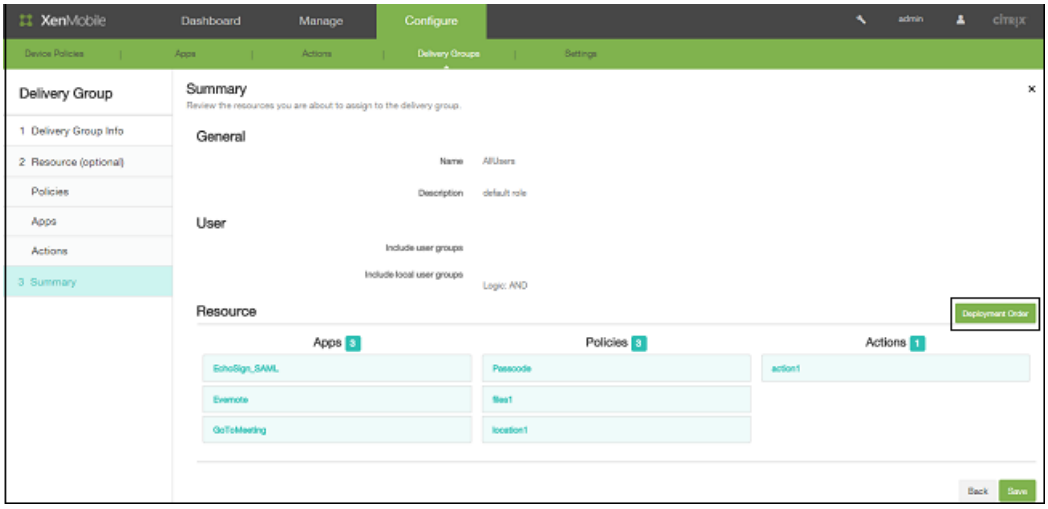
Info zu XenMobile Server 10.1

> Hinweis

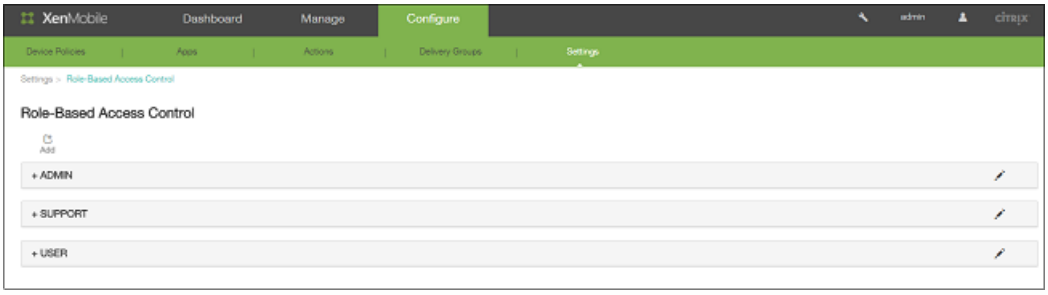
Neue Features und Verbesserungen für iOS und Android



