aparecerán en la tabla “Resultados de la prueba”.
7. Seleccione un servidor de la tabla para ver los resultados detallados de dicho servidor.

Customer Experience Improvement Program

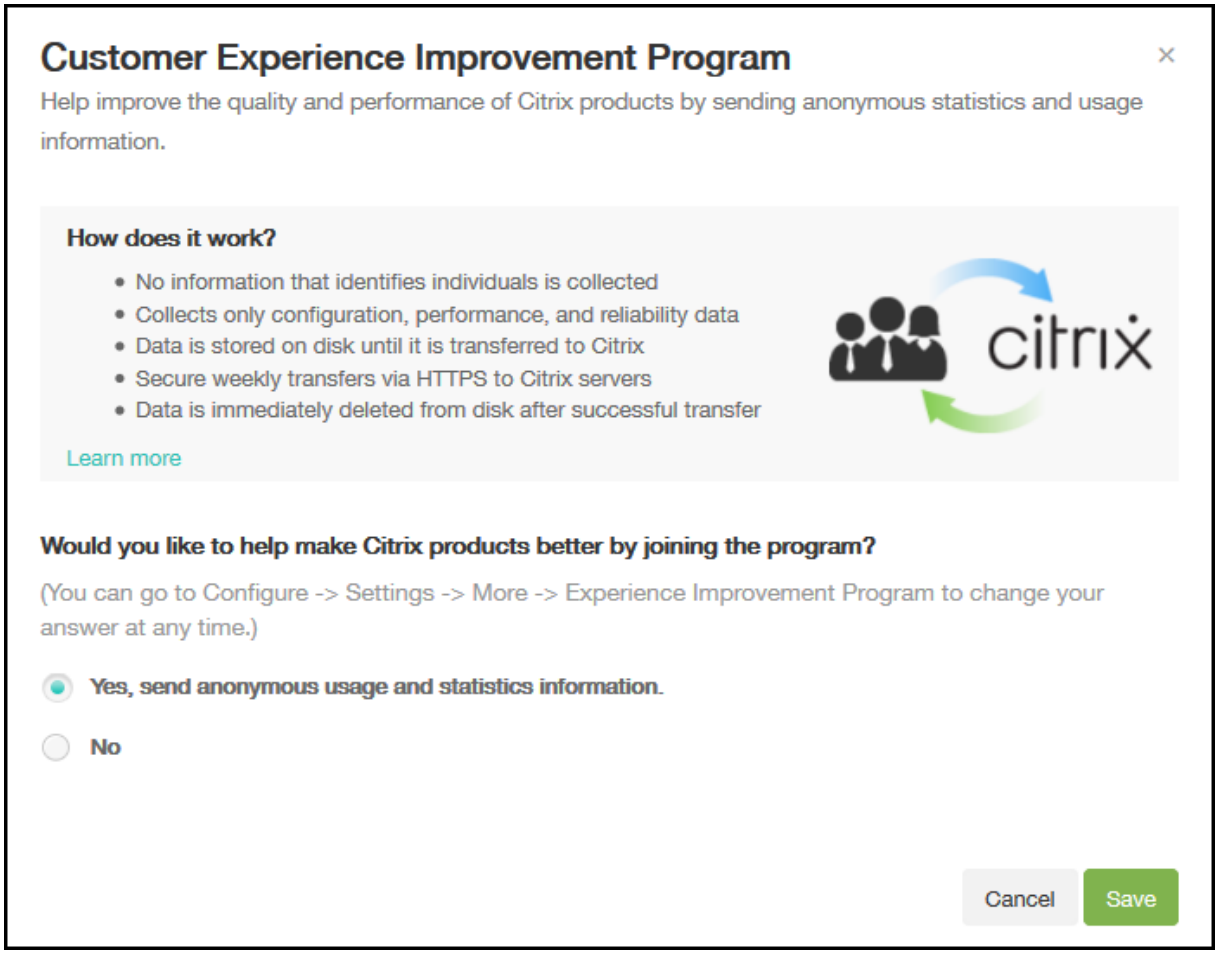
January 4, 2022

El programa para la mejora de la experiencia del usuario de Citrix (Customer Experience Improvement Program o CEIP) recopila información anónima de uso y de configuración de XenMobile y envía esos datos automáticamente a Citrix. Esos datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el

rendimiento de XenMobile. La participación en el programa CEIP es voluntaria. La opción de participar en el programa CEIP se ofrece la primera vez que se instala XenMobile o una actualización. Si participa en el programa, los datos de configuración se recopilan normalmente una vez por semana, mientras que los datos de uso y rendimiento se recopilan cada hora. Los datos se guardan en disco y se transfieren de manera segura vía HTTPS a Citrix una vez por semana. Puede cambiar la participación en el programa CEIP en la consola de XenMobile. Para obtener más información acerca del programa para la mejora de la experiencia del usuario, consulte Acerca del programa Customer Experience Improvement Program de Citrix (CEIP).

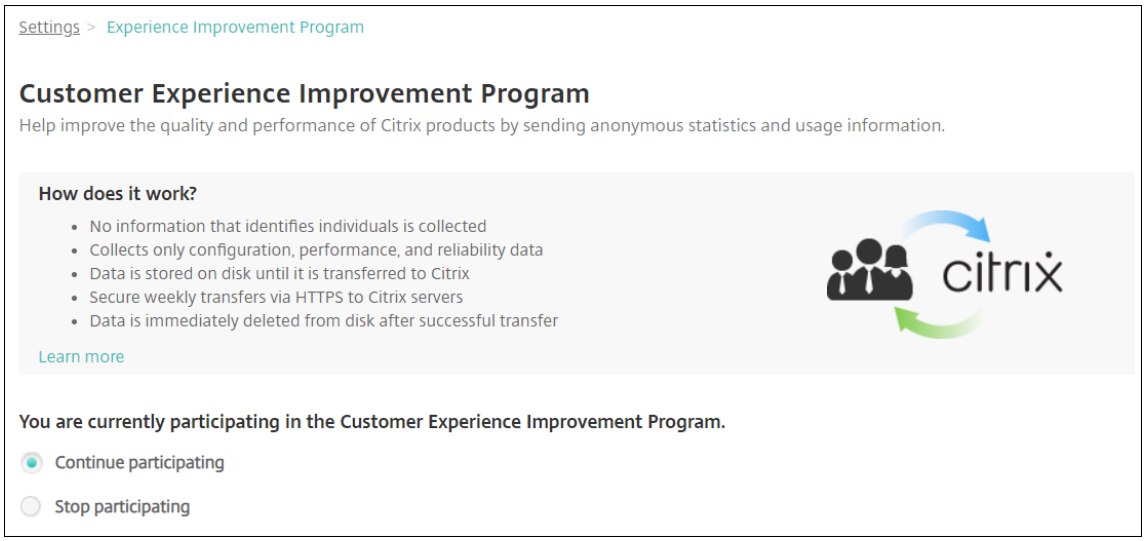
Participación optativa en el programa CEIP

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.



Cambiar el parámetro de participación en el programa CEIP

1. Para cambiar la 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 **Parámetros**.
2. En **Servidor**, haga clic en **Experience Improvement Program**. Aparecerá la página **Customer Experience Improvement Program**. La página exacta que vea depende de si participa actualmente en el programa CEIP.



3. Si participa actualmente en el programa CEIP y quiere dejar de hacerlo, haga clic en **Detener participación**.
4. Si no participa actualmente en el programa CEIP y quiere hacerlo, haga clic en **Iniciar participación**.
5. Haga clic en **Guardar**.

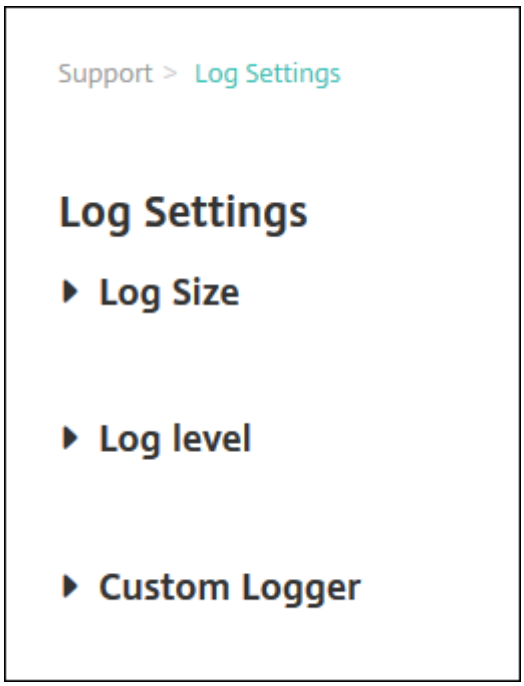
Registros

January 4, 2022

Puede configurar los parámetros de captura de registros para personalizar los registros que genera XenMobile. Si tiene un clúster de servidores de 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 **Asistencia**.

2. En **Operaciones con registros**, haga clic en **Parámetros de registros**. Aparecerá la página **Parámetros de registro**.

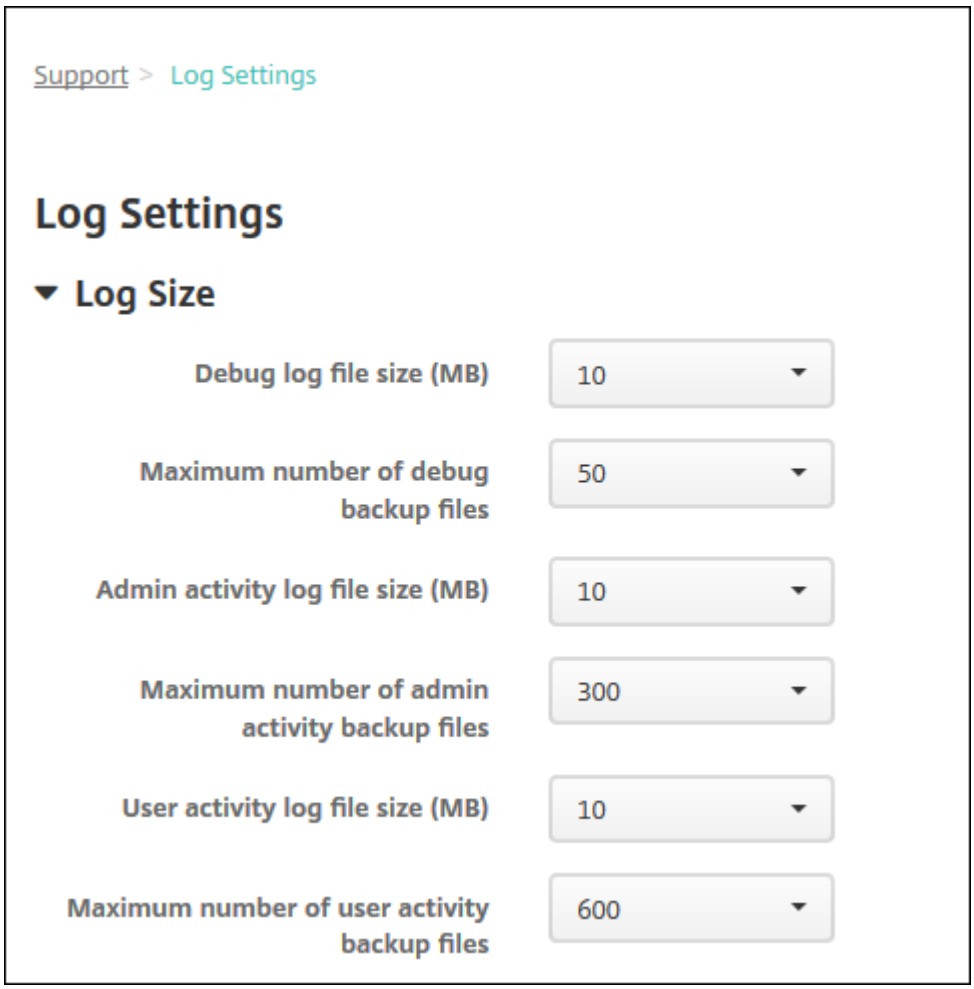


En la página **Parámetros de registro**, puede acceder a las siguientes opciones:

- **Tamaño de registro**. 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 “Tamaño de registro” se aplica a cada archivo de registros admitido por XenMobile (depuración, actividad de administración y actividad de usuarios).
- **Nivel de registro**. Use esta opción para cambiar el nivel de captura de registros o para conservar la configuración.
- **Registrador personalizado**. 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 **Parámetros de registros**, expanda **Tamaño de registro**.



2. Configure estos parámetros:

   - **Tamaño de archivo de registros de depuración (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**.
   - **Máximo de archivos de copia de seguridad de depuración:** En la lista, haga clic en la cantidad máxima de archivos de depuración que conservará el servidor. De forma predeterminada, XenMobile conserva 50 archivos de copias de seguridad en el servidor.
   - **Tamaño de archivo de registros de actividad de administradores (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**.
   - **Máximo de archivos de copia de seguridad de actividad de administradores:** En la lista, haga clic en la cantidad máxima de archivos de actividad de administración que conservará el servidor. De forma predeterminada, XenMobile conserva 300 archivos de copias de seguridad en el servidor.
   - **Tamaño de archivo de registros de actividad de usuarios (MB):** En la lista, haga clic en

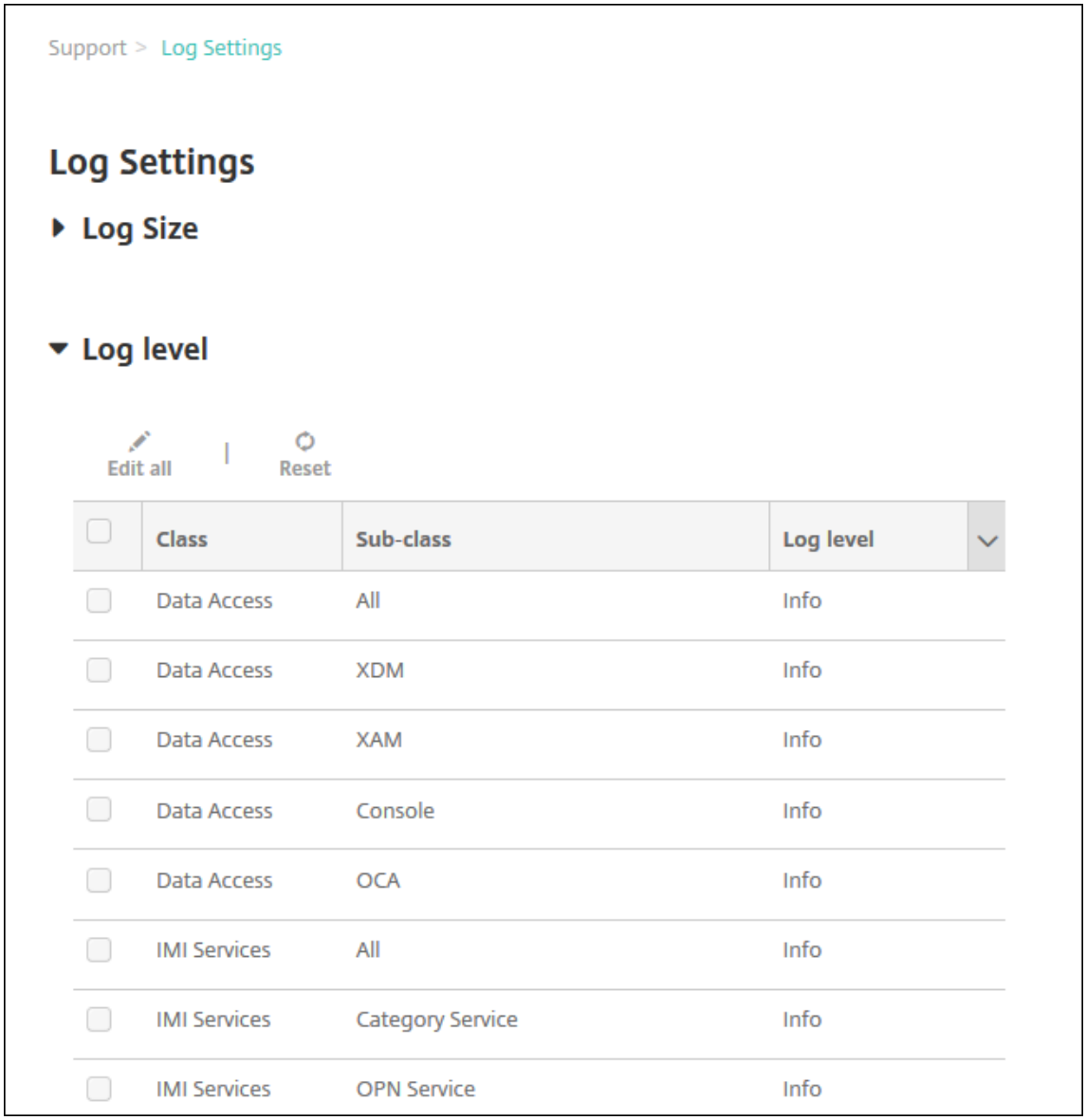
un tamaño comprendido entre 5 y 20 MB para cambiar el tamaño máximo del archivo de actividad de usuarios. El tamaño de archivo predeterminado es de **10 MB**.

- **Máximo de archivos de copia de seguridad de actividad de usuarios:** En la lista, haga clic en la cantidad máxima 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 “Nivel de registro” 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.

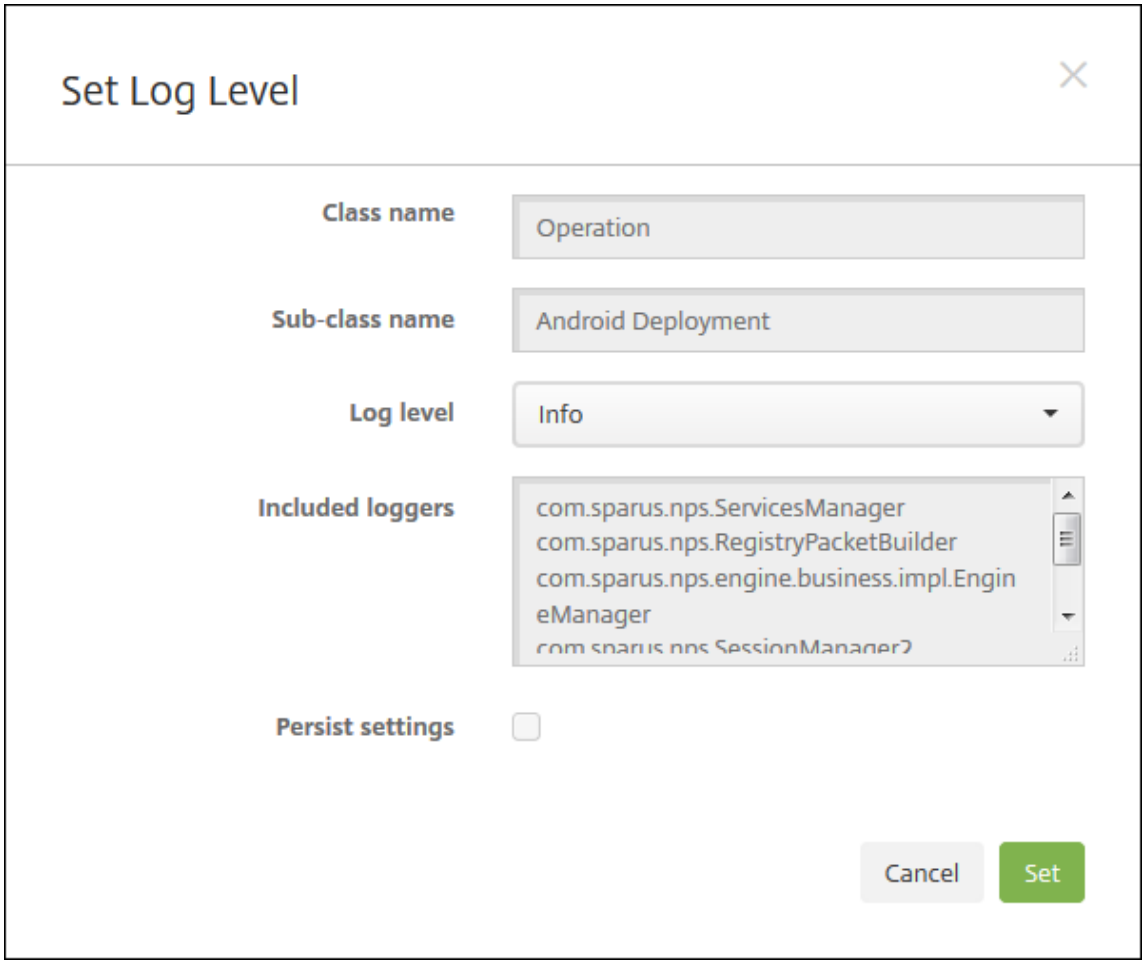
1. En la página **Parámetros de registro**, expanda **Nivel de registro**. Aparece la tabla con todas las clases de registros.



2. Lleve a cabo una de las siguientes acciones:

   - Marque la casilla junto a una clase y luego haga clic en **Definir nivel** para cambiar solo el nivel de registro de esa clase.
   - Haga clic en **Modificar todo** para aplicar el cambio de nivel de registro a todas las clases de la tabla.

   El cuadro de diálogo **Definir nivel de registro** aparece donde se puede establecer el nivel de registro y seleccionar si la configuración del nivel de registro se conserva tras reiniciar el servidor de XenMobile.



- **Nombre de clase:** Este campo muestra el valor “Todo” 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 modificable.
- **Nombre de subclase:** Este campo no se puede modificar. Muestra el valor “Todo” cuando se está cambiando el nivel de registro de todas las clases, o bien muestra el nombre de la subclase en particular.
- **Nivel de registro:** Haga clic en un nivel de registro en la lista. Los niveles de registro admitidos son:
  - Grave
  - Error
  - Advertencia
  - Información
  - Depuración
  - Seguimiento
  - No
- **Registradores incluidos:** 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

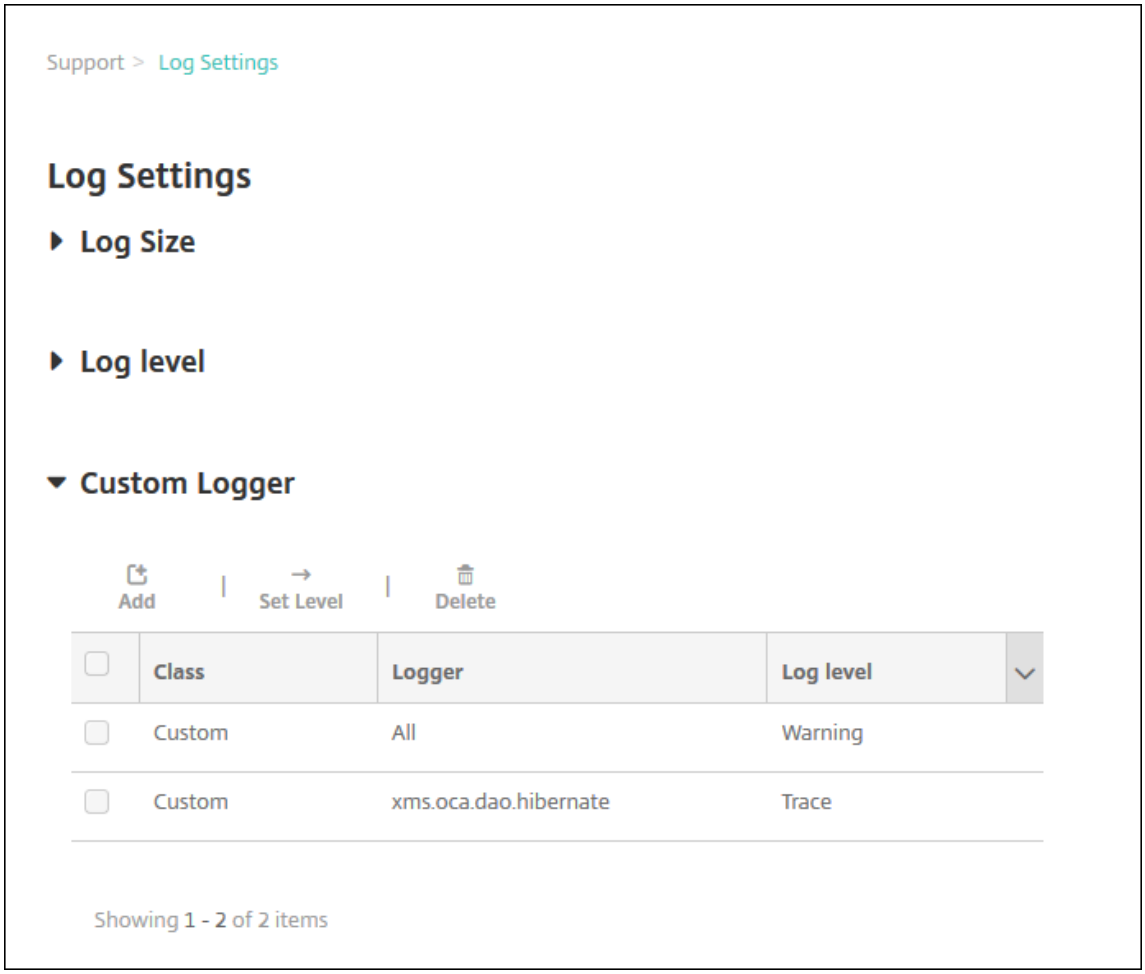
actualmente para una clase en concreto; no es un campo modificable.

- **Conservar los parámetros:** 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.

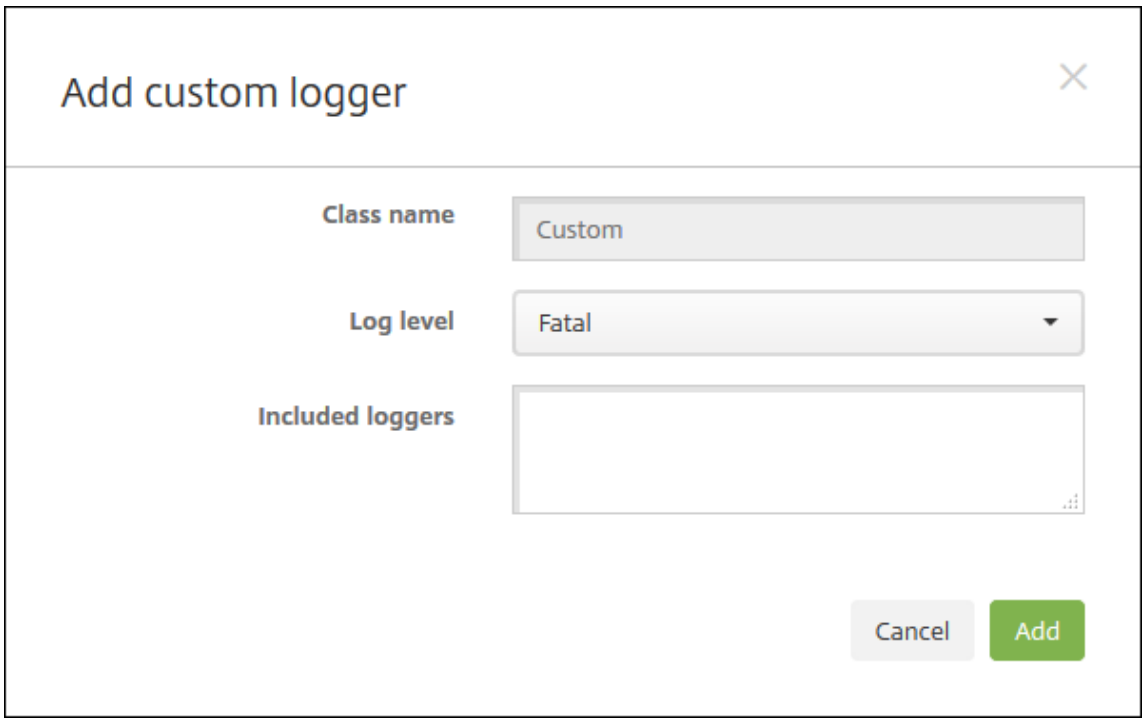
3. Haga clic en **Configurar** para confirmar los cambios.

Para agregar un registrador personalizado

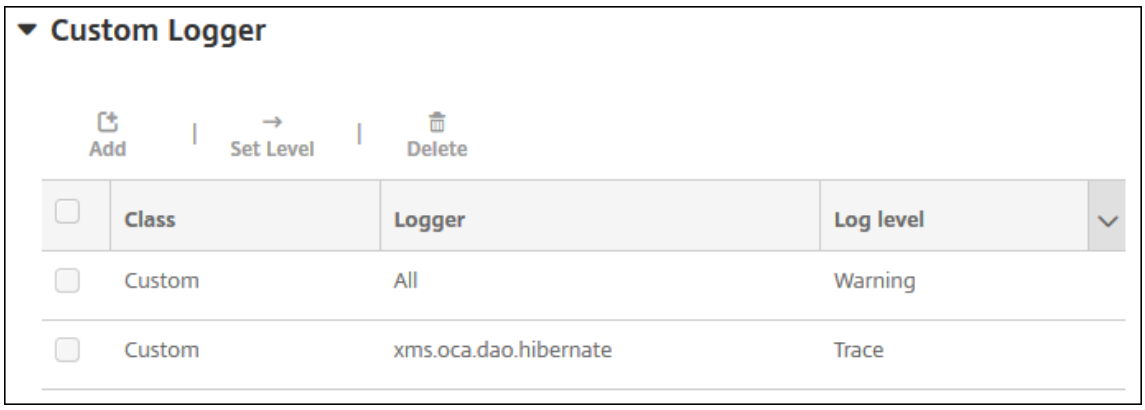
1. En la página **Parámetros de registros**, expanda **Registrador personalizado**. Aparecerá la tabla **Registrador personalizado**. Si no ha agregado aún registradores personalizados, la tabla está vacía.



2. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar registrador personalizado**.



3. Configure estos parámetros:
   - **Class Name**: Este campo muestra **Custom**; no es un campo modificable.
   - **Nivel de registro:** Haga clic en un nivel de registro en la lista. Los niveles de registro admitidos son:
     - Grave
     - Error
     - Advertencia
     - Información
     - Depuración
     - Seguimiento
     - No
   - **Registradores incluidos:** Escriba los registradores concretos que quiere incluir como registradores personalizados, o bien deje el campo en blanco para incluir todos los registradores.
4. Haga clic en **Agregar**. El registrador personalizado se agrega a la tabla **Registrador personalizado**.



Para eliminar un registrador personalizado

1. En la página **Parámetros de registros**, expanda **Registrador personalizado**.
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 **OK**.

> **Importante:**
>
> Esta operación no se puede deshacer.

Proveedor de servicios móviles

January 4, 2022

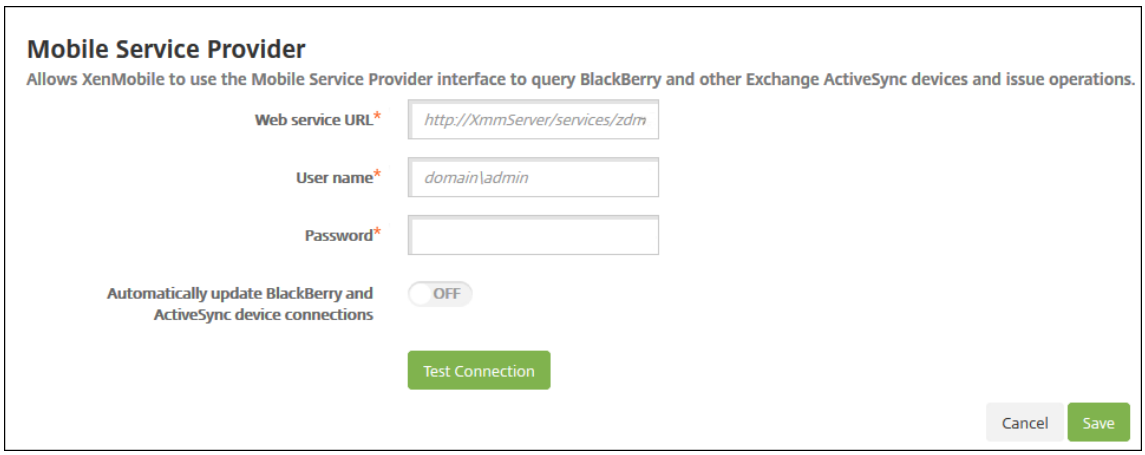
Puede habilitar XenMobile para que utilice la interfaz del proveedor de servicios móviles, para enviar consultas a dispositivos BlackBerry y Exchange ActiveSync y emitir operaciones.

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 **Parámetros**.

2. En **Servidor**, haga clic en **Proveedor de servicios móviles**. Aparece la página **Proveedor de servicios móviles**.



3. Configure estos parámetros:

   - **URL del servicio web:** Escriba la dirección URL del servicio web. Por ejemplo: `https://<XmmServer>/services/xdmservice`.
   - **Nombre de usuario:** Escriba el nombre de usuario con el formato dominio\admin.
   - **Contraseña:** Escriba la contraseña.
   - **Habilitar la actualización automática de conexiones de dispositivos BlackBerry y ActiveSync:** Seleccione si quiere actualizar automáticamente las conexiones de los dispositivos. Está **desactivado** de forma predeterminada.
   - Haga clic en **Probar conexión** para comprobar la conexión.

4. Haga clic en **Guardar**.

Informes

August 10, 2020

XenMobile ofrece los siguientes informes predefinidos que permiten analizar las implementaciones de dispositivos y aplicaciones. Cada informe aparece como un gráfico y una tabla. Puede ordenar y filtrar las tablas en función de cualquier columna. También puede seleccionar elementos de los gráficos para obtener información más detallada.

- **Total de intentos de implementación de la aplicación:** Ofrece una lista de las aplicaciones implementadas que los usuarios han intentado instalar en los dispositivos.
- **Aplicaciones por plataforma:** Ofrece una lista de las aplicaciones y sus versiones según la plataforma y la versión del dispositivo.
- **Aplicaciones por tipo:** Ofrece una lista de las aplicaciones según su versión, tipo o categoría.

- **Inscripción de dispositivos:** Ofrece una lista de todos los dispositivos inscritos.
- **Dispositivos y aplicaciones:** Ofrece una lista de los dispositivos que ejecutan aplicaciones administradas.
- **Dispositivos inactivos:** Ofrece una lista de los dispositivos que no hayan tenido ninguna actividad durante la cantidad de días que especifique la propiedad device.inactivity.days.threshold de XenMobile Server.
- **Dispositivos liberados por jailbreak/root:** Ofrece una lista de los dispositivos iOS liberados por jailbreak y de los dispositivos Android liberados por root.
- **Términos y condiciones:** Ofrece una lista de los usuarios que hayan aceptado o rechazado los contratos de términos y condiciones. Puede seleccionar áreas del gráfico para ver más detalles.
- **10 aplicaciones principales:** Fallo de implementación. Ofrece una lista de hasta 10 aplicaciones que no se pudieron implementar.
- **Aplicaciones en lista negra por dispositivo y usuario:** Ofrece una lista de las aplicaciones prohibidas que los usuarios tienen en sus dispositivos.

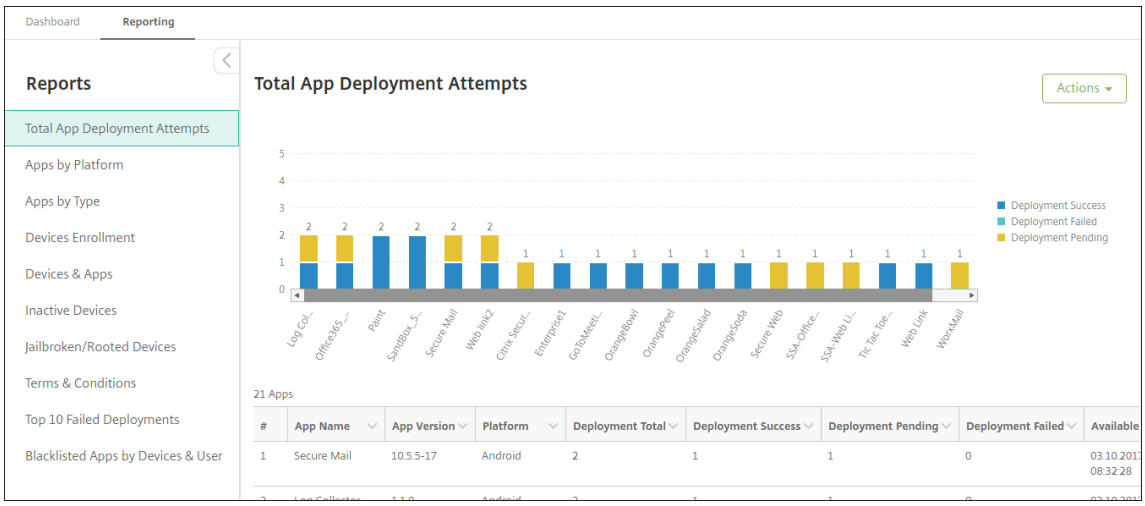
  > **Nota:**
  >
  > La consola de XenMobile Server contiene los términos “lista negra” y “lista blanca”. Estamos cambiando esos términos en una próxima versión a “lista de bloqueados” y “lista de permitidos”.

- **Dispositivos no conformes:** Muestra los dispositivos que no cumplen los criterios de conformidad, como, por ejemplo, si el dispositivo se ha liberado por jailbreak, la versión del sistema operativo y si el dispositivo tiene un código de acceso.

Puede exportar los datos de cada tabla en formato CSV, que puede abrir con programas como Microsoft Excel. Asimismo, puede exportar el gráfico de cada informe en formato PDF.

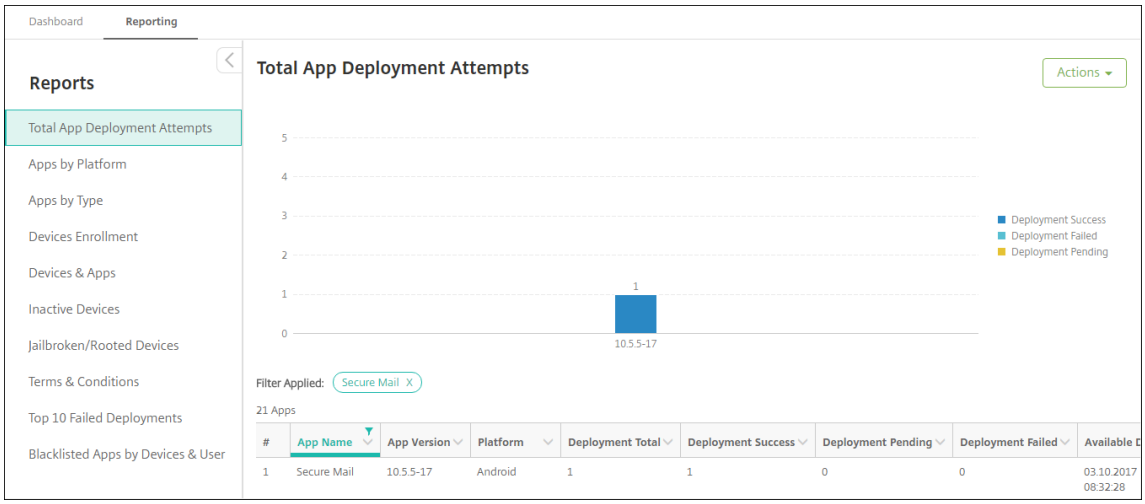
Para generar un informe

1. En la consola de XenMobile, haga clic en **Analizar > Informes**. Aparecerá la página **Informes**.
2. Haga clic en el informe que quiera generar.

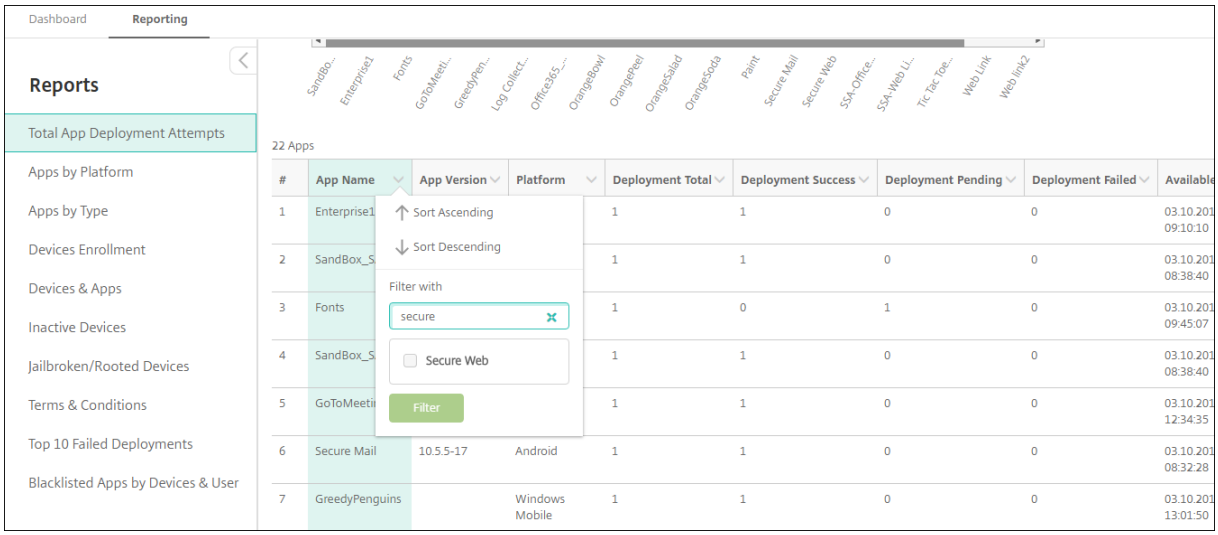


Para ver más datos de un informe

1. Haga clic en las áreas del gráfico para profundizar y ver información más detallada.

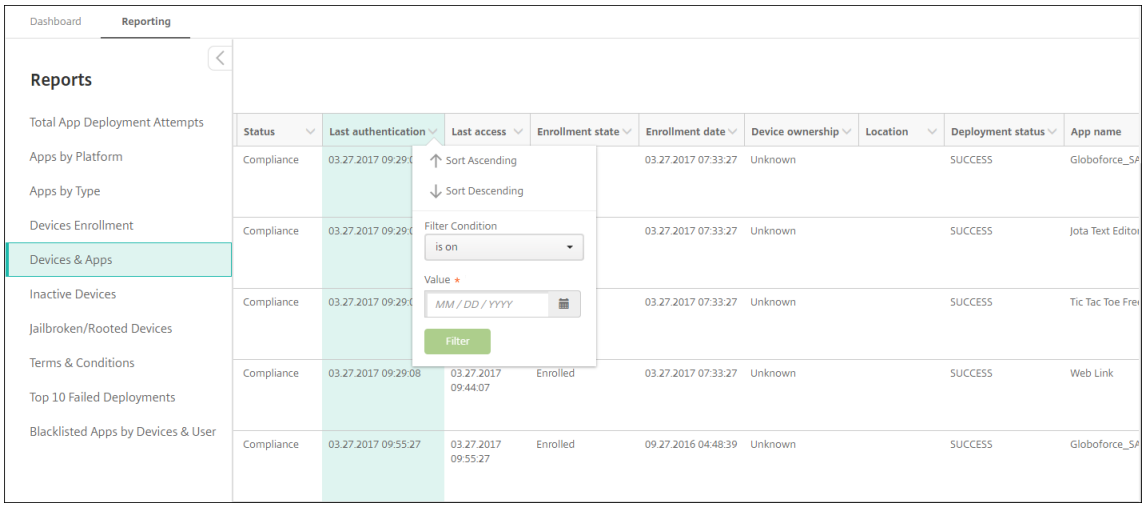


Para ordenar, filtrar o buscar en una columna de la tabla, haga clic en el encabezado de dicha columna

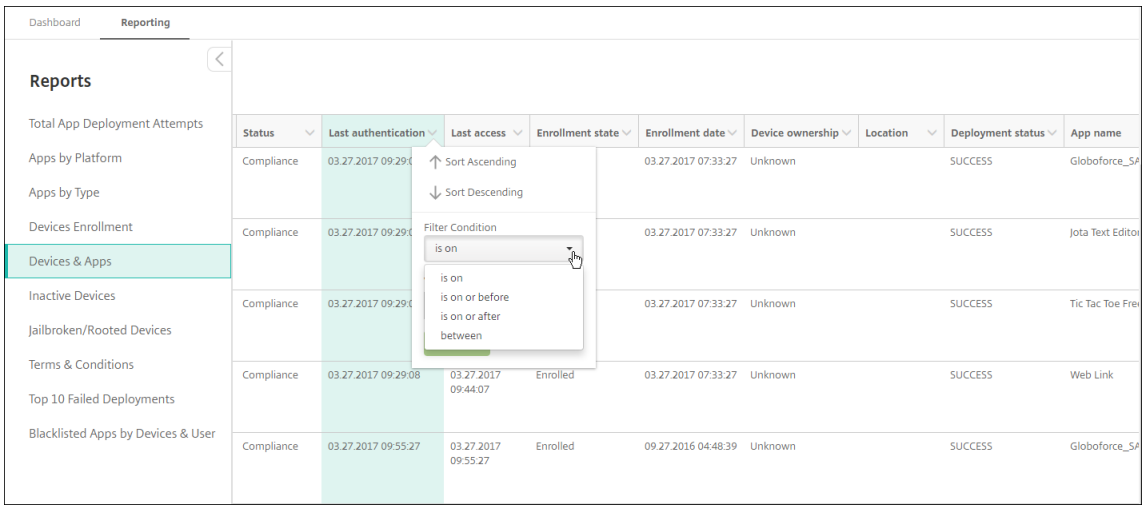


Para filtrar el informe por fecha

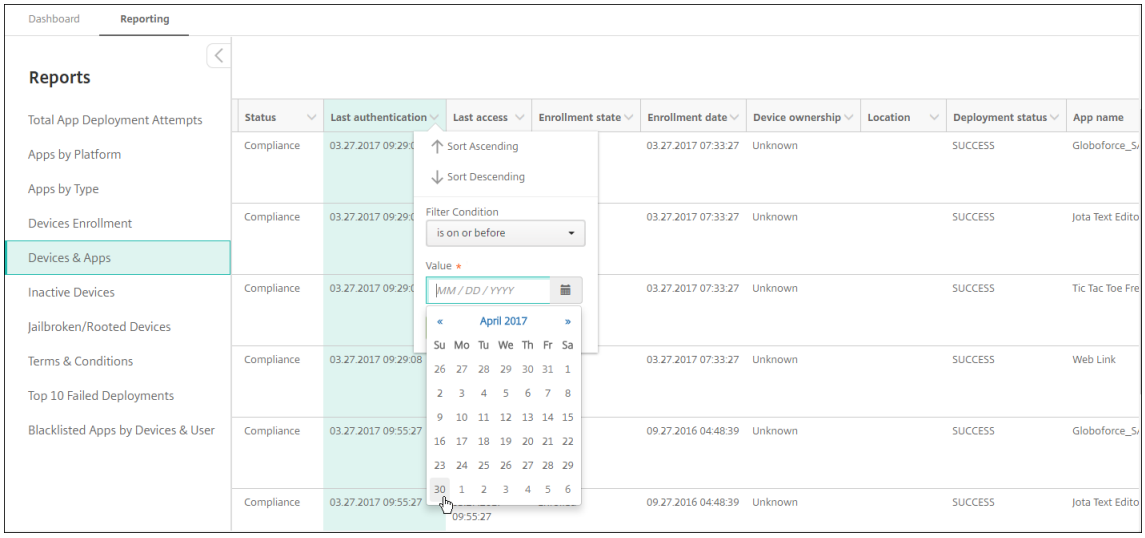
1. Haga clic en el encabezado de una columna para ver los parámetros de filtro.



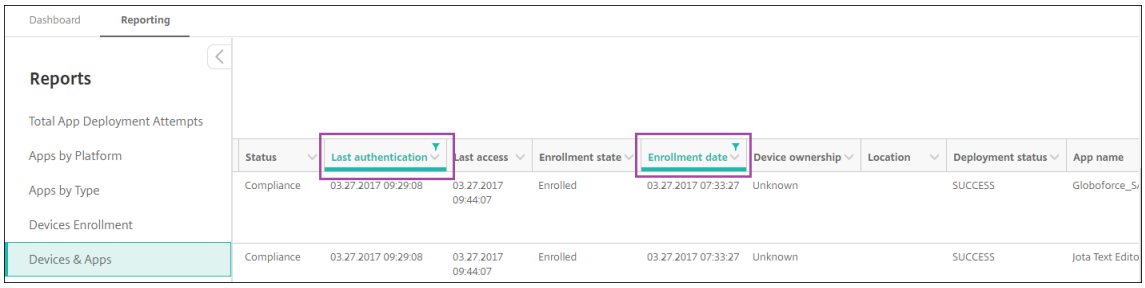
2. En **Condición de filtro**, elija cómo quiere restringir las fechas relevantes.



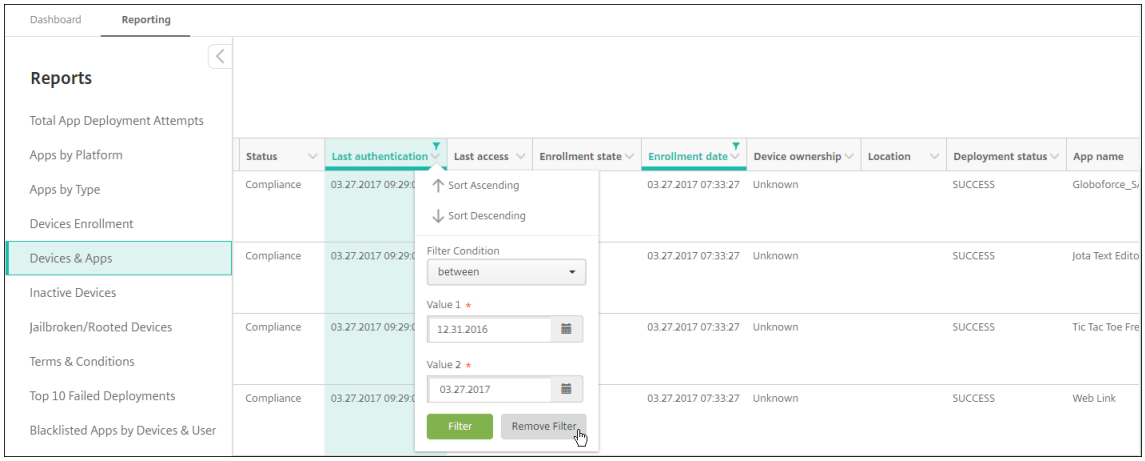
3. Use el selector de fecha para especificar las fechas.



4. Como se muestra el siguiente ejemplo, aparecerá una columna con un filtro de fecha.

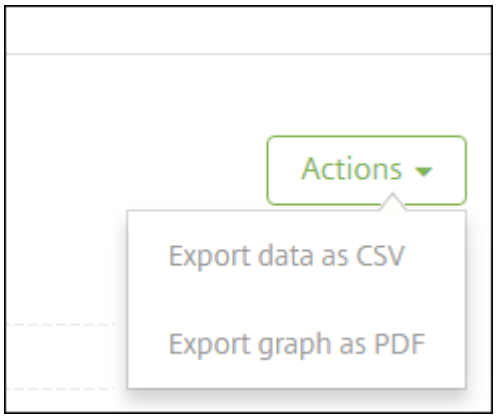


5. Para quitar un filtro, haga clic en el encabezado de la columna y, a continuación, haga clic en **Quitar filtro**.



Para exportar un gráfico o una tabla

- Para exportar el gráfico en formato PDF, haga clic en **Acciones** > **Exportar gráfico como PDF**.
- Para exportar los datos de la tabla en formato CSV, haga clic en **Acciones** > **Exportar datos como CSV**.



> **Importante:**
>
> Aunque es posible utilizar SQL Server para crear informes personalizados, Citrix no recomienda este método. Citrix no publica el esquema y puede cambiar el esquema sin notificación. Si decide seguir este método para generar informes, compruebe que las consultas SQL se ejecutan mediante una cuenta de solo lectura. Tenga en cuenta que una consulta con varios JOIN que tarde un tiempo en ejecutarse afectará al rendimiento del servidor de XenMobile Server durante ese tiempo.

Supervisión SNMP

January 4, 2022

Puede habilitar la supervisión de SNMP en XenMobile Server para que los sistemas de supervisión consulten y obtengan información sobre sus nodos de XenMobile. Las consultas usan parámetros, como Carga del procesador, Promedio de carga, Uso de la memoria y Conectividad. Para obtener más información sobre SNMP 3, como las especificaciones de autenticación y cifrado, consulte la documentación oficial de SNMP para RFC 3414.

> **Nota:**
>
> La supervisión SNMP 3 está disponible en XenMobile Server 10.8 y versiones posteriores.

Puede utilizar varias aplicaciones de supervisión que admiten la supervisión de SNMP, por ejemplo, SCOM. Para obtener información más detallada acerca de SCOM, consulte este artículo de asistencia de Citrix Knowledge Center.

Requisitos previos

Configure estos puertos TCP:

- **Puerto 161 (UDP):** Se usa para el tráfico SNMP mediante el protocolo UDP. El origen es SNMP Manager y el destino es XenMobile.
- **Puerto 162 (UDP):** Se usa para enviar las alertas de captura SNMP al SNMP Manager desde XenMobile. El origen es XenMobile y el destino es el SNMP Manager.

Para obtener más información acerca de la configuración de puertos de XenMobile, consulte Requisitos de puertos.

Para ver un diagrama de la arquitectura que tiene una implementación local de XenMobile que incluya SNMP, consulte Arquitectura de referencia para implementaciones locales.

Estos son los pasos generales para configurar SNMP.

1. **Agregar usuarios:** Los usuarios heredan el permiso de recibir capturas y supervisar XenMobile Server.
2. **Agregar un SNMP Manager para recibir capturas:** Las capturas son las alertas que genera XenMobile cuando el nodo de XenMobile supera el umbral máximo definido por el usuario.
3. **Configurar el SNMP Manager para la interacción con XenMobile:** XenMobile Server utiliza bases de datos de información de administración (MIB) para realizar operaciones. Puede descargar las MIB desde la página **Parámetros > Configuración de SNMP** en la consola de XenMobile. A continuación, importe las MIB en el SNMP Manager mediante un importador de MIB.

   > **Nota:**
   >
   > Cada SNMP Manager tiene su propio importador de MIB.

4. **Habilitar capturas:** En la consola de XenMobile, puede habilitar las capturas y definir los intervalos y los umbrales en función de su entorno.
5. **Ver capturas en el SNMP Manager de terceros:** Para ver las capturas, consulte el SNMP Manager. Sin embargo, en algunos administradores, puede permitir las notificaciones fuera del administrador. Puede configurar las notificaciones para que aparezcan, por ejemplo, en el correo electrónico.

Puede generar las siguientes capturas desde XenMobile.

Nombre de la captura: Carga del procesador.

- **ID del objeto de supervisión (OID):** .1.3.6.1.2.1.25.3.3.1.2
- **Descripción:** Supervisa la carga de la CPU del sistema durante el intervalo definido por el usuario. Si la carga supera el valor del umbral personalizado, XenMobile genera la captura SNMP.

Nombre de la captura: Carga media durante un minuto.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.2021.10.1.5.1
- **Descripción:** Supervisa la carga media del sistema durante un período de un minuto en el intervalo definido por el usuario. Si la carga media supera el valor del umbral personalizado, XenMobile genera la captura SNMP.

Nombre de la captura: Carga media durante cinco minutos.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.2021.10.1.5.2
- **Descripción:** Supervisa la carga media del sistema durante un período de cinco minutos en el intervalo definido por el usuario. Si la carga media supera el valor del umbral personalizado, XenMobile genera la captura SNMP.

Nombre de la captura: Carga media durante quince minutos.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.2021.10.1.5.3
- **Descripción:** Supervisa la carga media del sistema durante un período de quince minutos en cada intervalo definido por el usuario. Si la carga media supera el valor del umbral personalizado, XenMobile genera la captura SNMP.

Nombre de la captura: Memoria total disponible.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.2021.4.11
- **Descripción:** Supervisa la memoria disponible en cada intervalo definido por el usuario. Si la memoria disponible disminuye hasta ser inferior al valor del umbral personalizado, XenMobile genera la captura SNMP. Nota: La memoria total disponible incluye tanto la memoria RAM como la memoria de intercambio (memoria virtual). Para obtener la memoria total de intercambio, puede realizar la consulta con el OID de SNMP .1.3.6.1.4.1.2021.4.3. Para obtener la memoria disponible de intercambio, puede realizar la consulta con el OID de SNMP .1.3.6.1.4.1.2021.4.4.

Nombre de la captura: Total de almacenamiento en disco utilizado.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.2021.9.1.9.1
- **Descripción:** Supervisa el almacenamiento en disco del sistema durante cada intervalo definido por el usuario. Si el almacenamiento en disco supera el valor del umbral personalizado, XenMobile genera la captura SNMP.

Nombre de la captura: Uso de memoria heap de Java.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.2.4.0
- **Descripción:** Supervisa el uso de la memoria heap en la máquina virtual de Java (JVM) de XenMobile durante cada intervalo definido por el usuario. Si el uso supera el valor del umbral personalizado, XenMobile genera la captura SNMP.

Nombre de la captura: Uso de metaespacio de Java.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.2.5.0
- **Descripción:** Supervisa el uso del metaespacio de Java en XenMobile durante cada intervalo definido por el usuario. Si el uso supera el valor del umbral, XenMobile genera la captura SNMP.

Nombre de la captura: Conectividad LDAP.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.1.0
- **Descripción:** Supervisa la conectividad entre el servidor LDAP y el nodo de XenMobile en cada intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad DNS.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.2.0
- **Descripción:** Supervisa la conectividad entre el servidor DNS y el nodo de XenMobile en cada intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con el servidor de Google Store.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.3.0
- **Descripción:** Supervisa la conectividad entre el servidor de Google Store y el nodo de XenMobile en cada intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con Windows Phone Store.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.4.0
- **Descripción:** Supervisa la conectividad entre el servidor de Windows Phone Store y el nodo de XenMobile en cada intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con Windows Tab Store.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.5.0

- **Descripción:** Supervisa la conectividad entre el servidor de Windows Tab Store y los nodos de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con el servidor del token de seguridad Windows.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.6.0
- **Descripción:** Supervisa la conectividad entre el servidor del token de seguridad Windows y los nodos de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con el servidor de notificaciones de Windows.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.7.0
- **Descripción:** Supervisa la conectividad entre el servidor de notificaciones de Windows y los nodos de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con el servidor de Apple Push Notification Service (APNs).

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.8.0
- **Descripción:** Supervisa la conectividad entre el servidor APNs y los nodos de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con el servidor de Apple Feedback.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.9.0
- **Descripción:** Supervisa la conectividad entre el servidor de Apple Feedback y los nodos de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con el servidor de Apple Store.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.10.0
- **Descripción:** Supervisa la conectividad entre el servidor de Apple Store y los nodos de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con la base de datos XenMobile.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.11.0
- **Descripción:** Supervisa la conectividad entre el servidor de base de datos XenMobile y los nodos de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con el servidor de Firebase Cloud Messaging.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.12.0

- **Descripción:** Supervisa la conectividad entre el servidor de Firebase Cloud Messaging y los nodos de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con Citrix License Server.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- **Descripción:** Supervisa la conectividad entre Citrix License Server y los nodos de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con Citrix Gateway.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.15.0
- **Descripción:** Supervisa la conectividad entre Citrix Gateway y los nodos de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad entre nodos de XenMobile.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.16.0
- **Descripción:** Supervisa la conectividad entre los nodos en clúster de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Nombre de la captura: Conectividad con el servicio Tomcat de nodos de XenMobile.

- **ID del objeto de supervisión (OID):** .1.3.6.1.4.1.3845.5.1.1.18.17.0
- **Descripción:** Supervisa la conectividad entre el servicio Tomcat de nodos de XenMobile y los nodos de XenMobile durante el intervalo definido por el usuario. Si falla la conectividad, XenMobile genera una captura SNMP.

Para lograr el mejor rendimiento del servidor al configurar los umbrales de SNMP, tenga en cuenta los siguientes factores:

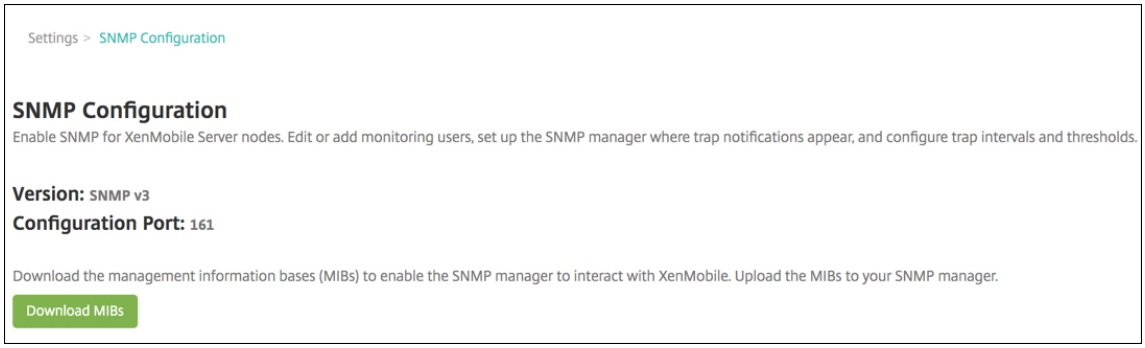
- La frecuencia de las llamadas
- Los datos de captura que se recopilarán y las comprobaciones de umbrales
- El mecanismo de comunicación entre nodos
- La frecuencia de las comprobaciones de conectividad
- Los tiempos de espera en los fallos durante las comprobaciones

Para agregar usuarios SNMP

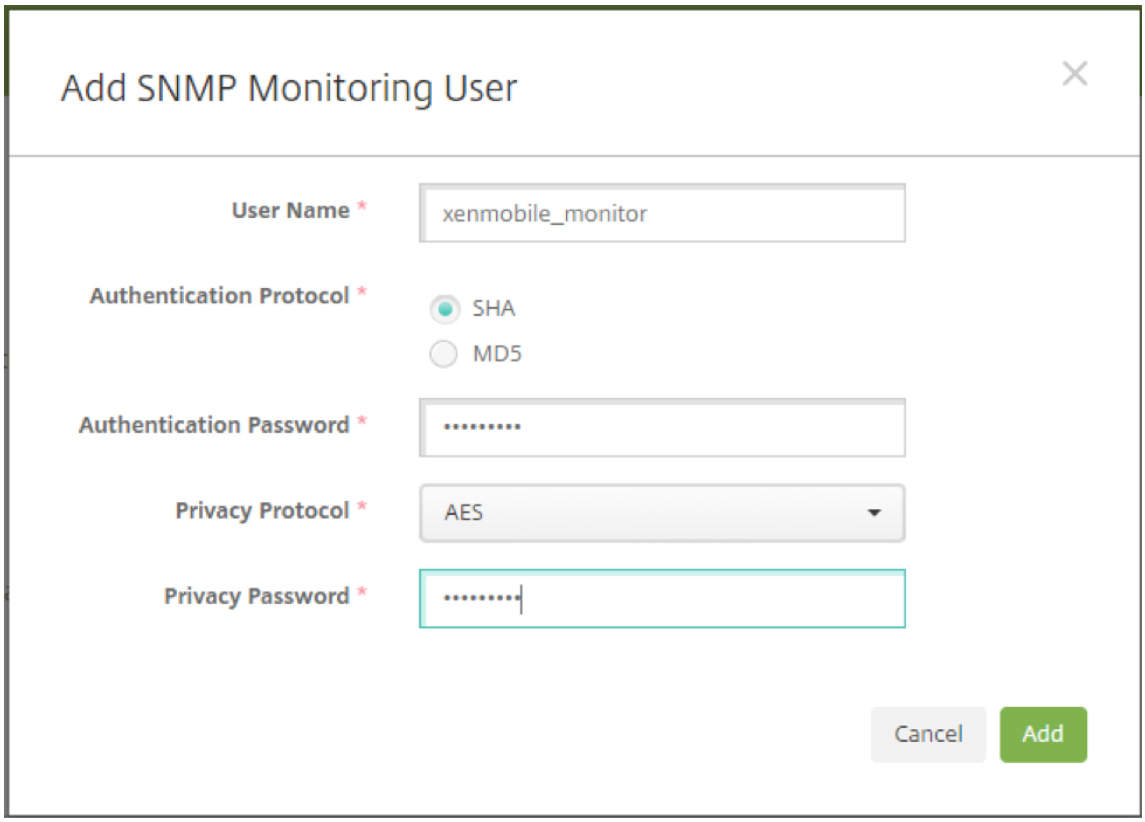
Los usuarios SNMP interactúan con los SNMP Managers y reciben las capturas.

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

2. En **Supervisión**, haga clic en **Configuración de SNMP**. Aparecerá la página **Configuración de SNMP**.



3. En **Usuarios de supervisión SNMP**, haga clic en **Agregar**.
4. En el cuadro de diálogo **Agregar usuario de supervisión SNMP**, configure los siguientes parámetros:



Nombre de usuario: El nombre de usuario utilizado para iniciar sesión en el SNMP Manager. Aunque puede usar caracteres alfanuméricos, guiones bajos y guiones, no puede usar espacios ni otros caracteres especiales en el nombre de usuario.

> **Nota:**
>
> No puede agregar el nombre de usuario “xmsmonitor” porque XenMobile se reserva este

> nombre para uso interno.

Protocolo de autenticación:

- **SHA** (Recomendado)
- **MD5**

Contraseña de autenticación: Escriba una contraseña de 8 a 18 caracteres. Puede incluir caracteres alfanuméricos y especiales.

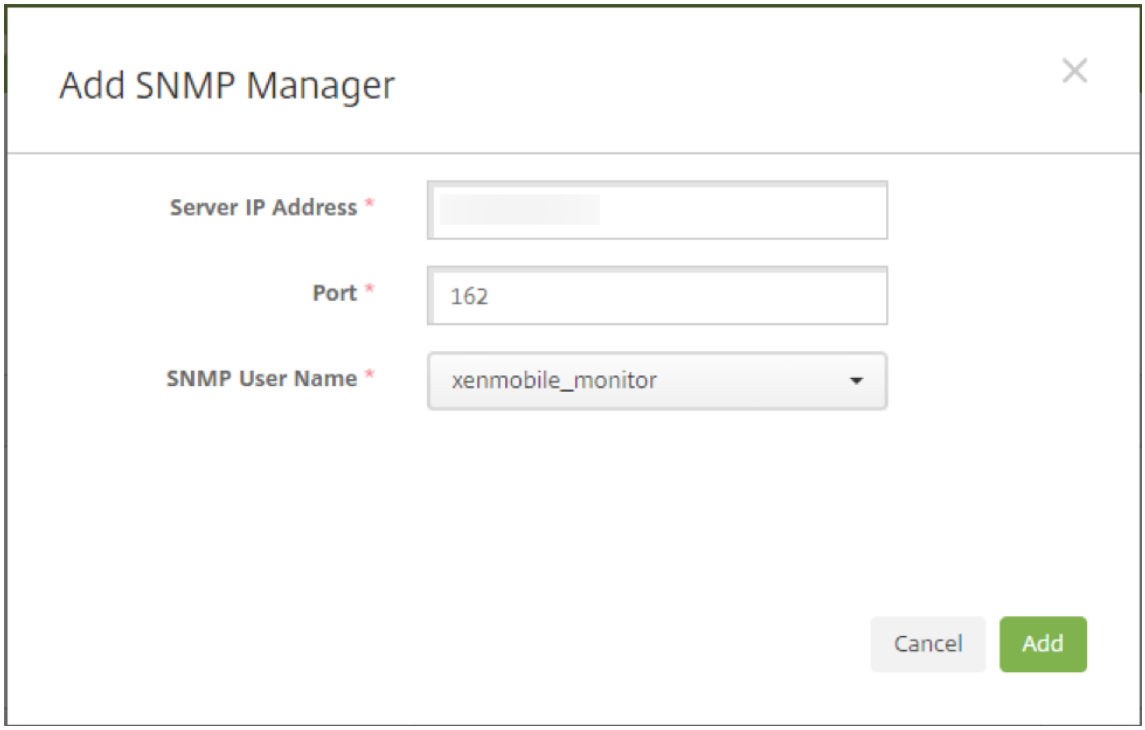
Protocolo de privacidad:

- **DES**
- **AES 128** (Recomendado)

Contraseña de privacidad: Escriba una contraseña de 8 a 18 caracteres. Puede incluir caracteres alfanuméricos y especiales.

Para agregar un SNMP Manager

1. En **SNMP Managers**, haga clic en **Agregar**.
2. En el cuadro de diálogo **Agregar SNMP Manager**, configure los siguientes parámetros:



Dirección IP del servidor: Escriba la dirección IP del SNMP Manager.

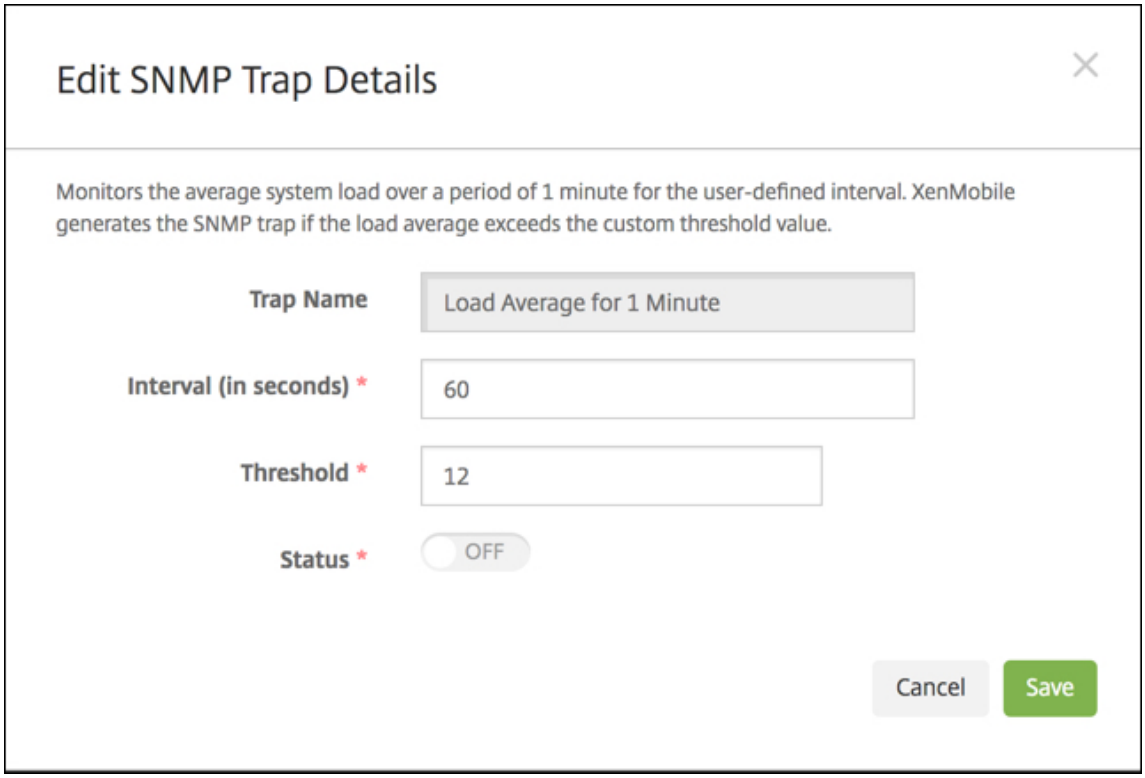
Puerto: Cambie el número de puerto si fuera necesario. El valor predeterminado es 162.

Nombre de usuario SNMP: Seleccione el nombre de un usuario con acceso al administrador.

Para habilitar y configurar capturas SNMP

Para ver una guía de los parámetros de captura adecuados a su entorno, consulte Escalabilidad y rendimiento. Por ejemplo, para supervisar la carga media de XenMobile durante un minuto, puede habilitar "Promedio de carga de 1 minuto" y proporcionar un valor de umbral. Si "Promedio de carga de 1 minuto" de XenMobile Server supera el umbral especificado, usted recibirá una captura en los SNMP Managers configurados.

1. Para habilitar capturas individuales, realice una de las siguientes acciones:
   - Marque la casilla situada junto al parámetro y haga clic en **Habilitar**.
   - Para habilitar todas las capturas de la lista, marque la casilla situada en la parte superior y haga clic en **Habilitar**.
2. Para modificar una captura, seleccione el parámetro y haga clic en **Modificar**.
3. En el cuadro de diálogo **Modificar detalles de captura SNMP**, puede modificar los umbrales de capturas concretas.



Nombre de captura: El nombre de la captura. No puede modificar este campo.

Intervalo (en segundos): El intervalo permitido es de 60 a 86 400 segundos (24 horas).

Umbral: Solo puede cambiar el umbral de estas capturas:

- Carga del procesador
- Promedio de carga de 1 minuto

- Promedio de carga de 5 minutos
- Promedio de carga de 15 minutos
- Memoria total disponible
- Total de almacenamiento en disco utilizado
- Uso de memoria heap de Java
- Uso de metaespacio de Java

Estado: Seleccione **Sí** para habilitar la supervisión SNMP en la captura. Seleccione **No** para inhabilitar la supervisión.

Para obtener más información útil sobre la supervisión de XenMobile mediante SNMP, consulte esta entrada de blog.

Paquetes de asistencia

January 4, 2022

Para informar a Citrix de un problema o para solucionar un problema, cree un paquete de asistencia. Luego, cargue esos paquetes de asistencia en Citrix Insight Services (CIS).

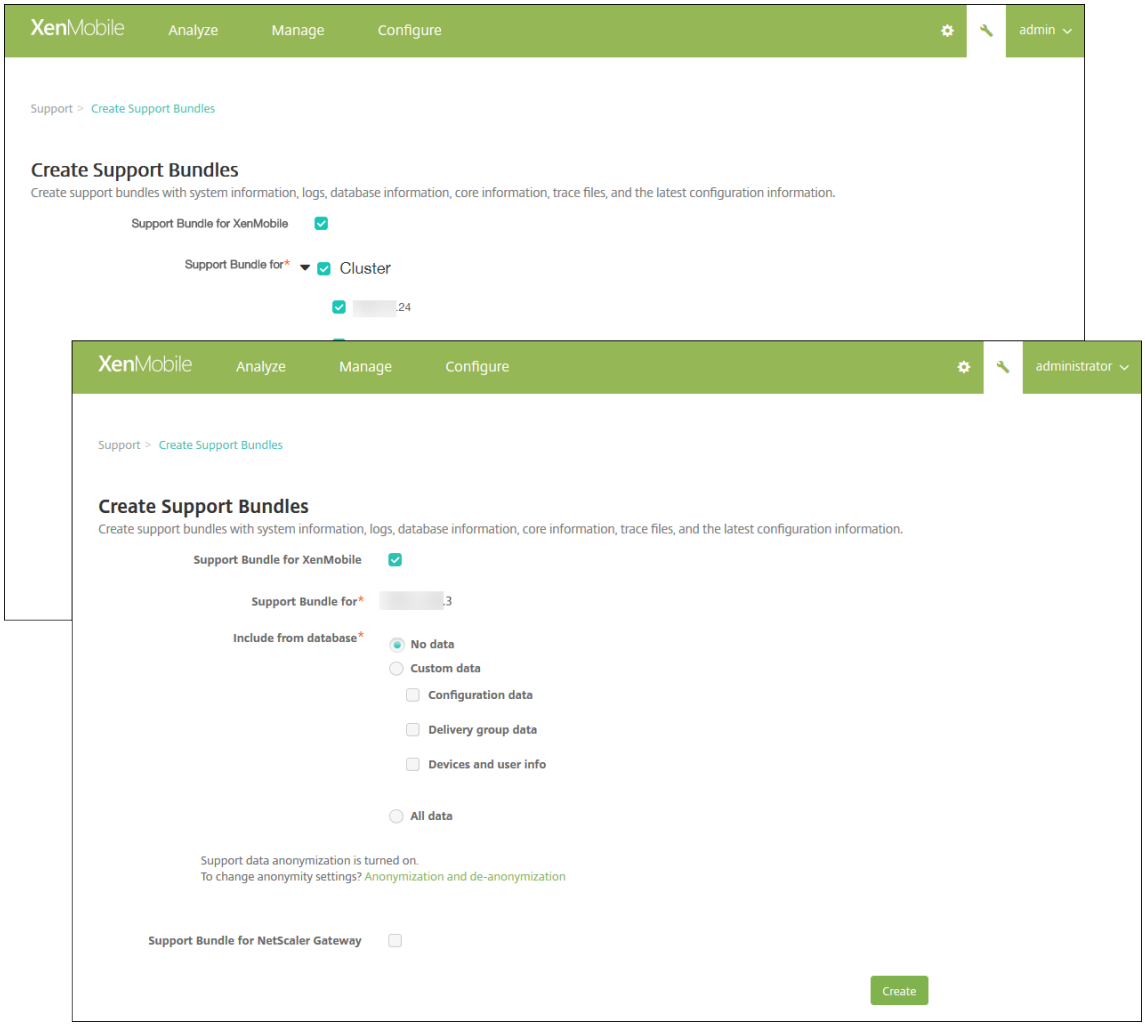
De forma predeterminada, un paquete de asistencia contiene un máximo de 100 archivos de copia de seguridad de los siguientes archivos. El tamaño predeterminado para estos archivos es 10 MB.

- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

Cuando el paquete de asistencia incluye 100 archivos de registros para cada una de esas categorías, el archivo de registros se transfiere. Si configura una cantidad máxima inferior de archivos de registro, XenMobile elimina inmediatamente los archivos de registro extraños en ese nodo de servidor. Para configurar la cantidad de archivos de registro, vaya a **Solución de problemas y asistencia > Parámetros de registros**.

Para crear un paquete de asistencia

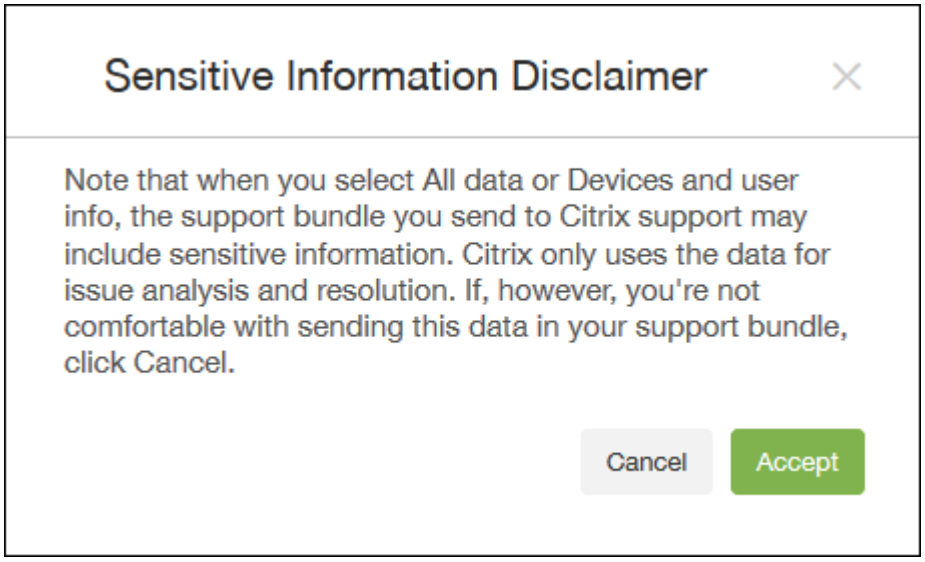
1. En la consola de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha. Aparecerá la página **Asistencia**.
2. En la página **Asistencia**, haga clic en **Crear paquetes de asistencia**. Aparecerá la página **Crear paquetes de asistencia**. Si su entorno de XenMobile contiene nodos en clúster, se muestran todos los nodos.



3. Compruebe que está marcada la casilla **Paquete de asistencia para XenMobile**.
4. Si su entorno de XenMobile contiene nodos en clúster, en **Paquete de asistencia para**, seleccione todos los nodos o cualquier combinación de nodos de los que obtener datos.
5. En **Incluir desde la base de datos**, realice una de las siguientes acciones:
   - Haga clic en **Ningún dato**.
   - Haga clic en **Datos personalizados**. De forma predeterminada, están seleccionadas todas estas opciones.
     - **Datos de configuración:** Incluye las configuraciones de certificados y las directivas del administrador de dispositivos.
     - **Datos de grupos de entrega:** 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.
     - **Información de dispositivos y usuarios:** Incluye aplicaciones, acciones, grupos de entrega y directivas de dispositivo.

- Haga clic en **Todos los datos**.

> **Nota:**
>
> Si elige **Información de dispositivos y usuarios** o **Todos los datos** y este es el primer paquete de asistencia que crea, aparecerá el cuadro de diálogo **Renuncia de responsabilidad de información confidencial**. Lea el aviso de declinación de responsabilidades y, a continuación, haga clic en **Aceptar** o **Cancelar**. Si hace clic en **Cancelar**, el paquete de asistencia no se podrá cargar en Citrix. Si hace clic en **Aceptar**, podrá cargar el paquete de asistencia en Citrix y no verá el aviso de declinación de responsabilidades la próxima vez que cree un paquete de asistencia que contenga datos de usuario o dispositivo.

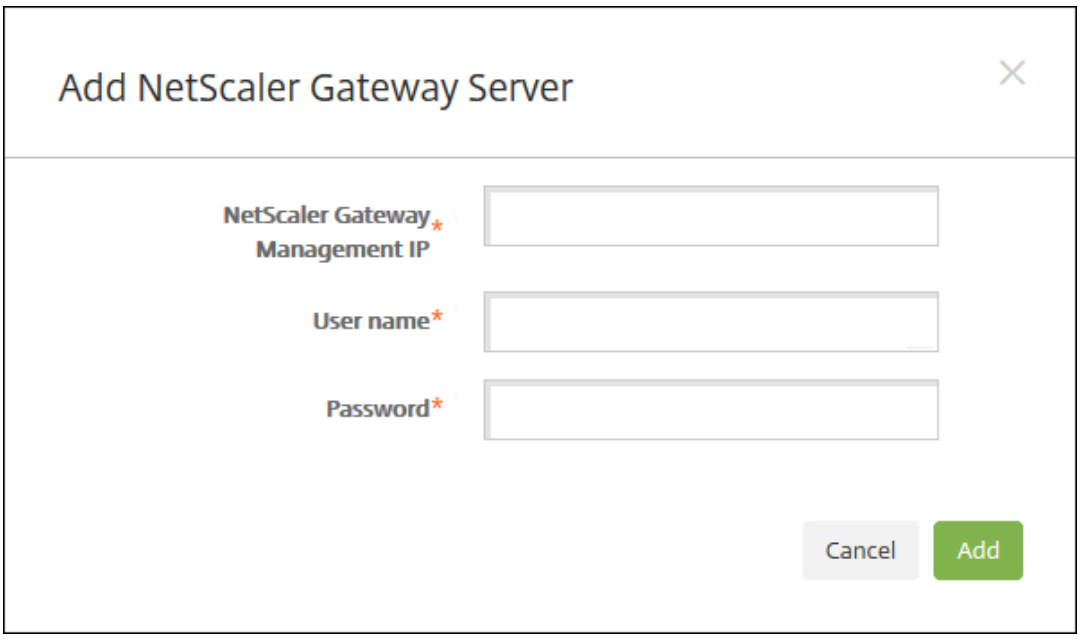


6. La opción **La anonimización de los datos de asistencia está activada** indica que la configuración predeterminada es hacer que los datos sean anónimos. La anonimización de datos significa que los datos confidenciales de usuario, servidor y red pasan a ser anónimos en los paquetes de asistencia.

   Para cambiar este parámetro, haga clic en **Anonimización y reidentificación**. Consulte Anonimato de datos en paquetes de asistencia para obtener más información acerca del anonimato de datos.

7. Marque la casilla **Paquete de asistencia para Citrix Gateway** si quiere incluir paquetes de asistencia de Citrix Gateway. A continuación, haga lo siguiente:

   a) Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar un servidor de Citrix Gateway**.



b) En **IP de administración de Citrix Gateway**, escriba la dirección IP de administración de Citrix ADC referente al dispositivo Citrix Gateway del que quiere extraer el paquete de asistencia.

> **Nota:**
>
> Si va a crear el paquete de un servidor de Citrix Gateway que ya se ha agregado, se proporciona la dirección IP.

c) En **Nombre de usuario** y **Contraseña**, escriba las credenciales de usuario necesarias para acceder al servidor con Citrix Gateway.

> **Nota:**
>
> Si va a crear un paquete de un servidor de Citrix Gateway que ya se ha agregado, se proporciona el nombre de usuario.

8. Haga clic en **Agregar**. El nuevo paquete de asistencia de Citrix Gateway se agrega a la tabla.
9. Repita el paso 7 para agregar más paquetes de asistencia de Citrix Gateway.
10. Haga clic en **Crear**. Se crea el paquete de asistencia y aparecen dos nuevos botones: **Cargar en CIS** y **Descargar en el cliente**.

Cargar 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.

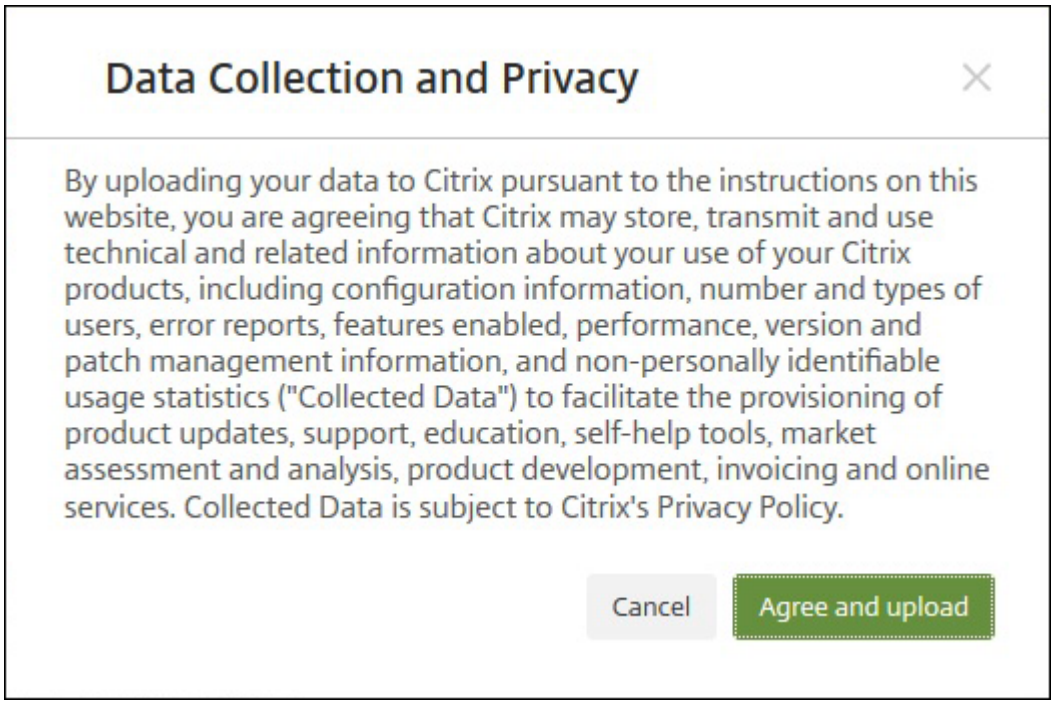
La carga desde XenMobile en CIS se realiza a través de una conexión SSL de salida. Abra el puerto 443

para la dirección IP del servidor CIS (52.88.24.76, 52.88.118.220, 52.11.72.119). Si dispone de un proxy para el tráfico HTTPS, verifique que el proxy pueda llegar a la dirección IP del servidor CIS.

A continuación, se presentan los pasos necesarios para cargar el paquete en CIS. Necesita un ID y una contraseña de My Citrix para cargar paquetes en CIS.

1. En la página **Crear paquetes de asistencia**, haga clic en **Cargar en CIS**. Aparecerá el cuadro de diálogo **Cargar en Citrix Insight Services (CIS)**.
2. En **Nombre de usuario**, escriba su ID de My Citrix.
3. En **Contraseña**, escriba su contraseña de My Citrix.
4. Para vincular este paquete con el número de una solicitud de servicio existente, marque la casilla **Asociar con número de SR** y, en los dos campos que aparecen, lleve a cabo lo siguiente:
   - En **Número de SR**, escriba el número de solicitud de servicio de ocho dígitos al que asociar este paquete.
   - En **Descripción de la SR**, escriba una descripción de la solicitud SR.
5. Haga clic en **Cargar**.

   Si es la primera vez que carga un paquete de asistencia en CIS y no ha creado ninguna cuenta en CIS con otro producto ni ha aceptado el acuerdo de recopilación de datos y privacidad, aparecerá el siguiente cuadro de diálogo. Debe aceptar el acuerdo para comenzar la carga. Si dispone de una cuenta en CIS y había aceptado el acuerdo, el paquete de asistencia se carga sin más preámbulos.



6. Lea el acuerdo y haga clic en **Aceptar y cargar**. Se cargará el paquete de asistencia.

Descargar 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 Crear paquetes de asistencia, haga clic en Descargar en el cliente. El paquete se descargará en su equipo.

El paquete de asistencia contiene archivos de valor analítico variable. Consulte la tabla siguiente para obtener una lista de archivos y su valor analítico.

Nombre del archivo	Tipo	Descripción	Valor
DbDump.json	Volcado de bases de datos JSON	Información de usuarios/dispositivos/aplicaciones	Alto
Garbage.html	Archivo HTML	Recolector de basura de Java	Bajo
MemoryInfo.html	Archivo HTML	Uso de memoria: Uso de memoria relacionada con Java	Alto
MultiNodeClusterInfo.html	Archivo HTML	Configuración del clúster	Alto
Patches.html	Archivo HTML	Información sobre parches. Mejor que xmspatches.txt	Alto
pg_dump0.sql	Volcado PG	Volcado de instancia de Postgres predeterminado	Medio
rt_db/*	Copia de base de datos (redundante, es una representación binaria de pg_dump0.sql)		N/D
sas_config/c3p0.properties	Archivo de propiedades	Propiedades de configuración de base de datos con C3P0	Medio
sas_config/catalina.pol	Archivo de directivas	Directivas de Web Server Catalina: Los archivos no cambian	Bajo

Nombre del archivo	Tipo	Descripción	Valor
sas_config/catalina.properties	Archivo de propiedades	Propiedades de Web Server Catalina: Los archivos no cambian	Bajo
sas_config/ew-config.properties	Archivo de propiedades	Información sobre la configuración del servidor XM	Alto
sas_config/ew-config-reloadable.properties	Archivo de propiedades	Información sobre el modelo de seguridad	Alto
sas_config/hazelcast.xr	Archivo XML	Registros de Hazelcast: Aparentemente, no muy útil.	Bajo
sas_config/pki.xml	Archivo XML	Se puede usar para determinar si hay un servidor PKI de terceros en uso.	Alto
sas_config/push_servic	Archivo XML	Servicios push: Los archivos no cambian	Bajo
sas_config/server.xml	Archivo XML	Información de cifrado: Relacionado con la seguridad	Alto
sas_config/sftu_config/	Archivo de propiedades	Propiedades de AppC: Los archivos no cambian	Bajo
sas_config/sftu_config/catalina.policy	Archivo de directivas	Directivas de Catalina: Los archivos no cambian	Bajo
sas_config/sftu_config/	Archivo de propiedades	Propiedades de Catalina: Los archivos no cambian	Bajo
sas_config/sftu_config/logging.properties	Archivo de propiedades	Propiedades de registro: Los archivos no cambian	Bajo

Nombre del archivo	Tipo	Descripción	Valor
sas_config/sftu_config/	Archivo XML	Información de cifrado: Relacionado con la seguridad	Alto
sas_config/sftu_config/server_migration.xml	Archivo XML	Información sobre migración	Alto
sas_config/sftu_config/	Archivo XML	Configuración de primer uso (FTU)	Alto
sas_config/sftu_config/tomcat-users.xml	Archivo XML	Usuarios de TomCat: Los archivos no cambian	Bajo
sas_config/sftu_config/	Archivo XML	Web: Los archivos no cambian	Bajo
sas_config/sftu.properties	Archivo de propiedades	Propiedades de configuración de SFTU	Alto
sas_config/variables.xml	Archivo XML	Variables: Los archivos no cambian	Bajo
sas_config/web.xml	Archivo XML	Información relacionada con el servidor web	Medio
sas_log/AdminAuditLog	Archivo de registro de Linux	Cualquier cambio de configuración	Alto
sas_log/create_sb_output.log	Archivo de registro de Linux	Salida del comando de generación de asistencia	Bajo
sas_log/DebugLogFile.log	Archivo de registro de Linux	Registro de todas las funciones	Alto
sas_log/HibernateStats.log	Archivo de registro de Linux	Registro de Hibernatestats	Bajo
sas_log/kafka-consumer.log	Archivo de registro de Linux	Registro de Kafka	Bajo
sas_log/kafka-server.log	Archivo de registro de Linux	Registro de Kafka	Bajo

Nombre del archivo	Tipo	Descripción	Valor
sas_log/kafka-topics.log	Archivo de registro de Linux	Registro de Kafka	Bajo
sas_log/LPE.log	Archivo de registro de Linux	Registro de LPE	Bajo
sas_log/migration.log	Archivo de registro de Linux	Salida del proceso de migración	Medio
sas_log/PlatformAuditLogFile.log	Archivo de registro de Linux	Información de nivel de auditoría de back-end	Alto
sas_log/PlatformDebug	Archivo de texto	Registros relacionados con el servidor back-end	Alto
sas_log/postgres.log	Archivo de registro de Linux	Registros de Postgres	Medio
sas_log/SFTU.log	Archivo de registro de Linux	Registro de SFTU	Medio
sas_log/tc1/catalina.log	Archivo de registro de Linux	Registro de Catalina	Bajo
sas_log/tc1/console	Archivo de registro de Linux	Consola	Bajo
sas_log/tc1/host-manager.log	Archivo de registro de Linux	Administrador de host	Bajo
sas_log/tc1/localhost.l	Archivo de registro de Linux	Host local	Bajo
sas_log/updates.log	Archivo de registro de Linux	Salida del proceso de aplicación de parches	Medio
sas_log/UserAuditLogF	Archivo de registro de Linux	Acciones del usuario	Alto
sas_log/zookeeper.txt	Archivo de texto	Registro de Zookeeper	Bajo
snmp/snmpd_etc_nets	Archivo de propiedades	Propiedades de configuración de SNMP	Bajo

Nombre del archivo	Tipo	Descripción	Valor
snmp/snmpd_privileges.conf	Archivo de propiedades	Propiedades de configuración de SNMP	Bajo
sys_info/arp_entries.txt	Archivo de texto	Entradas ARP en el servidor XMS	Medio
sys_info/chrony.txt	Archivo de texto	Registro de Chrony	Bajo
sys_info/diskspace_usa	Archivo de texto	Uso del espacio en disco	Alto
sys_info/firewall_rules.txt	Archivo de texto	Reglas de firewall definidas en XMS	Medio
sys_info/interface_conf	Archivo de texto	Salida de comando del sistema	Medio
sys_info/net_connections.txt	Archivo de texto	Salida de comando del sistema	Medio
sys_info/root_account_	Archivo de texto	Salida de comando del sistema	Medio
sys_info/routing_table.txt	Archivo de texto	Valor alto	Alto
sys_info/running_proce	Archivo de texto	Valor alto	Alto
sys_info/top.txt	Archivo de texto	Salida de comando del sistema	Medio
ThreadDump.html	Archivo HTML	Ya no se utiliza.	Bajo
ThreadDumpV2.html	Archivo HTML	Seguimiento de pila de subprocesos, etc.	Medio
var_log/auth.log	Archivo de registro de Linux	Registro de nivel del sistema operativo	Medio
var_log/boot.log	Archivo de registro de Linux	Registro de nivel del sistema operativo	Medio
var_log/btmp	Archivo de registro de Linux	Registro de nivel del sistema operativo	Medio
var_log/daemon.log	Archivo de registro de Linux	Registro de nivel del sistema operativo	Medio
var_log/kern.log	Archivo de registro de Linux	Registro de nivel del sistema operativo	Medio

Nombre del archivo	Tipo	Descripción	Valor
var_log/lastlog	Archivo de registro de Linux	Registro de nivel del sistema operativo	Medio
var_log/mail.log	Archivo de registro de Linux	Registro de nivel del sistema operativo	Medio
var_log/sys.log	Archivo de registro de Linux	Registro de nivel del sistema operativo	Medio
var_log/user.log	Archivo de registro de Linux	Registro de nivel del sistema operativo	Medio
var_log/wtmp	Archivo de registro de Linux	Registro de nivel del sistema operativo	Medio
version.txt	Archivo de texto	Versión del servidor XM	Medio
XENMOBILE-<IP Address>-ConnectivityCheckResults.xml	Archivo XML	Resultados de la comprobación de conectividad en el servidor XMS	Medio
xmspatches.txt	Archivo de texto	Información sobre parches.	Alto

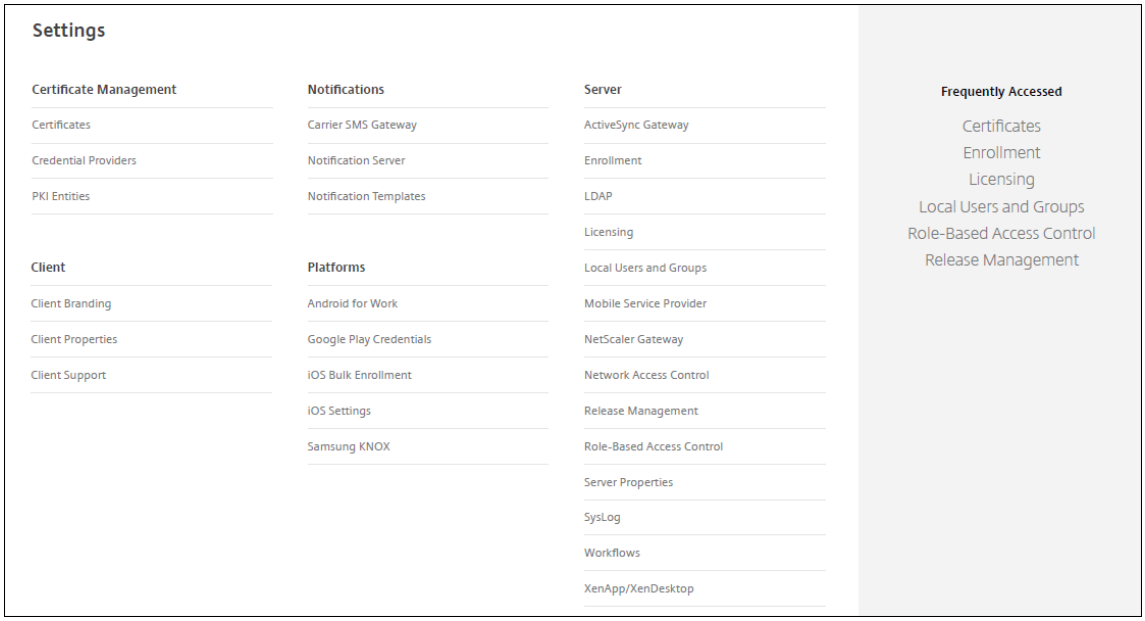
Opciones de asistencia y Remote Support

January 4, 2022

Puede proporcionar una dirección de correo electrónico para que los usuarios se pongan en contacto con el personal de asistencia. Cuando los usuarios soliciten asistencia desde sus dispositivos, verán esa dirección de correo.

También puede configurar cómo deben enviar los usuarios registros al servicio de asistencia desde sus dispositivos. Puede definir que los registros se envíen directamente o por correo electrónico.

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



2. En **Cliente**, haga clic en **Asistencia del cliente**. Aparecerá la página **Asistencia del cliente**.
3. Configure los siguientes parámetros:
   - **Correo electrónico de asistencia (servicio de asistencia técnica de TI):** Escriba la dirección de correo electrónico de contacto referente al servicio de asistencia de TI.
   - **Enviar registros del dispositivo al servicio de asistencia técnica de TI:** Seleccione si los registros del dispositivo se envían **directamente** o **por correo electrónico**. El valor predeterminado es **por correo electrónico**.
     - Cuando se habilita **directamente**, aparecen opciones de registros de almacén en ShareFile (ahora llamado Citrix Content Collaboration). Si habilita los registros de almacén en Citrix Content Collaboration, estos se envían directamente a Citrix Files. De lo contrario, los registros se enviarán a XenMobile y, a continuación, por correo electrónico al servicio de asistencia. Además, aparecerá la opción **Si el envío directo falla, usar el correo electrónico**, 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 inhabilita esta opción y hay problemas con el servidor, los registros no se enviarán.
     - Al habilitar la opción **por correo electrónico**, siempre se usará el correo electrónico del cliente para enviar los registros.
4. Haga clic en **Guardar**.

Remote Support

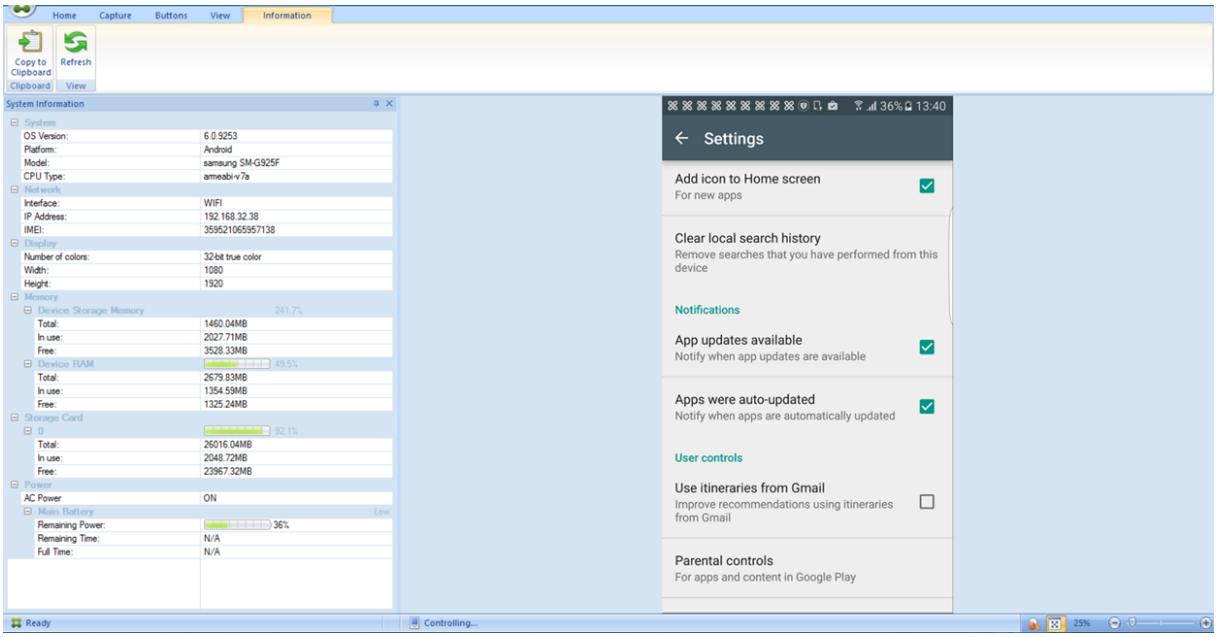
> **Nota:**
>
> Remote Support no está disponible para nuevos clientes desde el 1 de enero de 2019. Los clientes existentes pueden seguir utilizando el producto, pero Citrix no proporcionará mejoras ni correcciones.

Para las implementaciones locales de XenMobile Server, la asistencia remota (Remote Support) permite que el personal de Help Desk tome el control remoto de los dispositivos móviles Windows CE y Android administrados. La transmisión de la pantalla solo se admite en dispositivos Samsung Knox.

Remote Support no está disponible para implementaciones locales en clúster de XenMobile Server.

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 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 encuentra el dispositivo, puede borrarlo para salvaguardar la información confidencial que pueda contener.

Remote Support también permite al personal de asistencia técnica:

- Ver una lista de todos los dispositivos conectados en una o varias instancias XenMobile.
- Mostrar información del sistema, incluidos el modelo del dispositivo, el nivel del sistema operativo, la identidad de equipo móvil internacional (IMEI), el número de serie, el estado de la memoria y la batería, y la conectividad.
- Ver los usuarios y los grupos de 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 móviles de ancho de banda bajo gracias al control remoto en tiempo real de 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 en directo con una pizarra compartida, comunicaciones de voz basadas en VoIP y chat entre usuarios móviles y el personal de asistencia.

Requisitos del sistema para Remote Support

El software de Remote Support se puede instalar en equipos Windows que cumplan los siguientes requisitos. Para conocer los requisitos de puertos, consulte Requisitos de puertos.

Plataformas admitidas:

- 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 compatibles:

- 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 o Windows 11
- Microsoft Windows 8
- Microsoft Windows 7

Para instalar Remote Support desde la línea de comandos

Ejecute este comando:

```
1 \*RemoteSupport\*.exe /S
```

RemoteSupport es el nombre del programa de instalación. Por ejemplo:

```
1 XenMobileRemoteSupport-9.0.0.35265.exe /S
```

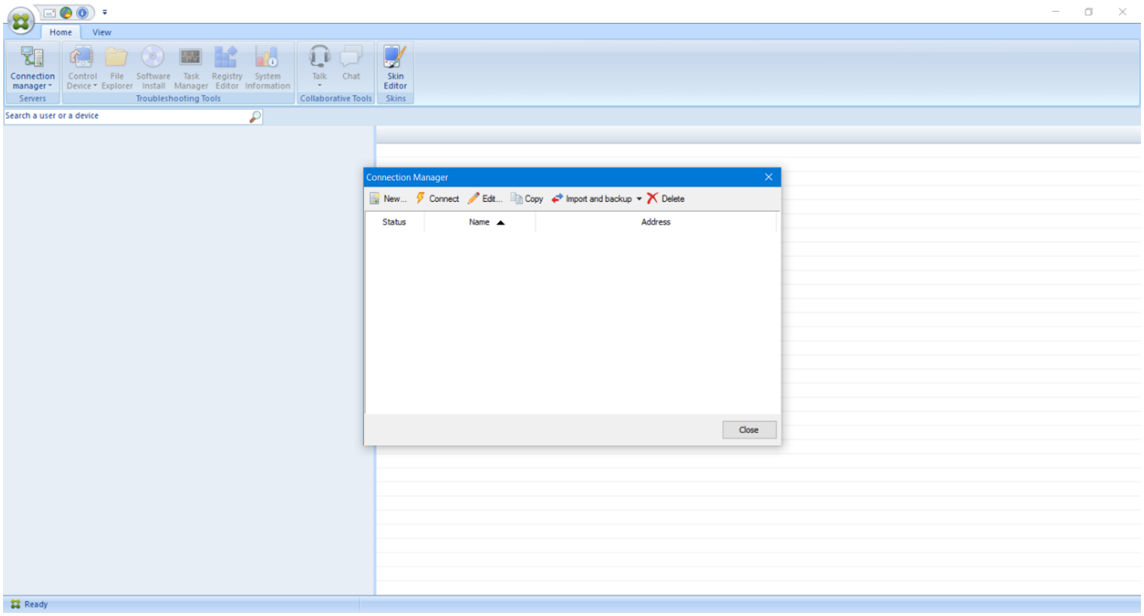
Puede utilizar las siguientes variables al instalar el software de Remote Support:

- /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 de 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**, escriba 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 de XenMobile Server.

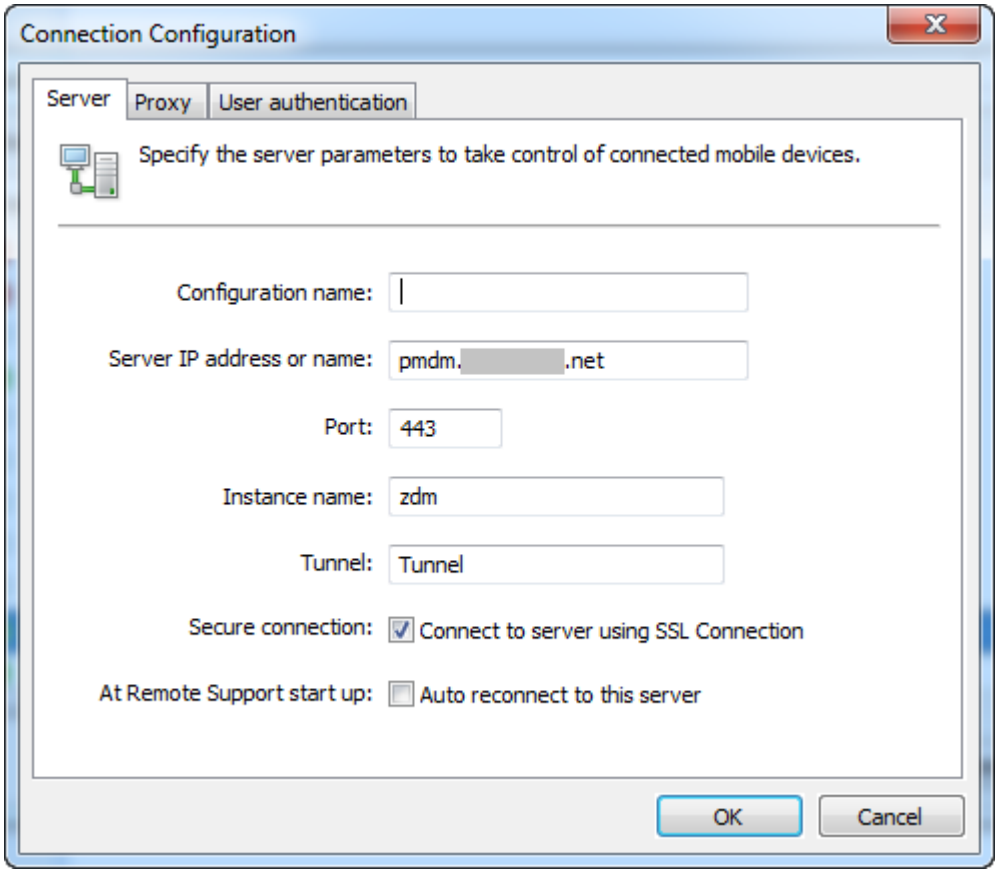
    c) En **Port**, escriba un número de puerto TCP, como se define en la configuración del servidor de XenMobile Server.

    d) En **Instance name**, si XenMobile forma parte de una implementación multiarrendatario, escriba un nombre de instancia.

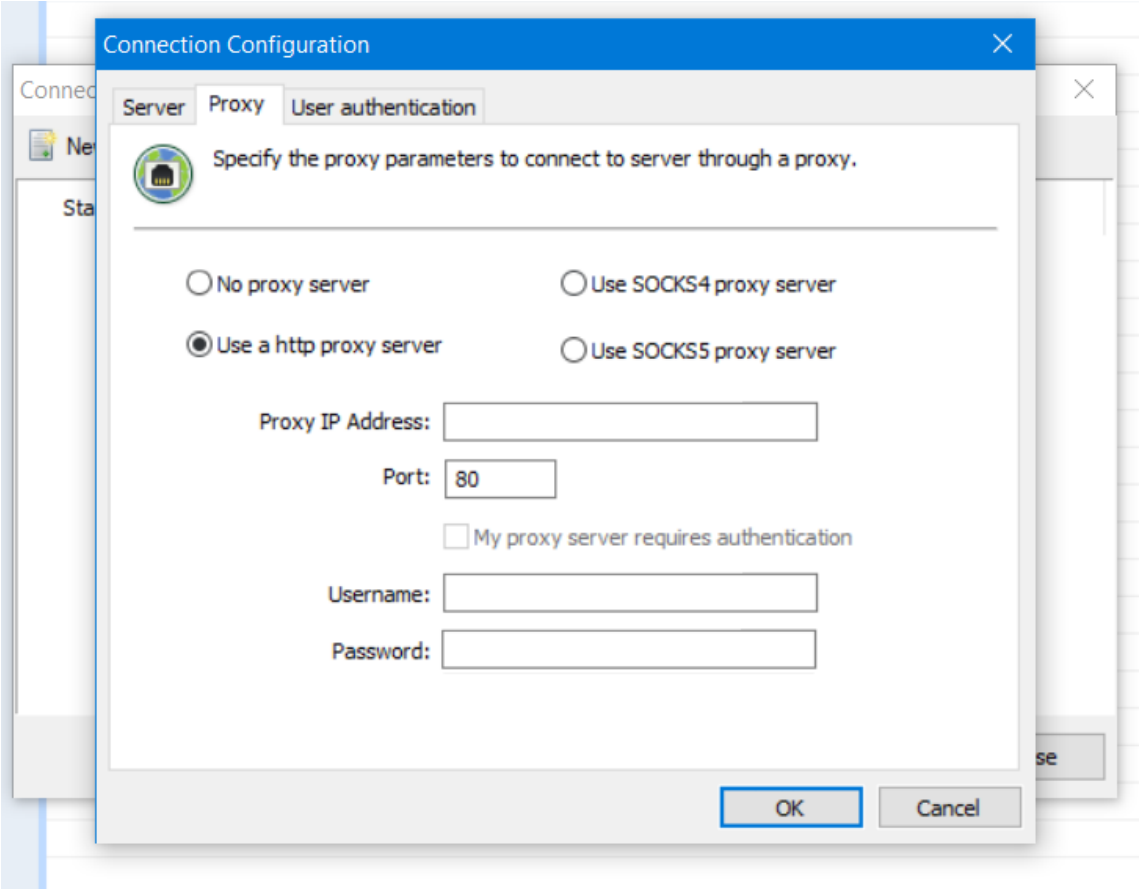
    e) En **Tunnel**, escriba el nombre de la directiva de túnel.

    f) Marque la casilla **Connect to server using SSL Connection**.

    g) Marque la casilla **Auto reconnect to this server** para conectarse al servidor de XenMobile Server configurado cada vez que se inicie la aplicación Remote Support.



4. En la ficha **Proxy**, seleccione **Use an 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 **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:

- **Básica:** Permite ver la información de diagnóstico sobre el dispositivo. Por ejemplo: 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.
- **Premium:** Permite controlar de forma remota la pantalla del dispositivo. Por ejemplo: permite controlar los colores de la ventana, establecer una sesión VoIP entre el servicio de asistencia y el usuario, y establecer una sesión de chat entre el usuario y el departamento de asistencia.

Para 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**. Para la plataforma Samsung SAFE, la clave ELM se implementa automáticamente en los dispositivos Samsung cuando se inscriben en XenMobile. Por lo tanto, no seleccione la plataforma Samsung SAFE para esta directiva. 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 Remote Support, consulte Directiva de Remote Support.

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 de XenMobile Server se indican con un icono verde.
2. Para ver 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 de XenMobile Server pero no asignados a ningún usuario aparecen en modo anónimo. (La cadena **Anonymous** aparecerá en la lista.) Estos dispositivos pueden controlarse como los de un usuario con sesión iniciada.

Para controlar un dispositivo, selecciónelo 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.
- Modificar 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 XenMobile Server.

Syslog

November 6, 2020

Puede configurar XenMobile Server (solo en implementaciones locales) 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

XenMobile utiliza el appender log4j de syslog para enviar mensajes de syslog con el formato RFC5424. Los datos del mensaje syslog no tienen ningún formato específico.

Puede usar esta información para analizar el origen de la alerta y, si fuera necesario, realizar las correcciones oportunas.

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Haga clic en **Syslog**. Aparecerá la página **Syslog**.
3. Configure estos parámetros:
    - **Servidor:** Escriba la dirección IP o el nombre de dominio completo (FQDN) del servidor syslog.
    - **Puerto:** Escriba el número de puerto. De forma predeterminada, el puerto está configurado en 514.

- **Información para registrar:** Marque o desmarque **Registros del sistema** y **Auditoría**.
  - 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.
  - Registros de depuración para XenMobile.

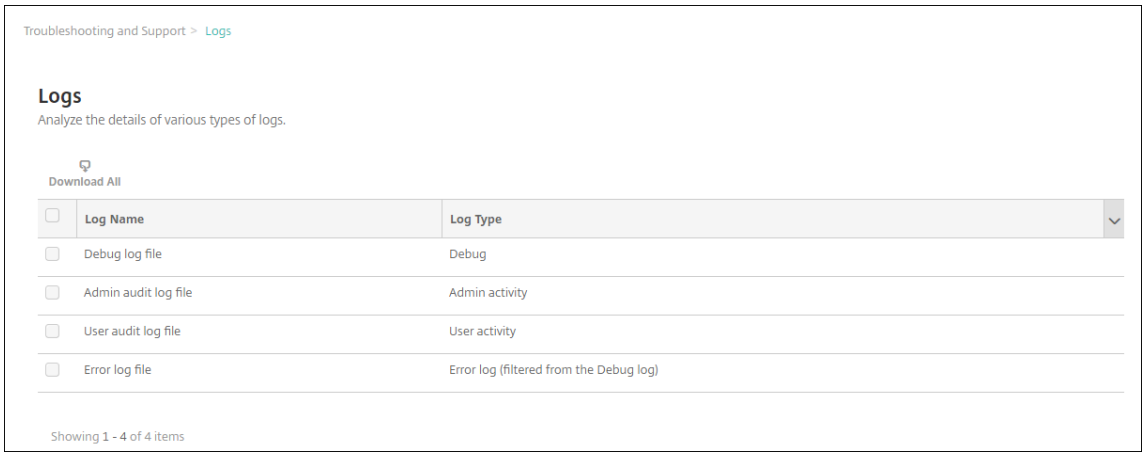
4. Haga clic en **Guardar**.

Ver archivos de registros en XenMobile

September 19, 2021

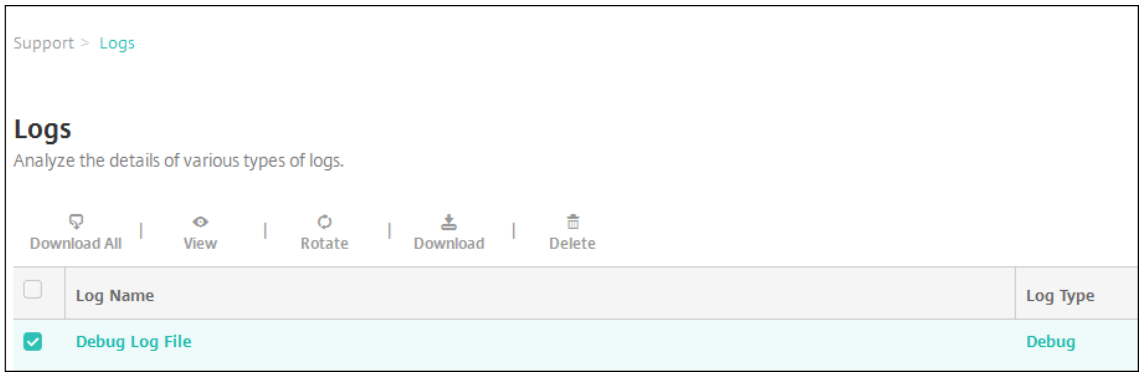
Consulte, modifique y descargue registros para la administración con XenMobile.

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. Se abrirá la página **Asistencia**.
2. En **Operaciones con registros**, haga clic en **Registros**. Aparecerá la página **Registros**. Los registros individuales se muestran en una tabla.



3. Seleccione el registro que quiera ver:
   - Los archivos de registros de depuración contienen información muy útil para Citrix Support, como, por ejemplo, mensajes de error y acciones relacionadas con el servidor.
   - Los archivos de registros de auditoría de administración contienen información de auditoría sobre actividad en la consola de XenMobile.
   - Los archivos de registros de auditoría de usuarios contienen información relacionada con los usuarios configurados.
   - Los archivos de registros de errores solo contienen mensajes de error filtrados de los registros de depuración.

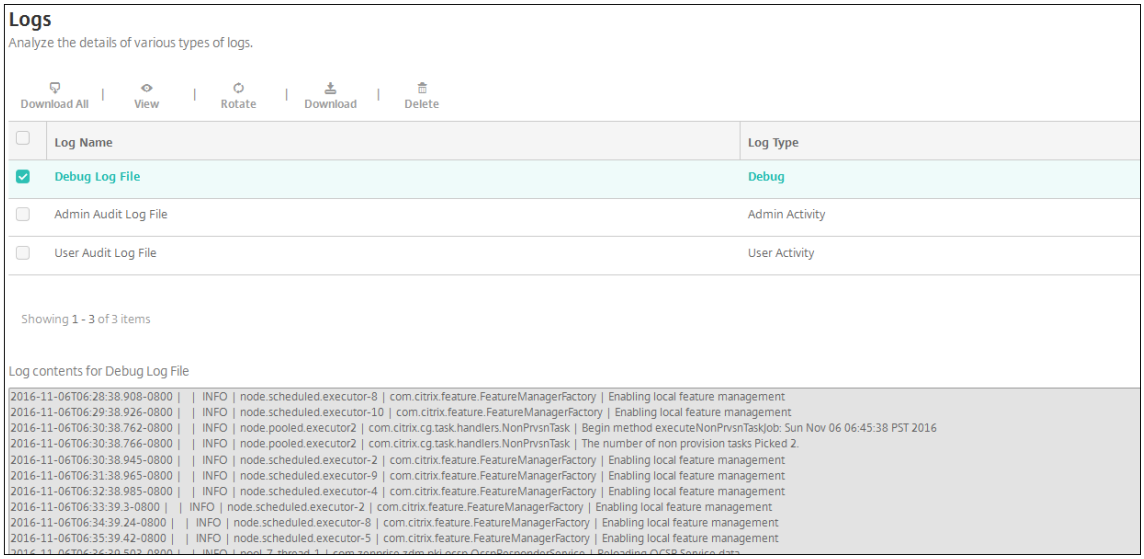
4. Use las acciones de la parte superior de la tabla para descargar uno o todos los registros, verlos, girarlos o eliminarlos.



> **Nota:**
>
> - Si selecciona varios archivos de registros, solo estarán disponibles las opciones **Descargar todo** y **Girar**.
> - Si tiene servidores de 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:

   - **Descargar todo:** 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).
   - **Ver:** Muestra, debajo de la tabla, el contenido de los registros seleccionados.
   - **Girar:** Almacena el archivo de registros 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 “Girar” para continuar.
   - **Descargar:** La consola descarga el único tipo de archivo de registros seleccionado y también descarga otros registros ya archivados del mismo tipo.
   - **Eliminar:** Quita permanentemente los archivos de registros seleccionados.



Herramienta XenMobile Analyzer

January 4, 2022

XenMobile Analyzer es una herramienta basada en la nube que sirve para diagnosticar y solucionar problemas relacionados con la configuración 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.

Configure la herramienta para que apunte a XenMobile Server y facilite información, como el tipo de implementación del servidor, la plataforma móvil, el tipo de autenticación y las credenciales de usuario. Cuando apunta al servidor pertinente, la herramienta se conecta a él y analiza el entorno para buscar problemas de configuración. Si XenMobile Analyzer detecta problemas, la herramienta muestra recomendaciones para corregirlos.

Funciones principales

- Microservicio seguro basado en la nube para solucionar todo tipo de problemas técnicos relacionados con XenMobile.
- Recomendaciones precisas para resolver los problemas de configuración de XenMobile.
- Menos llamadas de asistencia y solución de problemas más rápida en entornos de XenMobile.
- Asistencia inmediata para versiones de XenMobile Server.
- Programación de comprobaciones diarias o semanales del estado de la implementación.
- Comprobaciones de la configuración de Citrix ADC.
- 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) de Citrix Files.

Novedades

- El informe de configuración de Citrix ADC muestra una insignia de notificación que indica la cantidad de recomendaciones. Las recomendaciones se basan en comprobaciones de configuración esenciales en un dispositivo Citrix Gateway concreto.
- Los iconos en la barra de navegación global en la página Test Environment List se han cambiado de orden para mejorar la experiencia de usuario.

En el vídeo siguiente se muestran los cambios de navegación realizados en la interfaz de usuario.

Citrix XenMobile Analyzer: interfaz de la nueva lista de entornos

Esto es un vídeo insertado. Haga clic en el enlace para verlo

> **Nota:**
>
> Este vídeo no contiene sonido. Se ve mejor en el modo de pantalla completa.

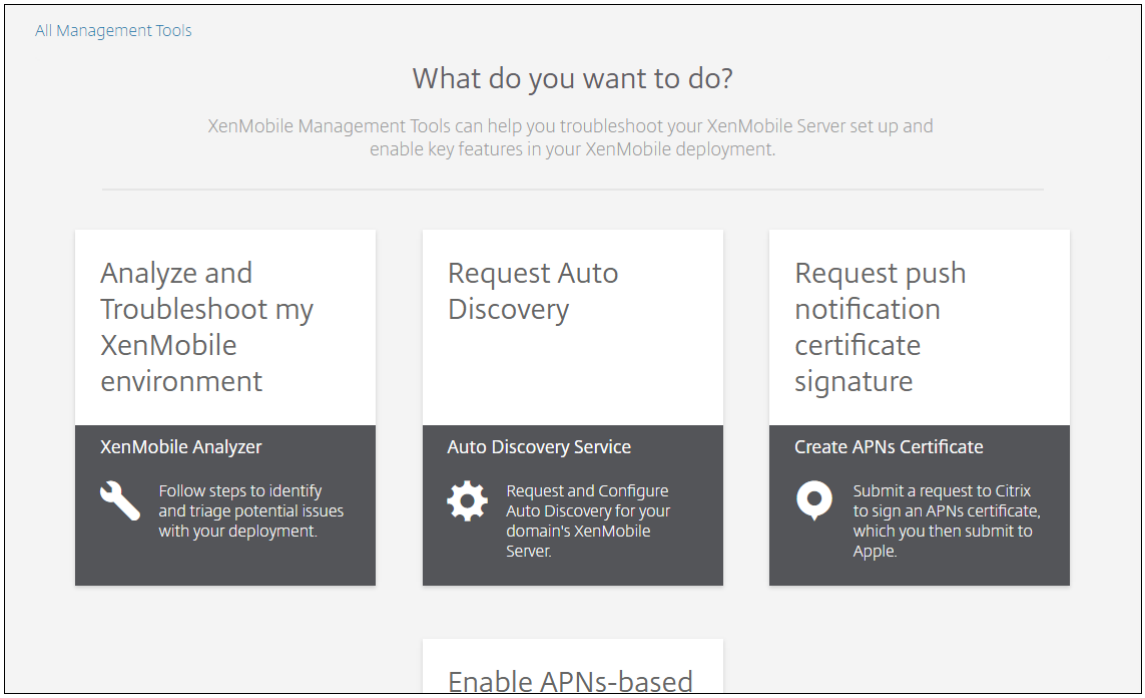
Acceder a XenMobile Analyzer e iniciarlo

Requisitos previos

Producto	Versión compatible
XenMobile Server	10.1.0 y versiones posteriores
Citrix Gateway	10.5 y versiones posteriores
Simulación de inscripción de clientes	iOS y Android

Se puede acceder a XenMobile Analyzer mediante estos métodos:

- En la consola de XenMobile, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha de la consola para abrir la página **Solución de problemas y asistencia**.
- Utilice sus credenciales de My Citrix para acceder a la herramienta desde https://tools.xm.cloud.com/. En la página XenMobile Management Tools que se abre, haga clic en **Analyze and Troubleshoot my XenMobile Environment** para iniciar XenMobile Analyzer.



XenMobile Analyzer contiene cinco opciones diseñadas para guiarle en el proceso de evaluación de errores y, con ello, reducir la cantidad de tíquets de asistencia. Las opciones pueden reducir los costes para todo el mundo.

Opciones disponibles:

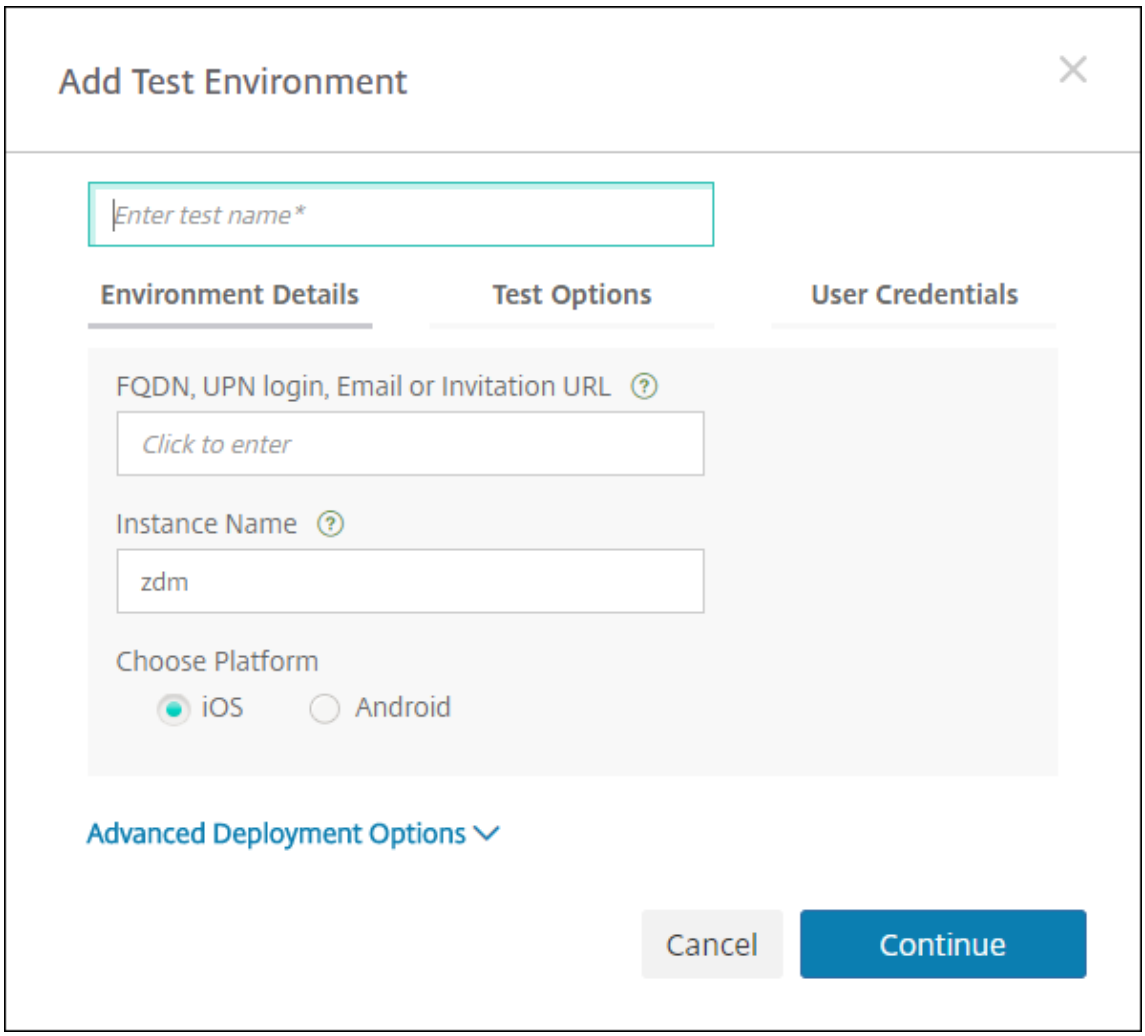
- **Environment Check (Comprobación del entorno):** Este paso le guía a la hora de configurar pruebas para comprobar si hay problemas. También ofrece recomendaciones y soluciones para problemas de dispositivo, inscripción de usuarios y autenticación.
- **Citrix ADC Check (Comprobación de Citrix ADC):** Este paso le guía en la comprobación de sus configuraciones de Citrix ADC para preparar la implementación de XenMobile.
- **Advanced Diagnostics (Diagnósticos avanzados):** Este paso ofrece información sobre cómo usar Citrix Insight Services para buscar otros problemas que no se hayan detectado en la comprobación del entorno.
- **Server Connectivity Checks (Comprobaciones de conectividad de los servidores):** Este paso indica cómo probar la conectividad de los servidores.
- **Contact Citrix Support (Contactar con la asistencia de Citrix):** Este paso enlaza con el sitio donde puede abrir un caso de asistencia técnica de Citrix Support, si los problemas no se han solucionado.

En las secciones siguientes se describe cada opción en más detalle.

Comprobación del entorno

1. Inicie sesión en XenMobile Analyzer y haga clic en **XenMobile Environment**.

2. Haga clic en **Add Test Environment**.
3. En el cuadro de diálogo **Add Test Environment**, lleve a cabo lo siguiente:



a) Proporcione un nombre único a la prueba para poder identificarla en el futuro.

b) En el campo **FQDN, UPN login, Email or URL Invitation**, escriba la información que va a utilizarse para acceder al servidor.

c) En **Instance Name**, escriba el valor de su instancia personalizada, si la usa.

d) 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. 1. Las opciones disponibles son: **Enterprise (MDM+MAM)**, **App Management (MAM)** o **Device Management (MDM)**.

f) Haga clic en **Continue**.

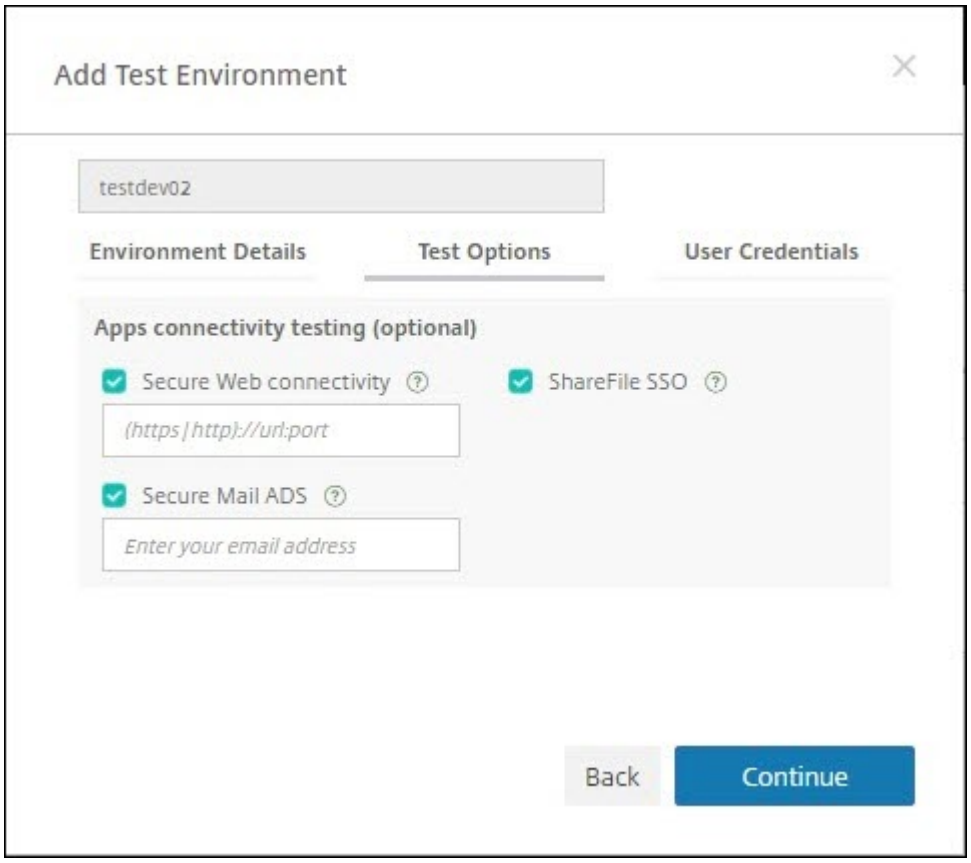
4. En la ficha **Test Options**, seleccione una o varias de las siguientes pruebas y, a continuación, haga clic en **Continue**.

a) **Secure Web Connectivity**. Proporcione una URL de intranet. La herramienta comprueba la disponibilidad de la URL. Se detectan problemas de conectividad, si los hay, que po-

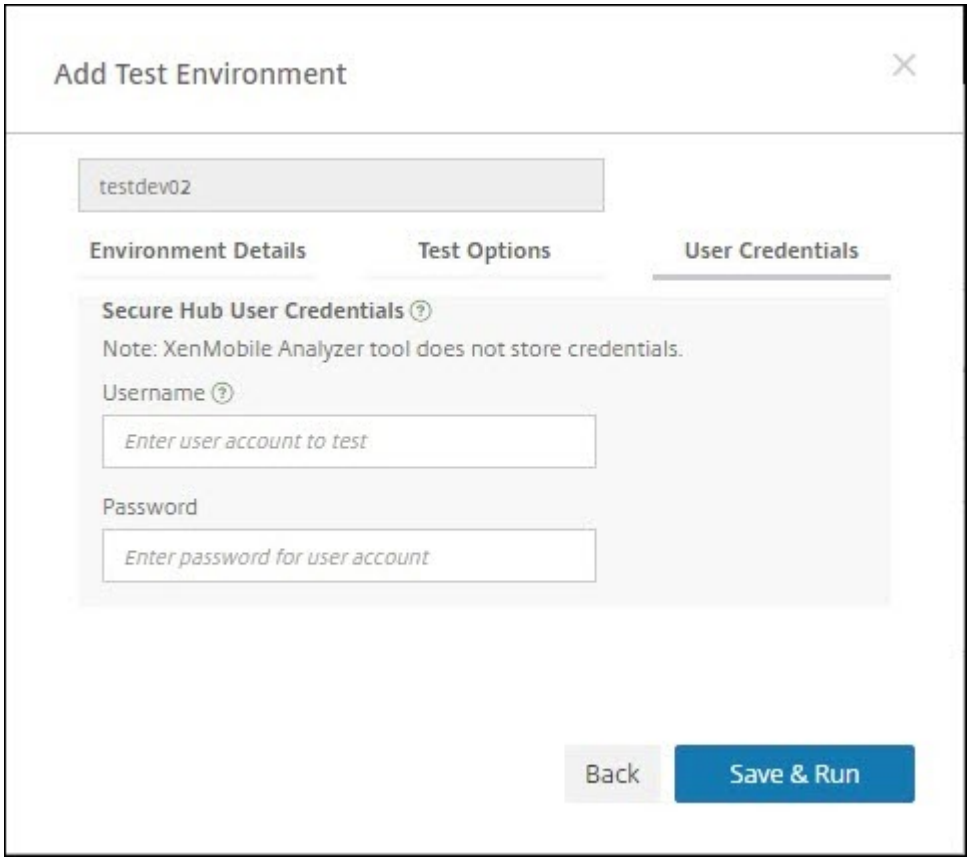
drían darse en la aplicación Secure Web cuando intente acceder a las direcciones URL de intranet.

b) **Secure Mail ADS**. Introduzca un ID de correo electrónico de usuario. Este ID se utiliza para comprobar la detección automática de Microsoft Exchange Server en el entorno de XenMobile. Detecta si hay problemas relacionados con la detección automática de Secure Mail.

c) **ShareFile SSO**. Si se selecciona, XenMobile Analyzer comprueba si la resolución de DNS de Citrix Files se realiza correctamente. La herramienta también comprueba si el inicio de sesión Single Sign-On (SSO) de Citrix Files es compatible con las credenciales de usuario proporcionadas.



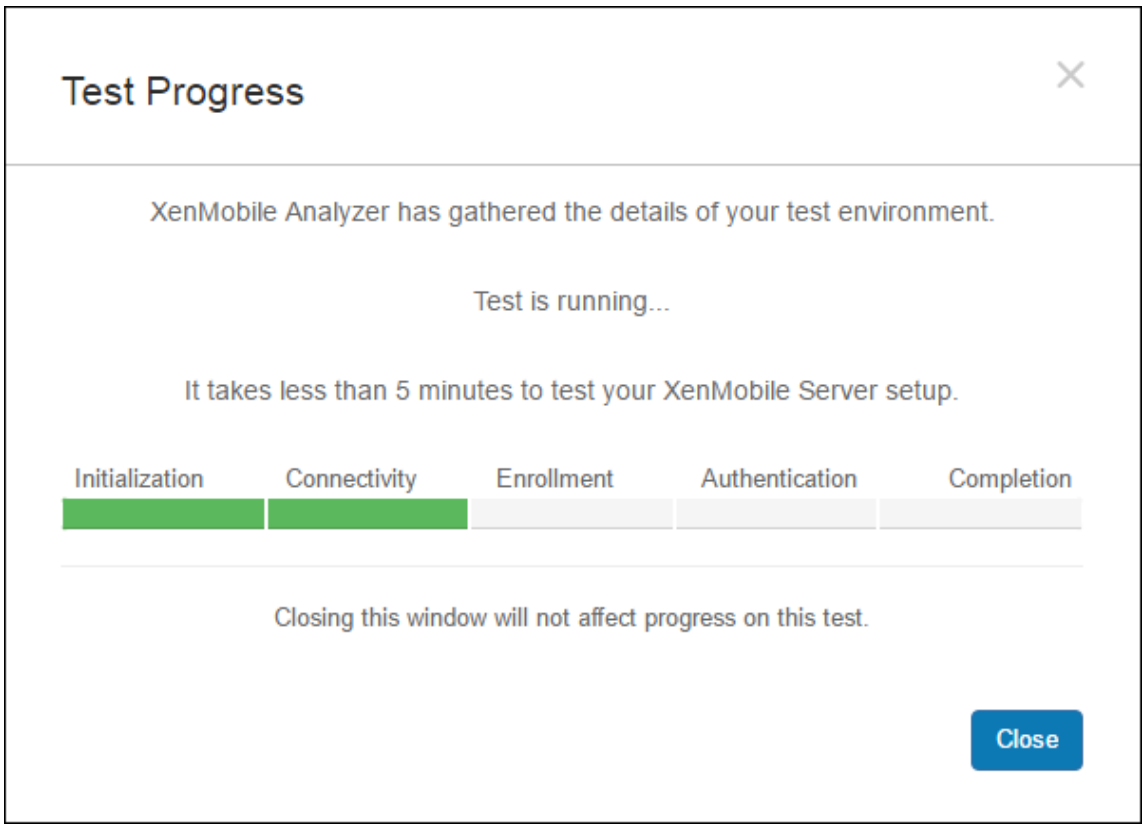
5. Según cómo esté configurado el servidor, verá diferentes campos disponibles para introducir las credenciales de usuario en la ficha **User Credentials**. Los campos posibles son: **Username**, **Username and Password** o **Username, Password** y **Enrollment PIN**.



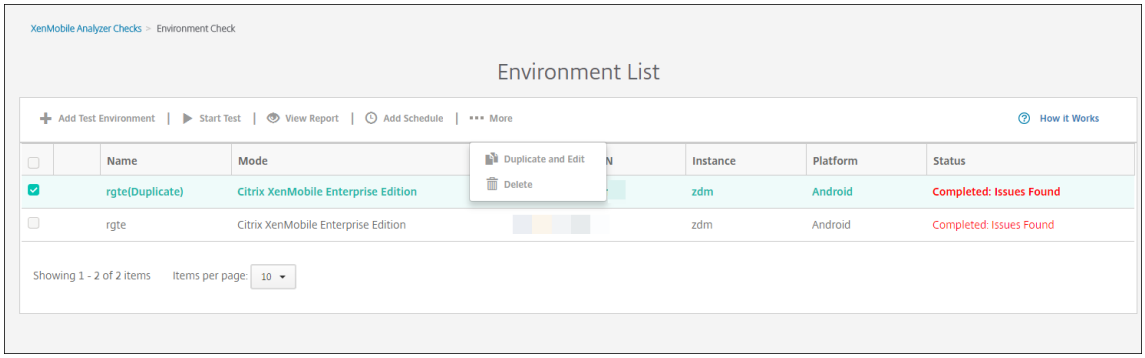
6. Haga clic en **Save & Run** para iniciar la ejecución de las pruebas.

   Aparecerá una notificación de progreso. Puede dejar el cuadro de diálogo de progreso abierto o cerrarlo; las pruebas continuarán ejecutándose.

   Las pruebas superadas aparecen en verde. Las pruebas que fallan aparecen en rojo.



Después de cerrar el cuadro de diálogo de progreso, volverá a la página **Environments List**.



La página **Results** muestra los detalles de la prueba, las recomendaciones y los resultados.

7. Haga clic en el icono **View Report** para ver los resultados de la prueba.

   Si las recomendaciones tienen artículos de Citrix Knowledge Base asociados a ellas, los artículos se enumeran en la página.

8. Haga clic en la ficha **Results** para ver la categoría individual y las pruebas realizadas por la herramienta, con sus resultados correspondientes.

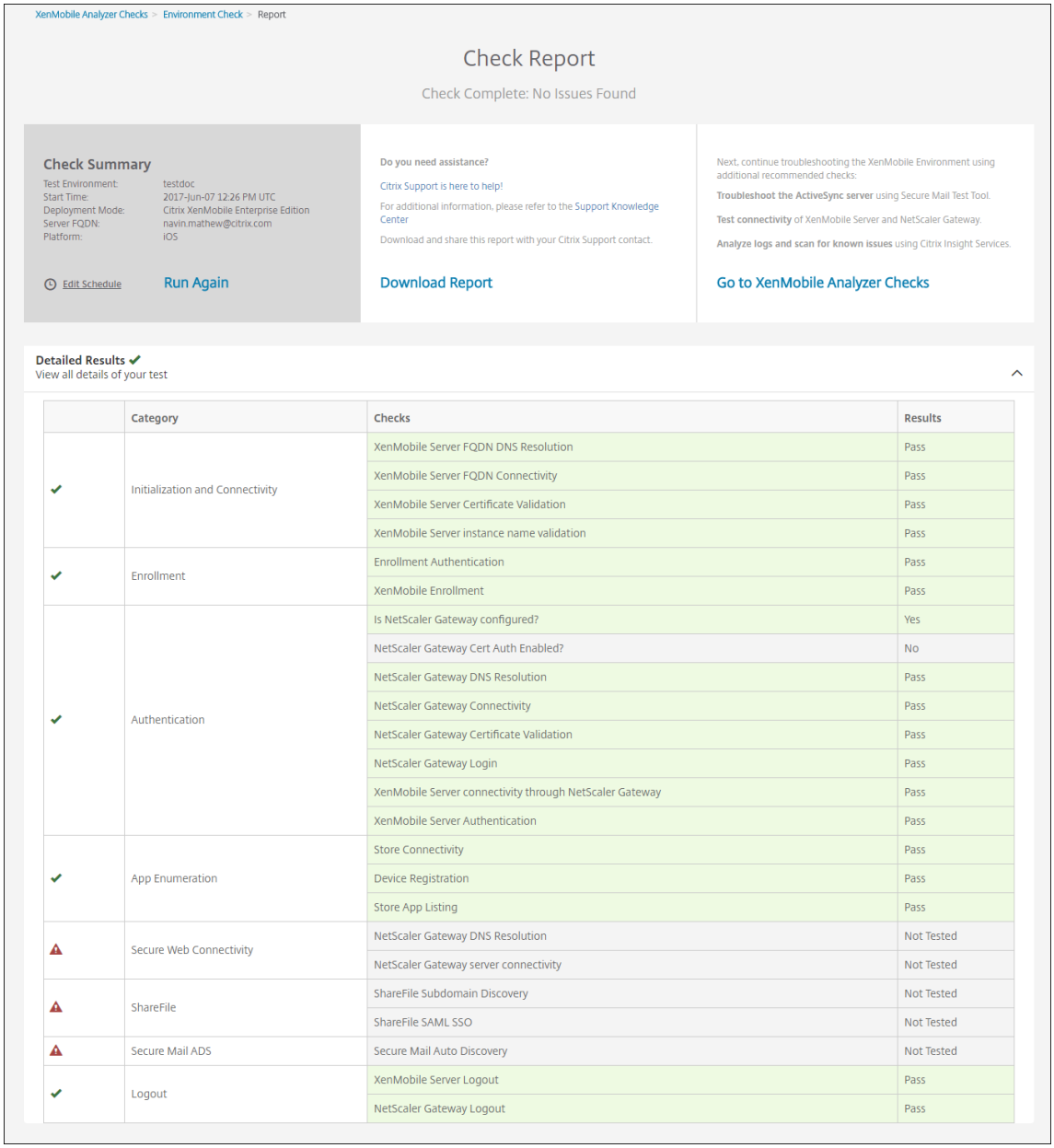
   a) Para descargar el informe, haga clic en **Download report**.

   b) Para volver a la lista de entornos de prueba, haga clic en **Environment Check**.

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**.

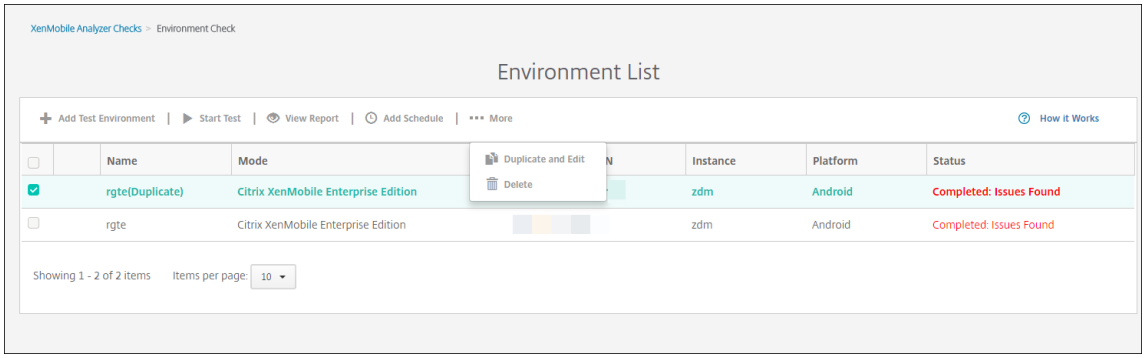
e) Para seleccionar otra opción de XenMobile Analyzer, haga clic en **Go To XenMobile Analyzer Checks**.

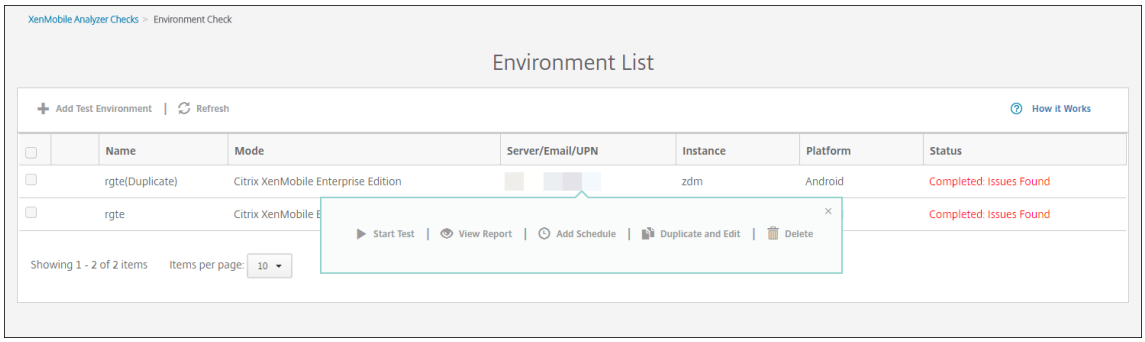


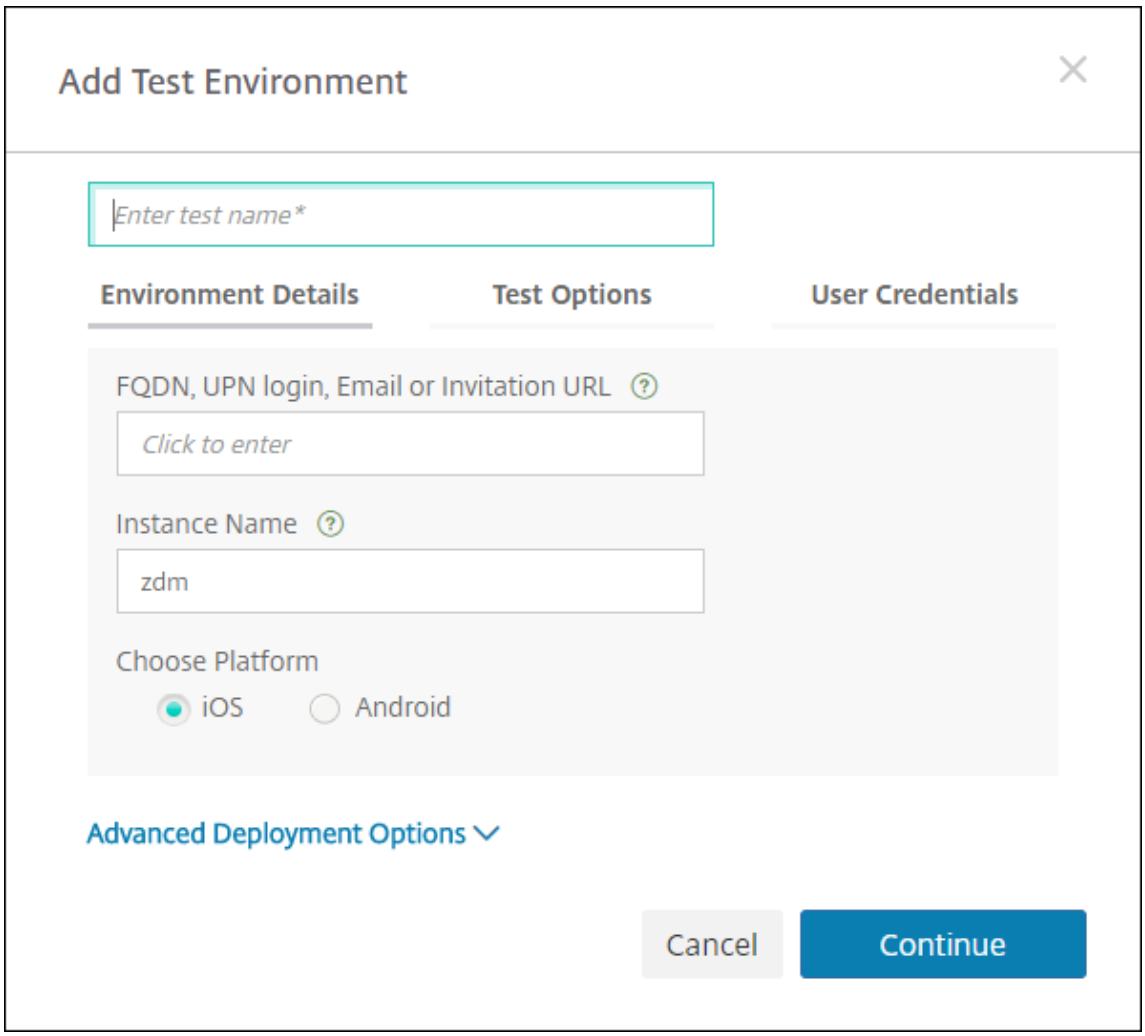
	Category	Checks	Results
✔	Initialization and Connectivity	XenMobile Server FQDN DNS Resolution	Pass
		XenMobile Server FQDN Connectivity	Pass
		XenMobile Server Certificate Validation	Pass
		XenMobile Server instance name validation	Pass
✔	Enrollment	Enrollment Authentication	Pass
		XenMobile Enrollment	Pass
✔	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	Store Connectivity	Pass
		Device Registration	Pass
		Store App Listing	Pass
⚠	Secure Web Connectivity	NetScaler Gateway DNS Resolution	Not Tested
		NetScaler Gateway server connectivity	Not Tested
⚠	ShareFile	ShareFile Subdomain Discovery	Not Tested
		ShareFile SAML SSO	Not Tested
⚠	Secure Mail ADS	Secure Mail Auto Discovery	Not Tested
✔	Logout	XenMobile Server Logout	Pass
		NetScaler Gateway Logout	Pass

9. Desde la página Test Environments, puede copiar y modificar las pruebas. Para ello, seleccione una prueba, y haga clic en **More**, y seleccione **Duplicate and Edit**.

   Se crea una copia de la prueba seleccionada y se abre el cuadro de diálogo “Add Test Environment”, lo que le permite modificar la nueva prueba.



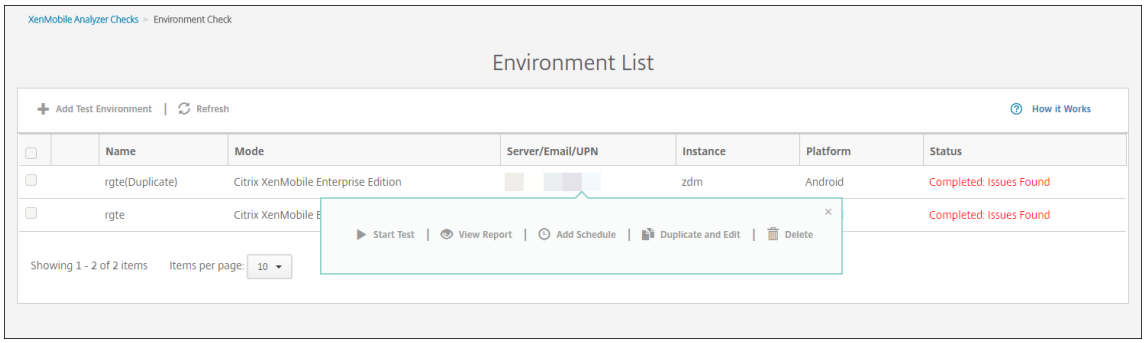




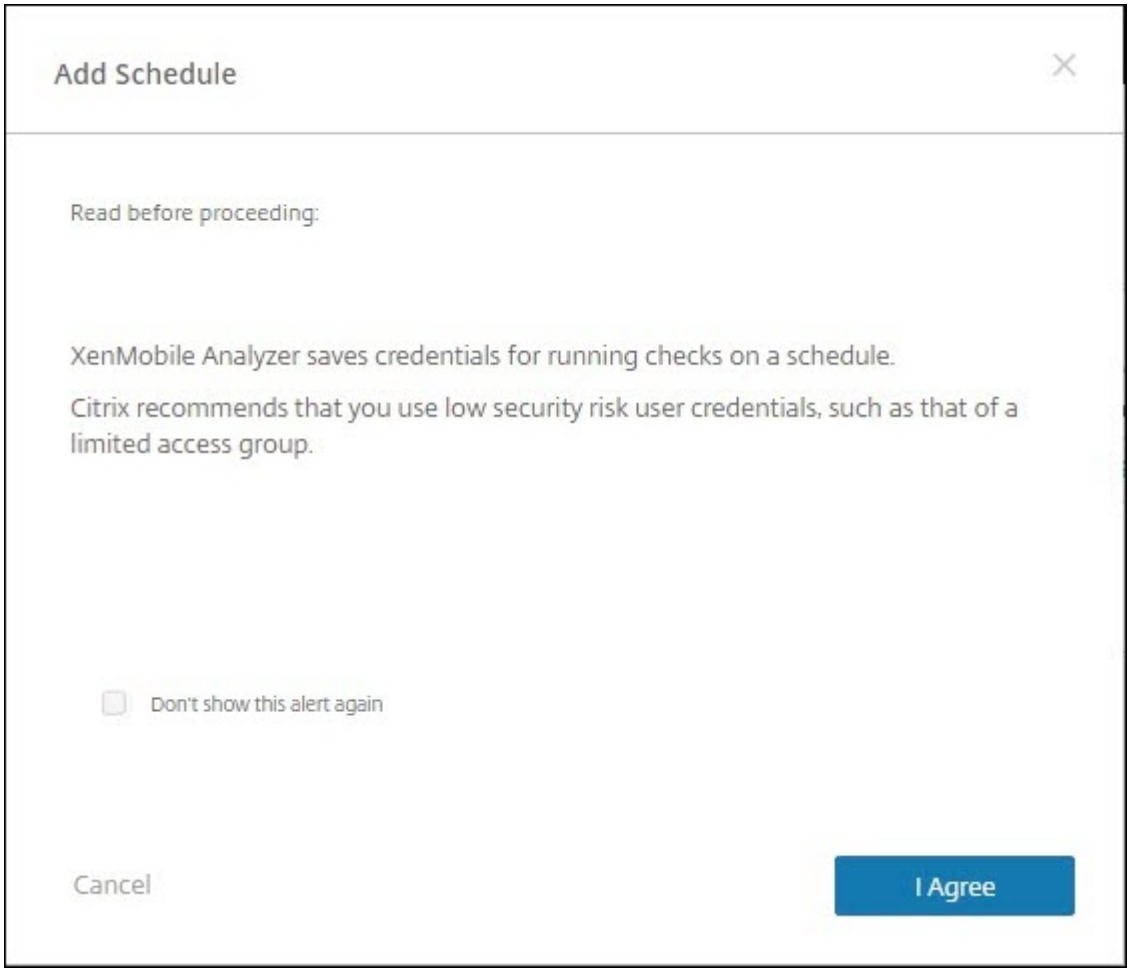
Agregar una programación para comprobaciones del entorno

Puede configurar las pruebas para que se ejecuten siguiendo una programación automática, con los resultados que se enviarán a la lista de usuarios que configure.

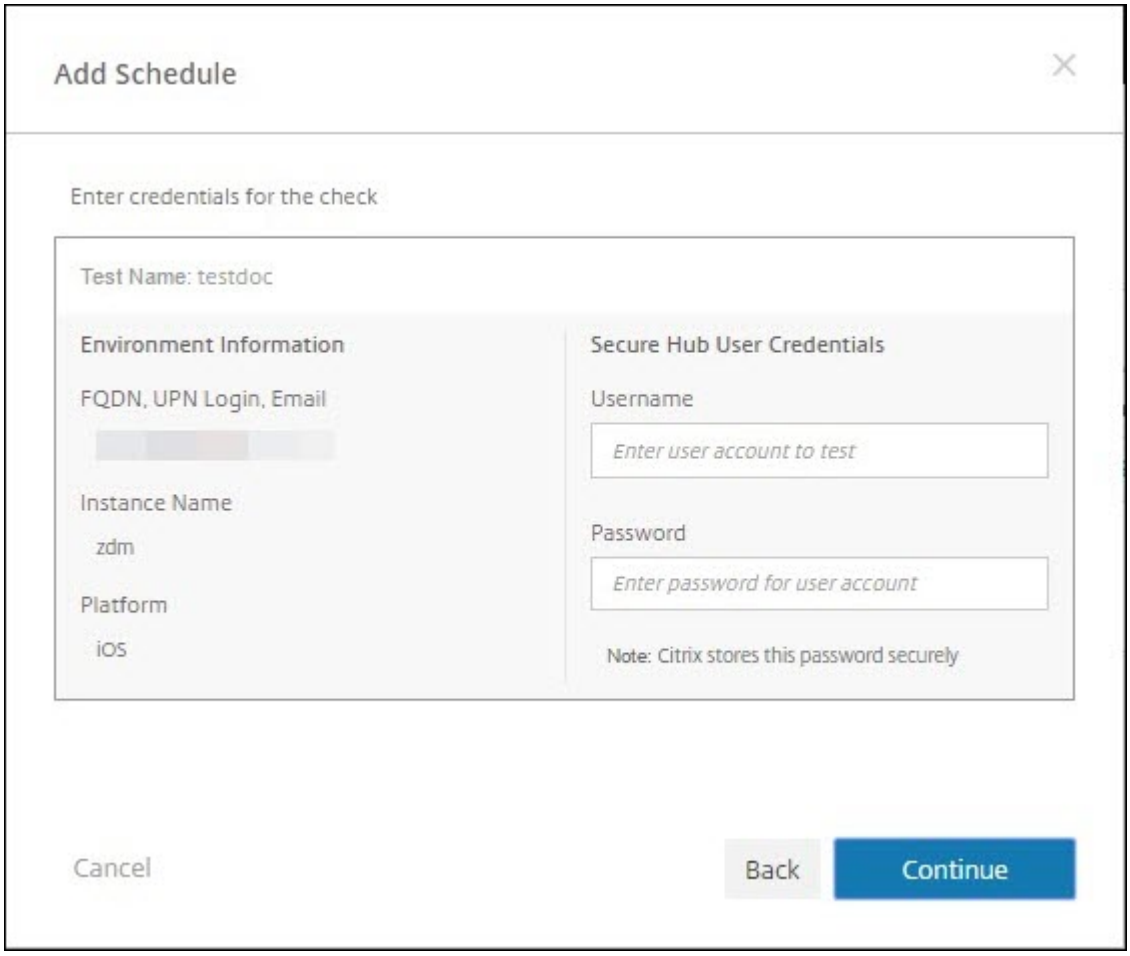
1. En la página **Environment List**, seleccione el entorno para el que quiere configurar una programación y haga clic en **Add schedule**.



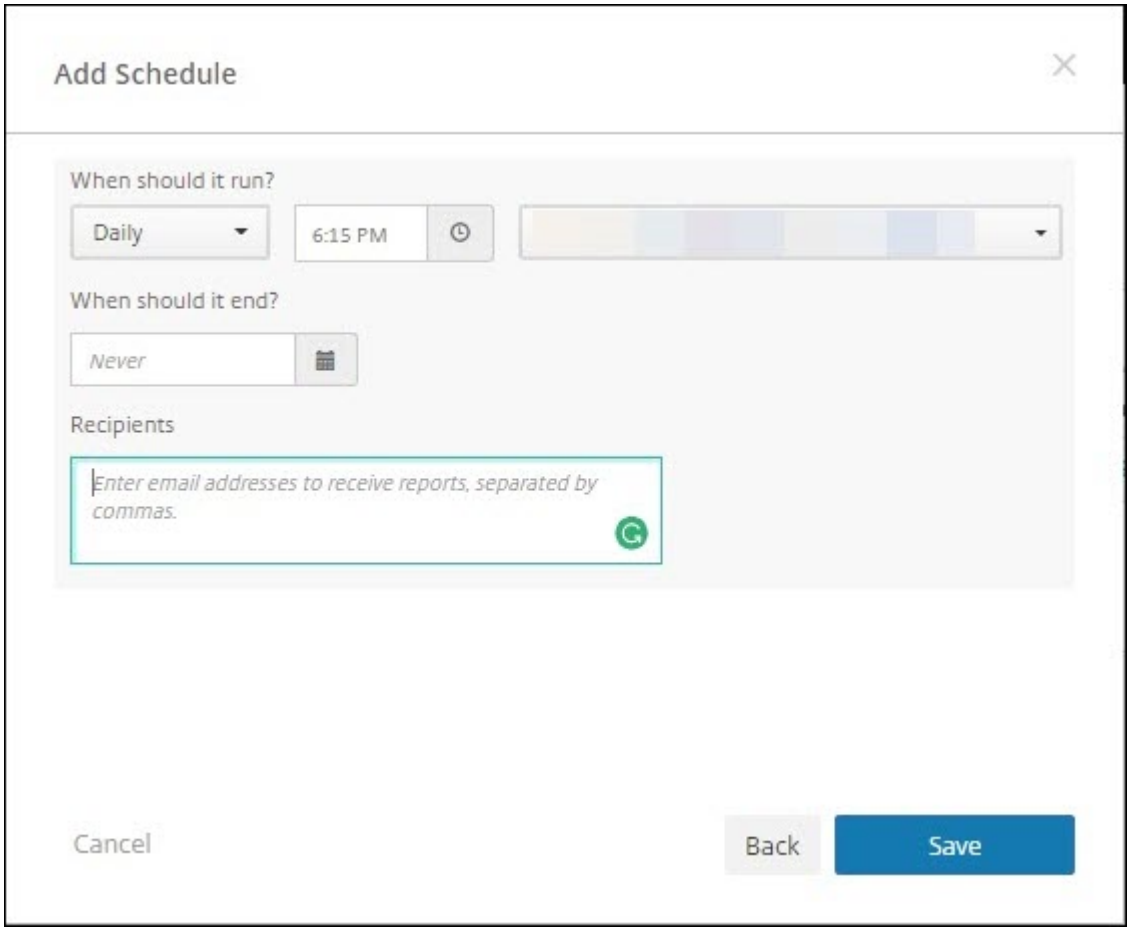
2. La ventana **Add Schedule** muestra un mensaje que le advierte de que XenMobile Analyzer guarda las credenciales para ejecutar pruebas programadas. Citrix recomienda utilizar una cuenta con acceso limitado para ejecutar pruebas programadas. Haga clic en **I Agree** para continuar.



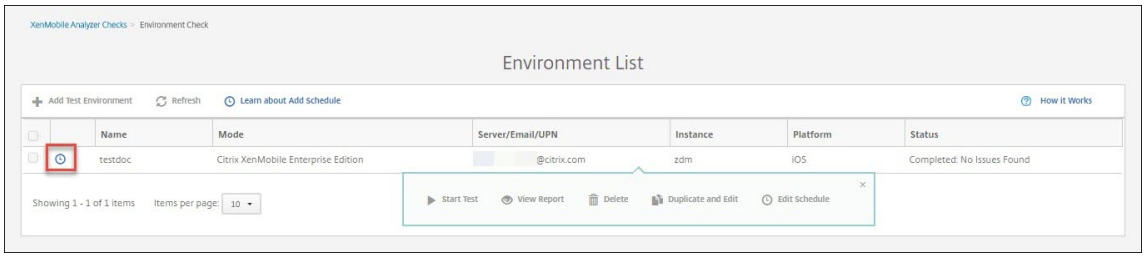
3. Introduzca un nombre de usuario en **Username** y una contraseña en **Password** para ejecutar la prueba.



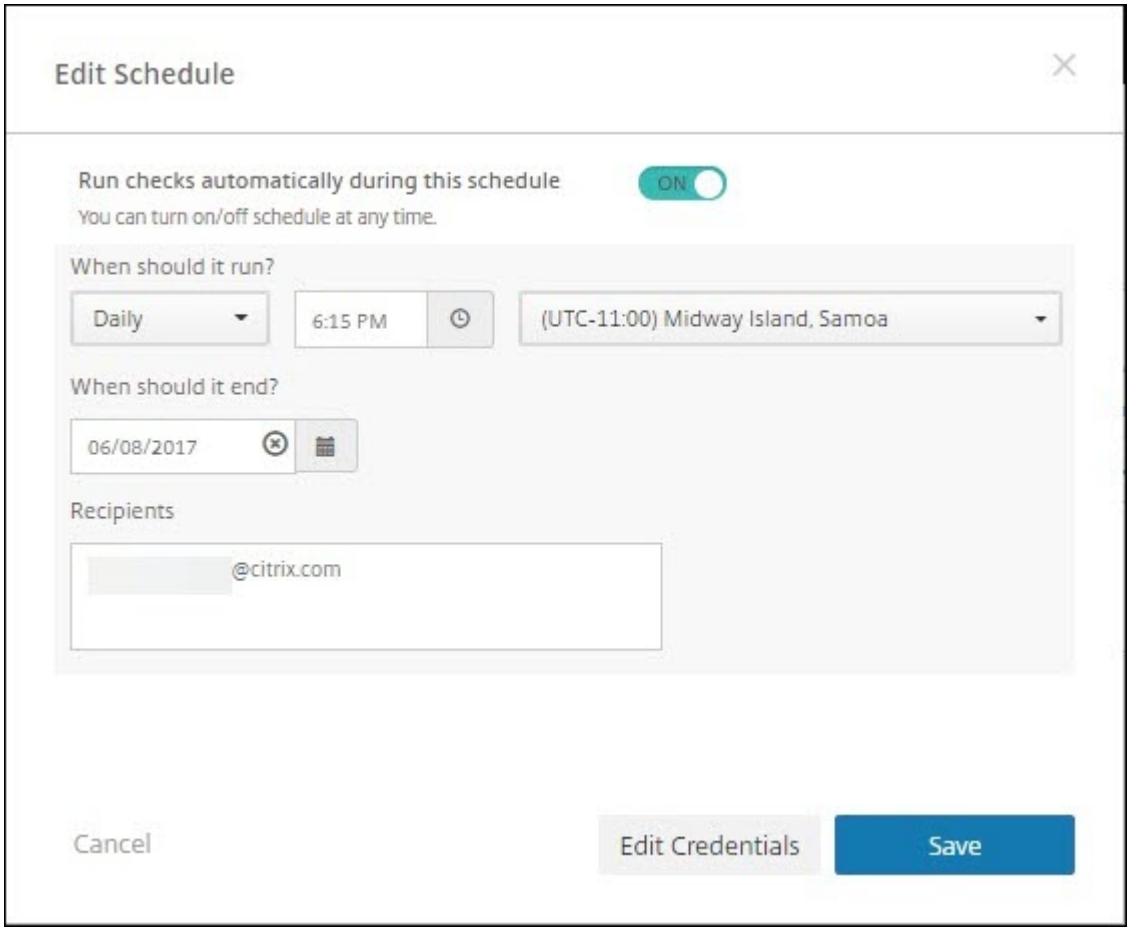
4. Configure una programación para la ejecución de la prueba. Puede seleccionar una ejecución diaria con la opción **Daily** o semanal con la opción **Weekly** en el menú desplegable. Seleccione una hora del día y una zona horaria para que se ejecute la prueba. Utilice el selector para seleccionar una fecha en la que la prueba programada deberá detenerse, o bien, deje en blanco para que la prueba se ejecute de forma indefinida. Especifique una lista de las direcciones de correo electrónico, separadas por comas, que recibirán los informes de la prueba. Haga clic en **Guardar**.



5. Un símbolo de reloj a la izquierda de la prueba indica que se ha configurado una programación. Si selecciona una prueba, puede hacer clic en **Edit Schedule** para cambiar el momento de ejecución de esa prueba.



6. En esta ventana, puede cambiar el momento en que se ejecuta la prueba. También puede desactivarla haciendo clic en el interruptor situado en la parte superior. Haga clic en **Save** cuando haya terminado.



Otras comprobaciones informativas

En XenMobile Analyzer, el paso “Environment Check” (Comprobación del entorno) es interactivo, mientras que las opciones siguientes son informativas. Cada una de estas opciones proporciona información acerca de otras herramientas de asistencia que puede usar para verificar que el entorno de XenMobile esté configurado correctamente.

- **Advanced Diagnostics:** Una 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.
- **Secure Mail Readiness:** 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.
- **Server Connectivity Checks:** Instrucciones para comprobar las conexiones con los servidores de XenMobile, de autenticación y de Content Collaboration.
- **Contact Citrix Support:** Si todo lo anterior falla, puede crear un tíquet de asistencia en Citrix Support.

Problemas conocidos

XenMobile Analyzer presenta los siguientes problemas conocidos:

- Al realizar comprobaciones de conectividad de Secure Web, no se admite la introducción de varias direcciones URL en el cuadro de texto.
- No se admite la función de autenticación de dispositivos compartidos en 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.

API de REST

January 4, 2022

> **Nota:**
>
> Este artículo contiene las API de REST para XenMobile Server. Si quiere conocer las API de REST para Endpoint Management, consulte API de REST.

Con la API de REST de XenMobile, puede invocar servicios que están expuestos a través de la consola de XenMobile. Puede invocar servicios de REST desde cualquier cliente REST. La API no requiere el inicio de sesión en la consola de XenMobile para llamar a los servicios.

Para ver todo el conjunto actual de interfaces API disponibles, descargue el archivo PDF Public API for REST Services.

Permisos necesarios para acceder a la API de REST

Para acceder a la API de REST, necesita uno de los siguientes permisos:

- Permiso de acceso a las API públicas establecido como parte de la configuración del acceso basado en roles. Para obtener información, 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.

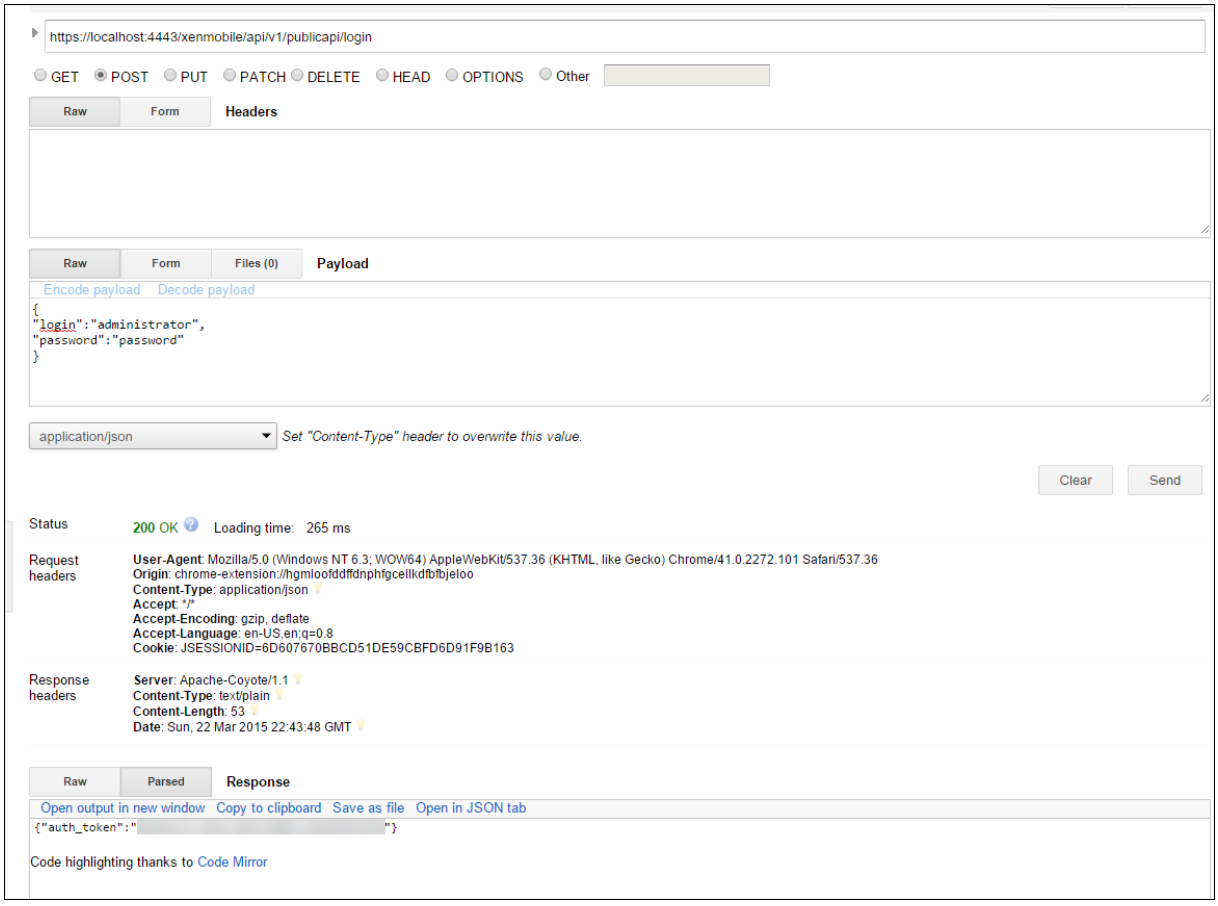
Inicio de sesión

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

Solicitud: `{ "login":"administrator", "password":"password"}`

Tipo de método: POST

Tipo de contenido: application/json



Información relacionada

- API de REST en XenMobile

Conector de Endpoint Management para Exchange ActiveSync

January 4, 2022

XenMobile Mail Manager ha pasado a ser el conector de Endpoint Management para Exchange ActiveSync. Para obtener más detalles sobre los productos unificados de Citrix, consulte la guía de productos de Citrix.

El conector amplía las prestaciones de XenMobile de este modo:

- Control de acceso dinámico para dispositivos Exchange ActiveSync (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 borrar un dispositivo móvil según el estado EAS.
- 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 borrar un dispositivo según el estado EAS, configure una acción automatizada con un desencadenante ActiveSync. Consulte Acciones automatizadas.

Para descargar el conector de Endpoint Management para Exchange ActiveSync:

1. Vaya a https://www.citrix.com/downloads.
2. Vaya a **Citrix Endpoint Management (y Citrix XenMobile Server) > XenMobile Server (local) > Software de producto > XenMobile Server 10 > Componentes de servidor**.
3. En el mosaico **Citrix Endpoint Management connector for Exchange ActiveSync**, haga clic en **Download File** (Descargar archivo).

Novedades

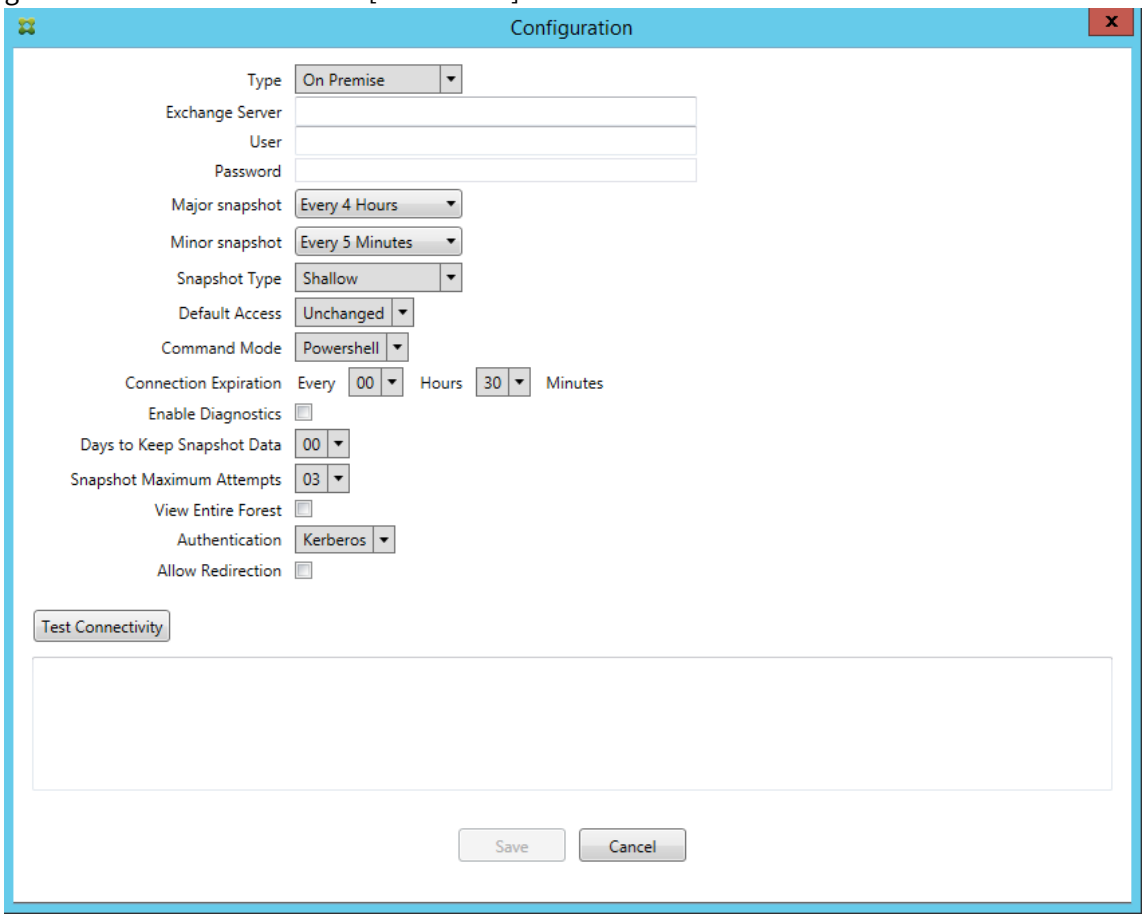
En las siguientes secciones, se detallan las novedades de Endpoint Management para Exchange ActiveSync (anteriormente, XenMobile Mail Manager).

Novedades en la versión 10.1.10

Se han corregido los siguientes problemas en la versión 10.1.10:

- Es posible que los clientes que sufren problemas frecuentes de red no puedan completar una instantánea en los tres intentos que se ofrecen. Con esta versión, un administrador puede configurar el máximo de intentos (1-10). Esta corrección permite que una instantánea pueda sufrir varias interrupciones de la comunicación sin abandonar completamente el proceso de

generación de la instantánea. [CXM-70837]



- En versiones anteriores, el tipo Instantánea no aparecía en la lista de configuraciones de Exchange. Ahora sí aparece el tipo Instantánea. [CXM-70846]
- La excepción PSRemotingTransport notificada por PowerShell indica que la sesión con Exchange ya no es viable. El estado se agrega de forma predeterminada a la lista Errores críticos del archivo de configuración. Al hacerlo, cuando se detecta PSRemotingTransportException, la conexión se marca como Error para eliminarla luego. La siguiente comunicación emplea una conexión válida o crea otra conexión. [XMHELP-2184, CXM-70836]
- Al guardar un cambio en la configuración, es posible que no todos los componentes internos previamente configurados se eliminaran correctamente antes de cargar la nueva configuración. Este problema puede provocar un comportamiento impredecible. Dicho comportamiento depende del cambio concreto y si el cambio entra en conflicto con la configuración anterior. En esta versión se eliminan todos los componentes internos antes de cargar la nueva configuración. [XMHELP-2259, CXM-71388]

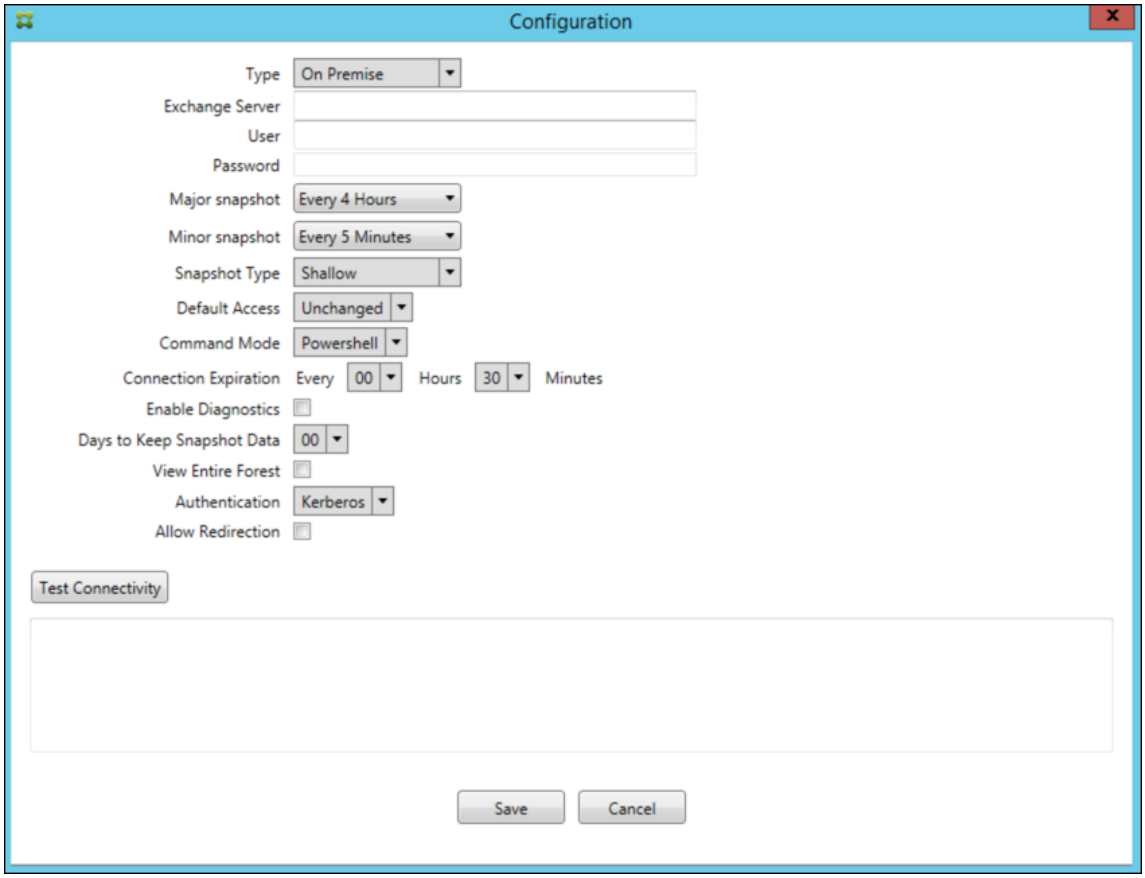
Novedades en versiones anteriores

En la siguiente sección, se indican las funciones y los problemas resueltos en versiones anteriores del conector de Endpoint Management para Exchange ActiveSync.

Novedades en la versión 10.1.9

Se han corregido los siguientes problemas en la versión 10.1.9:

- Ahora los cambios de configuración se gestionan de manera más coherente. Cuando el servicio detecta un cambio en la configuración, cada subsistema interno se detiene, lo que significa que cualquier procesamiento activo o programado se interrumpe. A continuación, se carga la nueva configuración y se inician de nuevo los subsistemas, por lo que todas las programaciones y otras infraestructuras internas se restablecen con parámetros nuevos. Esto corrige un problema conocido de la versión 10.1.8. [CXM-47709, CXM-61330]
- Durante la actualización de una versión, la configuración de la base de datos existente no se integraba en el nuevo archivo de configuración. Ahora la configuración de la base de datos se integra en el archivo de configuración actualizado. [CXM-49326]
- En los archivos de diagnóstico relacionados con la instantánea, faltaban los encabezados de columna. Los encabezados se han restaurado. [CXM-62680]
- Al actualizar una versión anterior, la sección de valores predeterminados del archivo de configuración quedaba sobrescrita por la sección análoga del archivo de configuración en uso. Este problema impedía que, tras la actualización, el servicio cargara aspectos agregados o mejorados de la sección de valores predeterminados. A partir de esta versión, la sección de valores predeterminados siempre refleja la configuración más reciente. [CXM-62681]
- Al ejecutar la aplicación, los administradores ya no pueden acceder a ciertas opciones al presionar Mayús. Antes estas opciones estaban disponibles con el permiso de Citrix. Ahora algunas opciones están totalmente disponibles, como Permitir redirección, y otras, como Detección de bloqueo y Corrección de recuento, se han retirado. [CXM-62767]



Novedades en la versión 10.1.8

Se han corregido los siguientes problemas en la versión 10.1.8:

- Es posible que Exchange limite la emisión demasiado frecuente de comandos por parte del servicio del conector de Citrix Endpoint Management para Exchange ActiveSync. Esto es habitual en las conexiones a Office 365. El efecto de la limitación requiere que el servicio se detenga durante un período de tiempo especificado antes de enviar el siguiente comando. Ahora, en el apartado “Configurar” de la consola, se muestra la cantidad de tiempo restante de pausa. [CXM-48044]
- Cuando se realizan modificaciones en las secciones “Watchdog” o “SpecialistsDefaults” del archivo de configuración (config.xml), los cambios no se reflejan en el archivo de configuración después de una actualización. Con esta versión, las modificaciones se fusionan correctamente en el nuevo archivo de configuración. [CXM-52523]
- Se han agregado más detalles a los análisis enviados a Google Analytics, especialmente en lo que respecta a las instantáneas. [CXM-56691]
- La función para probar la conectividad de Exchange intentaría inicializar la conexión solo una vez. Debido a que las conexiones de Office 365 se pueden limitar, era posible que una prueba de conectividad pareciera fallida cuando se limitaba. Ahora, el conector de Citrix Endpoint Man-

agement para Exchange ActiveSync intenta iniciar una conexión hasta tres veces. [CXM-58180]

- Para aplicar directivas en Exchange, el conector de Citrix Endpoint Management para Exchange ActiveSync debe compilar un comando **Set-CASMailbox** que incluya todos los dispositivos correspondientes a cada buzón en dos listas: permitir y bloquear. Si un dispositivo no está incluido en ninguna de las listas, Exchange vuelve a su estado de acceso predeterminado. Si ese estado de acceso predeterminado es diferente del estado deseado para un dispositivo, ese dispositivo queda como no conforme. En consecuencia, un usuario puede perder el acceso a su correo electrónico si el estado de acceso predeterminado de Exchange está bloqueado pero se debería permitir. O bien, un usuario cuyo acceso al correo electrónico debería estar bloqueado puede tener acceso a él. Ahora, el conector de Citrix Endpoint Management para Exchange ActiveSync garantiza que todos los dispositivos con un estado deseado válido se incluyan en cada comando **Set-CASMailbox**. [CXM-61251]

El siguiente problema en un problema conocido en la versión 10.1.8:

Si un administrador realiza un cambio en la aplicación de configuración que modifica los datos de configuración mientras el servicio realiza operaciones de larga duración (como una instantánea o evaluación de directiva), el servicio puede entrar en un estado indeterminado. Un posible síntoma puede ser que los cambios de directiva no se procesen o que las instantáneas no se inicien. Para que el servicio vuelva a un estado de funcionamiento, el servicio debe reiniciarse. Es posible que tenga que utilizar el administrador de servicios de Windows para finalizar el proceso del servicio antes de iniciar el servicio. [CXM-61330]

Novedades en la versión 10.1.7

- XenMobile Mail Manager ha pasado a ser el conector de Endpoint Management para Exchange ActiveSync.
- La opción **Disable Pipelining** ha dejado de usarse en el cuadro de diálogo de configuración de Exchange. Se obtiene el mismo resultado configurando varios pasos para cada comando en el archivo config.xml. [CXM-54593]

Se han corregido los siguientes problemas en la versión 10.1.7:

- En la ventana Snapshot History (historial de instantáneas), los mensajes de error pueden mostrarse con poco contexto. Ahora, los mensajes de error incluyen un prefijo con el contexto sobre el lugar donde se produjeron. [CXM-49157]
- El archivo XmmGoogleAnalytics.dll no tenía la versión de archivo correspondiente para esta versión. [CXM-52518]
- Para mejorar los diagnósticos, hemos cambiado recientemente el formato de cadena para una lista de ID de dispositivo que se utilizan para establecer un estado de buzón como permitido o bloqueado. Sin embargo, ante una indicación de demasiados dispositivos, excedía el tamaño máximo de la cadena. Ahora, usamos una estructura de datos de matriz interna. Esta estructura

no tiene límite de tamaño y da a los datos el formato apropiado para los diagnósticos. [CXM-52610]

- Cuando se detectan directivas de dispositivo que no están sincronizadas con Exchange, los comandos de estas directivas pueden incluir dispositivos que no pertenecen al buzón correspondiente. Ahora el conector de Endpoint Management para Exchange ActiveSync garantiza que los comandos a Exchange representen solo los dispositivos que pertenezcan a los buzones respectivos. [CXM-54842]
- En algunos entornos, no está disponible el ensamblado de Microsoft. Ahora el ensamblado requerido se instala explícitamente con la aplicación. [CXM-55439]
- Si los nombres distintivos de dispositivos o buzones contienen espacios entre el nombre del atributo y los signos igual (=), y/o espacios después de los signos igual y antes del valor, el conector de Endpoint Management para Exchange ActiveSync puede no asociar correctamente un dispositivo a su buzón y viceversa. El resultado podría ser que algunos dispositivos y/o buzones de correo se rechacen durante la conciliación de instantáneas. [CXM-56088]

> **Nota:**
>
> En las siguientes secciones se hace referencia al conector de Endpoint Management para Exchange ActiveSync por su nombre anterior, XenMobile Mail Manager. El nombre cambió a partir de la versión 10.1.7.