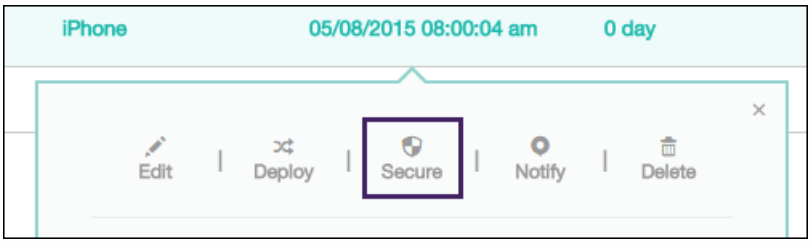
-
-

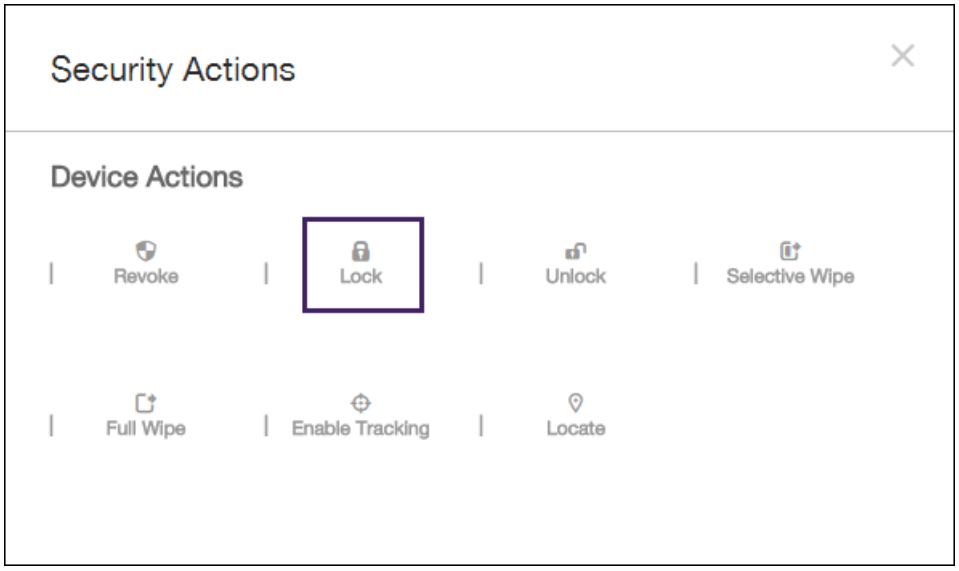
-
-
-
-
-

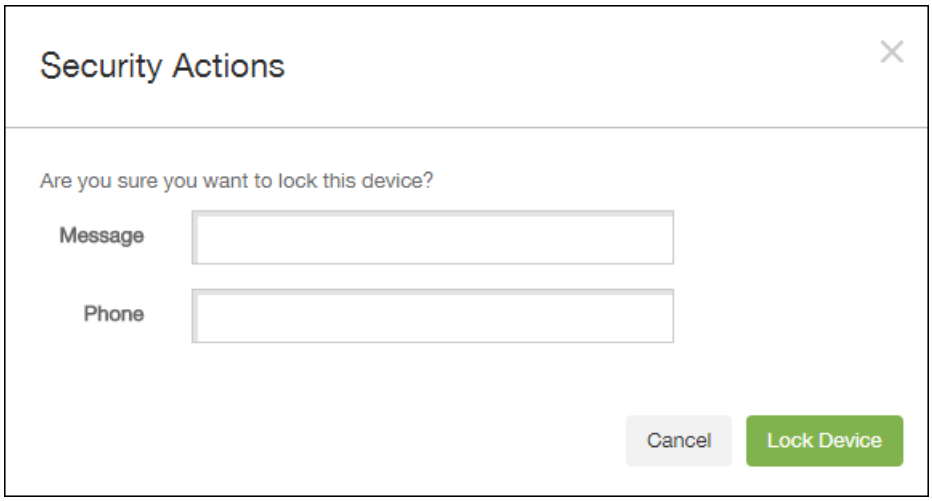
-
-



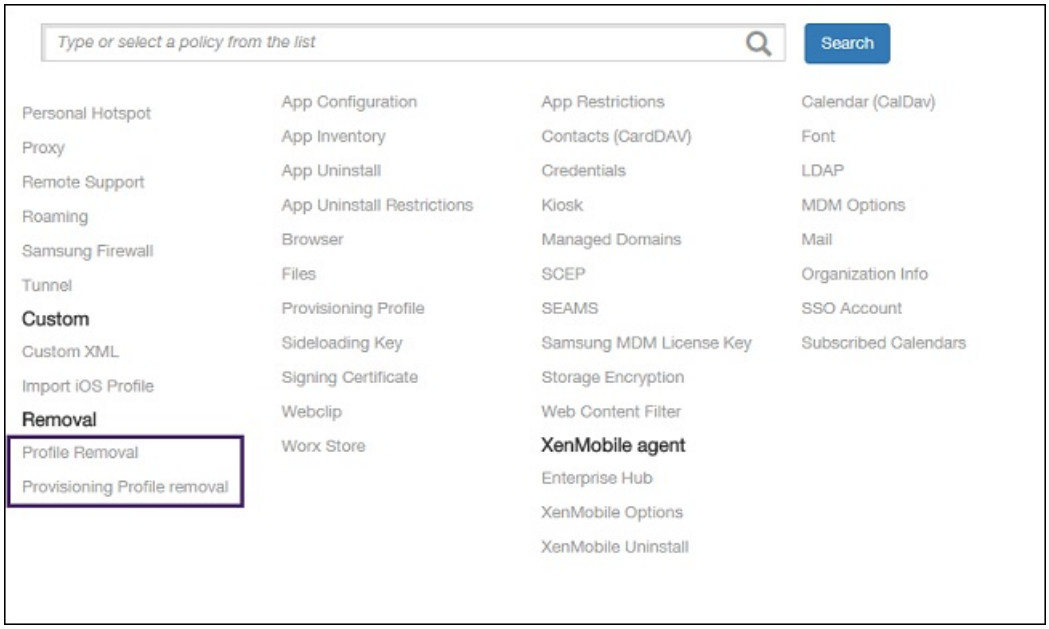
Neue Features und Verbesserungen für iOS