Actualización en la versión 10.1.6.20

Una actualización a 10.1.6 contiene la siguiente corrección en la versión 10.1.6.20:

- Cuando se detectan directivas de dispositivo que no están sincronizadas con Exchange, los comandos de estas directivas pueden incluir dispositivos que no pertenecen al buzón correspondiente. Ahora XenMobile Mail Manager garantiza que los comandos a Exchange representen solo los dispositivos que pertenezcan a los buzones respectivos. [CXM-54842]

Novedades en la versión 10.1.6

XenMobile Mail Manager 10.1.6 contiene los siguientes problemas resueltos y las siguientes mejoras:

- La ventana de historial de instantáneas entra a veces en un estado en que deja de actualizarse. El mecanismo de actualización de la ventana se ha mejorado y ahora es más fiable. [CXM-47983]
- Se han usado dos modos y rutas de código diferentes para instantáneas con particiones y sin particiones. Debido a que las instantáneas sin particiones equivalen a las instantáneas con particiones que tienen una configuración con una sola partición "*", se ha eliminado el modo de instantánea sin particiones. Ahora el modo de instantánea predeterminado son instantáneas con 36 particiones (de 0 a 9, de A a Z). [CXM-49093]

- En la ventana “Historial de instantáneas”, los mensajes de estado sobrescriben los mensajes de error. Ahora, XenMobile Mail Manager ofrece dos campos separados para que los usuarios puedan ver el estado y los errores simultáneamente. [CXM-51942]
- Al conectarse a Exchange Online (Office 365), las consultas relacionadas con las instantáneas pueden dar como resultado un conjunto de datos truncados. Este problema puede ocurrir cuando XenMobile Mail Manager ejecuta un script canalizado con comandos múltiples. Un comando no puede pasar los datos lo suficientemente rápido al comando siguiente, con lo que la función se completa antes de tiempo y resulta en datos incompletos. Ahora XenMobile Mail Manager puede imitar el proceso y esperar hasta que un comando esté listo antes de invocar el siguiente comando en sentido descendente. Este cambio debería dar como resultado que se procesen y se capturen todos los datos. [CXM-52280]
- Si se produce un error sin solución en un comando de actualización de directiva en Exchange, ese comando se devuelve a la cola de tareas repetidamente durante un largo período de tiempo. Esta situación provocaba que el comando se enviara muchas veces a Exchange. En esta versión de XenMobile Mail Manager, un comando que genera un error solo se devuelve a la cola de tareas una cantidad determinada de veces. [CXM-52633]
- Si una actualización de directiva para un buzón específico implicaba permitir o bloquear todos los dispositivos, el comando **Set-CASMailbox** emitido fallaba debido a que la lista vacía se convertía en una cadena vacía en lugar de **NULL**. Ahora se envían los datos correctos. [CXM-53759]
- Al procesar un nuevo dispositivo, Exchange puede devolver el estado “DeviceDiscovery” durante un período de tiempo (generalmente 15 minutos). XenMobile Mail Manager no gestionaba específicamente este estado. Ahora XenMobile Mail Manager gestiona ese estado. En la ficha “Monitor” de la interfaz de usuario, los usuarios pueden filtrar por dispositivos en ese estado. [CXM-53840]
- XenMobile Mail Manager no verificaba la capacidad de escribir en la base de datos de XenMobile Mail Manager. En consecuencia, si los permisos eran restringidos, el comportamiento no se podía prever. Ahora XenMobile Mail Manager captura y valida los permisos necesarios de la base de datos. XenMobile Mail Manager indica los permisos reducidos cuando se prueba la conexión (aparece un mensaje) o en el indicador “Database” (pase el puntero para ver el mensaje) en la parte inferior de la ventana principal “Configure”. [CXM-54219]
- Dependiendo de la carga de trabajo actual, cuando se dirige a XenMobile Mail Manager, es posible que el servicio no se detenga rápidamente. Por lo tanto, el servicio parece estar en un estado que no responde. Las mejoras permiten interrumpir las tareas en curso, lo que permite un apagado más fácil. [CXM-54282]

Novedades en la versión 10.1.5

XenMobile Mail Manager 10.1.5 contiene los siguientes problemas resueltos:

- Cuando Exchange aplica limitaciones a la actividad de XenMobile Mail Manager, no hay ninguna

indicación de ello (solo se indica en los registros). Con esta versión, un usuario puede colocar el puntero sobre la instantánea activa y aparece el estado “throttling” (limitación). Además, mientras se aplican limitaciones a XenMobile Mail Manager, se prohíbe el inicio de una instantánea principal hasta que Exchange deje de aplicarlas. [CXM-49617]

- Si Exchange aplica limitaciones a XenMobile Mail Manager durante una instantánea principal, puede que transcurra un tiempo insuficiente antes de ejecutar el siguiente intento de instantánea. Este problema resulta en más limitaciones y una instantánea fallida. Ahora XenMobile Mail Manager espera un mínimo del tiempo que Exchange especifica que debe esperar entre intentos de instantáneas. [CXM-49618]
- Cuando el diagnóstico está habilitado, el archivo de comandos muestra los comandos **Set-CASMailbox** con guiones que faltan antes de cada nombre de propiedad. Este problema solo ocurre en el formateo del archivo de diagnóstico, no en el comando real de Exchange. El guión que falta impide que un usuario corte el comando y lo pegue directamente en una ventana de PowerShell para probarlo o validarlo. Los guiones se han agregado. [CXM-52520]
- Si la identidad de un buzón tiene el formato “apellido, nombre”, Exchange agrega una barra diagonal inversa antes de la coma cuando devuelve datos de una consulta. Esta barra invertida se debe quitar cuando XenMobile Mail Manager usa la identidad para consultar más datos. [CXM-52635]

Limitación conocida

> **Nota:**
>
> Se ha resuelto la siguiente limitación en la versión 10.1.6.

XenMobile Mail Manager presenta una limitación conocida que puede hacer que fallen los comandos de Exchange. Para aplicar cambios de directiva a Exchange, XenMobile Mail Manager emite un comando **Set_CASMailbox**. Este comando puede tener en cuenta dos listas de dispositivos: una para Permitir y otra para Bloquear. El comando se aplica a los dispositivos asociados a un buzón.

Estas listas están limitadas a 256 caracteres cada una por la API de Microsoft. Si una de esas listas sobrepasa la limitación, todo el comando falla y no se define ninguna de las directivas para esos dispositivos del buzón. El error que se informa, que aparece en los registros de XenMobile Mail Manager, es similar a lo siguiente. El ejemplo es para la lista bloqueada.

“Message:’Cannot bind parameter ‘ActiveSyncBlockedDeviceIDs’ to the target. Exception setting “ActiveSyncBlockedDeviceIDs”: “The length of the property is too long. The maximum length is 256 and the length of the value provided is …”

La longitud de los ID de dispositivo pueden variar, pero una buena regla es que unos 10 dispositivos o más permitidos o bloqueados simultáneamente podrían sobrepasar el límite. Aunque tener tantos dispositivos asociados a un buzón específico es raro, existe esa posibilidad. Hasta que XenMobile Mail Manager se mejore para gestionar este caso, le recomendamos que limite la cantidad de dispositivos

asociados al usuario y al buzón a 10 o menos. [CXM-52633]

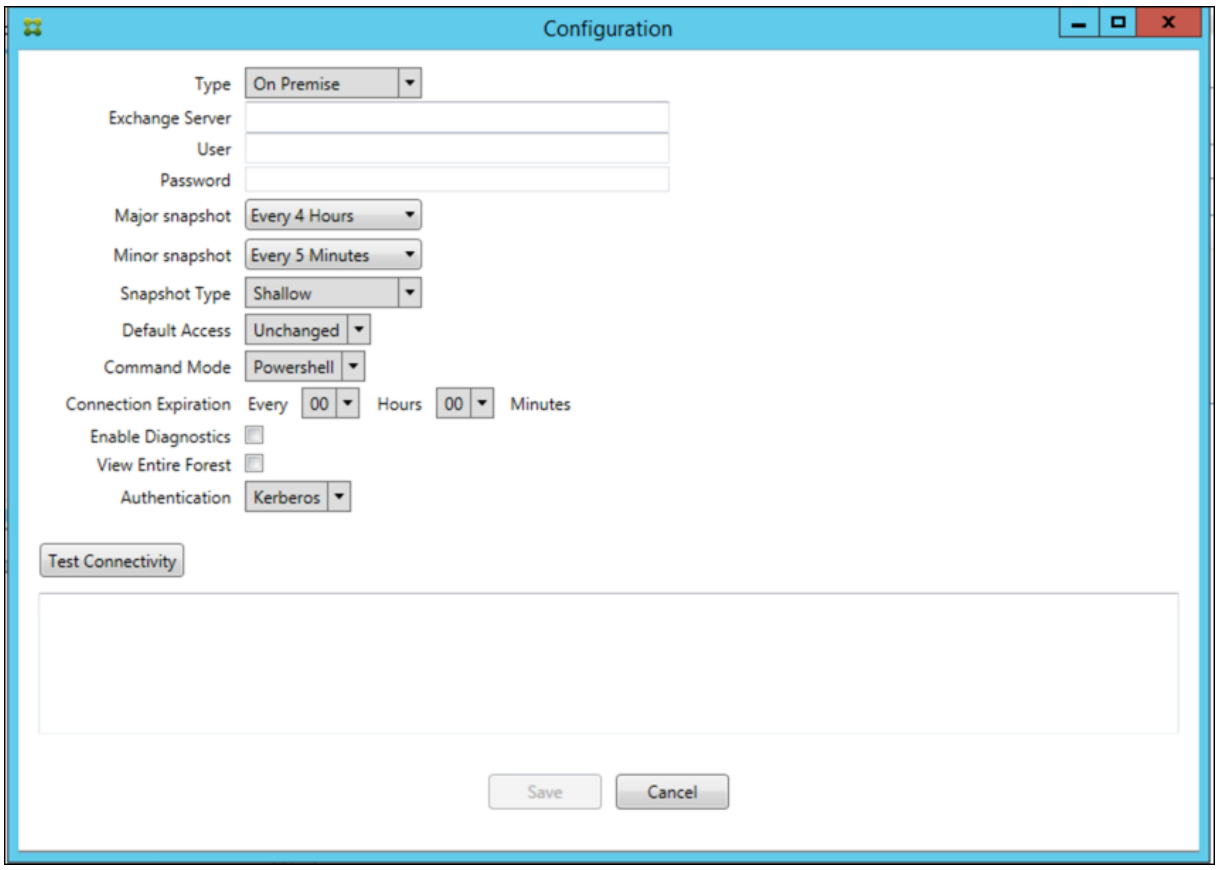
Novedades en la versión 10.1.4

XenMobile Mail Manager 10.1.4 contiene los siguientes problemas resueltos:

- Debido a la poca seguridad que ofrece, PCI Council ha retirado TLS 1.0. Se ha agregado la funcionalidad TLS 1.1 y 1.2 a XenMobile Mail Manager. [CXM-38573, CXM-32560]
- XenMobile Mail Manager incluye un nuevo archivo de diagnóstico. Cuando se selecciona **Enable Diagnostics** en la especificación de Exchange, se genera un nuevo archivo de historial de instantáneas. Con cada intento de instantánea, se agrega una línea al archivo con los resultados de la instantánea. [CXM-49631]
- En el archivo de diagnóstico de comandos, la lista de dispositivos permitidos o bloqueados no aparecía para el comando **Set-CASMailbox**. En cambio, el nombre de la clase interna se muestra en el archivo para los argumentos relacionados. Ahora, XenMobile Mail Manager muestra la lista de identificadores de dispositivo como una lista separada con comas. [CXM-50693]
- Cuando falla un intento de establecer conexión con Exchange debido a una especificación incorrecta, un mensaje incorrecto sobrescribe el mensaje de error: "All connections in use" (Todas las conexiones están en uso). Ahora, aparecen mensajes más descriptivos, como "All connections are inoperable" (Todas las conexiones están inoperativas), "Connection pool is empty" (El grupo de conexiones está vacío), "All connections are throttled" (Todas las conexiones están limitadas) y "No available connections" (No hay conexiones disponibles). [CXM-50783]
- En algunos casos, los comandos Allow, Block o Wipe se ponen en cola varias veces en la caché interna de XenMobile Mail Manager. Este problema provoca un retraso en el envío del comando a Exchange. Ahora, XenMobile Mail Manager solo pone en cola una instancia de cada comando. [CXM-51524]

Novedades en la versión 10.1.3

- **Compatibilidad con Google Analytics:** Nos gustaría saber cómo usa XenMobile Mail Manager para centrarnos en dónde mejorar el producto.
- **Parámetro para habilitar diagnósticos:** Aparece una casilla **Enable Diagnostics** en el cuadro de diálogo **Configuration** de la consola.



Problemas resueltos en la versión 10.1.3

- En la ventana **Snapshot History**, la información que muestra el estado actual de la instantánea no refleja el estado real. [CXM-5570]
  A veces, XenMobile Mail Manager no puede escribir en el archivo de diagnósticos de comandos. Cuando eso ocurre, el historial de comandos no se registra en su totalidad. [CXM-49217]
- Cuando ocurre un error con una conexión, la conexión puede no marcarse como “errored” (con errores). Como resultado, un comando posterior puede intentar usar la conexión y provocar otro error. [CXM-49495]
- Cuando se limita una acción desde Exchange Server, se puede iniciar una excepción en la rutina de comprobación de estado. Como resultado, puede que no se eliminen las conexiones con errores o las que han caducado. Además, XenMobile Mail Manager podría no crear conexiones hasta que se agote el tiempo de la limitación. [CXM-49794]
- Cuando se supera el recuento máximo de sesiones para Exchange, XenMobile Mail Manager informa del error “Device Capture Failed” (Fallo en la captura de dispositivos), que no es un mensaje preciso. En vez de este motivo, el mensaje debe indicar que las dos sesiones que suele usar XenMobile Mail Manager para la comunicación con Exchange ya están en uso. [CXM-49994]

Novedades en la versión 10.1.2

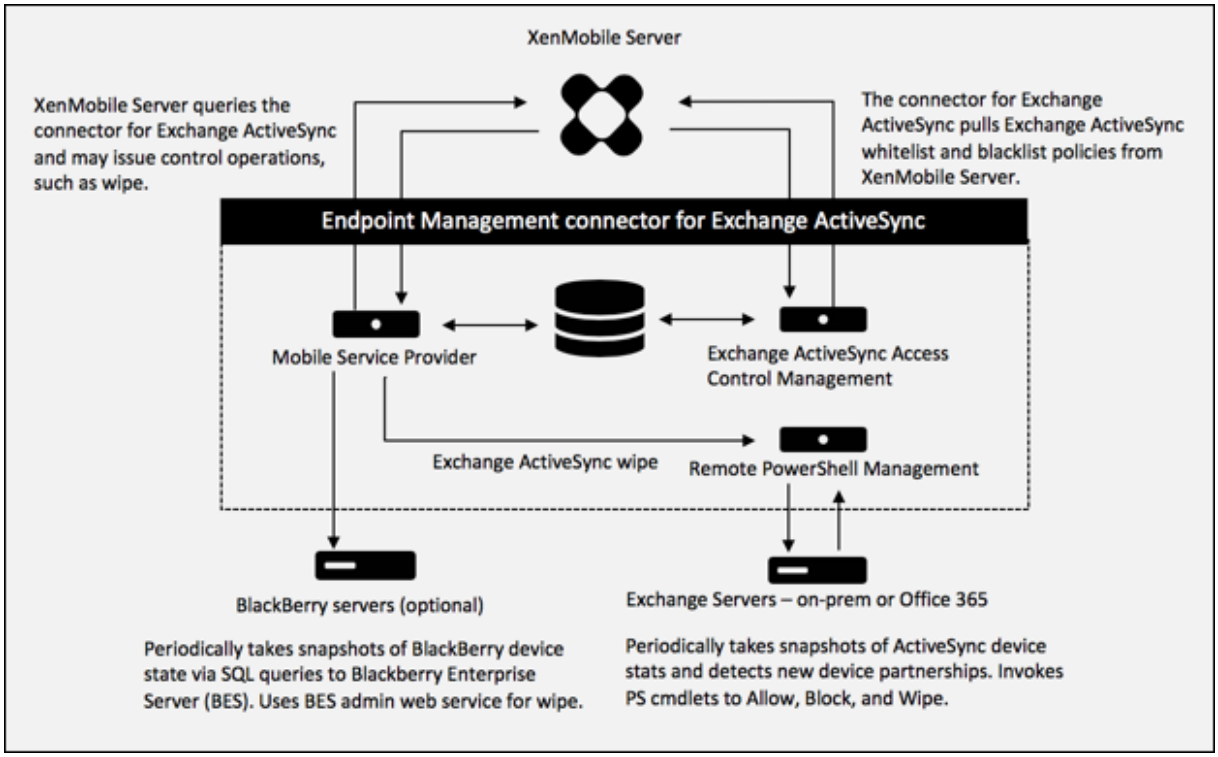
- **Conexión con Exchange mejorada**: XenMobile Mail Manager usa sesiones de PowerShell para comunicarse con Exchange. Una sesión de PowerShell, especialmente cuando se trata de Office 365, puede volverse inestable después de un tiempo, bloqueando el funcionamiento correcto de los siguientes comandos. XenMobile Mail Manager ahora puede establecer un período de caducidad para las conexiones. Cuando se agota el tiempo de la conexión, XenMobile Mail Manager cierra la sesión de PowerShell y crea una sesión. Al hacerlo, es menos probable que la sesión de PowerShell se vuelva inestable, lo que reduce significativamente la posibilidad de fallos en la instantánea.
- **Flujo de trabajo mejorado para las instantáneas**: Las instantáneas principales consumen mucho tiempo y requieren muchos recursos. Si se produce un error durante una instantánea, ahora XenMobile Mail Manager intenta completarla un máximo de tres veces. Los intentos posteriores no comienzan desde el principio. XenMobile Mail Manager continúa desde donde se quedó. Esta mejora aumenta la tasa general de instantáneas correctas, ya que permite errores transitorios mientras hay una instantánea en curso.
- **Diagnósticos mejorados**: Ahora las operaciones para solucionar problemas relacionadas con instantáneas son más fáciles, gracias a tres nuevos archivos de diagnóstico que se pueden generar durante una instantánea. Esos archivos ayudan a identificar problemas de comandos de PowerShell, buzones de correo con información incompleta y dispositivos que no se pueden relacionar a un buzón. Un administrador puede usar esos archivos para identificar datos que pueden no ser correctos en Exchange.
- **Uso mejorado de la memoria**: Ahora XenMobile Mail Manager es más eficiente en el consumo de la memoria. Los administradores pueden programar XenMobile Mail Manager para que se reinicie automáticamente y ofrezca un punto de partida raso al sistema.
- **Requisito previo de Microsoft .NET Framework 4.6**: El requisito previo para Microsoft .NET Framework ahora es la versión 4.6.

Problemas resueltos

- Error de solicitud de credenciales: La inestabilidad de las sesiones de Office 365 causa a menudo este error. Con la conexión mejorada con Exchange, se soluciona este problema. (XMHELP-293, XMHELP-311, XMHELP-801)
- Incoherencias de recuento entre buzones y dispositivos: XenMobile Mail Manager presenta un algoritmo mejorado para la asociación de buzones a dispositivos. La función de diagnósticos mejorados ayuda a identificar buzones y dispositivos que XenMobile Mail Manager considera fuera de su ámbito de responsabilidad. (XMHELP-623)
- No se reconocen los comandos Allow, Block ni Wipe: Se ha corregido un error donde, a veces, no se reconocen esos comandos de XenMobile Mail Manager. (XMHELP-489)
- Gestión de memoria: Mejor mitigación y gestión de memoria. (XMHELP-419)

Arquitectura

En la siguiente imagen, se muestran los componentes principales del conector de Endpoint Management para Exchange ActiveSync. Para obtener un diagrama detallado con una arquitectura como referencia, consulte Arquitectura.



Los tres componentes principales son:

- **Administración del control de acceso de Exchange ActiveSync:** Se comunica con XenMobile para recuperar una directiva de Exchange ActiveSync, 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).
- **Administración remota de PowerShell:** 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.
- **Proveedor de servicios móviles:** 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

Para usar el conector de Endpoint Management para Exchange ActiveSync, se deben cumplir los siguientes requisitos mínimos del sistema:

- Windows Server 2016, Windows Server 2012 R2 o Windows Server 2008 R2 Service Pack 1. Debe ser un servidor en inglés. Windows Server 2008 R2 Service Pack 1 dejará de ser compatible el 14 de enero de 2020.
- Microsoft SQL Server 2016 Service Pack 2 o SQL Server 2014 Service Pack 3.
- Microsoft .NET Framework 4.6
- BlackBerry Enterprise Service, versión 5 (optativo).

Versiones mínimas admitidas de Microsoft Exchange Server:

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 Service Pack 3 (dejará de ser compatible el 14 de enero de 2020)

Requisitos previos

- Windows Management Framework debe estar instalado.
  - PowerShell 5, 4 y 3
- 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 que ejecuta el conector de Endpoint Management para Exchange ActiveSync y el Exchange Server remoto.
- **Clientes de correo electrónico del dispositivo:** No todos los clientes de correo electrónico devuelven el mismo ID de ActiveSync para el mismo dispositivo. Debido a que el conector de Endpoint Management para Exchange ActiveSync 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 Samsung
  - Cliente de correo electrónico nativo de iOS
- **Exchange**: A continuación, se indican los requisitos para un equipo local con Exchange:

  Las credenciales especificadas en la interfaz de usuario de configuración de Exchange deben permitir la conexión al servidor de 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 de 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 el conector de Endpoint Management para Exchange ActiveSync 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 de Exchange mediante el shell remoto. De forma predeterminada, el usuario que haya instalado Exchange tiene ese derecho.
- Para establecer una conexión remota y ejecutar comandos remotos, las credenciales deben corresponder a un usuario que sea administrador en la máquina remota. Puede usar Set-PSSessionConfiguration para eliminar el requisito administrativo, pero en este documento no se describe ese comando. Para obtener más información, consulte el artículo About Session Configurations de Microsoft.
- 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 de 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, el conector de Endpoint Management

para Exchange ActiveSync no se puede conectar al Exchange Server. 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, el conector de Endpoint Management para Exchange ActiveSync no se puede conectar al Exchange Server. 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

1. Haga clic en el archivo XmmSetup.msi y, a continuación, siga las instrucciones del instalador para instalar el conector de Endpoint Management para Exchange ActiveSync.
2. Deje **Launch the Configure utility** marcado en la última pantalla del Asistente de configuración. O bien, desde el menú **Inicio**, abra el conector de Endpoint Management para Exchange ActiveSync.
3. Configure las siguientes propiedades de base de datos:

- Seleccione la ficha **Configure > Database**.
- Escriba el nombre del servidor SQL (el valor predeterminado es localhost).
- Conserve la opción predeterminada de la base de datos, **CitrixXmm**.

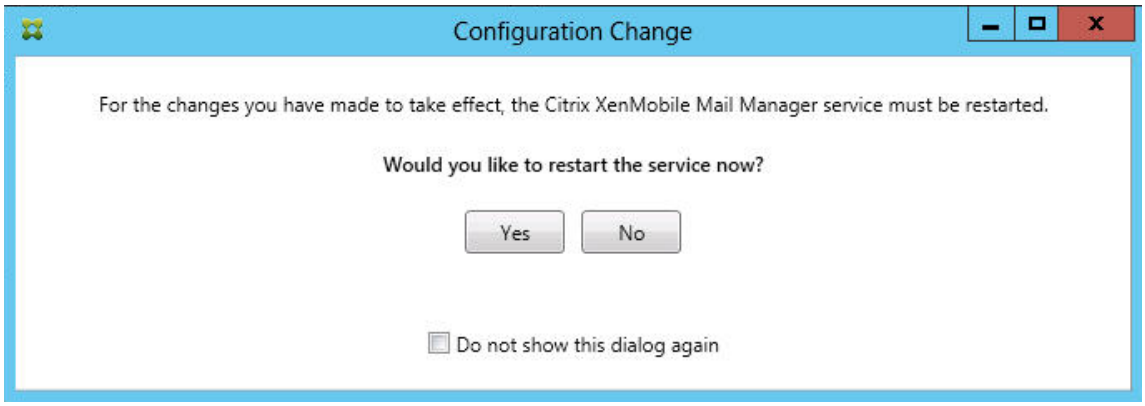
4. Seleccione uno de los siguientes modos de autenticación para SQL:

   - **SQL:** Escriba el nombre de usuario y la contraseña de un usuario de SQL válido.
   - **Integrada en Windows:** Si elige esta opción, las credenciales de inicio de sesión del servicio del conector de Endpoint Management para Exchange ActiveSync 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 del conector de Endpoint Management para Exchange ActiveSync y, a continuación, haga clic en la ficha **Iniciar sesión**.

   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.

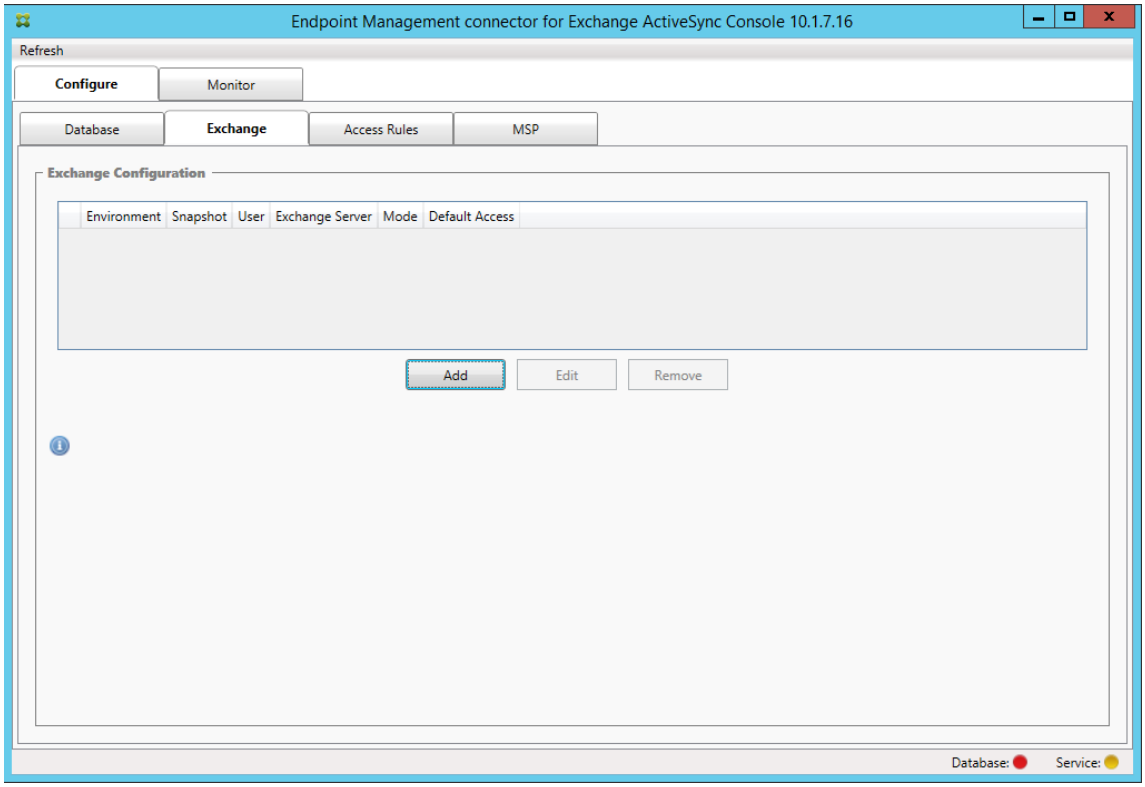
5. Haga clic en **Test Connectivity** para comprobar que se puede establecer conexión con el servidor SQL Server y, a continuación, haga clic en **Save**.

6. Un mensaje le solicitará que reinicie el servicio. Haga clic en **Yes**.



7. Configure uno o varios servidores Exchange:

   - Si administra un solo entorno de Exchange, solo deberá especificar un servidor. Si administra varios entornos de Exchange, deberá especificar un servidor de Exchange por cada entorno de Exchange.
   - Haga clic en la ficha **Configure > Exchange** y seleccione **Add**.



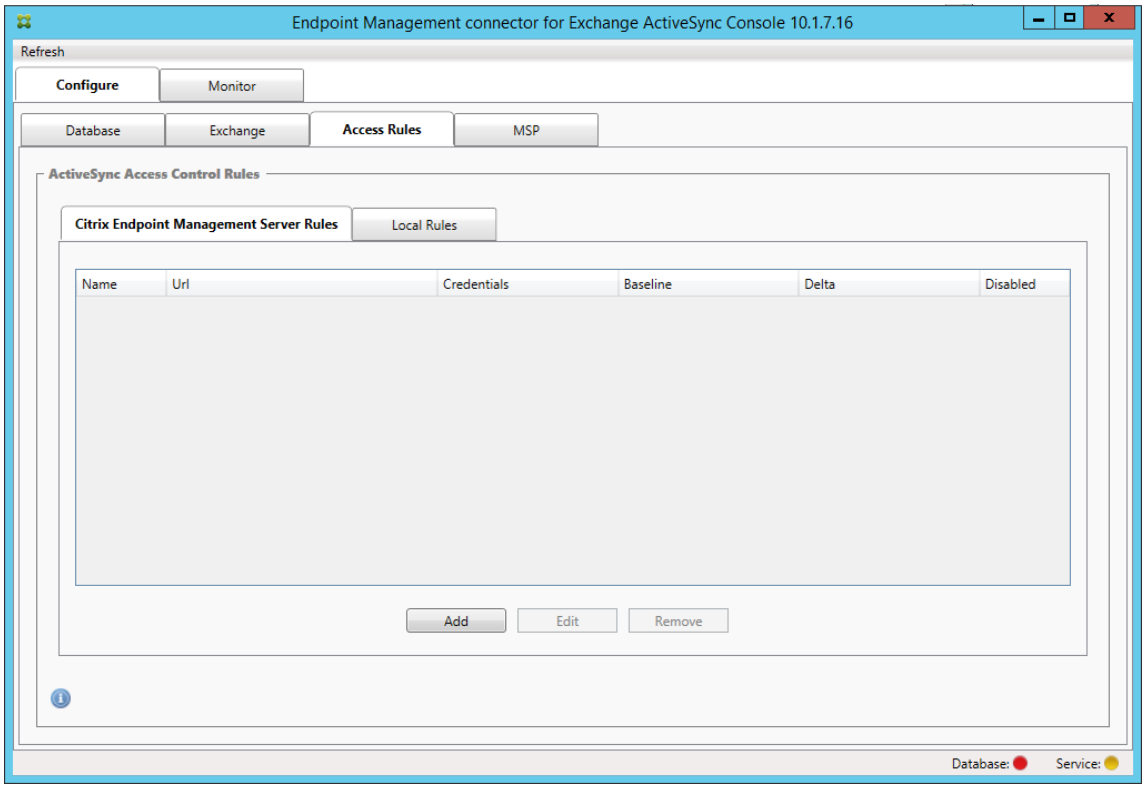
8. Seleccione el tipo de entorno de Exchange Server: **On Premise** u **Office 365**.

    - Si selecciona **On Premise**, escriba el nombre del servidor de Exchange que se usará para los comandos remotos de PowerShell.
    - Escriba el **nombre de usuario** de una identidad de Windows que tenga los permisos apropiados en el servidor de Exchange, como se especifica en el apartado "Requisitos". A continuación, escriba la **contraseña** del usuario.
    - Seleccione un horario para ejecutar las instantáneas principales. Una instantánea principal detecta cada asociación de Exchange ActiveSync.
    - Seleccione un horario para ejecutar las instantáneas secundarias. Una instantánea secundaria detecta asociaciones recién creadas de Exchange ActiveSync.
    - 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 el conector de Endpoint Management para Exchange ActiveSync. Las instantáneas completas (Deep) pueden tardar mucho más y solo son necesarias si el proveedor de servicios móviles está habilitado para ActiveSync. Esta opción permite que XenMobile envíe consultas sobre dispositivos no administrados.
    - Seleccione el acceso predeterminado: **Allow**, **Block** o **Unchanged**. Este parámetro controla cómo se tratan todos los dispositivos, excepto aquellos que XenMobile o las reglas locales identifiquen de forma explícita. Si selecciona **Allow**, todos esos dispositivos pueden acceder a ActiveSync. Si selecciona **Block**, se deniega el acceso. Si selecciona

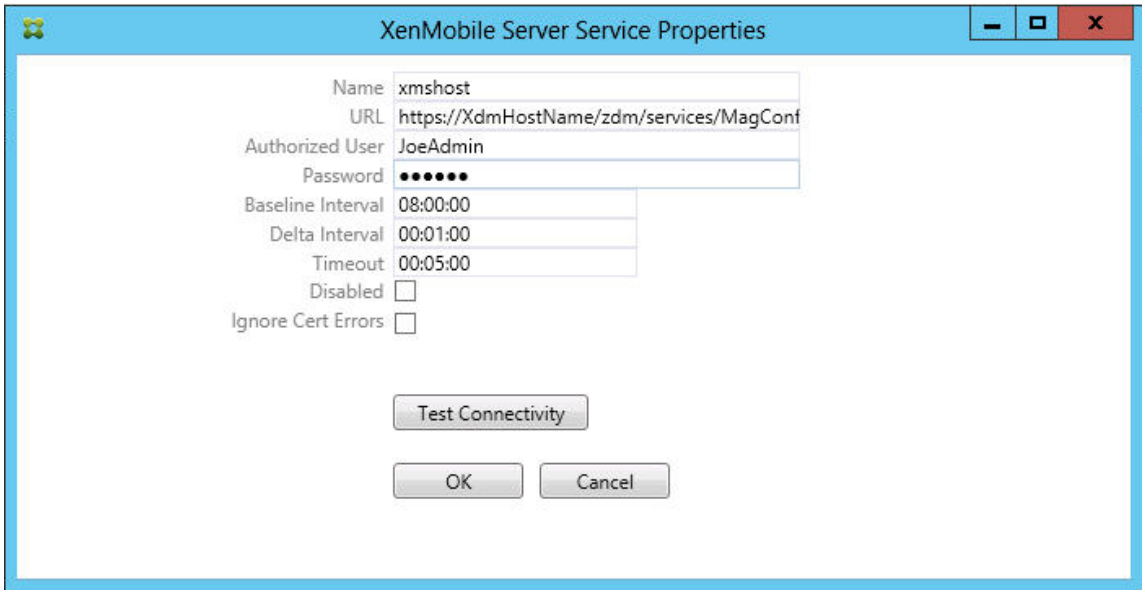
Unchanged, no se realiza ningún cambio.

- Seleccione el modo de comandos de ActiveSync: **PowerShell** o **Simulation**.
- En el modo **PowerShell**, el conector de Endpoint Management para Exchange ActiveSync emite comandos de PowerShell para permitir el control de acceso pertinente. En el modo "Simulation", el conector de Endpoint Management para Exchange ActiveSync no emite comandos de PowerShell, pero registra en la base de datos el comando en cuestión, así como los resultados esperados. En el modo Simulation, el usuario puede usar la ficha **Monitor** para ver lo que podría haber ocurrido si se hubiera habilitado el modo PowerShell.
- En **Connection Expiration**, configure las horas y los minutos de que dispondrá una conexión. Cuando una conexión alcanza la antigüedad especificada, se marca como caducada para que no se vuelva a usar. Cuando la conexión caducada ya no se usa, el conector de Endpoint Management para Exchange ActiveSync la cierra. Cuando se vuelve a necesitar una conexión, se inicializa una nueva si no hay ninguna disponible. Si no se especifica ningún valor, se usa el valor predeterminado de 30 minutos.
- Seleccione **View Entire Forest** para configurar el conector de Endpoint Management para Exchange ActiveSync y ver todo el bosque de Active Directory en el entorno de Exchange.
- Seleccione el protocolo de autenticación: **Kerberos** o **Basic**. El conector de Endpoint Management para Exchange ActiveSync admite la autenticación básica en implementaciones locales. De este modo, se puede utilizar el conector de Endpoint Management para Exchange ActiveSync cuando su servidor no pertenece al dominio en el que reside el servidor de Exchange.
- Haga clic en **Test Connectivity** para comprobar que se puede establecer conexión con el servidor de Exchange y, a continuación, haga clic en **Save**.
- Un mensaje le solicitará que reinicie el servicio. Haga clic en **Yes**.

9. Configure las reglas de acceso: seleccione la ficha **Configurar> Reglas de acceso**, haga clic en la ficha **XMS Rules** y luego haga clic en **Agregar**.



10. En la página **XenMobile Server Service Properties**, modifique la cadena de URL para que apunte a XenMobile Server. Por ejemplo, si el nombre de la instancia es **zdm**, escriba `https://<XdmHostName>/zdm/services/MagConfigService`. En el ejemplo, reemplace **XdmHostName** por la dirección IP o DNS de XenMobile Server.

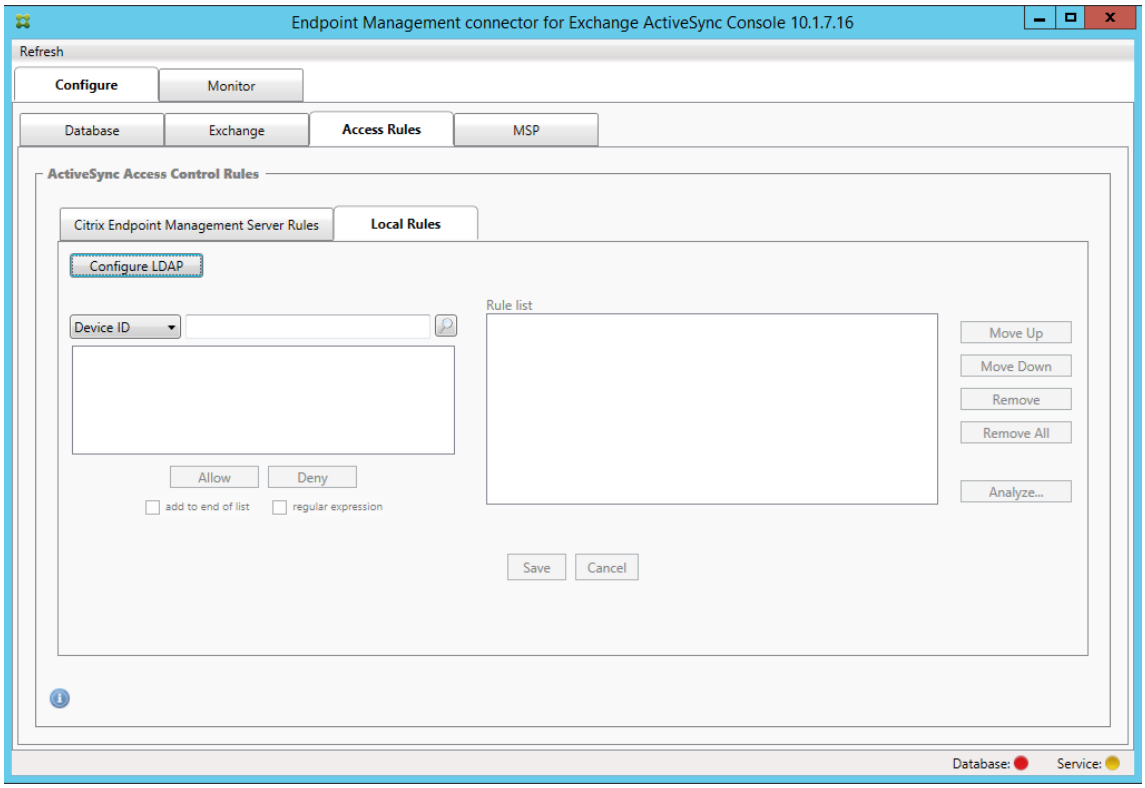


- Especifique un usuario autorizado del servidor.
- Escriba la contraseña del usuario.
- Conserve los valores predeterminados de **Baseline Interval**, **Delta Interval** y **Timeout**.

- Haga clic en **Test Connectivity** para probar la conexión con el servidor y haga clic en **OK**.

Si la casilla **Disabled** está marcada, el servicio de XenMobile Mail no recopila directivas de XenMobile.

11. Haga clic en la ficha **Local Rules**.



- 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.
- 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.

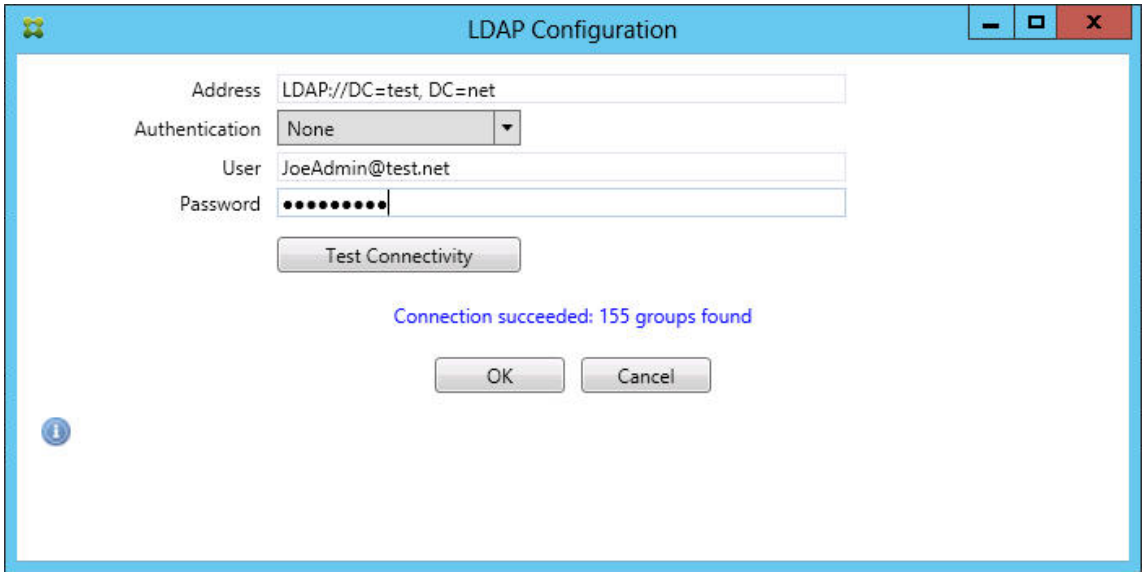
Para todos los criterios aparte de Group, el sistema se basa en los dispositivos que se han encontrado en una instantánea. Por lo tanto, si acaba de empezar y aún no ha completado ninguna instantánea, no habrá entidades disponibles.

- 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”.

- 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** y, a continuación, en **Save**.

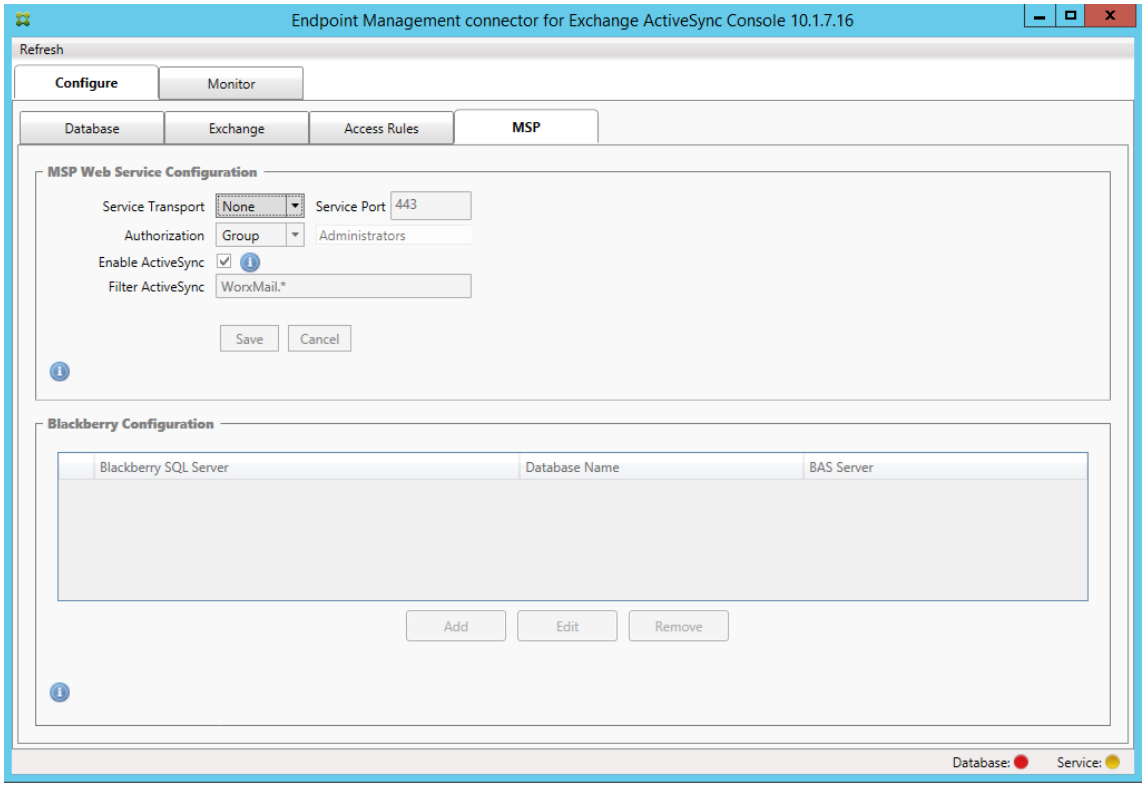
12. Si quiere crear reglas locales que operen en grupos de Active Directory, haga clic en **Configure LDAP** y, a continuación, configure las propiedades de conexión de LDAP.



13. Configure el proveedor de servicios móviles.

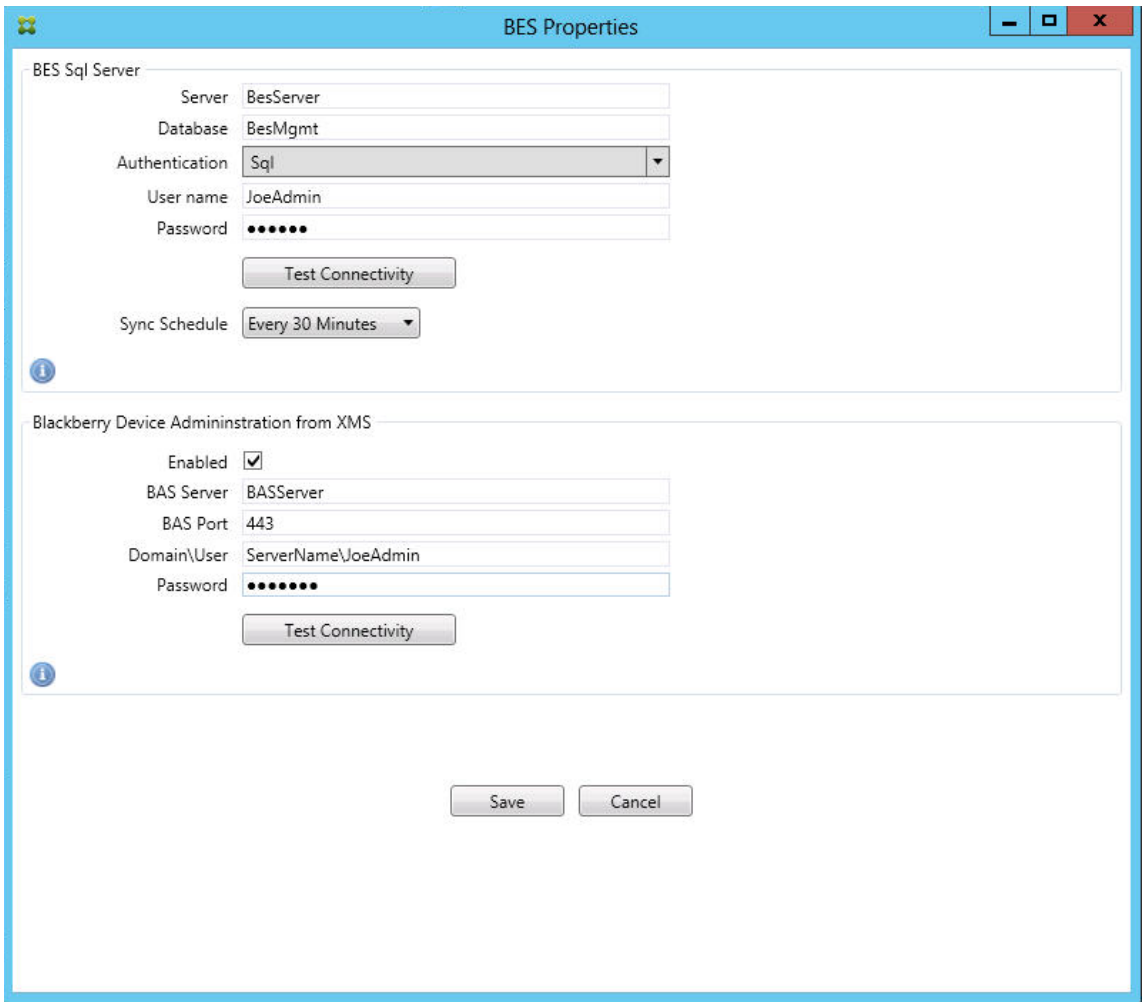
    El proveedor de servicios móviles es opcional. Ese parámetro solo es necesario si XenMobile también está configurado para usar la interfaz del proveedor de servicios móviles con el fin de consultar dispositivos no administrados.

    - Seleccione la ficha **Configure > MSP**.



- Establezca el tipo de servicio de transporte como **HTTP** o **HTTPS** para el servicio del proveedor de servicios móviles.
- Establezca el **puerto del servicio** (por regla general, 80 y 443) para el servicio del proveedor de servicios móviles. Si usa el puerto 443, ese puerto requiere un certificado SSL asociado a él en IIS.
- Defina el **grupo de autorización** o el **usuario**. 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. Si se habilitan las consultas de ActiveSync para XenMobile Server, el tipo de instantánea de uno o varios servidores Exchange debe ser **Deep**. Esta configuración puede generar costes importantes de rendimiento para realizar instantáneas.
- De forma predeterminada, los dispositivos ActiveSync que se corresponden con la expresión regular WorxMail.* no se enviarán a XenMobile. Para cambiar este comportamiento, modifique el campo **Filter ActiveSync** como sea necesario.
  Dejarlo en blanco significa que todos los dispositivos se reenviarán a XenMobile.
- Haga clic en **Guardar**.

14. Si quiere, configure una o varias instancias de BlackBerry Enterprise Server (BES). Para ello, haga clic en **Add** y escriba el nombre del servidor SQL de BES.



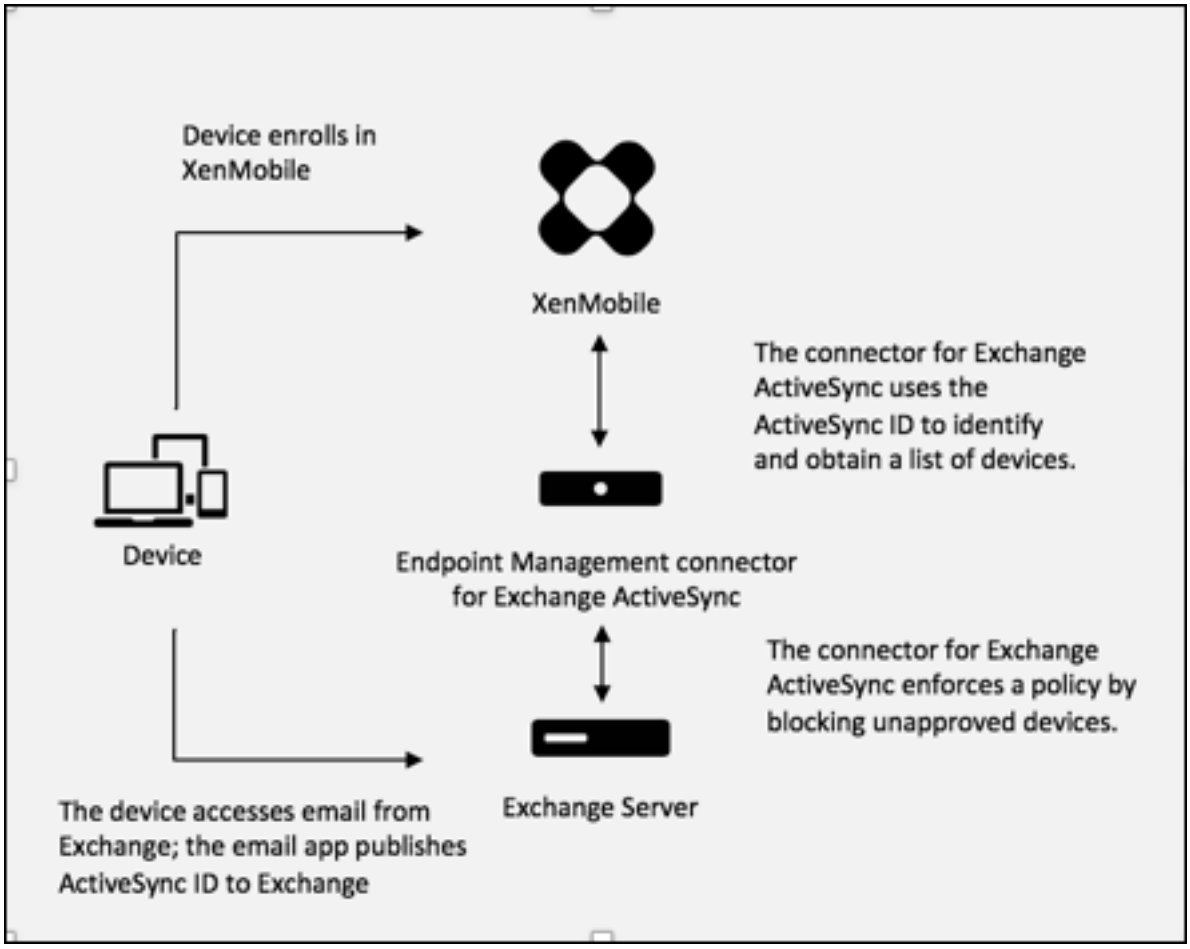
- Escriba el nombre de la base de datos de administración de BES.
- Seleccione el modo de **autenticación**. Si se selecciona la autenticación integrada de Windows, la cuenta de usuario del servicio del conector de Endpoint Management para Exchange ActiveSync será la cuenta utilizada para conectarse al servidor SQL para BES. Si también elige la autenticación integrada de Windows para la conexión de la base de datos del conector de Endpoint Management para Exchange ActiveSync, la cuenta de Windows especificada aquí también debe disponer de acceso a la base de datos del conector de Endpoint Management para Exchange ActiveSync.
- Si selecciona **SQL authentication**, especifique el nombre de usuario y la contraseña.
- 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.
- Haga clic en **Test Connectivity** para comprobar la conectividad con el servidor SQL. Si se selecciona la autenticación integrada de Windows, esta prueba utiliza el usuario actual que ha iniciado sesión, no el usuario del servicio del conector de Endpoint Management para Exchange ActiveSync; por lo tanto, la prueba de autenticación de SQL no es precisa.

- Si quiere admitir el borrado (Wipe) o el restablecimiento de contraseña (ResetPassword) remotos para los dispositivos BlackBerry desde XenMobile, marque la casilla **Enabled**.
- Introduzca el nombre de dominio completo (FQDN) de BES.
- Introduzca el puerto BES utilizado para el servicio web de admin.
- Escriba el nombre del usuario y la contraseña completos requeridos por el servicio de BES.
- Haga clic en **Test Connectivity** para probar la conexión al servidor BES.
- Haga clic en **Guardar**.

Aplicar directivas de correo electrónico con los ID de ActiveSync

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. El conector de Endpoint Management para Exchange ActiveSync y XenMobile operan juntos para aplicar este tipo de 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, el conector de Endpoint Management para Exchange ActiveSync aplica la directiva.

El cliente de correo electrónico en un dispositivo se anuncia a Exchange Server (u Office 365) mediante 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, el conector de Endpoint Management para Exchange ActiveSync 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 al conector de Endpoint Management para Exchange ActiveSync un ID de ActiveSync distinto del ID publicado por el dispositivo en Exchange, el conector de Endpoint Management para Exchange ActiveSync no podrá indicar a Exchange cómo debe proceder con respecto a dicho 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.

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 el conector de Endpoint Management para Exchange ActiveSync 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 en un dispositivo Android y si la detección de ID de ActiveSync no funciona correctamente, el empleado no podrá acceder al correo electrónico de la empresa.

Reglas de control de acceso

El conector de Endpoint Management para Exchange ActiveSync ofrece un enfoque basado en reglas para controlar de forma dinámica el acceso a los dispositivos Exchange ActiveSync. Una regla de control de acceso del conector de Endpoint Management para Exchange ActiveSync se compone 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 o 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.

El conector de Endpoint Management para Exchange ActiveSync contiene tres tipos de reglas: reglas locales, reglas de XenMobile Server, (también conocidas como reglas XDM) 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 de XenMobile Server ni la regla del acceso predeterminado. Las reglas locales se configuran localmente para el conector de Endpoint Management para Exchange ActiveSync, desde la ficha **Configurar > Reglas de acceso > Reglas locales**. La correspondencia de compatibilidad se basa en la pertenencia de un usuario a un grupo determinado de Active Directory. La correspondencia de compatibilidad 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 de XenMobile Server: Las reglas de XenMobile Server hacen referencia a un servidor externo de XenMobile que proporciona reglas sobre los dispositivos administrados. XenMobile Server se puede configurar con sus propias reglas de alto nivel, que identifican aquellos dispositivos que se van a permitir o bloquear en función de las propiedades que conozca XenMobile (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 al conector de Endpoint Management para Exchange ActiveSync.

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 de XenMobile Server, el estado del acceso al dispositivo lo determina el estado de la regla del acceso predeterminado.

- **Default Access – Allow (Acceso predeterminado: Permitir):** Se permitirá el acceso de cualquier dispositivo que no coincida con una regla local o de XenMobile Server.
- **Default Access – Block (Acceso predeterminado: Bloquear):** Se bloqueará el acceso de cualquier dispositivo que no coincida con una regla local o de XenMobile Server.
- **Default Access - Unchanged (Acceso predeterminado: Sin cambios):** El conector de Endpoint Management para Exchange ActiveSync no modificará el estado de acceso de un dispositivo que no coincida con ninguna regla local o de XenMobile Server. 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 una regla de Device Manager 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. conector de Endpoint Management para Exchange ActiveSync:

- Reglas locales
- Reglas de XenMobile Server
- 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 de XenMobile Server 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.

El conector de Endpoint Management para Exchange ActiveSync vuelve a cotejar el conjunto de reglas definido en cada momento cuando cambian las propiedades del dispositivo, cuando se agregan o quitan dispositivos o cuando cambian las propias reglas. 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 comprender el funcionamiento de estas reglas en el contexto del conector de Endpoint Management para Exchange ActiveSync. Exchange se puede configurar con tres niveles de reglas: exenciones personales, reglas de

dispositivos y parámetros de organización. El conector de Endpoint Management para Exchange ActiveSync automatiza el control del acceso a través de 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 el conector de Endpoint Management para Exchange ActiveSync se implementa, asume la capacidad de administración de las listas de exención en Exchange. Para obtener información detallada, consulte el artículo de Microsoft Controlling Device Access.

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 por grupos con el campo que se coteja (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

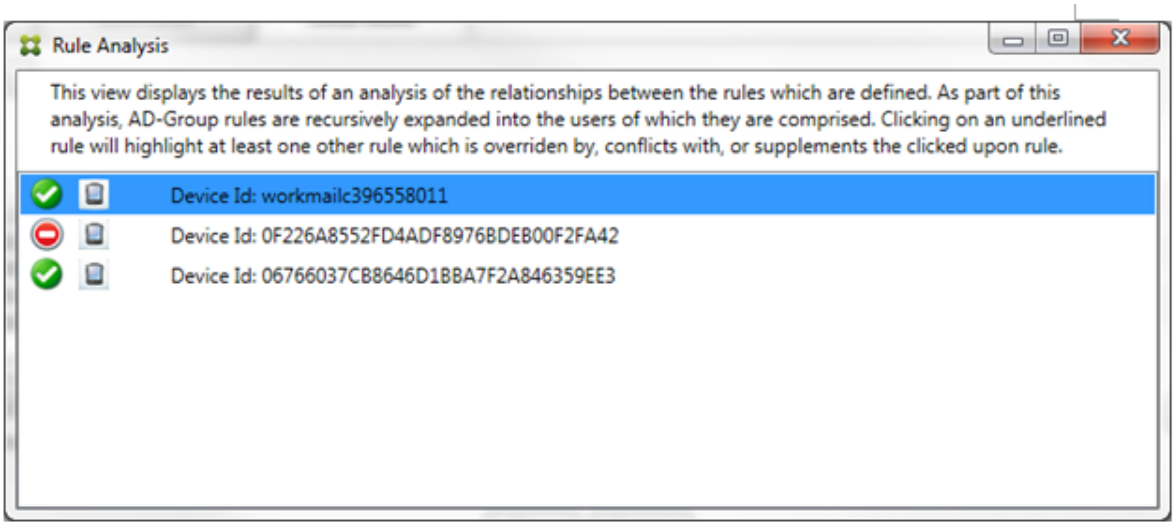
- **Overriding rule (Regla de invalidación):** Se produce una invalidación cuando hay más de una regla que se podría aplicar al mismo dispositivo. Como las reglas se cotejan por prioridad en la lista, es posible que las últimas instancias de reglas que se podrían aplicar nunca se cotejen.
- **Conflicting 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 en conflicto 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 hacia arriba, indica que hay reglas auxiliares que preceden la regla primaria. Si una flecha apunta hacia 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 invalida la regla auxiliar, y/o la regla auxiliar entra en conflicto en el acceso con la regla primaria, y/o la regla auxiliar

complementa la regla primaria.

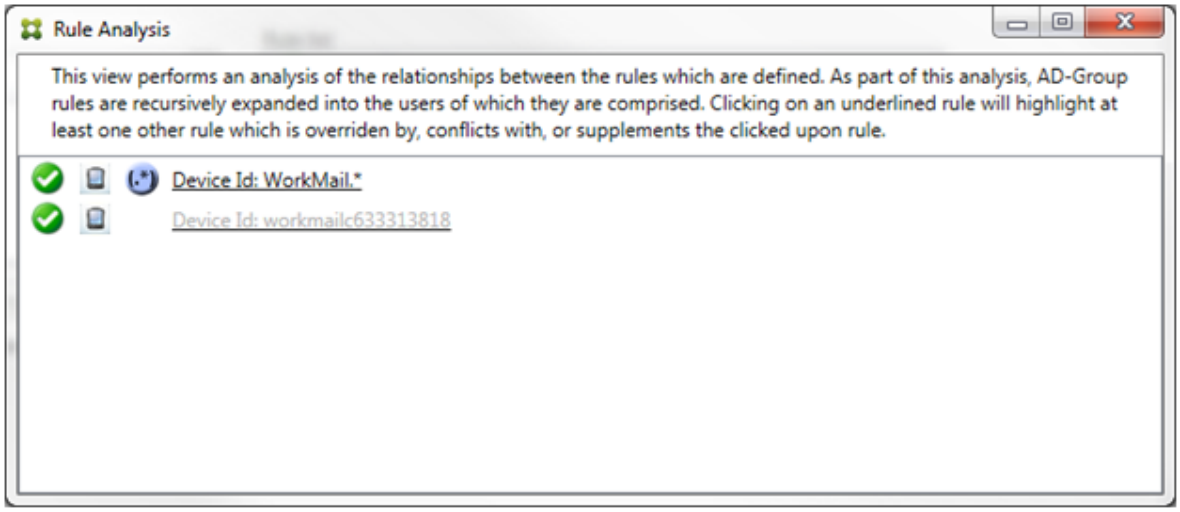
Cómo aparecen los tipos de reglas en el cuadro de diálogo Rule Analysis

Cuando no haya conflictos, invalidaciones ni 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.

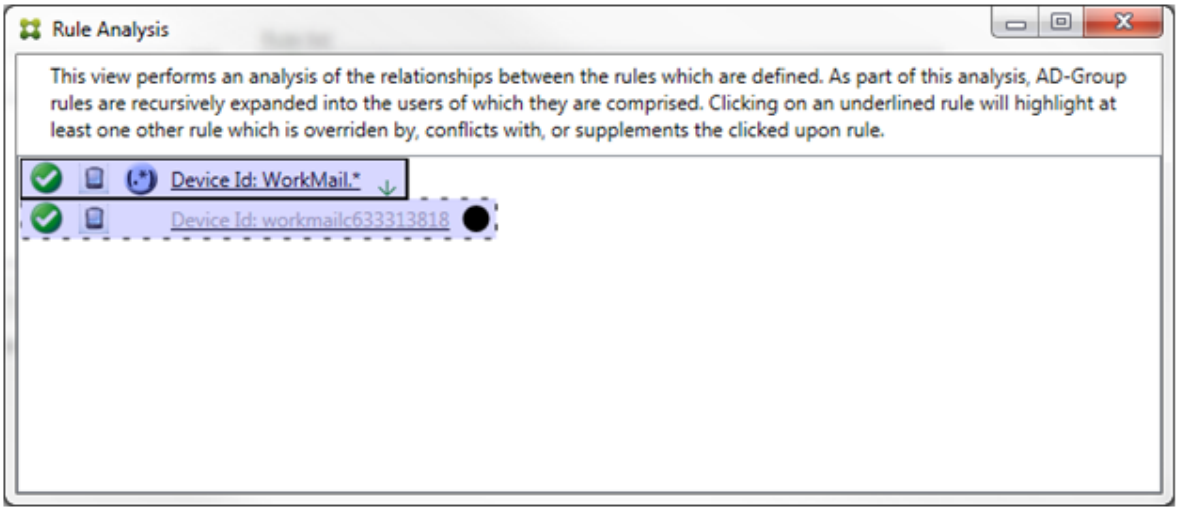
La ventana “Rule Analysis” tiene una casilla de verificación que, marcada, muestra únicamente las reglas con conflictos, invalidaciones, redundancias y complementaciones.



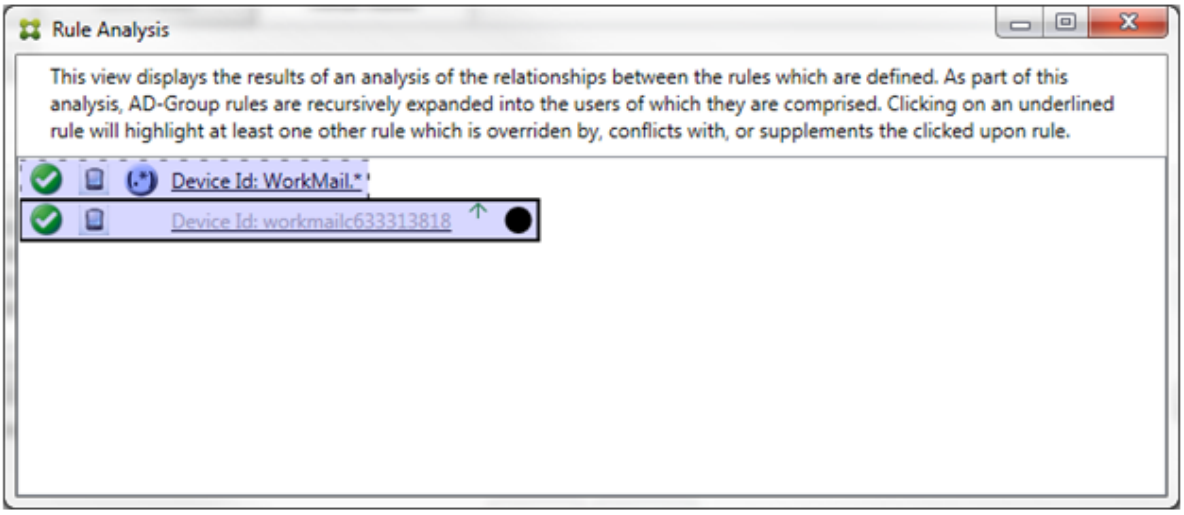
Cuando se produzca una invalidación, se subrayarán al menos dos reglas: la primaria y las auxiliares. Al menos una regla auxiliar aparece con una fuente más atenuada para indicar que se ha reemplazado por otra regla de mayor prioridad. Puede hacer clic en la regla invalidada para averiguar qué regla 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 visual de que la regla está inactiva. Por ejemplo, antes de hacer clic en la regla, el cuadro aparece de la siguiente manera:



Cuando haga clic en la regla de mayor prioridad, el cuadro aparecerá de la siguiente manera:

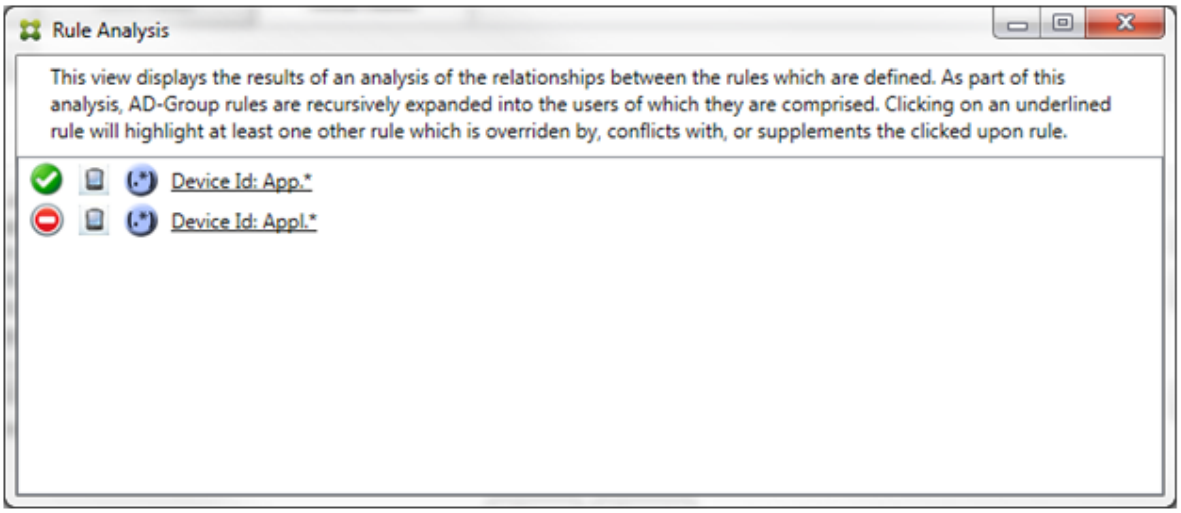


En este ejemplo, la regla de expresión regular `WorkMail.*` es la regla primaria (indicada con el borde sólido) y la regla normal `workmailc633313818` es una regla auxiliar (indicada con el borde discontinuo). El punto negro junto a la regla auxiliar es una indicación visual de que la regla está inactiva (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:



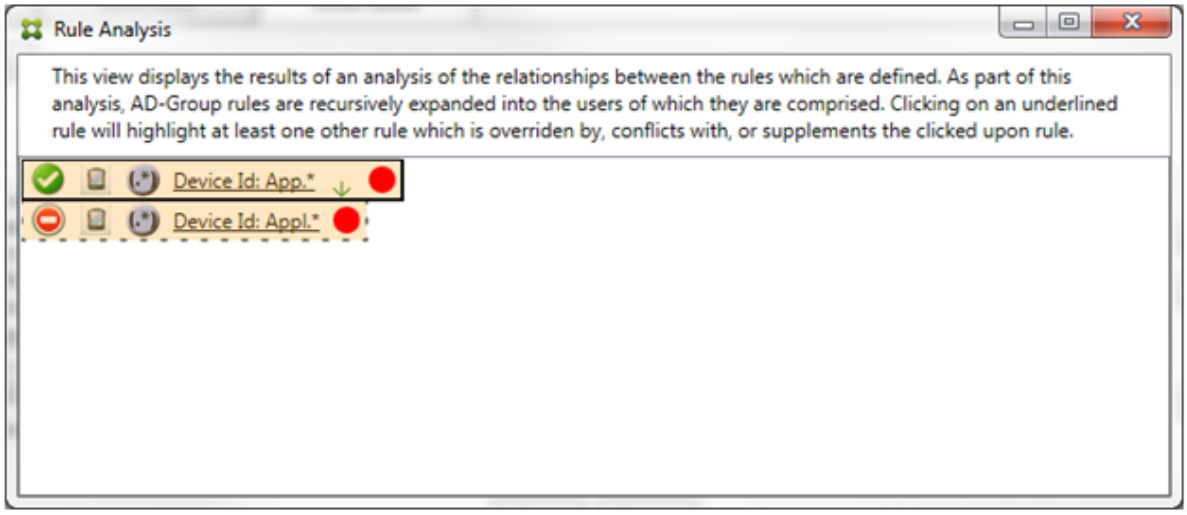
En el ejemplo anterior, la regla de expresión regular `WorkMail.*` es la regla auxiliar (indicada con el borde discontinuo) y la regla normal `workmailc633313818` es la regla primaria (indicada con el borde sólido). En este sencillo ejemplo, no hay mucha diferencia. Para un ejemplo más complejo, consulte 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 aparece de la siguiente manera:



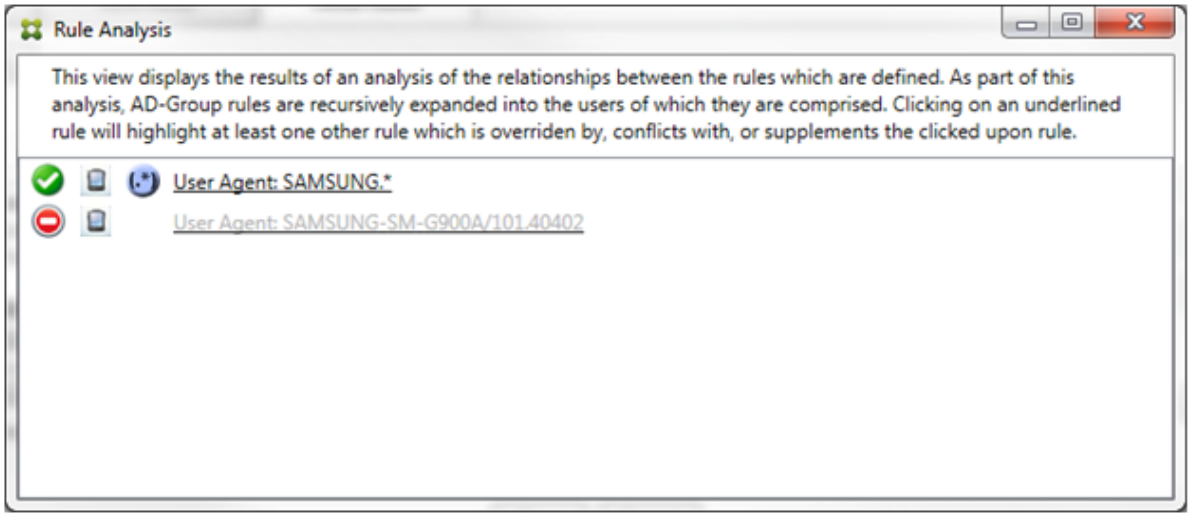
Tras examinar las dos reglas de expresiones regulares, es evidente que la primera regla permite el acceso a todos aquellos dispositivos con un ID de dispositivo que contenga “App” y la segunda regla niega el acceso a todos aquellos dispositivos con un ID de dispositivo que contenga “Appl”. Además,

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 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 aparece de la siguiente manera:



En este caso, tanto la regla primaria (la regla de expresión regular `App.*`) como la regla auxiliar (la regla de expresión regular `Appl.*`) se resaltan en amarillo. Este es simplemente un elemento visual que sirve para advertirle de que ha aplicado más de una regla de expresión regular a un único campo correspondiente, lo que puede derivar en un problema de redundancia o algo más grave.

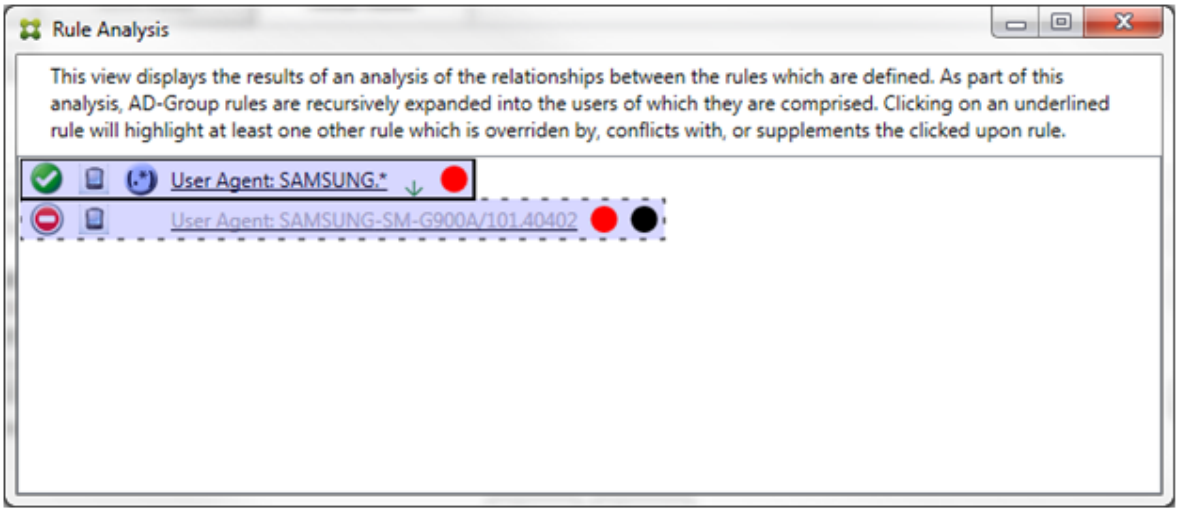
En un caso de conflicto e invalidación, la regla primaria (regla de expresión regular `App.*`) y la regla auxiliar (regla de expresión regular `Appl.*`) se resaltan en amarillo. Este es simplemente un elemento visual que sirve para advertirle de que ha aplicado más de una regla de expresión regular a un único campo correspondiente, lo que puede derivar en un problema de redundancia o algo más grave.



En el ejemplo anterior, es fácil observar que la primera regla (regla de expresión regular `SAMSUNG.*`)

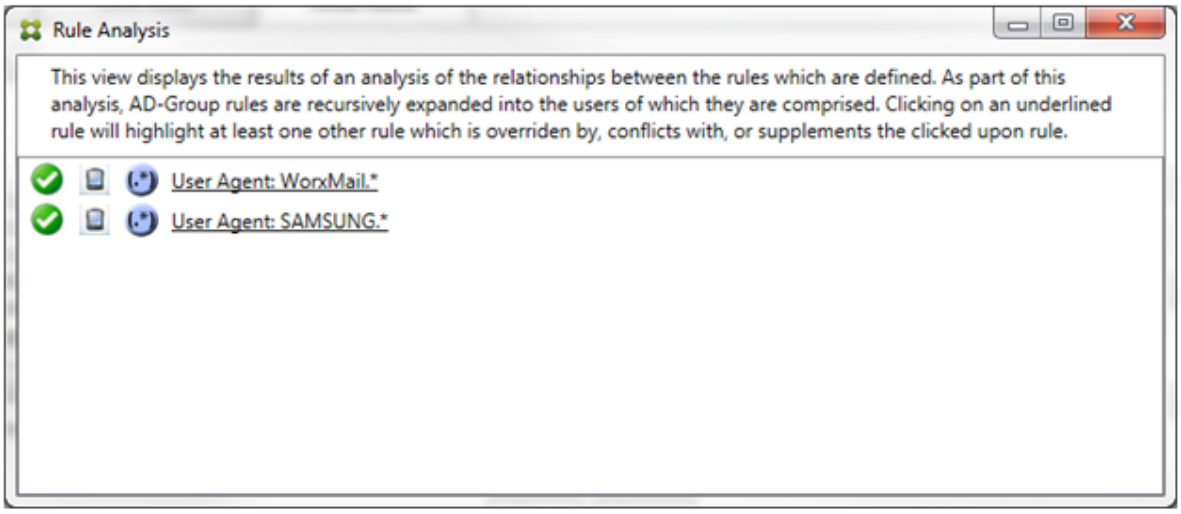
no solo invalida la siguiente regla (regla normal `SAMSUNG-SM-G900A/101.40402`), sino que las dos reglas se diferencian en su acceso (la primaria especifica Permitir, mientras que la auxiliar especifica Bloquear). La segunda regla (regla normal `SAMSUNG-SM-G900A/101.40402`) aparece con un texto más atenuado para indicar que se ha invalidado y está, por lo tanto, inactiva.

Después de hacer clic en la regla de expresión regular, el cuadro aparece de la siguiente manera:

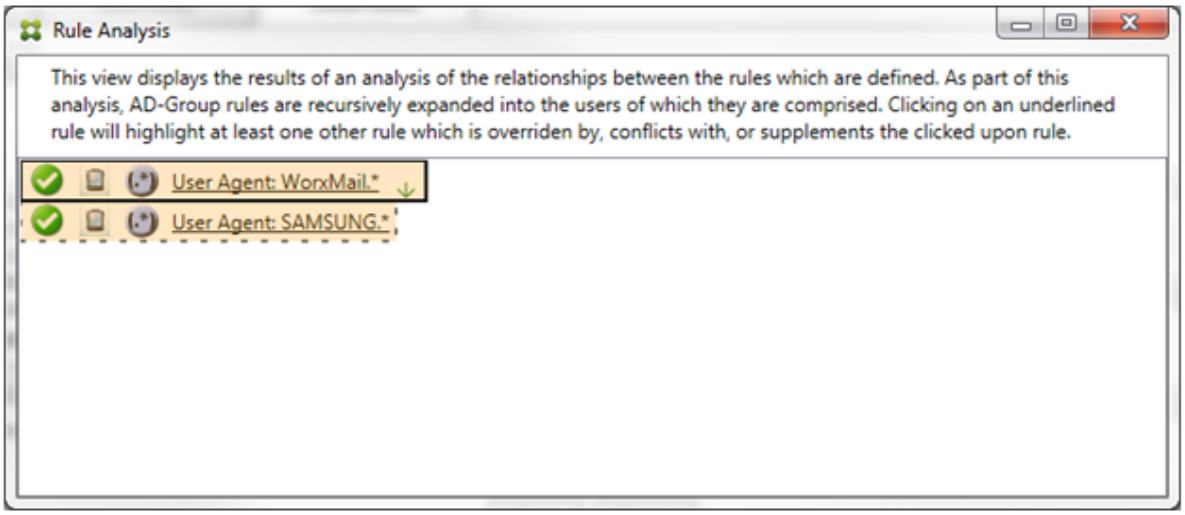


La regla primaria (regla de expresión regular `SAMSUNG.*`) va seguida de un punto rojo para indicar que su estado de acceso está en conflicto con una o varias reglas auxiliares. La regla auxiliar (regla normal `SAMSUNG-SM-G900A/101.40402`) va seguida de un punto rojo para indicar que su estado de acceso está en conflicto con la regla primaria. Esa regla también va seguida de un punto negro para indicar que está invalidada y, por lo tanto, 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 aparece de la siguiente manera:



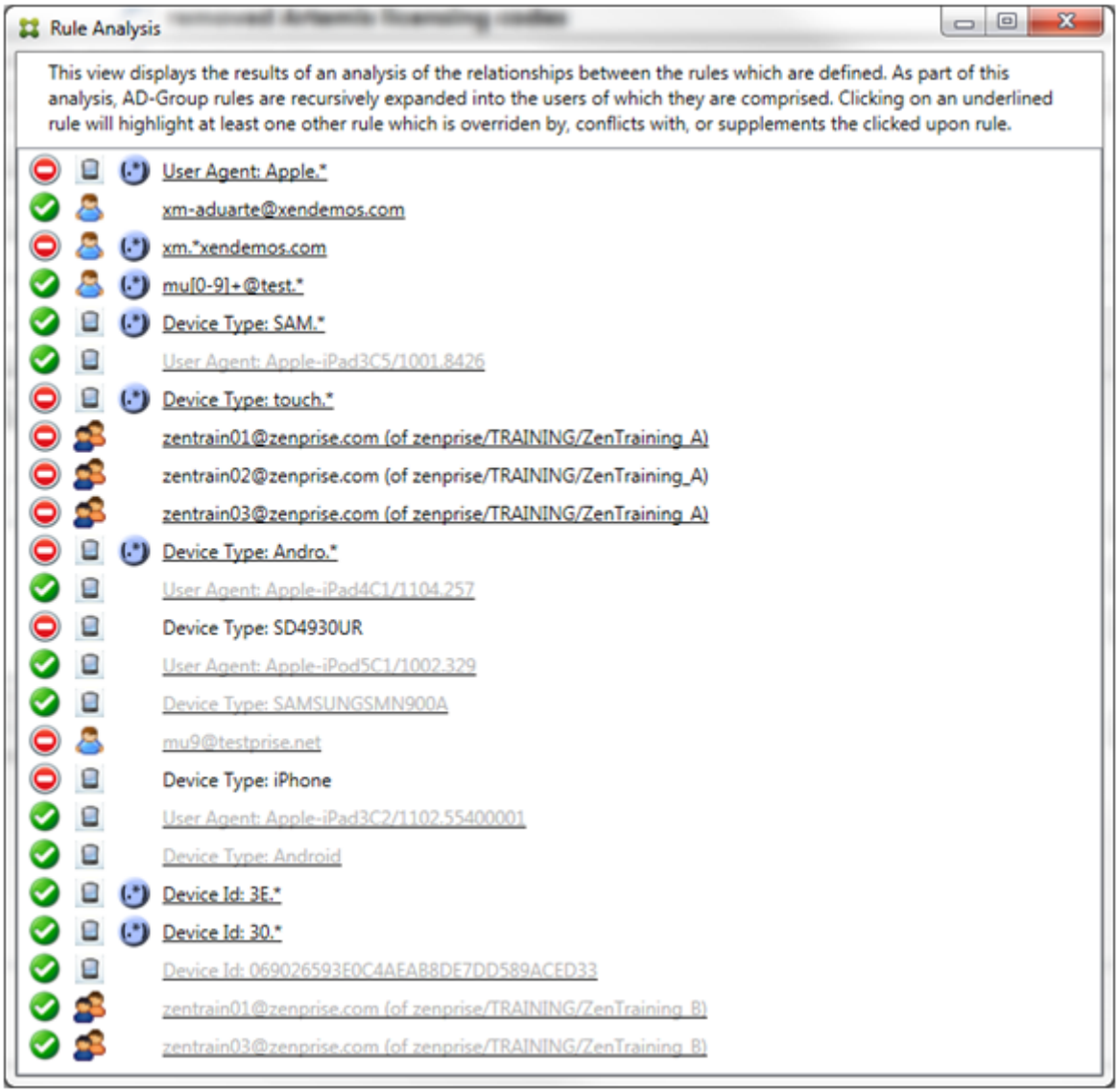
Tras echar un vistazo, es evidente que ambas reglas son de expresión regular y que se han aplicado al campo de ID de dispositivo ActiveSync en el conector de Endpoint Management para Exchange ActiveSync. Después de hacer clic en la primera regla, el cuadro aparece de la siguiente manera:



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 el conector de Endpoint Management para Exchange ActiveSync. En este caso, ese campo es el ID del dispositivo ActiveSync. Las expresiones regulares pueden superponerse. Le corresponde a usted decidir si sus expresiones regulares se han elaborado correctamente.

Ejemplo de una expresión compleja

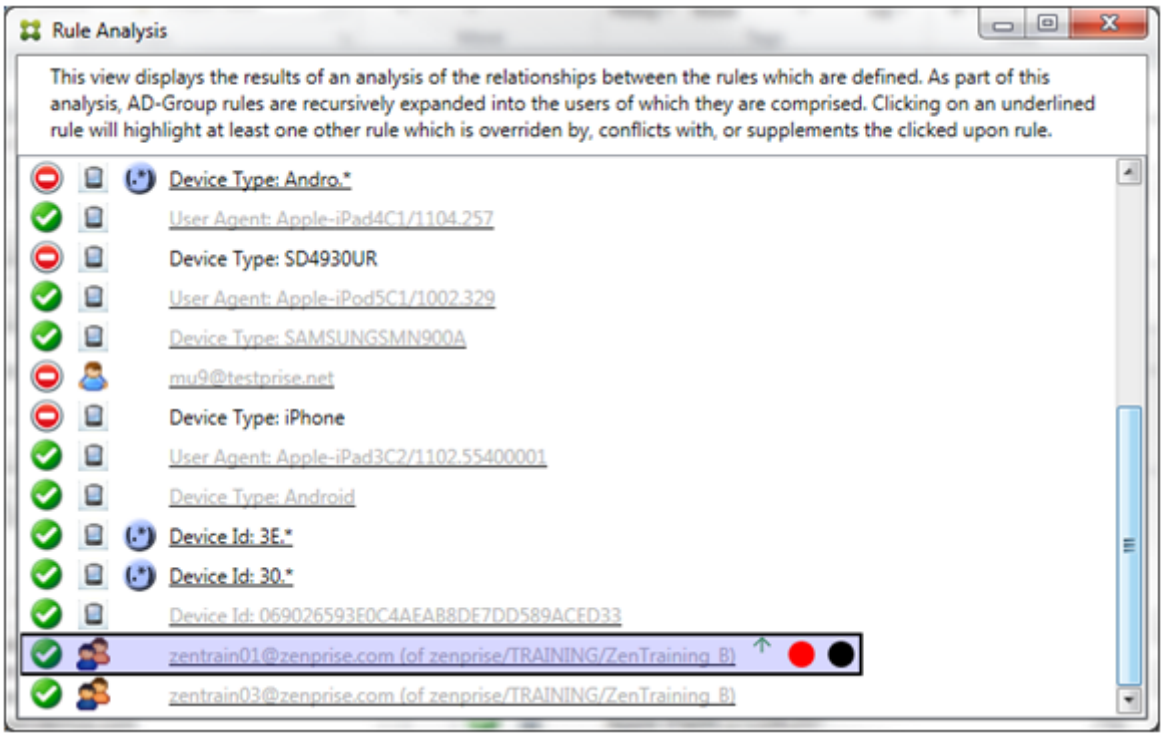
Se pueden producir tantos conflictos, invalidaciones o complementaciones que no se puede ofrecer un ejemplo para todos los casos posibles. En el siguiente ejemplo, se describe lo que no se recomienda hacer y también se ilustra el true potencial de la construcción visual del análisis de reglas. En la 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.

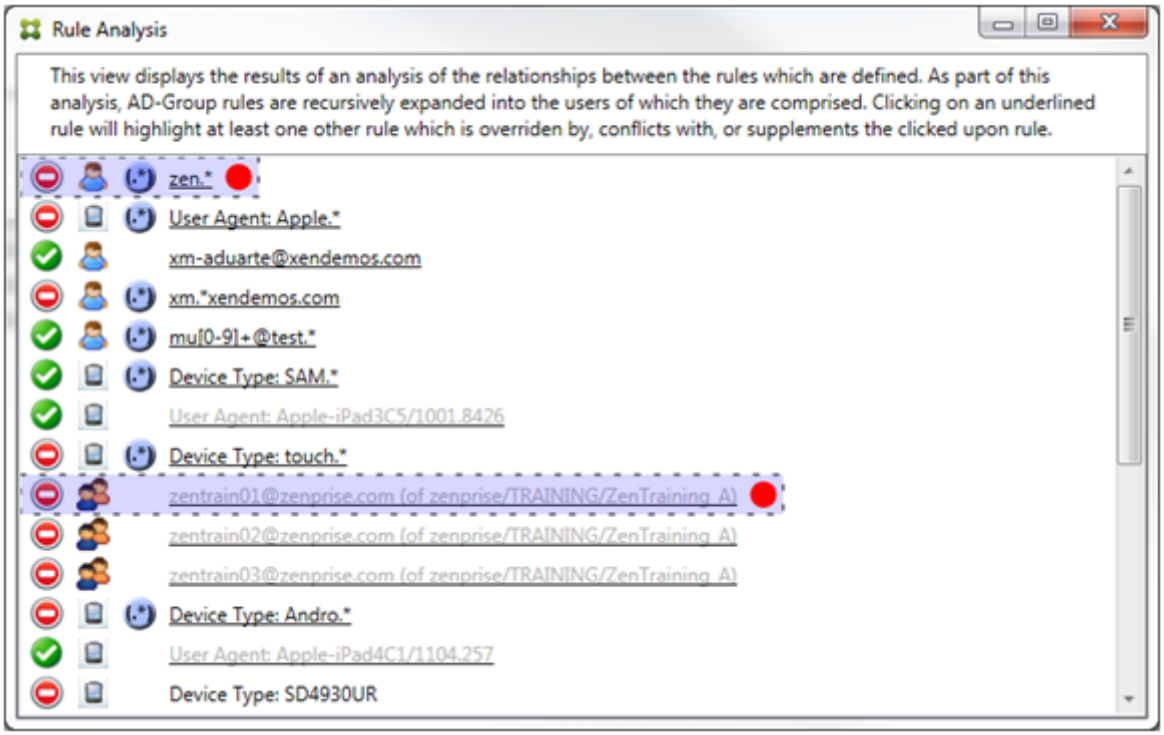
Ejemplo 1: En este ejemplo, se examina por qué `zentrain01@zenprise.com` se ha invalidado.



La regla primaria (regla del grupo AD `zenprise/TRAINING/ZenTraining B`, donde `zentrain01@zenprise.com` es miembro) tiene las siguientes características:

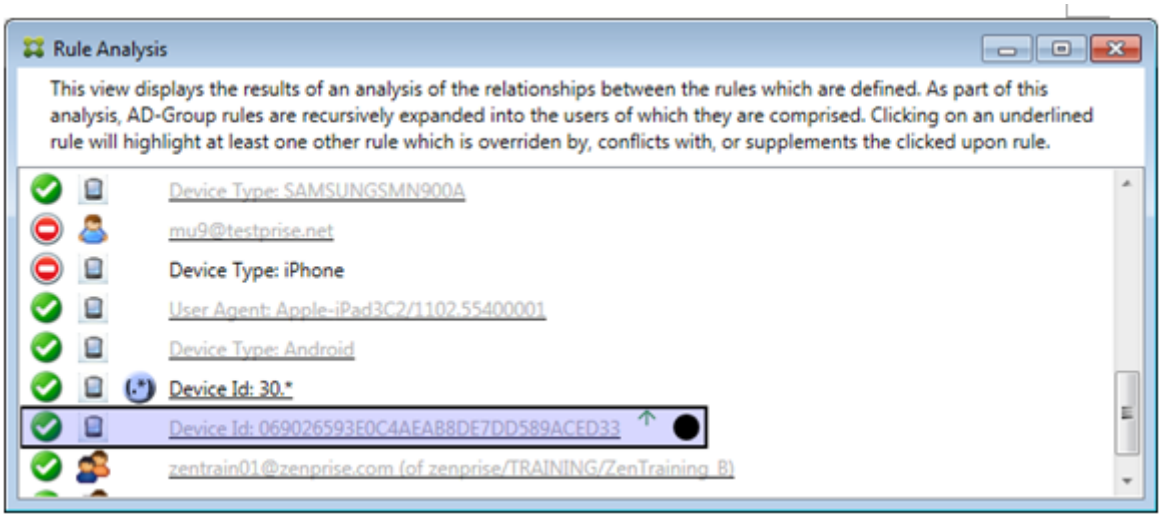
- Está resaltada en azul y tiene un borde sólido.
- Tiene una flecha verde que apunta hacia arriba (para indicar que las reglas auxiliares están todas encima de ella).
- Va seguida de un círculo rojo y uno negro para indicar, respectivamente, que una o más reglas están en conflicto con el acceso y que la regla primaria se ha invalidado y, por lo tanto, está inactiva.

Si se desplaza hacia arriba, verá lo siguiente:



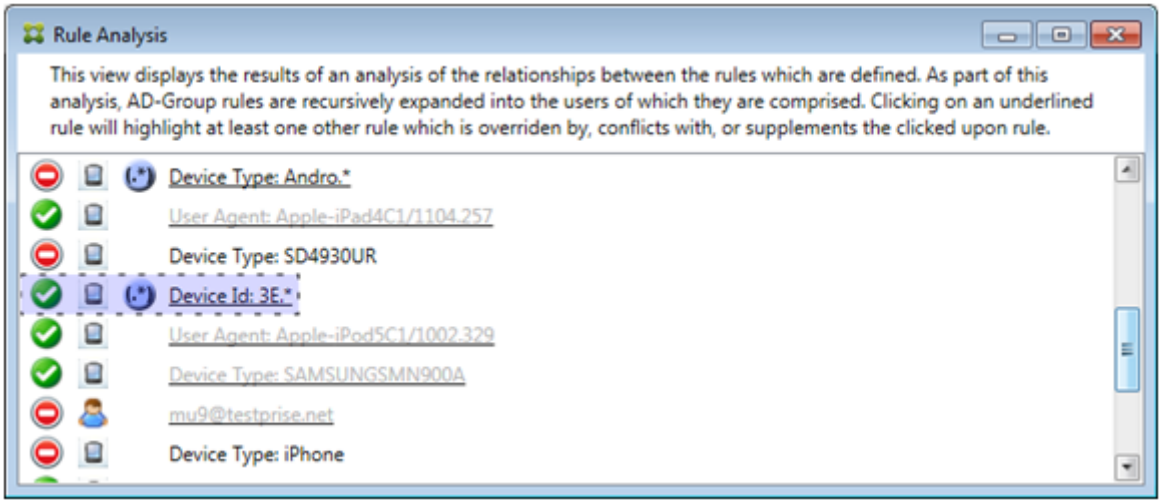
En este caso, hay dos reglas auxiliares que invalidan la regla primaria: la regla de expresión regular `zen.*` y la regla normal `zentrain01@zenprise.com` (de `zenprise/TRAINING/ZenTraining A`). En el caso de la última regla auxiliar, lo que ha ocurrido es que la regla del grupo de Active Directory `ZenTraining A` contiene el usuario `zentrain01@zenprise.com` y la regla del grupo de Active Directory `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.

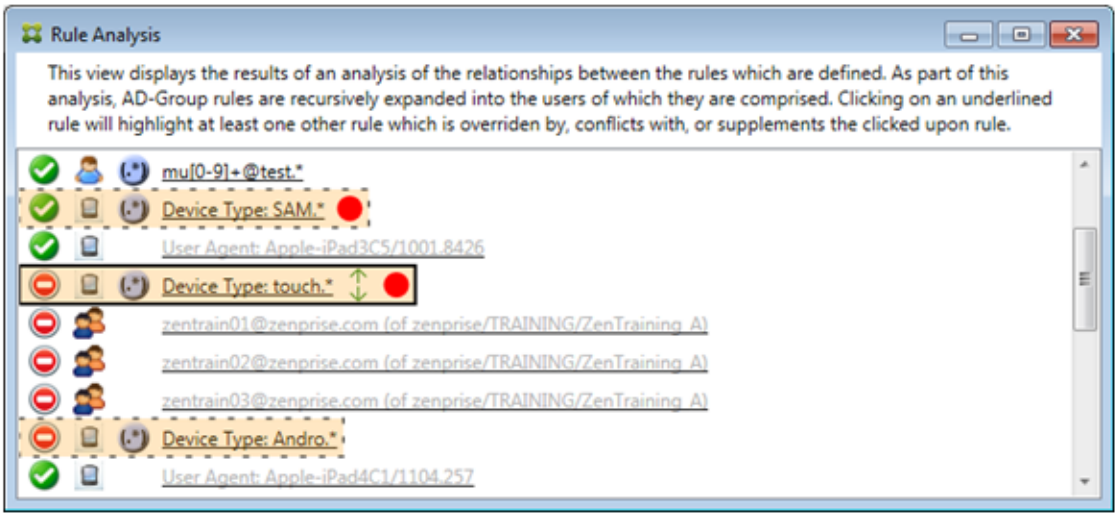


En este caso, una sola regla auxiliar invalida la regla primaria: la regla de expresión regular de ID de dispositivo ActiveSync es `3E.*`. Como la expresión regular `3E.*` se correspondería con `069026593E0C4AEAB8DE7DD589ACED33`, la regla primaria no se cotejará nunca.

Cómo analizar una complementación y un conflicto

En este caso, la regla primaria es la regla en forma de expresión regular del tipo de dispositivo ActiveSync `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 entra en conflicto con la regla primaria, cuyo acceso está establecido en Bloquear.
- Hay dos reglas auxiliares: la regla de expresión regular de tipo de dispositivo ActiveSync `SAM.*` y la regla de expresión regular de tipo de dispositivo ActiveSync`Andro.*`.
- Ambas reglas tienen bordes discontinuos para indicar que son auxiliares.
- Ambas reglas auxiliares tienen una capa amarilla para indicar que también se aplican 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

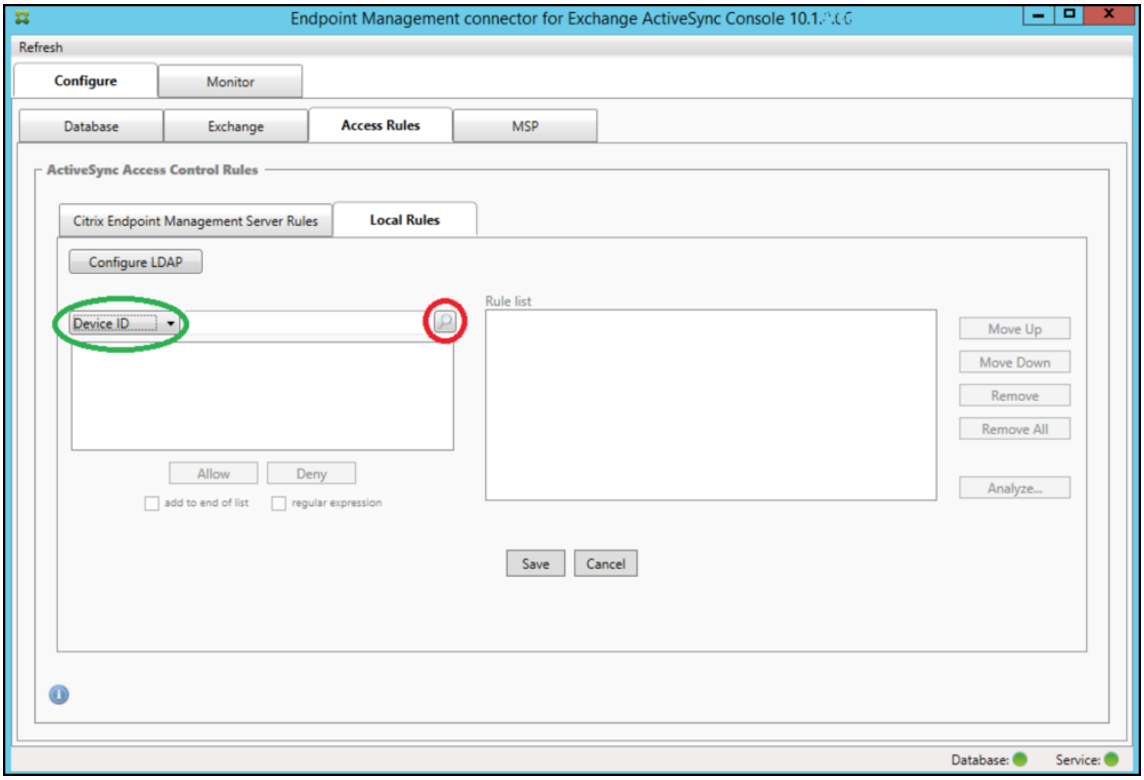
En este ejemplo, se describe cómo las relaciones entre reglas se dan siempre con respecto a la regla primaria. En el ejemplo anterior, se ha mostrado cómo un clic en la regla de expresión regular se

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.

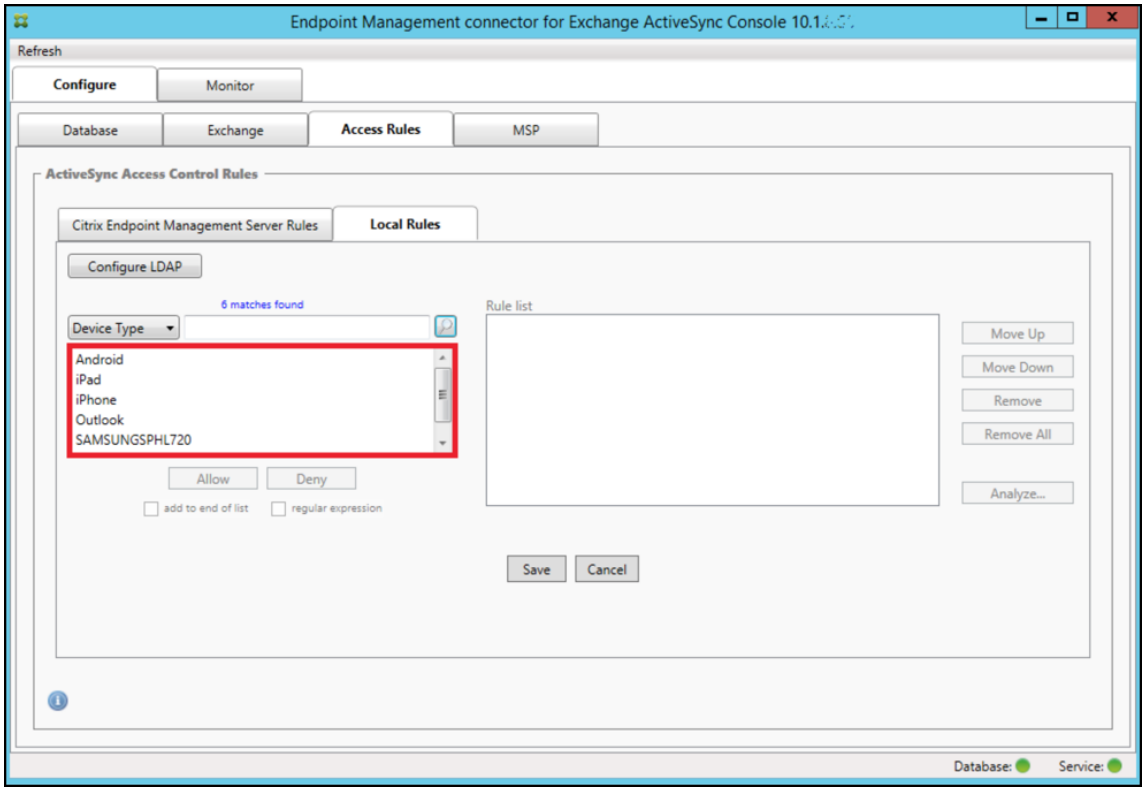
El ejemplo muestra una regla invalidada que se incluye en la relación de las reglas. Esta es la regla normal de tipo de dispositivo ActiveSync `Android`, que se ha invalidado (situación indicada con la fuente más atenuada y el círculo negro junto a ella) y también está en conflicto en el acceso con la regla primaria de expresión regular de tipo de dispositivo ActiveSync `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 expresión regular de tipo de dispositivo ActiveSync `touch.*`), no estaba relacionada con ella.

Para configurar una regla local de expresión normal

1. Haga clic en la ficha **Access Rules**.



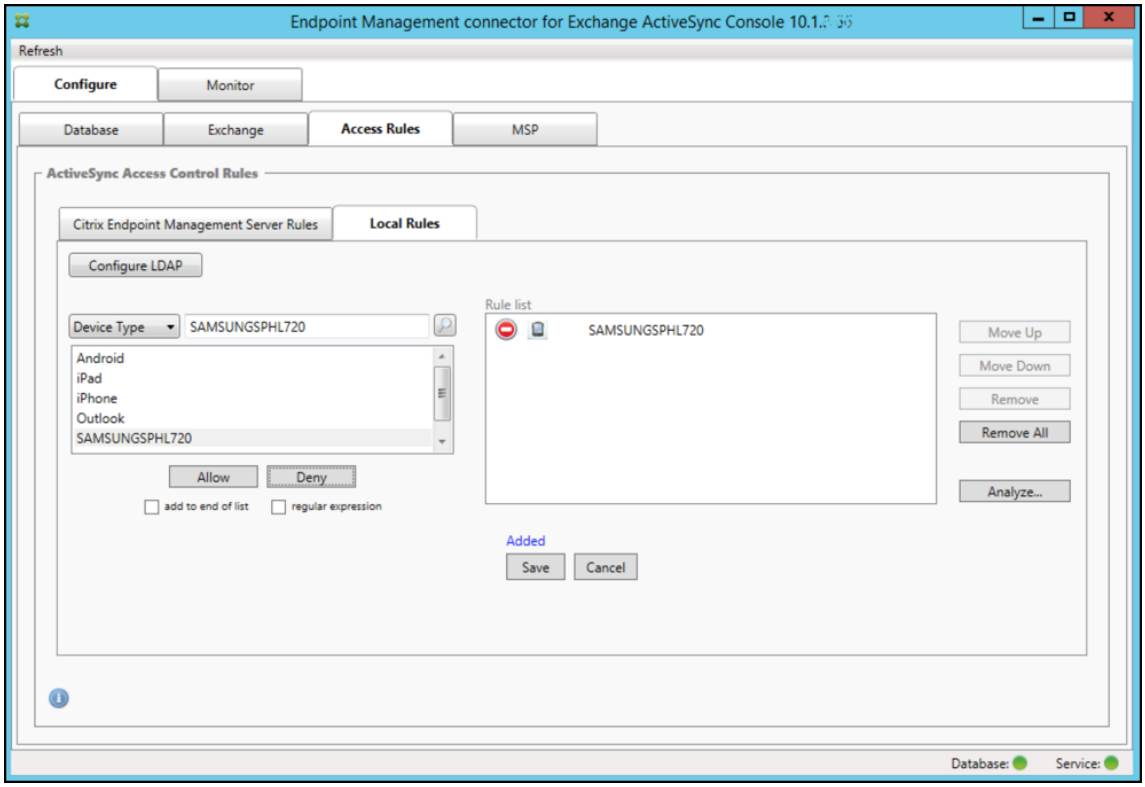
2. En la lista **Device ID**, seleccione el campo para el que quiere crear una regla local.
3. Haga clic en el icono de lupa para ver todas las correspondencias únicas con el campo seleccionado. En este ejemplo, se ha seleccionado el campo **Device Type**, y las opciones se muestran a continuación, en 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 SamsungSPhl720.



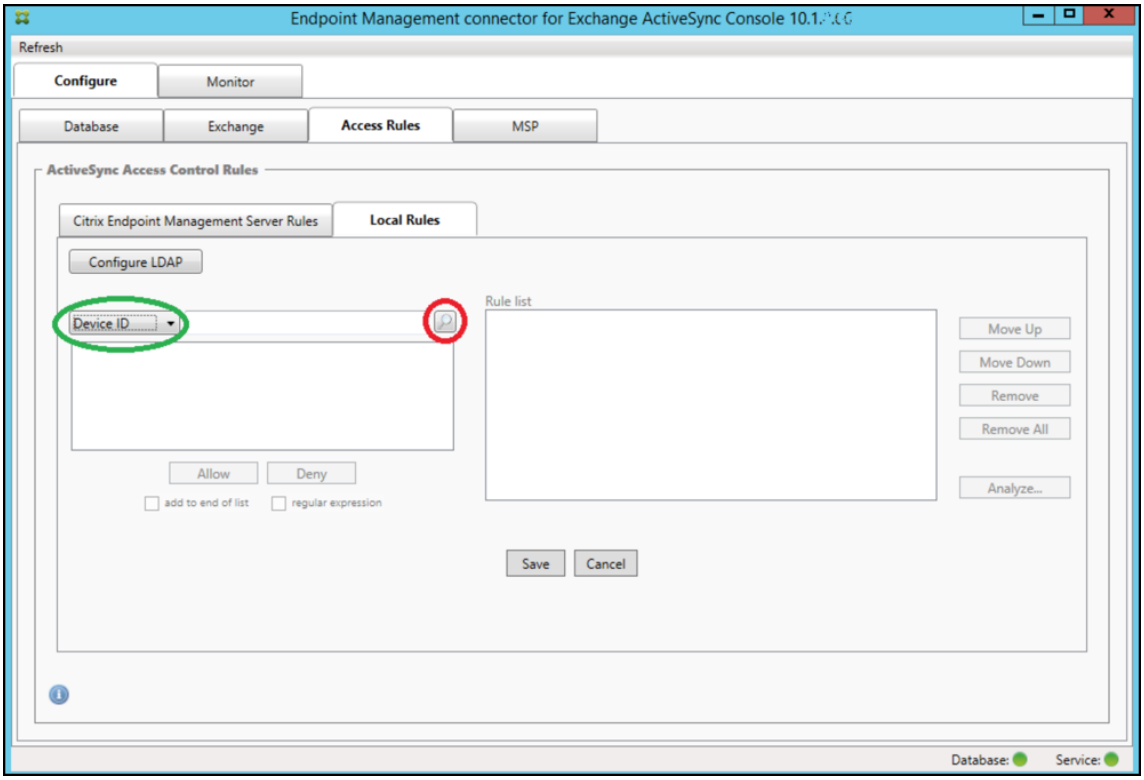
Para agregar una expresión regular

Las reglas locales de expresión regular se distinguen por el icono que aparece junto a ellas:  .

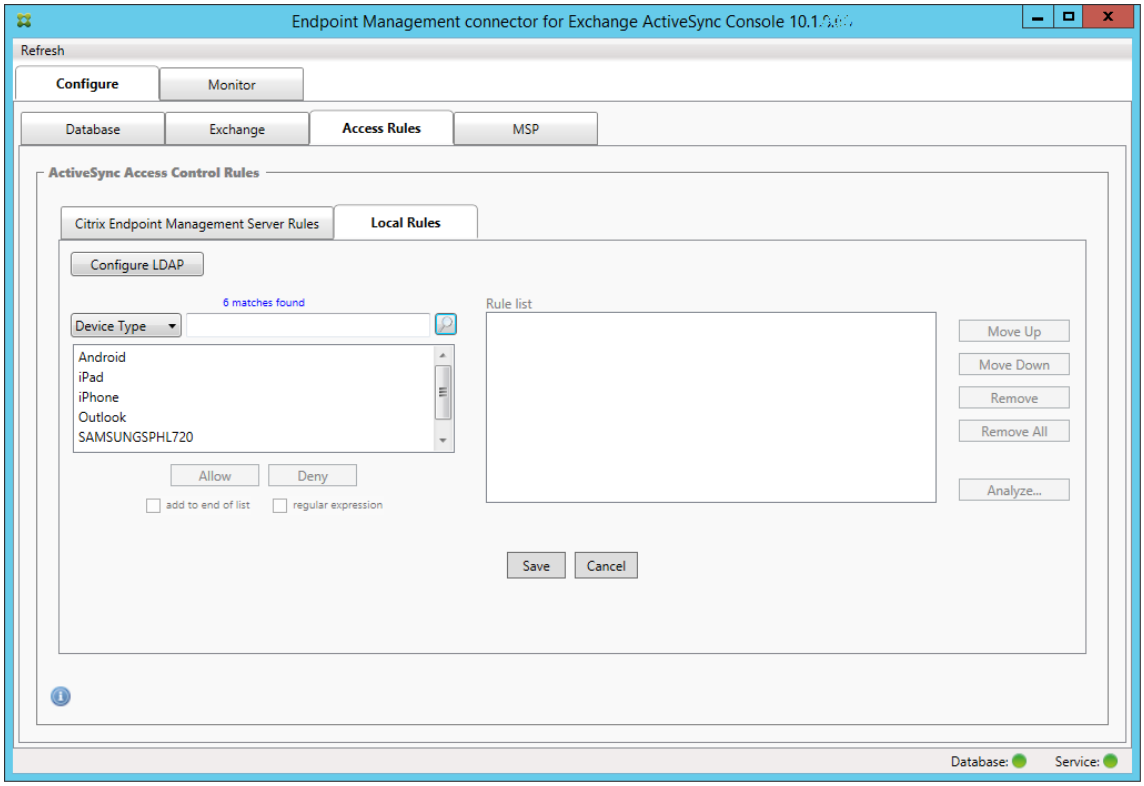
Para agregar una regla de expresión regular, puede crear una regla de expresión regular a partir de un valor existente de la lista de resultados de un campo determinado (siempre que se haya completado una instantánea principal), o bien puede, simplemente, escribir la expresión regular que quiera.

Para crear una expresión regular a partir de un valor de campo existente

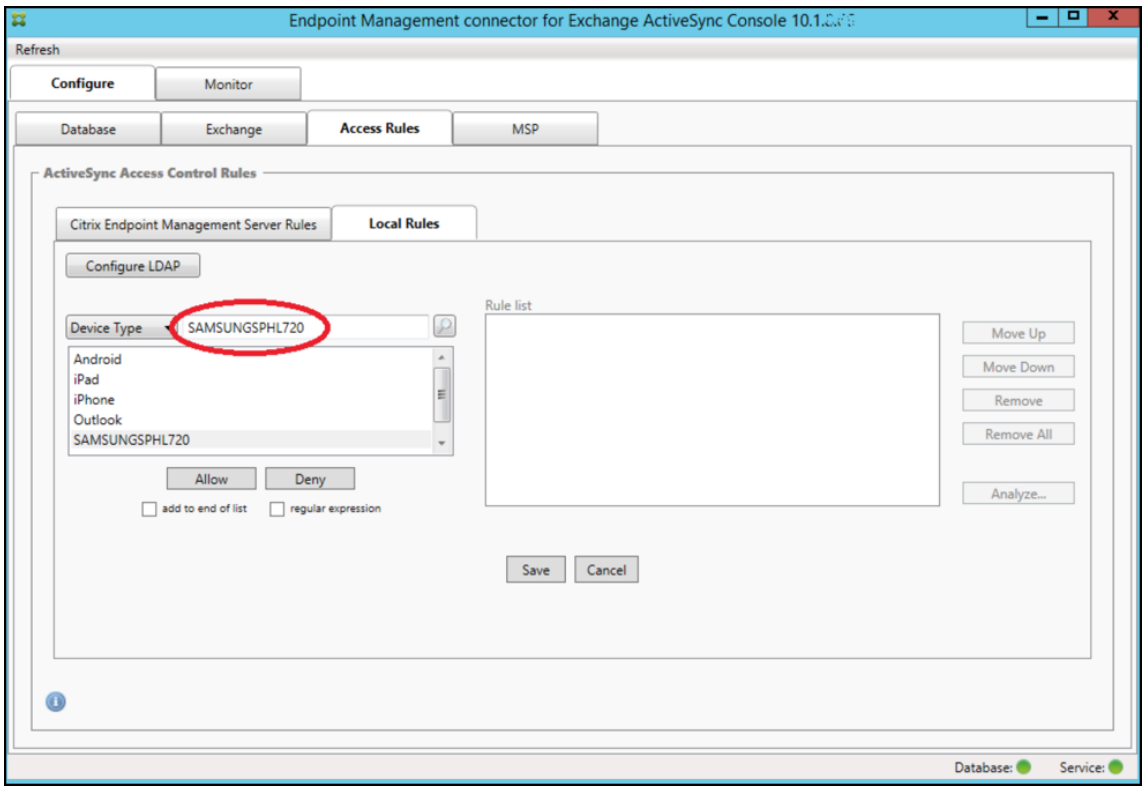
1. Haga clic en la ficha **Access Rules**.



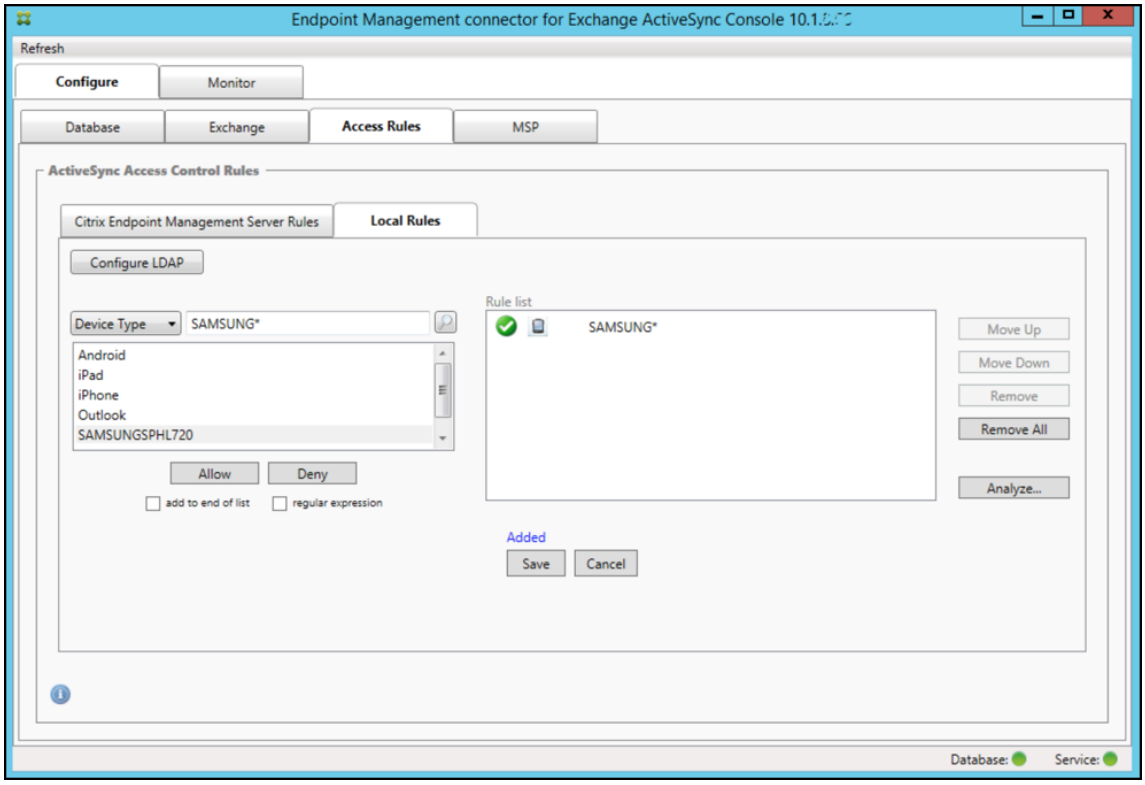
2. En la lista **Device ID**, seleccione el campo para el que quiere crear una regla local de expresión regular.
3. Haga clic en el icono de lupa para ver todas las correspondencias únicas con el campo seleccionado. En este ejemplo, se ha seleccionado el campo **Device Type**, y las opciones se muestran 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**.

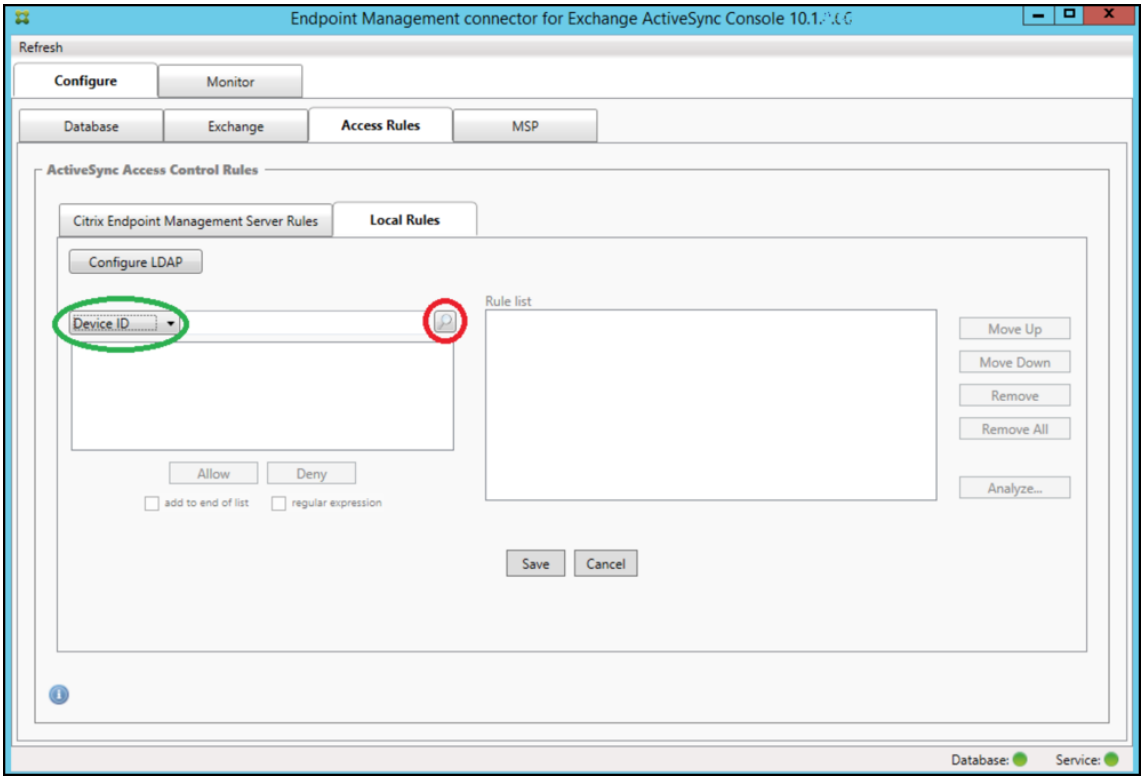


5. Para permitir el acceso a todos los tipos de dispositivos que contengan “Samsung” en su valor de tipo de dispositivo, siga estos pasos para agregar una regla de expresión regular:
   a) Haga clic en el cuadro de texto del elemento seleccionado.
   b) Cambie el texto de **SAMSUNGSPHL720** a **SAMSUNG.***.
   c) Compruebe que la casilla “regular expression” está marcada.
   d) Haga clic en **Allow**.

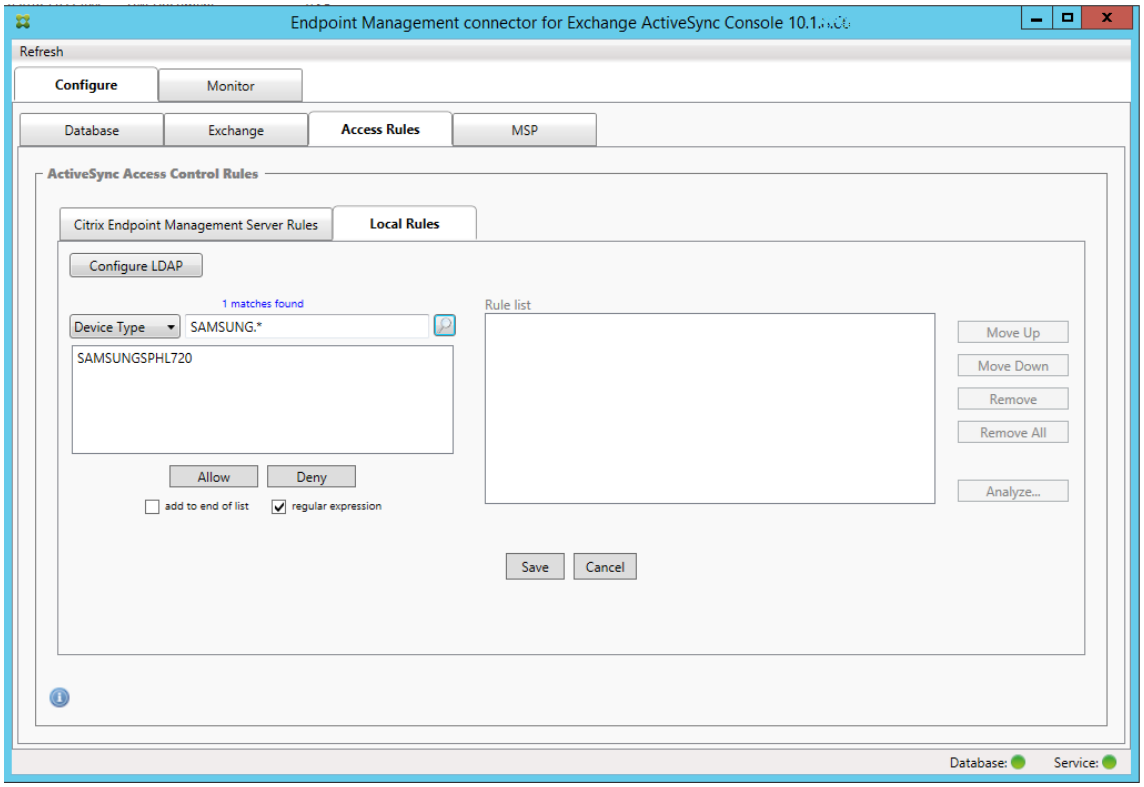


Para crear una regla de acceso

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.



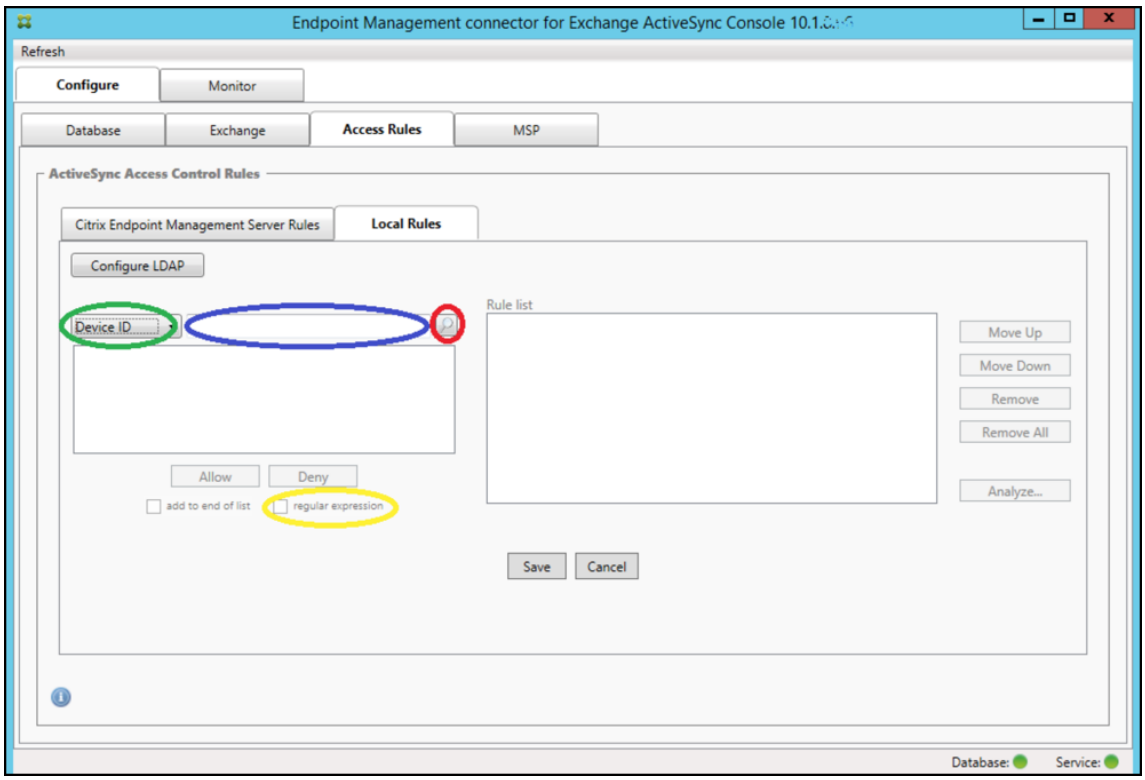
3. Seleccione el campo con el que corresponderse. En este ejemplo, se utiliza Device Type.
4. Escriba la expresión regular. En este ejemplo se usa `samsung.*`
5. Compruebe que la casilla “regular expression” está marcada y, a continuación, haga clic en **Allow** o **Deny**. En este ejemplo, se ha elegido **Allow**. El resultado final es el siguiente:



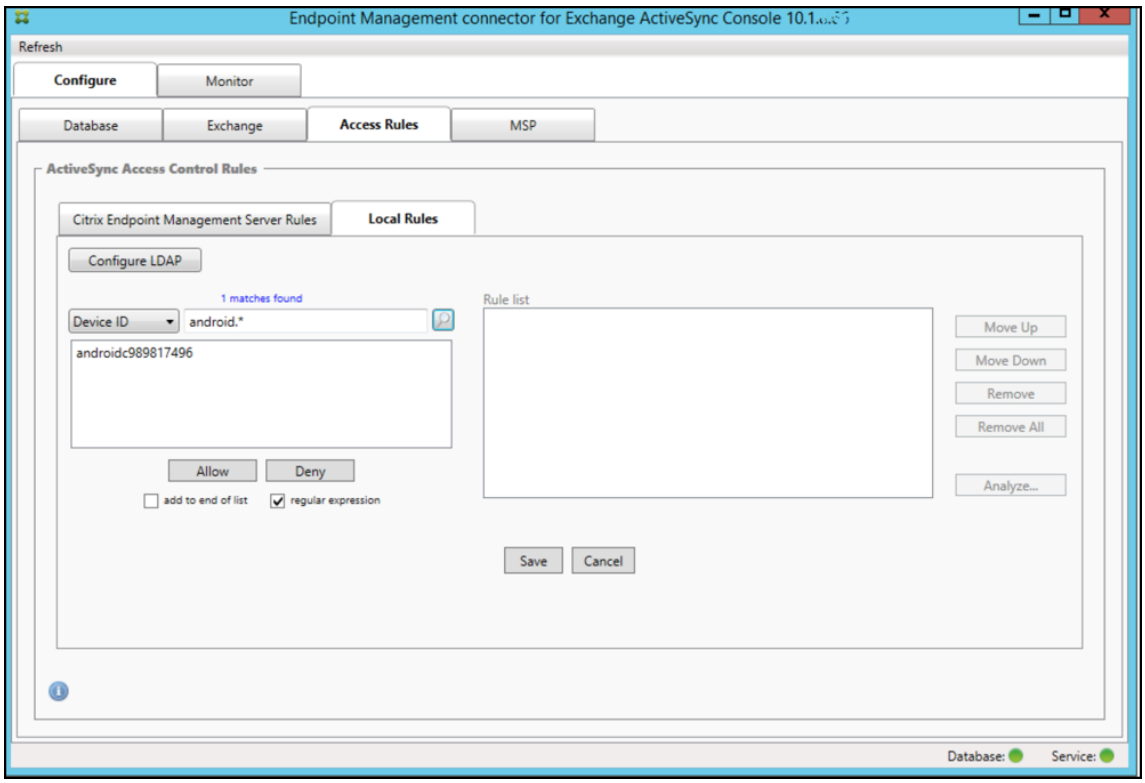
Para buscar dispositivos

Al marcar la casilla de expresión regular, 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 “regular expression” está marcada y, a continuación, haga clic en el icono de lupa para ver los resultados, tal y como se muestra en la siguiente imagen.

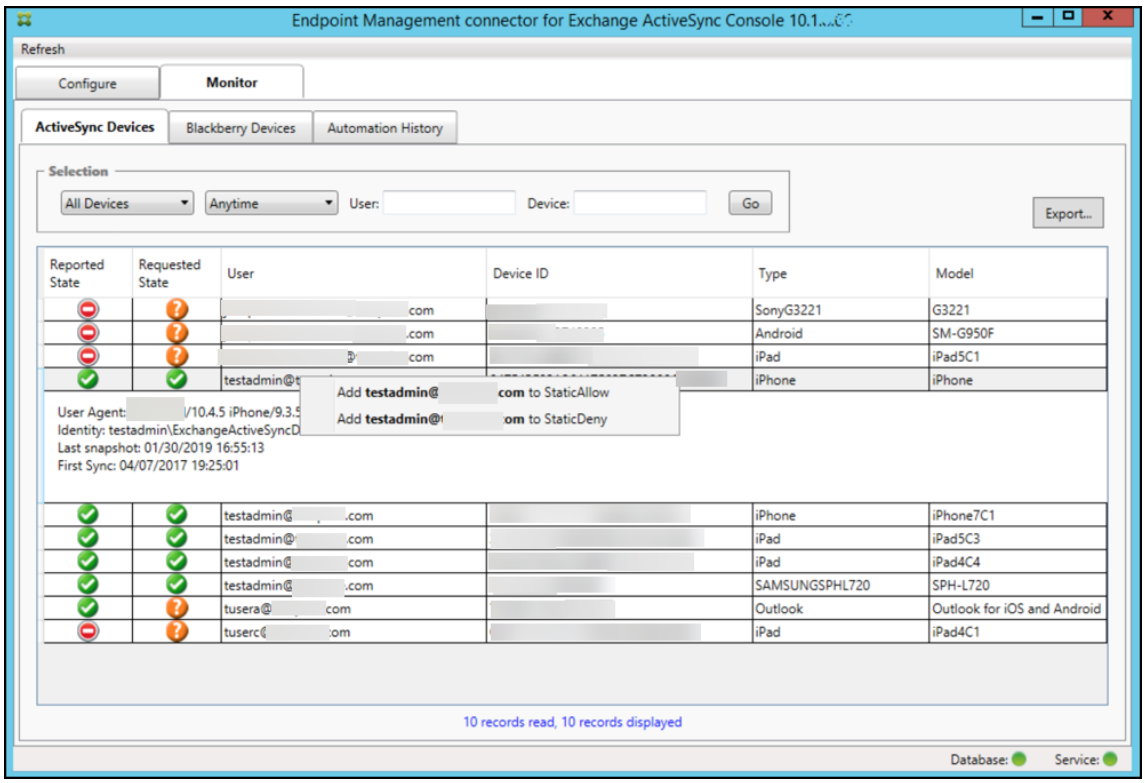


Para agregar un usuario individual, un dispositivo o un tipo de dispositivo a una regla

Puede agregar reglas estáticas basadas en el usuario, el ID de dispositivo o el tipo de dispositivo en la ficha ActiveSync Devices.

1. Haga clic en la ficha **ActiveSync Devices**.
2. En la lista, haga clic con el botón secundario en un usuario, un dispositivo o un tipo de dispositivo, y seleccione si permitir o denegar la selección.

   En la imagen siguiente, se muestra la opción de permitir o denegar cuando el usuario1 está seleccionado.



Supervisión de dispositivos

En el conector de Endpoint Management para Exchange ActiveSync, 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 hayan 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 de Exchange pertinente.
- En la ficha **MSP**, haga clic en el icono de información del servidor BlackBerry pertinente.

Solución de problemas y diagnósticos

El conector de Endpoint Management para Exchange ActiveSync registra errores y demás información operativa en el archivo de registro: *Carpeta de instalación*\log\XmmWindowsService.log. El conector de Endpoint Management para Exchange ActiveSync también registra los eventos significativos en el registro de eventos de Windows.

Para cambiar el nivel de registro

El conector de Endpoint Management para Exchange ActiveSync ofrece estos niveles de registro: error, información, advertencia, depuración y seguimiento.

> **Nota:**
>
> Cada nivel sucesivo genera más detalles (más datos). Por ejemplo, el nivel Error ofrece el menor detalle, mientras que el nivel de seguimiento proporciona el mayor detalle.

Para cambiar el nivel de registro, lleve a cabo lo siguiente:

1. En C:\Archivos de programas\Citrix\Citrix Endpoint Management connector, abra el archivo nlog.config.
2. En la sección `<rules>`, cambie el parámetro *minilevel* al nivel de registro que prefiera. Por ejemplo:

```
1      <rules>
2
3      <logger name="*" writeTo="file" minlevel="Debug" />
4
5      </rules>
6  <!--NeedCopy-->
```

3. Guarde el archivo.

   Los cambios surten efecto de inmediato. No es necesario reiniciar el conector para Exchange ActiveSync.

Errores comunes

En la lista siguiente, se incluyen errores frecuentes:

- El servicio del conector de Endpoint Management para Exchange ActiveSync 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 del conector de Endpoint Management para Exchange ActiveSync no puede acceder a 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 del conector de Endpoint Management para Exchange ActiveSync debe tener permitido el inicio de sesión en SQL. La cuenta del servicio del conector de Endpoint Management para Exchange ActiveSync 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.

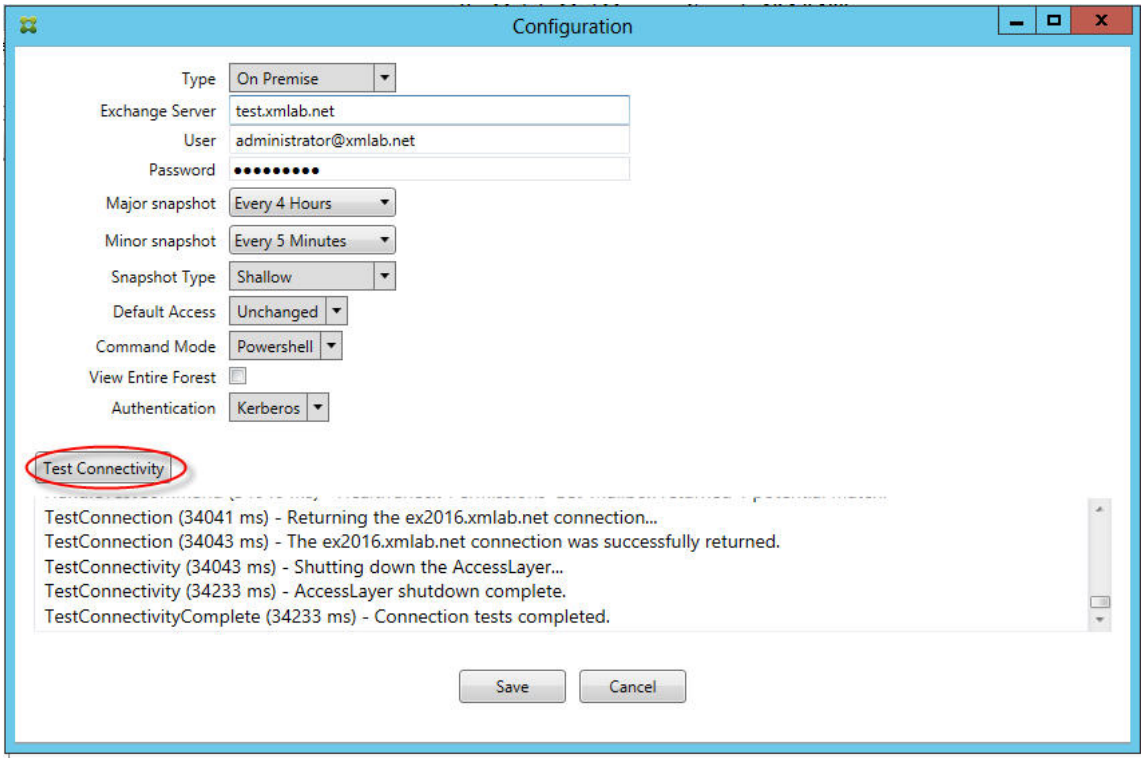
- XenMobile no puede conectarse a MSP

  Compruebe que el puerto y el transporte del servicio de MSP están correctamente configurados en la ficha **Configure > MSP** de la consola del conector de Endpoint Management para Exchange ActiveSync. 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 Cómo configurar un puerto con un certificado SSL para obtener más información sobre la instalación de certificados.

  El conector de Endpoint Management para Exchange ActiveSync incluye un programa de utilidad para probar la conectividad con el servicio de MSP. Ejecute el programa *Carpeta de instalación*\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 XenMobile Server 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).

  Cuando use **Test Connectivity**, debe tener al menos una entrada de registro de ActiveSyncDevice. De lo contrario, la prueba podría fallar.



Herramientas para solucionar 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.

Conector de Citrix Gateway para Exchange ActiveSync

January 21, 2021

XenMobile Citrix ADC Connector ahora es el conector de Citrix Gateway para Exchange ActiveSync. Para obtener más detalles sobre los productos unificados de Citrix, consulte la guía de productos de Citrix.

El conector para Exchange ActiveSync ofrece un servicio de autorización a Citrix ADC al nivel de dispositivos de los clientes de 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 el conector de Citrix Gateway para Exchange ActiveSync.

Para obtener más información, consulte ActiveSync Gateway.

Para obtener un diagrama detallado con una arquitectura como referencia, consulte Arquitectura.

La versión actual del conector de Citrix Gateway para Exchange ActiveSync es 8.5.2.

Novedades

En las siguientes secciones, se detallan las novedades de las versiones anteriores y actual del conector de Citrix Gateway para Exchange ActiveSync (anteriormente, XenMobile Citrix ADC Connector).

Novedades en la versión 8.5.3

- Esta versión funciona con los protocolos ActiveSync 16.0 y 16.1.
- Se han agregado más detalles a los análisis enviados a Google Analytics, especialmente en lo que respecta a las instantáneas. [CXM-52261]

Novedades en la versión 8.5.2

- XenMobile Citrix ADC Connector ahora es el conector de Citrix Gateway para Exchange ActiveSync.

Se han solucionado los problemas siguientes en esta versión:

- Si se usa más de un criterio para definir una regla de directiva y uno de los criterios implica el ID del usuario, si un usuario tiene más de un alias, los alias no se verifican al aplicar la regla. [CXM-55355]

> **Nota:**
>
> En la siguiente sección de novedades, se hace referencia al conector de Citrix Gateway para Exchange ActiveSync por su nombre anterior, XenMobile Citrix ADC Connector. El nombre cambió a partir de la versión 8.5.2.

Novedades en la versión 8.5.1.11

- **Cambio en los requisitos del sistema:** La versión actual de Citrix ADC Connector requiere Microsoft .NET Framework 4.5.
- **Compatibilidad con Google Analytics:** Nos gustaría saber cómo usa XenMobile Citrix ADC Connector para centrarnos en dónde mejorar el producto.

- **Disponibilidad de TLS 1.1 y 1.2:** Debido a la poca seguridad que ofrece, PCI Council ha retirado TLS 1.0. Se ha agregado la funcionalidad TLS 1.1 y 1.2 a XenMobile Citrix ADC Connector.

Supervisar el conector de Citrix Gateway para Exchange ActiveSync

La herramienta de configuración del conector de Citrix Gateway para Exchange ActiveSync ofrece un registro detallado que permite consultar todo el tráfico que pasa por el servidor Exchange que Secure Mobile Gateway permite o bloquea.

Use la ficha **Log** para ver el historial de las solicitudes de ActiveSync que ha reenviado Citrix ADC al conector de Exchange ActiveSync para la autorización.

Además, para comprobar que el servicio web del conector de Citrix Gateway para Exchange ActiveSync se está ejecutando, puede cargar esta URL en un explorador web presente en el servidor del conector: `https://<host:port>/services/ActiveSync/Version`. Si la dirección URL devuelve la versión de producto como una cadena, el servicio web funciona.

Para simular el tráfico de ActiveSync con el conector de Citrix Gateway para Exchange ActiveSync

Puede utilizar el conector de Citrix Gateway para Exchange ActiveSync para hacer una simulación del aspecto que presentaría el tráfico de ActiveSync en combinación con las directivas. En la herramienta de configuración del conector, seleccione la ficha **Simulator**. Los resultados muestran la manera en que se aplicarán las directivas en función de las reglas que haya configurado.

Seleccionar filtros para el conector de Citrix Gateway para Exchange ActiveSync

Los filtros del conector de Citrix Gateway para Exchange ActiveSync analizan un dispositivo para detectar la infracción de una directiva o un parámetro de propiedad concretos. Si el dispositivo cumple los criterios, se coloca en Device List. Esta lista de dispositivos, Device List, no es una lista de dispositivos permitidos ni bloqueados. Es una lista de los dispositivos que cumplen los criterios definidos. Los siguientes filtros están disponibles para el conector en XenMobile. Las dos opciones para cada filtro son **Permitir** o **Denegar**.

- **Dispositivos anónimos:** Permite o deniega aquellos dispositivos inscritos en XenMobile cuya identidad de usuario es desconocida. Por ejemplo, puede tratarse de un usuario que se haya inscrito, pero cuyas contraseñas de Active Directory estén caducadas, o bien un usuario que se ha inscrito con credenciales desconocidas.
- **Atestación de Samsung Knox fallida:** Los dispositivos Samsung tienen la funcionalidad de seguridad y diagnósticos. Este filtro proporciona la confirmación de que el dispositivo está configurado para Knox. Para obtener información detallada, consulte Samsung Knox.

- **Aplicaciones prohibidas:** Permite o deniega dispositivos basándose en la lista de dispositivos definida por las directivas de aplicaciones prohibidas y la presencia de esas aplicaciones.
- **Permitir / Denegar implícitamente:** Crea una lista de todos los dispositivos que no cumplen ninguno de los demás criterios de regla o filtro, y permite o deniega en función de esa lista. La opción "Permitir / Denegar implícitamente" garantiza que se habilite el estado del conector de Citrix Gateway para Exchange ActiveSync en la ficha "Dispositivos", y muestra el estado del conector para los dispositivos. La opción "Permitir / Denegar implícitamente" también controla todos los demás filtros del conector que no se han seleccionado. Por ejemplo, el conector deniega las aplicaciones bloqueadas, pero permite todos los demás filtros porque la opción "Permitir / Denegar implícitamente" está establecida en **Permitir**.
- **Dispositivos inactivos:** Crea una lista de los dispositivos que no se han comunicado con XenMobile durante un período de tiempo específico. Estos dispositivos se consideran inactivos. El filtro permite o niega esos dispositivos basándose en este filtro.
- **Aplicaciones obligatorias que faltan:** Cuando un usuario se inscribe, el usuario recibe una lista de las aplicaciones obligatorias que debe instalarse. El filtro "Aplicaciones obligatorias que faltan" indica que una o varias de esas aplicaciones ya no están presentes; por ejemplo, el usuario eliminó una o varias aplicaciones.
- **Aplicaciones no sugeridas:** Cuando un usuario se inscribe, recibe una lista de las aplicaciones que debería instalar. El filtro "Aplicaciones no sugeridas" examina el contenido del dispositivo en busca de las aplicaciones que no están en esa lista.
- **Contraseña no conforme:** Crea una lista de todos los dispositivos que no tienen código de acceso en el dispositivo.
- **Dispositivos no conformes:** Permite o deniega los dispositivos que cumplen los criterios propios del departamento interno de TI. La conformidad es un valor arbitrario definido por la propiedad de dispositivo denominada "No conforme", un marcador booleano que puede ser **true** o **false**. (Puede crear esta propiedad de forma manual y establecer su valor, o puede usar las acciones automatizadas para crear esta propiedad en un dispositivo en función de si este cumple un criterio específico.)
  - **No conforme = true**. Si el dispositivo no cumple los estándares de cumplimiento ni las definiciones de directivas establecidas por el departamento de TI, el dispositivo no cumple los requisitos.
  - **No conforme = false.** Si el dispositivo cumple los estándares de cumplimiento y las definiciones de directivas establecidas por el departamento de TI, el dispositivo cumple los requisitos.
- **Estado revocado:** Crea una lista de todos los dispositivos y permite o prohíbe dispositivos según el estado de revocación.
- **Dispositivos Android o iOS liberados por rooting o jailbreak**. Crea una lista de todos los dispositivos marcados como liberados por rooting y permite o deniega el acceso en función de ese estado.

- **Dispositivos no administrados**. Crea una lista de todos los dispositivos de la base de datos de XenMobile. Mobile Application Gateway debe implementarse en un modo de bloqueo.

Para configurar una conexión con el conector de Citrix Gateway para Exchange ActiveSync

El conector de Citrix Gateway para Exchange ActiveSync se comunica con XenMobile y otros proveedores remotos de configuración a través de servicios web seguros.

1. En la herramienta de configuración del conector, haga clic en la ficha **Config Providers** y, a continuación, haga clic en **Agregar**.
2. En el cuadro de diálogo **Config Providers**, en **Name**, escriba un nombre de usuario que tenga privilegios de administrador. Este usuario se utilizará para la autorización HTTP básica en XenMobile Server.
3. En **Url**, introduzca la dirección web del servicio GCS de XenMobile. Por norma general, en el formato: `https://<FQDN>/<instanceName>/services/<MagConfigService>`. En el nombre *MagConfigService* se distinguen mayúsculas de minúsculas.
4. En **Password**, introduzca la contraseña que se usará para la autorización básica de HTTP con XenMobile Server.
5. En **Managing Host**, escriba el nombre del servidor del conector.
6. En **Baseline Interval**, especifique un período de tiempo para la extracción, desde Device Manager, de un conjunto de reglas dinámicas actualizadas.
7. En **Delta interval**, especifique un período de tiempo para la extracción de una actualización de reglas dinámicas.
8. En **Request Timeout**, especifique el intervalo de tiempo de espera para solicitudes del servidor.
9. En **Config Provider**, seleccione si la instancia de servidor del proveedor de configuración proporciona la configuración de directivas.
10. En **Events Enabled**, habilite esta opción si quiere que el conector notifique a XenMobile cuando un dispositivo se bloquee. Se requiere esta opción si se utilizan reglas del conector en alguna de las acciones automatizadas de XenMobile.
11. Haga clic en **Save** y, a continuación, haga clic en **Test Connectivity** para probar la conectividad entre la puerta de enlace y el proveedor de configuración. Si se produce un error de conexión, compruebe que la configuración del firewall local permite la conexión o póngase en contacto con el administrador.
12. Si la conexión se realiza correctamente, desmarque la casilla **Disabled** y, a continuación, haga clic en **Save**.

Al agregar un nuevo proveedor de configuración, el conector de Citrix Gateway para Exchange ActiveSync crea automáticamente una o más directivas asociadas a ese proveedor. Estas directivas se definen mediante una plantilla contenida en config\policyTemplates.xml, en la sección NewPolicyTemplate. Se crea una nueva directiva por cada elemento de Policy definido en esta sección.

El operador puede agregar, quitar o modificar los elementos de directiva si el elemento de Policy corresponde con la definición de esquema y las cadenas de sustitución estándar (entre llaves) no se modifican. Luego, agregue nuevos grupos para el proveedor y actualice la directiva para incluir los nuevos grupos.

Para importar una directiva desde XenMobile

1. En la herramienta de configuración del conector de Citrix Gateway para Exchange ActiveSync, haga clic en la ficha **Config Providers** y, a continuación, haga clic en **Add**.
2. En el cuadro de diálogo **Config Providers**, en **Name**, escriba el nombre de usuario que se utilizará para la autorización HTTP básica en XenMobile Server y que tiene privilegios de administrador.
3. En **Url**, introduzca la dirección web del servicio Gateway Configuration Service de XenMobile. Por norma general, en el formato: `https://<xdmHost>/xdm/services/<MagConfigService>`. En el nombre MagConfigService se distinguen mayúsculas de minúsculas.
4. En **Password**, introduzca la contraseña que se usará para la autorización HTTP básica en XenMobile Server.
5. Haga clic en **Test Connectivity** para probar la conectividad entre la puerta de enlace y el proveedor de configuración. Si se produce un error de conexión, compruebe que la configuración del firewall local permite la conexión o póngase en contacto con el administrador.
6. Cuando la conexión se realice correctamente, desmarque la casilla **Disabled** y, a continuación, haga clic en **Save**.
7. En **Managing Host**, deje el nombre DNS predeterminado del equipo host local. Este parámetro se utiliza para coordinar la comunicación con XenMobile cuando hay varios servidores de Forefront Threat Management Gateway (TMG) configurados en una matriz.

   Después de guardar la configuración, abra GCS.

Configurar el modo de directiva en el conector de Citrix Gateway para Exchange ActiveSync

El conector de Citrix Gateway para Exchange ActiveSync se puede ejecutar en los seis modos siguientes:

- **Allow All**. Este modo de directiva concede acceso a todo el tráfico que pasa por el conector. No se utiliza ninguna otra regla de filtrado.
- **Deny All**. Este modo de directiva bloquea el acceso a todo el tráfico que pasa por el conector. No se utiliza ninguna otra regla de filtrado.

- **Static Rules: Block Mode** (Modo de bloqueo). Este modo de directiva ejecuta reglas estáticas con la instrucción implícita de denegar o bloquear al final. El conector bloquea aquellos dispositivos que otras reglas de filtrado no permitan.
- **Static Rules: Permit Mode** (Modo de permiso). Este modo de directiva ejecuta reglas estáticas con la instrucción implícita de permitir al final. El conector permite aquellos dispositivos que otras reglas de filtrado no bloqueen o denieguen.
- **Static + ZDM Rules: Block Mode** (Modo de bloqueo). Este modo de directiva ejecuta primero las reglas estáticas, seguidas de las reglas dinámicas de XenMobile con una instrucción implícita de denegar o bloquear al final. Los dispositivos se permiten o deniegan según los filtros definidos y las reglas de Device Manager. Los dispositivos que no coincidan con las reglas y los filtros definidos se bloquean.
- **Static + ZDM Rules: Permit Mode** (Modo de permiso). Este modo de directiva ejecuta primero las reglas estáticas, seguidas de las reglas dinámicas de XenMobile con una instrucción implícita de permitir al final. Los dispositivos se permiten o deniegan en función de los filtros definidos y las reglas de XenMobile. Los dispositivos que no coincidan con las reglas y los filtros definidos se permiten.

El proceso del conector de Citrix Gateway para Exchange ActiveSync permite o bloquea reglas dinámicas en función de identificadores únicos de ActiveSync para dispositivos iOS y dispositivos móviles de Windows recibidos desde XenMobile. El comportamiento de los dispositivos Android difiere según el fabricante y algunos no exponen con facilidad un ID único de ActiveSync. Para compensar, XenMobile envía información de ID del usuario de los dispositivos Android para la decisión de permitir o bloquear. Como resultado, si un usuario tiene un solo dispositivo Android, las acciones de permitir y bloquear funcionan de la manera habitual. En cambio, si el usuario dispone de varios dispositivos Android, se permiten todos los dispositivos porque los dispositivos Android no se pueden diferenciar. Puede configurar la puerta de enlace para bloquear estáticamente esos dispositivos en función de su ActiveSyncID, si este se conoce. Esta puerta también se puede configurar para bloquear según el tipo de dispositivo o el agente de usuario.

Para especificar el modo de directiva, en la herramienta de configuración del controlador SMG, realice lo siguiente:

1. Haga clic en la ficha **Path Filters** y, a continuación, haga clic en **Add**.
2. En el cuadro de diálogo **Path Properties**, seleccione un modo de directiva de la lista **Policy** y, a continuación, haga clic en **Save**.

Puede revisar las reglas en la ficha **Policies** de la herramienta de configuración. Las reglas se procesan en el conector de Citrix Gateway para Exchange ActiveSync de arriba abajo. Las directivas permitidas (Allow) se muestran con una marca de verificación verde. Las directivas denegadas (Deny) se muestran con un círculo rojo atravesado por una línea. Para actualizar la pantalla y ver las reglas actualizadas, haga clic en **Refresh**. También puede modificar el orden de las reglas en el archivo config.xml.

Para probar las reglas, haga clic en la ficha **Simulator**. Especifique los valores de los campos. Es-

tos también se pueden obtener a partir de los registros. Aparecerá un mensaje de resultados con la especificación Allow o Block.

Para configurar reglas estáticas

Introduzca reglas estáticas con valores que lean los filtros ISAPI de las solicitudes HTTP de conexión ActiveSync. Con las reglas estáticas, el conector de Citrix Gateway para Exchange ActiveSync puede permitir o bloquear el tráfico mediante los criterios siguientes:

- **User**. El conector de Citrix Gateway para Exchange ActiveSync usa la estructura del nombre y el valor del usuario autorizado capturado durante la inscripción del dispositivo. Generalmente, se encuentra como dominio\nombre_de_usuario, como consta en el servidor que ejecuta XenMobile conectado a Active Directory a través de LDAP. La ficha **Log** que contiene la herramienta de configuración del conector mostrará los valores que pasen a través de este. Los valores pasan si la estructura de esos valores es diferente o debe determinarse.
- **Deviceid (ActiveSyncID)**. También conocido como ActiveSyncID del dispositivo conectado. Este valor se suele encontrar en la página de propiedades del dispositivo específico, en la consola de XenMobile. Este valor también se puede consultar desde la ficha Log, en la herramienta de configuración del conector.
- **DeviceType**. El conector puede determinar si el dispositivo es un iPhone, un iPad, o cualquier otro tipo de dispositivo; puede permitirlos o bloquearlos basándose en esos criterios. En cuanto a otros valores, la herramienta de configuración del conector puede revelar todos los tipos de dispositivos conectados que se están procesando para la conexión ActiveSync.
- **UserAgent**. Contiene información sobre el cliente de ActiveSync que se utiliza. En la mayoría de los casos, el valor especificado corresponde a una versión y compilación determinadas de sistema operativo para la plataforma del dispositivo móvil.

La herramienta de configuración del conector que se ejecuta en el servidor siempre administra las reglas estáticas.

1. En la herramienta de configuración del controlador SMG, haga clic en la ficha **Static Rules** y, a continuación, haga clic en **Add**.
2. En el cuadro de diálogo **Static Rule Properties**, especifique los valores a usar como criterios. Por ejemplo, puede indicar un usuario al que permitir el acceso si escribe el nombre del usuario (por ejemplo, AllowedUser) y si, a continuación, desmarca la casilla **Disabled**.
3. Haga clic en **Guardar**.

   La regla estática está ahora activada. Además, puede usar expresiones regulares para definir los valores, pero debe habilitar el modo de procesamiento de reglas en el archivo config.xml.

Para configurar reglas dinámicas

En XenMobile, las directivas y las propiedades de dispositivo definen las reglas dinámicas y pueden activar un filtro dinámico del conector de Citrix Gateway para Exchange ActiveSync. La activación ocurre en caso de infracción de una directiva o un parámetro de propiedad. Los filtros del conector analizan un dispositivo para detectar la infracción de una directiva concreta o un parámetro de propiedad. Si el dispositivo cumple los criterios, se coloca en Device List. Esta lista Device List no es una lista de dispositivos permitidos ni bloqueados. Es una lista de los dispositivos que cumplen los criterios definidos. Con las siguientes opciones de configuración, puede definir si quiere permitir o denegar los dispositivos de Device List mediante el conector.

> **Nota:**
>
> Debe usar la consola de XenMobile para configurar las reglas dinámicas.

1. En la consola de XenMobile, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Servidor**, haga clic en **ActiveSync Gateway**. Aparecerá la página ActiveSync Gateway.
3. En **Activar las reglas siguientes**, seleccione las reglas que quiera activar.
4. En "Solo Android", haga clic en **Sí** en **Enviar usuarios de dominio Android a ActiveSync Gateway** para que XenMobile envíe información de dispositivos Android a Secure Mobile Gateway.

   Si esta opción está habilitada, XenMobile envía información de dispositivos Android al conector de Citrix Gateway para Exchange ActiveSync en el caso de que XenMobile no disponga del identificador de ActiveSync correspondiente al usuario del dispositivo Android.

Para configurar directivas personalizadas con la edición del archivo XML del conector de Citrix Gateway para Exchange ActiveSync

En la herramienta de configuración del conector de Citrix Gateway para Exchange ActiveSync, puede ver las directivas básicas en la configuración predeterminada de la ficha **Policies**. Si quiere crear directivas personalizadas, puede modificar el archivo de configuración XML del conector (config\config.xml).

1. Busque la sección **PolicyList** en el archivo y, a continuación, agregue un nuevo elemento **Policy**.
2. Si también se requiere un nuevo grupo (por ejemplo, otro grupo estático un grupo para admitir otro proveedor GCP), agregue el nuevo elemento **Group** a la sección **GroupList**.
3. Si quiere, puede cambiar el orden de los grupos dentro de una directiva existente. Para ello, reorganice los elementos de **GroupRef**.

Configurar el archivo XML del conector de Citrix Gateway para Exchange ActiveSync

El conector de Citrix Gateway para Exchange ActiveSync utiliza un archivo de configuración XML para dictar las acciones del conector. Entre otras entradas, en el archivo se especifica el grupo de archivos y las acciones asociadas que el filtro tendrá en cuenta y realizará al evaluar solicitudes HTTP. De forma predeterminada, el archivo se denomina config.xml y se encuentra en la siguiente ubicación: ..\Archivos de programa\Citrix\XenMobile Citrix ADC Connector\config.

Nodos GroupRef

Los nodos de GroupRef definen los nombres de los grupos lógicos. Los valores predeterminados son AllowGroup y DenyGroup.

> **Nota:**
>
> Es importante el orden de aparición de los nodos GroupRef en el nodo GroupRefList.

El valor de ID de un nodo GroupRef identifica un contenedor lógico o una colección de miembros, que se utilizan para hacer coincidir dispositivos o cuentas de usuario específicos. Los atributos de la acción especifican cómo tratará el filtro a un miembro que coincida con una regla de la colección. Por ejemplo, un dispositivo o cuenta de usuario que coincida con una regla del conjunto AllowGroup podrá "pasar". En este caso, "pasar" significa que se le permitirá acceder a Exchange CAS. En cambio, un dispositivo o cuenta de usuario que coincida con una regla del conjunto DenyGroup será "rechazada". En este caso, "rechazar" significa que no se le permitirá acceder a Exchange CAS.

Cuando un dispositivo o una cuenta de usuario determinados, o bien una combinación, cumplen las reglas de ambos grupos, se usa una convención de precedencia para dirigir el resultado de la solicitud. La precedencia se expresa en el orden de los nodos GroupRef en el archivo config.xml de arriba a abajo. Los nodos GroupRef están clasificados por orden de prioridad. Las reglas de una condición determinada del grupo Allow (Permitir) siempre prevalecerán sobre las reglas de la misma condición en el grupo Deny (Denegar).

Nodos Group

Además, el archivo config.xml define los nodos Group. Estos nodos enlazan los contenedores lógicos AllowGroup y DenyGroup a archivos XML. Las entradas almacenadas en los archivos externos forman la base de las reglas de filtrado.

> **Nota:**
>
> En esta versión, solo se admiten los archivos XML externos.

La instalación predeterminada implementa dos archivos XML en la configuración: allow.xml y deny.xml.

Configurar el conector de Citrix Gateway para Exchange ActiveSync

Puede configurar el conector de Citrix Gateway para Exchange ActiveSync de modo que este conector bloquee o permita solicitudes de ActiveSync de forma selectiva, en función de las propiedades **Active Sync Service ID**, **Device type**, **User Agent** (sistema operativo del dispositivo), **Authorized user** y **ActiveSync Command**.

La configuración predeterminada admite una combinación de grupos estáticos y dinámicos. Debe mantener grupos estáticos mediante la herramienta de configuración del controlador SMG. Los grupos estáticos pueden constar solo de las categorías conocidas de los dispositivos, como, por ejemplo, todos los dispositivos con un agente determinado de usuario.

Una fuente externa, llamada Gateway Configuration Provider (Proveedor de configuración de la puerta de enlace) mantiene los grupos dinámicos. El conector de Citrix Gateway para Exchange ActiveSync conecta los grupos de forma periódica. Con XenMobile, puede exportar grupos de dispositivos y usuarios permitidos y bloqueados al conector.

Los grupos dinámicos se mantienen mediante un recurso externo llamado Gateway Configuration Provider (proveedor de configuración de puerta de enlace). El conector de Citrix Gateway para Exchange ActiveSync recopila esos grupos de forma periódica. Con XenMobile, puede exportar grupos de dispositivos y usuarios permitidos y bloqueados al conector.

Una directiva es una lista ordenada de grupos, donde cada grupo tiene asociada una acción (permitir o bloquear), además de una lista de los miembros del grupo. Una directiva puede tener una cantidad infinita de grupos. El orden de los grupos en una directiva es importante porque, cuando se encuentra una coincidencia, se realiza la acción del grupo, y los demás grupos no se evalúan.

Un miembro define la manera de coincidir con las propiedades de una solicitud. Se puede coincidir con una sola propiedad, como ID de dispositivo, o con varias propiedades, como el tipo de dispositivo y el agente de usuario.

Seleccionar un modelo de seguridad para el conector de Citrix Gateway para Exchange ActiveSync

Establecer un modelo de seguridad es esencial para una buena implementación de dispositivos móviles en organizaciones de cualquier tamaño. Es frecuente utilizar un control de red protegida o en cuarentena para permitir el acceso a un usuario, un equipo o un dispositivo de forma predeterminada. Sin embargo, esta práctica no es siempre la más adecuada. Cada organización que administra la seguridad de TI puede tener un enfoque diferente o adaptado a la seguridad de los dispositivos móviles.

La misma lógica se aplica a la seguridad de los dispositivos móviles. Utilizar un modelo permisivo es una mala elección debido a la gran cantidad de: dispositivos móviles y sus tipos, dispositivos móviles

por usuario, así como aplicaciones y plataformas de sistemas operativos disponibles. En la mayoría de las organizaciones, el modelo restrictivo sería la elección más lógica.

Tipos de configuración que permite Citrix para integrar el conector de Citrix Gateway para Exchange ActiveSync en XenMobile:

Modelo permisivo (Permit mode)

El modelo de seguridad permisivo estipula que, de forma predeterminada, se permite o se concede acceso a todo. Solo se bloqueará el acceso a algo y se aplicará una restricción si existen reglas y filtros. El modelo de seguridad permisivo es una buena opción para organizaciones con un criterio de seguridad de dispositivos móviles relativamente laxo. Ese modelo solo aplica controles restrictivos para denegar el acceso cuando corresponda (si falla una regla de directiva).

Modelo restrictivo (Block Mode)

El modelo de seguridad restrictivo estipula que, de forma predeterminada, no se permite o no se concede acceso a nada. Todo lo que pasa por el punto de control de seguridad se filtra y se comprueba; se le deniega el acceso a menos que las reglas de acceso lo permitan. El modelo de seguridad restrictivo es una buena opción para organizaciones con un criterio de seguridad de dispositivos móviles relativamente estricto. Este modo solo concede acceso para uso y funciones con los servicios de red cuando todas las reglas de acceso lo permitan.

Administrar el conector de Citrix Gateway para Exchange ActiveSync

Puede utilizar el conector de Citrix Gateway para Exchange ActiveSync para crear reglas de control de acceso. Las reglas permiten o bloquean el acceso a las solicitudes de conexión de ActiveSync provenientes de los dispositivos administrados. El acceso se concede en función del estado del dispositivo, las aplicaciones permitidas o prohibidas u otras condiciones de cumplimiento.

Con la herramienta de configuración del conector de Citrix Gateway para Exchange ActiveSync, puede generar reglas dinámicas y estáticas que apliquen directivas de correo electrónico de empresa, por lo que podrá bloquear a los usuarios que infrinjan las normas. También puede configurar el cifrado de datos adjuntos de correo electrónico, de modo que todos esos datos que pasen a través del servidor Exchange hacia los dispositivos administrados se cifren y solo se puedan ver en dispositivos administrados por usuarios autorizados.

Para desinstalar el conector de Citrix Gateway para Exchange ActiveSync

1. Ejecute XncInstaller.exe con una cuenta de administrador.
2. Siga las instrucciones que aparecen en la pantalla para completar la desinstalación.

Para instalar, actualizar o desinstalar el conector de Citrix Gateway para Exchange ActiveSync

1. Ejecute XncInstaller.exe con una cuenta de administrador para instalar el conector o para permitir la actualización o la eliminación de un conector existente.
2. Siga las instrucciones en pantalla para completar la instalación, la actualización o la desinstalación.

Después de instalar el conector, debe reiniciar manualmente el servicio de notificación y el servicio de configuración de XenMobile.

Instalar el conector de Citrix Gateway para Exchange ActiveSync

El conector de Citrix Gateway para Exchange ActiveSync se instala en su propio servidor Windows.

La carga de la CPU que pone el conector en un servidor depende de la cantidad de dispositivos administrados. En caso de una gran cantidad de dispositivos (más de 50 000), puede que necesite aprovisionar más de un núcleo si no dispone de un entorno en clústeres. La superficie de memoria del conector no es lo suficientemente significativa como para garantizar una memoria adicional.

Requisitos del sistema para el conector de Citrix Gateway para Exchange ActiveSync

El conector de Citrix Gateway para Exchange ActiveSync se comunica con Citrix ADC a través de un puente SSL configurado en el dispositivo Citrix ADC. Ese puente permite al dispositivo pasar todo el tráfico seguro directamente a XenMobile. El conector requiere la siguiente configuración mínima de sistema:

Componente	Requisito
Equipo y procesador	Procesador Pentium III de 733 MHz o más. Procesador Pentium III de 2,0 GHz o más (recomendado)
Citrix ADC	Dispositivo Citrix ADC con la versión 10 del software
Memoria	1 GB
Disco duro	Partición local con formato NTFS, con 150 MB de espacio disponible en disco duro
Sistema operativo	Windows Server 2016, Windows Server 2012 R2 o Windows Server 2008 R2 Service Pack 1. Debe ser un servidor en inglés. Windows Server 2008 R2 Service Pack 1 dejará de ser compatible el 14 de enero de 2020.

Componente	Requisito
Otros dispositivos	Un adaptador de red compatible con el sistema operativo del host para la comunicación con la red interna
Microsoft .NET Framework	La versión 8.5.1.11 requiere Microsoft .NET Framework 4.5.
Visualización	Monitor VGA o de mayor resolución

El equipo host del conector de Citrix Gateway para Exchange ActiveSync requiere el siguiente espacio mínimo disponible en el disco duro:

- **Aplicación:** De 10 a 15 MB (se recomienda 100 MB)
- **Captura de registros:** 1 GB (se recomienda 20 GB)

Para obtener más información acerca de la compatibilidad de plataformas con el conector de Citrix Gateway para Exchange ActiveSync, consulte Sistemas operativos compatibles.

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 el conector de Citrix Gateway para Exchange ActiveSync 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 Samsung
- Cliente de correo electrónico nativo de iOS

Implementar el conector de Citrix Gateway para Exchange ActiveSync

El conector de Citrix Gateway para Exchange ActiveSync permite utilizar Citrix ADC para redirigir mediante proxy y equilibrar la carga de la comunicación entre XenMobile Server y los dispositivos administrados de XenMobile. El conector se comunica de forma periódica con XenMobile para sincronizar las directivas. El conector y XenMobile se pueden agrupar en clústeres (ya sea en un mismo clúster o en clústeres diferentes), y Citrix ADC puede equilibrar su carga.

Componentes del conector de Citrix Gateway para Exchange ActiveSync

- **Servicio del conector de Citrix Gateway para Exchange ActiveSync:** Este servicio ofrece una interfaz de servicio web REST que se puede invocar mediante Citrix ADC para determinar si se

autoriza una solicitud de ActiveSync desde un dispositivo.

- **Servicio de configuración de XenMobile:** Este servicio se comunica con XenMobile para sincronizar los cambios de las directivas de XenMobile con el conector.
- **Servicio de notificaciones de XenMobile:** Este servicio envía notificaciones a XenMobile acerca de accesos de dispositivos no autorizados. De esta forma, XenMobile puede tomar las medidas adecuadas, como notificar al usuario el motivo del bloqueo del dispositivo.
- **Herramienta de configuración del conector de Citrix Gateway para Exchange ActiveSync:** Esta aplicación permite al administrador configurar y supervisar el conector.

Para configurar las direcciones de escucha del conector de Citrix Gateway para Exchange ActiveSync

Para que el conector de Citrix Gateway para Exchange ActiveSync reciba solicitudes desde Citrix ADC para autorizar el tráfico de ActiveSync, debe: Especificar el puerto en el que el conector escucha las llamadas al servicio web de Citrix ADC.

1. En el menú **Inicio**, seleccione la herramienta de configuración del conector de Citrix Gateway para Exchange ActiveSync.
2. Haga clic en la ficha **Web Service** y, a continuación, escriba las direcciones de escucha para el servicio web del conector. Puede seleccionar **HTTP**, **HTTPS** o ambos. Si el conector y XenMobile están instalados en el mismo servidor, seleccione puertos que no entren en conflicto con XenMobile.
3. Después de configurar los valores, haga clic en **Save** y, a continuación, haga clic en **Start Service** para iniciar el servicio web.

Para configurar las directivas de control de acceso del dispositivo en el conector de Citrix Gateway para Exchange ActiveSync

Para configurar la directiva de control de acceso que quiere aplicar a los dispositivos administrados, haga lo siguiente:

1. En la herramienta de configuración del conector de Citrix Gateway para Exchange ActiveSync, haga clic en la ficha **Path Filters**.
2. Seleccione la primera fila **Microsoft-Server-ActiveSync is for ActiveSync** y, a continuación, haga clic en **Edit**.
3. En la lista **Policy**, seleccione la directiva pertinente. Para una directiva que incluya las directivas de XenMobile, seleccione **Static + ZDM: Permit Mode o Static + ZDM: Block Mode**. Estas directivas combinan reglas locales (o estáticas) con las reglas de XenMobile. El modo Permit Mode significa que se permite el acceso a ActiveSync por parte de todos los dispositivos no identificados específicamente mediante reglas. En cambio, el modo Block Mode significa que todos esos dispositivos serán bloqueados.

4. Después de establecer las directivas, haga clic en **Save**.

Para configurar la comunicación con XenMobile

Especifique el nombre y las propiedades de XenMobile Server (también llamado Config Provider) que quiere utilizar con el conector de Citrix Gateway para Exchange ActiveSync y Citrix ADC.

> **Nota:**
>
> En esta tarea, se presupone que XenMobile ya está instalado y configurado.

1. En la herramienta de configuración del conector de Citrix Gateway para Exchange ActiveSync, haga clic en la ficha **Config Providers** y, a continuación, haga clic en **Add**.
2. Indique el nombre y la dirección URL del servidor de XenMobile Server utilizado en esta implementación. Si dispone de varios XenMobile Servers implementados en una implementación multiarrendatario, este nombre debe ser único para cada instancia de servidor. Por ejemplo, en **Name**, podría escribir **XMS**.
3. En **Url**, introduzca la dirección web de GlobalConfig Provider (GCP) de XenMobile. Por norma general, en el formato: `https://<FQDN>/<instanceName>/services/<MagConfigService>`. En el nombre *MagConfigService* se distinguen mayúsculas de minúsculas.
4. En **Password**, introduzca la contraseña que se usará para la autorización básica de HTTP con el servidor web de XenMobile.
5. En **Managing Host**, introduzca el nombre del servidor donde se instaló el conector de Citrix Gateway para Exchange ActiveSync.
6. En **Baseline Interval**, especifique un período de tiempo para la extracción, desde XenMobile, de un conjunto de reglas dinámicas actualizadas.
7. En **Request Timeout**, especifique el intervalo de tiempo de espera para solicitudes del servidor.
8. En **Config Provider**, seleccione si la instancia de servidor de Config Provider proporciona la configuración de directivas.
9. Habilite la opción **Events Enabled** si quiere que Secure Mobile Gateway notifique a XenMobile cuando se bloquee un dispositivo. Se requiere esta opción si se utilizan reglas de Secure Mobile Gateway en alguna de las acciones automatizadas de Device Manager.
10. Una vez configurado el servidor, haga clic en **Test Connectivity** para comprobar la conexión con XenMobile.
11. Cuando se haya establecido la conectividad, haga clic en **Save**.

Implementar el conector de Citrix Gateway para Exchange ActiveSync para la redundancia y la escalabilidad

Si quiere ampliar la implementación del conector de Citrix Gateway para Exchange ActiveSync y XenMobile, puede instalar instancias del conector en varios servidores Windows que señalen a la misma

instancia de XenMobile y, a continuación, puede utilizar Citrix ADC para equilibrar la carga de los servidores.

La configuración del conector de Citrix Gateway para Exchange ActiveSync cuenta con dos modos:

- En el modo no compartido (non-shared mode), cada instancia del conector de Citrix Gateway para Exchange ActiveSync se comunica con XenMobile Server y mantiene su propia copia privada de la directiva resultante. Por ejemplo, si tiene un clúster de XenMobile Servers, puede ejecutar una instancia del conector en cada XenMobile Server, y el conector obtendría las directivas desde la instancia local de XenMobile.
- En modo compartido (shared mode), un nodo del conector se designa como el nodo principal y se comunica con XenMobile. La configuración resultante se comparte entre los demás nodos, ya sea mediante una replicación de Windows o un recurso compartido de red Windows (o de terceros).

Toda la configuración del conector se encuentra en una carpeta (de varios archivos XML). El proceso del conector detecta los cambios en los archivos de esta carpeta y vuelve a cargar automáticamente la configuración. No hay ninguna conmutación por error para el nodo principal en el modo compartido. Sin embargo, el sistema puede tolerar que el servidor principal esté inactivo durante unos minutos (por ejemplo, para reiniciarse) porque la última configuración válida conocida se almacena en caché en el proceso del conector.

Conceptos avanzados

January 4, 2022

> **Nota:**
>
> Este artículo contiene conceptos avanzados para XenMobile Server. Para obtener información exhaustiva sobre Citrix Endpoint Management, consulte Conceptos avanzados.

Los artículos de Conceptos avanzados de XenMobile ofrecen una visión más profundizada de la documentación del producto de XenMobile. El objetivo es ayudar a reducir el tiempo empleado en implementarlo, a través de técnicas de experto. Los expertos que hayan escrito el contenido pueden citarse en los artículos.

Para ver puntos a decidir, recomendaciones, preguntas frecuentes y casos de uso de un entorno XenMobile de extremo a extremo, consulte el manual de implementación de XenMobile en esta sección.

Para buscar asistencia técnica en los foros de la comunidad de XenMobile, consulte Citrix Discussions.

Interacción del XenMobile instalado localmente con Active Directory

January 4, 2022

Por Siddartha Vuppala

En este artículo, se explica la interacción entre XenMobile Server y Active Directory. XenMobile Server interactúa con Active Directory tanto en línea como en segundo plano. En las siguientes secciones, se ofrece más información sobre las operaciones en línea y en segundo plano que implican la interacción con Active Directory.

> **Nota:**
>
> Este artículo es una descripción general de la interacción, no es una explicación detallada. Para obtener más información sobre la configuración de Active Directory y LDAP en la consola de XenMobile, consulte Autenticación de dominio o dominio y token de seguridad.

Interacciones en línea

XenMobile Server se comunica con Active Directory a través de los parámetros de LDAP que define un administrador. Los parámetros recuperan información sobre usuarios y grupos. A continuación, dispone de las operaciones que resultan de la interacción entre XenMobile Server y Active Directory.

1. **Configuración de LDAP.** La configuración de Active Directory en sí resulta en una interacción con Active Directory. XenMobile Server intenta validar la información cotejándola con Active Directory. El servidor lo logra mediante el protocolo de Internet, el puerto y las credenciales suministradas de cuenta de servicio. Una comunicación satisfactoria indica que la conexión se ha configurado correctamente.
2. **Interacciones basadas en grupos**.
    a) Buscar uno o varios grupos durante la creación del control de acceso basado en roles (RBAC) y la definición de grupos de entrega. El administrador de XenMobile Server introduce una cadena de texto de búsqueda en la consola de XenMobile. XenMobile Server busca todos los grupos que contienen la subcadena indicada en el dominio seleccionado. A continuación, XenMobile Server recupera los atributos objectGUID, sAMAccountName y nombre distintivo de los grupos identificados en la búsqueda.

        > **Nota:**
        >
        > Esta información no se almacena en la base de datos de XenMobile Server.

    b) Agregar o actualizar RBAC y la definición del grupo de implementación. El administrador de XenMobile Server selecciona los grupos de interés de Active Directory en función de

la búsqueda anterior y los incluye en la definición del grupo de implementación. XenMobile Server busca el grupo específico, uno por uno, en Active Directory. XenMobile Server busca el atributo objectGUID y recupera los atributos seleccionados, incluida la información de pertenencia a grupos. La información de miembros del grupo ayuda a determinar la pertenencia entre el grupo recuperado y los usuarios o grupos existentes en la base de datos de XenMobile Server. Realizar cambios en la pertenencia a grupos genera una derivación del RBAC y el grupo de implementación para los usuarios miembros afectados, lo que resulta en derechos de usuario.

> **Nota:**
>
> Realizar cambios en la definición del grupo de implementación puede generar cambios en los derechos de aplicaciones o directivas para los usuarios afectados.

c) **Invitaciones de PIN de un solo uso (OTP)**. El administrador de XenMobile Server selecciona un grupo de la lista de grupos de Active Directory presentes en la base de datos de XenMobile Server. Para este grupo, todos los usuarios, tanto directos como indirectos, se recuperan de Active Directory. Las invitaciones OTP se envían a los usuarios que se identificaron en el paso anterior.

> **Nota:**
>
> Las tres interacciones mencionadas implican que las interacciones basadas en grupos se desencadenan en función de los cambios de configuración de XenMobile Server. Cuando no hay cambios en la configuración, las interacciones implican que no hay interacciones con Active Directory. También implican que no hay ningún requisito para que los trabajos en segundo plano capturen el lado grupal de los cambios de forma periódica.

3. **Interacción basada en el usuario**.

a) Autenticación de usuario. El flujo de trabajo de autenticación de un usuario conlleva dos interacciones con Active Directory:

- Se usa para autenticar al usuario con las credenciales proporcionadas.
- Agregar o actualizar atributos específicos de usuario en la base de datos de XenMobile Server, incluidos objectGUID, el nombre distintivo, sAMAccountName y pertenencia directa a grupos. Los cambios en la pertenencia a grupos generan una reevaluación de los derechos que tengan los miembros de grupo a la aplicación, la directiva y el acceso.

El usuario puede autenticarse desde el dispositivo o desde la consola de XenMobile Server. En ambos casos, la interacción con Active Directory tiene el mismo comportamiento.

b) Acceso y actualización de la tienda de aplicaciones. Una actualización de la tienda da como resultado una actualización de los atributos del usuario, incluida su pertenencia

directa al grupo. Esta acción permite una reevaluación de los derechos del usuario.

c) Comprobaciones del dispositivo. Los administradores pueden configurar en la consola de XenMobile una comprobación periódica del dispositivo. Cada vez que se comprueba un dispositivo, los atributos de usuario correspondientes se actualizan, incluida la pertenencia directa al grupo. Esas comprobaciones permiten una reevaluación de los derechos del usuario.

d) Invitaciones OTP por grupo. El administrador de XenMobile Server selecciona un grupo de la lista de grupos de Active Directory presentes en la base de datos de XenMobile Server. Los usuarios miembros, directos e indirectos (por anidamiento), se obtienen de Active Directory y se guardan en la base de datos de XenMobile Server. Las invitaciones OTP se envían a los usuarios miembros que se identificaron en el paso anterior.

e) Invitaciones OTP por usuario. El administrador introduce una cadena de texto de búsqueda en la consola de XenMobile. XenMobile Server consulta Active Directory y devuelve registros de usuario que coinciden con la cadena de texto de entrada. El administrador selecciona al usuario para enviarle la invitación OTP. XenMobile Server obtiene la información de usuario de Active Directory y actualiza los mismos datos en la base de datos antes de enviar la invitación al usuario.

Interacciones en segundo plano

Una conclusión de la comunicación en línea con Active Directory es que las interacciones basadas en grupos se activan al seleccionar cambios en la configuración de XenMobile Server. Cuando no hay cambios en la configuración, no hay interacciones con Active Directory para grupos.

Esta interacción requiere trabajos en segundo plano que se sincronicen periódicamente con Active Directory y actualicen los cambios relevantes en los grupos pertinentes.

A continuación, dispone de los trabajos en segundo plano que interactúan con Active Directory.

1. **Trabajo de sincronización de grupos**. El objetivo de este trabajo es consultar a Active Directory, un grupo a la vez, sobre grupos relevantes para cambios en los atributos de nombre distintivo o sAMAccountName. La consulta de búsqueda en Active Directory usa el atributo objectGUID del grupo relevante para obtener los valores actuales de los atributos de nombre distintivo y sAMAccountName. Los cambios en los valores de nombre distintivo o sAMAccountName de los grupos relevantes se actualizan en la base de datos.

   > **Nota:**
   >
   > Este trabajo no actualiza la información de pertenencia del usuario al grupo.

2. **Trabajo de sincronización de grupos anidados**. Este trabajo actualiza los cambios en la jerarquía de anidamiento de los grupos relevantes. XenMobile Server permite que los miembros

directos e indirectos de un grupo relevante obtengan derechos. La pertenencia directa de los usuarios se actualiza durante las interacciones en línea basadas en el usuario. En segundo plano, este trabajo rastrea las pertenencias indirectas. La pertenencia indirecta es cuando un usuario es miembro de un grupo que es miembro, a su vez, de un grupo relevante.

Este trabajo recopila la lista de grupos de Active Directory desde la base de datos de XenMobile Server. Esos grupos forman parte de la definición del grupo de implementación o de la definición de RBAC. Para cada grupo en esta lista, XenMobile Server obtiene los miembros del grupo. Los miembros de un grupo son una lista de nombres distintivos que representan usuarios y grupos. XenMobile Server realiza otra consulta a Active Directory para obtener solo los usuarios del grupo relevante. La diferencia entre las dos listas ofrece solo los miembros del grupo relevante. Los cambios en los grupos de miembros se actualizan a la base de datos. Se repite el mismo proceso para todos los grupos de la jerarquía.

Los cambios en el anidamiento provocan el procesamiento de los usuarios afectados para los cambios de derechos.

3. **Verificación de usuario inhabilitado**. Este trabajo solo se ejecuta cuando el administrador de XenMobile crea una acción para verificar si hay usuarios inhabilitados. El trabajo se ejecuta dentro del ámbito de un trabajo de sincronización de grupos. El trabajo consulta a Active Directory para comprobar el estado inhabilitado de los usuarios relevantes, un usuario a la vez.

Preguntas frecuentes

¿Con qué frecuencia predeterminada se ejecutan los trabajos en segundo plano?

- Los trabajos de sincronización de grupos se ejecutan cada cinco horas a partir de las 02:00 (hora local).
- Los trabajos de sincronización de los grupos anidados se ejecutan una vez al día a medianoche (hora local).

¿Para qué se necesita un trabajo de sincronización de grupos?

- El atributo memberOf de un registro de usuario en Active Directory presenta una lista de los grupos donde el usuario es un miembro directo. Si un grupo se mueve de una unidad organizativa a otra, el atributo memberOf refleja el último valor del nombre distintivo. La base de datos de XenMobile Server también tiene el último valor actualizado. Cualquier discrepancia entre los nombres distintivos de un grupo puede ocasionar que el usuario pierda acceso al grupo de implementación. El usuario también puede perder las aplicaciones y las directivas asociadas a ese grupo de implementación.
- El trabajo en segundo plano mantiene actualizado el atributo de nombre distintivo del grupo en la base de datos de XenMobile Server para garantizar que los usuarios tengan acceso a lo que les corresponde.

- Los trabajos de sincronización están programados para ejecutarse cada cinco horas porque se asume que los cambios de grupo en Active Directory son poco frecuentes.

¿Se puede desactivar un trabajo de sincronización de grupos?

- Puede desactivar los trabajos cuando sabe que los grupos relevantes no pasan de una unidad organizativa a otra.

¿Para qué se necesita un trabajo en segundo plano de procesamiento de grupos anidados?

- En Active Directory, los cambios en el anidamiento de grupos no son diarios. Los cambios en la jerarquía de anidamiento de los grupos relevantes producen cambios en los derechos de los usuarios afectados. Cuando se agrega un grupo a la jerarquía, sus usuarios miembros obtienen el derecho a los roles respectivos. Cuando un grupo abandona una estructura anidada, los usuarios miembros del grupo pueden perder el acceso a los derechos basados en roles.
- Los cambios en el anidamiento no se capturan durante la actualización de usuarios. Como los cambios de anidamiento no pueden realizarse a demanda, esos cambios se capturan a través de un trabajo en segundo plano.
- Se asume que los cambios de anidamiento son poco frecuentes y, por lo tanto, el trabajo en segundo plano se ejecuta una vez al día para comprobar si hay cambios.

¿Se puede desactivar un trabajo de procesamiento de grupos anidados?

- Puede desactivar los trabajos cuando sepa que no hay cambios de anidamiento en los grupos relevantes.

Implementar XenMobile

November 6, 2020

Hay muchos aspectos que tener en cuenta cuando se planifica una implementación de XenMobile.

- ¿Qué dispositivos elegir?
- ¿Cómo administrar los dispositivos?
- ¿Cómo asegurarse de que la red es segura y fácil de usar al mismo tiempo para los usuarios?
- ¿Qué hardware se necesita y cómo solucionar problemas en él?

Los artículos de esta sección tienen como objetivo responder a estas preguntas. Se incluyen casos de uso y recomendaciones sobre temas que cubren sus dudas sobre la implementación.

Tenga en cuenta que una guía o recomendación podría no aplicarse a todos los entornos o casos de uso. Debe configurar un entorno de prueba antes de lanzar una implementación de XenMobile.

Los artículos de esta sección cubren las siguientes áreas:

- **Evaluar:** Casos de uso y preguntas frecuentes a plantearse durante la planificación de la implementación.
- **Diseñar y configurar:** Recomendaciones para diseñar y configurar el entorno
- **Operar y supervisar:** Asegurar el buen funcionamiento del entorno de ejecución.

Evaluación

Como con cualquier implementación, evaluar sus necesidades es la máxima prioridad. ¿Qué necesita primordial lo lleva a XenMobile? ¿Necesita administrar todos los dispositivos de su entorno o solo las aplicaciones? Quizá necesite administrar ambos. ¿Qué nivel de seguridad necesita en su entorno de XenMobile? Veamos casos de uso y preguntas frecuentes a considerar cuando planifique su implementación.

- Modos de administración
- Requisitos de dispositivo
- Seguridad y experiencia del usuario
- Aplicaciones
- Comunidades de usuarios
- Estrategia de correo electrónico
- Integración de XenMobile
- Requisitos multisitio

Diseñar y configurar

Una vez que haya terminado de evaluar las necesidades de su implementación, puede determinar el diseño y la configuración de su entorno. Algunas cosas que necesita planificar:

- Elegir el hardware para su servidor
- Configurar directivas para aplicaciones y dispositivos
- Hacer que los usuarios se inscriban

Esta sección incluye casos de uso y recomendaciones para cada uno de estos casos, entre otros.

- Integración en Citrix Gateway y Citrix ADC
- Consideraciones sobre SSO y proxies para aplicaciones MDX
- Autenticación
- Arquitectura de referencia para implementaciones locales
- Propiedades de servidor
- Directivas de aplicación y de dispositivo
- Opciones de inscripción de usuarios
- Ajustar las operaciones de XenMobile

Operar y supervisar

Cuando su entorno XenMobile esté en funcionamiento, querrá supervisarlo para garantizar un funcionamiento óptimo. En la sección de supervisión se describe dónde se encuentran los varios registros y mensajes que generan XenMobile y sus componentes, además de indicarle cómo interpretar esos registros. Esta sección también incluye una serie de pasos para solucionar problemas frecuentes, que puede seguir para reducir el tiempo de comunicación con los equipos de asistencia al cliente.

- Aprovisionar y desaprovisionar aplicaciones
- Operaciones del panel de mandos
- Control de acceso basado en roles y asistencia en XenMobile
- Supervisar sistemas
- Recuperación ante desastres
- Proceso de asistencia de Citrix

Modos de administración

January 4, 2022

Para cada instancia de XenMobile (un solo servidor o un clúster de nodos), puede elegir si quiere administrar dispositivos, aplicaciones o ambos. XenMobile utiliza los siguientes términos para los modos de administración de dispositivos y aplicaciones:

- Modo de administración de dispositivos móviles (modo MDM)
- Modo de administración de aplicaciones móviles (modo MAM)
- Modo MDM+MAM (modo Enterprise)

Administración de dispositivos móviles (modo MDM)

> **Importante:**
>
> Si configura el modo MDM y después cambia al modo ENT, debe utilizar la misma autenticación (Active Directory). XenMobile no admite cambiar el modo de autenticación después de haber inscrito a los usuarios. Para obtener más información, consulte Actualizar.

Con MDM, puede configurar, proteger y ofrecer soporte a dispositivos móviles. MDM permite proteger los dispositivos y los datos contenidos en esos dispositivos a nivel de sistema. Puede configurar directivas, acciones y funciones de seguridad. Por ejemplo, puede borrar un dispositivo de forma selectiva si el dispositivo se pierde, deja de cumplir la normativa o se lo roban. Aunque la administración de aplicaciones no está disponible con el modo MDM, puede entregar aplicaciones móviles (por ejemplo, aplicaciones de almacén público y aplicaciones de empresa) en este modo. A continuación, se presentan los casos de uso más frecuentes para el modo MDM:

- Vale la pena tener el modo MDM en cuenta cuando se trata de dispositivos propiedad de la empresa donde se requieren restricciones o directivas de administración a nivel de dispositivo (como un borrado completo, un borrado selectivo o una localización geográfica).
- Cuando los clientes requieren la administración de un dispositivo real, pero no necesitan directivas MDX (por ejemplo, para la contenedorización de aplicaciones, para controlar el uso compartido de datos de las aplicaciones o la red micro VPN).
- Cuando los usuarios solo necesitan que se entregue el correo electrónico a los clientes de correo nativos presentes en sus dispositivos móviles, y ya se puede acceder externamente a Exchange ActiveSync o al servidor de acceso de cliente. En este caso, se puede usar la administración MDM para configurar la entrega de correo electrónico.
- Cuando implementa aplicaciones empresariales nativas (no MDX), aplicaciones de tiendas públicas o aplicaciones MDX entregadas desde tiendas públicas. Tenga en cuenta que una solución MDM por sí sola no evita la filtración de información confidencial entre las aplicaciones presentes en el dispositivo. La filtración de datos puede ocurrir con las operaciones “Copiar”, “Pegar” o “Guardar como” en las aplicaciones Office 365.