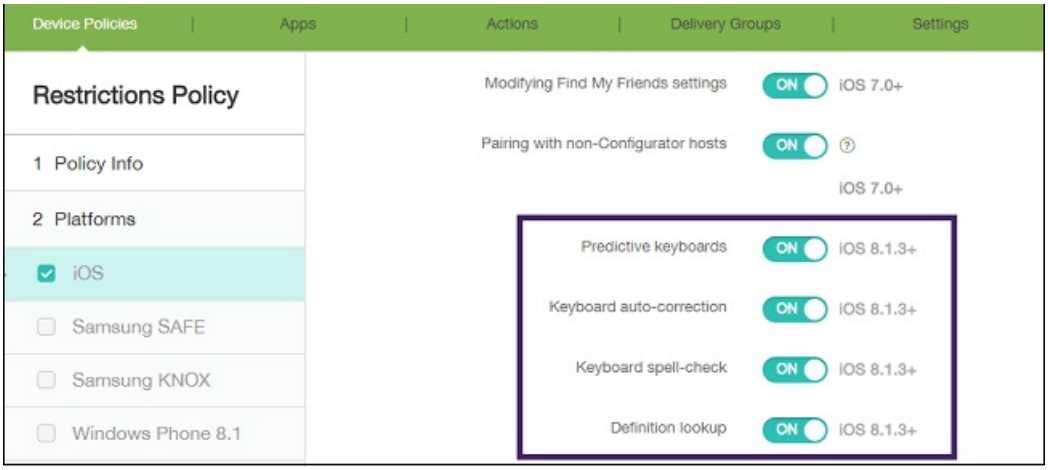


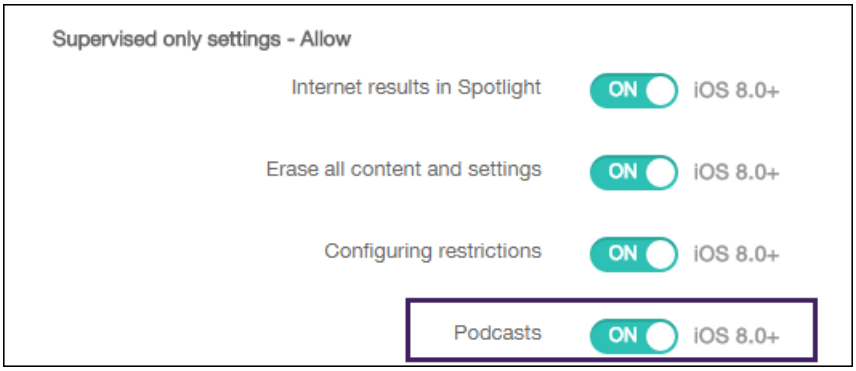


-
-
-



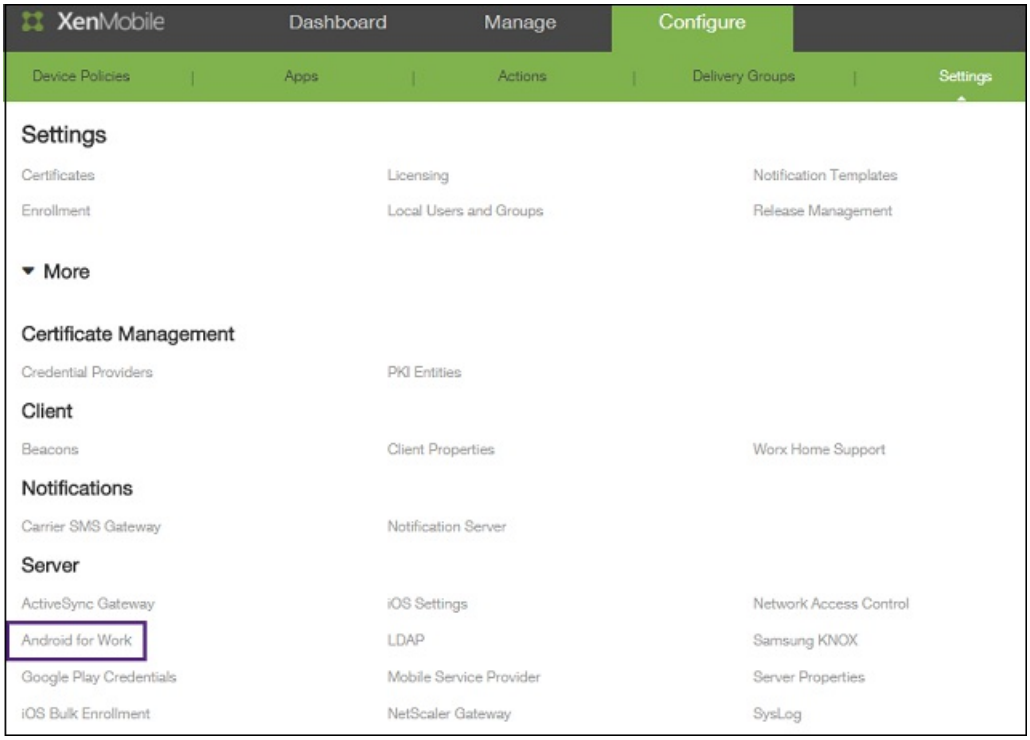
-
-
-
-

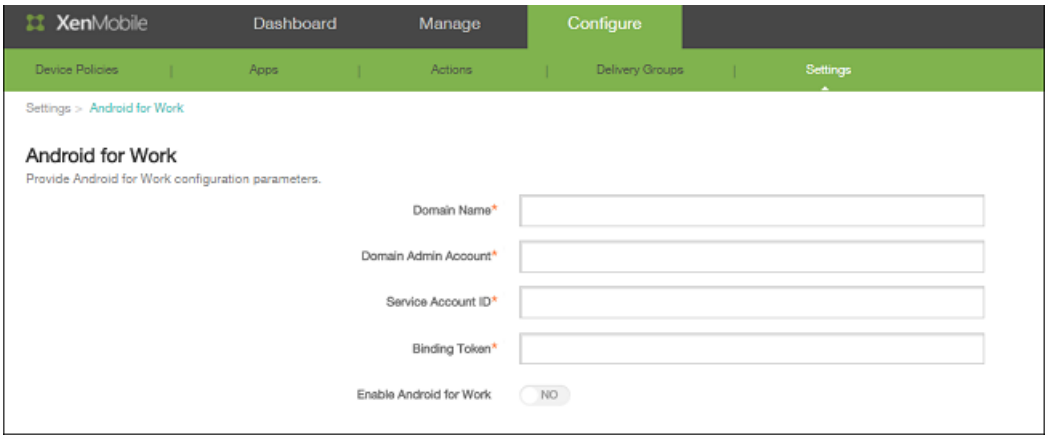


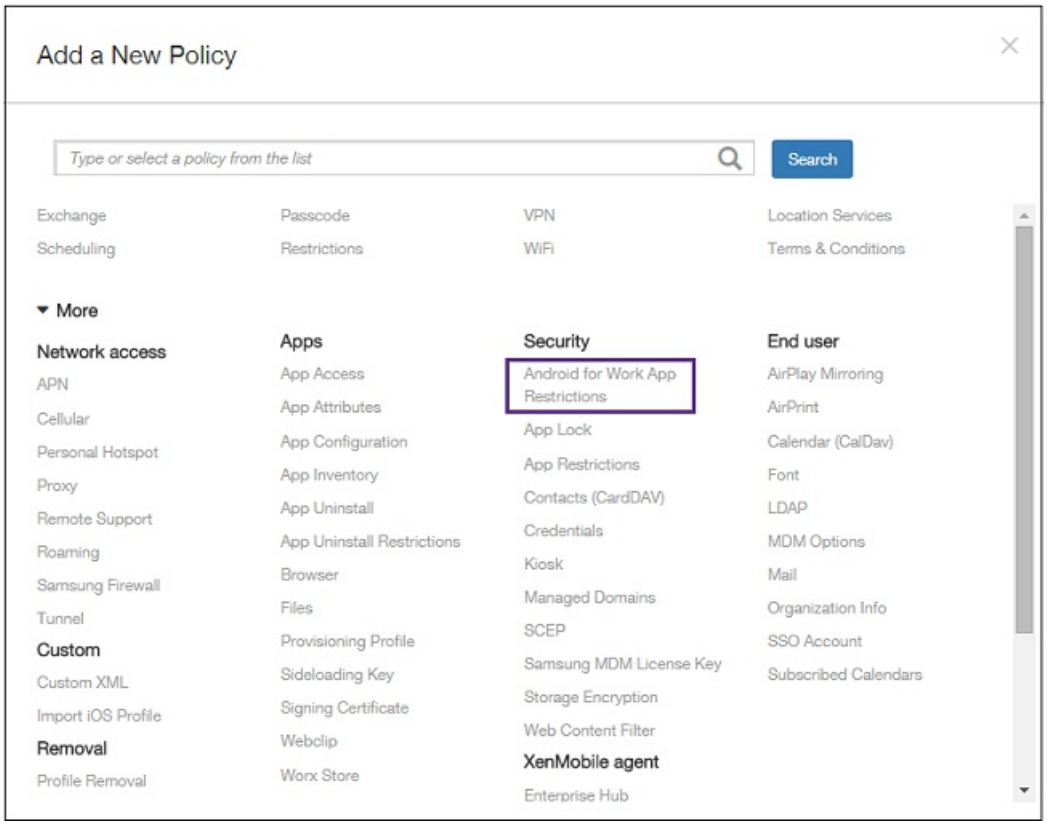
- 

Neue Features und Verbesserungen für Android

> Hinweis







Behobene Probleme bei XenMobile Server 10.1

-