Administración de aplicaciones móviles (modo MAM)

La administración MAM protege los datos de la aplicación y permite controlar el uso compartido de esos datos. MAM también permite administrar los datos y los recursos corporativos de manera separada de los datos personales. Con XenMobile configurado para el modo MAM, puede usar aplicaciones móviles habilitadas para MDX para proporcionar el control y la contenedorización para cada aplicación. El “modo MAM” también se denomina “modo solo MAM”. Este término distingue este modo de un modo MAM antiguo.

Al aprovechar las directivas MDX, XenMobile ofrece el control a nivel de aplicación sobre: el acceso a la red (por ejemplo, con una red micro VPN), la interacción de dispositivos y aplicaciones, el cifrado de datos y el acceso a aplicaciones.

MAM suele ser idóneo para dispositivos BYO porque, aunque el dispositivo no esté administrado, los datos corporativos permanecen protegidos. MDX tiene muchas directivas exclusivas de MAM que no requieren un control de MDM.

MAM también admite las aplicaciones móviles de productividad. Esta compatibilidad implica la entrega segura de correo electrónico a Citrix Secure Mail, el intercambio de datos entre las aplicaciones móviles de productividad seguras y el almacenamiento seguro de datos en Citrix Files. Para obtener más información, consulte Aplicaciones móviles de productividad.

A menudo, MAM conviene cuando:

- Entrega aplicaciones móviles, tales como aplicaciones MDX, administradas a nivel de aplicación.
- No necesita administrar dispositivos a nivel de sistema.

MDM+MAM (modo Enterprise)

El modo MDM+MAM es un modo híbrido, también denominado "modo Enterprise", que permite todos los conjuntos de funciones disponibles en la solución Enterprise Mobility Management (EMM o gestión de movilidad empresarial) de XenMobile. Configurar XenMobile en el modo MDM+MAM habilita las funciones MDM y MAM.

XenMobile permite especificar si los usuarios pueden optar por no administrar el dispositivo o si, en cambio, es necesario administrarlo. Esta flexibilidad es útil para entornos que incluyen una mezcla de casos de uso. Estos entornos pueden requerir o no la administración de un dispositivo a través de directivas MDM para acceder a los recursos MAM.

MDM+MAM conviene cuando:

- Dispone de un solo caso de uso donde se requieren MDM y MAM. Se necesita MDM para acceder a los recursos MAM.
- Algunos casos de uso requieren MDM, mientras que otros no.
- Algunos casos de uso requieren MAM, mientras que otros no.

El modo de administración de XenMobile Server se indica a través de la propiedad "Modo de servidor". Este parámetro se configura en la consola de XenMobile. El modo puede ser MDM, MAM o ENT (para MDM+MAM).

La edición de XenMobile para la que tiene licencia determina los modos de administración y otras funciones disponibles, como se muestra en la siguiente tabla.

XenMobile MDM Edition	XenMobile Advanced Edition	XenMobile Enterprise Edition
Funciones MDM	Funciones MDM	Funciones MDM
-	Funciones MAM	Funciones MAM
-	MDX Toolkit	MDX Toolkit
Secure Hub	Secure Hub	Secure Hub
-	Secure Mail	Secure Mail
-	Secure Web	Secure Web
QuickEdit	QuickEdit	QuickEdit
-	-	ShareConnect
-	-	Citrix Files

Modos de administración y perfiles de inscripción

Los modos de administración y los perfiles de inscripción funcionan juntos. Utilice un perfil de inscripción para configurar las opciones de inscripción para administración de dispositivos y aplicaciones con dispositivos Android e iOS. En el caso de Android, las opciones de inscripción disponibles para el modo de servidor MDM+MAM difieren de las opciones para el modo MDM. Para obtener más información, consulte Perfiles de inscripción.

Administración de dispositivos e inscripción MDM

Un entorno de XenMobile Enterprise puede incluir una mezcla de casos de uso, donde algunos de ellos requieren la administración de dispositivos a través de directivas MDM para permitir el acceso a los recursos MAM. Antes de implementar las aplicaciones móviles de productividad a los usuarios, debe evaluar de manera exhaustiva los casos de uso y decidir si requiere la inscripción MDM. Si más adelante decide cambiar el requisito de la inscripción MDM, es probable que los usuarios deban volver a inscribir sus dispositivos.

> **Nota:**
>
> Para especificar si necesita que los usuarios se inscriban en MDM, use la propiedad **Inscripción requerida** de XenMobile Server en la consola de XenMobile (**Parámetros > Propiedades de servidor**). Dicha propiedad de servidor global se aplica a todos los usuarios y dispositivos de la instancia de XenMobile. La propiedad se aplica solo cuando el modo de XenMobile Server es ENT.

A continuación, dispone de un resumen de las ventajas y las desventajas (junto con las maneras de atenuarlas) de requerir la inscripción MDM en una implementación de XenMobile en modo Enterprise.

Cuando la inscripción MDM es opcional

Ventajas:

- Los usuarios pueden acceder a los recursos MAM sin que sus dispositivos se administren por MDM. Esta opción puede aumentar la cantidad de usuarios.
- Posibilidad de proteger el acceso a los recursos MAM para, a su vez, proteger los datos de empresa.
- Las directivas MDX, como **Código de acceso de aplicación**, pueden controlar el acceso a cada aplicación MDX.
- Configurar Citrix ADC, XenMobile Server y tiempos de espera para cada aplicación, junto con el PIN de Citrix, ofrecen una capa extra de protección.
- Si bien las acciones de MDM no se aplican al dispositivo, dispone de determinadas directivas MDX para denegar el acceso a los recursos MAM. La denegación del acceso se basaría en la configuración del sistema, como dispositivos liberados por jailbreak o rooting.

- Los usuarios pueden elegir si inscribir sus dispositivos con MDM al primer uso.

Desventajas:

- Los recursos MAM están disponibles para los dispositivos que no están inscritos con MDM.
- Las acciones y las directivas MDM solo están disponibles en los dispositivos inscritos con MDM.

Opciones de mitigación:

- Haga que los usuarios acepten los términos y las condiciones de la empresa. Serán responsables frente a esta empresa si eligen dejar de cumplir las normas. Haga que los administradores supervisen los dispositivos no administrados.
- Administre la seguridad y el acceso a las aplicaciones a través de temporizadores de aplicación. Unos valores inferiores de tiempo de espera aumentan la seguridad, pero pueden afectar a la experiencia de usuario.
- Una posibilidad es un segundo entorno de XenMobile con la inscripción MDM requerida. Al considerar esta opción, tenga en cuenta los recursos adicionales necesarios y la sobrecarga adicional que implica administrar dos entornos.

Cuando la inscripción MDM es obligatoria

Ventajas:

- Posibilidad de restringir el acceso a los recursos MAM solo a los dispositivos administrados por MDM.
- Las acciones y las directivas MDM pueden aplicarse a todos los dispositivos del entorno como sea pertinente.
- Los usuarios no pueden optar por no inscribir su dispositivo.

Desventajas:

- Requiere que todos los usuarios se inscriban con MDM.
- Puede reducir la cantidad de usuarios, ya que los usuarios que no estén de acuerdo con que la empresa administre sus dispositivos personales pueden no inscribirse.

Opciones de mitigación:

- Informe a los usuarios sobre lo que XenMobile administra realmente en sus dispositivos e indíqueles a qué información pueden acceder los administradores.
- Puede usar un segundo entorno de XenMobile, donde la propiedad “Modo de servidor” tiene el valor “MAM” (también llamado “modo solo MAM”), para dispositivos que no necesitan la administración MDM. Al considerar esta opción, tenga en cuenta los recursos adicionales necesarios y la sobrecarga adicional que implica administrar dos entornos.

Acerca de los modos MAM y MAM antiguo

Con XenMobile 10.3.5, se introdujo el modo de servidor solo MAM. Para distinguir entre el modo MAM anterior y el nuevo, se utilizan estos términos en la documentación. El nuevo modo se llama "solo MAM" o "MA", mientras que el modo MAM anterior se llama "modo MAM antiguo".

El modo solo MAM se activa cuando la propiedad "Modo de servidor" de XenMobile tiene el valor MAM. Los dispositivos se registran en el modo MAM.

La funcionalidad MAM antigua se activa cuando la propiedad "Modo de servidor" de XenMobile tiene el valor ENT y los usuarios eligen no usar la administración de dispositivos. En ese caso, los dispositivos se registran en el modo MAM. Los usuarios que optan por no usar la administración MDM siguen recibiendo la funcionalidad de MAM antiguo.

> **Nota:**
>
> Anteriormente, configurar la propiedad "Modo de servidor" con el valor MAM tenía el mismo efecto que configurarla con el valor ENT, es decir, los usuarios que decidían no usar la administración MDM recibían la funcionalidad de MAM antiguo.

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

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

El modo solo MAM admite las siguientes funciones que anteriormente estaban disponibles solo para ENT. Estas funciones no están disponibles para Windows Phone.

- **Autenticación basada en certificados:** El modo solo MAM admite la autenticación con certificados. Los usuarios tendrán acceso continuo a sus aplicaciones, incluso cuando caduque su contraseña de Active Directory. Si usa la autenticación basada en certificados para los dispositivos MAM, debe configurar el dispositivo Citrix Gateway. De manera predeterminada, en

XenMobile, en **Parámetros > Citrix Gateway**, el parámetro “Entregar certificado de usuario para autenticación” está **desactivado**, lo que significa que se usa autenticación con nombre de usuario y contraseña. **Active** este parámetro para habilitar la autenticación por certificado.

- **Self-Help Portal:** Para permitir que los usuarios lleven a cabo por sí mismos las acciones de bloqueo y borrado de aplicaciones. Estas acciones tienen efecto en todas las aplicaciones del dispositivo. Puede configurar las acciones de bloqueo de aplicaciones y borrado de aplicaciones en **Configurar > Acciones**.
- **Todos los modos de seguridad para la inscripción:** Incluidos los de Alta seguridad, URL de invitación y Dos factores, configurados desde **Administrar > Invitaciones de inscripción**.
- **Límite de registro para dispositivos Android y iOS:** La propiedad de servidor **Cantidad de dispositivos por usuario** ahora se encuentra en **Configurar > Perfiles de inscripción** y se aplica a todos los modos de servidor.
- **API de solo MAM:** Para dispositivos solo MAM, puede invocar los servicios REST desde cualquier cliente REST mediante la API de REST de XenMobile para llamar los servicios que expone la consola de XenMobile.
- Las API de solo MAM permiten:
  - Enviar una URL de invitación y un PIN de un solo uso.
  - Emitir acciones de bloqueo y borrado de aplicaciones a los dispositivos.

En la siguiente tabla se resumen las diferencias entre la funcionalidad de MAM antiguo y solo MAM.

Casos de inscripción y otras funciones	MAM antiguo (modo de servidor = ENT)	Modo solo MAM (modo de servidor = MAM)
Autenticación de certificados	No se admite.	Se admite. Para la autenticación con certificados, es necesario usar Citrix Gateway.
Requisito de implementación	No es necesario que los dispositivos puedan acceder directamente al servidor de XenMobile Server.	No es necesario que los dispositivos puedan acceder directamente al servidor de XenMobile Server.
Opción de inscripción	Usar el nombre de dominio completo (FQDN) de Citrix Gateway o, cuando se usa el FQDN de MDM, optar por no inscribirse.	Usar el nombre de dominio completo (FQDN) de XenMobile Server.

Métodos de inscripción*	Nombre de usuario y contraseña	Nombre de usuario y contraseña; Alta seguridad; URL de invitación; URL de invitación y PIN, URL de invitación y contraseña, Dos factores, Nombre de usuario y PIN
Bloqueo y borrado de aplicaciones	Se admite.	Se admite.
Opciones del portal Self-Help Portal para el borrado y bloqueo de aplicaciones	No se admite.	Se admite.
Comportamiento del borrado de aplicaciones	Las aplicaciones permanecen en el dispositivo, pero no se pueden usar. XenMobile elimina la cuenta solo en el cliente.	Las aplicaciones permanecen en el dispositivo, pero no se pueden usar. XenMobile elimina la cuenta solo en el cliente.
Acciones automatizadas para usuarios del modo solo MAM.	Se admiten las acciones de evento, propiedad de dispositivo y propiedad de usuario. No se admiten las acciones automatizadas en aplicaciones instaladas.	Admite acciones de eventos, propiedades de dispositivo, propiedades de usuario y algunas acciones de aplicaciones, incluido el bloqueo de aplicaciones y el borrado de aplicaciones.
Acción integrada cuando se elimina un usuario de Active Directory	Admite el borrado de aplicaciones.	Admite el borrado de aplicaciones.
Límite de inscripción	Se admite; configurado en un perfil de inscripción.	Se admite; configurado en un perfil de inscripción.
Inventario de software	Se admite. XenMobile enumera las aplicaciones instaladas en un dispositivo	No se admite.

* **Con respecto a las notificaciones:** SMTP es el único método admitido para enviar invitaciones de inscripción.

> **Importante:**
>
> Para el modo solo MAM, los usuarios ya inscritos deben volver a inscribir sus dispositivos. Debe proporcionar a los usuarios el nombre de dominio completo (FQDN) de XenMobile Server que necesiten para la inscripción. En el modo solo MAM, al igual que en el modo ENT, los dispositivos se inscriben con el nombre FQDN de XenMobile Server (en el modo MAM antiguo, los dispositivos se inscriben mediante el nombre FQDN de Citrix Gateway).

Requisitos de dispositivo

January 4, 2022

Un punto importante tener en cuenta en toda implementación es el dispositivo que se va a utilizar. En las plataformas iOS, Android y Windows, existen varias opciones. Para ver la lista de los dispositivos compatibles en XenMobile, consulte Plataformas de dispositivos compatibles.

En un entorno BYOD, se puede dar una combinación de las plataformas compatibles. Sin embargo, tenga en cuenta las limitaciones descritas en el artículo "Plataformas de dispositivos admitidos" cuando informe a los usuarios sobre los dispositivos que pueden inscribir. Aunque solo permita uno o dos dispositivos en su entorno, el funcionamiento de XenMobile cambia ligeramente en dispositivos iOS, Android o Windows. En cada plataforma, están disponibles diferentes conjuntos de funciones.

Además, no todos los diseños de aplicaciones están orientados a tabletas y teléfonos a la vez. Antes de realizar cambios generalizados, pruebe las aplicaciones para asegurarse de que se ajustan a la pantalla del dispositivo donde quiere implementar el entorno.

También puede plantearse los factores de inscripción que va a utilizar. Apple y Google ofrecen programas de inscripción empresarial. A través del Programa de implementación de Apple y Google Android Enterprise, puede adquirir dispositivos preconfigurados y listos para que los usen los empleados.

Para obtener más información acerca de la inscripción, consulte Opciones de inscripción de usuarios.

Seguridad y experiencia del usuario

January 4, 2022

La seguridad es importante para cualquier organización, pero hay que encontrar el equilibrio entre la seguridad y la experiencia del usuario. Por ejemplo, es posible que tenga un entorno muy seguro que resulte difícil de usar para los usuarios. O, al contrario, es posible que su entorno resulte tan fácil de usar que el control del acceso no sea tan estricto como debiera. En las demás secciones de

este manual virtual se tratan detalladamente las funciones de seguridad. El propósito de este artículo es ofrecer una descripción general de los aspectos más comunes sobre seguridad y las opciones de seguridad disponibles en XenMobile.

Estas son algunas consideraciones clave que debe tener en cuenta para cada caso de uso:

- ¿Quiere proteger determinadas aplicaciones, todo el dispositivo o ambos?
- ¿Cómo quiere que los usuarios se autentiquen? ¿Piensa utilizar LDAP, la autenticación por certificado o una combinación de ambos?
- ¿Cómo quiere gestionar los tiempos de espera de sesión de usuario? Tenga en cuenta que existen valores de tiempo de espera diferentes para los servicios en segundo plano, Citrix ADC y para el acceso a aplicaciones sin conexión.
- ¿Quiere que los usuarios configuren una clave de acceso a nivel de dispositivo, a nivel de aplicación o ambos? ¿Cuántos intentos de inicio de sesión quiere permitir a los usuarios? Tenga en cuenta de qué manera los requisitos adicionales de autenticación por aplicación implementados con MAM podrían afectar a la experiencia del usuario.
- ¿Qué otras restricciones quiere imponer a los usuarios? ¿Quiere que los usuarios tengan acceso a servicios en la nube, como Siri? ¿Qué pueden hacer con cada aplicación que se ponga a su disposición y qué no pueden hacer? ¿Quiere implementar directivas de red Wi-Fi en la empresa para impedir que se consuman planes de datos móviles en las oficinas?

Aplicación o Dispositivo

Uno de los primeros aspectos que hay que considerar es si proteger solo ciertas aplicaciones con administración de aplicaciones móviles (MAM). O si también quiere administrar todo el dispositivo con administración de dispositivos móviles (MDM). Lo más frecuente es que, si no requiere control a nivel de dispositivo, solo administrará las aplicaciones móviles, sobre todo si la organización admite los dispositivos Bring Your Own Device (BYOD).

Los usuarios cuyos dispositivos no administra XenMobile pueden instalar aplicaciones a través de la tienda de aplicaciones. En lugar de controles a nivel de dispositivo (como el borrado completo o selectivo de datos), se puede controlar el acceso a las aplicaciones a través de directivas de aplicaciones. Las directivas, según los valores que se establezcan, requieren que el dispositivo consulte frecuentemente XenMobile para confirmar que las aplicaciones aún se pueden ejecutar.

MDM permite proteger un dispositivo completo, incluida la capacidad de realizar un inventario de todo el software presente en un dispositivo. Puede impedir la inscripción si el dispositivo está liberado por jailbreak, rooting o tiene instalado software no seguro. Sin embargo, asumir este nivel de control hace que los usuarios sean reacios a permitir tanto poder sobre sus dispositivos personales y puede reducir las tasas de inscripción.

Autenticación

La autenticación es donde se lleva a cabo una gran parte de la experiencia del usuario. Si la organización ya ejecuta Active Directory, usar Active Directory es la forma más sencilla de que los usuarios accedan al sistema.

Otra parte importante de la experiencia de autenticación de los usuarios son los tiempos de espera. En un entorno de alta seguridad, los usuarios inician sesión cada vez que acceden al sistema, pero esa opción no es idónea para todas las organizaciones. Por ejemplo, obligar a introducir las credenciales cada vez que se quiere acceder al correo electrónico puede afectar negativamente a la experiencia de usuario.

Entropía de usuario

Para obtener una mayor seguridad, puede habilitar una función llamada *entropía de usuario*. Citrix Secure Hub y otras aplicaciones a menudo comparten datos comunes (como contraseñas, números PIN y certificados) para garantizar que todo funciona correctamente. Esta información se almacena en una caja fuerte genérica dentro de Secure Hub. Si habilita la entropía del usuario a través de la opción **Cifrar secretos**, XenMobile crea una nueva caja fuerte llamada UserEntropy. XenMobile traslada la información desde la caja fuerte genérica a esta nueva caja. Para que Secure Hub u otra aplicación accedan a los datos, los usuarios deben escribir una contraseña o PIN.

Habilitar la entropía de usuario agrega otra capa de autenticación en varios lugares. Como resultado, los usuarios deben introducir una contraseña o un PIN cada vez que una aplicación requiere acceso a datos compartidos, incluidos certificados, en la caja fuerte UserEntropy.

Puede obtener más información sobre la entropía de usuario en Acerca de MDX Toolkit en la documentación de XenMobile. Para activar la entropía de usuario, dispone de la configuración relacionada en las Propiedades del cliente.

Directivas

Las directivas MDX y MDM ofrecen una gran flexibilidad a las organizaciones, pero también pueden imponer restricciones a los usuarios. Por ejemplo, puede que le interese bloquear el acceso a aplicaciones en la nube (como Siri o iCloud), con las que se pueden enviar datos confidenciales a diferentes destinos. Puede configurar una directiva para bloquear el acceso a estos servicios, pero tenga en cuenta que dicha directiva puede tener consecuencias no deseadas. El micrófono de teclado iOS también depende del acceso a la nube, con lo que puede que esa directiva bloquee el acceso a esa función.

Aplicaciones

La administración de movilidad empresarial (EMM) se divide en la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM). Si bien MDM permite a las organizaciones proteger y controlar dispositivos móviles, MAM facilita la administración y la entrega de aplicaciones. Con el aumento creciente de dispositivos BYOD, puede implementar una solución MAM que le ayude en la entrega de aplicaciones, la gestión de licencias de software, la configuración y la administración del ciclo de vida de las aplicaciones.

Con XenMobile, puede ir más allá y proteger estas aplicaciones mediante directivas MAM y configuraciones de VPN específicas para evitar filtraciones de datos y otras amenazas a la seguridad. XenMobile proporciona a las organizaciones la flexibilidad necesaria para implementar cualquiera de las siguientes soluciones:

- Entorno de solo MAM
- Entorno de solo MDM
- Entorno unificado de XenMobile Enterprise con funcionalidad MDM y MAM en la misma plataforma

Además de la capacidad de entregar aplicaciones a los dispositivos móviles, XenMobile ofrece la contenedorización de aplicaciones a través de la tecnología MDX. MDX protege las aplicaciones mediante un cifrado independiente del cifrado al nivel del dispositivo proporcionado por la plataforma. Puede borrar o bloquear una aplicación determinada. Las aplicaciones están sujetas a controles concisos basados en directivas. Los proveedores de software independientes (ISV) pueden aplicar estos controles mediante el Mobile Apps SDK.

En un entorno corporativo, los usuarios utilizan una variedad de aplicaciones móviles para desempeñar su trabajo. Las aplicaciones pueden ser: aplicaciones procedentes de la tienda pública, aplicaciones propias desarrolladas internamente y aplicaciones nativas. XenMobile clasifica estas aplicaciones de la siguiente manera:

Aplicaciones públicas: Este grupo contiene las aplicaciones, gratuitas o de pago, disponibles en una tienda pública de aplicaciones, como App Store de Apple o Google Play. Los proveedores externos a la organización suelen poner sus aplicaciones disponibles en las tiendas públicas de aplicaciones. Esta opción permite a sus clientes descargar las aplicaciones directamente desde Internet. Puede utilizar varias aplicaciones públicas en su organización, según las necesidades de los usuarios. GoToMeeting, Salesforce y EpicCare son ejemplos de tales aplicaciones.

Citrix no admite la descarga de archivos binarios de aplicación directamente desde tiendas públicas de aplicaciones y, a continuación, su empaquetado con el MDX Toolkit para la distribución empresarial. Para habilitar para MDX aplicaciones de terceros, póngase en contacto con su proveedor de aplicaciones para obtener los binarios de aplicación. Puede empaquetar los binarios con MDX Toolkit o integrar el SDK de MAM con los binarios.

Aplicaciones internas: Muchas organizaciones tienen desarrolladores internos que crean aplica-

ciones con una funcionalidad específica y que se desarrollan y distribuyen de manera independiente dentro de la organización. En ciertos casos, algunas organizaciones también pueden tener aplicaciones proporcionadas por los ISV. Puede implementar esas aplicaciones como nativas, o puede colocarlas en un contenedor con una solución MAM, como XenMobile. Por ejemplo, una organización de asistencia sanitaria puede crear una aplicación interna que permita a los médicos ver la información del paciente en dispositivos móviles. En ese caso, la organización puede habilitar el SDK de MAM o empaquetar con MDM la aplicación a fin de proteger la información del paciente y permitir el acceso por VPN al servidor back-end de la base de datos de pacientes.

Aplicaciones web y SaaS: Este grupo incluye aquellas aplicaciones a las que se puede acceder a través de una red interna (aplicaciones web) o a través de una red pública (aplicaciones SaaS). XenMobile también permite crear aplicaciones web y SaaS personalizadas mediante una lista de conectores de aplicaciones. Esos conectores de aplicaciones pueden facilitar el inicio Single Sign-On (SSO) en las aplicaciones web existentes. Para obtener más información, consulte Tipos de conectores de aplicaciones. Por ejemplo, puede usar Google Apps SAML para Single Sign-On basado en SAML (Security Assertion Markup Language) en aplicaciones de Google Apps.

Aplicaciones móviles de productividad: Aplicaciones desarrolladas por Citrix que se incluyen con la licencia de XenMobile. Para obtener más información, consulte Acerca de las aplicaciones móviles de productividad. Citrix también ofrece otras aplicaciones de negocio que los ISV desarrollan mediante el Mobile Apps SDK.

Aplicaciones HDX: Aplicaciones alojadas en Windows que se publican con StoreFront. Si dispone de un entorno de Citrix Virtual Apps and Desktops, puede integrar las aplicaciones en XenMobile para que estén disponibles a los usuarios inscritos.

La configuración y la arquitectura subyacentes varían en función del tipo de aplicaciones móviles que implementar y administrar a través de XenMobile. Por ejemplo, si varios grupos de usuarios con diferentes niveles de permisos utilizan una sola aplicación, puede crear grupos de entrega independientes para implementar dos versiones separadas de la misma. Además, deberá asegurarse de que la pertenencia a cada grupo de usuarios se excluya mutuamente, para evitar discrepancias entre las directivas que se apliquen a los dispositivos de los usuarios.

También sería conveniente administrar las licencias de las aplicaciones iOS a través de las compras por volumen de Apple. Para poder utilizar esta opción, deberá registrarse en el Programa de compras por volumen de Apple y configurar los parámetros de compras por volumen de XenMobile desde la consola de XenMobile para distribuir las aplicaciones con las licencias de compras por volumen. Dada la variedad de estos casos de uso, es importante evaluar y planificar la estrategia de MAM que va a seguir antes de implementar el entorno de XenMobile. Para comenzar a planificar su estrategia de MAM, defina lo siguiente:

Tipos de aplicaciones: Indique los diferentes tipos de aplicaciones que quiere admitir y clasifíquelas por categorías. Por ejemplo: aplicaciones públicas, nativas, móviles de productividad, web, internas, ISV, etc. Además, clasifique las aplicaciones según las diferentes plataformas de dispositivo (como iOS

y Android). Esta categorización le ayudará a adaptar los parámetros de XenMobile que se requieren para cada tipo de aplicación. Por ejemplo, algunas aplicaciones podrían requerir el uso del Mobile Apps SDK a fin de habilitar unas API especiales para la interacción con otras aplicaciones.

Requisitos de red: Las aplicaciones que tengan requisitos específicos de acceso a la red deben configurarse con los parámetros adecuados. Por ejemplo, ciertas aplicaciones pueden necesitar acceder a la red interna por VPN. En cambio, otras aplicaciones pueden requerir que el acceso a Internet se enrute a través de la zona DMZ. Para permitir que esas aplicaciones se conecten a la red requerida, debe configurar varios parámetros según corresponda. Definir unos requisitos de red por aplicación contribuye a precisar sus decisiones arquitectónicas desde el principio, lo que optimiza el proceso general de implementación.

Requisitos de seguridad: Es esencial definir los requisitos de seguridad que se aplicarán a aplicaciones individuales o a todas las aplicaciones. Esa planificación garantiza que cree las configuraciones correctas al instalar XenMobile Server. Aunque otros parámetros, como las directivas MDX, se aplican a aplicaciones individuales, los parámetros de sesión y autenticación se aplican a todas las aplicaciones. Algunas aplicaciones pueden presentar requisitos específicos de cifrado, contenedorización, empaquetado, cifrado, autenticación, geocercas, código de acceso o uso compartido de datos que puede esbozar de antemano para simplificar la implementación.

Requisitos de implementación: Puede que le interese una implementación basada en directivas si quiere permitir que solo los usuarios conformes descarguen las aplicaciones publicadas. Por ejemplo, puede interesarle que ciertas aplicaciones requieran cualquiera de estos aspectos:

- El cifrado por plataforma de dispositivos está habilitado
- El dispositivo está administrado
- El dispositivo tiene una versión mínima del sistema operativo
- Ciertas aplicaciones están disponibles solo para usuarios de empresa

También puede interesarle que ciertas aplicaciones estén disponibles solo para usuarios de empresa. Debe esbozar dichos requisitos con antelación para configurar las acciones o las reglas de implementación apropiadas.

Requisitos de licencia: Conserve un registro de los requisitos de licencia relacionados con las aplicaciones. Estas notas le servirán de ayuda para administrar de manera efectiva el uso de las licencias y decidir si configurar funciones específicas en XenMobile para optimizar la gestión de licencias. Por ejemplo, si implementa una aplicación iOS gratuita o de pago, Apple aplica requisitos de licencia a la aplicación porque obliga a los usuarios a iniciar sesión en su cuenta de iTunes. Puede registrarse en el programa de compras por volumen de Apple para distribuir y administrar esas aplicaciones a través de XenMobile. El programa de compras por volumen permite a los usuarios descargar las aplicaciones sin tener que iniciar sesión en la cuenta de iTunes. Además, las herramientas (como Samsung SAFE y Samsung Knox) presentan requisitos especiales de licencia que debe cumplir antes de implementar esas funciones.

Requisitos de lista de bloqueados o lista de permitidos: Es probable que quiera impedir que los usuarios instalen o utilicen algunas aplicaciones. Cree una lista de aplicaciones bloqueadas que cambian el estado de un dispositivo a no conforme. A continuación, configure las directivas para que se activen cuando un dispositivo pase a ser no conforme. Por otro lado, puede que acepte el uso de una aplicación, pero esta se incluya en la lista de aplicaciones bloqueadas por una razón u otra. En ese caso, puede agregar la aplicación a una lista de aplicaciones permitidas e indicar que se puede usar, pero no es obligatoria. Además, tenga en cuenta que las aplicaciones ya instaladas en los dispositivos nuevos pueden incluir algunas aplicaciones de uso común que no forman parte del sistema operativo. Estas aplicaciones pueden entrar en conflicto con su estrategia de listas de aplicaciones bloqueadas.

Aplicaciones: caso de uso

Una organización de asistencia sanitaria quiere implementar XenMobile como solución MAM para sus aplicaciones móviles. Las aplicaciones móviles se entregan a usuarios de empresa y usuarios BYOD. El departamento de TI decide entregar y administrar las siguientes aplicaciones:

- **Aplicaciones móviles de productividad:** Aplicaciones iOS y Android que proporciona Citrix.
- **Secure Mail:** Aplicación de correo electrónico, calendario y contactos.
- **Secure Web:** Explorador web seguro que ofrece acceso a los sitios de Internet e intranet.
- **Citrix Files:** Aplicación para acceder a datos compartidos y para compartir, sincronizar y modificar archivos.

Tienda pública de aplicaciones

- **Citrix Secure Hub:** Cliente que utilizan todos los dispositivos móviles para comunicarse con XenMobile. El departamento de TI envía los parámetros de seguridad, las configuraciones y las aplicaciones móviles a los dispositivos móviles a través del cliente de Secure Hub. Los dispositivos Android y iOS se inscriben en XenMobile a través de Secure Hub.
- **Citrix Receiver:** Aplicación móvil que permite a los usuarios abrir las aplicaciones que aloja Virtual Apps and Desktops en dispositivos móviles.
- **GoToMeeting:** Un cliente de reuniones en línea, uso compartido de escritorios y videoconferencias que permite a los usuarios reunirse con clientes, colegas u otros usuarios de equipos a través de Internet en tiempo real.
- **SalesForce1:** Permite a los usuarios acceder a Salesforce desde dispositivos móviles, y reúne todos los procesos de negocio y las aplicaciones personalizadas, Chatter y CRM, en una experiencia unificada para cualquier usuario de Salesforce.
- **RSA SecurID:** Token basado en software para la autenticación de dos factores.
- **Aplicaciones EpicCare:** Estas aplicaciones ofrecen a los profesionales de la salud un acceso seguro y portátil a los gráficos de pacientes, las listas de pacientes, los horarios y los mensajes.
  - **Haiku:** Aplicación móvil para teléfonos Android y iPhone.
  - **Canto:** Aplicación móvil para el iPad.

  - **Rover:** Aplicaciones móviles para iPhone y iPad.

HDX: Estas aplicaciones se entregan a través de Citrix Virtual Apps and Desktops.

- **Epic Hyperspace:** Aplicación cliente de Epic para la administración electrónica de registros de salud.

ISV

- **Vocera:** Aplicación móvil de mensajería y VoIP compatible con HIPAA, que extiende las ventajas de la tecnología de voz de Vocera para poder aprovecharlas en cualquier momento y cualquier lugar desde smartphones iPhone y Android.

Aplicaciones internas

- **HCMail:** Aplicación que ayuda a redactar mensajes cifrados, buscar en las libretas de direcciones en servidores de correo interno y enviar los mensajes cifrados a los contactos mediante un cliente de correo electrónico.

Aplicaciones web internas

- **PatientRounding:** Aplicación web utilizada para registrar la información sanitaria del paciente por diferentes departamentos.
- **Outlook Web Access:** Permite el acceso al correo electrónico a través de un explorador web.
- **SharePoint:** Se usa para compartir archivos y datos por toda la organización.

En la tabla siguiente, se muestra la información básica necesaria para la configuración de MAM.

Nombre de la aplicación	Tipo de aplicación	Empaquetado MDX	iOS	Android
Secure Mail	Aplicación XenMobile	No a partir de la versión 10.4.1	Sí	Sí
Secure Web	Aplicación XenMobile	No a partir de la versión 10.4.1	Sí	Sí
Citrix Files	Aplicación XenMobile	No a partir de la versión 10.4.1	Sí	Sí
Secure Hub	Aplicación pública	NA	Sí	Sí
Citrix Receiver	Aplicación pública	NA	Sí	Sí

GoToMeeting-	Aplicación pública	NA	Sí	Sí
SalesForce1	Aplicación pública	NA	Sí	Sí
RSA SecurID	Aplicación pública	NA	Sí	Sí
Epic Haiku	Aplicación pública	NA	Sí	Sí
Epic Canto	Aplicación pública	NA	Sí	No
Epic Rover	Aplicación pública	NA	Sí	No
Epic Hyperspace	Aplicación HDX	NA	Sí	Sí
Vocera	Aplicación de ISV	Sí	Sí	Sí
HCMail	Aplicación interna	Sí	Sí	Sí
PatientRounding	Aplicación web	NA	Sí	Sí
Outlook Web Access	Aplicación web	NA	Sí	Sí
SharePoint	Aplicación web	NA	Sí	Sí

En la siguiente tabla, se ofrece una lista de los requisitos específicos que puede consultar para la configuración de directivas MAM en XenMobile.

Nombre de la aplicación	**Se requiere VPN**	**Interacción**	**Interacción**	**Cifrado por plataforma de dispositivos**
		(con aplicaciones fuera del contenedor)	**(desde aplicaciones fuera del contenedor)**	
————	—	———————	———————	————
Secure Mail	S	Se permite de manera selectiva	Se permite	No se requiere
Secure Web	S	Se permite	Se permite	No se requiere
Citrix Files	S	Se permite	Se permite	No se requiere
Secure Hub	S	N/D	N/D	N/D
Citrix Receiver	S	N/D	N/D	N/D
GoToMeeting-	N	N/D	N/D	N/D
SalesForce1	N	N/D	N/D	N/D

RSA SecurID	N	N/D	N/D	N/D
Epic Haiku	S	N/D	N/D	N/D
Epic Canto	S	N/D	N/D	N/D
Epic Rover	S	N/D	N/D	N/D
Epic Hyperspace	S	N/D	N/D	N/D
Vocera	S	Bloqueada	Bloqueada	No se requiere
HCMail	S	Bloqueada	Bloqueada	Si son necesarias
PatientRounding	S	N/D	N/D	Si son necesarias
Outlook Web Access	S	N/D	N/D	No se requiere
SharePoint	S	N/D	N/D	No se requiere

Nombre de la aplicación	Filtrado de proxy	Licencias	Geocerca	Mobile Apps SDK	Versión mínima del sistema operativo
Secure Mail	Si son necesarias	N/D	Se requiere de manera selectiva	N/D	Se aplica
Secure Web	Si son necesarias	N/D	No se requiere	N/D	Se aplica
Citrix Files	Si son necesarias	N/D	No se requiere	N/D	Se aplica
Secure Hub	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Citrix Receiver	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
GoToMeeting-	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
SalesForce1	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
RSA SecurID	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Haiku	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Canto	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica

Nombre de la aplicación	Filtrado de proxy	Licencias	Geocerca	Mobile Apps SDK	Versión mínima del sistema operativo
Epic Rover	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Hyperspace	No se requiere	N/D	No se requiere	N/D	No se aplica
Vocera	Si son necesarias	N/D	Si son necesarias	Si son necesarias	Se aplica
HCMail	Si son necesarias	N/D	Si son necesarias	Si son necesarias	Se aplica
PatientRoundir	Si son necesarias	N/D	No se requiere	N/D	No se aplica
Outlook Web Access	Si son necesarias	N/D	No se requiere	N/D	No se aplica
SharePoint	Si son necesarias	N/D	No se requiere	N/D	No se aplica

Comunidades de usuarios

Cada organización consta de diversas comunidades de usuarios que operan en diferentes roles funcionales. Estas comunidades de usuarios realizan diferentes tareas y funciones de oficina mediante diversos recursos que usted proporciona a través de los dispositivos móviles de esos usuarios. Los usuarios pueden trabajar desde casa o en oficinas remotas mediante dispositivos móviles que usted proporcione. O bien, los usuarios pueden usar sus propios dispositivos móviles, lo que les permite acceder a herramientas que están sujetas a ciertas reglas de seguridad.

Con la cantidad creciente de comunidades de usuarios que usan dispositivos móviles, la administración Enterprise Mobility Management (EMM) se ha convertido en un elemento vital para evitar la filtración de datos y para hacer cumplir las restricciones de seguridad. Para una administración eficiente y más sofisticada de dispositivos móviles, puede categorizar las comunidades de los usuarios. Al hacerlo, se simplifica la asignación de usuarios a los recursos y se garantiza que se apliquen las directivas de seguridad correspondientes a los usuarios indicados.

El siguiente ejemplo ilustra cómo se clasifican para EMM las comunidades de usuarios de una organización de asistencia sanitaria.

Comunidades de usuarios: caso de uso

Esta organización sanitaria de ejemplo ofrece recursos tecnológicos y acceso a varios usuarios, incluidos los voluntarios, los empleados en la red y los empleados asociados. La organización ha decidido aplicar la solución EMM solo para usuarios no ejecutivos.

En esta organización, las funciones y los roles se pueden dividir en estos subgrupos: sanitarios, no sanitarios y contratistas. Un conjunto seleccionado de los usuarios recibe dispositivos móviles de empresa, mientras que otras personas pueden acceder a recursos limitados de la empresa desde sus dispositivos personales. Para hacer cumplir el nivel apropiado de restricciones de seguridad y evitar la filtración de datos, la organización decidió que el departamento de TI corporativo administrara cada dispositivo inscrito, ya fuera este propiedad de la empresa o del usuario. Además, los usuarios pueden inscribir un solo dispositivo.

La siguiente sección ofrece una descripción general de los roles y las funciones de cada subgrupo:

Sanitarios

- Enfermeros
- Médicos (doctores, cirujanos, etc.)
- Especialistas (dietistas, anestesiólogos, radiólogos, cardiólogos, oncólogos, etc.)
- Médicos externos (médicos que no son empleados y empleados de oficina que trabajan desde oficinas remotas)
- Servicios de cuidados a domicilio (empleados de oficina y móviles que desempeñan tareas de cuidado sanitario en visitas a domicilio de los pacientes)
- Especialista en investigación (trabajadores intelectuales y usuarios avanzados en seis institutos de investigación que realizan investigaciones clínicas para buscar respuestas a problemas en Medicina)
- Educación y formación (enfermeros, médicos y especialistas en educación y formación)

No sanitarios

- Servicios compartidos (empleados de oficina que realizan varias funciones administrativas, entre ellas: recursos humanos, nóminas, contabilidad, servicio de cadena de suministro, etc.)
- Servicios médicos (empleados de oficina que realizan diversos servicios de administración de cuidados médicos, servicios administrativos y procesos comerciales para proveedores, incluidos: servicios administrativos, análisis e inteligencia empresarial, sistemas de negocio, servicios al cliente, finanzas, gestión de cuidados realizados, soluciones de acceso a pacientes, soluciones de ciclo de ingresos, etc.)
- Servicios de asistencia técnica (empleados de oficina que realizan varias funciones no clínicas, por ejemplo: gestión de ganancias y beneficios, integración clínica, comunicaciones, compensación y gestión del rendimiento, servicios de instalaciones y propiedades, sistemas de tec-

nología de recursos humanos, servicios de información, auditoría interna y mejora de procesos, etc.)
- Programas filantrópicos (empleados de oficina y móviles que realizan diversas funciones en apoyo a programas filantrópicos)

Contratistas

- Socios de fabricantes y proveedores (in situ y conectados de forma remota a través de la VPN de sitio a sitio, ofrecen varias funciones de asistencia no sanitaria)

En función de la información anterior, la organización crea las siguientes entidades. Para obtener más información acerca de los grupos de entrega en XenMobile, consulte Implementar recursos.

Grupos y unidades organizativas (OU) de Active Directory

Como OU **=** Recursos de XenMobile:

- OU = Sanitarios; Groups =
  - XM-Enfermería
  - XM-Médicos
  - XM-Especialistas
  - XM-Médicos externos
  - XM-Servicios de cuidados a domicilio
  - XM-Especialista en investigación
  - XM-Educación y formación
- OU = No sanitarios; Groups =
  - XM-Servicios compartidos
  - XM-Servicios médicos
  - XM-Servicios de asistencia técnica
  - XM-Programas filantrópicos

Grupos y usuarios locales de XenMobile

Como Group= Contratistas, Users =

- Proveedor1
- Proveedor2
- Proveedor3
- … Proveedor10

Grupos de entrega de XenMobile

- Sanitario-Enfermeros

- Sanitario-Médicos
- Sanitario-Especialistas
- Sanitario-Médicos externos
- Sanitario-Servicios de cuidados a domicilio
- Sanitario-Especialista en investigación
- Sanitario-Educación y formación
- No-Sanitario-Servicios compartidos
- No-Sanitario-Servicios médicos
- No-Sanitario-Servicios de asistencia técnica
- No-Sanitario-Programas filantrópicos

Asignación de grupos de usuario y grupos de entrega

Grupos de Active Directory	Grupos de entrega de XenMobile
XM-Enfermería	Sanitario-Enfermeros
XM-Médicos	Sanitario-Médicos
XM-Especialistas	Sanitario-Especialistas
XM-Médicos externos	Sanitario-Médicos externos
XM-Servicios de cuidados a domicilio	Sanitario-Servicios de cuidados a domicilio
XM-Especialista en investigación	Sanitario-Especialista en investigación
XM-Educación y formación	Sanitario-Educación y formación
XM-Servicios compartidos	No-Sanitario-Servicios compartidos
XM-Servicios médicos	No-Sanitario-Servicios médicos
XM-Servicios de asistencia técnica	No-Sanitario-Servicios de asistencia técnica
XM-Programas filantrópicos	No-Sanitario-Programas filantrópicos

Asignación de recursos y grupos de entrega

En las siguientes tablas, se indican los recursos asignados a cada grupo de entrega en este caso de uso. La primera tabla contiene las asignaciones de aplicaciones móviles. La segunda tabla muestra la aplicación pública, las aplicaciones HDX y los recursos de administración de dispositivos.

Grupos de entrega de XenMobile	Aplicaciones móviles de Citrix	Aplicaciones móviles públicas	Aplicaciones móviles HDX
Sanitario-Enfermeros	X		
Sanitario-Médicos			
Sanitario-Especialistas			
Sanitario-Médicos externos	X		
Sanitario-Servicios de cuidados a domicilio	X		
Sanitario-Especialista en investigación	X		
Sanitario-Educación y formación		X	X
No-Sanitario-Servicios compartidos		X	X
No-Sanitario-Servicios médicos		X	X
No-Sanitario-Servicios de asistencia técnica	X	X	X
No-Sanitario-Programas filantrópicos	X	X	X
Contratistas	X	X	X

Grupos de entrega de XenMobile	Aplicación pública: RSA SecurID	Aplicación pública: EpicCare Haiku	Aplicación HDX: Epic Hyperspace	Directiva de código de acceso	Restriccior de dispositivo	Acciones automatizadas	Directiva de Wi-Fi
Sanitario-Enfermeros							X
Sanitario-Médicos					X		
Sanitario-Especialistas							
Sanitario-Médicos externos							
Sanitario-Servicios de cuidados a domicilio							
Sanitario-Especialista en investigación							
Sanitario-Educación y formación		X	X				
No-Sanitario-Servicios compartidos		X	X				

No-Sanitario-Servicios médicos	X	X
No-Sanitario-Servicios de asistencia técnica	X	X

Notas y consideraciones

- XenMobile crea un grupo de entrega predeterminado llamado AllUsers (Todos los usuarios) durante la configuración inicial. Si no inhabilita este grupo de entrega, todos los usuarios de Active Directory tendrán derecho a inscribirse en XenMobile.
- XenMobile sincroniza los grupos y los usuarios de Active Directory a demanda mediante una conexión dinámica al servidor LDAP.
- Si un usuario forma parte de un grupo que no está asignado en XenMobile, dicho usuario no podrá inscribirse. Del mismo modo, si un usuario es miembro de múltiples grupos, XenMobile clasificará al usuario como perteneciente solo a los grupos asignados a XenMobile.
- Para que la inscripción MDM sea obligatoria, debe establecer la opción Inscripción requerida en Verdadero en las Propiedades de servidor de la consola de XenMobile. Para obtener más información, consulte Propiedades de servidor.
- Para eliminar un grupo de usuarios de un grupo de entrega de XenMobile, elimine la entrada en la base de datos de SQL Server, en dbo.userlistgrps.
  Precaución: Antes de realizar esta acción, cree una copia de seguridad de XenMobile y la base de datos.

Acerca de la pertenencia de dispositivos en XenMobile

Puede agrupar a los usuarios en función del propietario de un dispositivo de usuario. La propiedad de un dispositivo puede ser de la empresa o del usuario; esta última también se conoce como uso de dispositivos personales en el trabajo (bring your own device, BYOD). Puede gestionar la manera en que los dispositivos de los usuarios se conectan a la red desde dos lugares de la consola de XenMobile: las reglas de implementación para cada tipo de recurso y las propiedades del servidor en la página **Parámetros**. Para obtener más información acerca de las reglas de implementación, consulte Con-

figurar reglas de implementación en la documentación de XenMobile. Para obtener más información sobre las propiedades de servidor, consulte Propiedades de servidor.

Puede requerir que los usuarios con dispositivos BYOD acepten que la empresa administre sus dispositivos para poder acceder a las aplicaciones. O bien, puede permitir a los usuarios acceder a las aplicaciones de empresa sin administrar sus dispositivos.

Si establece la propiedad de servidor **wsapi.mdm.required.flag** en **verdadero**, XenMobile administra todos los dispositivos BYOD y niega el acceso a las aplicaciones a todo usuario que rechace la inscripción. Puede establecer **wsapi.mdm.required.flag** en **true** en entornos en que los equipos de TI de la empresa necesitan niveles altos de seguridad y una buena experiencia de usuario al inscribir dispositivos de usuario en XenMobile.

Si deja **wsapi.mdm.required.flag** en **false** (la configuración predeterminada), los usuarios pueden rechazar la inscripción sin, por ello, perder el acceso a las aplicaciones en sus dispositivos a través de XenMobile Store. Puede establecer **wsapi.mdm.required.flag** en **false** en entornos en que las restricciones de privacidad, legales o normativas no requieren la administración de dispositivos, sino solo la administración de las aplicaciones de empresa.

Los usuarios cuyos dispositivos no administre XenMobile no pueden instalarse aplicaciones a través de XenMobile Store. En lugar de controles a nivel de dispositivo (como el borrado completo o selectivo de datos), se puede controlar el acceso a las aplicaciones a través de directivas de aplicaciones. Las directivas, según los valores que se establezcan, requieren que el dispositivo consulte frecuentemente XenMobile Server para confirmar que las aplicaciones aún se pueden ejecutar.

Requisitos de seguridad

La cantidad de consideraciones de seguridad al implementar un entorno de XenMobile puede convertirse rápidamente en abrumadora. Hay muchas piezas y parámetros interconectados. Para ayudarle a ponerse en marcha y elegir un nivel aceptable de protección, Citrix ofrece recomendaciones para un nivel de seguridad alto, superior y máximo, como se describe en la siguiente tabla

La seguridad por sí sola no debería dictar la elección del modo de implementación. También es importante revisar los requisitos del caso de uso y decidir si puede mitigar los problemas de seguridad antes de elegir el modo de implementación.

Alto: Usar estas configuraciones proporciona una experiencia de usuario óptima, al mismo tiempo que se mantiene un nivel básico de seguridad aceptable para la mayoría de las organizaciones.

Superior: Estas configuraciones logran un mayor equilibrio entre seguridad y usabilidad.

Máximo: Seguir estas recomendaciones proporciona un alto nivel de seguridad a costa de la usabilidad y el aumento de la cantidad de usuarios.

Consideraciones sobre seguridad en el modo de implementación

La siguiente tabla contiene los modos de implementación para cada nivel de seguridad.

High Security (Nivel alto de seguridad)	Higher Security (Mayor nivel de seguridad)	Highest Security (El mayor nivel de seguridad)
MAM o MDM	MDM+MAM	MDM+MAM; más FIPS

Notas:

- Dependiendo del caso de uso, una implementación de solo MDM o solo MAM puede satisfacer los requisitos de seguridad y proporcionar una buena experiencia de usuario.
- Si no necesita contenedores de aplicaciones, redes micro VPN ni directivas específicas de aplicación, MDM es suficiente para administrar y proteger los dispositivos.
- Para casos de uso como BYOD, donde los contenedores de aplicaciones por sí solos pueden satisfacer todos los requisitos de empresa y de seguridad, Citrix recomienda el modo solo MAM.
- Para entornos de alta seguridad (y dispositivos que distribuyan las empresas), Citrix recomienda MDM+MAM para utilizar todas las capacidades de seguridad disponibles. Asegúrese de aplicar la inscripción MDM.
- Opciones de FIPS para entornos con las necesidades de seguridad máxima, como el gobierno.

Si habilita el modo FIPS, debe configurar SQL Server para cifrar el tráfico SQL.

Consideraciones sobre la seguridad de Citrix ADC y Citrix Gateway

La siguiente tabla contiene recomendaciones de Citrix ADC y Citrix Gateway para cada nivel de seguridad.

High Security (Nivel alto de seguridad)	Higher Security (Mayor nivel de seguridad)	Highest Security (El mayor nivel de seguridad)

Se recomienda Citrix ADC. Se requiere Citrix Gateway para MAM y ENT; se recomienda para MDM.	Configuración estándar del asistente de Citrix ADC para XenMobile con puente SSL si XenMobile está en la zona DMZ. O descarga de SSL si es necesario para cumplir con los estándares de seguridad cuando XenMobile Server se encuentra en la red interna.	Descarga de SSL con cifrado de extremo a extremo

Notas:

- Exponer XenMobile Server a Internet a través de NAT o de equilibradores de carga y proxy de terceros puede ser una opción para MDM. Sin embargo, esa configuración requiere que el tráfico SSL termine en XenMobile Server, lo que supone un riesgo potencial para la seguridad.
- Para entornos de alta seguridad, Citrix ADC con la configuración predeterminada de XenMobile cumple o supera normalmente los requisitos de seguridad.
- Para entornos MDM con exigencias de seguridad máxima, la finalización de SSL en Citrix ADC permite inspeccionar el tráfico en el perímetro y mantiene el cifrado SSL de extremo a extremo.
- Opciones para definir cifrados SSL/TLS.
- El hardware SSL FIPS de Citrix ADC también está disponible.
- Para obtener más información, consulte Integrar en Citrix Gateway y Citrix ADC.

Consideraciones sobre seguridad para la inscripción

La siguiente tabla contiene recomendaciones de Citrix ADC y Citrix Gateway para cada nivel de seguridad.

High Security (Nivel alto de seguridad)	Higher Security (Mayor nivel de seguridad)	Highest Security (El mayor nivel de seguridad)
Solo miembros del grupo de Active Directory. Inhabilitado el grupo de entrega Todos los usuarios.	Modo de seguridad de inscripción solo por invitación. Solo miembros del grupo de Active Directory. Inhabilitado el grupo de entrega Todos los usuarios.	Modo de seguridad de inscripción vinculado al ID del dispositivo. Solo miembros del grupo de Active Directory. Inhabilitado el grupo de entrega Todos los usuarios.

Notas:

- Por regla general, Citrix recomienda que restrinja la inscripción a solamente aquellos usuarios que formen parte de los grupos predefinidos de Active Directory. Esa configuración requiere inhabilitar el grupo de entrega integrado Todos los usuarios.
- Puede utilizar las invitaciones de inscripción para restringir la inscripción a los usuarios que tengan una invitación. Las invitaciones de inscripción no están disponibles para dispositivos Windows.
- Puede usar invitaciones de inscripción con PIN de un solo uso (OTP) como una solución de dos factores. Así también puede controlar la cantidad de dispositivos que un usuario puede inscribir Las invitaciones de OTP no están disponibles para dispositivos Windows.

Consideraciones sobre la seguridad de los códigos de acceso de dispositivo

Esta tabla contiene las recomendaciones para el código de acceso de dispositivo en cada nivel de seguridad.

High Security (Nivel alto de seguridad)	Higher Security (Mayor nivel de seguridad)	Highest Security (El mayor nivel de seguridad)
Recomendado. Se requiere un nivel alto de seguridad para el cifrado a nivel de dispositivo. Aplicado mediante el uso de MDM. Puede establecer un nivel alto de seguridad como obligatorio solo para MAM mediante la directiva MDX Comportamiento de dispositivos no conformes.	Aplicado mediante directiva MDM, MDX o ambas.	Aplicado mediante directiva MDM y MDX. Directiva MDM “Código de acceso complejo”.

Notas:

- Citrix recomienda usar un código de acceso de dispositivo.
- Puede aplicar un código de acceso de dispositivo a través de una directiva MDM.
- Puede usar una directiva MDX para requerir un código de acceso de dispositivo al usar aplicaciones administradas. Por ejemplo, para casos de uso de dispositivos personales en el trabajo (BYOD).

- Citrix recomienda combinar las opciones de directivas MDM y MDX para una mayor seguridad en los entornos MDM+MAM.
- Para entornos con los requisitos máximos de seguridad, puede configurar directivas "Código de acceso complejo" y aplicarlas con MDM. Puede configurar acciones automáticas que notifiquen a los administradores, o puede emitir borrados selectivos o completos cuando un dispositivo no cumple una directiva de código de acceso.

Aplicaciones

January 4, 2022

La administración de movilidad empresarial (EMM) se divide en la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM). Si bien MDM permite a las organizaciones proteger y controlar dispositivos móviles, MAM facilita la administración y la entrega de aplicaciones. Para posibilitar la adopción de un entorno BYOD, puede implementar una solución MAM, como XenMobile, que sirva de ayuda para lo siguiente:

- entrega de aplicaciones
- licencias de software
- configuración
- administración del ciclo de vida de las aplicaciones

Puede requerir o permitir que los usuarios opten también por la administración MDM.

Con XenMobile, puede ir más allá y proteger estas aplicaciones mediante directivas MAM y configuraciones de VPN específicas para evitar filtraciones de datos y otras amenazas a la seguridad. XenMobile proporciona a las organizaciones la flexibilidad necesaria para implementar su solución como:

- Entorno de solo MAM
- Entorno de solo MDM
- entorno unificado de XenMobile Enterprise con funcionalidad MDM y MAM

Además de la capacidad de entregar aplicaciones a los dispositivos móviles, XenMobile ofrece la contenedorización de aplicaciones a través de la tecnología MDX. Las aplicaciones están sujetas a controles concisos basados en directivas. Los proveedores de software independientes (ISV) pueden aplicar estos controles mediante el Mobile Apps SDK.

En un entorno corporativo, los usuarios utilizan una variedad de aplicaciones móviles para desempeñar su trabajo. Las aplicaciones pueden ser: aplicaciones procedentes de la tienda pública, aplicaciones propias desarrolladas internamente o aplicaciones nativas. XenMobile clasifica estas aplicaciones de la siguiente manera:

- **Aplicaciones públicas:** Este grupo contiene las aplicaciones, gratuitas o de pago, disponibles en una tienda pública de aplicaciones, como App Store de Apple o Google Play. Los proveedores

externos a la organización suelen poner sus aplicaciones disponibles en las tiendas públicas de aplicaciones. Esta opción permite a sus clientes descargar las aplicaciones directamente desde Internet. Puede utilizar varias aplicaciones públicas en su organización, según las necesidades de los usuarios. GoToMeeting, Salesforce y EpicCare son ejemplos de tales aplicaciones.

  - **Si utiliza el SDK de MAM:** Obtenga los binarios de aplicación de su proveedor de aplicaciones. A continuación, integre el SDK de MAM en la aplicación.
  - **Si utiliza MDX Toolkit:** Citrix no admite la descarga de archivos binarios de aplicación directamente desde tiendas públicas de aplicaciones y, a continuación, su empaquetado con el MDX Toolkit para la distribución empresarial. Para empaquetar aplicaciones de terceros, debe colaborar con su proveedor de aplicaciones para obtener los archivos binarios de aplicación. A continuación, podrá empaquetar esos archivos binarios con MDX Toolkit.

- **Aplicaciones internas:** Muchas organizaciones tienen desarrolladores internos que crean aplicaciones con una funcionalidad específica y que se desarrollan y distribuyen de manera independiente dentro de la organización. En ciertos casos, algunas organizaciones también pueden tener aplicaciones proporcionadas por los ISV. Puede implementar esas aplicaciones como nativas, o puede colocarlas en un contenedor con una solución MAM, como XenMobile.

  Por ejemplo, una organización de asistencia sanitaria puede crear una aplicación interna que permita a los médicos ver la información del paciente en dispositivos móviles. A continuación, esa organización puede proteger la información del paciente y habilitar el acceso por VPN a la base de datos de pacientes mediante uno de los siguientes procedimientos:

  - SDK de MAM
  - MDX Toolkit

- **Aplicaciones web y SaaS:** Este grupo incluye aquellas aplicaciones a las que se puede acceder a través de una red interna (aplicaciones web) o a través de una red pública (aplicaciones SaaS). XenMobile también permite crear aplicaciones web y SaaS personalizadas mediante una lista de conectores de aplicaciones. Esos conectores de aplicaciones pueden facilitar el inicio Single Sign-On (SSO) en las aplicaciones web existentes. Para obtener más información, consulte Tipos de conectores de aplicaciones. Por ejemplo, puede usar Google Apps SAML para Single Sign-On basado en SAML (Security Assertion Markup Language) en aplicaciones de Google Apps.

- **Aplicaciones móviles de productividad:** Se trata de aplicaciones desarrolladas por Citrix que se incluyen con la licencia de XenMobile. Para obtener más información, consulte Acerca de las aplicaciones móviles de productividad. Citrix también ofrece otras aplicaciones de negocio que los ISV desarrollan mediante el Mobile Apps SDK.

- **Aplicaciones HDX:** Se trata de aplicaciones alojadas en Windows que se publican con StoreFront. Si utiliza Citrix Virtual Apps and Desktops y Citrix Workspace, las aplicaciones HDX están disponibles para los usuarios inscritos.

La configuración y la arquitectura subyacentes pueden variar en función del tipo de aplicaciones móviles que se van a implementar y administrar a través de XenMobile. Por ejemplo, varios grupos de usuarios con diferentes niveles de permisos utilizan una sola aplicación. En ese caso, puede crear grupos de entrega independientes para implementar dos versiones separadas de la misma aplicación. Además, deberá asegurarse de que la pertenencia a cada grupo de usuarios se excluya mutuamente, para evitar discrepancias entra las directivas que se apliquen a los dispositivos de los usuarios.

También puede administrar las licencias de las aplicaciones iOS a través de las compras por volumen de Apple. Para poder utilizar esta opción, deberá registrarse en el Programa de compras por volumen y definir los parámetros de compras por volumen desde la consola de XenMobile. Esta configuración permite distribuir las aplicaciones con las licencias de compras por volumen. Dada la variedad de casos de uso, es importante analizar y planificar la estrategia de MAM que va a seguir antes de implementar el entorno de XenMobile. Para comenzar a planificar su estrategia de MAM, defina lo siguiente:

- **Tipos de aplicaciones:** Indique los diferentes tipos de aplicaciones que quiere admitir y clasifíquelas por categorías (por ejemplo, aplicaciones públicas, nativas, web, internas o ISV). Además, clasifique las aplicaciones según las diferentes plataformas de dispositivo (como iOS y Android). Esta categorización ayudará a encajar los distintos parámetros de XenMobile que se requieren para cada tipo de aplicación. Por ejemplo, algunas aplicaciones pueden requerir el uso del Mobile Apps SDK a fin de habilitar unas API especiales para la interacción con otras aplicaciones.
- **Requisitos de red:** Deberán configurarse los parámetros de las aplicaciones que tengan requisitos específicos de acceso a la red. Por ejemplo, ciertas aplicaciones pueden necesitar acceder a la red interna por VPN. En cambio, otras aplicaciones pueden requerir que el acceso a Internet se enrute a través de la zona DMZ. Para permitir que esas aplicaciones se conecten a la red requerida, debe configurar varios parámetros según corresponda. Definir unos requisitos de red por aplicación contribuye a precisar sus decisiones arquitectónicas desde el principio, lo que optimiza el proceso general de implementación.
- **Requisitos de seguridad:** Puede definir requisitos de seguridad que se aplicarán a aplicaciones individuales o a todas las aplicaciones.
  - Las configuraciones, como las directivas MDX, se aplican a aplicaciones individuales
  - Las configuraciones de sesión y autenticación se aplican a todas las aplicaciones
  - Algunas aplicaciones pueden presentar requisitos específicos de contenedorización, MDX, autenticación, geocercas, código de acceso o uso compartido de datos.

  Debe prever esos requisitos para facilitar la implementación. Para obtener más información sobre la seguridad en Endpoint Management, consulte Seguridad y experiencia de usuario.
- **Requisitos de implementación:** Puede que le interese una implementación basada en directivas si quiere permitir que solo los usuarios conformes descarguen las aplicaciones publicadas. Por ejemplo, es posible que ciertas aplicaciones necesiten que el dispositivo esté administrado

o que tengan instalada una versión mínima del sistema operativo. También puede interesarle que ciertas aplicaciones estén disponibles solo para usuarios de empresa. Debe esbozar dichos requisitos con antelación para configurar las acciones o las reglas de implementación apropiadas.

- **Requisitos de licencia:** Conserve un registro de los requisitos de licencia relacionados con las aplicaciones. Las notas pueden servirle de ayuda para administrar de manera efectiva el uso de las licencias y decidir si configurar funciones específicas en XenMobile para optimizar la gestión de licencias. Por ejemplo, si implementa una aplicación iOS gratuita o de pago, Apple aplica requisitos de licencia a la aplicación, lo que obliga a los usuarios a iniciar sesión en su cuenta de App Store.

  Sin embargo, puede registrarse en el Programa de compras por volumen de Apple para distribuir y administrar esas aplicaciones a través de XenMobile. El Programa de compras por volumen permite a los usuarios descargar las aplicaciones sin tener que iniciar sesión en la cuenta del App Store.

  Algunas plataformas (como Samsung SAFE y Samsung Knox) presentan requisitos especiales de licencia que debe cumplir antes de implementar esas funciones.

- **Requisitos de lista de aplicaciones permitidas o bloqueadas:** Puede identificar las aplicaciones que no quiere que los usuarios se instalen o usen. Para empezar, cree una lista donde defina un evento de incumplimiento que será motivo de bloqueo. A continuación, configure directivas para que se activen cuando se produzca el evento. Por otro lado, puede que acepte el uso de una aplicación, pero esta se incluya en la lista de bloqueo por alguna razón. En ese caso, puede agregar la aplicación a una lista de aplicaciones permitidas e indicar que se puede usar, pero no es obligatoria. Además, tenga en cuenta que las aplicaciones ya instaladas en los dispositivos nuevos pueden incluir algunas aplicaciones de uso común que no forman parte del sistema operativo. Estas aplicaciones pueden entrar en conflicto con su estrategia de listas de aplicaciones bloqueadas.

Caso de uso

Una organización de asistencia sanitaria quiere implementar XenMobile como solución MAM para sus aplicaciones móviles. Las aplicaciones móviles se entregan a usuarios de empresa y usuarios BYOD. El departamento de TI decide entregar y administrar las siguientes aplicaciones:

Aplicaciones móviles de productividad: Aplicaciones iOS y Android que proporciona Citrix. Para obtener más información, consulte Aplicaciones móviles de productividad.

Citrix Secure Hub: Cliente que utilizan todos los dispositivos móviles para comunicarse con XenMobile. Los parámetros de seguridad, las configuraciones y las aplicaciones móviles se envían a los dispositivos móviles a través de Secure Hub. Los dispositivos Android y iOS se inscriben en XenMobile a través de Secure Hub.

Citrix Receiver: Aplicación móvil que permite a los usuarios de dispositivos móviles abrir aplicaciones alojadas en Citrix Virtual Apps.

GoToMeeting: Un cliente de reuniones en línea, uso compartido de escritorios y videoconferencias que permite a los usuarios reunirse con clientes, colegas u otros usuarios de equipos a través de Internet en tiempo real.

SalesForce1: Permite a los usuarios acceder a Salesforce desde dispositivos móviles, y reúne todos los procesos de negocio y las aplicaciones personalizadas, Chatter y CRM, en una experiencia unificada para cualquier usuario de Salesforce.

RSA SecurID: Token basado en software para la autenticación de dos factores.

Aplicaciones EpicCare: Estas aplicaciones ofrecen a los profesionales de la salud un acceso seguro y portátil a los gráficos de pacientes, las listas de pacientes, los horarios y los mensajes.

Haiku: Aplicación móvil para teléfonos Android y iPhone.

Canto: Aplicación móvil para el iPad.

Rover: Aplicaciones móviles para iPhone y iPad.

HDX: Citrix Virtual Apps entrega aplicaciones HDX.

- **Epic Hyperspace:** Aplicación cliente de Epic para la administración electrónica de registros de salud.

ISV:

- **Vocera:** Aplicación móvil de mensajería y VoIP compatible con HIPAA, que extiende las ventajas de la tecnología de voz de Vocera para poder aprovecharlas en cualquier momento y cualquier lugar desde smartphones iPhone y Android.

Aplicaciones internas:

- **HCMail:** Aplicación que ayuda a redactar mensajes cifrados, buscar en las libretas de direcciones en servidores de correo interno y enviar los mensajes cifrados a los contactos mediante un cliente de correo electrónico.

Aplicaciones web internas:

- **PatientRounding:** Aplicación web utilizada para registrar la información sanitaria del paciente por diferentes departamentos.
- **Outlook Web Access:** Permite el acceso al correo electrónico a través de un explorador web.
- **SharePoint:** Se usa para compartir archivos y datos por toda la organización.

En la tabla siguiente, se muestra la información básica necesaria para la configuración de MAM.

Nombre de la aplicación	Tipo de aplicación	Integración del SDK de MAM o empaquetado MDX	iOS	Android
Secure Mail	Aplicación XenMobile	No a partir de la versión 10.4.1	Sí	Sí
Secure Web	Aplicación XenMobile	No a partir de la versión 10.4.1	Sí	Sí
Citrix Files	Aplicación XenMobile	No a partir de la versión 10.4.1	Sí	Sí
Secure Hub	Aplicación pública	N/D	Sí	Sí
Citrix Receiver	Aplicación pública	N/D	Sí	Sí
GoToMeeting-	Aplicación pública	N/D	Sí	Sí
SalesForce1	Aplicación pública	N/D	Sí	Sí
RSA SecurID	Aplicación pública	N/D	Sí	Sí
Epic Haiku	Aplicación pública	N/D	Sí	Sí
Epic Canto	Aplicación pública	N/D	Sí	No
Epic Rover	Aplicación pública	N/D	Sí	No
Epic Hyperspace	Aplicación HDX	N/D	Sí	Sí
Vocera	Aplicación de ISV	Sí	Sí	Sí
HCMail	Aplicación interna	Sí	Sí	Sí
PatientRounding	Aplicación web	N/D	Sí	Sí
Outlook Web Access	Aplicación web	N/D	Sí	Sí

SharePoint	Aplicación web	N/D	Sí	Sí

En la siguiente tabla, se ofrece una lista de los requisitos específicos que puede consultar para la configuración de directivas MAM en XenMobile.

Nombre de la aplicación	Se requiere VPN	Interacción (con aplicaciones fuera del contenedor)	Interacción (desde aplicaciones fuera del contenedor)	Filtrado de proxy	Licencias	Geocerca	Mobile Apps SDK	Versión mínima del sistema operativo
Secure Mail	S	Se permite de manera selectiva	Se permite	Si son necesarias	N/D	Se requiere de manera selectiva	N/D	Se aplica
Secure Web	S	Se permite	Se permite	Si son necesarias	N/D	No se requiere	N/D	Se aplica
Citrix Files	S	Se permite	Se permite	Si son necesarias	N/D	No se requiere	N/D	Se aplica
Secure Hub	S	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Citrix Receiver	S	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
GoToMeeting	No	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica

Nombre de la aplicación	Se requiere VPN	Interacción (con aplicaciones fuera del contenedor)	Interacción (desde aplicaciones fuera del contenedor)	Filtrado de proxy	Licencias	Geocerca	Mobile Apps SDK	Versión mínima del sistema operativo
SalesForc	N	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
RSA SecurID	N	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Haiku	S	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Canto	S	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Rover	S	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Hyperspace	S	N/D	N/D	No se requiere	N/D	No se requiere	N/D	No se aplica
Vocera	S	Bloquead	Bloqueac	Si son necesarias	N/D	Si son necesarias	Si son necesarias	Se aplica
HCMail	S	Bloqueada	Bloqueada	Si son necesarias	N/D	Si son necesarias	Si son necesarias	Se aplica
PatientRc	S	N/D	N/D	Si son necesarias	N/D	No se requiere	N/D	No se aplica

Nombre de la aplicación	Se requiere VPN	Interacción (con aplicaciones fuera del contenedor)	Interacción (desde aplicaciones fuera del contenedor)	Filtrado de proxy	Licencias	Geocerca	Mobile Apps SDK	Versión mínima del sistema operativo
Outlook Web Access	S	N/D	N/D	Si son necesarias	N/D	No se requiere	N/D	No se aplica
SharePoi	S	N/D	N/D	Si son necesarias	N/D	No se requiere	N/D	No se aplica

Comunidades de usuarios

January 4, 2022

Cada organización consta de diversas comunidades de usuarios que operan en diferentes roles funcionales. Estas comunidades de usuarios realizan diferentes tareas y funciones de oficina mediante diversos recursos que usted proporciona a través de los dispositivos móviles de esos usuarios. Los usuarios pueden trabajar desde casa o en oficinas remotas mediante dispositivos móviles que usted proporcione. O bien, los usuarios pueden usar dispositivos móviles personales, lo que les permite acceder a herramientas que están sujetas a ciertas reglas de seguridad.

Con la cantidad creciente de comunidades de usuarios que usan dispositivos móviles, la administración Enterprise Mobility Management (EMM) se ha convertido en un elemento vital para evitar la filtración de datos y para hacer cumplir las restricciones de seguridad de la organización. Para una administración eficiente y más sofisticada de dispositivos móviles, puede categorizar sus comunidades de usuarios. Al hacerlo, se simplifica la asignación de usuarios a los recursos y se garantiza que se apliquen las directivas de seguridad correspondientes a los usuarios indicados.

La categorización de las comunidades de usuarios puede incluir el uso de los siguientes componentes:

- Grupos y unidades organizativas (OU) de Active Directory

  Los usuarios agregados a grupos de seguridad de Active Directory específicos pueden recibir recursos tales como aplicaciones y directivas. Quitar usuarios de los grupos de seguridad de

Active Directory, elimina el acceso que tenían esos usuarios a los recursos de XenMobile previamente permitidos.

- Grupos y usuarios locales de XenMobile

  Para los usuarios que no tienen cuenta de Active Directory, puede crear usuarios locales de XenMobile. Puede agregar usuarios locales a grupos de entrega y aprovisionarles recursos de la misma manera que a los usuarios de Active Directory.

- Grupos de entrega de XenMobile

  Si varios grupos de usuarios con diferentes niveles de permisos utilizan una sola aplicación, puede que le interese crear grupos de entrega independientes. Con grupos de entrega separados, puede implementar dos versiones independientes de la misma aplicación.

- Asignación de grupos de usuario y grupos de entrega

  Las asignaciones de grupos de entrega a grupos de Active Directory pueden ser uno a uno, o uno a varios. Asigne aplicaciones y directivas base a grupos de entrega. La asignación puede ser de tipo “de uno a varios”, es decir una aplicación y directiva base se pueden asignar a varios grupos de entrega. Asigne aplicaciones y directivas específicas por función a las asignaciones uno a uno de grupos de entrega.

- Asignación de aplicaciones por recursos y grupos de entrega

  Asigne aplicaciones específicas a cada grupo de entrega.

- Asignación de recursos MDM por recursos y grupos de entrega

  Asigne aplicaciones y recursos de administración de dispositivos específicos a cada grupo de entrega. Por ejemplo: Configure un grupo de entrega con cualquier combinación de las siguientes acciones: tipos de aplicaciones (públicas, HDX, etc.), aplicaciones específicas por tipo de aplicación y recursos (como directivas de dispositivo y acciones automatizadas).

El siguiente ejemplo ilustra cómo se clasifican para EMM las comunidades de usuarios de una organización de asistencia sanitaria.

Caso de uso

Esta organización sanitaria de ejemplo ofrece recursos tecnológicos y acceso a varios usuarios, incluidos los voluntarios, los empleados en la red y los empleados asociados. La organización ha decidido aplicar la solución EMM solo para usuarios no ejecutivos.

En esta organización, las funciones y los roles se pueden dividir en estos subgrupos: sanitarios, no sanitarios y contratistas. Un conjunto seleccionado de los usuarios recibe dispositivos móviles de empresa, mientras que otras personas pueden acceder a recursos limitados de la empresa desde sus dispositivos personales (BYOD). Para hacer cumplir el nivel apropiado de restricciones de seguridad

y evitar la filtración de datos, la organización decidió que el departamento de TI corporativo administrara cada dispositivo inscrito. Además, los usuarios pueden inscribir un solo dispositivo.

Las siguientes secciones ofrecen una descripción general de los roles y las funciones de cada subgrupo:

Sanitarios

- Enfermeros
- Médicos (doctores, cirujanos, etc.)
- Especialistas (dietistas, flebotomistas, anestesiólogos, radiólogos, cardiólogos, oncólogos, etc.)
- Médicos externos (médicos que no son empleados y empleados de oficina que trabajan desde oficinas remotas)
- Servicios de cuidados a domicilio (empleados de oficina y móviles que desempeñan tareas de cuidado sanitario en visitas a domicilio de los pacientes)
- Especialista en investigación (trabajadores intelectuales y usuarios avanzados en seis institutos de investigación que realizan investigaciones clínicas para buscar respuestas a problemas en Medicina)
- Educación y formación (enfermeros, médicos y especialistas en educación y formación)

No sanitarios

- Servicios compartidos (empleados de oficina que realizan varias funciones administrativas, entre ellas: recursos humanos, nóminas, contabilidad, servicio de cadena de suministro, etc.)
- Servicios médicos (empleados de oficina que realizan diversos servicios de administración de cuidados médicos, servicios administrativos y procesos comerciales para proveedores, incluidos: servicios administrativos, análisis e inteligencia empresarial, sistemas de negocio, servicios al cliente, finanzas, gestión de cuidados realizados, soluciones de acceso a pacientes, soluciones de ciclo de ingresos, etc.)
- Servicios de asistencia técnica (empleados de oficina que realizan varias funciones no clínicas, por ejemplo: gestión de ganancias y beneficios, integración clínica, comunicaciones, compensación y gestión del rendimiento, servicios de instalaciones y propiedades, sistemas de tecnología de recursos humanos, servicios de información, auditoría interna y mejora de procesos, etc.).
- Programas filantrópicos (empleados de oficina y móviles que realizan diversas funciones en apoyo a programas filantrópicos)

Contratistas

- Socios de fabricantes y proveedores (in situ y conectados de forma remota a través de la VPN de sitio a sitio, ofrecen varias funciones de asistencia no sanitaria)

En función de la información anterior, la organización crea las siguientes entidades. Para obtener más información acerca de los grupos de entrega en XenMobile, consulte Implementar recursos en la documentación de producto de XenMobile.

Grupos y unidades organizativas (OU) de Active Directory

Como OU = Recursos de XenMobile

- OU = Sanitarios; Groups =
  - XM-Enfermería
  - XM-Médicos
  - XM-Especialistas
  - XM-Médicos externos
  - XM-Servicios de cuidados a domicilio
  - XM-Especialista en investigación
  - XM-Educación y formación
- OU = No sanitarios; Groups =
  - XM-Servicios compartidos
  - XM-Servicios médicos
  - XM-Servicios de asistencia técnica
  - XM-Programas filantrópicos

Grupos y usuarios locales de XenMobile

Como Group= Contratistas, Users =

- Proveedor1
- Proveedor2
- Proveedor3
- … Proveedor10

Grupos de entrega de XenMobile

- Sanitario-Enfermeros
- Sanitario-Médicos
- Sanitario-Especialistas
- Sanitario-Médicos externos
- Sanitario-Servicios de cuidados a domicilio
- Sanitario-Especialista en investigación
- Sanitario-Educación y formación
- No-Sanitario-Servicios compartidos

- No-Sanitario-Servicios médicos
- No-Sanitario-Servicios de asistencia técnica
- No-Sanitario-Programas filantrópicos

Asignación de grupos de usuario y grupos de entrega

Grupos de Active Directory	Grupos de entrega de XenMobile
XM-Enfermería	Sanitario-Enfermeros
XM-Médicos	Sanitario-Médicos
XM-Especialistas	Sanitario-Especialistas
XM-Médicos externos	Sanitario-Médicos externos
XM-Servicios de cuidados a domicilio	Sanitario-Servicios de cuidados a domicilio
XM-Especialista en investigación	Sanitario-Especialista en investigación
XM-Educación y formación	Sanitario-Educación y formación
XM-Servicios compartidos	No-Sanitario-Servicios compartidos
XM-Servicios médicos	No-Sanitario-Servicios médicos
XM-Servicios de asistencia técnica	No-Sanitario-Servicios de asistencia técnica
XM-Programas filantrópicos	No-Sanitario-Programas filantrópicos

Asignación de aplicaciones por recursos y grupos de entrega

	Secure Mail	Secure Web	ShareFil	Receiver	SalesFor	RSA Se-curID	EpicCare Haiku	Epic Hyper-space
Sanitario-Enfermeros	X	X	X					
Sanitario-Médicos								
Sanitario-Especialistas								

Sanitario· Médicos exter-nos	X	X			
Sanitario- Servicios de cuida-dos a domi-cilio	X	X			
Sanitario· Especialis en investi-gación	X	X			
Sanitario- Educación y forma-ción				X	X
No-Sanitario· Servicios com-par-tidos				X	X
No-Sanitario- Servicios médi-cos				X	X

No-Sanitario-Servicios de asistencia técnica	X		X			X	X
No-Sanitario-Programas filantrópicos	X		X			X	X
Contratis	X		X	X	X	X	X

Asignación de recursos MDM por recursos y grupos de entrega

	MDM: Directiva de código de acceso	MDM: Restricciones de dispositivo	MDM: Acciones automatizadas	MDM: Directiva de Wi-Fi
Sanitario-Enfermeros				X
Sanitario-Médicos		X		
Sanitario-Especialistas				
Sanitario-Médicos externos				
Sanitario-Servicios de cuidados a domicilio				

Sanitario-Especialista en investigación	
Sanitario-Educación y formación	
No-Sanitario-Servicios compartidos	
No-Sanitario-Servicios médicos	
No-Sanitario-Servicios de asistencia técnica	
No-Sanitario-Programas filantrópicos	
Contratistas	X

Notas y consideraciones

- XenMobile crea un grupo de entrega predeterminado llamado AllUsers (Todos los usuarios) durante la configuración inicial. Si no inhabilita este grupo de entrega, todos los usuarios de Active Directory tendrán derecho a inscribirse en XenMobile.
- XenMobile sincroniza los grupos y los usuarios de Active Directory a demanda mediante una conexión dinámica al servidor LDAP.
- Si un usuario forma parte de un grupo que no está asignado en XenMobile, dicho usuario no podrá inscribirse. Del mismo modo, si un usuario es miembro de múltiples grupos, XenMobile solo clasificará al usuario como perteneciente a los grupos asignados a XenMobile.
- Para que la inscripción MDM sea obligatoria, establezca la opción **Inscripción requerida** en **Verdadero** en las **Propiedades de servidor** de la consola de XenMobile. Para obtener más información, consulte Propiedades de servidor.

- Para eliminar un grupo de usuarios de un grupo de entrega de XenMobile, elimine la entrada en la base de datos de SQL Server, en dbo.userlistgrps.

> **Precaución:**
>
> Antes de realizar esta acción, cree una copia de seguridad de XenMobile y la base de datos.

Acerca de la pertenencia de dispositivos en XenMobile

Puede agrupar a los usuarios en función del propietario de un dispositivo de usuario. La propiedad de un dispositivo puede ser de la empresa o del usuario; esta última también se conoce como uso de dispositivos personales en el trabajo (bring your own device, BYOD). Puede gestionar la manera en que los dispositivos de los usuarios se conectan a la red desde dos lugares de la consola de XenMobile: la página "Reglas de implementación" y las propiedades del servidor de XenMobile en la página **Parámetros**. Para obtener más información acerca de las reglas de implementación, consulte Implementar recursos en la documentación de XenMobile. Para obtener más información sobre las propiedades de servidor, consulte Propiedades de servidor en este manual.

Al configurar las propiedades de servidor, puede requerir que los usuarios con dispositivo BYOD acepten que la empresa administre sus dispositivos para poder acceder a las aplicaciones. O bien, puede permitir a los usuarios acceder a las aplicaciones de empresa sin administrar sus dispositivos.

Si establece la propiedad de servidor **wsapi.mdm.required.flag** en **verdadero**, XenMobile administrará todos los dispositivos BYOD y negará el acceso a las aplicaciones a todo usuario que rechace la inscripción. Puede establecer **wsapi.mdm.required.flag** en **true** en entornos en que los equipos de TI de la empresa necesitan niveles altos de seguridad y una experiencia de usuario segura durante la inscripción.

Si deja **wsapi.mdm.required.flag** en **false**, que es la opción predeterminada, los usuarios pueden rechazar la inscripción. Sin embargo, pueden acceder aplicaciones en sus dispositivos a través de XenMobile Store. Puede establecer **wsapi.mdm.required.flag** en **false** en entornos en que las restricciones de privacidad, legales o normativas no requieren la administración de dispositivos, sino solo la administración de las aplicaciones de empresa.

Los usuarios cuyos dispositivos no administre XenMobile no pueden instalarse aplicaciones a través de XenMobile Store. En lugar de controles a nivel de dispositivo (como el borrado completo o selectivo de datos), se puede controlar el acceso a las aplicaciones a través de directivas de aplicaciones. Algunas configuraciones de directiva requieren que el dispositivo consulte frecuentemente al servidor de XenMobile para confirmar que las aplicaciones aún se pueden ejecutar.

Estrategia de correo electrónico

January 4, 2022

El acceso seguro al correo electrónico desde dispositivos móviles es uno de los motivos principales detrás de una iniciativa de administración de la movilidad en todas las organizaciones. Decidir la estrategia de correo electrónico adecuada suele ser un componente clave a la hora de diseñar elementos en XenMobile. XenMobile ofrece varias opciones para adaptarse a diferentes casos de uso, en función de la seguridad, la experiencia del usuario y los requisitos de integración. En este artículo se documenta el proceso de toma de decisiones sobre un diseño típico y se indican criterios para elegir la solución adecuada, desde la selección del cliente hasta el flujo del tráfico de correo.

Elegir los clientes de correo electrónico

Generalmente, la elección de un cliente encabeza la lista a la hora de diseñar la estrategia a seguir para el correo electrónico. Puede elegir entre varios clientes: Citrix Secure Mail, el correo nativo que se incluye con el sistema operativo de la plataforma móvil en cuestión, o bien otros clientes de terceros, disponibles a través de las tiendas públicas de aplicaciones. En función de sus necesidades, puede ofrecer soporte a comunidades de usuarios con un solo cliente (estándar) o puede que necesite usar una combinación de clientes.

En la siguiente tabla se describen algunos criterios de diseño para las diferentes opciones de cliente disponibles:

Temática	Secure Mail	Nativo (por ejemplo, iOS Mail)	Correo de terceros
Edición mínima de XenMobile	Avanzado	MDM	MDM

Configuración	Perfiles de cuentas de Exchange configurados a través de una directiva MDX.	Perfiles de cuenta de Exchange configurados a través de una directiva MDM. La compatibilidad con Android está limitada a: SAFE/Knox y Android Enterprise. Todos los demás clientes se consideran clientes de terceros.	Generalmente requiere una configuración manual por parte del usuario.
Seguridad	Seguro gracias a su diseño, con lo que proporciona la seguridad más alta. Utiliza directivas MDX con niveles agregados de cifrado de datos. Secure Mail es una aplicación administrada totalmente a través de una directiva MDX. Capa agregada de autenticación con el PIN de Citrix.	Según el conjunto de funciones del proveedor o la aplicación. Proporciona más seguridad. Utiliza la configuración de cifrado del dispositivo (sin seguridad desde las directivas MDX). Se basa en la autenticación a nivel de dispositivo para acceder a la aplicación.	Según el conjunto de funciones del proveedor o la aplicación. Proporciona alta seguridad.

Integración	Permite la interacción con aplicaciones administradas (MDX) de forma predeterminada. Permite abrir direcciones URL con Citrix Secure Web. Guardar archivos y adjuntarlos desde Citrix Files. Unirse directamente o acceder por teléfono a reuniones en GoToMeeting.	Solo puede interactuar con otras aplicaciones no administradas (que no sean MDX) de forma predeterminada.	Solo puede interactuar con otras aplicaciones no administradas (que no sean MDX) de forma predeterminada.
Implementación o Licencias	Puede enviar Secure Mail a través de MDM, directamente desde las tiendas públicas de aplicaciones. Incluido con las licencias XenMobile Advanced y Enterprise.	La aplicación del cliente, incluida con el sistema operativo de la plataforma. Sin requisitos de licencia adicionales.	Puede enviarse a través de MDM, como una aplicación de empresa o directamente desde las tiendas públicas de aplicaciones. Costes o modelos de licencia asociados según el proveedor de la aplicación.

Asistencia	Soporte del proveedor único para el cliente y la solución de EMM (Citrix). Información de contacto de asistencia integrada en las capacidades del registro de depuración en Secure Hub o la aplicación. Un cliente al que ofrecer soporte.	Soporte definido por el proveedor (Apple o Google). Puede que necesite ofrecer soporte a diferentes clientes, según la plataforma del dispositivo.	Soporte definido por el proveedor. Un cliente al que ofrecer soporte, suponiendo que el cliente de terceros es compatible con todas las plataformas de los dispositivos administrados.

Consideraciones sobre el filtrado y el flujo del tráfico de correo

En esta sección se tratan los tres casos principales y las consideraciones sobre el diseño con respecto al flujo del tráfico de correo (ActiveSync) en el contexto de XenMobile.

Caso 1: Exchange expuesto

Los entornos que admiten clientes externos suelen tener los servicios de Exchange ActiveSync expuestos a Internet. Los clientes móviles de ActiveSync se conectan por esta ruta externa a través de un proxy inverso (por ejemplo, Citrix ADC) o a través de un servidor perimetral. Esta opción es necesaria para usar clientes de correo nativos o de terceros, con lo que estos clientes se convierten en la elección típica en este caso. Aunque sea poco frecuente, también puede usar el cliente de Secure Mail en este caso. Al hacerlo, aprovecha las funciones de seguridad que ofrecen el uso de las directivas MDX y la administración de la aplicación.

Caso 2: Túnel a través de Citrix ADC (micro VPN y STA)

Este es el caso predeterminado cuando se utiliza el cliente de Secure Mail, debido a sus capacidades de micro VPN. En este caso, el cliente de Secure Mail establece una conexión segura con ActiveSync a través de Citrix Gateway. Básicamente, puede considerar Secure Mail como el cliente que se conecta directamente a ActiveSync desde la red interna. Los clientes de Citrix suelen usar Secure Mail como el cliente móvil preferido para ActiveSync. Esa decisión forma parte de una iniciativa para evitar exponer los servicios de ActiveSync a Internet en un servidor Exchange ya expuesto (primer caso descrito).

Solo las aplicaciones habilitadas para el SDK de MAM o empaquetadas con MDX pueden usar la función micro VPN. Este supuesto no es aplicable a los clientes nativos si se utiliza el empaquetado con MDX. Aunque es posible empaquetar clientes de terceros con el MDX Toolkit, no es frecuente. El uso de clientes VPN a nivel de dispositivo para permitir el acceso por túnel a clientes nativos o de terceros ha resultado ser engorroso y no es una solución viable

Caso 3: Servicios de Exchange alojados en la nube

El uso de los servicios de Exchange alojados en la nube, como Microsoft Office 365, está cada vez más extendido. En el contexto de XenMobile, este caso se puede tratar de la misma manera que el primero, porque aquí el servicio ActiveSync también está expuesto a Internet. En este caso, los requisitos del proveedor de servicios en la nube dictan las opciones del cliente. Las opciones suelen ser compatibles con la mayoría de los clientes ActiveSync, como Secure Mail y otros clientes nativos o de terceros.

XenMobile puede agregar valor en tres áreas de este caso:

- Clientes con directivas MDX y administración de aplicaciones con Secure Mail
- Configuración de clientes con una directiva MDM en clientes de correo nativos admitidos
- Opciones de filtrado de ActiveSync mediante el conector de Endpoint Management para Exchange ActiveSync

Consideraciones sobre el filtrado del tráfico de correo

Al igual que con la mayoría de los servicios expuestos a Internet, debe proteger la ruta y proporcionar filtros para el acceso autorizado. La solución XenMobile incluye dos componentes diseñados específicamente para proporcionar las capacidades de filtrado de ActiveSync a clientes nativos y de terceros: conector de Citrix Gateway para Exchange ActiveSync y conector de Endpoint Management para Exchange ActiveSync.

Conector de Citrix Gateway para Exchange ActiveSync

El conector de Citrix Gateway para Exchange ActiveSync ofrece el filtrado de ActiveSync en el perímetro, mediante Citrix ADC como proxy para el tráfico de ActiveSync. Así, el componente de filtrado se encuentra en la ruta de tráfico del correo: lo intercepta a medida que entra o sale del entorno. El conector de Citrix Gateway para Exchange ActiveSync actúa como intermediario entre Citrix ADC y XenMobile Server. Cuando un dispositivo se comunica con Exchange a través del servidor virtual de ActiveSync presente en Citrix ADC, Citrix ADC realiza una llamada HTTP al servicio del conector para Exchange ActiveSync. Ese servicio verifica el estado del dispositivo a través de XenMobile. El conector para Exchange ActiveSync responde a Citrix ADC en función del estado del dispositivo para permitir o denegar la conexión. También se pueden configurar reglas estáticas para filtrar el acceso en función del usuario, el agente, el ID o el tipo de dispositivo.

Esta configuración permite que los servicios Exchange ActiveSync se expongan a Internet con una capa adicional de seguridad para evitar el acceso no autorizado. En las consideraciones sobre el diseño se incluye:

- Servidor de Windows: El componente del conector para Exchange ActiveSync requiere un servidor de Windows.
- Conjunto de reglas de filtrado: El conector para Exchange ActiveSync está diseñado para filtrar según el estado y la información del dispositivo, en lugar de la información del usuario. Aunque puede configurar reglas estáticas para filtrar por ID de usuario, no existen opciones para filtrar según la pertenencia a un grupo de Active Directory, por ejemplo. Si hay un requisito para el filtrado por grupos de Active Directory, puede usar el conector de Endpoint Management para Exchange ActiveSync en su lugar.
- Escalabilidad de Citrix ADC: Dado el requisito de proxy para el tráfico de ActiveSync a través de Citrix ADC, un tamaño adecuado de la instancia de Citrix ADC es fundamental para admitir la carga de trabajo adicional de todas las conexiones SSL de ActiveSync.
- Almacenamiento en caché integrado de Citrix ADC: La configuración del conector para Exchange ActiveSync en Citrix ADC utiliza la función “Almacenamiento en caché integrado” para almacenar en caché las respuestas de este componente. Como resultado de esa configuración, Citrix ADC no necesita emitir ninguna solicitud para el conector de Citrix Gateway para Exchange ActiveSync para cada transacción de ActiveSync en las sesiones. Esa configuración también es vital para un rendimiento y una escala adecuados. El “Almacenamiento en caché integrado” está disponible con Citrix ADC Platinum Edition, o puede licenciar la función por separado para las ediciones Enterprise.
- Directivas de filtrado personalizadas: Puede que necesite crear directivas personalizadas de Citrix ADC para restringir algunos clientes de ActiveSync que no sean los clientes móviles nativos estándar. Esta configuración requiere conocimiento sobre las solicitudes HTTP de ActiveSync y la creación de directivas del respondedor de Citrix ADC.
- Clientes de Secure Mail: Secure Mail ofrece redes micro VPN, que eliminan la necesidad de filtros en el perímetro. Por regla general, el cliente de Secure Mail se trataría como un cliente de ActiveSync interno (de confianza) cuando se conecta a través de Citrix Gateway. Si se necesita la funcionalidad para clientes nativos y de terceros (con el conector para Exchange ActiveSync) y Secure Mail: Citrix recomienda que el tráfico de Secure Mail no fluya a través del servidor virtual de Citrix ADC utilizado para el conector para Exchange ActiveSync. Puede lograr este flujo de tráfico a través de DNS y evitar que la directiva del conector para Exchange ActiveSync afecte a los clientes de Secure Mail.

Para ver un diagrama de Citrix Gateway connector for Exchange ActiveSync en una implementación de XenMobile, consulte Arquitectura de referencia para implementaciones locales.

Conector de Endpoint Management para Exchange ActiveSync

El conector de Endpoint Management para Exchange ActiveSync es un componente de XenMobile que ofrece el filtrado de ActiveSync al nivel de servicio de Exchange. Así, el filtrado solo se produce una vez que el correo haya llegado al servicio de Exchange, en lugar de hacerlo en cuanto entre en el entorno de XenMobile. Mail Manager utiliza PowerShell para consultar Exchange ActiveSync cuando busca información de asociación de dispositivos y para controlar el acceso a través de acciones de cuarentena de dispositivos. Estas acciones ponen los dispositivos en cuarentena, y los sacan de ella, en función de los criterios de las reglas del conector de Endpoint Management para Exchange ActiveSync. De forma similar al conector de Citrix Gateway para Exchange ActiveSync, el conector de Endpoint Management para Exchange ActiveSync comprueba el estado del dispositivo con XenMobile para filtrar el acceso en función de la conformidad del dispositivo. También se pueden configurar reglas estáticas para filtrar el acceso en función del ID o el tipo de dispositivo, la versión del agente y la pertenencia al grupo de Active Directory.

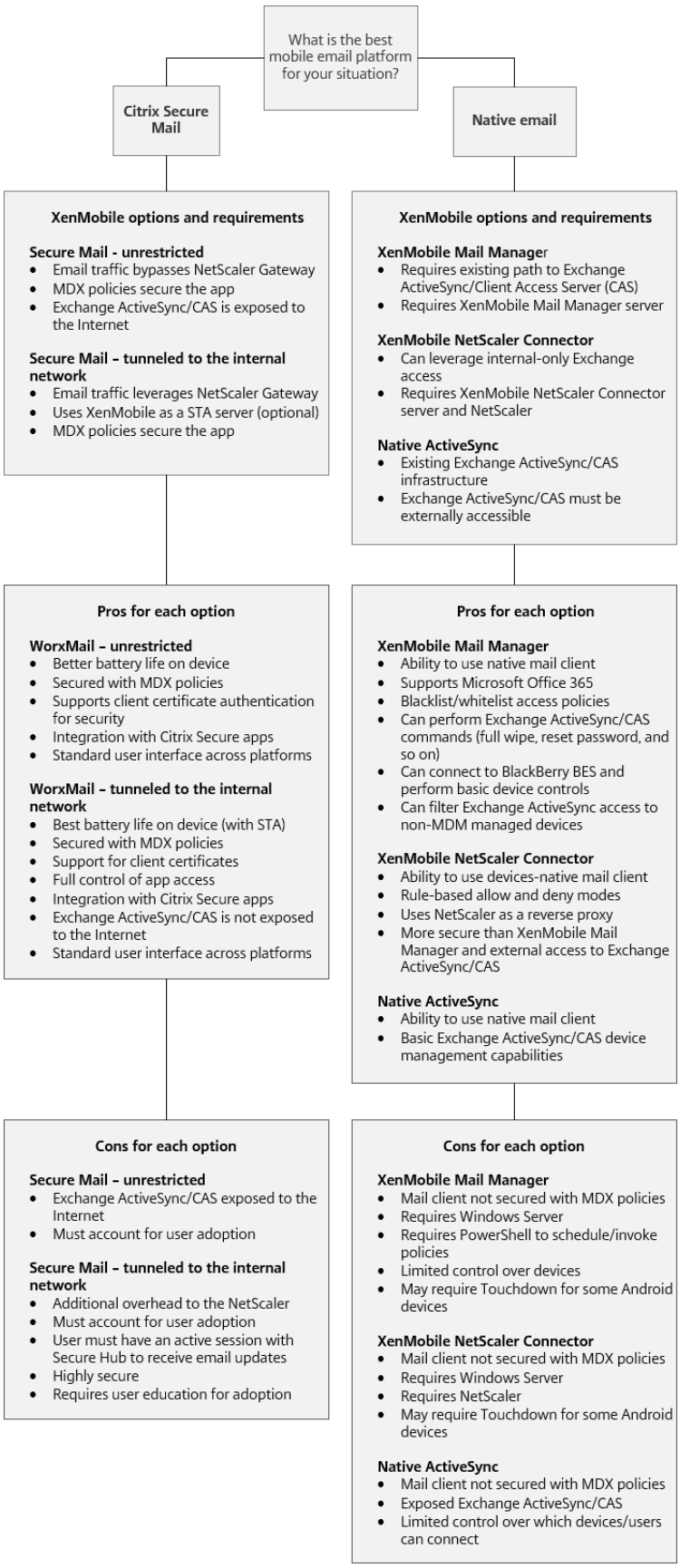
Esta solución no requiere el uso de Citrix ADC. Puede implementar el conector de Endpoint Management para Exchange ActiveSync sin cambiar la redirección del tráfico de ActiveSync existente. En las consideraciones sobre el diseño se incluye:

- Servidor Windows Server: El componente del conector de Endpoint Management para Exchange ActiveSync requiere la implementación de un servidor Windows Server.
- Conjunto de reglas de filtro: Al igual que el conector de Citrix Gateway para Exchange ActiveSync, el conector de Endpoint Management para Exchange ActiveSync incluye reglas de filtro para evaluar el estado del dispositivo. Además, el conector de Endpoint Management para Exchange ActiveSync también admite reglas estáticas para filtrar según la pertenencia al grupo de Active Directory.
- Integración de Exchange: El conector de Endpoint Management para Exchange ActiveSync requiere acceso directo al servidor de acceso de cliente (CAS) de Exchange que aloja el rol de ActiveSync y controla las acciones de cuarentena del dispositivo. Este requisito puede ser un problema dependiendo de la arquitectura del entorno y las indicaciones de seguridad. Es fundamental que evalúe este requisito técnico por adelantado.
- Otros clientes de ActiveSync: Como el conector de Endpoint Management para Exchange ActiveSync filtra en el nivel de servicio de ActiveSync, tenga en cuenta otros clientes de ActiveSync fuera del entorno de XenMobile. Puede configurar reglas estáticas del conector de Endpoint Management para Exchange ActiveSync para evitar un impacto involuntario sobre otros clientes de ActiveSync.
- Funciones extendidas de Exchange: A través de la integración directa con Exchange ActiveSync, el conector de Endpoint Management para Exchange ActiveSync ofrece la capacidad de que XenMobile borre los datos de Exchange ActiveSync que haya en un dispositivo móvil. El conector de Endpoint Management para Exchange ActiveSync también permite que XenMobile acceda a información sobre dispositivos BlackBerry y realice otras operaciones de control.

Para ver un diagrama de Endpoint Management connector for Exchange ActiveSync en una implementación de XenMobile, consulte Arquitectura de referencia para implementaciones locales.

Árbol de decisiones sobre la plataforma de correo electrónico

La siguiente imagen tiene por objetivo facilitar la distinción entre las ventajas y las desventajas que ofrecen las soluciones de correo electrónico nativas o Secure Mail en su implementación de XenMobile. Cada opción conlleva que las opciones y los requisitos de XenMobile asociados permitan el acceso al servidor, la red y la base de datos. En los criterios de pros y contras se incluyen detalles sobre seguridad, directivas e interfaz de usuario.



Integración de XenMobile

January 4, 2022

En este artículo se describen los elementos a tener en cuenta al planificar cómo se integra XenMobile en su red y sus soluciones existentes. Por ejemplo, si ya está utilizando Citrix ADC para Virtual Apps and Desktops:

- ¿Debería utilizar la instancia existente de Citrix ADC o una nueva instancia dedicada?
- ¿Quiere integrar en XenMobile las aplicaciones HDX que se han publicado con StoreFront?
- ¿Piensa utilizar Citrix Files con XenMobile?
- ¿Tiene una solución de control de acceso a la red que quiera integrar en XenMobile?
- ¿Implementa proxys Web para todo el tráfico saliente de la red?

Citrix ADC y Citrix Gateway

Citrix Gateway es obligatorio para los modos ENT y MAM de XenMobile. Citrix Gateway proporciona una ruta de red micro VPN para acceder a todos los recursos de empresa. Asimismo, admite la autenticación de varios factores. El equilibrio de carga de Citrix ADC es obligatorio para todos los modos de dispositivo que ofrece XenMobile Server:

- Si tiene varios servidores de XenMobile
- O bien, si XenMobile Server se encuentra en la zona desmilitarizada o la red interna (y, por lo tanto, el tráfico va desde los dispositivos a Citrix ADC a XenMobile).

Puede usar instancias existentes de Citrix ADC o configurar nuevas para XenMobile. En las secciones siguientes se indican las ventajas y las desventajas de utilizar las instancias de Citrix ADC existentes o unas instancias nuevas dedicadas.

Citrix ADC MPX compartido con una dirección IP virtual de Citrix Gateway creada para XenMobile

Ventajas:

- Utiliza una instancia común de Citrix ADC para todas las conexiones remotas de Citrix: Citrix Virtual Apps and Desktops, VPN completa y VPN sin cliente.
- Utiliza las configuraciones existentes de Citrix ADC; por ejemplo, para la autenticación con certificados y para acceder a servicios como DNS, LDAP y NTP.
- Utiliza una única licencia de plataforma de Citrix ADC.

Desventajas:

- Es más difícil planificar la escalabilidad cuando se enfrenta a dos casos de uso diferentes en el mismo dispositivo Citrix ADC.

- A veces necesita una versión específica de Citrix ADC para un caso de uso de Citrix Virtual Apps and Desktops. Esa misma versión podría tener problemas conocidos para XenMobile. O XenMobile podría presentar problemas conocidos para la versión de Citrix ADC.
- Si ya existe un dispositivo Citrix Gateway, no puede ejecutar el asistente de Citrix ADC para XenMobile por segunda vez para crear la configuración de Citrix ADC para XenMobile.
- Excepto cuando se usan licencias Platinum de Citrix Gateway 11.1 o posterior, se agrupan las licencias de acceso de usuario instaladas en Citrix ADC, necesarias para la conectividad VPN. Puesto que esas licencias están disponibles para todos los servidores virtuales de Citrix ADC, unos servicios que no sean XenMobile pueden potencialmente consumirlas.

Instancia VPX o MPX dedicada de Citrix ADC

Ventajas:

Citrix recomienda usar una instancia dedicada de Citrix ADC.

- Es más fácil planear la escalabilidad en ella. Además, así el tráfico de XenMobile se separa de una instancia de Citrix ADC que podría ya tener restricciones de recursos.
- Evita problemas cuando XenMobile y Citrix Virtual Apps and Desktops necesitan diferentes versiones de software de Citrix ADC. Por lo general, es mejor utilizar la versión y la compilación más recientes de Citrix ADC compatibles con XenMobile.
- Permite configurar Citrix ADC para XenMobile gracias al asistente integrado de Citrix ADC para XenMobile.
- Separación virtual y física de servicios.
- Salvo cuando las licencias Platinum se usan para Citrix Gateway 11.1 o una versión posterior, las licencias de acceso de usuario necesarias para XenMobile solo están disponibles para los servicios de XenMobile en Citrix ADC.

Desventajas:

- Requiere la instalación y la configuración de servicios adicionales en Citrix ADC para admitir la configuración de XenMobile.
- Requiere otra licencia de plataforma de Citrix ADC. Cada instancia de Citrix ADC debe tener una licencia de Citrix Gateway.

Para obtener información sobre qué tener en cuenta a la hora de integrar Citrix ADC y Citrix Gateway en cada modo de servidor de XenMobile, consulte Integración en Citrix ADC y Citrix Gateway.

StoreFront

Si tiene un entorno de Citrix Virtual Apps and Desktops, puede usar StoreFront para integrar aplicaciones HDX en XenMobile. Cuando integra aplicaciones HDX en XenMobile:

- Las aplicaciones están disponibles para los usuarios que están inscritos en XenMobile.

- Las aplicaciones se muestran en XenMobile Store junto con otras aplicaciones móviles.
- XenMobile utiliza el sitio antiguo de (servicios) PNAgent en StoreFront.
- Cuando Citrix Receiver está instalado en un dispositivo, las aplicaciones HDX comienzan a usar Receiver.

StoreFront presenta una limitación de un sitio de servicios por instancia de StoreFront. Supongamos que tiene varios almacenes y quiere separarlos de otro uso de producción. En ese caso, Citrix recomienda generalmente que se plantee un nuevo sitio de servicios y una nueva instancia de StoreFront para XenMobile.

En las consideraciones se incluye:

- ¿Hay algún requisito de autenticación diferente para StoreFront? El sitio de servicios de StoreFront requiere credenciales de Active Directory para el inicio de sesión. Los clientes que solo usan la autenticación basada en certificados no pueden enumerar las aplicaciones a través de XenMobile con el mismo dispositivo Citrix Gateway.
- ¿Usar el mismo almacén o crear otro?
- ¿Usar el mismo servidor de StoreFront o no?

En las siguientes secciones se indican las ventajas y las desventajas de utilizar instancias de StoreFront separados o combinados para Receiver y las aplicaciones móviles de productividad.

Integrar la instancia existente de StoreFront en el servidor de XenMobile

Ventajas:

- Mismo almacén: No se requiere configuración adicional de StoreFront para XenMobile, suponiendo que utilice la misma dirección IP virtual de Citrix ADC para el acceso HDX. Supongamos que elige usar la misma tienda y quiere dirigir el acceso de Receiver a una nueva dirección IP virtual de Citrix ADC. En ese caso, agregue la configuración apropiada de Citrix Gateway a StoreFront.
- Mismo servidor de StoreFront: Utiliza la instalación y la configuración del StoreFront existente.

Desventajas:

- Mismo almacén: Cualquier cambio en la configuración de StoreFront para admitir las cargas de trabajo de Virtual Apps and Desktops puede afectar negativamente a XenMobile.
- Mismo servidor StoreFront: En entornos grandes, tenga en cuenta la carga adicional que provocará el uso de PNAgent por parte de XenMobile para la enumeración y el inicio de las aplicaciones.

Usar una instancia nueva y dedicada de StoreFront para la integración en el servidor de XenMobile

Ventajas:

- Nuevo almacén: Ningún cambio en la configuración del almacén StoreFront para XenMobile debería afectar las cargas de trabajo existentes de Virtual Apps and Desktops.
- Nuevo servidor StoreFront: Los cambios en la configuración del servidor no deberían afectar al flujo de trabajo de Citrix Virtual Apps and Desktops. Además, la carga no derivada del uso de PNAgent por parte de XenMobile para la enumeración y el inicio de aplicaciones no debe afectar a la escalabilidad.

Desventajas:

- Nuevo almacén: Configuración del almacén StoreFront.
- Nuevo servidor de StoreFront: Requiere una nueva instalación y configuración de StoreFront.

Para obtener más información, consulte Virtual Apps and Desktops a través de Citrix Secure Hub en la documentación de XenMobile.

Citrix Content Collaboration y Citrix Files

Citrix Files permite a los usuarios acceder y sincronizar todos sus datos desde cualquier dispositivo. Con Citrix Files, los usuarios pueden compartir datos de forma segura con personas tanto dentro como fuera de la organización. Si integra Citrix Content Collaboration con XenMobile Advanced Edition o Enterprise Edition, XenMobile puede proporcionar a Citrix Files:

- Autenticación Single Sign-On para los usuarios de las aplicaciones de XenMobile.
- Aprovisionamiento de cuentas de usuario basado en Active Directory.
- Directivas integrales para controlar el acceso.

Los usuarios móviles pueden aprovechar el conjunto completo de funciones de la cuenta Enterprise.

También puede configurar XenMobile para integrarlo solamente con conectores de zonas de almacenamiento. A través de conectores de zonas de almacenamiento, Citrix Files proporciona acceso a:

- Documentos y carpetas
- Recursos compartidos de red
- En sitios de SharePoint: Colecciones de sitios y bibliotecas de documentos.

Los recursos compartidos conectados pueden incluir las mismas unidades “home” de red utilizadas en entornos de Citrix Virtual Apps and Desktops. Puede utilizar la consola de XenMobile para configurar la integración en Citrix Files o los conectores de zonas de almacenamiento. Para obtener más información, consulte Uso de Citrix Files con XenMobile.

En las siguientes secciones se indican las preguntas a contestar cuando se decide el diseño de Citrix Files.

Integrar en Citrix Files o solo en conectores de zonas de almacenamiento

Preguntas que formular:

- ¿Necesita almacenar datos en las zonas de almacenamiento que administra Citrix?
- ¿Quiere ofrecer a los usuarios funciones de intercambio y sincronización de archivos?
- ¿Quiere que los usuarios puedan acceder a los archivos que se encuentran en el sitio web de Citrix Files? ¿O que puedan acceder al contenido de Office 365 y los conectores de nube personal desde dispositivos móviles?

Decisión en cuanto a diseño:

- Si la respuesta a cualquiera de esas preguntas es "sí", intégrelo en Citrix Files.
- Una integración en solo conectores de zonas de almacenamiento permite a los usuarios iOS un acceso móvil seguro a repositorios de almacenamiento locales existentes, como sitios de SharePoint y recursos compartidos de archivos de red. En esta configuración no se requiere configurar ningún subdominio de Content Collaboration, aprovisionar usuarios a Citrix Files ni alojar datos de Citrix Files. El uso de conectores de zonas de almacenamiento con XenMobile cumple las restricciones de seguridad contra la filtración de datos del usuario fuera de la red corporativa.

Ubicación de los servidores de controladores de zonas de almacenamiento

Preguntas que formular:

- ¿Necesita almacenamiento local o funciones como conectores de zonas de almacenamiento?
- Si usa las funciones locales de Citrix Files, ¿dónde se ubicarán los controladores de zonas de almacenamiento en la red?

Decisión en cuanto a diseño:

- Determine si ubicar los servidores de los controladores de las zonas de almacenamiento en la nube de Citrix Files, en su sistema local de almacenamiento de arrendatarios individuales o en un almacenamiento en la nube de terceros compatible.
- Los controladores de zonas de almacenamiento requieren acceso a Internet para comunicarse con el plano de control de Citrix Files. Puede conectarse de varias formas, incluido el acceso directo, las configuraciones NAT/PAT o proxy.

Conectores de zonas de almacenamiento

Preguntas que formular:

- ¿Cuáles son las rutas a recursos CIFS?
- ¿Cuáles son las URL de SharePoint?

Decisión en cuanto a diseño:

- Determine si son necesarios unos controladores de zonas de almacenamiento locales para acceder a esas ubicaciones.

- Debido a la comunicación del controlador de zonas de almacenamiento con recursos internos (como repositorios de archivos, recursos CIFS y SharePoint), Citrix recomienda que esos controladores residan en la red interna, detrás de los firewalls DMZ y de Citrix ADC.

Integración de SAML con XenMobile Enterprise

Preguntas que formular:

- ¿Se requiere la autenticación de Active Directory para Citrix Files?
- ¿Se requiere SSO la primera vez que se usa la aplicación Citrix Files para XenMobile?
- ¿Hay un proveedor de identidades estándar en el entorno actual?
- ¿Cuántos dominios se requieren para usar SAML?
- ¿Hay varios alias de correo electrónico para los usuarios de Active Directory?
- ¿Hay alguna migración de dominio de Active Directory en curso o programada próximamente?

Decisión en cuanto a diseño:

Los entornos de XenMobile Enterprise pueden optar por utilizar SAML como el mecanismo de autenticación para Citrix Files. Las opciones de autenticación son:

- Utilizar el servidor de XenMobile como el proveedor de identidades (IdP) para SAML

Esta opción puede: proporcionar una excelente experiencia de usuario, automatizar la creación de cuentas de Citrix Files y habilitar las funciones de Single Sign-On para las aplicaciones móviles.

- El servidor de XenMobile se ha mejorado para este proceso, ya que no requiere la sincronización de Active Directory.
- Usar la herramienta Citrix Files User Management Tool para el aprovisionamiento de usuarios.
- Usar un proveedor de terceros compatible en calidad de IdP para SAML

Si tiene un IdP existente compatible y no requiere capacidades SSO para aplicaciones móviles, esta puede ser la opción más adecuada. Esta opción también requiere la herramienta Citrix Files User Management Tool para el aprovisionamiento de cuentas.

Usar soluciones IdP de terceros, como ADFS, también puede proporcionar capacidades SSO en el lado del cliente Windows. Debe valorar los casos de uso antes de elegir su IdP SAML para Citrix Files.

Además, para ambos casos de uso, puede configurar ADFS y XenMobile como un IdP dual.

Aplicaciones móviles

Preguntas que formular:

- ¿Qué aplicación móvil de Citrix Files va a usar (pública, MDM, MDX)?

Decisión en cuanto a diseño:

- Puede distribuir las aplicaciones móviles de productividad desde Apple App Store y Google Play Store. Con esa distribución desde el tienda pública de aplicaciones, se obtienen aplicaciones empaquetadas desde la página Descargas de Citrix.
- Si el nivel de seguridad es bajo y no se necesitan contenedores, puede que la aplicación pública de Citrix Files no sea la adecuada. En un entorno solo MDM, puede entregar la versión MDM de la aplicación Citrix Files mediante XenMobile en modo MDM.
- Para obtener más información, consulte Aplicaciones y Citrix Files para XenMobile.

Seguridad, directivas y control de acceso

Preguntas que formular:

- ¿Qué restricciones necesita para usuarios móviles, Web y de escritorio?
- ¿Qué configuración estándar quiere para controlar el acceso de los usuarios?
- ¿Qué directiva de retención de archivos va a usar?

Decisión en cuanto a diseño:

- Citrix Files permite administrar los permisos de los empleados y la seguridad de los dispositivos. Para obtener información, consulte Permisos de empleado y Administrar dispositivos y aplicaciones.
- Determinadas directivas MDX y configuraciones de Citrix Files para la seguridad del dispositivo controlan las mismas funciones. En esos casos, tienen prioridad las directivas de XenMobile, seguidas de las configuraciones de Citrix Files para la seguridad de los dispositivos. Ejemplos: Si inhabilita aplicaciones externas en Citrix Files, pero las habilita en XenMobile, las aplicaciones externas se inhabilitan en Citrix Files. Puede configurar las aplicaciones para que XenMobile no requiera PIN o código de acceso, pero la aplicación Citrix Files lo requiere.

Zonas de almacenamiento estándar o restringidas

Preguntas que formular:

- ¿Necesita zonas de almacenamiento restringidas?

Decisión en cuanto a diseño:

- Una zona de almacenamiento estándar está diseñada para almacenar datos no confidenciales, y permite a los empleados compartir datos con otras personas ajenas a la empresa. En esta opción se admiten flujos de trabajo que implican compartir datos fuera del dominio.
- Una zona de almacenamiento restringida protege datos confidenciales, por lo que solo los usuarios de dominio autenticados pueden acceder a los datos almacenados en estas zonas.

Proxys Web

El caso más probable para enrutar el tráfico de XenMobile a través de un proxy HTTP/SOCKS o HTTP-S/SOCKS es el siguiente: cuando la subred en la que reside el servidor de XenMobile no tiene acceso saliente a Internet hacia las direcciones IP requeridas de Apple, Google o Microsoft. Puede especificar la configuración del servidor proxy en XenMobile para enrutar todo el tráfico de Internet al servidor proxy. Para obtener más información, consulte Habilitar servidores proxy.

En la siguiente tabla se describen las ventajas y las desventajas del proxy más común utilizado con XenMobile.

Opción	Ventajas	Desventajas
Utilizar un proxy HTTP/SOCKS o HTTPS/SOCKS con el servidor de XenMobile.	En los casos en que las directivas no permiten conexiones salientes de Internet desde la subred del servidor de XenMobile, puede configurar un proxy SOCKS de HTTP o HTTPS para ofrecer la conectividad con Internet.	Si el servidor proxy falla, se interrumpe la conectividad con APNs (iOS) o Firebase Cloud Messaging (Android). Como resultado, las notificaciones de dispositivo fallan para todos los dispositivos iOS y Android.
Utilizar un proxy HTTP o HTTPS con Secure Web.	Puede supervisar el tráfico HTTP o HTTPS para asegurarse de que la actividad de Internet cumple con los estándares de la organización.	Esta configuración requiere que todo el tráfico de Internet relativo a Secure Web pase a través de un túnel de nuevo a la red corporativa antes de que enviarse a Internet. Si la conexión a Internet restringe la navegación, esta configuración podría afectar el rendimiento de la navegación por Internet.

La configuración del perfil de sesión de Citrix ADC para el túnel dividido afecta al tráfico de la siguiente manera.

Cuando el túnel dividido de Citrix ADC está **desactivado**:

- Si la directiva MDX **Acceso de red** es **Túnel a la red interna**, todo el tráfico se ve obligado a utilizar el túnel de la micro VPN o la VPN sin cliente (cVPN) de nuevo a Citrix Gateway.

- Configure las directivas o los perfiles de tráfico de Citrix ADC para el servidor proxy y vincúlelos a la dirección IP virtual de Citrix Gateway.

> **Importante:**
>
> El tráfico cVPN de Secure Hub no debe estar incluido en el proxy.

- Para obtener más información, consulte XenMobile Secure Hub Traffic Through Proxy Server in Secure Browse Mode.

Cuando el **túnel dividido de Citrix ADC** está **activado**:

- Cuando las aplicaciones están configuradas con la directiva MDX **Acceso de red** establecida en **Túnel a la red interna**, las aplicaciones intentan primero obtener directamente el recurso web. Si el recurso web no está disponible públicamente, esas aplicaciones recurren a Citrix Gateway.
- Configure las directivas o los perfiles de tráfico de Citrix ADC para el servidor proxy. Luego, vincule esas directivas y esos perfiles a la dirección IP virtual de Citrix Gateway.

> **Importante:**
>
> El tráfico cVPN de Secure Hub no debe estar incluido en el proxy.

La configuración del perfil de sesión de Citrix ADC para **DNS dividido** (en **Experiencia del cliente**) funciona de manera similar a Túnel dividido.

Con **DNS dividido** habilitado y establecido en **Ambos**:

- El cliente intenta primero resolver el FQDN localmente y luego recurre a Citrix ADC para la resolución de DNS durante el fallo.

Con **DNS dividido** establecido en **Remoto**:

- La resolución de DNS ocurre solo en Citrix ADC.

Con **DNS dividido** establecido en **Local**:

- El cliente intenta resolver el FQDN localmente. Citrix ADC no se utiliza para la resolución de DNS.

Control de acceso

Las empresas pueden administrar dispositivos móviles dentro y fuera de las redes. Las soluciones de administración de la movilidad empresarial (como XenMobile) son excelentes para proporcionar la seguridad de los dispositivos móviles y control sobre ellos, independientemente de la ubicación. Sin embargo, cuando esas soluciones se combinan con una solución de control de acceso a la red (NAC), puede agregar QoS y un control más preciso a los dispositivos internos de su red. Esa combinación le permite extender a la solución NAC la evaluación de seguridad de dispositivos que ofrece XenMobile. La solución NAC puede usar la evaluación de seguridad de XenMobile para facilitar y gestionar las decisiones de autenticación.

Puede utilizar cualquiera de estas soluciones para aplicar directivas de NAC:

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

Citrix no garantiza la integración de otras soluciones NAC.

Las ventajas de la integración de una solución NAC en XenMobile son:

- Una seguridad, conformidad y control mejores para todos los dispositivos de punto final en una red empresarial.
- Una solución NAC puede:
  - Detectar dispositivos en el instante en que intentan conectarse a la red.
  - Buscar atributos de los dispositivos en XenMobile.
  - Luego, usar esa información para determinar si permitir, bloquear, limitar o redirigir esos dispositivos. Esas decisiones dependen de las directivas de seguridad que elija aplicar.
- Una solución NAC ofrece a los administradores de TI una visión que engloba dispositivos no administrados y no conformes.

Para obtener una descripción de los filtros de conformidad de NAC que admite XenMobile y una introducción a la configuración, consulte Control de acceso de red.

Requisitos multisitio

January 4, 2022

Puede planificar y configurar implementaciones de XenMobile que contengan varios sitios para la alta disponibilidad y la recuperación ante desastres. En este artículo se ofrece una descripción general de los modelos de alta disponibilidad y recuperación ante desastres que se utilizan en las implementaciones de XenMobile.

Alta disponibilidad

- Para los nodos en clúster de XenMobile, Citrix ADC se encarga de gestionar el equilibrio de carga. Para obtener más información, consulte Configurar clústeres.
- Los nodos del servidor de XenMobile operan en una configuración activa/activa.
- Se agregan nodos de servidor de XenMobile adicionales a un clúster de alta disponibilidad a medida que se requiera más capacidad. Un nodo puede encargarse de aproximadamente 8500 dispositivos de usuario como máximo (consulte Escalabilidad y rendimiento para obtener más información).

- Citrix recomienda configurar servidores de XenMobile sobre la base de “n + 1”, es decir, un servidor por cada 8500 dispositivos de usuario y un servidor adicional para la redundancia.
- Citrix recomienda una alta disponibilidad para todas las instancias de Citrix ADC siempre que sea posible, de modo que las configuraciones se sincronicen con un segundo dispositivo Citrix ADC.
- El par estándar de alta disponibilidad de Citrix ADC funciona en una configuración activa/pasiva.

Una implementación típica de XenMobile de alta disponibilidad suele incluir:

- Dos instancias de Citrix ADC (VPX o MPX). Si se utiliza la plataforma Citrix ADC SDX, también debe considerarse la alta disponibilidad.
- Dos o más servidores de XenMobile configurados con los mismos parámetros de base de datos.

Recuperación ante desastres

Puede configurar XenMobile para la recuperación ante desastres en dos centros de datos, con un centro de datos activo y el otro centro de datos pasivo. Se utilizan Citrix ADC y Global Server Load Balancing (GSLB) para crear una ruta de datos activa/activa, de modo que la experiencia del usuario sea la de una configuración activa/activa.

Para la recuperación ante desastres, una implementación de XenMobile incluye:

- Dos centros de datos; cada uno con una o varias instancias de Citrix ADC, servidores de XenMobile y bases de datos de SQL Server.
- Un servidor GSLB para dirigir el tráfico a los centros de datos. El servidor GSLB se configura tanto para la URL de inscripción de XenMobile como para la URL de Citrix Gateway que gestiona el tráfico al sitio.
- Cuando se utiliza el asistente de Citrix ADC para XenMobile para configurar Citrix Gateway, de manera predeterminada, el GSLB no está habilitado para resolver el tráfico al servidor de inscripción de XenMobile ni el tráfico a Citrix Gateway, en ruta al servidor de equilibrio de carga de MAM. Por eso, se requieren pasos adicionales. Para obtener más información sobre la preparación y la implementación de estos pasos, consulte Recuperación ante desastres.
- Servidores SQL en clúster de grupos de disponibilidad AlwaysOn.
- La latencia entre los servidores de XenMobile y SQL Server debe ser inferior a 5 ms.

> **Nota:**
>
> Los métodos de recuperación ante desastres descritos en este manual solo ofrecen la recuperación automática ante desastres para la capa de acceso. Debe iniciar manualmente todos los nodos de servidor de XenMobile y la base de datos de SQL Server en el sitio de conmutación por error para que los dispositivos se puedan conectar el servidor de XenMobile.

Integración en Citrix Gateway y Citrix ADC

January 4, 2022

Cuando se integra en XenMobile, Citrix Gateway ofrece un mecanismo de autenticación para el acceso de dispositivos MAM remotos a la red interna. Esta integración permite a las aplicaciones móviles de productividad conectarse a los servidores de empresa ubicados en la intranet a través de una red micro VPN. Porque se crea una micro VPN que se extiende desde las aplicaciones presentes en el dispositivo móvil hasta Citrix Gateway. Citrix Gateway proporciona una ruta de red micro VPN para acceder a todos los recursos de empresa. Asimismo, admite la autenticación de varios factores.

El equilibrio de carga de Citrix ADC es obligatorio para todos los modos de dispositivo que ofrece XenMobile Server en los siguientes casos:

- Si tiene varios servidores de XenMobile
- O bien, si XenMobile Server se encuentra en la zona desmilitarizada o la red interna (y, por lo tanto, el tráfico va desde los dispositivos a Citrix ADC y a XenMobile).

Requisitos de integración para los modos de XenMobile Server

Los requisitos para integrar Citrix Gateway y Citrix ADC varían en función de los modos de XenMobile Server: ENT, MDM y MAM.

MAM

Con XenMobile Server en modo MAM:

- Se requiere **Citrix Gateway**. Citrix Gateway proporciona una ruta de red micro VPN para acceder a todos los recursos de empresa. Asimismo, admite la autenticación de varios factores.
- Se recomienda usar **Citrix ADC** para el equilibrio de carga.

  Citrix recomienda implementar XenMobile en una configuración de alta disponibilidad, que requiere un equilibrador de carga delante de XenMobile. Para obtener más información, consulte Acerca de los modos MAM y MAM antiguo.

MDM

Con XenMobile Server en modo MDM:

- No se requiere Citrix Gateway. Para implementaciones MDM, Citrix recomienda Citrix Gateway para la VPN de dispositivos móviles.

- Se recomienda usar Citrix ADC para la seguridad y el equilibrio de carga.

  Citrix recomienda implementar un dispositivo Citrix ADC delante de XenMobile Server, por motivos de seguridad y equilibrio de carga. Para implementaciones estándar con XenMobile en la zona desmilitarizada (DMZ), Citrix recomienda el asistente de Citrix ADC para XenMobile junto con el equilibrio de carga de XenMobile Server en el modo Puente SSL. También puede considerar la descarga de SSL para implementaciones en las que:

  - XenMobile Server reside en la red interna, en lugar de en la zona DMZ
  - O bien, su equipo de seguridad requiere una configuración de puente SSL

  Citrix no recomienda exponer XenMobile Server a Internet a través de NAT o proxy de terceros o equilibradores de carga para MDM. Esas configuraciones suponen un riesgo potencial para la seguridad, incluso si el tráfico SSL finaliza en XenMobile Server (Puente SSL).

  Para entornos de alta seguridad, Citrix ADC con la configuración predeterminada de XenMobile cumple o supera los requisitos de seguridad.

  Para entornos MDM con exigencias de seguridad máxima, la finalización de SSL en Citrix ADC permite inspeccionar el tráfico en el perímetro, al mismo tiempo que se mantiene el cifrado SSL de extremo a extremo. Para obtener más información, consulte Requisitos de seguridad. Citrix ADC ofrece opciones para definir el cifrado SSL o TLS y el hardware SSL FIPS de Citrix ADC.

ENT (MDM+MAM)

Con XenMobile Server en modo ENT:

- Se requiere Citrix Gateway. Citrix Gateway proporciona una ruta de red micro VPN para acceder a todos los recursos de empresa. Asimismo, admite la autenticación de varios factores.

  Cuando el modo de XenMobile Server es ENT y un usuario deja la inscripción MDM, el dispositivo opera en el modo MAM antiguo. En el modo MAM antiguo, los dispositivos se inscriben mediante el nombre FQDN de Citrix Gateway. Para obtener más información, consulte Acerca de los modos MAM y MAM antiguo.

- Se recomienda usar Citrix ADC para el equilibrio de carga. Para obtener más información, consulte el apartado anterior sobre Citrix ADC en “MDM”.

> **Importante:**
>
> Para la inscripción inicial, el tráfico desde los dispositivos de usuario se autentica en XenMobile Server, tanto si configura los servidores virtuales de equilibrio de carga en Descarga de SSL como si los configura en Puente SSL.

Decisiones en cuanto a diseño

En las secciones siguientes, se resumen las diversas decisiones de diseño a considerar durante la planificación de una integración de Citrix Gateway en XenMobile.

Licencia y edición

Detalles de la decisión:

- ¿Qué edición de Citrix ADC piensa utilizar?
- ¿Ha aplicado licencias de plataforma a Citrix ADC?
- Si necesita la funcionalidad MAM, ¿ha aplicado las licencias Citrix ADC Universal Access?

Guía de diseño:

Compruebe que aplica las licencias adecuadas a Citrix Gateway. Si usa el conector de Citrix Gateway para Exchange ActiveSync, podría ser necesario el almacenamiento en caché integrado. Por lo tanto, debe comprobar que esté disponible la edición de Citrix ADC correspondiente.

A continuación, dispone de los requisitos de licencias para habilitar las funciones de Citrix ADC.

- El equilibrio de carga MDM de XenMobile requiere, como mínimo, una licencia de plataforma Citrix ADC Standard.
- El equilibrio de carga de Content Collaboration con controladores de zonas de almacenamiento requiere, como mínimo, una licencia de plataforma Standard de Citrix ADC.
- La edición XenMobile Enterprise incluye las licencias Citrix Gateway Universal necesarias para MAM.
- El equilibrio de carga de Exchange requiere una licencia de plataforma Citrix ADC Platinum o una licencia de plataforma Citrix ADC Enterprise, además de una licencia de caché integrada (Integrated Caching).

Versión de Citrix ADC para XenMobile

Detalles de la decisión:

- ¿Qué versión ejecuta Citrix ADC en el entorno de XenMobile?
- ¿Necesita una instancia aparte?

Guía de diseño:

Citrix recomienda usar una instancia dedicada de Citrix ADC para el servidor virtual de Citrix Gateway. Compruebe que se usen la versión y la compilación de Citrix ADC mínimas requeridas en el entorno de XenMobile. Por lo general, es mejor utilizar la versión y la compilación más recientes de Citrix ADC compatibles con XenMobile. Si actualizar la versión de Citrix Gateway afectaría sus entornos existentes, podría interesarle tener una segunda instancia dedicada para XenMobile.

Si va a compartir una instancia de Citrix ADC entre XenMobile y otras aplicaciones que usan conexiones de red VPN, compruebe que dispone de licencias VPN suficientes para ambos. Tenga en cuenta que los entornos de prueba y producción de XenMobile no pueden compartir una instancia de Citrix ADC.

Certificados

Detalles de la decisión:

- ¿Necesita mayor grado de seguridad para las inscripciones y el acceso al entorno de XenMobile?
- ¿LDAP no es una opción?

Guía de diseño:

En XenMobile, la autenticación predeterminada 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. Puede usar certificados con LDAP para la autenticación de dos factores, lo que proporciona un grado mayor de seguridad sin necesidad de un servidor RSA.

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. Cuando el usuario tiene acceso, XenMobile crea e implementa el certificado utilizado a partir de entonces para autenticarse en el entorno de XenMobile.

XenMobile admite 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 Citrix ADC para administrar la revocación. Al configurar la autenticación por certificados de cliente, plantéese si es necesario configurar el parámetro de lista de revocación de certificados (CRL) de Citrix ADC, **Enable CRL Auto Refresh**. Este paso garantiza que el usuario de un dispositivo inscrito en MAM solo no pueda autenticarse con un certificado existente en el dispositivo. XenMobile vuelve a emitir un certificado nuevo, porque no impide que un usuario genere un certificado de usuario si uno se revoca. Este parámetro aumenta la seguridad de las entidades PKI cuando la lista de revocación de certificados comprueba si hay entidades PKI caducadas.

Topología de red

Detalles de la decisión:

- ¿Qué topología de Citrix ADC se necesita?

Guía de diseño:

Citrix recomienda usar una instancia de Citrix ADC para XenMobile. Sin embargo, es posible que no usted no quiera que el tráfico vaya de la red interna a la zona DMZ. En tal caso, considere la posibilidad de configurar una instancia adicional de Citrix ADC. Utilice una instancia de Citrix ADC para usuarios

internos y otra para usuarios externos. Cuando los usuarios cambien entre las redes interna y externa, el almacenamiento en caché de los registros DNS puede dar lugar a un aumento de las solicitudes de inicio de sesión en Secure Hub.

XenMobile no admite el doble salto de Citrix Gateway.

Direcciones IP virtuales dedicadas o compartidas de Citrix Gateway

Detalles de la decisión:

- ¿Utiliza actualmente Citrix Gateway para Virtual Apps and Desktops?
- ¿Tiene previsto que XenMobile utilice el mismo dispositivo Citrix Gateway que Virtual Apps and Desktops?
- ¿Cuáles son los requisitos de autenticación para ambos flujos de tráfico?

Guía de diseño:

Cuando el entorno de Citrix incluye XenMobile con Virtual Apps and Desktops, puede usar la misma instancia de Citrix ADC y el mismo servidor virtual de Citrix Gateway para ambos. Debido a posibles conflictos de versiones y al aislamiento del entorno, se recomiendan una instancia de Citrix ADC dedicada y Citrix Gateway para cada entorno de XenMobile. Sin embargo, si una instancia de Citrix ADC dedicada no es una opción, Citrix recomienda usar un servidor virtual de Citrix Gateway dedicado para separar los flujos de tráfico para Secure Hub. Se recomienda esa configuración, en lugar de un servidor virtual compartido entre XenMobile y Virtual Apps and Desktops.

Si usa la autenticación LDAP, Receiver y Secure Hub pueden autenticarse en el mismo dispositivo Citrix Gateway sin problemas. Si usa la autenticación basada en certificados, XenMobile envía un certificado al contenedor MDX y Secure Hub utiliza ese certificado para autenticarse en Citrix Gateway. Receiver es independiente de Secure Hub y no puede usar el mismo certificado que Secure Hub para autenticarse en el mismo dispositivo Citrix Gateway.

Puede plantearse la siguiente solución temporal, que permite usar un mismo FQDN para dos direcciones IP virtuales de Citrix Gateway.

- Crear dos direcciones IP virtuales de Citrix Gateway con la misma dirección IP. La de Secure Hub utilizará el puerto 443 estándar y la de Virtual Apps and Desktops (que implementa Citrix Receiver) utilizará el puerto 444.
- De este modo, un solo nombre de dominio completo se resuelve en la misma dirección IP.
- Para esta solución temporal, puede configurar StoreFront para devolver un archivo ICA para el puerto 444, en lugar de la opción predeterminada, el puerto 443. Esta solución temporal no requiere que los usuarios introduzcan ningún número de puerto.

Tiempos de espera de Citrix Gateway

Detalles de la decisión:

- ¿Cómo quiere configurar los tiempos de espera de Citrix Gateway para el tráfico de XenMobile?

Guía de diseño:

Citrix Gateway contiene los parámetros “Session time-out” (Tiempo de espera de la sesión) y “Forced time-out” (Tiempo de espera forzado). Para obtener más información, consulte Configuraciones recomendadas. Tenga en cuenta que existen valores de tiempo de espera diferentes para los servicios en segundo plano, Citrix ADC y para el acceso a aplicaciones sin conexión.

Dirección IP del equilibrador de carga de XenMobile para MAM

Detalles de la decisión:

- ¿Usa direcciones IP internas o externas para las direcciones IP virtuales?

Guía de diseño:

En entornos donde puede usar direcciones IP públicas para las direcciones IP virtuales de Citrix Gateway, asignar la dirección y la dirección IP virtual de equilibrio de carga de XenMobile de esta manera provoca fallos de inscripción.

Compruebe que la dirección IP virtual de equilibrio de carga usa una IP interna para evitar errores de inscripción en este caso. Esa dirección IP virtual debe seguir el estándar RFC 1918 para direcciones IP privadas. Si usa una dirección IP no privada para este servidor virtual, Citrix ADC no puede comunicarse correctamente con XenMobile Server durante el proceso de autenticación. Para obtener información detallada, consulte https://support.citrix.com/article/CTX200430.

Mecanismo de equilibrio de carga para MDM

Detalles de la decisión:

- ¿Cómo equilibrará Citrix Gateway la carga de los servidores de XenMobile?

Guía de diseño:

Use el puente SSL cuando XenMobile está en la red perimetral. Use la descarga de SSL, si es necesaria para cumplir las normas de seguridad, cuando XenMobile se encuentre en la red interna.

- Cuando equilibra la carga de XenMobile Server con direcciones IP virtuales de Citrix ADC en el modo Puente SSL, el tráfico de Internet va directamente a XenMobile Server, donde se terminan las conexiones. El modo Puente SSL es el más simple de configurar. También son más fáciles de solucionar los problemas que causa.
- Cuando equilibra la carga de XenMobile Server con direcciones IP virtuales de Citrix ADC en el modo Descarga de SSL, el tráfico de Internet va directamente a Citrix ADC, donde se terminan las conexiones. A continuación, Citrix ADC establece nuevas sesiones de Citrix ADC a XenMobile Server. El modo Descarga de SSL implica una complejidad adicional durante la configuración y la solución de problemas.

Puerto de servicio para el equilibrio de carga MDM con Descarga de SSL

Detalles de la decisión:

- Si piensa utilizar el modo Descarga de SSL para el equilibrio de carga, ¿qué puerto utilizará el servicio back-end?

Guía de diseño:

Para la descarga de SSL, seleccione el puerto 80 o 8443 como se muestra a continuación:

- Utilice el puerto 80 para el tráfico a XenMobile Server, para una descarga efectiva.
- El cifrado de extremo a extremo, es decir, volver a cifrar el tráfico, no se admite. Para obtener más información, consulte el artículo de asistencia de Citrix Supported Architectures Between NetScaler and XenMobile Server.

Nombre de dominio completo para la inscripción

Detalles de la decisión:

- ¿Qué nombre FQDN piensa utilizar para la inscripción y la instancia de XenMobile o la dirección IP virtual de equilibrio de carga?

Guía de diseño:

La configuración inicial del primer XenMobile Server de un clúster requiere que escriba el FQDN de XenMobile Server. Ese FQDN debe coincidir con su URL de dirección IP virtual de MDM y su URL de dirección IP virtual interna de equilibrio de carga para MAM (un registro interno de dirección de Citrix ADC resuelve la dirección IP virtual de equilibrio de carga para MAM). Para obtener más información, consulte “FQDN de inscripción para cada modo de administración” más adelante en este artículo.

Además, debe usar el siguiente certificado:

- Certificado de escucha SSL de XenMobile
- Certificado de dirección IP virtual interna de equilibrio de carga para MAM
- Certificado de dirección IP virtual para MDM (si se utiliza Descarga de SSL para la dirección IP virtual de MDM)

> **Importante:**
>
> Después de configurar el FQDN de inscripción, no puede modificarlo. Un nuevo FQDN de inscripción requiere una nueva base de datos de SQL Server y la reconstrucción de XenMobile Server.

Tráfico de Secure Web

Detalles de la decisión:

- ¿Tiene previsto restringir Secure Web a la navegación web interna solamente?

- ¿Tiene previsto habilitar Secure Web para la navegación web interna y externa?

Guía de diseño:

Si utiliza Secure Web únicamente para la navegación web en interno, la configuración de Citrix Gateway es sencilla. De forma predeterminada, Secure Web debe llegar a todos los sitios internos. Es posible que tenga que configurar firewalls y servidores proxy.

Si va a utilizar Secure Web para la navegación interna y externa, debe habilitar la dirección IP de subred (SNIP) para tener acceso saliente a Internet. El departamento de TI suele considerar los dispositivos inscritos (mediante el contenedor MDX) una extensión de la red corporativa. Por lo tanto, TI normalmente quiere que las conexiones de Secure Web vuelvan a Citrix ADC, pasen por un servidor proxy y, a continuación, salgan a Internet. De forma predeterminada, Secure Web usa un túnel VPN por aplicación hacia la red interna, para todo el acceso de red. Citrix ADC utiliza una configuración de túnel dividido.

Para obtener información sobre las conexiones de Secure Web, consulte Configurar conexiones de usuario.

Notificaciones push para Secure Mail

Detalles de la decisión:

- ¿Tiene previsto usar notificaciones push?

Guía de diseño para iOS:

La configuración de Citrix Gateway podría incluir Secure Ticket Authority (STA), con túnel dividido desactivado. Citrix Gateway debe permitir el tráfico desde Secure Mail hacia las direcciones URL del servicio de escucha de Citrix indicadas en “Notificaciones push” en Secure Mail para iOS.

Guía de diseño para Android:

Utilice Firebase Cloud Messaging (FCM) para controlar cómo y cuándo los dispositivos Android se conectan a XenMobile. Con FCM configurado, toda acción de seguridad o comando de implementación desencadena una notificación push en Secure Hub para pedir al usuario que se reconecte a XenMobile Server.

STA HDX

Detalles de la decisión:

- ¿Qué STA usar si piensa integrar el acceso a aplicaciones HDX?

Guía de diseño:

Los STA de HDX deben coincidir con los STA en StoreFront y deben ser válidos para la comunidad de Virtual Apps and Desktops.

Citrix Files y Citrix Content Collaboration

Detalles de la decisión:

- ¿Tiene previsto usar controladores de zonas de almacenamiento en el entorno?
- ¿Qué URL de dirección IP virtual de Citrix Files tiene pensado usar?

Guía de diseño:

Si incluye controladores de zonas de almacenamiento en su entorno, asegúrese de configurar correctamente lo siguiente:

- Dirección IP virtual de conmutación de Citrix Files (utilizada por el plano de control de Citrix Files para comunicarse con los servidores de los controladores de zonas de almacenamiento)
- Direcciones IP virtuales del equilibrio de carga de Citrix Files
- Todas las directivas y perfiles necesarios

Para obtener información, consulte la documentación sobre controladores de zonas de almacenamiento.

Proveedor de identidades SAML

Detalles de la decisión:

- Si se necesita SAML para Citrix Files, ¿quiere usar XenMobile como proveedor de identidades SAML?

Guía de diseño:

Se recomienda integrar Citrix Files en XenMobile Advanced Edition o XenMobile Enterprise Edition, que es una alternativa más sencilla que configurar la federación basada en SAML. Cuando utiliza Citrix Files con esas ediciones de XenMobile, XenMobile proporciona Citrix Files con:

- Autenticación Single Sign-On (SSO) para los usuarios de las aplicaciones móviles de productividad
- Aprovisionamiento de cuentas de usuario basado en Active Directory
- Directivas completas de control de acceso

La consola de XenMobile permite configurar Citrix Files y supervisar los niveles de servicio y uso de licencias.

Hay dos tipos de clientes de Citrix Files: Citrix Files para clientes de XenMobile (también conocidos como Citrix Files empaquetados) y clientes móviles de Citrix Files (también conocidos como Citrix Files sin empaquetar). Para entender las diferencias, consulte En qué se diferencian los clientes de Citrix Files para XenMobile de los clientes móviles de Citrix Files.

Puede configurar XenMobile y Citrix Content Collaboration para que utilicen SAML con el fin de ofrecer acceso SSO a:

- Aplicaciones móviles de Citrix Files
- Clientes de Citrix Files no empaquetados, como el sitio web, Outlook Plug-in o clientes de sincronización

Para usar XenMobile como proveedor de identidades SAML para Citrix Files, compruebe que estén definidas las configuraciones adecuadas. Para obtener más información, consulte SAML para SSO en Citrix Files.

Conexiones directas con ShareConnect

Detalles de la decisión:

- ¿Deberán acceder los usuarios a un equipo host desde un equipo o dispositivo móvil que ejecuta ShareConnect con conexiones directas?

Guía de diseño:

ShareConnect permite a los usuarios conectarse a sus equipos de forma segura a través de iPads, tabletas y teléfonos Android para el acceso a sus archivos y aplicaciones. Para las conexiones directas, XenMobile utiliza Citrix Gateway para proporcionar acceso seguro a los recursos de fuera de la red local. Para obtener más información de configuración, consulte ShareConnect.

FQDN de inscripción para cada modo de administración

Modo de administración	Nombre de dominio completo para la inscripción
Enterprise (MDM+MAM) con inscripción MDM obligatoria	FQDN de XenMobile Server
Enterprise (MDM+MAM) con inscripción MDM opcional	FQDN de XenMobile Server o FQDN de Citrix Gateway
Solo MDM	FQDN de XenMobile Server
Solo MAM (antiguo)	FQDN de Citrix Gateway
Solo MAM	FQDN de XenMobile Server

Resumen de implementación

Citrix recomienda usar el asistente de Citrix ADC para XenMobile si quiere asegurarse de una configuración correcta. Solo puede utilizar el asistente una vez. Si tiene varias instancias de XenMobile (por ejemplo, para entornos de prueba, desarrollo y producción) debe configurar Citrix ADC manualmente

para los entornos adicionales. Si dispone de un entorno de trabajo, tome nota de la configuración antes de intentar configurar Citrix ADC manualmente para XenMobile.

La decisión clave que debe tomar al utilizar el asistente es si usar HTTPS o HTTP para comunicarse con XenMobile Server. HTTPS ofrece una comunicación back-end segura, ya que se cifra el tráfico entre Citrix ADC y XenMobile. El recifrado afecta al rendimiento de XenMobile Server. HTTP ofrece un mejor rendimiento de XenMobile Server. El tráfico entre Citrix ADC y XenMobile no está cifrado. En las siguientes tablas, se muestran los requisitos de puertos HTTP y HTTPS para Citrix ADC y XenMobile Server.

HTTPS

Por regla general, Citrix recomienda el puente SSL para los parámetros del servidor virtual MDM de Citrix ADC. Para usar la descarga de SSL de Citrix ADC con servidores virtuales MDM, XenMobile admite solo el puerto 80 como servicio back-end.

Modo de administración	Método de equilibrio de carga de Citrix ADC	Recifrado SSL	Puerto del servidor de XenMobile
MDM	Puente SSL	N/D	443, 8443
MAM	Descarga de SSL	Habilitado	8443
Empresarial	MDM: Puente SSL	N/D	443, 8443
Empresarial	MAM: Descarga de SSL	Habilitado	8443

HTTP

Modo de administración	Método de equilibrio de carga de Citrix ADC	Recifrado SSL	Puerto del servidor de XenMobile
MDM	Descarga de SSL	No se admite	80
MAM	Descarga de SSL	Habilitado	8443
Empresarial	MDM: Descarga de SSL	No se admite	80

Empresarial	MAM: Descarga de SSL	Habilitado	8443

Para obtener diagramas de Citrix Gateway en implementaciones de XenMobile, consulte Arquitectura de referencia para implementaciones locales.

Consideraciones sobre SSO y proxies para aplicaciones MDX

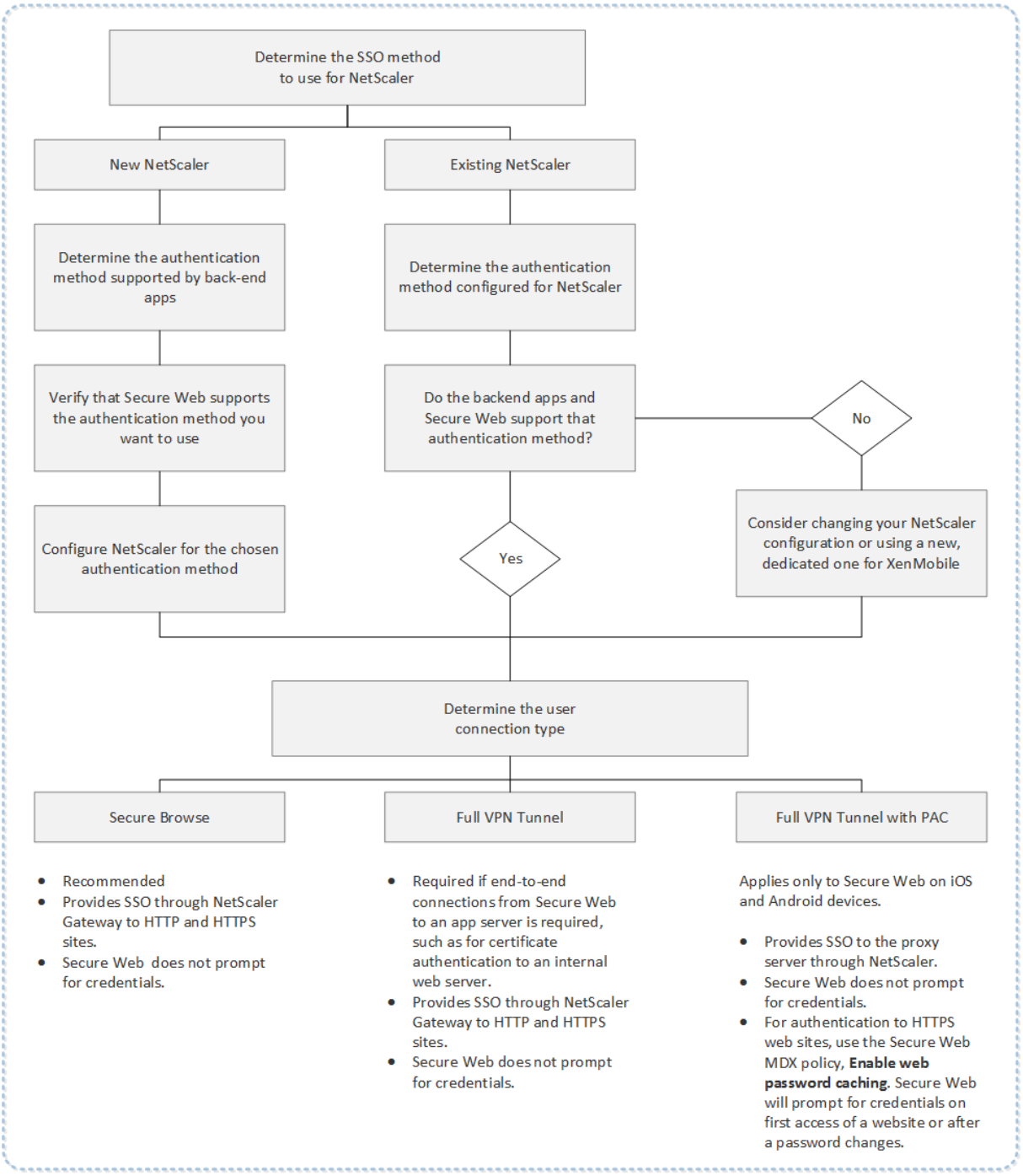
January 4, 2022

La integración de XenMobile con Citrix ADC le permite ofrecer Single Sign-On (SSO) a los usuarios a todos los recursos back-end HTTP o HTTPS. Según los requisitos de autenticación de SSO, puede configurar las conexiones de usuario para que una aplicación MDX use cualquiera de estas opciones:

- Secure Browse (un tipo de VPN sin cliente)
- Túnel VPN completo

Si Citrix ADC no es el mejor medio para ofrecer SSO en el entorno, puede configurar directivas para que las aplicaciones MDX almacenen las contraseñas en caché local. En este artículo se exploran las diversas opciones SSO y proxy, centrándose sobre todo en Secure Web. Los conceptos se aplican a otras aplicaciones MDX.

En el siguiente diagrama de flujo, se resume el recorrido de decisiones para SSO y las conexiones de usuario.



Métodos de autenticación de Citrix ADC

En esta sección se ofrece información general sobre los métodos de autenticación que admite Citrix ADC.

Autenticación SAML

Cuando configura Citrix ADC para SAML (Security Assertion Markup Language), los usuarios pueden conectarse a las aplicaciones web que admiten el protocolo SAML para Single Sign-On. Citrix Gateway admite Single Sign-On del proveedor de identidades (IdP) para aplicaciones web SAML.

Configuración requerida:

- Configure SSO con SAML en el perfil de tráfico de Citrix ADC.
- Configure un proveedor de identidades con SAML para el servicio solicitado.

Autenticación NTLM

Si Single Sign-On en aplicaciones web está habilitado en el perfil de la sesión, Citrix ADC realiza automáticamente la autenticación NTLM.

Configuración requerida:

- Habilite SSO en la sesión o el perfil de tráfico de Citrix ADC.

Suplantación Kerberos

XenMobile solo admite Kerberos para Secure Web. Al configurar Citrix ADC para Single Sign-On de Kerberos, Citrix ADC utiliza suplantación cuando una contraseña de usuario está disponible para Citrix ADC. La suplantación significa que Citrix ADC usa credenciales de usuario para obtener el tíquet necesario y acceder a servicios como Secure Web.

Configuración requerida:

- Configure la directiva de sesión “Worx” de Citrix ADC para que pueda identificar el territorio Kerberos en la conexión.
- Configure una cuenta de delegación limitada de Kerberos (KCD) en Citrix ADC. Configure esa cuenta sin contraseña y vincúlela a una directiva de tráfico en la puerta de enlace de XenMobile.
- Para conocer esos y otros detalles de configuración, consulte el blog de Citrix: WorxWeb and Kerberos Impersonation SSO.

Delegación limitada de Kerberos

XenMobile solo admite Kerberos para Secure Web. Al configurar Citrix ADC para Single Sign-On de Kerberos, Citrix ADC utiliza la delegación limitada cuando una contraseña de usuario no está disponible para Citrix ADC.

Con la delegación limitada, Citrix ADC usa una cuenta de administrador específica para obtener tíquets en nombre de los usuarios y los servicios.

Configuración requerida:

- Configure una cuenta KCD en Active Directory con los permisos necesarios y una cuenta KCD en Citrix ADC.
- Habilite SSO en el perfil de tráfico de Citrix ADC.
- Configure el sitio web back-end para la autenticación Kerberos.

Autenticación con rellenado de formularios

Cuando configura Citrix ADC para Single Sign-On basado en formularios, los usuarios pueden iniciar sesión una vez para acceder a todas las aplicaciones protegidas de la red. Este método de autenticación se aplica a las aplicaciones que usan los modos Secure Browse o Túnel VPN completo.

Configuración requerida:

- Configure el inicio SSO basado en formularios en el perfil de tráfico de Citrix ADC.

Autenticación HTTP implícita

Si habilita Single Sign-On para las aplicaciones web en el perfil de la sesión, Citrix ADC realiza automáticamente la autenticación HTTP implícita. Este método de autenticación se aplica a las aplicaciones que usan los modos Secure Browse o Túnel VPN completo.

Configuración requerida:

- Habilite SSO en la sesión o el perfil de tráfico de Citrix ADC.

Autenticación HTTP básica

Si habilita Single Sign-On para las aplicaciones web en el perfil de la sesión, Citrix ADC realiza automáticamente la autenticación HTTP básica. Este método de autenticación se aplica a las aplicaciones que usan los modos Secure Browse o Túnel VPN completo.

Configuración requerida:

- Habilite SSO en la sesión o el perfil de tráfico de Citrix ADC.

Secure Browse, Túnel VPN completo o Túnel VPN completo con archivo PAC

En las secciones siguientes, se describen los tipos de conexión de usuario para Secure Web. Para obtener más información, consulte este artículo de Secure Web en Configuración de conexiones de usuario de la documentación de Citrix.

Túnel VPN completo

Las conexiones por túnel a la red interna pueden usar un túnel VPN completo. Establezca la directiva "Modo preferido de VPN" de Secure Web en el valor "Túnel VPN completo". Citrix recomienda el valor "Túnel VPN completo" para conexiones que usan certificados de cliente o SSL de extremo a extremo para conectarse a un recurso de la red interna. El modo "Túnel VPN completo" gestiona cualquier protocolo por TCP. Puede usar el túnel VPN completo con dispositivos Windows, Mac, iOS y Android.

En el modo "Túnel VPN completo", Citrix ADC no tiene visibilidad dentro de una sesión HTTPS.

Secure Browse

Las conexiones por túnel a la red interna pueden utilizar una variante de VPN sin cliente conocida como "Secure Browse". Esta es la configuración predeterminada para la directiva **Modo preferido de VPN** de Secure Web. Citrix recomienda el valor "Secure Browse" para conexiones que requieren Single Sign-On (SSO).

En el modo "Exploración segura", Citrix ADC divide la sesión HTTPS en dos partes:

- Del cliente a Citrix ADC
- Desde Citrix ADC hasta el servidor back-end del recurso.

De esta manera, Citrix ADC tiene una visibilidad total de todas las transacciones entre el cliente y el servidor, lo que le permite ofrecer SSO.

También puede configurar los servidores proxy de Secure Web cuando se usa el modo "Secure Browse". Para obtener más información, consulte el blog XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode.

Túnel VPN completo con archivo PAC

Puede usar un archivo de configuración automática de proxy (PAC) con una implementación de túnel VPN completo para un Secure Web presente en dispositivos iOS y Android. XenMobile admite la autenticación de proxy proporcionada por Citrix ADC. Un archivo PAC contiene reglas que definen el modo en que los exploradores web seleccionan un proxy para acceder a una dirección URL especificada. Las reglas del archivo PAC pueden especificar cómo gestionar tanto sitios internos como sitios externos. Secure Web analiza las reglas del archivo PAC y envía la información del servidor proxy a Citrix Gateway. Citrix Gateway no detecta el archivo PAC ni el servidor proxy.

Para la autenticación en sitios web HTTPS, la directiva MDX **Habilitar caché de contraseñas Web** permite a Secure Web autenticarse y ofrecer SSO en el servidor proxy a través de MDX.

Túnel dividido de Citrix ADC

Cuando planifique la configuración de SSO y proxy, también debe decidir si usar el túnel dividido de Citrix ADC o no. Citrix recomienda que utilice el túnel dividido de Citrix ADC solo si es necesario. En esta sección se ofrece información exhaustiva sobre cómo funciona el túnel dividido. Para empezar, Citrix ADC determina la ruta del tráfico en función de su tabla de enrutamiento. Cuando el túnel dividido de Citrix ADC está activado, Secure Hub distingue el tráfico de red interno (protegido) del tráfico de Internet. Secure Hub realiza esa distinción en función del sufijo DNS y las aplicaciones de la intranet. A continuación, Secure Hub envía por el túnel VPN solo el tráfico de la red interna. Cuando el túnel dividido de Citrix ADC está desactivado, todo el tráfico pasa por el túnel VPN.

- Si, por motivos de seguridad, prefiere supervisar todo el tráfico, inhabilite el túnel dividido de Citrix ADC. Como resultado, todo el tráfico pasará por el túnel VPN.
- Si usa "Túnel VPN completo con archivo PAC", debe inhabilitar el túnel dividido de Citrix Gateway. Si el túnel dividido está activado y se configura un archivo PAC, las reglas del archivo PAC anulan las reglas del túnel dividido de Citrix ADC. Un servidor proxy configurado en una directiva de tráfico no anula las reglas de túnel dividido de Citrix ADC.

De forma predeterminada, la directiva **Acceso de red** tiene el valor **Túnel a la red interna** para Secure Web. Con esa configuración, las aplicaciones MDX utilizan los parámetros del túnel dividido de Citrix ADC. El valor predeterminado de la directiva **Acceso de red** difiere de una aplicación a otra de las aplicaciones móviles de productividad.

Citrix Gateway también tiene un modo de túnel dividido revertido de micro VPN. Esta configuración admite una lista de exclusión de direcciones IP que no se envían por túnel a Citrix ADC. En vez de ello, esas direcciones se envían mediante la conexión a Internet del dispositivo. Para obtener más información sobre el túnel dividido revertido, consulte la documentación de Citrix Gateway.

XenMobile incluye una **Lista de exclusión para revertir túnel dividido**. Para impedir que determinados sitios web usen el túnel a través de Citrix Gateway, agregue una lista de nombres de dominio completo (FQDN) o sufijos DNS, separados por comas, para que se conecten a través de la red LAN en lugar del túnel. Esta lista se aplica solamente al modo "Exploración segura" cuando Citrix Gateway está configurado en el modo túnel dividido revertido.

Autenticación

January 4, 2022

En una implementación de XenMobile, entran varias consideraciones en juego a la hora de decidir cómo configurar la autenticación. Esta sección ofrece una guía para comprender los diversos factores que afectan a la autenticación porque se analiza lo siguiente:

- Las principales directivas MDX, las propiedades del cliente XenMobile y las configuraciones de Citrix Gateway relacionadas con la autenticación.
- Las formas en que interactúan estas directivas, parámetros y propiedades de cliente.
- Los pros y contras de cada elección.

Este artículo también contiene tres ejemplos de configuraciones recomendadas para aumentar los grados de seguridad.

En términos generales, una seguridad más alta empobrece la experiencia del usuario, ya que los usuarios deben autenticarse más a menudo. La forma de equilibrar estos aspectos, la seguridad y la fluidez de la experiencia del usuario depende de las necesidades y las prioridades de su organización. El objetivo de ofrecer esas tres configuraciones recomendadas es conferirle una mayor comprensión de la interacción de las medidas de autenticación disponibles y orientarle a comprender cómo implementar mejor su propio entorno de XenMobile.

Modos de autenticación

Autenticación con conexión: Permite a los usuarios conectarse a la red de XenMobile. Requiere una conexión a Internet.

Autenticación sin conexión: Ocurre en el dispositivo. Los usuarios desbloquean la caja fuerte segura y tienen acceso sin conexión a elementos (como el correo descargado, los sitios web almacenados en caché y las notas).

Métodos de autenticación

Factor único

LDAP: En XenMobile, puede configurar una conexión a uno o varios directorios (como Active Directory) compatibles con el Protocolo ligero de acceso a directorios (LDAP). Este es un método frecuente para ofrecer el inicio Single Sign-On (SSO) en entornos de empresa. Puede optar por el PIN de Citrix con el almacenamiento en caché de la contraseña de Active Directory para mejorar la experiencia del usuario con LDAP al mismo tiempo que proporciona la seguridad de contraseñas complejas en la inscripción, la caducidad de contraseñas y el bloqueo de la cuenta.

Para obtener más información, consulte Dominio o dominio + STA.

Certificado de cliente: XenMobile puede integrarse con entidades de certificación estándar del sector para usar certificados como método único de la autenticación en línea. XenMobile ofrece este certificado una vez los usuarios se han inscrito, por lo que requiere una contraseña de un solo uso, una URL de invitación o credenciales LDAP. Cuando se usa un certificado de cliente como el método principal de autenticación, se necesita un PIN de Citrix en entornos de solo certificado de cliente para proteger el certificado en el dispositivo.

XenMobile solo admite la lista de revocación de certificados (CRL) cuando se trata de una entidad de certificación (CA) de terceros. Si dispone de una entidad de certificación de Microsoft configurada, XenMobile utiliza Citrix ADC para administrar la revocación. Al configurar la autenticación por certificados de cliente, plantéese si es necesario configurar el parámetro de lista de revocación de certificados (CRL) de Citrix ADC, Enable CRL Auto Refresh. Este paso garantiza que el usuario de un dispositivo en modo solo MAM no pueda autenticarse con 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.

Para ver un diagrama que muestre la implementación necesaria si va a usar la autenticación basada en certificados para los usuarios o si necesita usar la entidad de certificación (CA) de su empresa para emitir los certificados de dispositivo, consulte Arquitectura de referencia para implementaciones locales.

Dos factores

LDAP + Certificado de cliente: 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 Citrix ADC. Al usar certificados de cliente y LDAP conjuntamente, la seguridad se basa en algo que los usuarios conocen (sus contraseñas de Active Directory) y en algo que poseen (certificados de cliente en sus dispositivos). Secure Mail (y otras aplicaciones móviles de productividad) puede configurar y proporcionar automáticamente una experiencia de primer uso perfecta junto con la autenticación de certificados de cliente, con un entorno de acceso al servidor Exchange configurado correctamente. Para una experiencia de uso óptima, puede combinar esta opción con el PIN de Citrix y el almacenamiento en caché de contraseñas de Active Directory.

LDAP + token: Esta configuración permite la configuración clásica de credenciales LDAP y una contraseña de un solo uso, mediante el protocolo RADIUS. Para una experiencia de uso óptima, puede combinar esta opción con el PIN de Citrix y el almacenamiento en caché de contraseñas de Active Directory.

Directivas, configuraciones y propiedades de cliente importantes necesarias para la autenticación

Las siguientes propiedades de cliente, configuraciones y directivas intervienen en las tres configuraciones recomendadas indicadas más adelante:

Directivas MDX

Código de acceso de aplicación: Cuando se establece en **Sí**, se requiere un PIN o un código de acceso de Citrix para desbloquear la aplicación cuando ésta se inicia o se reanuda después de un período de inactividad. De forma predeterminada, está **activado**.

Para configurar el temporizador de inactividad para todas las aplicaciones, establezca el valor de INACTIVITY_TIMER en minutos, en la consola de XenMobile, desde la ficha **Parámetros**, en **Propiedades de cliente**. El valor predeterminado es 15 minutos. Para inhabilitar el temporizador de inactividad, de modo que la petición de PIN o código de acceso aparezca solo cuando se inicie la aplicación, establezca un valor de cero.

> **Nota:**
>
> Si selecciona Acceso seguro sin conexión para la directiva Claves de cifrado, esta directiva se habilita automáticamente.

Sesión con conexión requerida: Cuando se establece en **Sí**, el usuario debe contar con una sesión activa y una conexión a la red de la empresa para poder acceder a la aplicación presente en el dispositivo. Cuando se establece en **No**, no se requiere una sesión activa para poder acceder a la aplicación presente en el dispositivo. Está **desactivado** de forma predeterminada.

Período máximo sin conexión (horas): Define el período de tiempo máximo que una aplicación puede ejecutarse sin tener que volver a confirmar los derechos a utilizarla ni actualizar las directivas desde XenMobile. Cuando establece la directiva MDX "Período máximo sin conexión", si Secure Hub para iOS tiene un token válido de Citrix Gateway, la aplicación obtiene de XenMobile directivas nuevas para aplicaciones MDX sin interrupciones para los usuarios. En cambio, si Secure Hub no tiene un token válido de Citrix ADC, los usuarios deben autenticarse en Secure Hub para que se actualicen las directivas de las aplicaciones. El token de Citrix ADC puede dejar de ser válido debido a la inactividad en la sesión de Citrix Gateway o a alguna directiva de tiempo de espera forzado para la sesión. Cuando los usuarios vuelvan a iniciar sesión en Secure Hub, podrán continuar ejecutando la aplicación.

Los usuarios reciben un recordatorio para que inicien sesión 30, 15 y 5 minutos antes de que acabe el período. Una vez se acabe el período, la aplicación se bloquea hasta que los usuarios inicien sesión. El valor predeterminado es **72 horas (3 días)**. El período mínimo de tiempo es 1 hora.

> **Nota:**
>
> Tenga en cuenta que, cuando los usuarios viajan con frecuencia y usan la itinerancia internacional, el valor predeterminado de 72 horas (3 días) puede ser demasiado corto.

Caducidad del tíquet de servicios en segundo plano: El período de validez que tiene un tíquet del servicio de red en segundo plano. Cuando Secure Mail se conecta a través de Citrix Gateway a un servidor de Exchange con ActiveSync, XenMobile emite un token que Secure Mail usa para conectarse al servidor de Exchange interno. Esta propiedad determina cuánto tiempo Secure Mail puede usar el token sin necesidad de uno nuevo para la autenticación y la conexión con Exchange Server. Cuando se

alcanza el límite de tiempo, los usuarios deben volver a iniciar sesión para generar un nuevo token. El valor predeterminado es **168 horas (7 días)**. Cuando se agota este tiempo de espera, se interrumpen las notificaciones por correo.

Período de gracia para requerir sesión con conexión: Determina cuántos minutos puede un usuario utilizar una aplicación sin conexión, antes de que la directiva "Sesión con conexión requerida" le impida seguir utilizándola (hasta que la sesión con conexión sea validada). El valor predeterminado es 0 (no hay período de gracia).

Para obtener información acerca de las directivas de autenticación, consulte:

- Si utiliza el SDK de MAM: Introducción al SDK de MAM
- Si usa MDX Toolkit: Directivas MDX para iOS y Directivas MDX para Android

Propiedades de cliente XenMobile

> **Nota:**
>
> Las propiedades de cliente son una configuración global que se aplica a todos los dispositivos que se conectan a XenMobile.

PIN de Citrix: Para una experiencia sencilla de inicio de sesión, puede optar por habilitar el PIN de Citrix. Con el PIN, los usuarios no tienen que introducir repetidamente otras credenciales (como los nombres de usuario y las contraseñas de Active Directory). Puede configurar el PIN de Citrix como una autenticación independiente que solo funciona sin conexión. También puede combinar el PIN con el almacenamiento en caché de contraseñas de Active Directory para una usabilidad óptima y fluida. Configure el PIN de Citrix en **Parámetros > Cliente > Propiedades de cliente** en la consola de XenMobile.

A continuación dispone de un resumen con algunas propiedades importantes. Para obtener más información, consulte Propiedades de cliente.

ENABLE_PASSCODE_AUTH

Nombre simplificado: Enable Citrix PIN Authentication

Esta clave 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. Habilite esta configuración si la propiedad **ENABLE_PASSWORD_CACHING** está habilitada o si XenMobile usa la autenticación por certificado.

Valores posibles: true o **false**

Valor predeterminado: false

ENABLE_PASSWORD_CACHING

Nombre simplificado: Enable User Password Caching

Esta clave permite que la contraseña de Active Directory de los usuarios se almacene en la memoria caché local del dispositivo móvil. Al establecer esta clave en true, se solicita a los usuarios que establezcan un PIN o un código de acceso de Citrix. El valor de la clave ENABLE_PASSCODE_AUTH debe establecerse en true cuando esta clave se establece en **true**.

Valores posibles: true o **false**

Valor predeterminado: false

PASSCODE_STRENGTH

Nombre simplificado: PIN Strength Requirement

Esta clave 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

INACTIVITY_TIMER

Nombre simplificado: Inactivity Timer

Esta clave define el tiempo en minutos que los usuarios pueden dejar su dispositivo inactivo y luego acceder a una aplicación sin que se solicite un PIN o un código de acceso de Citrix. Si quiere habilitar esta configuración para una aplicación MDX, debe **activar** la configuración "Código de acceso de aplicación". Si el parámetro Código de acceso de aplicación está **desactivado**, se redirige a los usuarios a Secure Hub para realizar una autenticación completa. Al cambiar este parámetro, el valor se aplicará la próxima vez que los usuarios deban autenticarse. El valor predeterminado es 15 minutos.

ENABLE_TOUCH_ID_AUTH

Nombre simplificado: Enable Touch ID Authentication

Permite el uso del lector de huellas dactilares (solo en iOS) para la autenticación sin conexión. La autenticación en línea aún requerirá el método de autenticación principal.

ENCRYPT_SECRETS_USING_PASSCODE

Nombre simplificado: Encrypt secrets using Passcode

Esta clave permite que los datos confidenciales se almacenen en el dispositivo móvil, en un almacén secreto, en lugar de guardarse en un almacén nativo basado en la plataforma, como el llavero de iOS. Esta clave de configuración permite un cifrado seguro de los objetos clave, pero también agrega la entropía de usuario (un código PIN aleatorio generado por el usuario y que solo el usuario conoce).

Valores posibles: true o **false**

Valor predeterminado: false

Configuración de Citrix ADC

Tiempo de desconexión de la sesión: Si se habilita esta configuración, Citrix Gateway desconecta la sesión si Citrix ADC no detecta ninguna actividad de red durante un intervalo especificado. Esta configuración se aplica a los usuarios que se conectan con Citrix Gateway Plug-in, Citrix Receiver, Secure Hub o mediante un explorador web. El valor predeterminado es **1440 minutos**. Si se establece este valor en cero, el parámetro queda inhabilitado.

Tiempo de espera forzado: Si habilita este parámetro, Citrix Gateway desconecta la sesión una vez transcurrido el intervalo del tiempo de espera, independientemente de la actividad del usuario. No existe ninguna acción que el usuario pueda realizar para evitar que se produzca la desconexión cuando se agota el tiempo de espera. Esta configuración se aplica a los usuarios que se conectan con Citrix Gateway Plug-in, Citrix Receiver, Secure Hub o mediante un explorador web. Si Secure Mail usa STA, un modo especial de Citrix ADC, el parámetro "Tiempo de espera forzado" no se aplica a las sesiones de Secure Mail. El valor predeterminado es **1440 minutos**. Si deja este valor en blanco, la configuración se desactiva.

Para obtener más información sobre parámetros de tiempo de espera en Citrix Gateway, consulte la documentación de Citrix ADC.

Para obtener más información acerca de los casos en que se solicita a los usuarios que se autentiquen en XenMobile con credenciales en sus dispositivos, consulte Situaciones de petición de credenciales.

Parámetros predeterminados de configuración

Estos parámetros son los valores predeterminados proporcionados por:

- Asistente de NetScaler para XenMobile
- SDK de MAM o MDX Toolkit
- Consola de XenMobile

Parámetro	Dónde encontrar el parámetro	Configuración predeterminada
Tiempo de desconexión de la sesión	Citrix Gateway	1440 minutos
Tiempo de espera forzado	Citrix Gateway	1440 minutos
Período máximo sin conexión	Directivas MDX	72 horas
Caducidad del tíquet de servicios en segundo plano	Directivas MDX	168 horas (7 días)
Sesión con conexión requerida	Directivas MDX	No

Parámetro	Dónde encontrar el parámetro	Configuración predeterminada
Período de gracia para requerir sesión con conexión	Directivas MDX	0
Código de acceso de aplicación	Directivas MDX	Sí
Cifrar secretos mediante un código de acceso	Propiedades de cliente XenMobile	false
Enable Citrix PIN Authentication	Propiedades de cliente XenMobile	false
Requisito de seguridad de código PIN	Propiedades de cliente XenMobile	Medio
Tipo de código PIN	Propiedades de cliente XenMobile	Numérico
Enable User Password Caching (Habilitar almacenamiento en caché de la contraseña del usuario)	Propiedades de cliente XenMobile	false
Inactivity Timer (Temporizador de inactividad)	Propiedades de cliente XenMobile	15
Enable Touch ID Authentication	Propiedades de cliente XenMobile	false

Configuraciones recomendadas

En esta sección se ofrecen ejemplos de tres configuraciones de XenMobile, desde la configuración de seguridad más baja y la experiencia de usuario óptima, hasta la configuración de mayor seguridad y experiencia de usuario más intrusiva. El objetivo de estos ejemplos es proporcionarle puntos de referencia para decidir a qué altura de la escala quiere colocar su propia configuración. Tenga en cuenta que modificar estas configuraciones puede requerir que modifique otras configuraciones también. Por ejemplo, el "Periodo máximo sin conexión" siempre debe ser menor que "Session time-out" (Tiempo de desconexión de la sesión).

Highest Security (El mayor nivel de seguridad)

Esta configuración ofrece el nivel más alto de seguridad, pero contiene inconvenientes significativos para la facilidad de uso.

Parámetro	Dónde encontrar el parámetro	Configuración recomendada	Impacto en el comportamiento
Tiempo de desconexión de la sesión	Citrix Gateway	1440	Los usuarios introducen sus credenciales de Secure Hub solo cuando se necesita la autenticación en línea (cada 24 horas)
Tiempo de espera forzado	Citrix Gateway	1440	La autenticación en línea será estrictamente requerida cada 24 horas. La actividad no prolonga la vida de la sesión.
Período máximo sin conexión	Directivas MDX	23	Requiere la actualización de la directiva cada día.

Caducidad del tíquet de servicios en segundo plano	Directivas MDX	72 horas	Tiempo de espera para STA, lo que permite sesiones duraderas sin token de sesión de Citrix Gateway. En el caso de Secure Mail, aumentar el tiempo de espera de STA más del tiempo de espera de sesión evita que las notificaciones de correo dejen de recibirse sin solicitar al usuario si este no abre la aplicación antes de que se agote el tiempo de espera de la sesión.
Sesión con conexión requerida	Directivas MDX	No	Garantiza una conexión de red válida y una sesión de Citrix Gateway para usar aplicaciones.
Período de gracia para requerir sesión con conexión	Directivas MDX	0	Sin período de gracia (si habilitó “Sesión con conexión requerida”).
Código de acceso de aplicación	Directivas MDX	Sí	Requerir código de acceso para la aplicación.
Cifrar secretos mediante un código de acceso	Propiedades de cliente XenMobile	true	Una clave derivada de la entropía del usuario protege la caja fuerte.

Enable Citrix PIN Authentication	Propiedades de cliente XenMobile	true	El PIN de Citrix simplifica la experiencia de autenticación del usuario.
Requisito de seguridad de código PIN	Propiedades de cliente XenMobile	Fuerte	Altos requisitos de complejidad para la contraseña.
Tipo de código PIN	Propiedades de cliente XenMobile	Alfanumérico	El PIN es una secuencia alfanumérica.
Habilitar	Propiedades de cliente XenMobile	false	La contraseña de Active Directory no se almacena en caché y el PIN de Citrix se usará para las autenticaciones sin conexión.
Inactivity Timer (Temporizador de inactividad)	Propiedades de cliente XenMobile	15	Si el usuario no usa Secure Hub o las aplicaciones MDX durante este período de tiempo, se pide la autenticación sin conexión.
Enable Touch ID Authentication	Propiedades de cliente XenMobile	false	Inhabilita Touch ID para casos de autenticación sin conexión en iOS.

Higher Security (Mayor nivel de seguridad)

Con un enfoque más intermedio, esta configuración requiere que los usuarios se autentiquen más a menudo, cada 3 días a lo sumo (en lugar de 7), y ofrece una mayor seguridad. Esta mayor cantidad de autenticaciones bloquea el contenedor de datos más a menudo, lo que garantiza la seguridad de los datos cuando los dispositivos no están en uso.

Parámetro	Dónde encontrar el parámetro	Configuración recomendada	Impacto en el comportamiento
Tiempo de desconexión de la sesión	Citrix Gateway	4320	Los usuarios introducen sus credenciales de Secure Hub solo cuando se necesita la autenticación en línea (cada 3 días)
Tiempo de espera forzado	Citrix Gateway	Ningún valor	Las sesiones se extenderán si hay alguna actividad.
Período máximo sin conexión	Directivas MDX	71	Requiere la actualización de la directiva cada 3 días. La diferencia de hora es para permitir la actualización antes de que se agote el Tiempo de desconexión de la sesión (Session time-out).

Caducidad del tíquet de servicios en segundo plano	Directivas MDX	168 horas	Tiempo de espera para STA, lo que permite sesiones duraderas sin token de sesión de Citrix Gateway. En el caso de Secure Mail, aumentar el tiempo de espera de STA más del tiempo de espera de sesión evita que las notificaciones de correo dejen de recibirse sin solicitar al usuario si este no abre la aplicación antes de que se agote el tiempo de espera de la sesión.
Sesión con conexión requerida	Directivas MDX	No	Garantiza una conexión de red válida y una sesión de Citrix Gateway para usar aplicaciones.
Período de gracia para requerir sesión con conexión	Directivas MDX	0	Sin período de gracia (si habilitó “Sesión con conexión requerida”).
Código de acceso de aplicación	Directivas MDX	Sí	Requerir código de acceso para la aplicación.
Cifrar secretos mediante un código de acceso	Propiedades de cliente XenMobile	false	No se requiere entropía de usuario para cifrar la caja fuerte.

Enable Citrix PIN Authentication	Propiedades de cliente XenMobile	true	El PIN de Citrix simplifica la experiencia de autenticación del usuario.
Requisito de seguridad de código PIN	Propiedades de cliente XenMobile	Medio	Aplica reglas de complejidad media a la contraseña.
Tipo de código PIN	Propiedades de cliente XenMobile	Numérico	El PIN es una secuencia numérica.
Habilitar	Propiedades de cliente XenMobile	true	El PIN del usuario se almacena en caché y protege la contraseña de Active Directory.
Inactivity Timer (Temporizador de inactividad)	Propiedades de cliente XenMobile	30	Si el usuario no usa Secure Hub o las aplicaciones MDX durante este período de tiempo, se pide la autenticación sin conexión.
Enable Touch ID Authentication	Propiedades de cliente XenMobile	true	Permite Touch ID para casos de autenticación sin conexión en iOS.

High Security (Nivel alto de seguridad)

Esta configuración, la más conveniente para los usuarios, proporciona una seguridad base.

Parámetro	Dónde encontrar el parámetro	Configuración recomendada	Impacto en el comportamiento

Tiempo de desconexión de la sesión	Citrix Gateway	10080	Los usuarios introducen sus credenciales de Secure Hub solo cuando se necesita la autenticación en línea (cada 7 días)
Tiempo de espera forzado	Citrix Gateway	Ningún valor	Las sesiones se extenderán si hay alguna actividad.
Período máximo sin conexión	Directivas MDX	167	Requiere una actualización de directivas por semana (cada 7 días). La diferencia de hora es para permitir la actualización antes de que se agote el Tiempo de desconexión de la sesión (Session time-out).

Caducidad del tíquet de servicios en segundo plano	Directivas MDX	240	Tiempo de espera para STA, lo que permite sesiones duraderas sin token de sesión de Citrix Gateway. En el caso de Secure Mail, aumentar el tiempo de espera de STA más del tiempo de espera de sesión evita que las notificaciones de correo dejen de recibirse sin solicitar al usuario si este no abre la aplicación antes de que se agote el tiempo de espera de la sesión.
Sesión con conexión requerida	Directivas MDX	No	Garantiza una conexión de red válida y una sesión de Citrix Gateway para usar aplicaciones.
Período de gracia para requerir sesión con conexión	Directivas MDX	0	Sin período de gracia (si habilitó “Sesión con conexión requerida”).
Código de acceso de aplicación	Directivas MDX	Sí	Requerir código de acceso para la aplicación.
Cifrar secretos mediante un código de acceso	Propiedades de cliente XenMobile	false	No se requiere entropía de usuario para cifrar la caja fuerte.

Enable Citrix PIN Authentication	Propiedades de cliente XenMobile	true	El PIN de Citrix simplifica la experiencia de autenticación del usuario.
Requisito de seguridad de código PIN	Propiedades de cliente XenMobile	Bajo	Sin requisitos de complejidad para la contraseña
Tipo de código PIN	Propiedades de cliente XenMobile	Numérico	El PIN es una secuencia numérica.
Habilitar	Propiedades de cliente XenMobile	true	El PIN del usuario se almacena en caché y protege la contraseña de Active Directory.
Inactivity Timer (Temporizador de inactividad)	Propiedades de cliente XenMobile	90	Si el usuario no usa Secure Hub o las aplicaciones MDX durante este período de tiempo, se pide la autenticación sin conexión.
Enable Touch ID Authentication	Propiedades de cliente XenMobile	true	Permite Touch ID para casos de autenticación sin conexión en iOS.

Usar una autenticación de nivel superior

Algunas aplicaciones pueden requerir una autenticación mejorada (por ejemplo, un factor secundario de autenticación, como un token, o tiempos agresivos de desconexión de la sesión). Se puede controlar este método de autenticación a través de una directiva MDX. El método también requiere un servidor virtual independiente para controlar los métodos de autenticación (en el mismo dispositivo Citrix ADC o en varios).

Parámetro	Dónde encontrar el parámetro	Configuración recomendada	Impacto en el comportamiento
Citrix Gateway alternativo	Directivas MDX	Requiere el FQDN y el puerto del dispositivo Citrix ADC secundario.	Permite la autenticación mejorada, controlada por las directivas de sesión y autenticación del dispositivo Citrix ADC secundario.

Si un usuario abre una aplicación que inicia sesión en la instancia de Citrix Gateway alternativo, todas las demás aplicaciones usarán esa instancia de Citrix Gateway para la comunicación con la red interna. La sesión solo volverá a la instancia de menor seguridad de Citrix Gateway cuando se agote su tiempo de espera en la instancia de Citrix Gateway con seguridad mejorada.

Usar la sesión con conexión requerida

Para ciertas aplicaciones, como Secure Web, puede que le interese asegurarse de que los usuarios ejecuten una aplicación solo cuando tienen una sesión autenticada y mientras el dispositivo está conectado a una red. Esta directiva aplica esa opción y permite un período de gracia para que los usuarios puedan finalizar su trabajo.

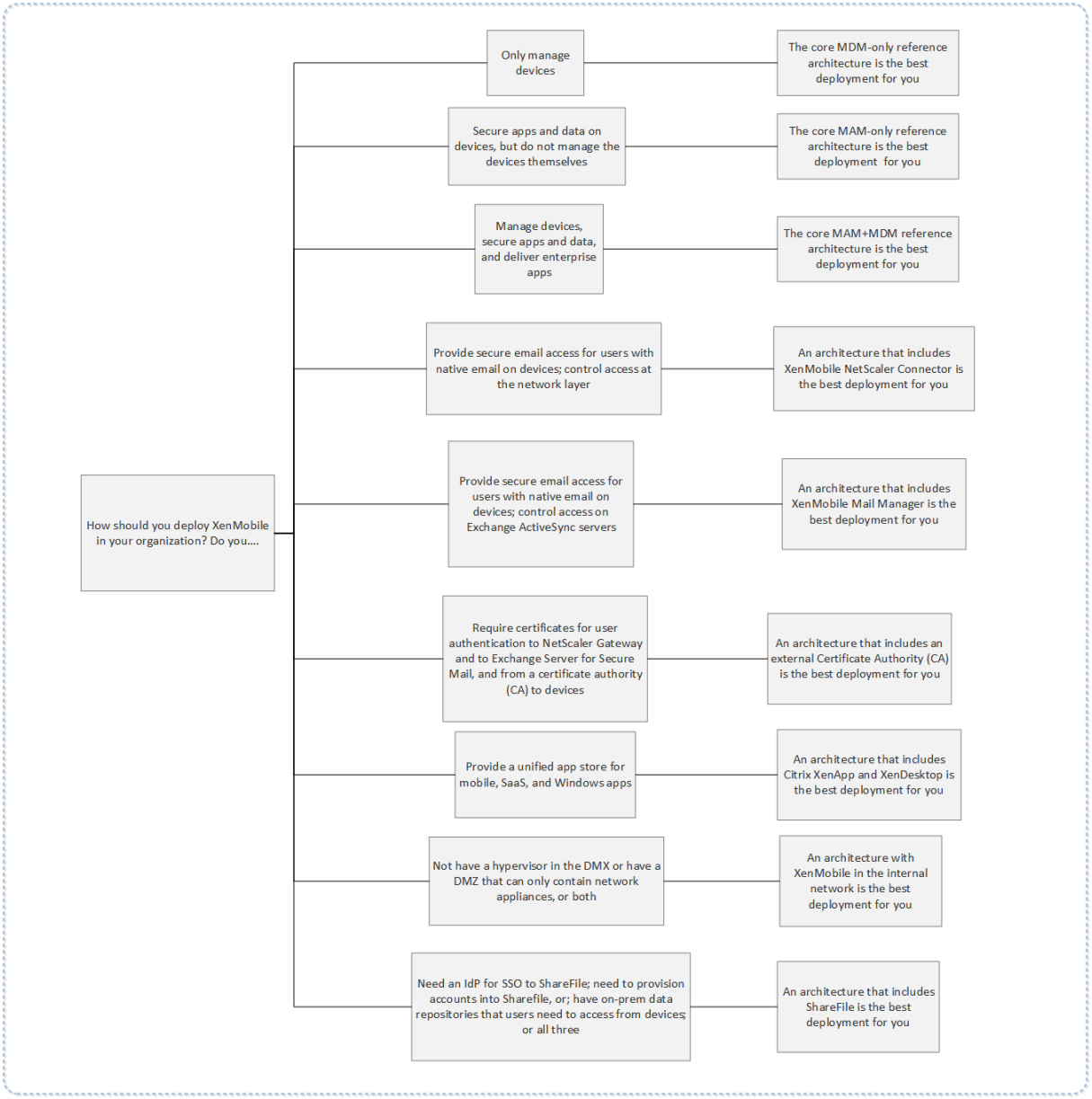
Parámetro	Dónde encontrar el parámetro	Configuración recomendada	Impacto en el comportamiento
Sesión con conexión requerida	Directivas MDX	Sí	Garantiza que el dispositivo está conectado y tiene un token de autenticación válido.
Período de gracia para requerir sesión con conexión	Directivas MDX	15	Permite un período de gracia de 15 minutos antes de que el usuario ya no pueda usar las aplicaciones

Arquitectura de referencia para implementaciones locales

January 4, 2022

En las siguientes imágenes, se muestran las arquitecturas de referencia para la implementación local de XenMobile. Las implementaciones pueden ser: solo MDM, solo MAM, MDM junto con MAM como arquitecturas principales, así como aquellas que incluyen componentes, como SNMP Manager, el conector de Citrix Gateway para Exchange ActiveSync, el conector de Endpoint Management para Exchange ActiveSync y Virtual Apps and Desktops. En las imágenes se muestran los componentes mínimos requeridos para XenMobile.

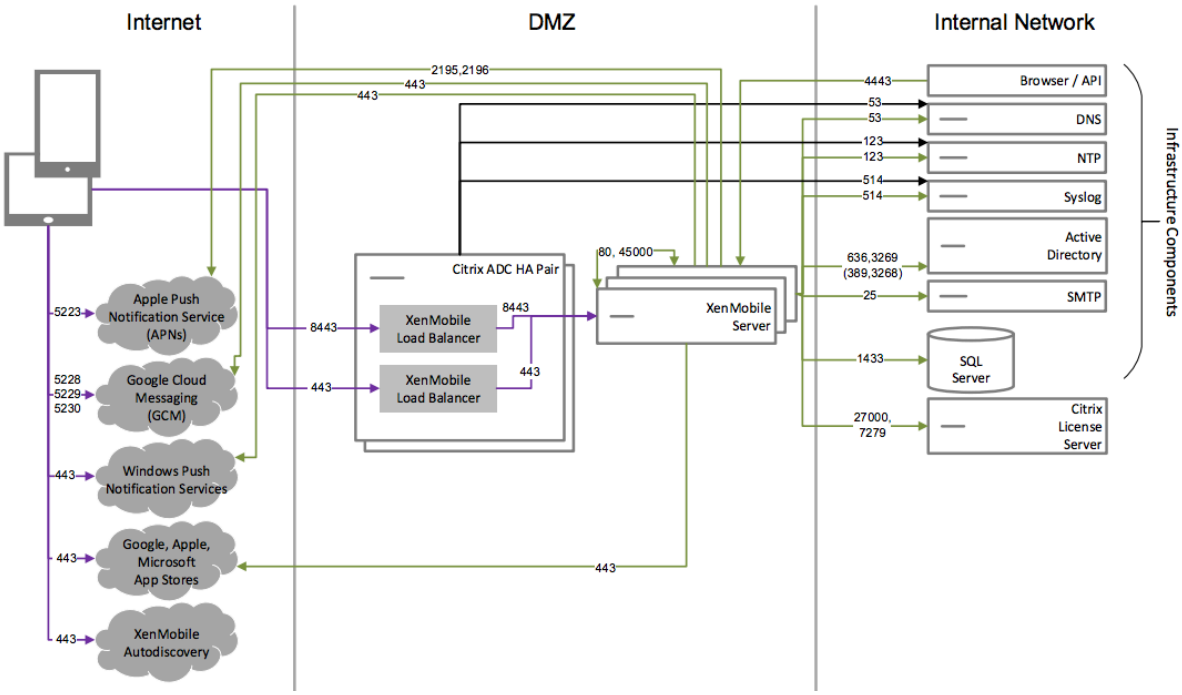
Utilice este diagrama como una guía general para las decisiones de implementación.



En las imágenes, los números de los conectores representan los puertos que se deben abrir para permitir las conexiones entre los componentes. Para ver una lista completa de los puertos, consulte Requisitos de puertos en la documentación de XenMobile.

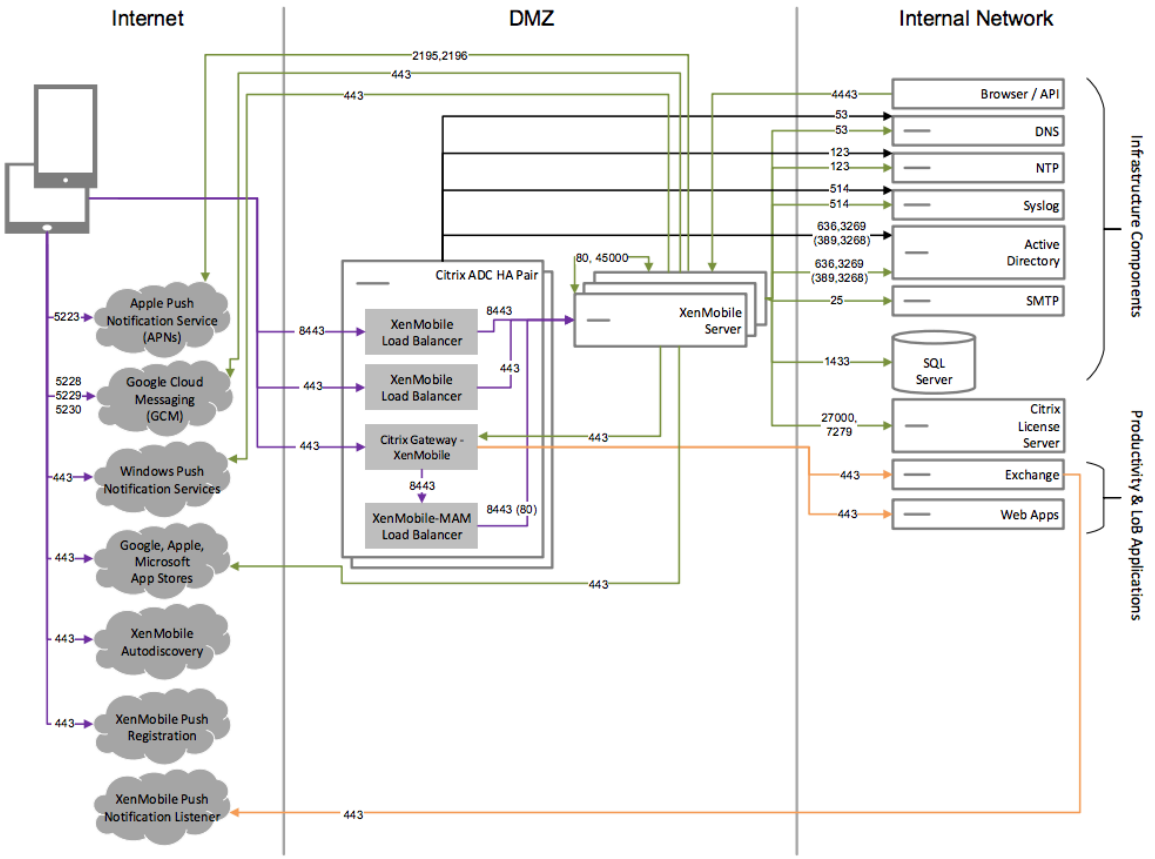
Arquitectura principal de referencia para solo MDM

Implemente esta arquitectura si va a utilizar solamente las funciones 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.