-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-
-
-
-

-
-
-
-
-

Bekannte Probleme bei XenMobile Server 10.1

-
-
-
-
-
-
-
-
-
-
-
  -
  -
  -

-
-
-
-
-
-
-
-
-
-

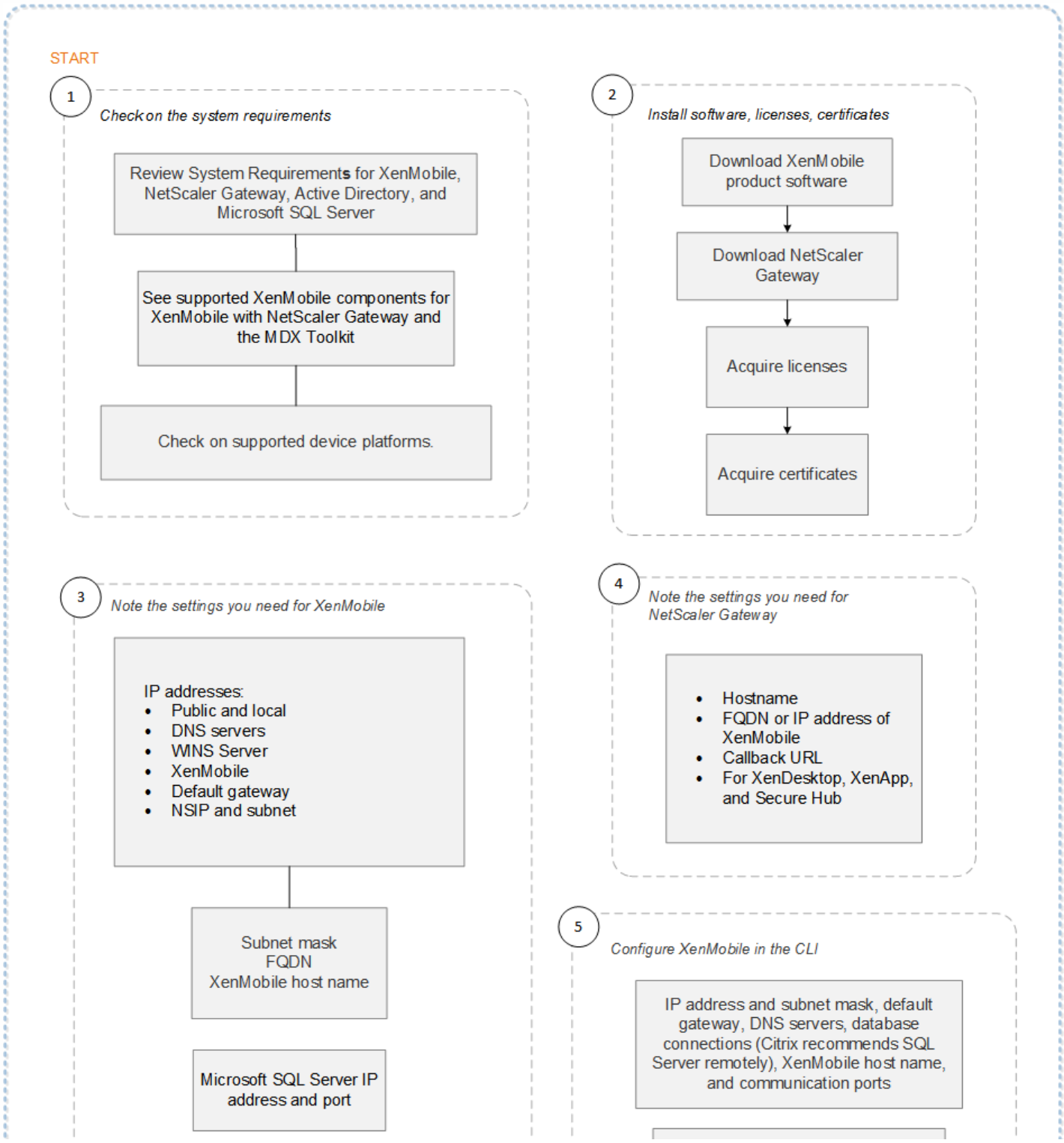
-
-
-
-
-

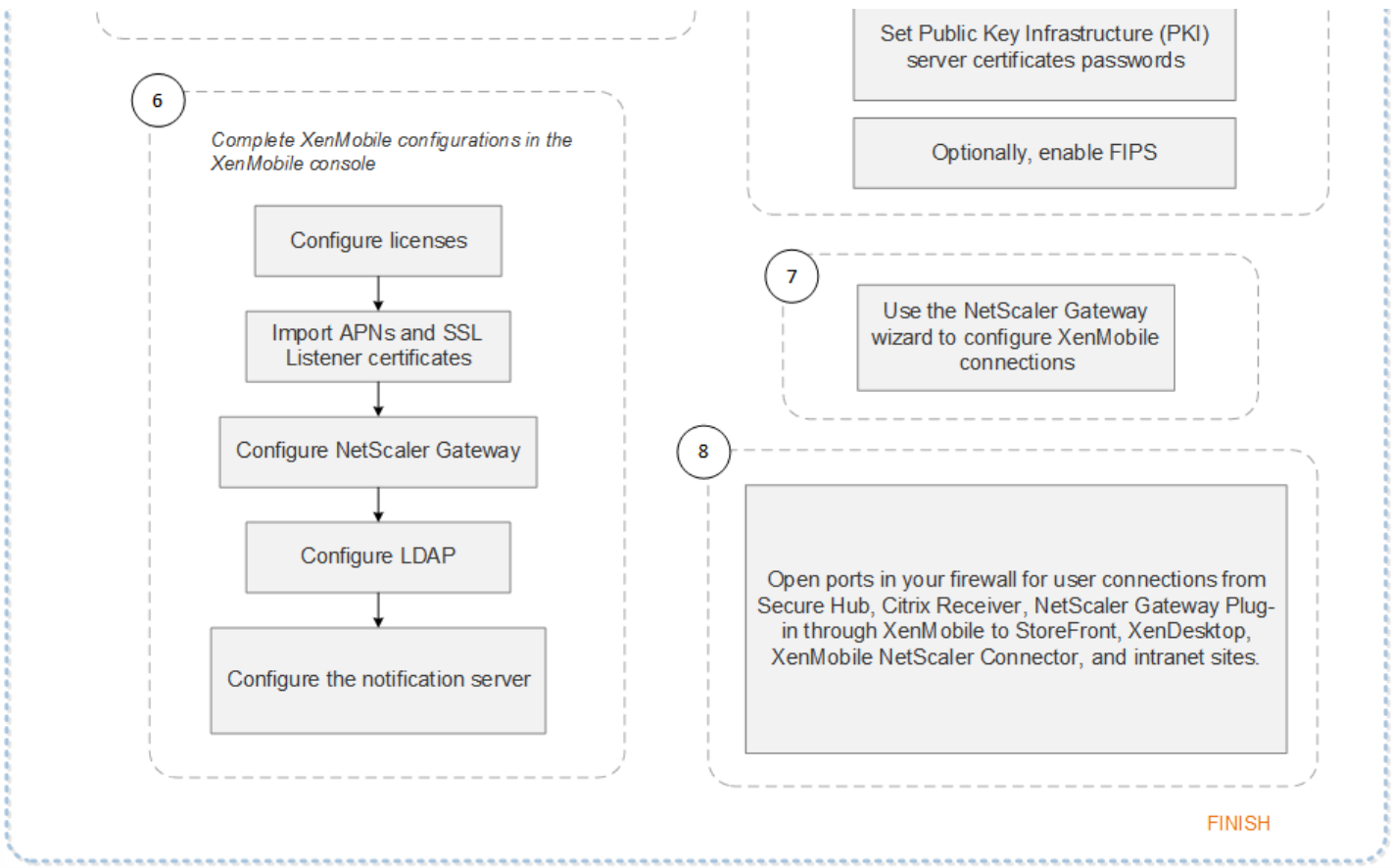
Architektur im Überblick

-
-
-
-
-
-
-
-
-

-
-

Flussdiagramm der Bereitstellung von XenMobile mit NetScaler Gateway