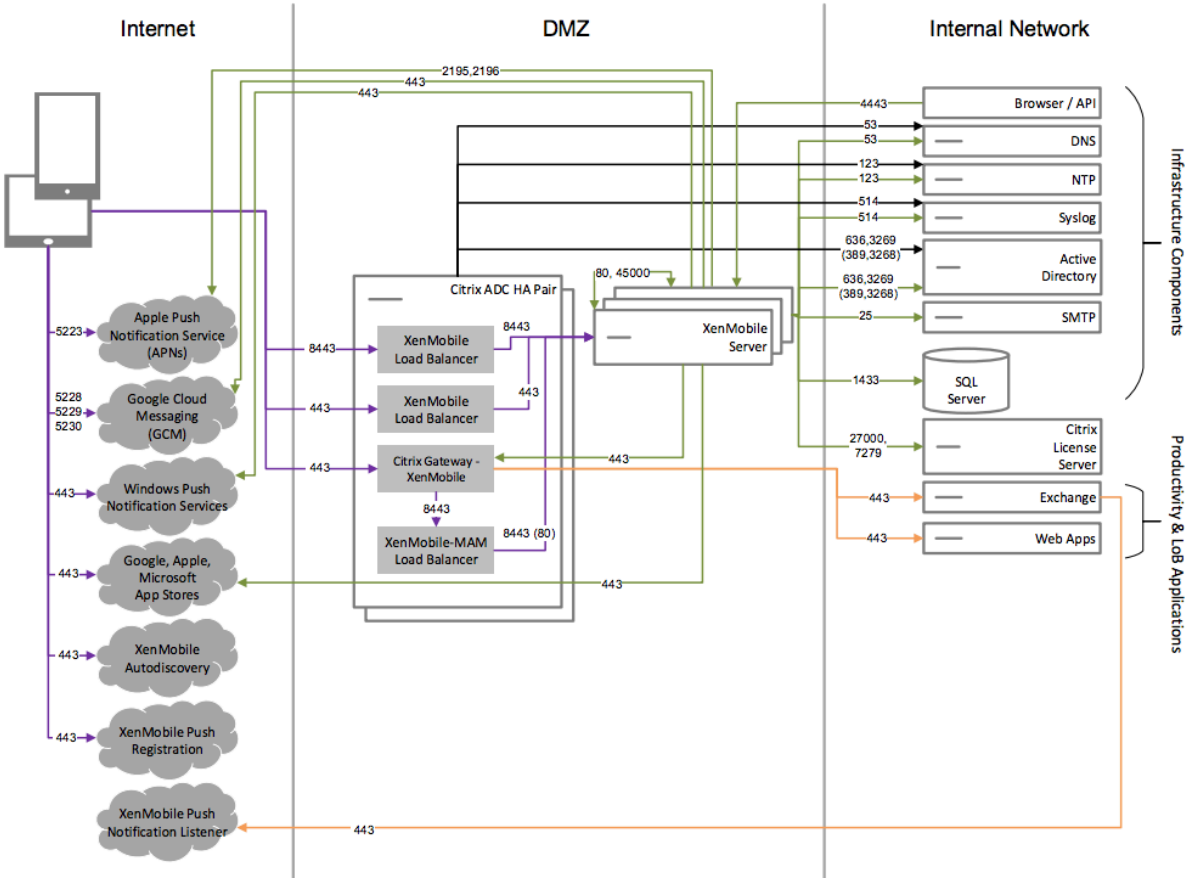
Arquitectura principal de referencia para solo MAM

Implemente esta arquitectura si va a utilizar solamente las funciones MAM de XenMobile sin hacer que los dispositivos se inscriban para la administración 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.



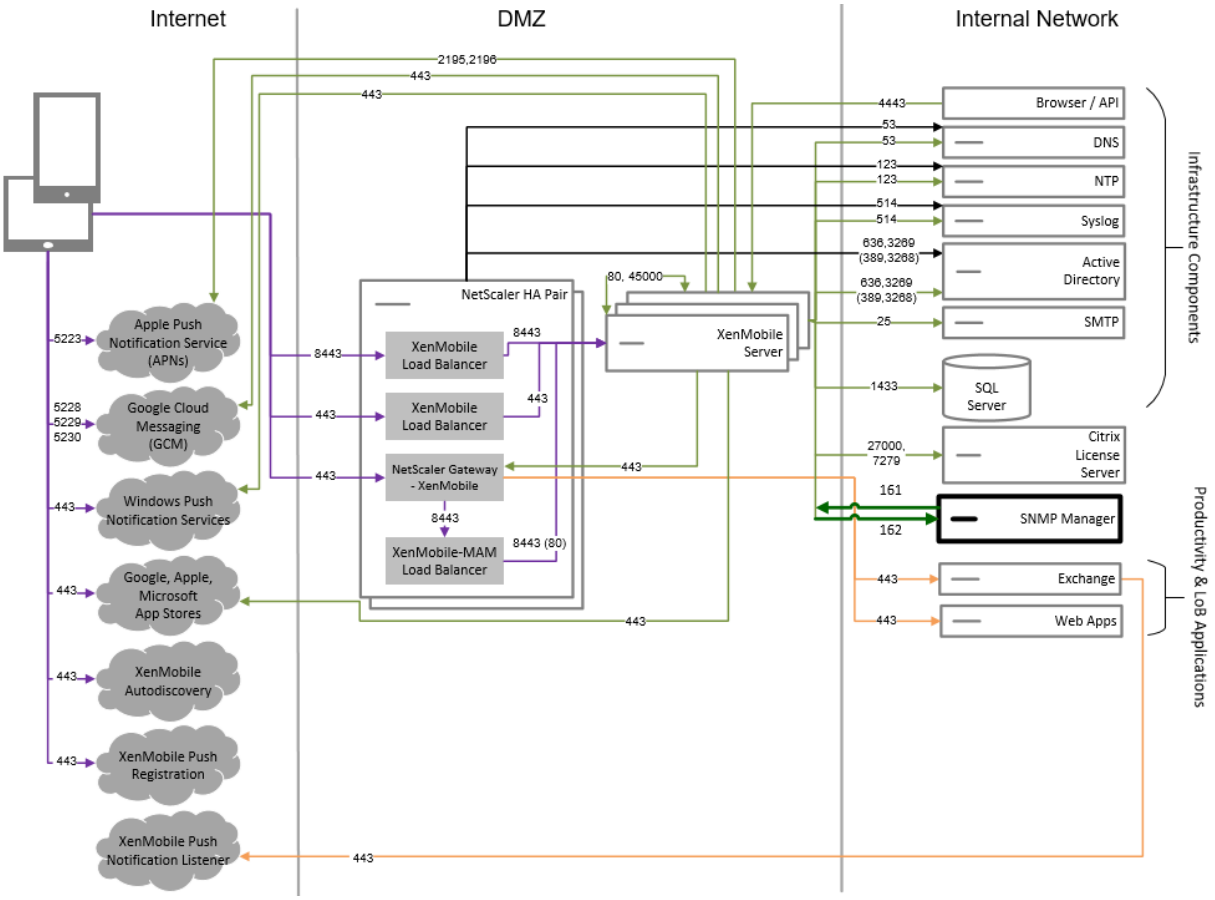
Arquitectura principal de referencia para MAM y MDM

Implemente esta arquitectura si va a utilizar las funciones de MDM y MAM de XenMobile. Por ejemplo, elija este modo si quiere administrar dispositivos entregados por la empresa a través de MDM, quiere implementar directivas de dispositivo y aplicación, obtener un inventario de activos y poder borrar dispositivos. En este caso, también quiere poder entregar aplicaciones móviles de la empresa, bloquear aplicaciones y borrar los datos en los dispositivos.



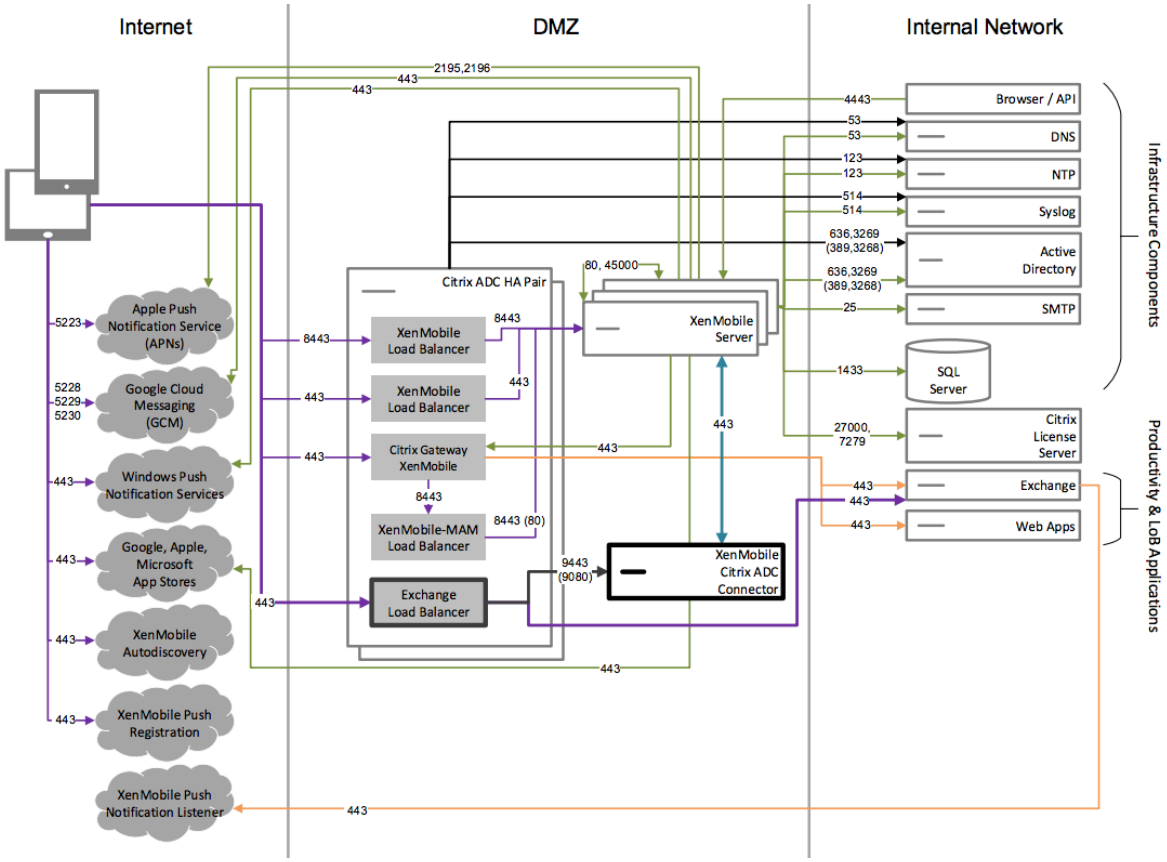
Arquitectura de referencia con SNMP

Implemente esta arquitectura si va a habilitar la supervisión de SNMP con XenMobile. Por ejemplo, para que los sistemas de supervisión consulten y obtengan información sobre los nodos de XenMobile. Para obtener información más detallada, consulte Supervisión de SNMP.



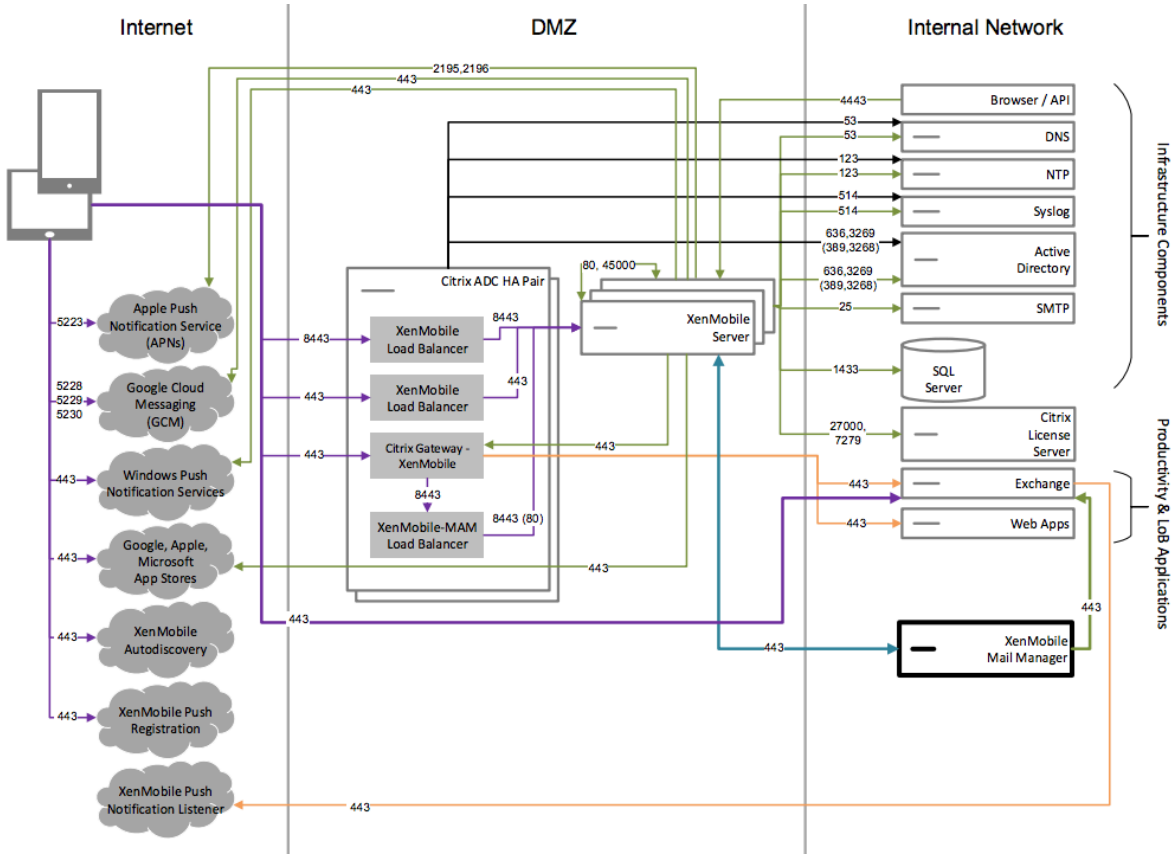
Arquitectura de referencia con el conector de Citrix Gateway para Exchange ActiveSync

Implemente esta arquitectura si tiene previsto utilizar el conector de Citrix Gateway para Exchange ActiveSync con XenMobile. Por ejemplo, para ofrecer acceso seguro al correo electrónico para los usuarios que usan aplicaciones móviles nativas de correo electrónico. Esos usuarios seguirán accediendo al correo electrónico a través de una aplicación nativa, aunque también puede hacer una transición paulatina a Citrix Secure Mail. El acceso debe controlarse en la capa de red, antes de que el tráfico llegue a los servidores de Exchange Active Sync. Aunque en el diagrama se muestre el conector para Exchange ActiveSync implementado en una arquitectura de MDM y MAM, puede implementarlo de la misma manera cuando forma parte de una arquitectura de solo MDM.



Arquitectura de referencia con el conector de Endpoint Management para Exchange ActiveSync

Implemente esta arquitectura si tiene previsto utilizar el conector de Endpoint Management para Exchange ActiveSync con XenMobile. Por ejemplo, para ofrecer acceso seguro al correo electrónico para los usuarios que usan aplicaciones móviles nativas de correo electrónico. Esos usuarios seguirán accediendo al correo electrónico a través de una aplicación nativa, aunque también puede hacer una transición paulatina a Secure Mail. Puede controlar el acceso a los servidores de Exchange ActiveSync. Aunque en el diagrama se muestre el conector de Endpoint Management para Exchange ActiveSync implementado en una arquitectura de MDM y MAM, puede implementarlo de la misma manera cuando forma parte de una arquitectura de solo MDM.

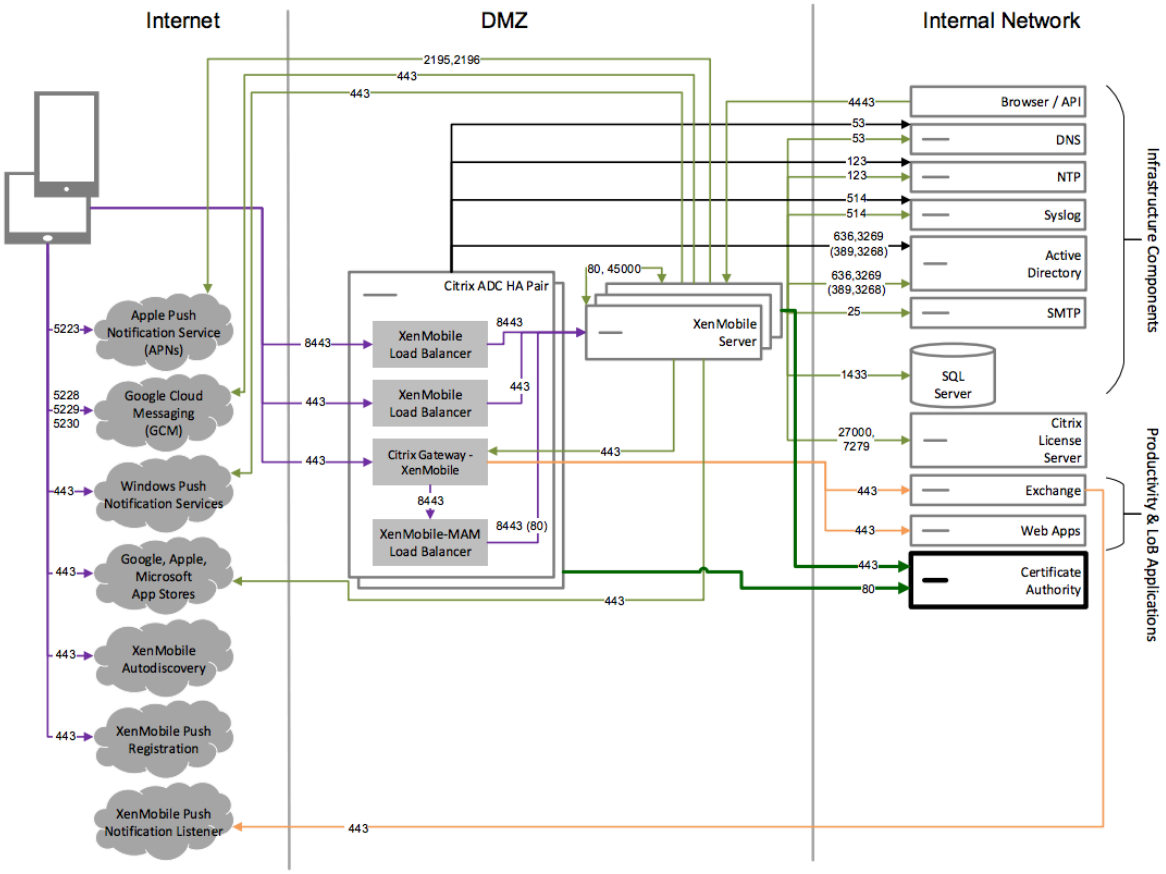


Arquitectura de referencia con una entidad de certificación externa

Se recomienda una implementación que incluya una entidad de certificación externa para cumplir uno o varios de los siguientes requisitos:

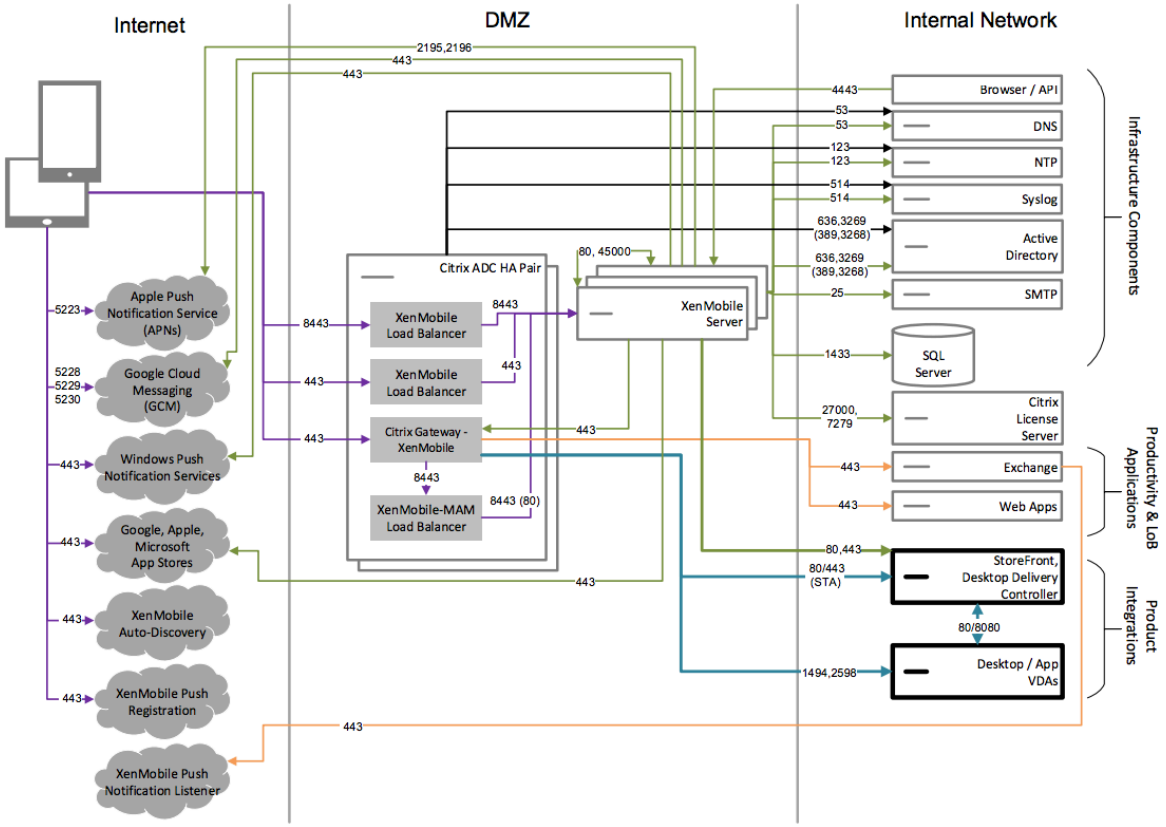
- Necesita certificados de usuario para la autenticación de usuarios en Citrix Gateway (para el acceso a la intranet).
- Necesita que los usuarios de Secure Mail se autentiquen en Exchange Server mediante un certificado de usuario.
- Debe enviar certificados emitidos por la entidad de certificación de empresa a los dispositivos móviles para el acceso a la red inalámbrica, por ejemplo.

Aunque en el diagrama se muestre una entidad de certificación externa implementada en una arquitectura de MDM y MAM, puede implementarla de la misma manera cuando forma parte de una arquitectura de solo MDM o solo MAM.



Arquitectura de referencia con Virtual Apps and Desktops

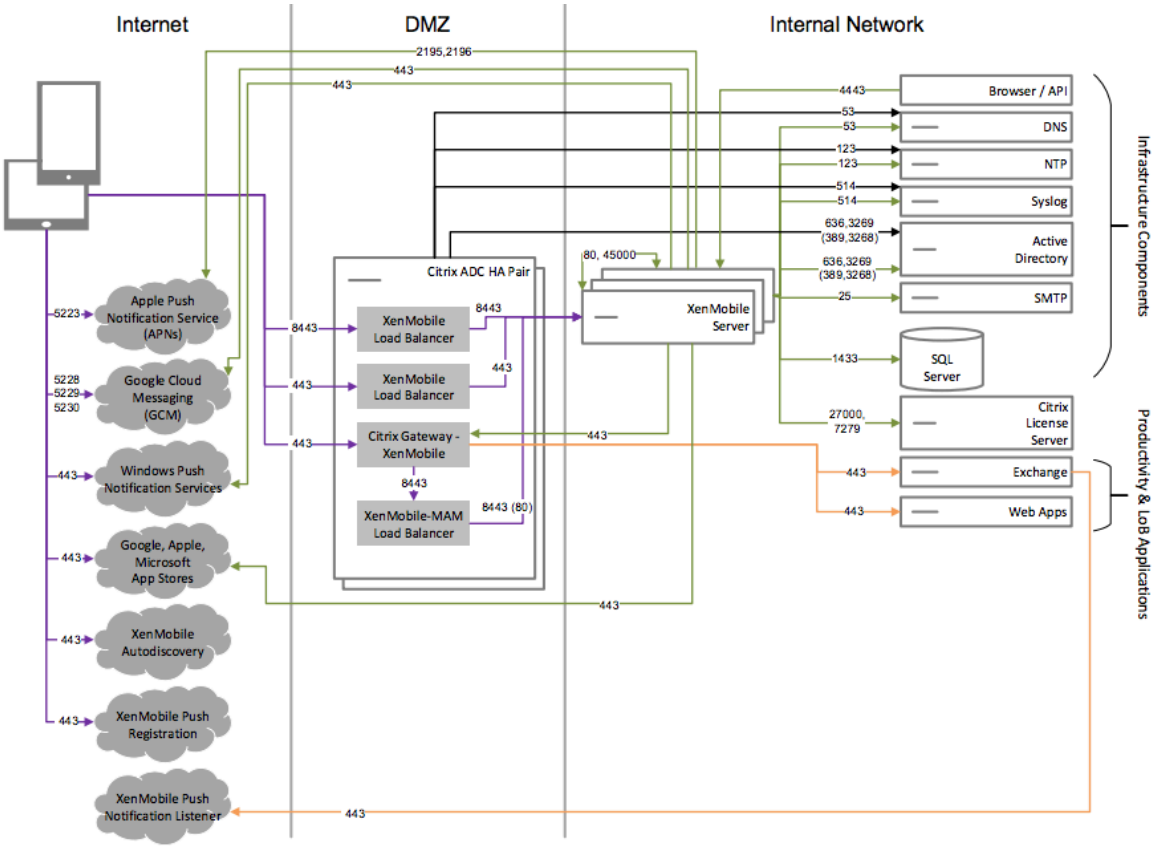
Implemente esta arquitectura si va a integrar Virtual Apps and Desktops en XenMobile. Por ejemplo, para ofrecer una tienda de aplicaciones unificada a usuarios móviles, que contenga todo tipo de aplicaciones (móvil, SaaS y Windows). Aunque en el diagrama se muestre Virtual Desktops implementado en una arquitectura de MDM y MAM, puede implementarlo de la misma manera cuando forma parte de una arquitectura de solo MAM.



Arquitectura de referencia con XenMobile en la red interna

Puede implementar una arquitectura con XenMobile en la red interna si se dan estas condiciones:

- No dispone de un hipervisor en la DMZ o no se le permite usar uno.
- Su DMZ solo puede contener dispositivos de red.
- Los requisitos de seguridad que tiene requieren la descarga SSL.



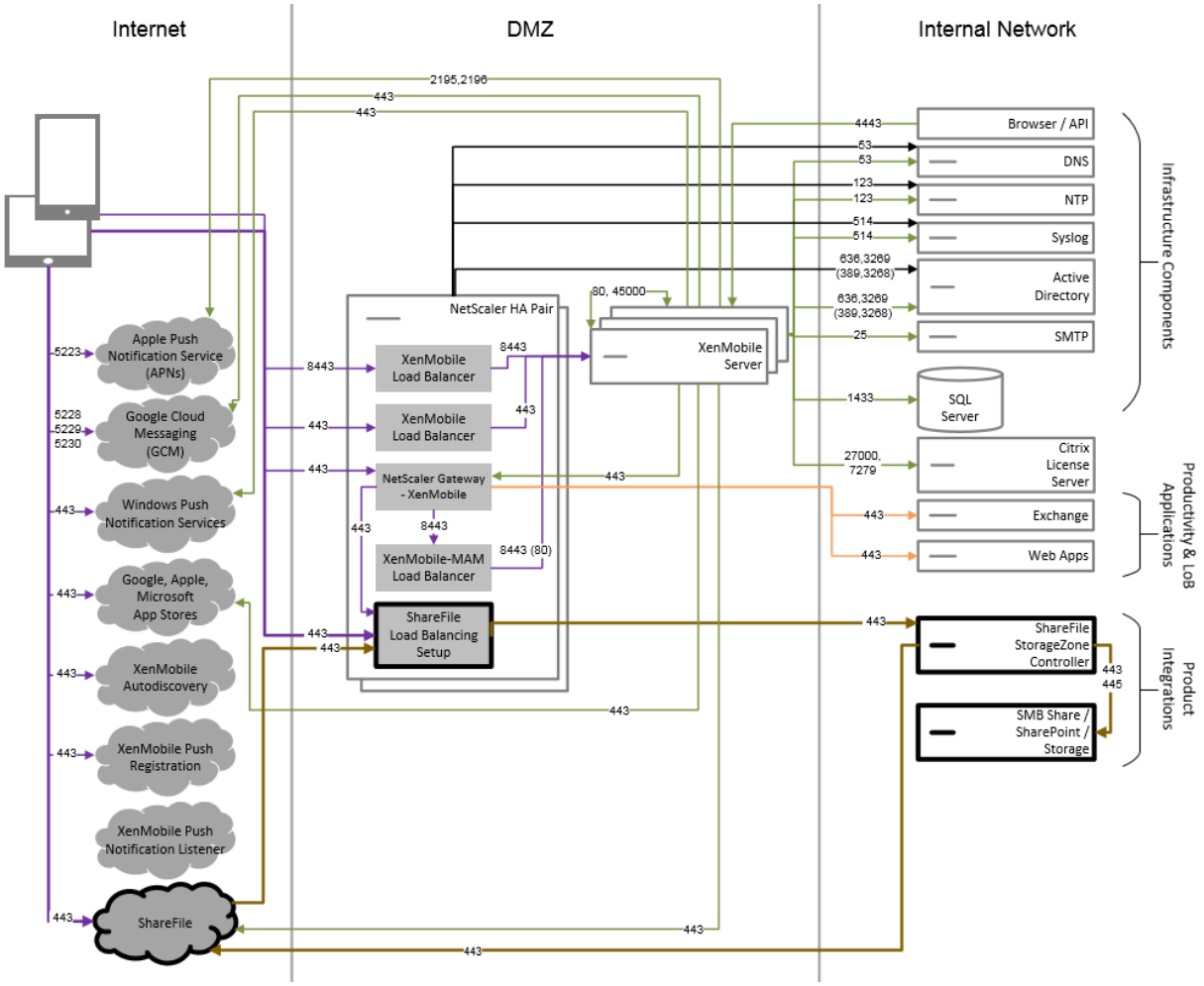
Arquitectura de referencia con Citrix Content Collaboration

Implemente esta arquitectura si quiere integrar Citrix Files o solo conectores de zonas de almacenamiento en XenMobile. La integración de Citrix Files permite cumplir uno o varios de los siguientes requisitos:

- Necesita un IdP para ofrecer a los usuarios Single Sign-On (SSO) en ShareFile.com.
- Necesita una manera de aprovisionar cuentas en ShareFile.com.
- Tiene repositorios de datos locales a los que se debe acceder desde dispositivos móviles.

Una integración con solo conectores de zonas de almacenamiento permite a los usuarios un acceso móvil seguro a los repositorios de almacenamiento locales existentes, como sitios de SharePoint y recursos compartidos de archivos de red. En esta configuración no necesita configurar ningún subdominio de Citrix Content Collaboration, aprovisionar usuarios a Citrix Files ni alojar datos de Citrix Files.

Aunque en el diagrama se muestre Citrix Files implementado en una arquitectura de MDM y MAM, puede implementarlo de la misma manera cuando forma parte de una arquitectura de solo MAM.



Propiedades de servidor

January 4, 2022

Las propiedades de servidor se aplican globalmente a operaciones, usuarios y dispositivos en toda la instancia de XenMobile. Citrix recomienda que evalúe si son útiles para su entorno las propiedades de servidor descritas en este artículo. Debe consultar con Citrix antes de cambiar otras propiedades de servidor.

Un cambio en algunas propiedades de servidor requiere un reinicio de cada nodo del servidor de XenMobile. XenMobile le notifica cuando es necesario un reinicio.

Algunas propiedades de servidor ayudan a mejorar el rendimiento y la estabilidad. Para obtener información más detallada, consulte Ajustar las operaciones de XenMobile.

Entregar aplicaciones de Android antiguo a dispositivos Android Enterprise: Si `afw.allow.legacy.apps` se establece en **`true`**, los dispositivos Android Enterprise reciben tanto aplicaciones

de Android antiguo como aplicaciones Android Enterprise. Si se establece en **false**, los dispositivos Android Enterprise solo reciben aplicaciones Android Enterprise. El valor predeterminado es **true**.

Permitir extensiones de archivo para la directiva de archivos: Configure `file.extension.whitelist` con una lista separada por comas de tipos de archivo que los administradores pueden cargar mediante la directiva de archivos. Estos tipos de archivo no se pueden cargar aunque los agregue a esta lista de permitidos:

- .cab
- .appx
- .ipa
- .apk
- .xap
- .mdx
- .exe

El valor predeterminado es `7z,rar,zip,csv,xls,xlsx,jad,jar,pdf,bmp,gif,jpg,png,pps,ppt,pptx,bsh,js,lua,mscr,pl,py,rb,sh,tcl,txt,htm,html,doc,docx,rtf,xap`.

Acceder a todas las aplicaciones en la tienda administrada de Google Play. Si es **true**, XenMobile hace que todas las aplicaciones de la tienda pública de Google Play sean accesibles desde la tienda administrada de Google Play. Al establecer esta propiedad en **true**, se permiten las aplicaciones de la tienda pública de Google Play para todos los usuarios de Android Enterprise. A continuación, los administradores pueden usar la directiva de restricciones para controlar el acceso a estas aplicaciones. El valor predeterminado es **false**.

Perfil de trabajo de Android Enterprise de trabajo en la inscripción de dispositivos que son propiedad de la empresa. Al establecer `afw.work_profile_for_corporate_owned_device.enrollment_mode.enabled` en **true**, los dispositivos con Android 11 o una versión posterior pueden inscribirse en el modo de perfil de trabajo en dispositivos propiedad de la empresa (WPCOD). La consola de XenMobile Server refleja los cambios realizados en este modo de inscripción. Si se establece en **false**, no hay parámetros de WPCOD disponibles. El valor predeterminado es **true**.

Parámetros de restricción adicionales de Android Enterprise. Si la propiedad `afw.restriction.policy.v2` se establece en **true**, estos parámetros de restricción están disponibles para dispositivos Android Enterprise:

- Permitir la desinstalación de aplicaciones
- Permitir la opción Compartir Bluetooth

Para obtener más información sobre estos parámetros, consulte Directiva de restricciones.

Restricciones de Android Enterprise para dispositivos COPE. Establezca `afw.restriction.cope` en **true** para habilitar el parámetro **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa** en la directiva de

restricciones. El valor predeterminado es **true**. Para obtener más información sobre este parámetro, consulte Directiva de restricciones.

Permitir nombres de host para enlaces de App Store de iOS: La propiedad `ios.app.store.allowed.hostnames` es una lista de nombres de host permitidos que se utilizan al cargar aplicaciones de tienda pública de aplicaciones en el servidor mediante las API públicas. Si tiene previsto cargar aplicaciones de tienda pública de aplicaciones con las API públicas, en lugar de cargarlas a través del servidor, configure esta propiedad. El valor predeterminado es `itunes.apple.com,vpp.itunes.apple.com,apps.apple.com`.

Puerto de APNs alternativo. Puede utilizar el puerto 2197 en lugar del puerto 443 para enviar y recibir notificaciones de APNs desde `api.push.apple.com`. El puerto utiliza la API del proveedor de APNs basada en HTTP/2. Establezca la propiedad `apns.http2.alternate.port.enabled` en **true** para usar el puerto 2197. El valor predeterminado de la propiedad `apns.http2.alternate.port.enabled` del servidor es **false**.

Habilitar la validación de contraseñas para evitar que los usuarios locales usen contraseñas débiles. Si `enable.password.strength.validation` se establece en **true**, no puede agregar usuarios locales con contraseñas débiles. Si se establece en **false**, puede crear usuarios locales con contraseñas débiles mediante la API pública. El valor predeterminado es **true**.

Bloquear inscripción de dispositivos iOS y Android liberados por jailbreak o rooting: Cuando esta propiedad tiene el valor **true**, XenMobile bloquea las inscripciones de dispositivos Android liberados por rooting y dispositivos iOS liberados por jailbreak. El valor predeterminado es **true**. El valor recomendado es **true** para todos los niveles de seguridad.

Inscripción requerida: `wsapi.mdm.required.flag`, que se aplica solo cuando el modo de XenMobile Server es ENT, especifica si se requiere que los usuarios se inscriban en MDM. Esta propiedad se aplica a todos los usuarios y dispositivos de la instancia de XenMobile. Requerir la inscripción ofrece un mayor nivel de seguridad. Sin embargo, esa decisión depende de si quiere o no requerir MDM. De forma predeterminada, no se requiere la inscripción.

Cuando esta propiedad tiene el valor **false**, los usuarios pueden rechazar la inscripción sin, por ello, perder el acceso a las aplicaciones en sus dispositivos a través de XenMobile Store. Cuando esta propiedad tiene el valor **true**, se niega el acceso a las aplicaciones a todo usuario que rechace la inscripción.

Si cambia esta propiedad después de que los usuarios se inscriban, los usuarios deben volver a inscribirse.

Para ver información sobre si requerir la inscripción en MDM o no, consulte Administración de dispositivos e inscripción MDM.

Habilitar inscripción multimodo: La propiedad `enable.multimode.xms` le permite crear perfiles de inscripción en un servidor de XenMobile Server que controle los parámetros de inscripción para

la administración de dispositivos y aplicaciones de dispositivos Android e iOS. Además, la nueva funcionalidad de perfiles de inscripción mejorados permite la inscripción de dispositivos dedicados para Android y la inscripción solo MAM para dispositivos Android e iOS. Cuando esta propiedad tiene el valor **`false`**, esas opciones de inscripción no están disponibles al configurar perfiles de inscripción. El valor predeterminado es **`true`**. Los dispositivos que se inscriben cuando esta propiedad tiene el valor **`true`** sigue funcionando si el valor de la propiedad se cambia a **`false`**.

Habilitar Self Help Portal: Si `shp.console.enable` tiene el valor **`false`**, impide el acceso a Self Help Portal. Los usuarios que navegan a Self-Help Portal en el puerto 443 obtienen un error 404. Los usuarios que navegan al portal en el puerto 4443 reciben el mensaje "Acceso denegado". Si tiene el valor **`true`**, ofrece acceso a Self Help Portal a través del puerto 443. El valor predeterminado es **`false`**.

Límite de bloqueo de cuentas de usuario locales: Mediante la directiva de restricción, puede establecer un límite a los intentos de inicio de sesión para los usuarios de Active Directory. Utilice la clave `local.user.account.lockout.limit` para hacer lo mismo con las cuentas de usuario locales. Después de que los usuarios intenten iniciar sesión la cantidad de veces especificada, no podrán volver a intentarlo hasta que pase un tiempo. Puede configurar ese tiempo con la propiedad **Tiempo de bloqueo de cuenta de usuario local**. El valor predeterminado es `6`.

Tiempo de bloqueo de cuenta de usuario local: La propiedad `local.user.account.lockout.time` le permite establecer una cantidad de minutos que deben transcurrir antes de que se pueda intentar iniciar sesión de nuevo en una cuenta de usuario local bloqueada. El valor predeterminado es `30` minutos.

Restricción sobre tamaño máximo para carga de archivos habilitada: Cuando `max.file.size.upload.restriction` tiene el valor **`true`**, se habilita la restricción sobre tamaño máximo para la carga de archivos. Si habilita esta restricción, configure el tamaño máximo de archivo con `max.file.size.upload.allowed`. El valor predeterminado de esta propiedad es **`true`**.

Tamaño máximo permitido para carga de archivos: Con `max.file.size.upload.allowed`, puede especificar un tamaño máximo de archivo para carga. Valores de ejemplo incluyen `500 B`, `1 KB`, `1 MB`, `1 MiB`, `1 G` o `1 GiB`. El valor predeterminado es `5 MB`.

Tiempo de espera de inactividad en minutos: La cantidad de minutos que deben transcurrir antes de que XenMobile cierre la sesión de un usuario inactivo que usó la API pública de XenMobile Server 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. Para las aplicaciones de terceros que acceden a la API, normalmente es necesario iniciar sesión. El valor predeterminado es `5`.

Inscripción en administración de dispositivos iOS: Instalar CA raíz si es necesario: El flujo de trabajo de inscripción más reciente de Apple requiere que los usuarios instalen manualmente los perfiles MDM. Ese flujo de trabajo no se aplica a la inscripción MDM a servidores asignados en Apple Business Manager o Apple School Manager. Sin embargo, durante la inscripción manual en MDM, los usuarios de dispositivos iOS solo reciben una solicitud de certificados de dispositivos MDM.

Para proporcionar una mejor experiencia de usuario durante la inscripción manual, Citrix recomienda cambiar la propiedad de servidor de `ios.mdm.enrollment.installRootCaIfRequired` a **`false`** . El valor predeterminado es **`true`**. Con ese cambio, se abre una ventana de Safari durante la inscripción en MDM para simplificar la instalación del perfil para los usuarios.

Intervalo de línea base mínimo de VPP: La propiedad `vpp.baseline` establece el intervalo mínimo tras el cual XenMobile vuelve a importar, de Apple, las licencias del programa de compras por volumen. Actualizar la información de las licencias garantiza que XenMobile refleja todos los cambios (por ejemplo, si elimina manualmente una aplicación importada del programa de compras por volumen). De forma predeterminada, XenMobile actualiza el punto de referencia para las licencias de compra por volumen cada `1440` minutos como mínimo.

Si tiene una gran cantidad de licencias de compras por volumen instaladas (por ejemplo, más de 50.000), Citrix recomienda aumentar el intervalo del punto de referencia para reducir la importación de licencias y el consumo de recursos que eso conlleva. Si espera cambios frecuentes en las licencias de compras por volumen por parte de Apple, Citrix recomienda reducir el valor para mantener XenMobile actualizado con los cambios. El intervalo mínimo entre dos puntos de referencia es de 60 minutos. Debido a que la tarea automática cron job se ejecuta cada 60 minutos, si el intervalo del punto de referencia de compras por volumen es de 60 minutos, el intervalo entre los puntos de referencia puede retrasarse hasta 119 minutos.

Intervalo máximo de inactividad para la consola de XenMobile MDM Self-Help Portal (en minutos): Este nombre de propiedad refleja las versiones anteriores de XenMobile. La propiedad controla el intervalo máximo de inactividad en la consola XenMobile. Ese intervalo es la cantidad de minutos, transcurridos los cuales, XenMobile cierra la sesión de un usuario inactivo en la consola de XenMobile. Un tiempo de espera de 0 significa que no se cierra la sesión del usuario inactivo. El valor predeterminado es `30`.

Directivas de aplicación y de dispositivo

January 4, 2022

Las directivas de dispositivo y aplicación de XenMobile permiten optimizar el equilibrio entre los siguientes factores:

- Seguridad de la empresa
- Protección de datos y activos de la empresa
- Privacidad de los usuarios
- Experiencias de usuario productivas y positivas

El equilibrio óptimo entre esos factores puede variar. Por ejemplo, las organizaciones altamente reguladas (como las del ámbito de finanzas), requieren controles de seguridad más estrictos que las em-

presas de otros sectores (como la educación y el comercio), donde la productividad del usuario es una consideración primordial.

Puede controlar y configurar de manera centralizada las directivas en función de la identidad, el dispositivo, la ubicación y el tipo de conectividad de los usuarios para restringir el uso malintencionado del contenido corporativo. En caso de pérdida o robo de un dispositivo, puede desactivar, bloquear o borrar las aplicaciones y los datos corporativos de forma remota. El resultado global es una solución que aumenta la satisfacción y la productividad de los empleados, al mismo tiempo que garantiza la seguridad y el control administrativo.

El enfoque principal de este artículo es la cantidad de directivas de dispositivo y aplicación relacionadas con la seguridad.

Directivas que abordan los riesgos de seguridad

Las directivas de dispositivo y aplicación de XenMobile abordan muchas situaciones que pueden poner en riesgo la seguridad, tales como las siguientes acciones:

- Cuando los usuarios intentan acceder a aplicaciones y datos desde dispositivos con los que no existe una relación de confianza y desde ubicaciones inesperadas.
- Cuando los usuarios transfieren datos de un dispositivo a otro.
- Cuando un usuario no autorizado trata de acceder a los datos.
- Cuando un usuario que usaba su propio dispositivo (BYOD) deja la empresa.
- Cuando un usuario pierde de vista un dispositivo.
- Cuando los usuarios necesitan acceder a la red de forma segura en todo momento.
- Cuando los usuarios tienen su propio dispositivo administrado y se necesita separar los datos de trabajo de los datos personales.
- Cuando un dispositivo está inactivo y se requiere la verificación de las credenciales de usuario de nuevo.
- Cuando los usuarios copian y pegan contenido confidencial en sistemas de correo electrónico no protegidos.
- Cuando los usuarios reciben datos adjuntos de correo electrónico o enlaces Web con datos confidenciales en un dispositivo que contiene tanto cuentas personales como empresariales.

Estas circunstancias están relacionadas con las dos áreas principales que adquieren importancia cuando se trata de proteger los datos de empresa, que se dan cuando los datos:

- Están en reposo
- En tránsito

Cómo protege XenMobile los datos en reposo

Los datos almacenados en dispositivos móviles se denominan datos en reposo. XenMobile utiliza el cifrado de dispositivos proporcionado por las plataformas iOS y Android. XenMobile complementa el cifrado por plataforma con funciones como los controles de conformidad, disponibles a través del SDK de Citrix MAM.

En XenMobile, las funciones de administración de aplicaciones móviles (MAM) permiten una administración, una seguridad y un control completos sobre las aplicaciones móviles de productividad, las aplicaciones habilitadas para MDX y sus datos asociados.

Mobile Apps SDK permite la implementación de aplicaciones a XenMobile gracias a la tecnología de contenedor de aplicaciones MDX de Citrix. La tecnología de contenedor separa las aplicaciones corporativas, los datos de las aplicaciones personales y los datos de un dispositivo de usuario. La separación de datos permite proteger cualquier aplicación móvil propia, de terceros o desarrollada a medida con la ayuda de controles exhaustivos basados en directivas.

XenMobile también incluye el cifrado al nivel de las aplicaciones. XenMobile cifra por separado los datos almacenados en una aplicación habilitada para MDX sin necesidad de un código de acceso de dispositivo y sin que deba administrar el dispositivo para aplicar la directiva.

Las directivas y el Mobile Apps SDK permiten:

- Separar las aplicaciones y los datos de empresa de los personales en un contenedor móvil seguro.
- Proteger aplicaciones con el cifrado y otras tecnologías móviles para la prevención de pérdida de datos (DLP).

Las directivas MDX proporcionan muchos controles operativos. Puede lograr una integración perfecta entre aplicaciones habilitadas para el SDK de MAM o empaquetadas con MDX, a la vez que controla toda la comunicación. De esta manera, puede aplicar directivas para, por ejemplo, asegurarse de que solo las aplicaciones habilitadas para el SDK de MAM o empaquetadas con MDX accedan a los datos.

Más allá del control que ofrecen las directivas de dispositivo y aplicación, la mejor forma de salvaguardar los datos en reposo es el cifrado. XenMobile agrega una capa de cifrado a todos los datos almacenados en una aplicación habilitada para MDX, lo que le confiere el control sobre funciones (como el cifrado de archivos públicos, el cifrado de archivos privados y las exclusiones al cifrado) a través de las directivas. El Mobile Apps SDK utiliza el cifrado AES de 256 bits compatible con FIPS 140-2, junto con claves almacenadas en una caja fuerte protegida llamada Citrix Secret Vault.

Cómo protege XenMobile los datos en tránsito

Los datos que se estén transfiriendo entre los dispositivos móviles del usuario y la red interna se conocen como datos en tránsito. La tecnología del contenedor de aplicaciones MDX ofrece el acceso VPN por aplicación a la red interna a través de Citrix Gateway.

Tenga en cuenta los casos en que un empleado quiera acceder desde un dispositivo móvil a estos recursos que residen en la red empresarial segura:

- El servidor de correo electrónico corporativo
- Una aplicación web con SSL habilitado alojada en la intranet corporativa
- Documentos almacenados en un servidor de archivos o Microsoft SharePoint

MDX permite el acceso a todos esos recursos de la empresa desde dispositivos móviles a través de una micro VPN específica para cada aplicación. Cada dispositivo dispone de su propio túnel micro VPN dedicado.

La funcionalidad Micro VPN no requiere de una VPN para todo el dispositivo, lo que puede poner en peligro la seguridad en los dispositivos móviles que no son de confianza. Como resultado, la red interna no está expuesta al malware ni a ataques que podrían infectar todo el sistema corporativo. Las aplicaciones móviles de empresa y las aplicaciones móviles personales pueden coexistir en un solo dispositivo.

Para ofrecer niveles de seguridad aún más altos, puede configurar aplicaciones habilitadas para MDX con una directiva "Citrix Gateway alternativo", que se utiliza para la autenticación y para sesiones de micro VPN con una aplicación. Puede utilizar la directiva "Citrix Gateway alternativo" junto con la directiva "Sesión con conexión requerida" para obligar a las aplicaciones a volver a autenticarse en la puerta de enlace específica. Estas puertas de enlace suelen tener directivas de administración de tráfico y requisitos de autenticación diferentes (mayor nivel de control).

Además de las funciones de seguridad, la funcionalidad micro VPN también ofrece técnicas de optimización de datos, incluidos algoritmos de compresión. Los algoritmos de compresión garantizan que:

- Solo se transfieren datos mínimos.
- La transferencia se realiza en el tiempo más rápido posible. La velocidad mejora la experiencia del usuario, que es un factor clave de éxito en la adopción de dispositivos móviles.

Debe volver a evaluar las directivas de dispositivo periódicamente, como en estas situaciones:

- Cuando una nueva versión de XenMobile incluye directivas nuevas o actualizadas debido a la publicación de actualizaciones para el sistema operativo del dispositivo.
- Cuando agrega un tipo de dispositivo:

  Aunque muchas directivas sean las mismas para todos los dispositivos, cada dispositivo tiene un conjunto específico de directivas para su sistema operativo. En consecuencia, se pueden encontrar muchas diferencias entre dispositivos iOS, Android y Windows, e incluso entre los dispositivos Android de diferentes fabricantes.

- Para mantener el funcionamiento de XenMobile sincronizado con los cambios empresariales o industriales, como nuevas directrices de seguridad o nuevas normativas corporativas

- Cuando una nueva versión del SDK de MAM incluye directivas nuevas o actualizadas
- Cuando agrega o actualiza una aplicación.
- Cuando necesita integrar nuevos flujos de trabajo para sus usuarios debido a aplicaciones o requisitos nuevos.

Directivas de aplicación y casos de uso

Aunque puede elegir las aplicaciones que estarán disponibles a través de Secure Hub, puede que también le interese definir cómo interactúan esas aplicaciones con XenMobile. Use directivas de aplicación:

- Si quiere que los usuarios se autentiquen después de un determinado período de tiempo.
- Si quiere ofrecer a los usuarios acceso sin conexión a la información.

Las siguientes secciones incluyen algunas de las directivas y ejemplos de uso.

- Para obtener una lista de las directivas de terceros que puede integrar en su aplicación iOS y Android mediante el SDK de MAM, consulte Introducción al SDK de MAM.
- Para ver una lista de todas las directivas MDX desglosadas por plataforma, consulte Directivas MDX.

Directivas de autenticación

- **Código de acceso de dispositivo**

  Por qué usar esta directiva: Habilite la directiva “Código de acceso del dispositivo” para estipular que un usuario solo pueda acceder a una aplicación MDX si el dispositivo tiene un código de acceso de dispositivo habilitado. Esta función garantiza el uso del cifrado de iOS al nivel del dispositivo.

  Ejemplo para el usuario: Habilitar esta directiva significa que el usuario debe definir un código de acceso en su dispositivo iOS para poder acceder a la aplicación MDX.

- **Código de acceso de aplicación**

  Por qué usar esta directiva: Habilite la directiva “Código de acceso de aplicación” para que Secure Hub pida al usuario que se autentique en la aplicación administrada para poder abrirla y acceder a los datos. El usuario puede autenticarse con su contraseña de Active Directory, el PIN de Citrix o TouchID de iOS, dependiendo de lo que configure en “Propiedades de cliente”, en “Parámetros” de XenMobile Server. Puede establecer un temporizador de inactividad en “Propiedades de cliente” para que, con el uso continuado, Secure Hub no pida al usuario que se autentique en la aplicación administrada nuevamente hasta que el temporizador expire.

  El código de acceso a la aplicación difiere del código de acceso al dispositivo en que, con una directiva “Código de acceso del dispositivo” que se envía a un dispositivo, Secure Hub pide al

usuario que defina un código de acceso o PIN para acceder a su dispositivo cuando lo encienda o cuando caduque el temporizador de inactividad. Para obtener más información, consulte Autenticación en XenMobile.

Ejemplo para el usuario: Al abrir la aplicación Citrix Secure Web en el dispositivo, el usuario debe introducir su PIN de Citrix para poder navegar por sitios web si ha transcurrido el período de inactividad.

- **Sesión con conexión requerida**

  Por qué usar esta directiva: Si una aplicación requiere acceso a una aplicación web (servicio web) para funcionar, habilite esta directiva para que XenMobile pida al usuario que se conecte a la red de la empresa o tenga una sesión activa antes de usar la aplicación.

  Ejemplo para el usuario: Cuando un usuario intenta abrir una aplicación MDX que tiene habilitada la directiva "Sesión con conexión requerida", no puede utilizar la aplicación hasta que se conecte a la red con un servicio de telefonía móvil o Wi-Fi.

- **Período máximo sin conexión**

  Por qué usar esta directiva: Use esta directiva como una opción adicional de seguridad, para asegurarse de que los usuarios no puedan ejecutar una aplicación sin conexión durante largos períodos de tiempo sin volver a confirmar que tienen derecho a utilizar la aplicación y sin actualizar las directivas de XenMobile.

  Ejemplo para el usuario: Si configura una aplicación MDX con un "Período máximo sin conexión", los usuarios pueden abrir y utilizar la aplicación sin conectarse a la red hasta que caduque el período del temporizador sin conexión. En ese momento, el usuario debe volver a conectarse a la red a través del servicio móvil o Wi-Fi y volver a autenticarse, si se le solicita.

Otras directivas de acceso

- **Período de gracia de actualización de aplicación (horas)**

  Por qué usar esta directiva: El período de gracia para la actualización de aplicaciones es el tiempo de que dispone el usuario para actualizar una aplicación que tenga una versión más reciente publicada en XenMobile Store. Transcurrido este período, el usuario debe actualizar la aplicación para poder acceder a los datos que esta contiene. Cuando establezca el valor de esta directiva, tenga en cuenta las necesidades de su personal móvil, en particular las necesidades de aquellos empleados que podrían verse expuestos a largos períodos sin conexión durante viajes internacionales.

  Ejemplo para el usuario: Se carga una nueva versión de Secure Mail en XenMobile Store y, a continuación, se establece un período de gracia para la actualización de aplicaciones de 6 horas. Todos los usuarios de Secure Mail verán un mensaje donde se les pedirá que actualicen

su aplicación de Secure Mail hasta que transcurran las 6 horas. Transcurridas 6 horas, Secure Hub dirige a los usuarios a XenMobile Store.

- **Período de sondeo activo (minutos)**

  Por qué usar esta directiva: El período de sondeo activo es el intervalo durante el cual XenMobile examina las aplicaciones para realizar acciones de seguridad, tales como el bloqueo de aplicaciones y el borrado de aplicaciones.

  Ejemplo para el usuario: Si establece la directiva "Período de sondeo activo" en 60 minutos, cuando envíe el comando "Bloqueo de aplicaciones" desde XenMobile al dispositivo, el bloqueo se producirá 60 minutos después del último sondeo.

Directivas de comportamiento de dispositivos no conformes

Cuando un dispositivo no cumple todos los requisitos mínimos de conformidad, la directiva Comportamiento de dispositivos no conformes le permite seleccionar qué hacer al respecto. Para obtener información, consulte Comportamiento de dispositivos no conformes.

Directivas de interacción entre aplicaciones

Por qué usar estas directivas: Puede usar las directivas de interacción entre aplicaciones para controlar el flujo de documentos y datos desde las aplicaciones MDX a otras aplicaciones en el dispositivo. Por ejemplo, puede impedir que un usuario mueva datos a sus aplicaciones personales de fuera del contenedor o pegue datos desde fuera del contenedor a las aplicaciones del contenedor.

Ejemplo para el usuario: Usted establece la directiva "Interacción entre aplicaciones" en "Restringida", lo que significa que un usuario puede copiar texto desde Secure Mail a Secure Web, pero no puede copiar esos datos a su explorador personal Safari o Chrome que está fuera del contenedor. Además, el usuario puede abrir un documento adjunto desde Secure Mail en Citrix Files o Quick Edit, pero no puede abrirlo en sus propias aplicaciones de visualización de archivos personales que están fuera del contenedor.

Directivas de restricciones a aplicaciones

Por qué usar estas directivas: Puede usar las directivas de restricciones a aplicaciones para controlar a qué funciones pueden acceder los usuarios mientras está abierta una aplicación MDX. Eso ayuda a garantizar que no haya actividades maliciosas mientras se ejecuta la aplicación. Las directivas de restricciones a aplicaciones varían ligeramente entre iOS y Android. Por ejemplo, en iOS puede bloquear el acceso a iCloud mientras se ejecuta la aplicación MDX. En Android, puede detener el uso de NFC mientras se ejecuta la aplicación MDX.

Ejemplo para el usuario: Si se habilita la directiva "Restricciones a aplicaciones" para bloquear el dictado en una aplicación MDX en iOS, el usuario no puede usar la función de dictado en el teclado iOS mientras se ejecuta la aplicación MDX. Por lo tanto, los datos que dictan los usuarios no se transfieren al servicio, no seguro, de dictado en la nube de terceros. Cuando el usuario abre sus aplicaciones personales fuera del contenedor, la opción de dictado permanece disponible para el usuario para las comunicaciones personales.

Directivas de acceso de las aplicaciones a la red

Por qué usar estas directivas: Puede utilizar las directivas del acceso de las aplicaciones a la red para proporcionar el acceso desde una aplicación MDX ubicada en el contenedor del dispositivo a los datos que se encuentran dentro de la red corporativa. En la directiva "Acceso de red", defina la opción **Túnel a la red interna** para automatizar una micro VPN desde la aplicación MDX a través de Citrix ADC a un servicio web back-end o almacén de datos.

Ejemplo para el usuario: Cuando un usuario abre una aplicación MDX, por ejemplo Secure Web, que tiene habilitado el túnel, el explorador web abre e inicia un sitio de intranet sin que el usuario tenga que iniciar una VPN. La aplicación Secure Web accede automáticamente al sitio interno mediante la tecnología de red micro VPN.

Directivas de geocercas y geolocalización de aplicaciones

Por qué usar estas directivas: Las directivas que controlan las geocercas y la geolocalización de aplicaciones incluyen la longitud del punto central, la latitud del punto central y el radio. Esas directivas limitan el acceso a los datos en las aplicaciones MDX en función de un área geográfica específica. Las directivas definen un área geográfica por un radio y unas coordenadas de latitud y longitud. Si un usuario intenta usar una aplicación fuera del radio definido, la aplicación permanece bloqueada y el usuario no puede acceder a los datos de la aplicación.

Ejemplo para el usuario: Un usuario puede acceder a los datos de fusión y adquisición mientras se encuentra en su oficina. Cuando sale de su oficina, esos datos confidenciales dejan de estar accesibles.

Directivas de Secure Mail

- **Servicios de red en segundo plano**

  Por qué usar esta directiva: Los servicios de red en segundo plano en Secure Mail usan Secure Ticket Authority (STA), que es a efectos prácticos un proxy SOCKS5 para conectarse a través de Citrix Gateway. STA admite conexiones de larga duración y ofrece una mejor duración de la batería que una red micro VPN. Por lo tanto, STA es ideal para aplicaciones de correo, que se

conectan constantemente. Citrix recomienda configurar estos parámetros para Secure Mail. El asistente de Citrix ADC para XenMobile establece automáticamente STA para Secure Mail.

Ejemplo para el usuario: Cuando STA no está habilitado y un usuario Android abre Secure Mail, se le solicita que abra una VPN, que permanece abierta en el dispositivo. Cuando STA está habilitado y el usuario Android abre Secure Mail, esta aplicación se conecta sin necesidad de VPN.

- **Intervalo de sincronización predeterminado**

  Por qué usar esta directiva: Esta configuración especifica los días predeterminados de correo electrónico que se sincronizan con Secure Mail cuando el usuario accede a Secure Mail por primera vez. Tenga en cuenta que, si indica 2 semanas de correo electrónico, la sincronización tarda más que si indica 3 días. Además, el proceso de configuración es más largo para el usuario.

  Ejemplo para el usuario: Si el intervalo de sincronización predeterminado está establecido en 3 días cuando el usuario configura Secure Mail por primera vez, el usuario verá en su Bandeja de entrada todos los correos que haya recibido durante los últimos 3 días. Si el usuario quiere ver mensajes anteriores a 3 días, puede buscarlos. Tras la búsqueda, Secure Mail muestra los mensajes anteriores almacenados en el servidor. Después de instalar Secure Mail, cada usuario puede cambiar este parámetro para adaptarlo mejor a sus necesidades.

Directivas de dispositivo y comportamiento de caso de uso

Las directivas de dispositivo, también conocidas como directivas MDM, determinan el funcionamiento de XenMobile en los dispositivos. Aunque muchas directivas sean las mismas para todos los dispositivos, cada dispositivo tiene un conjunto específico de directivas para su sistema operativo. En la siguiente lista se incluyen algunas de las directivas de dispositivo y se describe cómo se pueden usar. Para ver una lista de todas las directivas de dispositivo, consulte los artículos de Directivas de dispositivo.

- **Directiva de inventario de aplicaciones**

  Por qué usar esta directiva: Implemente la directiva “Inventario de aplicaciones” en un dispositivo si quiere ver las aplicaciones que haya instalado personalmente un usuario. Si no implementa la directiva “Inventario de aplicaciones”, solo verá las aplicaciones que un usuario haya instalado desde XenMobile Store, no las aplicaciones que haya instalado personalmente. Debe usar esta directiva si quiere prohibir la ejecución de determinadas aplicaciones en los dispositivos de empresa.

  Ejemplo para el usuario: Un usuario con un dispositivo MDM administrado no puede inhabilitar esta funcionalidad. Los administradores de XenMobile pueden ver las aplicaciones que el usuario se haya instalado personalmente.

- **Directiva de bloqueo de aplicaciones**

Por qué usar esta directiva: En Android, puede permitir o bloquear aplicaciones gracias a la directiva "Bloqueo de aplicaciones". Por ejemplo, con las aplicaciones permitidas, puede configurar un dispositivo como quiosco. Por lo general, la directiva "Bloqueo de aplicaciones" solo se implementa en dispositivos de empresa, ya que limita las aplicaciones que los usuarios pueden instalar. Puede establecer una contraseña de anulación para ofrecer acceso a las aplicaciones bloqueadas.

Ejemplo para el usuario: Supongamos que implementa una directiva "Bloqueo de aplicaciones" que bloquea la aplicación Angry Birds. El usuario puede instalarse la aplicación Angry Birds desde Google Play, pero, cuando intenta abrirla, un mensaje le informa que el administrador ha bloqueado la aplicación.

- **Directiva de programación de conexiones**

  Por qué usar esta directiva: Debe usar la directiva "Programación de conexiones" para que los dispositivos móviles Windows se conecten a XenMobile Server para la implementación de directivas, el envío de aplicaciones y la administración MDM. Para dispositivos Android, Android Enterprise y Chrome OS, use Google Firebase Cloud Messaging (FCM), en lugar de esta directiva, para controlar las conexiones a XenMobile Server. Las opciones de programación son:

  - **Siempre:** Mantiene la conexión activa de forma permanente. Citrix recomienda esta opción para optimizar la seguridad. Cuando seleccione **Siempre**, use también la directiva "Temporizador de conexión" para que la conexión no consuma 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 **Implementar para conexiones permanentes** en "Programación de la implementación" para cada directiva de programación que implemente en el dispositivo.
  - **Nunca:** Se conecta manualmente. Citrix no recomienda la opción **Nunca** para las implementaciones de producción, ya que impide implementar directivas de seguridad en los dispositivos; por lo tanto, los usuarios no recibirán nunca aplicaciones ni directivas nuevas.
  - **Cada:** Se conecta en el intervalo predeterminado. Cuando esta opción está activa y se envía una directiva de seguridad (como un bloqueo o un borrado), XenMobile procesa la directiva en el dispositivo la próxima vez que el dispositivo se conecta.
  - **Definir programación:** Cuando está habilitada, XenMobile intenta volver a conectar el dispositivo del usuario al servidor de XenMobile si se pierde la conexión de red. Asimismo, XenMobile supervisa la conexión porque transmite paquetes de control a intervalos periódicos durante el período de tiempo que usted defina.

  Ejemplo para el usuario: Quiere implementar una directiva "Código de acceso" en los dispositivos inscritos. La directiva de programación garantiza que los dispositivos se conecten al servidor en un intervalo periódico para recopilar la nueva directiva.

- **Directiva de credenciales**

  Por qué usar esta directiva: A menudo se usa juntamente con una directiva "Wi-Fi". La directiva "Credenciales" permite implementar certificados para la autenticación en recursos internos que requieren la autenticación por certificado.

  Ejemplo para el usuario: Usted implementa una directiva "Wi-Fi" que configura una red inalámbrica en el dispositivo. La red Wi-Fi requiere un certificado para la autenticación. La directiva "Credenciales" implementa un certificado que se almacena en el almacén de claves del sistema operativo. El usuario puede seleccionar el certificado cuando está conectado al recurso interno.

- **Directiva de Exchange**

  Por qué usar esta directiva: Con XenMobile, tiene dos opciones para entregar el correo electrónico de Microsoft Exchange ActiveSync.

  - **La aplicación Secure Mail:** Puede entregar el correo electrónico a través de la aplicación Secure Mail, que usted distribuye desde XenMobile Store o la tienda pública de aplicaciones.
  - **Aplicación nativa de correo:** Use la directiva "Exchange" para habilitar el correo electrónico ActiveSync para el cliente de correo nativo del dispositivo. Con la directiva "Exchange" para el correo electrónico nativo, puede usar macros para rellenar los datos de usuario desde sus atributos de Active Directory, por ejemplo, ${user.username} para rellenar el nombre de usuario y ${user.domain} para rellenar el dominio de usuario.

  Ejemplo para el usuario: Cuando envía la directiva "Exchange", envía también los detalles del servidor Exchange al dispositivo. A continuación, Secure Hub solicita al usuario que se autentique y el correo electrónico comienza a sincronizarse.

- **Directiva de localización geográfica**

  Por qué usar esta directiva: La directiva "Localización geográfica" se puede usar para ubicar geográficamente los dispositivos en un mapa, siempre que el dispositivo tenga habilitado el GPS para Secure Hub. Tras implementar esta directiva, si envía un comando de localización geográfica desde el servidor de XenMobile, el dispositivo responde con las coordenadas de la ubicación.

  Ejemplo para el usuario: Cuando implementa la directiva "Localización geográfica" y el GPS está habilitado en el dispositivo, si el usuario pierde su dispositivo, puede iniciar sesión en XenMobile Self-Help Portal y elegir la opción de localización para ver la ubicación de su dispositivo en un mapa. Tenga en cuenta que el usuario elige permitir que Secure Hub use los servicios de localización. Los servicios de localización geográfica no se pueden aplicar cuando los usuarios inscriben un dispositivo por sí mismos. Otra consideración a tener en cuenta a la hora de usar esta directiva es el efecto sobre la duración de la batería.

- **directiva de código de acceso**

  Por qué usar esta directiva: La directiva "Código de acceso" permite imponer un código de acceso (PIN o contraseña) en un dispositivo administrado. Con esta directiva, se puede definir la complejidad y el tiempo de espera del código de acceso en el dispositivo.

  Ejemplo para el usuario: Cuando implementa una directiva "Código de acceso" en un dispositivo administrado, Secure Hub pide al usuario que defina un código de acceso o PIN que deberá introducir para acceder a su dispositivo cuando lo encienda o cuando caduque el temporizador de inactividad.

- **Directiva de eliminación de perfiles**

  Por qué usar esta directiva: Supongamos que implementa una directiva a un grupo de usuarios y, más tarde, necesita quitar dicha directiva de un subconjunto de los usuarios. Puede quitar la directiva de los usuarios seleccionados. Para ello, debe crear una directiva "Eliminación de perfiles" y usar reglas de implementación para implementar esa directiva solo a los nombres de usuario especificados.

  Ejemplo para el usuario: Tras implementar una directiva "Eliminación de perfiles" en los dispositivos de usuario, es posible que los usuarios no noten ningún cambio. Por ejemplo, si la directiva "Eliminación de perfiles" elimina una restricción que inhabilitaba la cámara del dispositivo, el usuario no sabrá que ahora se permite el uso de la cámara. Considere la posibilidad de avisar a los usuarios cuando se produzcan cambios que afecten a su experiencia.

- **Directiva de restricciones**

  Por qué usar esta directiva: La directiva "Restricciones" le ofrece diversas opciones para bloquear y controlar las funciones y la funcionalidad de los dispositivos administrados. Puede habilitar cientos de opciones de restricción en los dispositivos admitidos: desde inhabilitar la cámara o el micrófono del dispositivo móvil, hasta imponer reglas de itinerancia y acceso a servicios de terceros (como almacenes de aplicaciones).

  Ejemplo para el usuario: Si implementa una restricción en un dispositivo iOS, es posible que el usuario no pueda acceder a iCloud o al App Store.

- **Directiva de términos y condiciones**

  Por qué usar esta directiva: Puede que necesite advertir a los usuarios de las implicaciones legales de tener su dispositivo administrado. Además, puede que quiera asegurarse de que los usuarios conocen los riesgos a la seguridad cuando se envían datos de empresa al dispositivo. El documento de términos y condiciones personalizado permite publicar reglas y avisos legales antes de que el usuario se inscriba.

  Ejemplo para el usuario: El usuario ve la información de términos y condiciones durante el proceso de inscripción. Si no acepta las condiciones estipuladas, el proceso de inscripción finaliza y no puede acceder a los datos de empresa. Puede generar un informe que facilitar a

los equipos jurídicos o de Recursos Humanos para que estos vean quién aceptó o rechazó los términos.

- **directiva de VPN**

  Por qué usar esta directiva: Use la directiva "VPN" para proporcionar acceso a sistemas back-end con la ayuda de tecnología antigua de puerta de enlace VPN. La directiva admite varios proveedores de VPN, incluidos Cisco AnyConnect, Juniper y Citrix VPN. También es posible vincular esta directiva a una entidad de certificación (CA) y una VPN habilitada a demanda (siempre que la puerta de enlace VPN admita esta opción).

  Ejemplo para el usuario: Con la directiva de red VPN habilitada, el dispositivo del usuario abre una conexión VPN cuando el usuario accede a un dominio interno.

- **Directiva de clip web**

  Por qué usar esta directiva: Use la directiva "Clip web" si quiere enviar a los dispositivos un icono que abra directamente un sitio web. Un clip web contiene un enlace a un sitio web y puede incluir un icono personalizado. En un dispositivo, un clip web parece un icono de aplicación.

  Ejemplo para el usuario: Un usuario puede hacer clic en un icono de clip web para abrir un sitio de Internet que ofrezca los servicios que necesita. Un enlace Web es más conveniente que tener que abrir una aplicación de explorador web y escribir una dirección de enlace.

- **Directiva de Wi-Fi**

  Por qué usar esta directiva: La directiva "Wi-Fi" permite implementar detalles de red inalámbrica (como el SSID, los datos de autenticación y los datos de configuración) en un dispositivo administrado.

  Ejemplo para el usuario: Cuando implementa la directiva "Wi-Fi", el dispositivo se conecta automáticamente a la red inalámbrica y autentica al usuario para que este acceda a la red.

- **Directiva de Windows Information Protection**

  Por qué usar esta directiva: Use la directiva "Windows Information Protection" (WIP) para protegerse contra la posible filtración de datos de empresa. Puede especificar las aplicaciones que requieren Windows Information Protection al nivel de exigencia que necesite. Por ejemplo, puede bloquear toda forma inadecuada de compartir datos, o advertir a los usuarios sobre formas inadecuadas de compartir datos y permitir que anulen la directiva. Puede ejecutar WIP de forma silenciosa mientras inicia sesión y permite formas inadecuadas de compartir datos.

  Ejemplo para el usuario: Supongamos que configura la directiva WIP para bloquear toda forma inadecuada de compartir datos. Si un usuario copia o guarda un archivo protegido en una ubicación no protegida, aparecerá un mensaje similar a este: No puede colocar contenido protegido de empresa en esta ubicación.

- **Directiva de XenMobile Store**

Por qué usar esta directiva: XenMobile Store es una tienda de aplicaciones unificada donde los administradores pueden publicar todas las aplicaciones de empresa y todos los recursos de datos de empresa que los usuarios puedan necesitar. Un administrador puede agregar:

- Aplicaciones web, aplicaciones SaaS y aplicaciones habilitadas para el SDK de MAM o empaquetadas con MDX
- Aplicaciones móviles de productividad de Citrix
- Aplicaciones móviles nativas, como archivos .ipa o .apk
- Aplicaciones del App Store y Google Play
- Enlaces web
- Citrix Virtual Apps publicadas mediante Citrix StoreFront

Ejemplo para el usuario: Después de que un usuario inscriba el dispositivo en XenMobile, puede acceder a XenMobile Store a través de la aplicación Citrix Secure Hub. Allí, el usuario verá todos los servicios y las aplicaciones de empresa que tiene disponibles. El usuario puede hacer clic en una aplicación para instalarla, evaluarla, revisarla y acceder a sus datos, así como descargar actualizaciones de la aplicación desde XenMobile Store.

Opciones de inscripción de usuarios

September 19, 2021

Puede hacer que los usuarios inscriban sus dispositivos en XenMobile de varias maneras. Antes de considerar los detalles, decida qué dispositivos quiere inscribir en MDM+MAM, MDM o MAM. Para obtener más información sobre estos modos de administración, consulte Modos de administración.

En el nivel más alto, hay cuatro opciones de inscripción:

- **Invitación de inscripción:** Puede enviar una URL de invitación o una invitación de inscripción a los usuarios. Las URL y las invitaciones de inscripción no están disponibles para dispositivos Windows.
- **Self-Help Portal:** Puede configurar un portal que los usuarios visiten para descargarse Secure Hub e inscribir sus dispositivos ellos mismos o enviarse a ellos mismos una invitación para la inscripción.
- **Inscripción manual:** Puede enviar un correo electrónico, un manual u otro comunicado para que los usuarios sepan que el sistema está disponible para inscripción. Entonces, los usuarios se descargan Secure Hub e inscriben sus dispositivos manualmente.
- **Empresa:** Otra opción para la inscripción de dispositivos es mediante un Programa de implementación de Apple y Google Android Enterprise. A través de cada uno de estos programas, puede adquirir dispositivos preconfigurados y listos para que los usen los empleados. Para obtener más información, consulte los artículos del Programa de implementación de Apple en

el Soporte de Apple y la documentación de Google Android Enterprise en el sitio web de Android Enterprise.

Invitación de inscripción

Puede enviar una invitación de inscripción a usuarios de dispositivos iOS, macOS, Android Enterprise o Android heredado. Las URL y las invitaciones de inscripción no están disponibles para dispositivos Windows.

También puede enviar un enlace de instalación por SMTP o SMS a los usuarios con dispositivos iOS, macOS, Android o Windows. Para obtener más información, consulte Inscribir dispositivos.

Si decide utilizar el método de invitación para la inscripción, puede:

- Seleccionar el modo de seguridad de inscripción **URL de invitación**, **URL de invitación + PIN** o **URL de invitación + contraseña**.
- Usar cualquier combinación de los distintos modos.
- Habilitar o inhabilitar los modos en la página **Parámetros**.

Para obtener información sobre cada modo de seguridad de inscripción, consulte Configurar modos de seguridad de inscripción.

Las invitaciones tienen muchos fines. El uso más común de las invitaciones es notificar a los usuarios de que el sistema está disponible y pueden inscribirse. Las URL de invitación son únicas. Una vez que un usuario utiliza una URL de invitación, dicha URL deja de estar disponible. Puede usar esta propiedad para limitar la cantidad de usuarios o dispositivos que se inscriben en su sistema.

Al configurar un perfil de inscripción, puede controlar la cantidad de dispositivos que usuarios específicos pueden inscribir, en función de los grupos de Active Directory. Por ejemplo, puede autorizar solo un dispositivo por usuario a la división Finanzas.

Tenga en cuenta los costes adicionales y las dificultades de algunas opciones de inscripción. Por ejemplo, el envío de invitaciones mediante SMS requiere una infraestructura adicional. Para obtener más información sobre esta opción, consulte Notificaciones.

Asimismo, para enviar invitaciones por correo electrónico, debe comprobar que los usuarios tengan una manera de acceder al correo electrónico que no sea a través de Secure Hub. Para la inscripción MDM, puede utilizar el modo de seguridad de inscripción con contraseña de un solo uso (OTP) como alternativa a las contraseñas de Active Directory.

Self Help Portal

Los usuarios puedan solicitar una invitación de inscripción mediante el portal Self Help Portal. Para obtener información sobre cómo configurar Self Help Portal, consulte Configurar modos de seguridad de inscripción.

Inscripción manual

Con la inscripción manual, los usuarios se conectan a XenMobile a través de la detección automática, o bien, introducen la información del servidor. Con la detección automática, los usuarios pueden iniciar sesión solamente con su dirección de correo electrónico o sus credenciales de Active Directory en el formato de nombre principal de usuario. Sin la detección automática, deben introducir la dirección del servidor y sus credenciales de Active Directory. Para obtener más información sobre cómo configurar la detección automática, consulte XenMobile AutoDiscovery Service.

Puede facilitar la inscripción manual de varias maneras. Puede crear una guía, distribuirla a los usuarios y hacer que se inscriban ellos mismos. Puede hacer que su departamento de TI inscriba manualmente a los grupos de usuarios durante determinados periodos de tiempo. Puede usar cualquier método similar donde los usuarios deban introducir sus credenciales o la información del servidor, o ambas.

Incorporación de usuarios

Una vez que haya configurado su entorno, debe decidir cómo introducir a los usuarios en su entorno. En un apartado anterior de este artículo se analizan los detalles de los modos de seguridad para la inscripción de los usuarios. En esta sección se describe cómo establecer comunicación con los usuarios.

Inscripción abierta frente a invitación selectiva

Al incorporar usuarios, puede permitir la inscripción a través de dos métodos básicos:

- Inscripción abierta. De forma predeterminada, cualquier usuario con credenciales LDAP y la información del entorno de XenMobile puede inscribirse.
- Inscripción limitada. Puede limitar la cantidad de usuarios al permitir que solo los usuarios con invitaciones se inscriban. También puede limitar la inscripción abierta por grupo de Active Directory.

Con el método de invitación, también puede limitar la cantidad de dispositivos que puede inscribir un usuario. En la mayoría de las situaciones, la inscripción abierta es una buena opción, pero hay aspectos a tener en cuenta:

- Para la inscripción en MAM, puede limitar fácilmente la inscripción abierta según la pertenencia a grupos de Active Directory.
- Para la inscripción en MDM, puede limitar la cantidad de dispositivos que pueden inscribirse en función de la pertenencia a grupos de Active Directory. Normalmente, no es ningún problema que solo permita dispositivos de empresa en su entorno. Sin embargo, conviene que tenga en cuenta este método en un área de trabajo BYOD donde quiera limitar la cantidad de dispositivos en el entorno.

La invitación selectiva generalmente se realiza con menos frecuencia porque requiere un poco más de trabajo que la inscripción abierta. Para que los usuarios puedan inscribir sus dispositivos en el entorno, debe enviar una invitación única a cada usuario. Para obtener información sobre cómo enviar una invitación de inscripción, consulte Enviar una invitación de inscripción.

Aunque puede utilizar grupos de Active Directory para crear invitaciones por lotes, debe seguir este enfoque por fases.

Primer contacto con los usuarios

Después de decidir entre la inscripción abierta o la invitación selectiva y de configurar esos entornos, debe informar a los usuarios sobre las opciones de inscripción de que disponen.

Si usa el método de invitación selectiva, los mensajes de correo electrónico y SMS intervienen en el proceso. También puede enviar correos electrónicos desde la consola de XenMobile para la inscripción abierta. Para obtener más información, consulte Enviar una invitación de inscripción.

En ambos casos, tenga en cuenta que, para los correos electrónicos, necesitará un servidor SMTP. Para los mensajes de texto, necesita un servidor SMS. Esos servidores podrían implicar costes adicionales a considerar a la hora de tomar su decisión. Antes de seleccionar un método, debe decidir cómo prevé que los nuevos usuarios accedan a la información (por ejemplo, por correo electrónico). Si quiere que todos los usuarios accedan a su correo electrónico a través de XenMobile, enviarles un correo electrónico de invitación podría ser problemático.

También puede enviar comunicaciones por otro medio que no sea XenMobile para un entorno de inscripción abierta. Para esa opción, asegúrese de incluir toda la información relevante. Indique a los usuarios dónde pueden obtener la aplicación Secure Hub y qué método deben utilizar para inscribirse. Si la detección está desactivada, proporcione también a los usuarios la dirección de XenMobile Server. Para obtener más información sobre la detección automática, consulte XenMobile AutoDiscovery Service.

Ajustar las operaciones de XenMobile

May 19, 2021

El rendimiento y la estabilidad de las operaciones de XenMobile implican muchas configuraciones en XenMobile y dependen de la configuración de Citrix ADC y la base de datos de SQL Server. Este artículo se centra en los parámetros que definen con mayor frecuencia los administradores, relacionadas con los ajustes y la optimización de XenMobile. Citrix recomienda que evalúe cada una de las configuraciones en este artículo antes de implementar XenMobile.

> **Importante:**
>
> En estas pautas se asume que la CPU y la RAM del servidor de XenMobile corresponden con la cantidad de dispositivos. Para obtener más información acerca de la escalabilidad, consulte Escalabilidad y rendimiento.

Las siguientes propiedades de servidor se aplican globalmente a operaciones, usuarios y dispositivos en toda la instancia de XenMobile. Un cambio en algunas propiedades de servidor requiere un reinicio de cada nodo del servidor de XenMobile. XenMobile le notifica cuando es necesario un reinicio.

Estas indicaciones de ajustes se aplican a entornos agrupados en clúster y no agrupados.

hibernate.c3p0.idle_test_period

Esta propiedad del servidor de XenMobile, una clave personalizada (Custom Key), determina el tiempo de inactividad, en segundos, antes de que se valide automáticamente una conexión. Configure la clave de este modo. El valor predeterminado es **30**.

- Clave: **Clave personalizada**
- Clave: **hibernate.c3p0. idle_test_period**
- Valor: **120**
- Nombre simplificado: **hibernate.c3p0. idle_test_period**
- Descripción: **Período de prueba para el tiempo de espera antes de hibernar**

hibernate.c3p0.max_size

Esta clave personalizada determina la cantidad máxima de conexiones a la base de datos de SQL Server que puede abrir XenMobile. XenMobile utiliza el valor que se especifica para esta clave personalizada como el límite máximo. Las conexiones se abren solo si las necesita. Debe establecer sus parámetros en función de la capacidad del servidor de la base de datos.

Tenga en cuenta la siguiente ecuación en una configuración en clúster. La conexión c3p0 multiplicada por la cantidad de nodos equivale a su cantidad máxima real de conexiones a la base de datos de SQL Server que XenMobile puede abrir.

En configuraciones agrupadas en clúster o sin clústeres, establecer el valor demasiado alto con un SQL Server demasiado pequeño puede causar problemas de recursos en el lado de SQL durante la carga máxima. Establecer un valor demasiado bajo puede derivar en que no aproveche los recursos SQL disponibles.

Configure la clave de este modo. El valor predeterminado es **1000**.

- Clave: **hibernate.c3p0.max_size**
- Valor: **1000**
- Nombre simplificado: **hibernate.c3p0.max_size**

- Descripción: Conexiones de base de datos a SQL

hibernate.c3p0.min_size

Esta clave personalizada determina la cantidad mínima de conexiones a la base de datos de SQL Server que puede abrir XenMobile. Configure la clave de este modo. El valor predeterminado es **100**.

- Clave: **hibernate.c3p0.min_size**
- Valor: **100**
- Nombre simplificado: **hibernate.c3p0.min_size**
- Descripción: Conexiones de base de datos a SQL

hibernate.c3p0.timeout

Esta clave personalizada determina el tiempo de espera de inactividad. Si usa la conmutación por error en los clústeres de la base de datos, Citrix recomienda agregar esta clave personalizada y definirla para reducir el tiempo de inactividad. El valor predeterminado es **120**.

- Clave: **Clave personalizada**
- Clave: **hibernate.c3p0.timeout**
- Valor: **120**
- Nombre simplificado: **hibernate.c3p0.timeout**
- Descripción: Tiempo de espera de inactividad que tiene la base de datos

Intervalo de latido de Push Services

Esta configuración determina la frecuencia con la que un dispositivo iOS verifica si una notificación de APNs se ha entregado en el intervalo. Aumentar la frecuencia de latidos del APNs puede optimizar las comunicaciones de la base de datos. Un valor demasiado grande puede agregar una carga innecesaria. Esta configuración solo se aplica a dispositivos iOS. El valor predeterminado es **20** horas.

Si tiene una gran cantidad de dispositivos iOS en su entorno, el intervalo de latidos puede generar una carga mayor de la necesaria. Las acciones de seguridad, como el borrado selectivo, el bloqueo y el borrado completo, no dependen de este latido. Esto se debe a que se envía una notificación de APNs al dispositivo cuando se ejecutan estas acciones. Este valor determina la rapidez con la que se actualiza una directiva después de que cambien los miembros de los grupos de Active Directory. Como tal, a menudo es conveniente aumentar este valor a entre 12 y 20 horas para reducir la carga.

Tamaño de la agrupación de conexiones APNS de iOS MDM

Una agrupación de conexiones APNs que es demasiado pequeña puede afectar negativamente al rendimiento de las actividades APNs si dispone de más de 100 dispositivos. Los problemas de

rendimiento incluyen una implementación más lenta de aplicaciones y directivas en los dispositivos y un registro más lento de los dispositivos. El valor predeterminado es **1**. Le recomendamos aumentar este valor en 1 por cada 400 dispositivos aproximadamente.

auth.ldap.connect.timeout

Para compensar las respuestas LDAP lentas, Citrix recomienda que agregue propiedades de servidor a la siguiente clave personalizada.

- Clave: **Clave personalizada**
- Clave: **auth.ldap.connect.timeout**
- Valor: **60000**
- Nombre simplificado: **auth.ldap.connect.timeout**
- Descripción: **Tiempo de espera de la conexión LDAP**

auth.ldap.read.timeout

Para compensar las respuestas LDAP lentas, Citrix recomienda que agregue propiedades de servidor a la siguiente clave personalizada.

- Clave: **Clave personalizada**
- Clave: **auth.ldap.read.timeout**
- Valor: **60000**
- Nombre simplificado: **auth.ldap.read.timeout**
- Descripción: **Tiempo de lectura de la conexión LDAP**

Otras optimizaciones de servidor

Propiedad de servidor	Configuración predeterminada	¿Por qué cambiar esta configuración?

Implementación en segundo plano	1440 minutos	La frecuencia de las implementaciones de directivas en segundo plano, en minutos. Se aplica solo a las conexiones permanentes de dispositivos Android. Aumentar la frecuencia de las implementaciones de directivas reduce la carga del servidor. La configuración recomendada es **1440** (24 horas).
Inventario de hardware en segundo plano	1440 minutos	La frecuencia del inventario de hardware en segundo plano, en minutos. Se aplica solo a las conexiones permanentes de dispositivos Android. Aumentar la frecuencia del inventario de hardware reduce la carga del servidor. La configuración recomendada es **1440** (24 horas).
Intervalo de verificación de usuarios eliminados de AD	15 minutos	El tiempo de sincronización estándar para Active Directory es **15** minutos. El valor **0** impide que XenMobile verifique si hay usuarios eliminados de Active Directory. La configuración recomendada es **15** minutos.

MaxNumberOfWorker	3	La cantidad de subprocesos que se utilizan cuando se importa una gran cantidad de licencias de compras por volumen. El valor predeterminado es **3**. Si necesita mayor optimización, puede aumentar la cantidad de subprocesos. No obstante, con una mayor cantidad de subprocesos (por ejemplo, 6), una importación de compras por volumen consume mucha CPU.

Cómo consultar interbloqueos en una BD SQL y eliminar datos históricos

Cuando detecte interbloqueos, ejecute la siguiente consulta para verlos. A continuación, un administrador de bases de datos o un equipo de Microsoft SQL puede confirmar la información.

Consulta SQL

```
SELECT

db.name DB_Service,

tl.request_session_id,

wt.blocking_session_id,

OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,

tl.resource_type,

h1.TEXT AS RequestingText,

h2.TEXT AS BlockingTest,

tl.request_mode
```



```
18
19 FROM sys.dm_tran_locks AS tl
20
21 INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id
22
23 INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address = wt.
      resource_address
24
25 INNER JOIN sys.partitions AS p ON p.hobt_id = tl.
      resource_associated_entity_id
26
27 INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id = tl.
      request_session_id
28
29 INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id = wt.
      blocking_session_id
30
31 CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1
32
33 CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2
34
35 GO
36 <!--NeedCopy-->
```

Limpiar la base de datos

> **Importante:**
>
> Realice una copia de seguridad de la base de datos antes de modificar las tablas.

1. Ejecute la siguiente consulta para comprobar los datos históricos.

```
1 select COUNT(\*) as total_record from dbo.EWDEPLOY_HISTO;
2 select COUNT(\*) as total_record from dbo.EWSESS;
3 select COUNT(*) as total_record from dbo.EWAUDIT;
4 <!--NeedCopy-->
```

2. Elimine los datos de las tres tablas anteriores.

> **Nota:**
>
> Es posible que no vea datos históricos en una tabla. En tal caso, omita la ejecución de la consulta truncate para dicha tabla.

```
1 truncate TABLE dbo.EWDEPLOY_HISTO;
2 truncate TABLE dbo.EWSESS;
```



```
truncate TABLE dbo.EWAUDIT;
<!--NeedCopy-->
```

3. Desbloquee las consultas SELECT que se bloquearon con los interbloqueos. Este paso se encarga de posteriores interbloqueos.

```
ALTER DATABASE <database_name> SET       READ_COMMITTED_SNAPSHOT
    ON WITH ROLLBACK IMMEDIATE
<!--NeedCopy-->
```

4. De forma predeterminada, la limpieza de la base de datos se realiza cada siete días para conservar datos de retención de sesión y de retención de auditoría, un valor elevado para muchos usuarios. Cambie el valor de limpieza a 1 o 2 días. En las propiedades del servidor, realice el siguiente cambio:

```
zdm.dbcleanup.sessionRetentionTimeInDays = 1 day
zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day
zdm.dbcleanup.auditRetentionTimeInDays=1 day
<!--NeedCopy-->
```

Borrar huérfanos de la tabla KEYSTORE

Si los nodos de XenMobile no rinden como es debido, compruebe si la tabla KEYSTORE es demasiado grande. XenMobile almacena los certificados de inscripción en las tablas ENROLLMENT_CERTIFICATE y KEYSTORE. Cuando elimina o vuelve a inscribir dispositivos, se eliminan los certificados de la tabla ENROLLMENT_CERTIFICATE. Las entradas de la tabla KEYSTORE permanecen, lo que puede causar problemas de rendimiento. Siga este procedimiento para borrar los huérfanos de la tabla KEYSTORE.

> **Importante:**
>
> Realice una copia de seguridad de la base de datos antes de modificar las tablas.

1. Ejecute la siguiente consulta para comprobar los datos históricos.

```
select COUNT(*) from KEYSTORE
<!--NeedCopy-->
```

2. Compruebe si hay huérfanos en la tabla KEYSTORE con la siguiente consulta.

```
WITH cte(KEYSTORE_ID)
AS (SELECT KEYSTORE_ID
    FROM ENROLLMENT_CERTIFICATE
    UNION
    SELECT CA_KEYSTORE_ID
```



```
    FROM LDAP_CONFIG
    UNION
    SELECT CLIENT_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT KEYSTORE_ID
    FROM SAML_SERVICE_PROVIDER
    UNION
    SELECT KEYSTORE_ID
    FROM SERVER_CERTIFICATE)
SELECT keystore.id
FROM keystore
    LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
WHERE KEYSTORE_ID IS NULL;
<!--NeedCopy-->
```

3. Borre los huérfanos mediante la siguiente consulta.

```
WITH cte(KEYSTORE_ID)
    AS (SELECT KEYSTORE_ID
        FROM ENROLLMENT_CERTIFICATE
        UNION
        SELECT CA_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT CLIENT_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT KEYSTORE_ID
        FROM SAML_SERVICE_PROVIDER
        UNION
        SELECT KEYSTORE_ID
        FROM SERVER_CERTIFICATE)
    DELETE FROM keystore
    WHERE id IN
    (
        SELECT keystore.id
        FROM keystore
            LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
        WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'
    );
<!--NeedCopy-->
```

4. Agregue un índice a la tabla KEYSTORE para mejorar la eficiencia de las búsquedas.


```
DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";
ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;
CREATE INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE"("NAME") INCLUDE ("
    ID", "TYPE", "CONTENT", "PASSWORD", "PUBLICLY_TRUSTED", "
    DESCRIPTION", "ALIAS", "MODIFICATION_DATE");
<!--NeedCopy-->
```

Aprovisionar y desaprovisionar aplicaciones

January 4, 2022

El aprovisionamiento de aplicaciones gira en torno a la administración del ciclo de vida de las aplicaciones móviles: preparar, configurar, entregar y administrar aplicaciones móviles dentro de un entorno de XenMobile. En algunos casos, el desarrollo o la modificación del código de la aplicación también puede formar parte del proceso de aprovisionamiento. XenMobile está equipado con varias herramientas y procesos que puede usar para el aprovisionamiento de las aplicaciones.

Antes de leer este artículo sobre el aprovisionamiento de aplicaciones, se recomienda leer lo siguiente:

- Aplicaciones - Comunidades de usuarios

Una vez que haya decidido el tipo de aplicaciones que su organización quiere entregar a los usuarios, puede precisar el proceso para administrar las aplicaciones a lo largo de sus ciclos de vida.

Tenga en cuenta los siguientes puntos a la hora de definir su proceso de aprovisionamiento de aplicaciones:

- **Creación de perfiles de aplicación:** Puede que su organización empiece con una cantidad limitada de aplicaciones. No obstante, la cantidad de aplicaciones a administrar podría aumentar rápidamente, a medida que la cantidad de usuarios aumente y su entorno crezca. Debe definir perfiles de aplicación específicos desde el principio para que el aprovisionamiento de aplicaciones sea fácil de administrar. Crear perfiles de aplicación ayuda a distribuir aplicaciones en grupos lógicos desde una perspectiva no técnica. Por ejemplo, puede crear perfiles de aplicación en función de los siguientes factores:
  - Versión: La versión de la aplicación para el seguimiento
  - Instancias: Varias instancias que se implementan para conjuntos diferentes de usuarios, por ejemplo, usuarios con diferentes niveles de acceso
  - Plataforma: iOS, Android o Windows
  - Público objetivo: Usuarios estándar, departamentos, ejecutivos de alto nivel
  - Propiedad: El departamento es propietario de la aplicación

- Tipo: Enlaces web o aplicaciones públicas, MDX o web y SaaS
- Ciclo de actualización: Con qué frecuencia se actualiza la aplicación
- Licencias: Requisitos y propiedad de las licencias
- Directivas de MDX o SDK de MAM: Para aplicar funcionalidades de MDX a sus aplicaciones móviles
- Acceso a la red: Tipo de acceso, como Secure Browse o Túnel VPN completo

  > **Nota:**
  > SSO Web en túnel es el nombre de Secure Browse en los parámetros de MDX. El comportamiento es el mismo.

Ejemplo:

Factor	Secure Mail	Correo	Interna	Epic Rover
Versión	10.1	10.1	X.x	X.x
Instancia	Dirección IP virtual	Médicos	Sanitarios	Sanitarios
Platform	iOS	iOS	iOS	iOS
Usuarios de destino	Usuarios de direcciones IP virtuales	Médicos	Personal sanitario	Personal sanitario
Propietario	TI	TI	TI	TI
Tipo	MDX	MDX	Nativa	Público
Ciclo de actualización	Trimestral	Trimestral	Anual	N/D
Licencias	N/D	N/D	N/D	Compras por volumen
Directivas MDX	Sí	Sí	Sí	No
Acceso de red	VPN	VPN	VPN	Público

- **Control de versiones de aplicación:** El mantenimiento y el seguimiento de las versiones de las aplicaciones son una parte fundamental del proceso de aprovisionamiento. El control de versiones es claro para los usuarios. Solo reciben notificaciones cuando hay una nueva versión de la aplicación disponible para descargar. En cuanto a usted, revisar y probar cada versión de la aplicación sin la capacidad propia del entorno de producción también es fundamental a fin de evitar el impacto en la producción.

  También es importante evaluar si se requiere una actualización específica. Las actualizaciones

de aplicaciones suelen ser de dos tipos: el primero es una actualización menor (como una corrección de un error específico). El segundo es una publicación de versión importante, que introduce mejoras y cambios significativos en la aplicación. En ambos casos, debe consultar detenidamente las notas de la versión de las aplicaciones para evaluar si la actualización es necesaria.