1

-
-
-

2

-
-
-

3

-

4

-

5

-

6

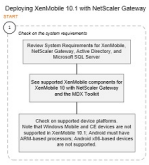
-

7

-

8

-



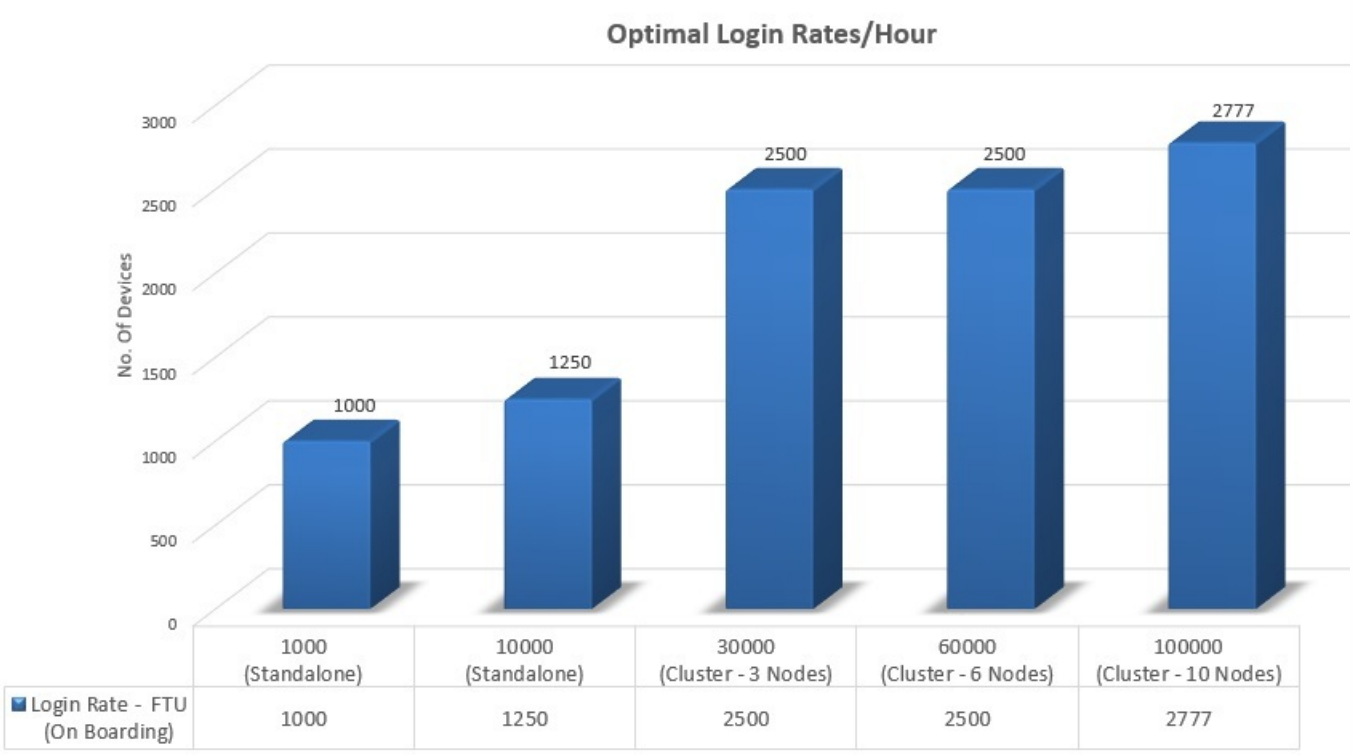
Skalierung von XenMobile

Richtlinien für Leistung und Skalierbarkeit

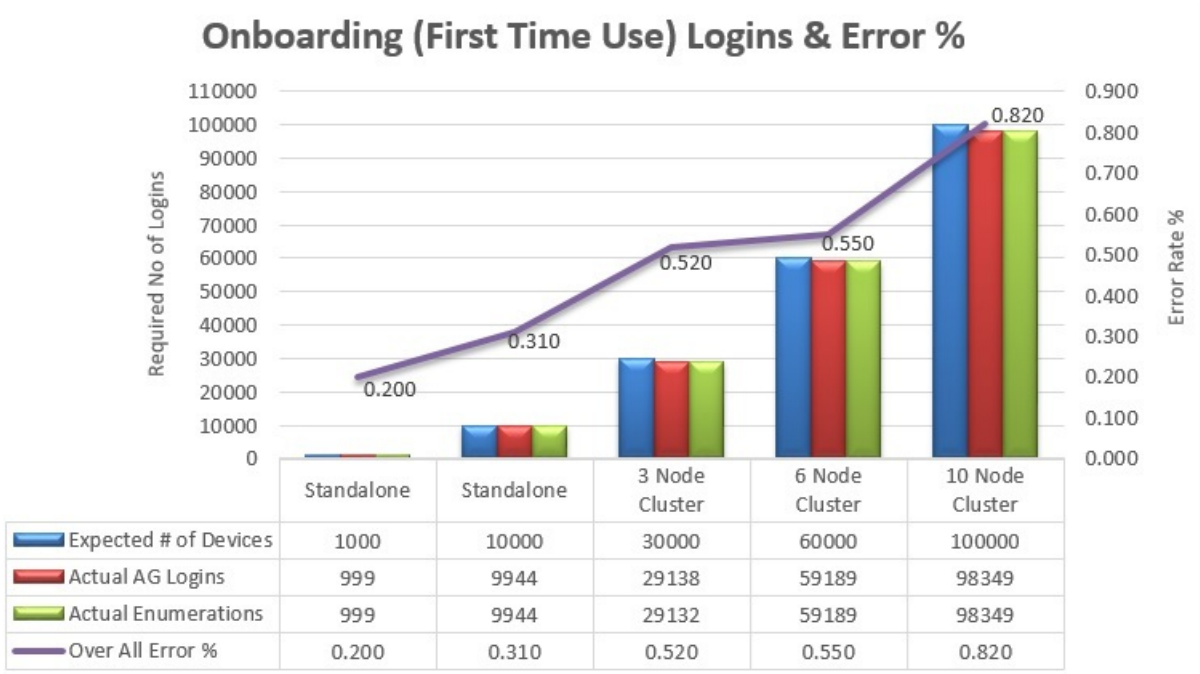
-
-
  -
  -

Systemkonfiguration und Testergebnisse

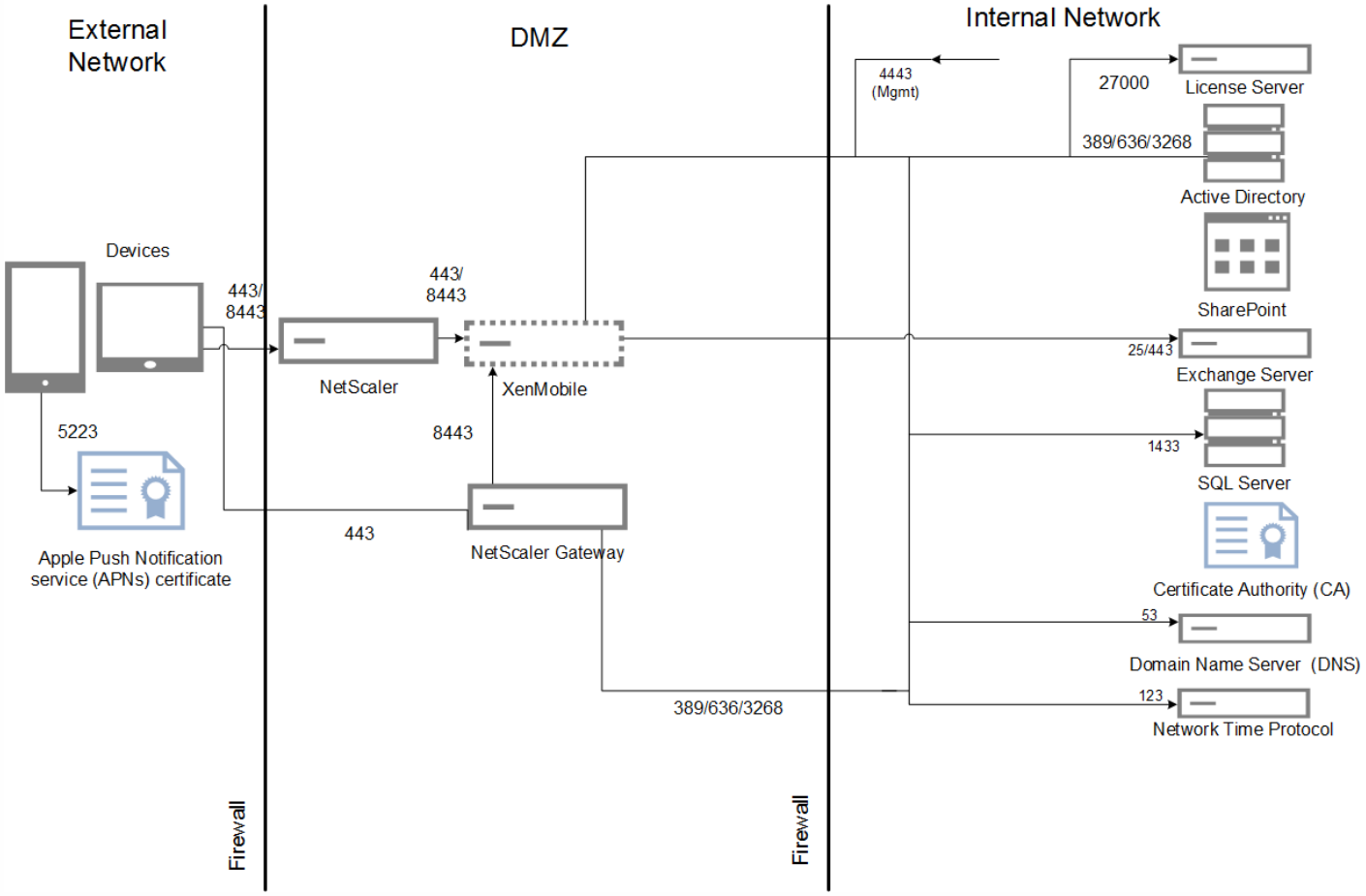
-
-
-
-

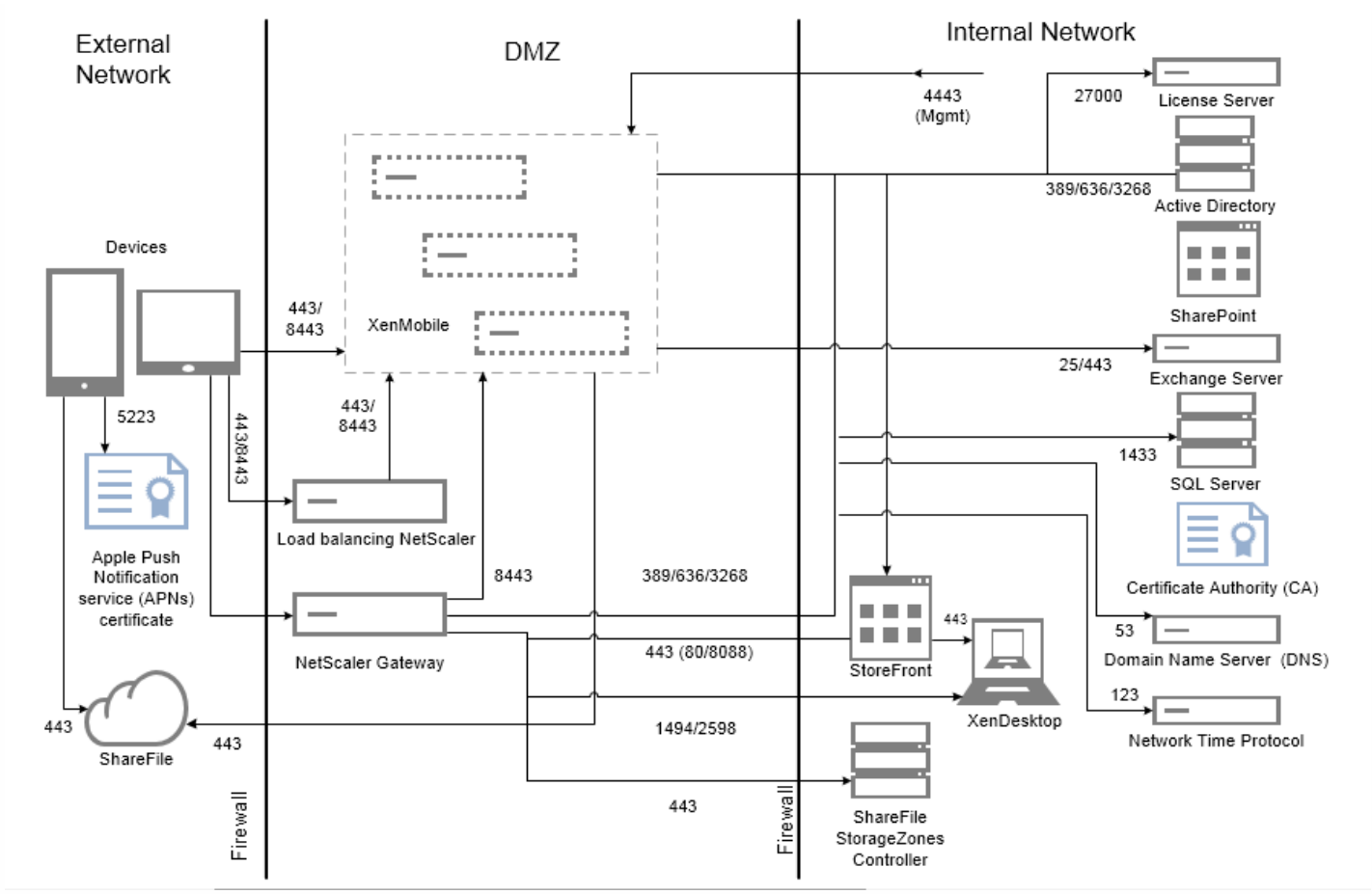


-
  -
  -
  -
-
  -
  -



	Standalone	Standalone	3 Node Cluster	6 Node Cluster	10 Node Cluster
Expected # of Devices	1000	10000	30000	60000	100000
Actual AG Logins	999	9944	29138	59189	98349
Actual Enumerations	999	9944	29132	59189	98349
Over All Error %	0.200	0.310	0.520	0.550	0.820