- **Desarrollo de aplicaciones:** Cuando integra el SDK de MAM en las aplicaciones móviles que desarrolla, aplica funcionalidades de MDX a esas aplicaciones. Consulte Introducción al SDK de MAM.

  El SDK de MAM reemplaza a MDX Toolkit, cuya retirada está programada para marzo de 2022. Para obtener información sobre el empaquetado de aplicaciones, consulte MDX Toolkit. El proceso de aprovisionamiento de una aplicación empaquetada es distinto del proceso de aprovisionamiento de una aplicación estándar no empaquetada.

- **Seguridad de las aplicaciones:** Definir los requisitos de seguridad necesarios para las aplicaciones o los perfiles de aplicaciones forma parte del proceso de aprovisionamiento. Puede asignar los requisitos de seguridad a directivas específicas de MDM o MAM antes de implementar las aplicaciones. Esa planificación simplifica y agiliza la implementación de aplicaciones. Por ejemplo:

  - Puede que le interese implementar ciertas aplicaciones de forma diferente.
  - Es posible que quiera realizar cambios de arquitectura en el entorno de XenMobile. Los cambios dependen del tipo de cumplimiento de seguridad que requieren las aplicaciones. Por ejemplo, puede interesarle que el dispositivo esté cifrado para permitir el uso de una aplicación importante de inteligencia empresarial, o puede que una aplicación requiera unas geocercas o un cifrado SSL de punto a punto.

- **Entrega de aplicaciones:** XenMobile permite entregar aplicaciones como aplicaciones MDM o como aplicaciones MAM. Las aplicaciones MDM aparecen en XenMobile Store. Este almacén permite entregar convenientemente aplicaciones públicas o nativas a los usuarios. El único control de aplicaciones MDM que gestiona es aplicar restricciones en el nivel de dispositivo. Sin embargo, la entrega de aplicaciones mediante MAM ofrece un control total, tanto sobre la entrega de la aplicación como sobre la aplicación en sí. Por lo general, entregar las aplicaciones a través de MAM es lo más adecuado.

- **Mantenimiento de aplicaciones:**

  - Lleve a cabo una auditoría inicial. Realice un seguimiento de la versión de aplicación presente en el entorno de producción y del último ciclo de actualización. Tome nota de las funciones o las correcciones de errores específicas que requirieron la actualización.
  - Establezca puntos de referencia. Cree una lista de la versión estable más reciente de cada aplicación. Esta versión de la aplicación debe estar disponible para poder volver a ella en caso de que ocurran problemas imprevistos después de la actualización. Desarrolle

también un plan de reversión. Pruebe las actualizaciones de aplicaciones en un entorno de prueba antes de implementarlas en producción. Si es posible, implemente la actualización primero en un subconjunto de usuarios de producción y, a continuación, en toda la base de usuarios.

- Suscríbase a las notificaciones de actualización de software de Citrix y las notificaciones de proveedores de software de terceros. Es importante para estar al día con la versión más reciente de las aplicaciones. También puede haber disponible una compilación de acceso anticipado (EAR) para realizar pruebas.
- Diseñe una estrategia para notificar a los usuarios. Debe definir una estrategia para notificar a los usuarios cuando las actualizaciones de la aplicación estén disponibles. Forme a los usuarios antes de la implementación. Puede enviar varias notificaciones antes de actualizar las aplicaciones. Dependiendo de la aplicación, el mejor método de notificación pueden ser notificaciones por correo electrónico o sitios web.

La administración del ciclo de vida de una aplicación implica todo el ciclo de vida, desde la implementación inicial hasta la retirada. El ciclo de vida de una aplicación consta de estas fases:

1. Requisitos para especificaciones. Empezar con los requisitos de usuario y el caso concreto del negocio.
2. Desarrollo: Validar que la aplicación cumple las necesidades del negocio.
3. Pruebas: Identificar usuarios de prueba, problemas y errores.
4. Implementación: Implementar la aplicación a los usuarios de producción.
5. Mantenimiento: Actualizar la versión de la aplicación. Implemente la aplicación en un entorno de prueba antes de actualizar la aplicación en un entorno de producción.

Ejemplo del ciclo de vida de aplicaciones con Secure Mail

1. Requisitos para especificaciones. Como requisito de seguridad, se necesita una aplicación de correo electrónico que se encuentre en el contenedor y admita las directivas MDX de seguridad.
2. Desarrollo: Validar que la aplicación cumple las necesidades del negocio. Debe poder aplicar controles de directivas MDX a la aplicación.
3. Pruebas. Asigne Secure Mail a un grupo de usuarios de prueba e implemente el archivo MDX correspondiente desde XenMobile Server. Los usuarios de la prueba validan que pueden enviar y recibir correos electrónicos correctamente, y tienen acceso al calendario y los contactos. Los usuarios de la prueba también informan de problemas e identifican errores. En función de los comentarios de los usuarios de la prueba, optimice la configuración de Secure Mail para su uso en producción.
4. Implementación. Una vez completada la fase de prueba, asigne Secure Mail a los usuarios de producción e implemente el archivo MDX correspondiente desde XenMobile.
5. Mantenimiento. Está disponible una nueva actualización de Secure Mail. Descargue el nuevo archivo MDX desde las descargas de Citrix y reemplace el archivo MDX existente en XenMobile

Server. Indique a los usuarios que realicen la actualización. Nota: Citrix recomienda completar y probar este proceso en un entorno de prueba. A continuación, cargue la aplicación en un entorno de producción de XenMobile y póngala a disposición de los usuarios.

Para obtener más información, consulte Empaquetar aplicaciones móviles iOS y Empaquetar aplicaciones móviles Android.

Operaciones del panel de mandos

January 4, 2022

Puede ver toda la información de un vistazo desde su panel de mandos en la consola de XenMobile. En esta información, puede utilizar widgets para ver rápidamente los problemas y las operaciones correctas que se hayan producido.

Por regla general, el panel de mandos es la pantalla que aparece al iniciar sesión por primera vez en la consola de XenMobile. Para acceder al panel de mandos desde cualquier otro sitio de la consola, haga clic en **Analizar**. Haga clic en **Personalizar** en el panel de mandos para modificar el diseño de la página y para modificar los widgets que aparecen.

- **Mis paneles de mandos:** Puede guardar hasta cuatro paneles de mandos diferentes. Puede seleccionar cada panel guardado para verlo y modificarlo por separado.
- **Estilo de diseño:** En esta fila, puede seleccionar la cantidad de widgets que aparecerán en el panel de mandos y cómo se etiquetarán.
- **Selección de widget:** Puede elegir qué información se mostrará en el panel de mandos.
  - **Notificaciones:** Marque la casilla situada encima de los números en la parte izquierda para agregar una barra de notificaciones encima de los widgets. Esta barra muestra la cantidad de dispositivos conformes, dispositivos inactivos, dispositivos borrados o dispositivos inscritos en las últimas 24 horas.
  - **Dispositivos por plataforma:** Muestra la cantidad de dispositivos administrados y no administrados por plataforma.
  - **Dispositivos por operador:** Muestra la cantidad de dispositivos administrados y no administrados por operador. Haga clic en cada barra para ver un desglose por plataforma.
  - **Dispositivos administrados por plataforma:** Muestra la cantidad de dispositivos administrados por plataforma.
  - **Dispositivos no administrados por plataforma:** Muestra la cantidad de dispositivos no administrados por plataforma. Los dispositivos que aparecen en este gráfico pueden tener un agente instalado, pero se les han borrado los datos o se les han revocado los privilegios.
  - **Dispositivos por estado de ActiveSync Gateway:** Muestra la cantidad de dispositivos agrupados por estado de ActiveSync Gateway. La información se muestra como estado

Bloqueado, Permitido o Desconocido. Puede hacer clic en cada barra para desglosar los datos por plataforma.
- **Dispositivos por propietario:** Muestra la cantidad de dispositivos agrupados por propietario. La información se muestra como propiedad de la empresa, del empleado o propietario desconocido.
- **Implementaciones fallidas de grupos de entrega:** Muestra la cantidad total de implementaciones fallidas desglosadas por paquete. Solo se muestran los paquetes de implementaciones con errores.
- **Dispositivos por motivo de bloqueo:** Muestra la cantidad de dispositivos bloqueados por ActiveSync.
- **Aplicaciones instaladas:** Con este widget, puede escribir un nombre de aplicación y aparecerá un gráfico con información acerca de esa aplicación.
- **Uso de licencias de aplicaciones de compras por volumen:** Muestra estadísticas sobre el uso de licencias por parte de las aplicaciones de compras por volumen de Apple.

Casos de uso

A continuación, dispone de algunos ejemplos de las muchas maneras en que puede usar los widgets del panel de mandos para supervisar el entorno.

- Ha implementado las aplicaciones móviles de productividad y recibe tíquets de asistencia relacionados con ellas, donde se le informa que no se pueden instalar en los dispositivos. Utilice los widgets **Dispositivos no conformes** y **Aplicaciones instaladas** para ver los dispositivos que no tienen instaladas las aplicaciones móviles de productividad.
- Quiere supervisar los dispositivos inactivos para eliminarlos del entorno y reclamar las licencias. Use el widget **Dispositivos inactivos** para hacer un seguimiento de estos datos.
- Recibe tíquets de asistencia relacionados con datos que no se sincronizan correctamente. Puede utilizar los widgets **Dispositivos por estado de ActiveSync Gateway** y **Dispositivos por motivo de bloqueo** para determinar si el problema está relacionado con ActiveSync.

Informes

Una vez el entorno está configurado y los usuarios se han inscrito, puede ejecutar informes para conocer datos de su implementación. XenMobile incluye una serie de informes integrados para ver con mayor precisión los dispositivos que se ejecutan en su entorno. Para obtener más información, consulte Informes.

> **Importante:**
>
> 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 consecuen-

> cias 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.

Control de acceso basado en roles y asistencia en XenMobile

January 4, 2022

XenMobile utiliza el control de acceso basado en roles (RBAC) para restringir el acceso de grupos y usuarios a las funciones del sistema de XenMobile, como la consola de XenMobile, Remote Support y la API pública. En este artículo, se describen los roles integrados en XenMobile y se incluyen consideraciones a tener en cuenta para elegir un modelo de asistencia de XenMobile que utilice RBAC.

> **Nota:**
>
> Remote Support no está disponible para nuevos clientes desde el 1 de enero de 2019. Los clientes existentes pueden seguir utilizando el producto, pero Citrix no proporcionará mejoras ni correcciones.

Roles integrados

Puede agregar roles y cambiar el acceso concedido a los siguientes roles integrados. Para conocer el conjunto completo de los permisos de funciones y accesos asociados a cada rol y su configuración predeterminada, descargue Role-Based Access Control Defaults desde la documentación de XenMobile. Para ver una definición de cada función, consulte Configurar roles con RBAC en la documentación de XenMobile.

Rol de administrador

Acceso predeterminado concedido:

- Acceso completo al sistema, excepto a Remote Support.
- De forma predeterminada, los administradores pueden realizar algunas tareas de asistencia, (por ejemplo, comprobar la conectividad y crear paquetes de asistencia).

Consideraciones:

- ¿Algunos o todos sus administradores necesitan acceso a Remote Support? Si es así, puede modificar el rol Admin o agregar roles de administrador.
- Para restringir más el acceso de algunos administradores o grupos de administradores, agregue roles basados en la plantilla de administrador y modifique los permisos.

Aprovisionamiento de dispositivos

Acceso predeterminado concedido:

- Acceder a la consola de XenMobile para realizar una administración básica en dispositivos Windows CE: agregar, cambiar y quitar dispositivos; utilice la página “Parámetros”.

Consideraciones:

- Se aplica solo a dispositivos con Windows CE.

Asistencia

Acceso predeterminado concedido:

- Acceso a Remote Support.

Consideraciones:

- Para las implementaciones locales de XenMobile Server, la asistencia remota (Remote Support) permite que el personal de Help Desk tome el control remoto de los dispositivos móviles Windows CE y Android administrados. La transmisión de la pantalla solo se admite en dispositivos Samsung Knox.
- Remote Support no está disponible para implementaciones locales en clúster de XenMobile Server.

Usuario

Acceso predeterminado concedido:

- Acceso restringido a la consola de XenMobile: funciones del dispositivo (como borrar, bloquear o desbloquear el dispositivo, bloquear o desbloquear el contenedor, ver la ubicación y establecer restricciones geográficas, hacer sonar el dispositivo, restablecer la contraseña del contenedor); agregar, eliminar y enviar invitaciones de inscripción.

Consideraciones:

- El rol Usuario permite habilitar usuarios para que se ayuden a sí mismos.
- Para admitir dispositivos compartidos, cree un rol de usuario para la inscripción de dispositivos compartidos.

Consideraciones para un modelo de asistencia de XenMobile

Los modelos de asistencia que puede adoptar varían ampliamente y pueden implicar a terceros que gestionen la asistencia de nivel 1 y 2, mientras que los empleados gestionan la asistencia de nivel 3

y 4. Independientemente de cómo distribuya la carga de la asistencia, tenga en cuenta las consideraciones en esta sección que sean específicas para su implementación de XenMobile y su base de usuarios.

¿Los usuarios tienen dispositivos propiedad de la empresa o BYOD?
La pregunta principal que influye en la asistencia es a quién pertenece el dispositivo del usuario en su entorno XenMobile. Si sus usuarios tienen dispositivos propiedad de la empresa, puede ofrecer un nivel de asistencia más bajo, como una forma de bloquear completamente los dispositivos. En ese caso, puede proporcionar un servicio de asistencia que ayude a los usuarios con los problemas de los dispositivos y les guíe para saber cómo usarlos. Según los tipos de dispositivo para los que vaya a ofrecer asistencia, plantéese cómo usar los roles de RBAC "Aprovisionamiento de dispositivos" y "Asistencia" para el servicio de asistencia.

Si los usuarios tienen dispositivos BYOD, puede que la organización espere que busquen sus propias fuentes de ayuda con el dispositivo. En ese caso, la asistencia que ofrezca la organización es más bien un rol administrativo centrado en los problemas específicos de XenMobile.

¿Cuál es su modelo de asistencia para los escritorios?
Plantéese si el modelo de asistencia para los escritorios se puede aplicar a otros dispositivos propiedad de la empresa. ¿Puede usar la misma organización de asistencia? ¿Qué formación adicional necesitará?

¿Quiere dar a los usuarios acceso a Self Help Portal de XenMobile?
Utilice **Parámetros > Inscripción** para habilitar Self Help Portal para un modo de seguridad de la inscripción. Desde Self Help Portal, los usuarios pueden generar enlaces de inscripción que les permitan inscribir sus propios dispositivos o enviarse la invitación a una inscripción. Consulte Configurar modos de seguridad de inscripción.

Supervisar sistemas

January 4, 2022

Para garantizar un tiempo de actividad óptimo para la conectividad y el acceso a las aplicaciones, debe supervisar los siguientes componentes principales en el entorno de XenMobile.

Servidor de XenMobile

El servidor de XenMobile genera y almacena registros en el almacenamiento local; también se pueden exportar a un servidor de registros del sistema (servidor syslog). Puede configurar parámetros de registro que especifiquen restricciones de tamaño, de nivel de registro, o puede crear registradores personalizados para filtrar eventos específicos. Puede realizar búsquedas en los registros del servidor de

XenMobile desde la consola de XenMobile en cualquier momento. También puede exportar la información contenida en los registros, a través del servidor syslog, a los servidores de registro Splunk de producción.

En la lista siguiente, se describen los diferentes tipos de archivos de registros disponibles en XenMobile:

Archivo de registros de depuración: Contiene información del nivel de depuración sobre los servicios web centrales de XenMobile, incluidos los mensajes de error y las acciones relacionadas con el servidor.

Formato del mensaje:

```
<date> <timestamp> <loglevel> <class name (including the package)> - <id> <
log message>
```

- donde <id> es un identificador único, como sessionID.
- donde <log message> es el mensaje suministrado por la aplicación.

Archivo de registros de auditoría de administración: Contiene información de auditoría sobre actividad en la consola de XenMobile.

> **Nota:**
>
> Se utiliza el mismo formato para los registros de auditoría de usuario y auditoría de administración.

Formato del mensaje:

A excepción de los valores de Fecha y Marca de hora necesarios, todos los demás atributos son opcionales. Los campos opcionales se representan con “” en el mensaje.

```
<date> <timestamp> "<username/id>""<sessionid>""<deviceid>""<clientip>"
"<action>""<status>""<application name>""<app user id>""<user agent>""<
details>"
```

La siguiente tabla contiene los eventos disponibles para el registro de auditoría de administración:

Mensajes de registro de auditoría de administrador para eventos	Estado
Inicio de sesión	completado/error
Cierre de sesión	completado/error
Obtener administrador	completado/error
Actualizar administrador	completado/error
Obtener aplicación	completado/error
Agregar aplicación	completado/error

Mensajes de registro de auditoría de administrador para eventos	Estado
Actualizar aplicación	completado/error
Eliminar aplicación	completado/error
Vincular aplicación	completado/error
Desvincular aplicación	completado/error
Inhabilitar aplicación	completado/error
Habilitar aplicación	completado/error
Obtener categoría	completado/error
Agregar categoría	completado/error
Actualizar categoría	completado/error
Eliminar categoría	completado/error
Agregar certificado	completado/error
Eliminar certificado	completado/error
Activar certificado	completado/error
Certificado de CSR	completado/error
Exportar certificado	completado/error
Eliminar cadena de certificados	completado/error
Agregar cadena de certificados	completado/error
Obtener conector	completado/error
Agregar conector	completado/error
Eliminar conector	completado/error
Actualizar conector	completado/error
Obtener dispositivo	completado/error
Bloquear dispositivo	completado/error
Desbloquear dispositivo	completado/error
Borrar datos del dispositivo	completado/error
Anular borrado de datos del dispositivo	completado/error
Eliminar dispositivo	completado/error
Obtener rol	completado/error

Mensajes de registro de auditoría de administrador para eventos	Estado
Agregar rol	completado/error
Actualizar rol	completado/error
Eliminar rol	completado/error
Vincular rol	completado/error
Desvincular rol	completado/error
Actualizar parámetros de configuración	completado/error
Actualizar correo electrónico de flujo de trabajo	completado/error
Agregar flujo de trabajo	completado/error
Eliminar flujo de trabajo	completado/error
Agregar Active Directory	completado/error
Actualizar Active Directory	completado/error
Agregar masteruserlist	completado/error
Actualizar masteruserlist	completado/error
Actualizar DNS	completado/error
Actualizar red	completado/error
Actualizar servidor de registros	completado/error
Transferir registro desde el servidor de registros	completado/error
Actualizar syslog	completado/error
Actualizar actualizaciones de Receiver	completado/error
Actualizar servidor horario	completado/error
Actualizar confianza	completado/error
Agregar registro de servicios	completado/error
Actualizar registro de servicios	completado/error
Actualizar correo electrónico de Receiver	completado/error
Cargar revisión	completado/error
Importar instantánea	completado/error
Obtener detalles de aplicación desde tienda de aplicaciones	completado/error

Mensajes de registro de auditoría de administrador para eventos	Estado
Actualizar MDM	completado/error
Eliminar MDM	completado/error
Agregar HDX	completado/error
Actualizar HDX	completado/error
Eliminar HDX	completado/error
Agregar personalización de marca	completado/error
Eliminar personalización de marca	completado/error
Actualizar descarga de SSL	completado/error
Agregar propiedad de cuenta	completado/error
Eliminar propiedad de cuenta	completado/error
Actualizar propiedad de cuenta	completado/error
Agregar baliza	completado/error

Archivo de registro de auditoría de usuario: Contiene información relacionada con la actividad de usuario, proveniente de los dispositivos inscritos.

> **Nota:**
>
> Se utiliza el mismo formato para los registros de auditoría de usuario y auditoría de administración.

Formato del mensaje:

A excepción de los valores de Fecha y Marca de hora necesarios, todos los demás atributos son opcionales. Los campos opcionales se representan con “” en el mensaje. Por ejemplo:

```
<date> <timestamp> "<username/id>""<sessionid>""<deviceid>""<clientip>"
"<action>""<status>""<application name>""<app user id>""<user agent>""<
details>"
```

La siguiente tabla contiene los eventos disponibles para el registro de auditoría de usuario:

Mensajes de registro de auditoría de usuario para eventos	Estado
Inicio de sesión	completado/error
Tiempo de desconexión de la sesión	completado/error

Mensajes de registro de auditoría de usuario para eventos	Estado
Suscribir	completado/error
Cancelar suscripción	completado/error
Preinicio	completado/error
AGEE SSO	completado/error
Token SAML para Citrix Files	completado/error
Registro de dispositivos	completado/error
Comprobación de dispositivo	bloquear o borrar
Actualización de dispositivo	completado/error
Actualización de token	completado/error
Secreto guardado	completado/error
Secreto recuperado	completado/error
Cambio de contraseña iniciado por el usuario	completado/error
Descarga de cliente móvil	completado/error
Cierre de sesión	completado/error
Servicio de detección	completado/error
Servicio de dispositivo de punto final	completado/error

Funciones de MDM	Estado
REGHIVE	completado/error
Inventario de CAB	completado/error
CAB	completado/error
Instalación automática de CAB	completado/error
Instalación de shell de CAB	completado/error
Carpeta de creación CAB	completado/error
Obtener archivo CAB	completado/error
Carpeta de creación de archivos	completado/error
Obtener archivo	completado/error
Archivo enviado	completado/error

Funciones de MDM	Estado
Carpeta de creación de scripts	completado/error
Obtener script	completado/error
Script enviado	completado/error
Ejecución de script de shell	completado/error
Ejecución automática de script	completado/error
Inventario APK	completado/error
APK	completado/error
Instalación de shell APK	completado/error
Instalación automática de APK	completado/error
Carpeta de creación de APK	completado/error
Obtener archivo APK	completado/error
Aplicación APK	completado/error
Aplicación EXT	completado/error
Obtener lista	completado/error
Lista enviada	completado/error
Ubicar dispositivo	completado/error
CFG	completado/error
Desbloquear	completado/error
Borrado de SharePoint	completado/error
Configuración de SharePoint	completado/error
Eliminar perfil	completado/error
Quitar aplicación	completado/error
Quitar aplicación no administrada	completado/error
Quitar perfil no administrado	completado/error
Aplicación IPA	completado/error
Aplicación EXT	completado/error
Aplicar código de canje	completado/error
Aplicar parámetros	completado/error
Habilitar seguimiento de dispositivo	completado/error

Funciones de MDM	Estado
Directiva de administración de aplicaciones	completado/error
Borrado de tarjeta SD	completado/error
Datos adjuntos de correo cifrados	completado/error
Personalización de marca	completado/error
Secure Browser	completado/error
Explorador de contenedor	completado/error
Desbloquear contenedor	completado/error
Restablecimiento de contraseña de contenedor	completado/error
Credenciales de autenticación del cliente AG	completado/error

Citrix ADC también supervisa el estado de servicio web de XenMobile, que está configurado con sondeos inteligentes de supervisión para simular solicitudes HTTP a cada nodo del clúster del servidor de XenMobile. Los sondeos determinan si el servicio está en línea y responden según la respuesta recibida. En caso de que un nodo no responda según lo previsto, Citrix ADC marca el servidor como inactivo. Además, Citrix ADC saca el nodo del grupo de equilibrio de carga y registra el evento para usarlo en la generación de alertas a través de la solución de supervisión de Citrix ADC.

También puede usar las herramientas estándares de supervisión que ofrece el hipervisor para supervisar las máquinas virtuales de XenMobile y proporcionar las alertas relevantes referentes a la unidad CPU, la memoria y las métricas de utilización del almacenamiento.

SQL Server y la base de datos

El rendimiento de SQL Server y de la base de datos afecta directamente a los servicios de XenMobile. La instancia de XenMobile requiere acceso a la base de datos en todo momento y se desconecta (por ejemplo, deja de responder) en caso de una interrupción en la infraestructura SQL. La consola de XenMobile puede seguir funcionando durante cierto tiempo después de un problema de espacio en disco con SQL Server. Para garantizar el máximo tiempo de actividad de la base de datos y el rendimiento adecuado para la carga de trabajo de XenMobile, debe supervisar proactivamente el estado de sus servidores SQL. Para obtener más información sobre la supervisión de los servidores SQL, consulte Introducción a la supervisión y optimización del rendimiento. Además, debe ajustar la asignación de recursos de la CPU, la memoria y el almacenamiento para garantizar los contratos de nivel de servicio a medida que su entorno de XenMobile siga creciendo.

Citrix ADC

Con Citrix ADC, puede registrar métricas en el almacenamiento interno o enviar registros a un servidor de registros externo. Puede configurar el servidor de syslog para exportar los registros de Citrix ADC a los servidores de captura de registros Splunk de producción. En Citrix ADC están disponibles los siguientes niveles de registros:

- Emergencia
- Alerta
- Grave
- Error
- Advertencia
- Información

Los archivos de registros también se almacenan en el almacenamiento de Citrix ADC, en el directorio /var/log/ns.log, y se llaman newnslog. Citrix ADC transfiere y comprime los archivos mediante el algoritmo GZIP. Los nombres del archivo de registros son newnslog.xx.gz, donde xx representa un número consecutivo.

Citrix ADC también admite alertas y capturas SNMP como una opción de supervisión. Para ver una lista de las capturas de SNMP, consulte Supervisión de SNMP.

Recuperación ante desastres

January 4, 2022

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 desde el sitio activo al sitio pasivo.

La estrategia recomendada de recuperación ante desastres que se describe en este artículo consiste en:

- Un solo sitio activo de XenMobile en el centro de datos de una ubicación geográfica que sirve a todos los usuarios de empresa a nivel mundial, conocido como el sitio principal.
- Un segundo sitio de XenMobile en el centro de datos de una segunda ubicación geográfica, conocido como el sitio de recuperación ante desastres. Este sitio de recuperación ante desastres ofrece una conmutación por error desde el sitio activo al sitio pasivo si se produce un error en el centro de datos del sitio principal. El sitio principal incluye XenMobile, la base de datos SQL, la infraestructura de Citrix ADC para facilitar la conmutación por error y ofrecer a los usuarios acceso a XenMobile si falla la conectividad con el sitio principal.

Los servidores de XenMobile presentes en el sitio de recuperación ante desastres permanecen fuera de línea durante las operaciones habituales. Solo se ponen en línea en situaciones de recuperación ante desastres, donde se requiere una conmutación por error completa del sitio principal al sitio de recuperación ante desastres. Los servidores SQL presentes en el sitio de recuperación ante desastres deben estar activos y listos para ofrecer conexiones antes de iniciarse los servidores de XenMobile en el sitio de recuperación ante desastres.

Esta estrategia de recuperación ante desastres se basa en la conmutación por error manual del nivel de acceso de Citrix ADC mediante cambios de DNS para enrutar las conexiones de MDM y MAM al sitio de recuperación ante desastres en caso de una interrupción.

> **Nota:**
>
> Para poder usar esta arquitectura, debe tener un proceso implementado para copias de seguridad asíncronas de las bases de datos y alguna forma de garantizar una alta disponibilidad de la infraestructura SQL.

Proceso de conmutación por error en caso de recuperación ante desastres

1. Si está probando su proceso de conmutación por error en caso de recuperación ante desastres, apague los servidores de XenMobile que haya presentes en el sitio principal para simular un fallo del sitio.
2. Modifique los registros DNS públicos para que los servidores de XenMobile apunten a las direcciones IP externas del sitio de recuperación ante desastres.
3. Modifique el registro DNS interno para que SQL Server apunte a la dirección IP del servidor SQL presente en el sitio de recuperación ante desastres.
4. Ponga en línea las bases de datos SQL de XenMobile en el sitio de recuperación ante desastres. Compruebe que el servidor SQL Server y la base de datos estén activos y listos para ofrecer conexiones desde los servidores de XenMobile locales en el sitio.
5. Encienda los servidores de XenMobile en el sitio de recuperación ante desastres.

Proceso de actualización de XenMobile Server

Siga estos pasos cada vez que actualice XenMobile con parches y versiones para mantener uniforme el código de los servidores principales y de recuperación ante desastres.

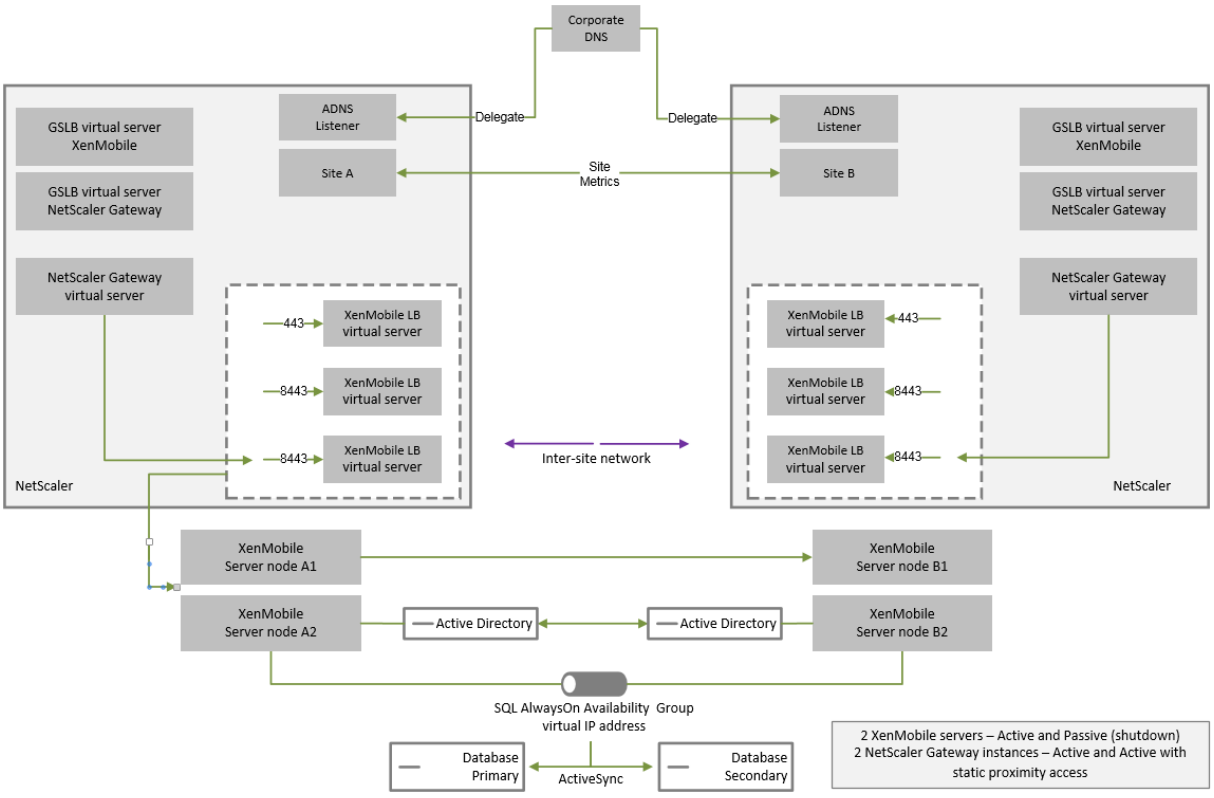
1. Compruebe que los servidores de XenMobile en el sitio principal disponen de los parches más recientes o están actualizados.
2. Compruebe que el registro DNS para el servidor SQL se esté resolviendo en la base de datos activa del servidor SQL en el sitio principal.
3. Ponga en línea los servidores de XenMobile del sitio de recuperación ante desastres. Esos servidores se conectan a la base de datos del sitio principal a través de WAN solo durante el proceso

de actualización.

4. Aplique las actualizaciones y los parches necesarios a todos los servidores de XenMobile del sitio de recuperación ante desastres.
5. Reinicie los servidores de XenMobile y confirme que el parche o la actualización se haya realizado correctamente.

Diagrama de la arquitectura de referencia en una recuperación ante desastres

En el siguiente diagrama se muestra la arquitectura de alto nivel para una implementación de recuperación ante desastres de XenMobile.



GSLB para la recuperación ante desastres

Un elemento clave de esta arquitectura es el uso de Global Server Load Balancing (GSLB) para dirigir el tráfico al centro de datos correcto.

De forma predeterminada, el asistente de Citrix ADC para XenMobile configura Citrix Gateway de una manera que no permite el uso de GSLB para la recuperación ante desastres. Por lo tanto, se deben tomar medidas adicionales.

Cómo funciona GSLB

GSLB es, principalmente, un tipo de DNS. Los dispositivos Citrix ADC que intervienen actúan como servidores DNS autorizados y resuelven los registros DNS a la dirección IP correcta (por regla general, la dirección IP virtual que debe recibir tráfico). El dispositivo Citrix ADC comprueba el estado del sistema antes de responder a una consulta de DNS y dirigir el tráfico a ese sistema.

Tras resolverse el registro, termina el rol de GSLB en resolver el tráfico. El cliente se comunica directamente con la dirección IP virtual (VIP) de destino. El comportamiento del cliente DNS desempeña un papel importante en cómo y cuándo caduca un registro. Eso está en gran medida fuera de los límites del sistema de Citrix ADC. Como tal, GSLB está sujeto a las mismas limitaciones que la resolución de nombres DNS. Los clientes guardan en caché las respuestas. Por tanto, este equilibrio de carga no es tan inmediato como el equilibrio de carga tradicional.

La configuración de GSLB en Citrix ADC, incluidos los sitios, los servicios y las supervisiones, existe para proporcionar la resolución de nombres DNS correcta.

La configuración real para los servidores de publicación (en este caso, la configuración que crea el asistente de Citrix ADC para XenMobile) no se ve afectada por el GSLB. GSLB es un servicio independiente en Citrix ADC.

Dificultades con la delegación de dominio al usar GSLB con XenMobile

El asistente de Citrix ADC para XenMobile configura Citrix Gateway para XenMobile. Este asistente genera tres servidores virtuales de equilibrio de carga y un servidor virtual de Citrix Gateway.

Dos de los servidores virtuales de equilibrio de carga gestionan el tráfico MDM, en los puertos 443 y 8443. Citrix Gateway recibe el tráfico MAM y lo reenvía al tercer servidor, el servidor virtual de equilibrio de carga de MAM, en el puerto 8443. Todo el tráfico enviado al servidor virtual de equilibrio de carga de MAM pasa a través de Citrix Gateway.

El servidor virtual de equilibrio de carga de MAM requiere el mismo certificado SSL que los servidores de XenMobile y utiliza el mismo FQDN que se usa para inscribir los dispositivos. El servidor de equilibrio de carga de MAM también utiliza el mismo puerto (8443) que uno de los servidores de equilibrio de carga de MDM. Para permitir que el tráfico se resuelva, el asistente de Citrix ADC para XenMobile crea un registro DNS local en Citrix Gateway. El registro DNS coincide con el FQDN utilizado para inscribir los dispositivos.

Esta configuración es eficaz cuando la URL del servidor de XenMobile no es una URL de dominio GSLB. Si se utiliza una URL de dominio GSLB como URL del servidor de XenMobile, como se requiere para la recuperación ante desastres, el registro DNS local impide que Citrix Gateway resuelva el tráfico a los servidores de equilibrio de carga de MDM.

Usar el método CNAME para la recuperación ante desastres de GSLB

Para solucionar las dificultades que presenta la configuración predeterminada creada por el asistente de Citrix ADC para XenMobile, puede crear un registro CNAME para el FQDN del servidor de XenMobile en el dominio principal (`company.com`) y apuntar un registro en la subzona delegada (`gslb.company.com`) para la cual Citrix ADC está autorizado. Al hacerlo, se permite la creación del registro A de DNS estático para la dirección IP virtual de equilibrio de carga MAM requerida para resolver el tráfico.

1. En el DNS externo, cree un CNAME para el FQDN del servidor de XenMobile que apunte al FQDN de dominio GSLB en GSLB de Citrix ADC. Necesita dos dominios GSLB: uno para el tráfico MDM y otro para el tráfico MAM (Citrix Gateway).

   Ejemplo:

   ```
   CNAME = xms.company.com IN CNAME xms.gslb.comany.com
   ```

2. En la instancia de Citrix Gateway de cada sitio, cree un servidor virtual GSLB con el FQDN al que apunta el registro CNAME.

   Ejemplo:

   ```
   bind gslb vserver xms-gslb -domainName xms.gslb.company.com
   ```

   Cuando utilice el asistente de Citrix ADC para XenMobile para implementar Citrix Gateway, use la URL del servidor de XenMobile cuando configure el servidor de equilibrio de carga de MAM. Así, crea un registro A de DNS estático para la URL del servidor de XenMobile.

3. Realice pruebas con los clientes que se inscriban en Secure Hub con la URL del servidor de XenMobile (`xms.company.com`).

   En este ejemplo se utilizan los siguientes FQDN:

   - `xms.company.com` es la URL utilizada por el tráfico de MDM y utilizada por los dispositivos que se inscriben; se ha configurado en este ejemplo desde el asistente de Citrix ADC para XenMobile.
   - `xms.gslb.company.com` es el FQDN de dominio GSLB para el servidor de XenMobile.

Proceso de asistencia de Citrix

January 4, 2022

Puede acudir a los servicios de asistencia técnica de Citrix para obtener ayuda con problemas relacionados con los productos Citrix. El personal de asistencia ofrece soluciones temporales y resoluciones, además de trabajar codo con codo con los equipos de desarrollo para ofrecer soluciones.

Citrix Consulting Services o Citrix Education Services ofrecen ayuda relacionada con la formación referente a los productos, y recomendaciones para el uso, la configuración, la instalación del producto o el diseño y la arquitectura del entorno.

Citrix Consulting ayuda con los proyectos relacionados con productos Citrix, incluidas las pruebas de concepto, las evaluaciones del impacto económico, las comprobaciones del estado de la infraestructura, el análisis de los requisitos de diseño, la verificación del diseño de la arquitectura, la integración y el desarrollo de los procesos operativos.

Citrix Education ofrece la mejor formación y certificación de TI de su clase en Citrix Virtualization, Citrix Cloud y las tecnologías de red.

Citrix recomienda que aproveche al máximo los recursos de ayuda de Citrix y sus recomendaciones antes de abrir un caso de asistencia. Por ejemplo, hay varios lugares desde donde puede acceder a artículos y publicaciones, escritos por expertos técnicos de Citrix. Asimismo, puede acudir a la documentación del producto para conocer las soluciones y las tecnologías Citrix, leer directamente las publicaciones de los ejecutivos, los equipos de producto y los expertos técnicos de Citrix. Consulte las páginas de Knowledge Center, la documentación de producto y los blogs, respectivamente.

Si lo que busca es una asistencia más interactiva, puede participar en los foros, donde puede hacer preguntas y obtener respuestas reales de otros clientes, compartir ideas, opiniones, información técnica y recomendaciones en grupos de usuarios y grupos de interés. En esos foros, también puede comunicarse con los ingenieros de asistencia de Citrix que supervisan las redes sociales de Citrix Support. Consulte las páginas Support Forums y Citrix Community) respectivamente.

También tiene acceso a cursos de formación y certificación para desarrollar sus habilidades. Consulte Citrix Education.

Citrix Insight Services ofrece una sencilla plataforma de resolución de problemas en línea, que también puede comprobar el estado de su entorno Citrix. Disponible para Citrix XenMobile, Citrix Virtual Apps and Desktops, Citrix Hypervisor y Citrix Gateway. Consulte Analysis Tool.

Para buscar asistencia técnica, puede crear un caso de asistencia por teléfono o a través de la red. Puede usar el sitio web para problemas de intensidad baja y media; recomendamos la opción de teléfono para problemas de alta intensidad. Para saber cómo ponerse en contacto con la asistencia en caso de problemas de XenMobile, consulte How to Contact Support.

Si busca un punto de contacto único altamente capacitado con amplia experiencia en la entrega de soluciones Citrix, Citrix Services ofrece un Technical Relationship Manager (un gestor técnico que mantiene contacto directo con el cliente). Para obtener más información sobre las ventajas y la oferta de los servicios de Citrix, consulte Citrix Worldwide Services.

Enviar invitaciones de inscripción a grupos en XenMobile

January 4, 2022

Por John Bartel III

En XenMobile Server, puede enviar invitaciones de inscripción a grupos y grupos anidados. Las invitaciones de inscripción no están disponibles para dispositivos Windows.

Al configurar la invitación de grupo, puede especificar una o varias plataformas de dispositivo. También puede etiquetar los dispositivos para distinguir, por ejemplo, los dispositivos propiedad de la empresa y los dispositivos propiedad de los empleados. A continuación, puede establecer el tipo de autenticación para los dispositivos de usuario.

> **Nota:**
>
> Si va a utilizar plantillas de notificaciones personalizadas, debe definir esas plantillas antes de configurar los modos de seguridad para la inscripción. Para obtener más información acerca de las plantillas de notificaciones, consulte Crear y actualizar plantillas de notificaciones.

Para obtener más información sobre la configuración básica de cuentas de usuario, roles, modos de seguridad de inscripción e invitaciones, consulte Inscripción, roles y cuentas de usuario.

Pasos generales

1. En la consola de XenMobile, vaya a **Administrar > Invitaciones de inscripción**.
2. Haga clic en la opción **Agregar**, situada en la parte superior izquierda de la pantalla, y haga clic en **Agregar invitación**.
3. Haga clic en **Grupo**, en el menú **Destinatario**.

   Este paso permite elegir una o varias plataformas. Si tiene varias plataformas distintas de sistemas operativos en la empresa, elija todas las plataformas. Deseleccione una plataforma solo si sabe pertinentemente que no hay usuarios que utilicen esa plataforma.
4. Puede etiquetar dispositivos durante el proceso de invitación. Elija **Empresa** o **Empleado**.

   El etiquetado facilita la separación de dispositivos que sean propiedad de la empresa y dispositivos que sean propiedad de los empleados.
5. En la lista **Dominio**, elija el dominio donde existe el grupo.
6. En la lista **Grupo**, seleccione el grupo de Active Directory al que quiere enviar las invitaciones.
7. El **Modo de inscripción** permite establecer el tipo de seguridad de autenticación que prefiera para los usuarios.

- Nombre de usuario y contraseña
- High Security (Nivel alto de seguridad)
- URL de invitación
- URL de invitación y PIN
- URL de invitación y contraseña
- Dos factores
- Nombre de usuario + PIN

> **Nota:**
>
> Para enviar invitaciones de inscripción, solo puede utilizar los modos de seguridad de inscripción **URL de invitación**, **URL de invitación + PIN** o **URL de invitación + contraseña**. Para los dispositivos que se inscriben con **Nombre de usuario + contraseña**, **Dos factores** o **Nombre de usuario + PIN**, los usuarios deben introducir manualmente sus credenciales en Secure Hub.

8. Para las plantillas **Descarga de agente**, **URL de inscripción**, **PIN de inscripción** y **Confirmación de inscripción**, elija la plantilla de notificaciones personalizada que creó antes. O bien, elija el valor predeterminado que aparece en la lista.

   Si va a utilizar plantillas de notificaciones personalizadas, debe definir esas plantillas antes de configurar los modos de seguridad para la inscripción. Para obtener más información acerca de las plantillas de notificaciones, consulte Notificaciones.

   Para estas plantillas de notificaciones, use la configuración del servidor SMTP definida en XenMobile. Configure la información SMTP antes de continuar.

   > **Nota:**
   >
   > Las opciones **Caduca después de** y **Máximo de intentos** cambian en función de la opción de **Modo de inscripción** que elija. Esas opciones no se pueden cambiar.

9. Seleccione "Sí" en **Enviar invitación** y haga clic en **Guardar y enviar** para completar el proceso.

Admitir grupos anidados

Puede enviar invitaciones a grupos anidados. Por lo general, los grupos anidados se usan en entornos grandes, donde los grupos con permisos similares están vinculados entre sí.

Vaya a **Parámetros > LDAP** y, a continuación, habilite la opción **Admitir grupos anidados**.

Solución de problemas y limitaciones conocidas

Problema: Las invitaciones se envían a los usuarios, aunque estos se hayan eliminado de los grupos de Active Directory.

Solución: La propagación de los cambios depende del tamaño de su entorno de Active Directory. En un entorno grande, los cambios pueden tardar hasta seis horas en propagarse a todos los servidores. Si un usuario o grupo anidado se han eliminado recientemente, XenMobile aún puede considerar a esos usuarios como parte del grupo.

Por lo tanto, es mejor esperar un máximo de seis horas antes de enviar otra invitación al grupo.

Configurar un servidor Device Health Attestation local

January 4, 2022

Por Sanket Mishra

Puede habilitar Device Health Attestation (DHA) para dispositivos móviles con Windows 10 o Windows 11 a través de un servidor Windows local. Para habilitar DHA local, primero debe configurar un servidor DHA.

Después de configurar el servidor DHA, cree una directiva de XenMobile Server para habilitar el servicio DHA local. Para obtener información sobre cómo crear esta directiva, consulte Directiva de Device Health Attestation.

Requisitos previos para un servidor DHA

- Un servidor con Windows Server Technical Preview 5 o una versión posterior, instalado mediante la opción de instalación “Experiencia de escritorio”.
- Uno o varios dispositivos cliente con Windows 10 o Windows 11. Estos dispositivos deben tener TPM 1.2 o 2.0 con la versión más reciente de Windows.
- Los certificados:
  - **Certificado SSL de DHA.** Un certificado SSL x.509 encadenado a un certificado raíz empresarial de confianza con una clave privada exportable. Este certificado protege las comunicaciones de datos DHA en tránsito, incluidas las comunicaciones de servidor a servidor (servicio DHA y servidor MDM) y de servidor a cliente (servicio DHA y dispositivo Windows 10 o Windows 11).
  - **Certificado de firma de DHA.** Un certificado x.509 encadenado a un certificado raíz empresarial de confianza con una clave privada exportable. El servicio DHA usa este certificado para la firma digital.
  - **Certificado de cifrado de DHA.** Un certificado x.509 encadenado a un certificado raíz empresarial de confianza con una clave privada exportable. El servicio DHA también utiliza este certificado para el cifrado.
- Elija uno de estos modos de validación de certificados:

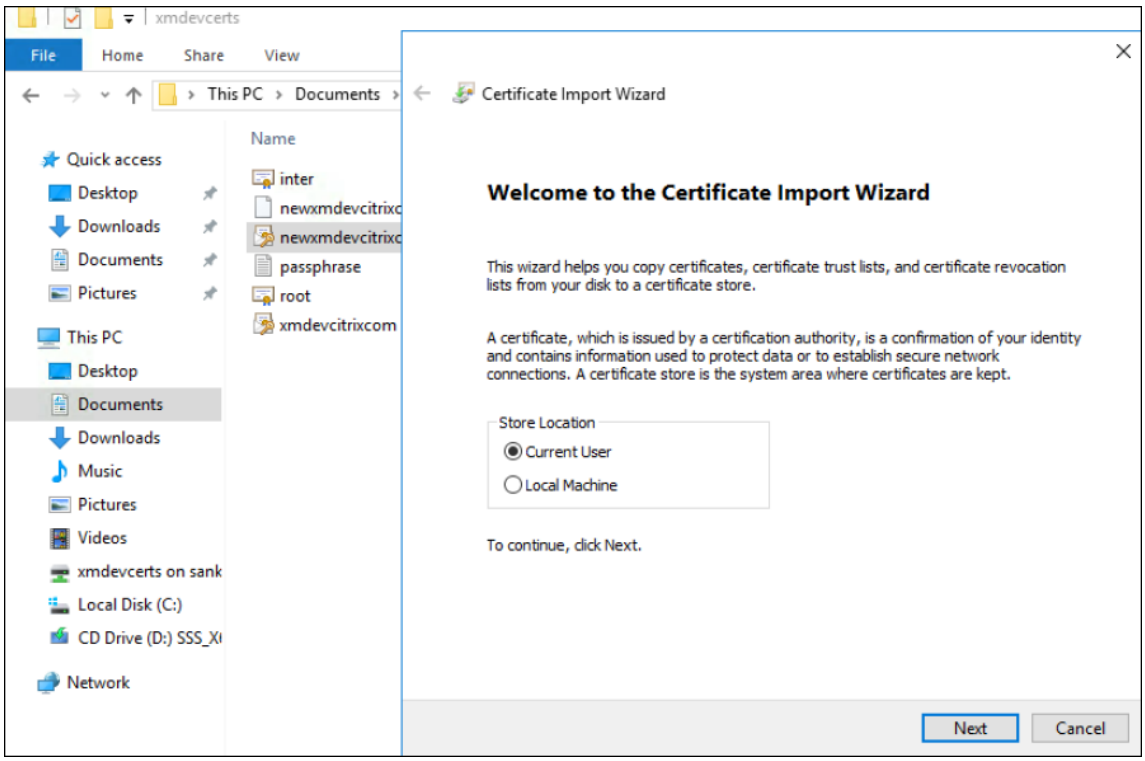
- **EKCert.** El modo de validación EKCert está optimizado para dispositivos en organizaciones que no están conectadas a Internet. Los dispositivos que se conectan a un servicio DHA que se ejecuta en modo de validación EKCert no tienen acceso directo a Internet.
- **AIKCert.** El modo de validación AIKCert está optimizado para entornos operativos que sí tienen acceso a Internet. Los dispositivos que se conectan a un servicio DHA que se ejecuta en modo de validación AIKCert deben tener acceso directo a Internet y pueden obtener un certificado AIK de Microsoft.

Agregar el rol del servidor DHA al servidor Windows

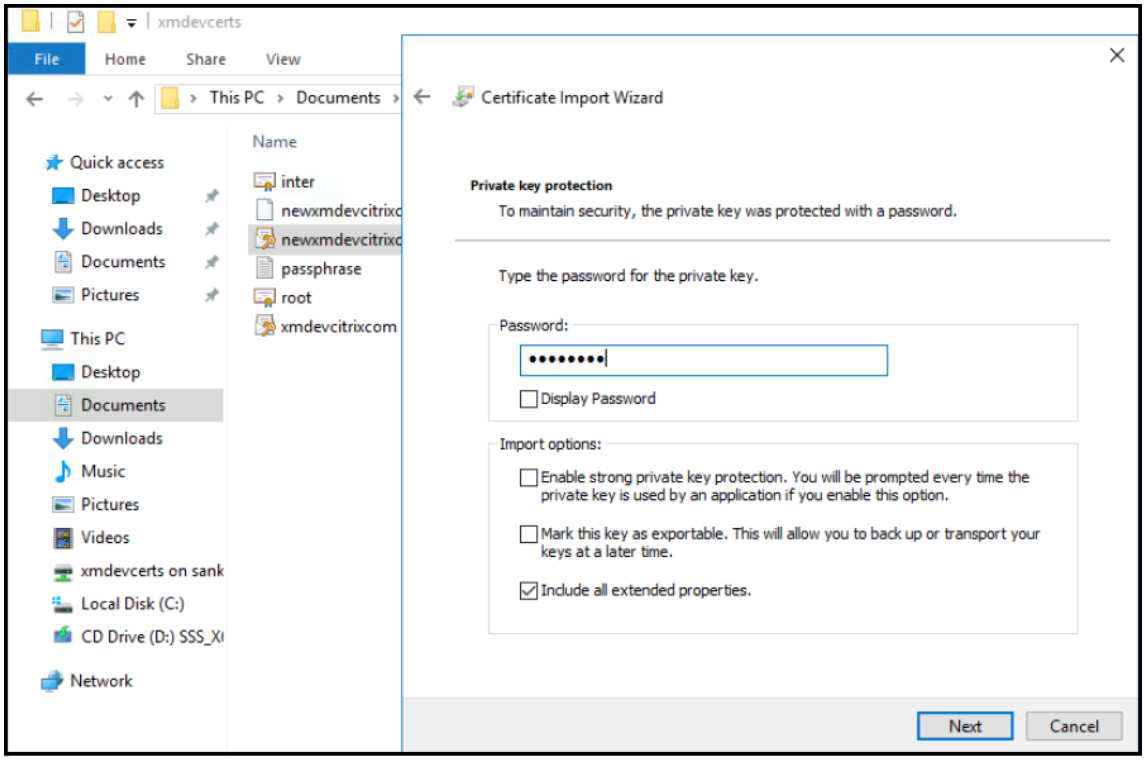
1. En el servidor Windows, si el Administrador de servidores aún no está abierto, haga clic en **Inicio** y luego en **Administrador de servidores**.
2. Haga clic en **Agregar roles y características**.
3. En la página **Antes de empezar**, haga clic en **Siguiente**.
4. En la página **Seleccionar tipo de instalación**, haga clic en **Instalación basada en características o en roles**, y luego haga clic en **Siguiente**.
5. En la página **Seleccionar servidor de destino**, marque **Seleccionar un servidor del grupo de servidores**, seleccione el servidor y luego haga clic en **Siguiente**.
6. En la página **Seleccionar roles de servidor**, marque la casilla “Atestación de estado de dispositivo”.
7. Opcional: Haga clic en **Agregar características** para instalar otros servicios y funciones que requiera el rol.
8. Haga clic en **Siguiente**.
9. En la página **Seleccionar características**, haga clic en **Siguiente**.
10. En la página **Rol de servidor web (IIS)**, haga clic en **Siguiente**.
11. En la página **Seleccionar servicios de rol**, haga clic en **Siguiente**.
12. En la página **Servicio de atestación de mantenimiento del dispositivo**, haga clic en **Siguiente**.
13. En la página **Confirmar selecciones de instalación**, haga clic en **Instalar**.
14. Cuando termine la instalación, haga clic en **Cerrar**.

Agregar el certificado SSL al almacén de certificados del servidor

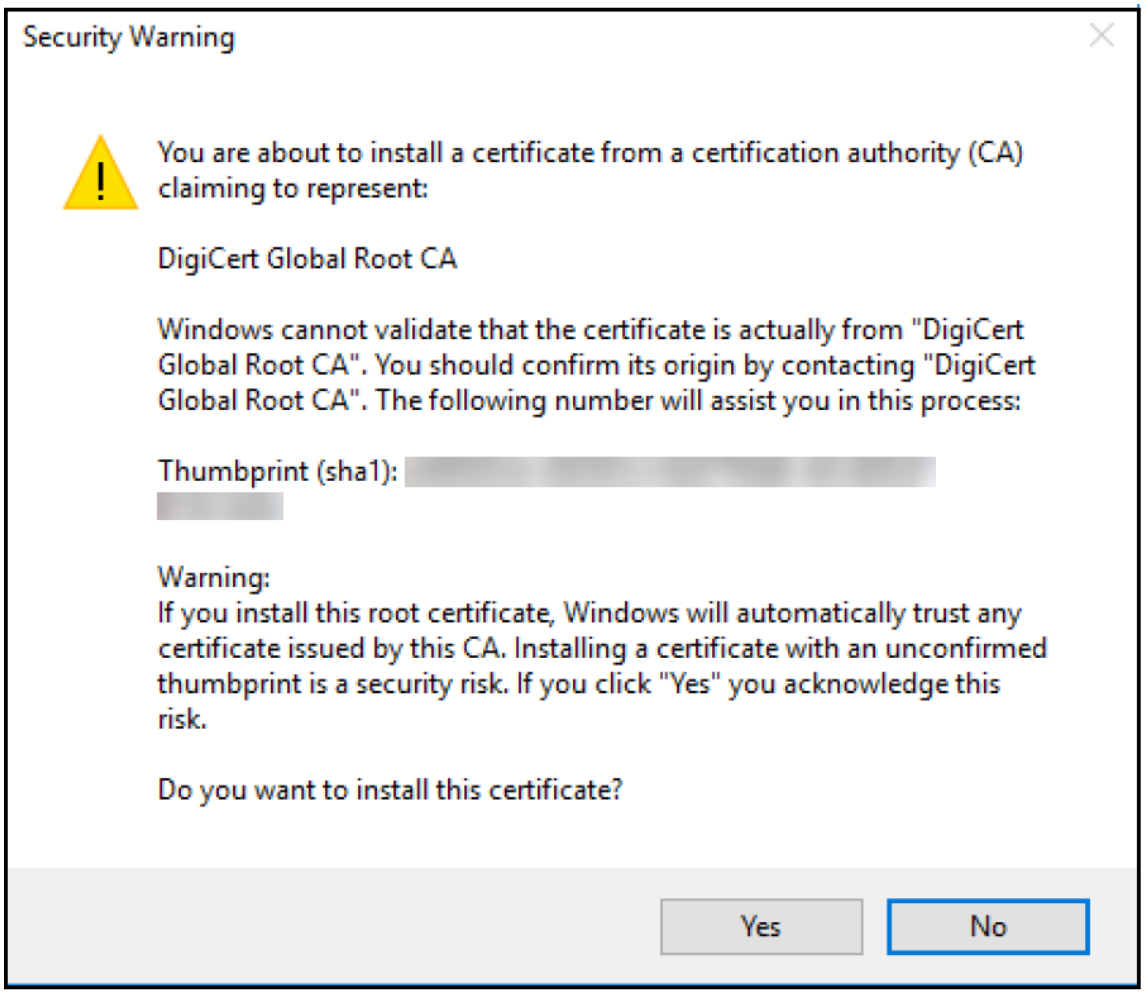
1. Vaya al archivo del certificado SSL y selecciónelo.
2. Seleccione **Usuario actual** como la ubicación del almacén y haga clic en **Siguiente**.



3. Escriba la contraseña de la clave privada.
4. Compruebe que la opción de importación **Incluir todas las propiedades extendidas** está seleccionada. Haga clic en **Siguiente**.



5. Cuando aparezca esta ventana, haga clic en **Sí**.



6. Confirme que el certificado está instalado:

   a) Abra la ventana del símbolo del sistema.

   b) Escriba **mmc** y presione la tecla ENTRAR. Para ver los certificados ubicados en el almacén de la máquina local, debe tener el rol Administrador.

   c) En el menú “Archivo”, haga clic en **Agregar o quitar complemento**.

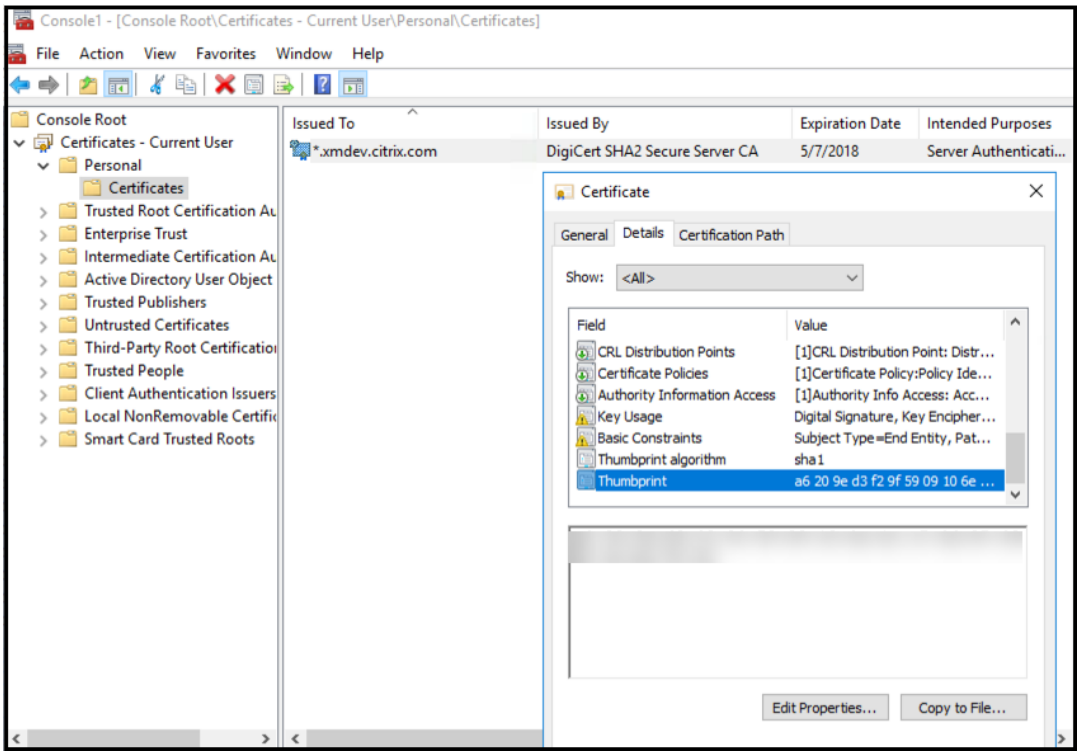
   d) Haga clic en **Agregar**.

   e) En el cuadro de diálogo “Agregar un complemento independiente”, seleccione **Certificados**.

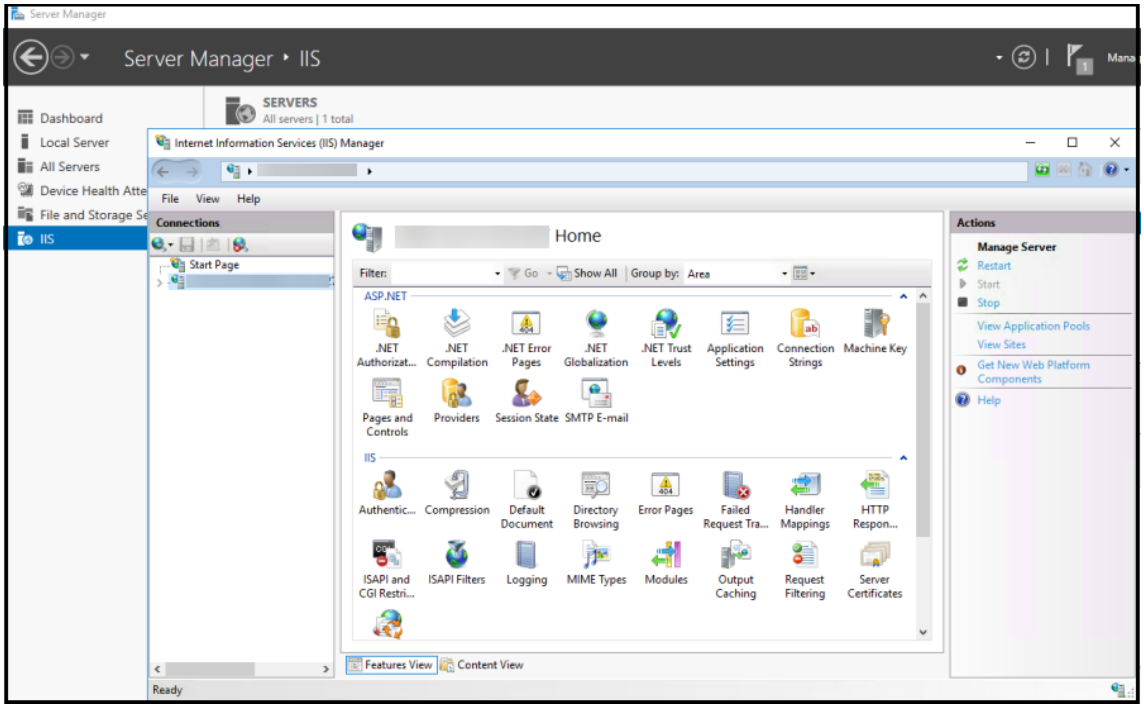
   f) Haga clic en **Agregar**.

   g) En el cuadro de diálogo del complemento “Certificados”, seleccione **Mi cuenta de usuario**. (Si ha iniciado sesión como titular de la cuenta de servicio, seleccione **Cuenta de servicio**.)

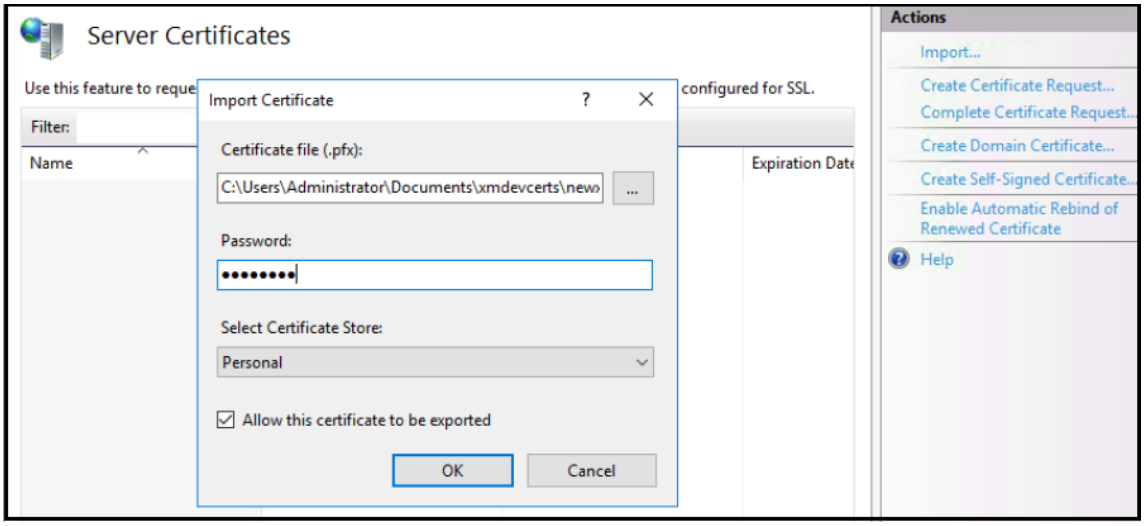
   h) En el cuadro de diálogo “Seleccionar equipo”, haga clic en **Finalizar**.



7. Vaya a **Administrador de servidores > IIS** y seleccione **Certificados de servidor** entre los iconos de la lista.

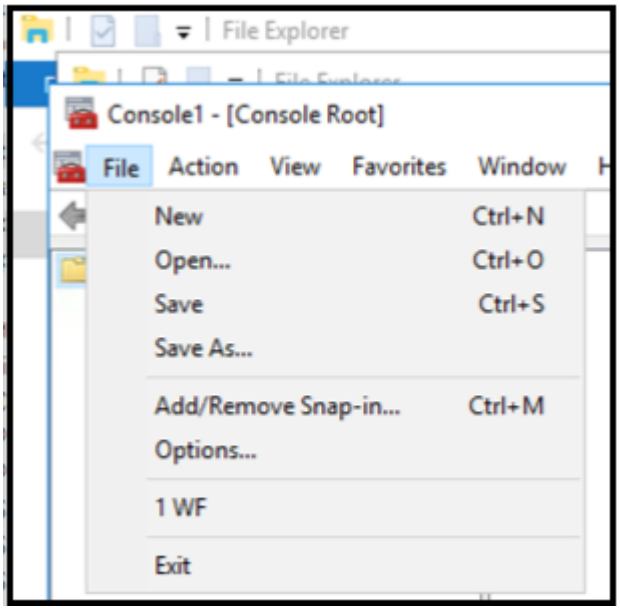


8. En el menú “Acción”, seleccione **Importar...** para importar el certificado SSL.

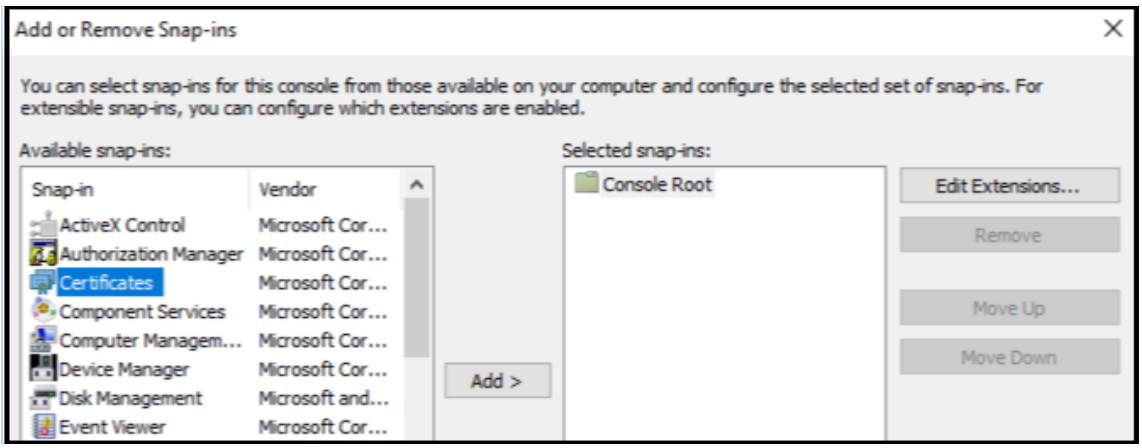


Recuperar y guardar la huella digital del certificado

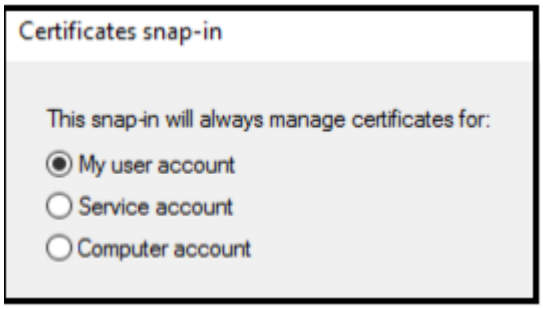
1. En la barra de búsqueda del Explorador de archivos, escriba **mmc**.
2. En la ventana “Raíz de consola”, haga clic en **Archivo > Agregar o quitar complemento**.



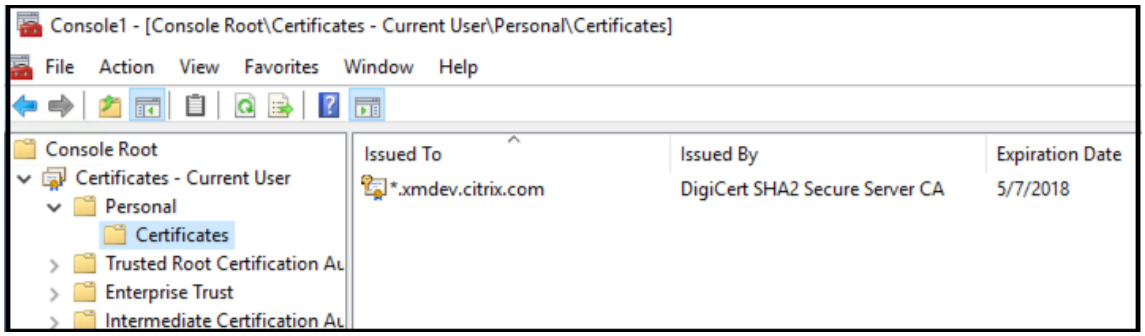
3. Seleccione el certificado del complemento disponible y agréguelo a los complementos seleccionados.



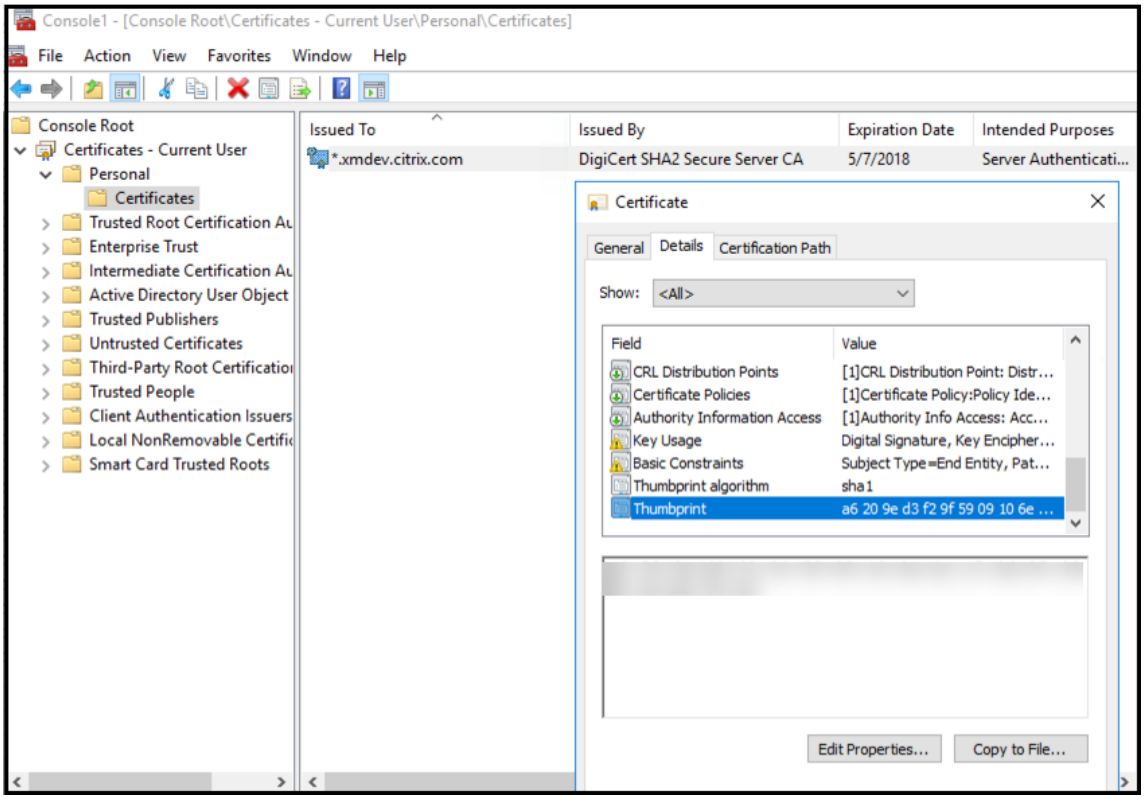
4. Seleccione **Mi cuenta de usuario**.



5. Seleccione el certificado y haga clic en **Aceptar**.



6. Haga doble clic en el certificado y en la ficha **Detalles**. Desplácese hacia abajo para ver la huella digital del certificado.



7. Copie la huella digital a un archivo. Elimine los espacios cuando use la huella digital en los comandos de PowerShell.

Instalar los certificados de firma y cifrado

Ejecute estos comandos de PowerShell en el servidor Windows para instalar los certificados de firma y cifrado.

Reemplace el marcador de posición ReplaceWithThumbprint y escríbalo entre comillas dobles, como se muestra a continuación.

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
 $_.Thumbprint -like "ReplaceWithThumbprint" }


$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys" +
   $keyname icacls $keypath /grant IIS_IUSRS`:R
<!--NeedCopy-->
```


Extraer el certificado raíz de TPM e instalar el paquete de certificado de confianza

Ejecute estos comandos en el servidor Windows:

```
mkdir .\TrustedTpm

expand -F:* .\TrustedTpm.cab .\TrustedTpm

cd .\TrustedTpm

.\setup.cmd
<!--NeedCopy-->
```

Configurar el servicio DHA

Ejecute este comando en el servidor Windows para configurar el servicio DHA.

Reemplace el marcador de posición ReplaceWithThumbprint.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
    ReplaceWithThumbprint

-SigningCertificateThumbprint ReplaceWithThumbprint

-SslCertificateStoreName My -SslCertificateThumbprint
    ReplaceWithThumbprint

-SupportedAuthenticationSchema "AikCertificate"
<!--NeedCopy-->
```

Ejecute estos comandos en el servidor Windows para configurar la directiva de cadena de certificados para el servicio DHA:

```
$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
<!--NeedCopy-->
```

Responda a estas indicaciones de la siguiente manera:

```
  Confirm

    Are you sure you want to perform this action?
```



```
4
5       Performing the operation "Install-DeviceHealthAttestation" on
            target "WIN-N27D1FKCEBT".
6
7       [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?]
            Help (default is "Y"): A
8
9       Adding SSL binding to website 'Default Web Site'.
10
11      Add SSL binding?
12
13      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
14
15      Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17      Add application pool?
18
19      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
20
21      Adding web application 'DeviceHealthAttestation' to website '
            Default Web Site'.
22
23      Add web application?
24
25      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
26
27      Adding firewall rule 'Device Health Attestation Service' to allow
            inbound connections on port(s) '443'.
28
29      Add firewall rule?
30
31      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
32
33      Setting initial configuration for Device Health Attestation Service
            .
34
35      Set initial configuration?
36
37      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
38
39      Registering User Access Logging.
40
41      Register User Access Logging?
42
43      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```



```
<!--NeedCopy-->
```

Consultar la configuración

Para comprobar si DHASActiveSigningCertificate está activo, ejecute este comando en el servidor:

```
Get-DHASActiveSigningCertificate
```

Si el certificado está activo, aparece el tipo de certificado (de firma) y la huella digital.

Para comprobar si DHASActiveSigningCertificate está activo, ejecute estos comandos en el servidor.

Reemplace el marcador de posición ReplaceWithThumbprint y escríbalo entre comillas dobles, como se muestra a continuación.

```
Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
    -Force

Get-DHASActiveEncryptionCertificate
<!--NeedCopy-->
```

Si el certificado está activo, se muestra la huella digital.

Para realizar una comprobación final, vaya a la dirección URL:

```
https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate
/v1
```

Si el servicio DHA se está ejecutando, se muestra “Método no permitido”.

Configurar la autenticación por certificado en EWS para notificaciones push de Secure Mail

January 4, 2022

Por Vijay Kumar Kunchakuri

Para comprobar que las notificaciones push de Secure Mail funcionan, es necesario configurar el servidor Exchange Server para la autenticación basada en certificados. Este requisito es especialmente necesario cuando Secure Hub se inscribe en XenMobile con la autenticación basada en certificados.

Debe configurar Active Sync y el directorio virtual de Servicios web de Exchange (EWS) en el servidor de correo de Exchange con la autenticación basada en certificados.

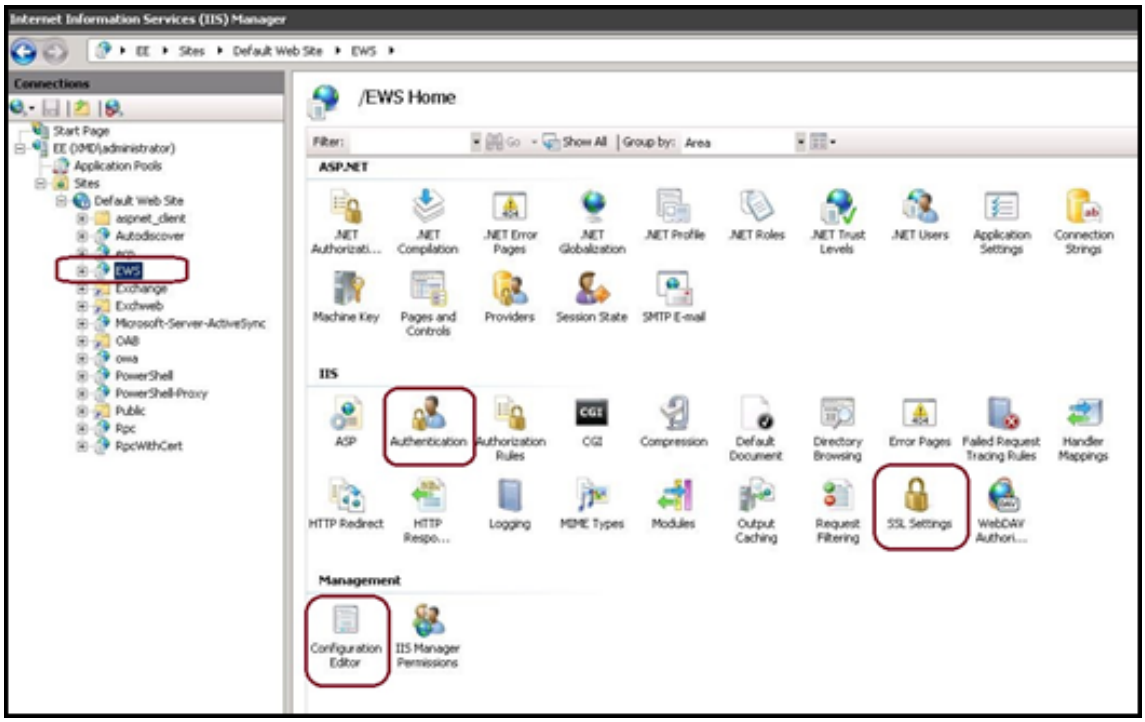
A menos que complete estas configuraciones, la suscripción a las notificaciones push de Secure Mail falla y las insignias de Secure Mail no se actualizan.

En este artículo se describen los pasos para configurar la autenticación basada en certificados. Las configuraciones son específicas para el directorio virtual EWS en Exchange Server.

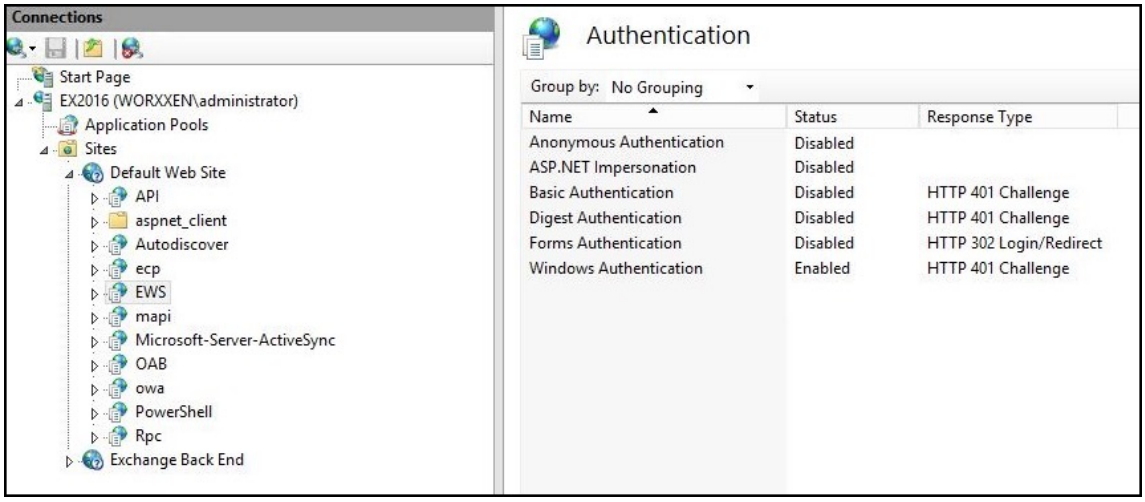
Para comenzar con la configuración, lleve a cabo lo siguiente:

1. Inicie sesión en el servidor o los servidores donde está instalado el directorio virtual de EWS.
2. Abra la consola del Administrador IIS.
3. En **Sitio web predeterminado**, haga clic en el directorio virtual de EWS.

   Los complementos de la autenticación, el editor de configuración y SSL están en el lado derecho de la consola del Administrador de IIS.



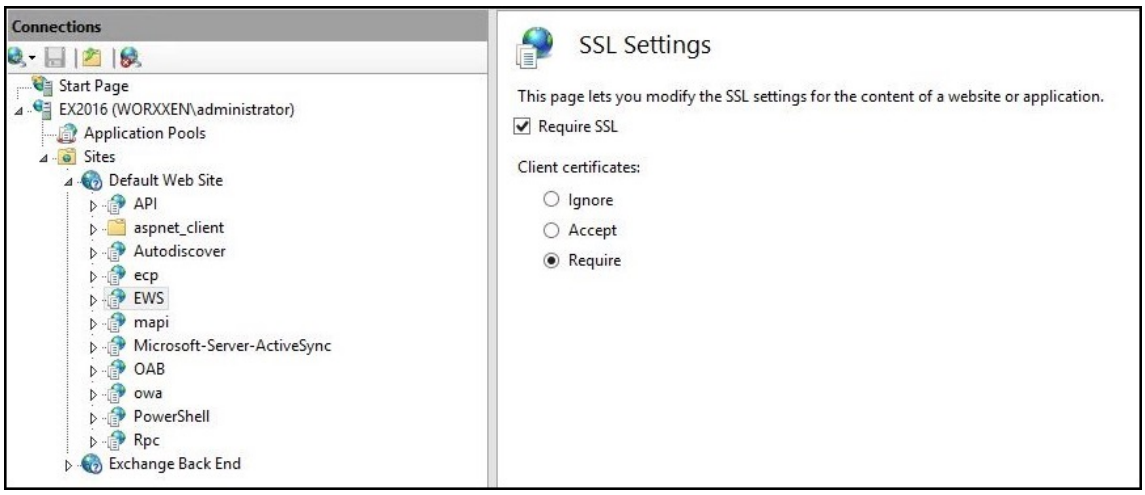
4. Compruebe que las configuraciones de **Autenticación de EWS** están configurados como se muestra en la siguiente imagen.



5. Defina la **Configuración de SSL** para el directorio virtual de EWS.

   a) Marque la casilla **Requerir SSL**.

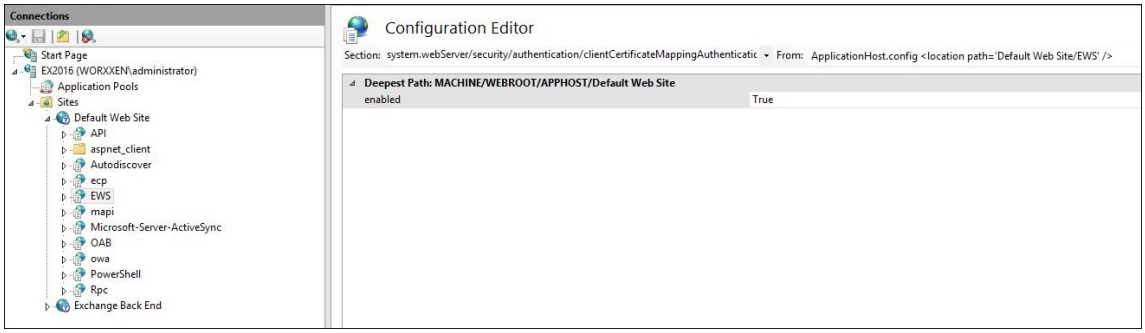
   b) En **Certificados de cliente**, haga clic en **Obligatorio**. Puede establecer esta opción en **Aceptar** si otros clientes de correo EWS se conectan con el nombre de usuario y la contraseña como credenciales para autenticarse y conectarse al servidor Exchange.



6. Haga clic en **Editor de configuración** y, en la lista desplegable **Sección**, vaya a la sección siguiente:

   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. Defina **Habilitado** con el valor **True**.

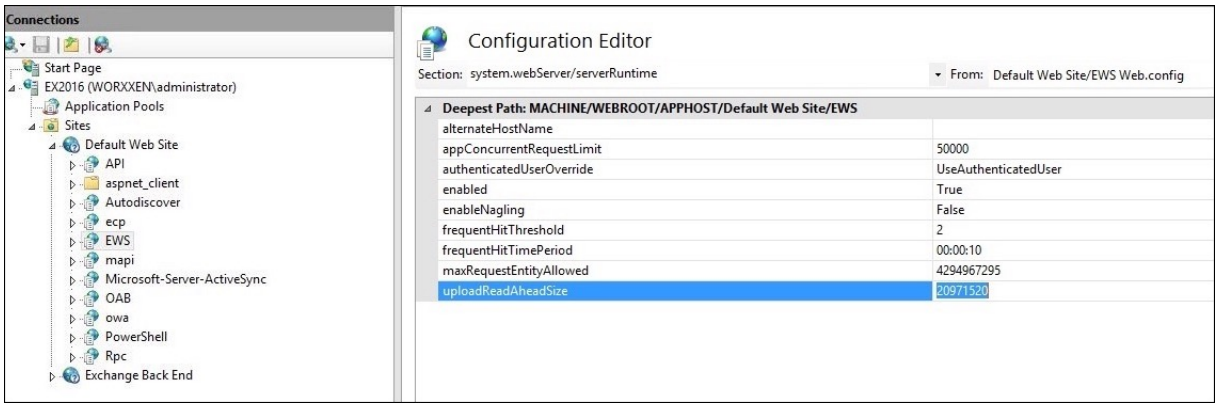


8. Haga clic en **Editor de configuración** y, en la lista desplegable **Sección**, vaya a la sección siguiente:
    - **system.webServer/serverRuntime**
9. Establezca el valor de **uploadReadAheadSize** en **10485760** (10 MB) o **20971520** (20 MB) o en el valor correspondiente que requiera su organización.

    > **Importante:**
    >
    > Si no establece este valor correctamente, la autenticación por certificado puede fallar con el código de error 413 durante la suscripción a las notificaciones push de EWS.
    >
    > No establezca este valor en **0**.

Para obtener más información, consulte los siguientes recursos de terceros:

- Tiempo de ejecución del servidor de Microsoft IIS
- Blog de administración de clientes Butsch



Para obtener más información acerca de la solución de problemas de Secure Mail con las notificaciones push de iOS, consulte este artículo de Citrix Support Knowledge Center.

Información relacionada

Notificaciones push en Secure Mail para iOS

Integrar la administración de dispositivos móviles (MDM) de XenMobile en Cisco Identity Services Engine (ISE)

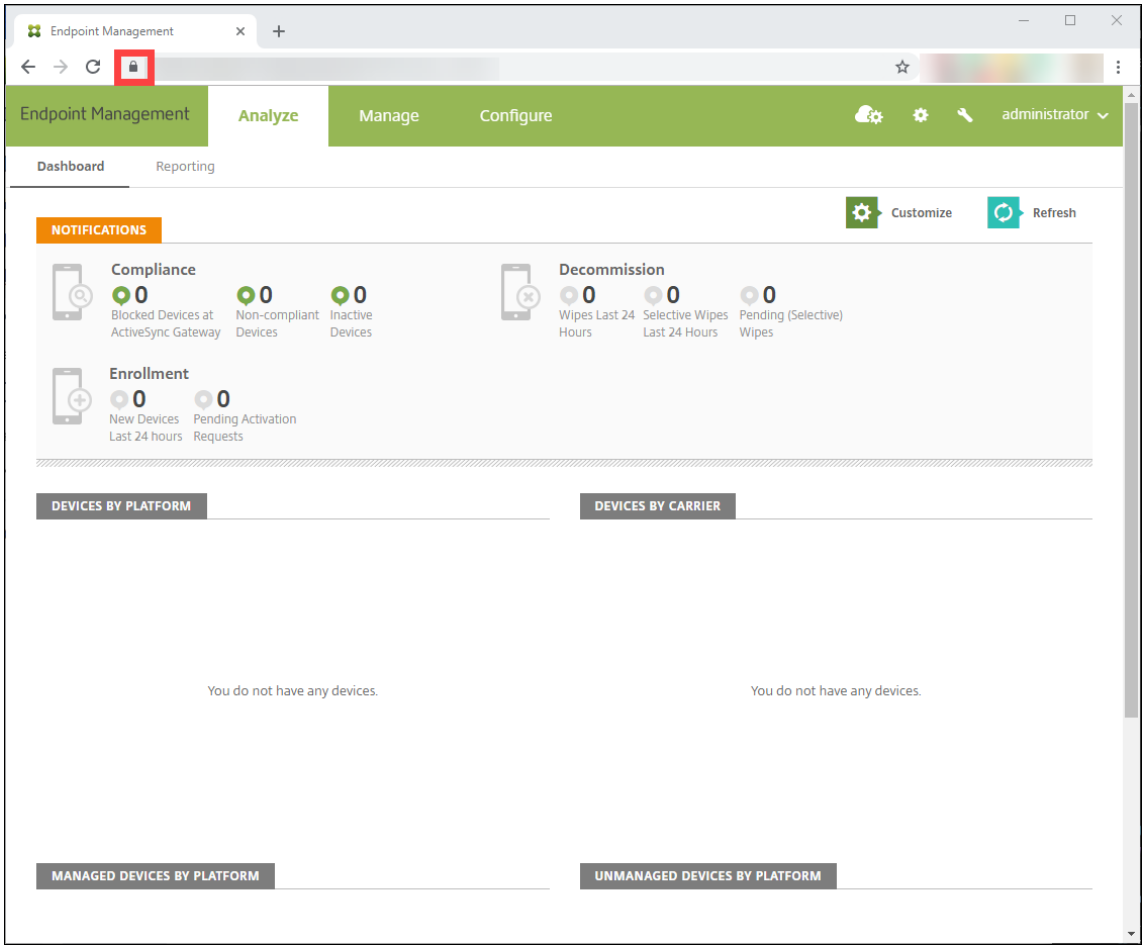
January 4, 2022

Por John Bartel III

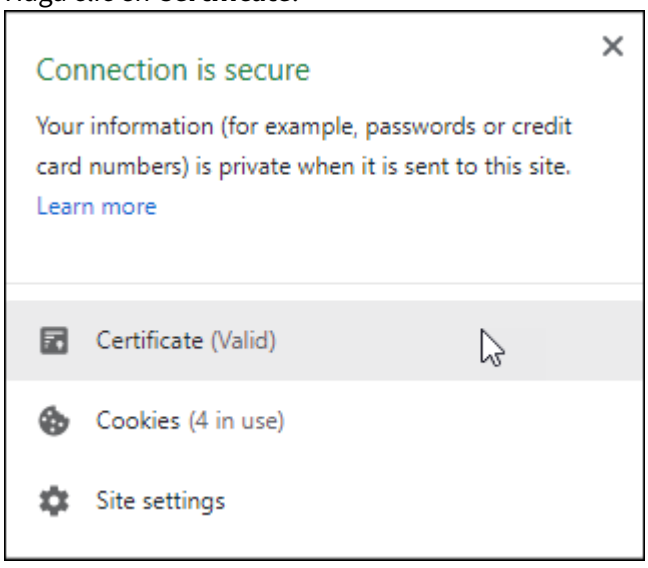
Cisco ISE se utiliza para implementar, proteger, supervisar, integrar y administrar dispositivos móviles en el lugar de trabajo. El software descargado en el dispositivo móvil controla la distribución de aplicaciones y parches, y controla los datos y la configuración en el dispositivo de punto final. XenMobile se puede integrar en Cisco ISE para administrar dispositivos no conformes y no administrados en la consola de Cisco ISE. XenMobile también le permite permitir, denegar o poner en cuarentena de manera selectiva el acceso a los servicios corporativos.

Para configurar la integración en XenMobile, cree una cuenta de servicio local en XenMobile Server con el rol de administrador RBAC asignado. Este rol permite a Cisco ISE acceder a la API de XenMobile. ISE debe confiar en el certificado de XenMobile. Para descargar este certificado, abra un explorador web, vaya a la URL de su servidor e inicie sesión.

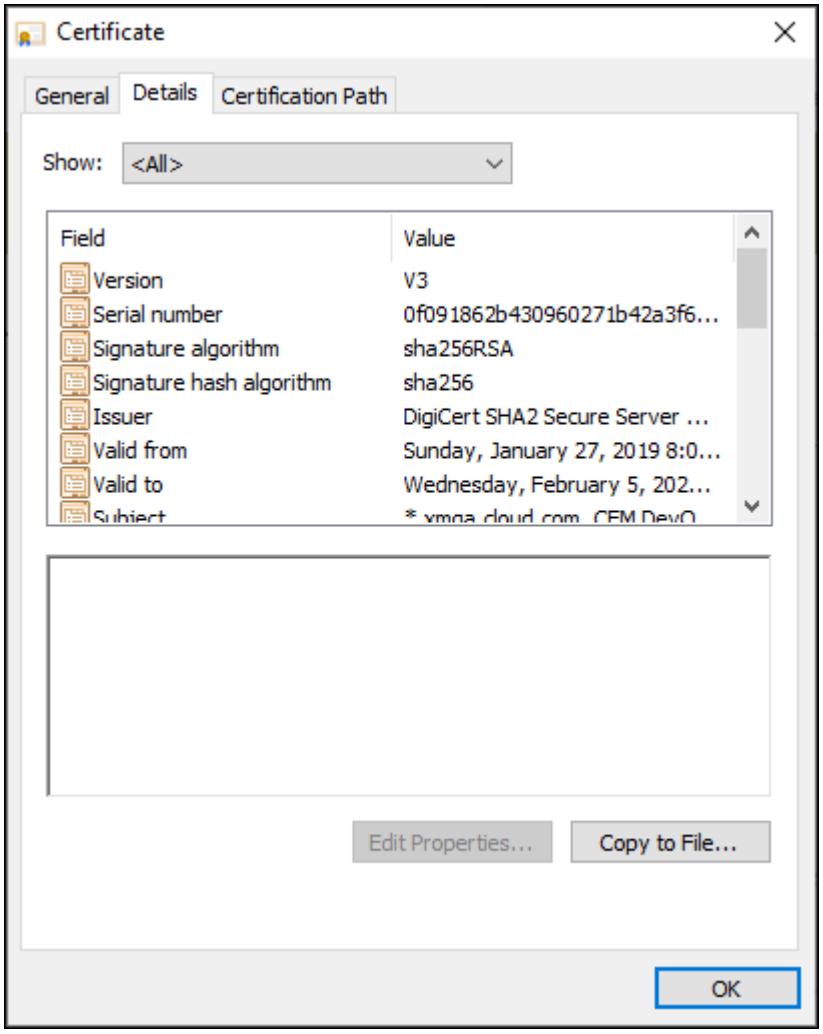
1. Una vez que haya iniciado sesión, haga clic en el candado situado junto a la URL, en la barra de direcciones.



2. Haga clic en **Certificate**.



3. Seleccione la ficha **Details** y haga clic en **Copy to File**.



4. Siga las instrucciones del asistente para guardar el certificado de manera local.
5. Inicie sesión en la consola de Cisco ISE e importe el certificado de XenMobile que descargó antes. Importe el certificado en el almacén de certificados de confianza de Cisco ISE. Esta importación es necesaria para que Cisco ISE confíe en la comunicación con XenMobile Server.
    a) Vaya a **Administration > System > Certificates > Certificate Management > Trusted Certificates**. Haga clic en **Importar**.
    b) Asigne un nombre al certificado y marque las casillas **Trust for authentication within ISE** y **Trust for authentication of Cisco Services**.
6. Agregue XenMobile como MDM externo dentro de Cisco ISE.
    a) Vaya a **Administration > Network Resource > External MDM**. Haga clic en **Add** y rellene lo siguiente:
        - **Server Host:** Su FQDN de XenMobile.
        - **Port:** 443.
        - **Instance name:** El nombre de la instancia de XenMobile Server. El nombre de la instancia es “zdm” de forma predeterminada en la mayoría de las implementaciones.

- **User Name:** Escriba el nombre del usuario que creó para esta tarea. El usuario debe ser una cuenta de administrador local en el grupo de administradores RBAC original.
- **Password:** La contraseña del usuario que acaba de agregar.
- Compruebe allí donde dice **Enable**.

7. Si la prueba se realiza correctamente, haga clic en **Submit**.

Para obtener más información sobre Cisco ISE, consulte la documentación de Cisco.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States