Testmethode

Arbeitslasten

-
-
-

-
-
-
-
-
-
-

-
-

-
-

Ausgangskriterien

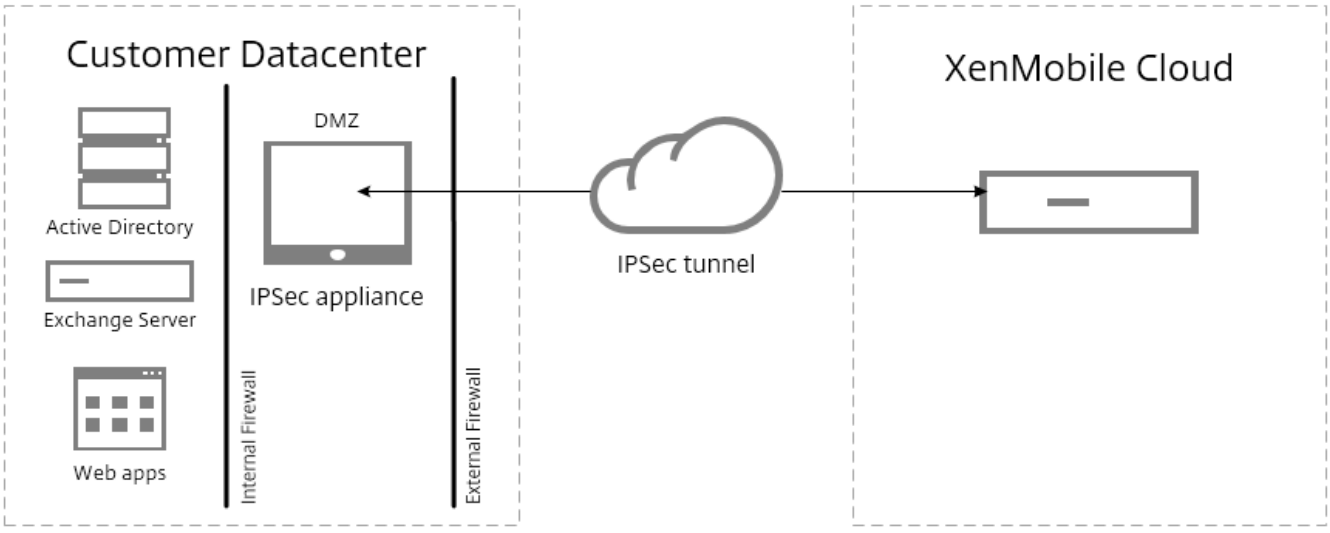
-
  -
-
  -
-
  -
  -

Angaben zu Software und Hardware

Info über XenMobile Cloud

Hinweis

-
-
-

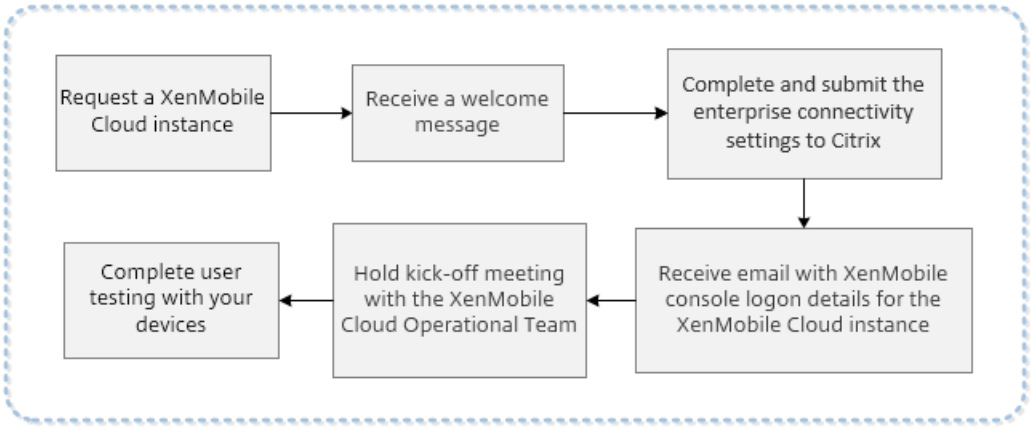


Rollen in XenMobile Cloud

-
-
-
-

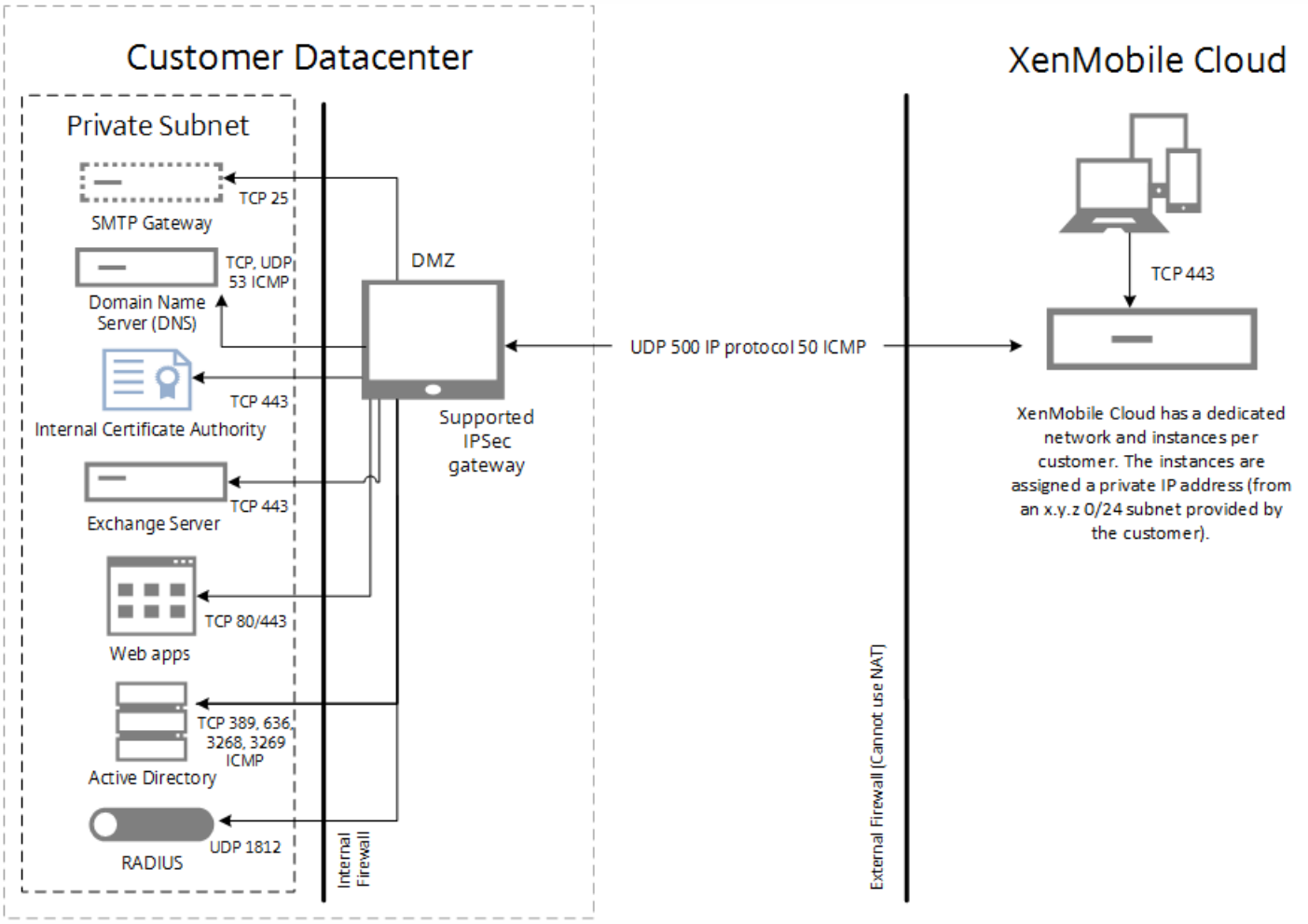
-
-
-

XenMobile Cloud – Voraussetzungen und Verwaltung



IPSec-Tunnelgateways für XenMobile Cloud

> Hinweis



APNs-Zertifikat von Apple für XenMobile

iOS-Pushbenachrichtigungszertifikat für WorxMail

XenMobile MDX Toolkit

XenMobile-Autodiscovery für die Windows Phone-Registrierung

Die XenMobile-Konsole

Geräteregistrierung bei XenMobile

XenMobile-Support

Unterstützen mobiler Plattformen in XenMobile Cloud

Android

-
-
-
-

iOS

-
-
-

Windows

-
-
-
-

Systemanforderungen

-
  -
  -
  -
-
-
-
-
-
-

Systemanforderungen für NetScaler Gateway

-
  -
  -
  -
-
-
-

XenMobile 10.1 – Datenbankanforderungen

-

-

XenMobile 10.1 – E-Mail-Serveranforderungen

-
-

XenMobile-Kompatibilität

Unterstützte Geräteplattformen

Portanforderungen

Öffnen von Ports für NetScaler Gateway und XenMobile zum Verwalten von Apps

Öffnen von XenMobile-Ports zum Verwalten von Geräten

Portanforderungen für die Verbindung mit Auto Discovery Service

-
-

FIPS 140-2-Richtlinientreue

Sprachunterstützung für XenMobile

Sprachunterstützung für Worx-Apps

Sprachunterstützung für die XenMobile-Konsole

Checkliste vor der Installation

Grundlegende Netzwerkeinstellungen

	• •		

Zertifikate

Ports

Datenbank

Active Directory-Einstellungen

Verbindungen zwischen XenMobile und NetScaler Gateway

Benutzerverbindungen: Zugriff auf XenDesktop, XenApp und Worx Home

Installieren von XenMobile

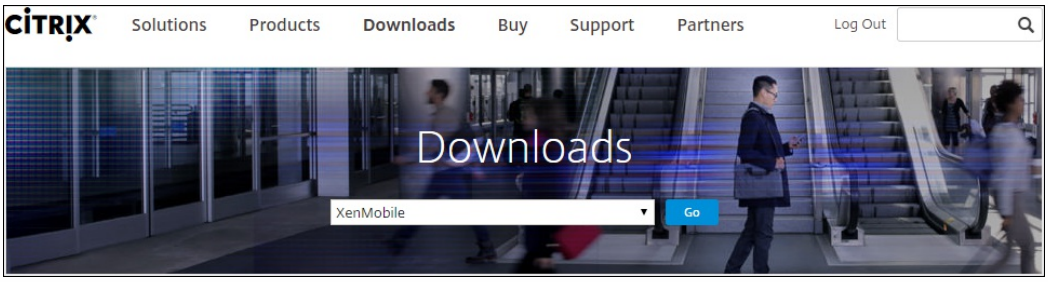
-
-

-

-
  -
  -

Download der XenMobile-Produktsoftware

So laden Sie die Software für XenMobile herunter



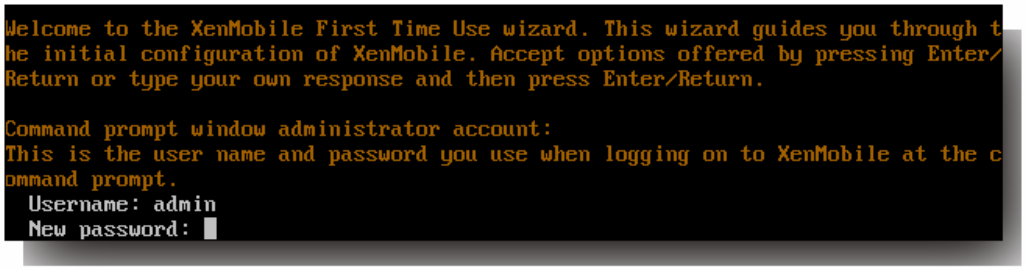
So laden Sie die Software für NetScaler Gateway herunter

Konfigurieren von XenMobile für die Erstverwendung

Hinweis

Konfigurieren von XenMobile im Eingabeaufforderungsfenster

1. Importieren Sie die virtuelle XenMobile-Maschine in Citrix XenServer, Microsoft Hyper-V oder VMware ESXi. Weitere Informationen finden Sie in der Dokumentation zu XenServer, Hyper-V oder VMware.
2. Wählen Sie im Hypervisor die importierte XenMobile-VM aus und rufen Sie das Eingabeaufforderungsfenster auf. Informationen hierzu finden Sie in der Dokumentation zum Hypervisor.
3. Erstellen Sie von der Konsolenseite des Hypervisors aus ein Administratorkonto für XenMobile im Eingabeaufforderungsfenster. Geben Sie dazu den Administratorbenutzernamen und das Administratorkennwort ein.
   Wichtig:
   Wenn Sie Kennwörter für das Administratorkonto an der Eingabeaufforderung, für Public Key-Infrastruktur-Serverzertifikate und FIPS erstellen oder ändern, erzwingt XenMobile die folgenden Regeln für alle Benutzer außer Active Directory-Benutzer, deren Kennwörter außerhalb von XenMobile verwaltet werden:
   - Das Kennwort muss mindestens 8 Zeichen lang sein und es muss mindestens drei der folgenden Komplexitätskriterien erfüllen:
     - Großbuchstaben (A bis Z)
     - Kleinbuchstaben (a bis z)
     - Ziffern (0 bis 9)
     - Sonderzeichen (z. B. !, #, $, %)



   Hinweis: Bei der Eingabe des neuen Kennworts werden keine Zeichen (Sternchen o. Ä.) angezeigt. Es wird nichts angezeigt.

4. Geben Sie die folgenden Netzwerkinformationen an und geben Sie danny ein, um die Einstellungen zu speichern:
   1. IP-Adresse
   2. Netzwerkmaske
   3. Standardgateway
   4. Primärer DNS-Server
   5. Sekundärer DNS-Server (optional)

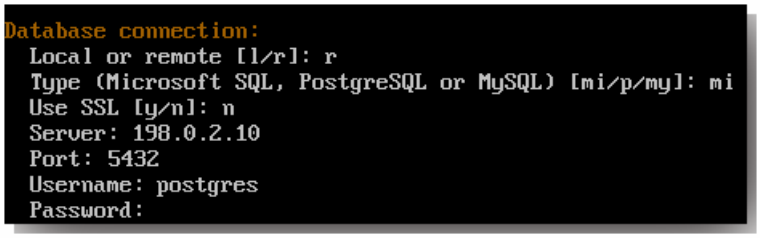
   Hinweis: Die abgebildeten Adressen sind nicht funktionsfähig und dienen nur als Beispiel.

5. Eingabey ein, um die Sicherheit zu erhöhen, indem Sie eine zufällige Passphrase zur Verschlüsselung generieren lassen, odern , um Ihre eigene Passphrase einzugeben. Citrix empfiehlt die Eingabe vony zum Generieren einer zufälligen Passphrase. Die Passphrase ist Teil des Schutzes der Verschlüsselungsschlüssel für vertrauliche Daten. Ein Hash der Passphrase, der im Dateisystem des Servers gespeichert ist, wird zum Abrufen der Schlüssel während der Datenverschlüsselung und -entschlüsselung verwendet. Die Passphase kann nicht angezeigt werden.

   Hinweis: Wenn Sie Ihre Umgebung erweitern und zusätzliche Server konfigurieren möchten, sollten Sie eine eigene Passphrase eingeben. Es gibt keine Möglichkeit, die Passphrase anzuzeigen, wenn Sie eine zufällige Passphrase nehmen.

6. Aktivieren Sie optional Federal Information Processing Standard (FIPS). Details über FIPS finden Sie unter FIPS 140-2-Konformität von XenMobile. Stellen Sie sicher, dass die unter Konfigurieren von FIPS mit XenMobile erläuterten Voraussetzungen erfüllt sind.

7. Geben Sie die folgenden Informationen zum Konfigurieren der Datenbankverbindung an:

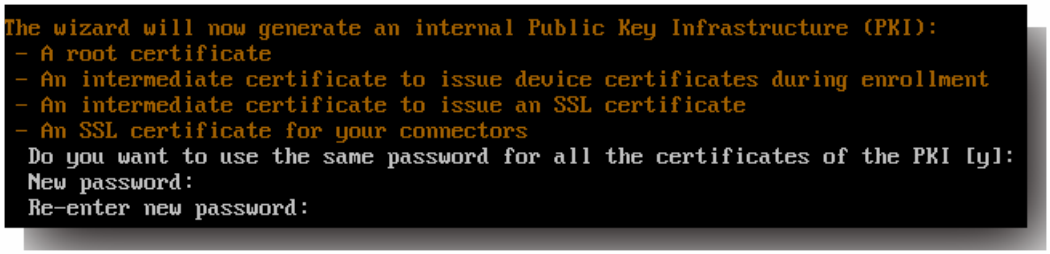


   1. Sie können eine lokale oder remote Datenbank verwenden. Eingabel für lokal oderr für remote ein.
   2. Wählen Sie den Datenbanktyp. Eingabemi für Microsoft SQL oderp für PostgreSQL ein.
      Wichtig:
      - Citrix empfiehlt die Remote-Verwendung von Microsoft SQL. PostgreSQL ist Teil von XenMobile und sollte lokal oder remote nur in Testumgebungen verwendet werden.
      - Eine Datenbankmigration wird nicht unterstützt. In einer Testumgebung erstellte Datenbanken können nicht in eine Produktionsumgebung übertragen werden.
   3. Optional können Siey eingeben, damit SSL-Authentifizierung für die Datenbank verwendet wird.
   4. Geben Sie den vollqualifizierten Domänennamen (FQDN) des Datenbankservers ein. Dieser Hostserver wird sowohl für die Geräteverwaltung als auch für die App-Verwaltung verwendet.
   5. Geben Sie Ihre Datenbankportnummer ein, wenn sie sich von der Standardportnummer unterscheidet. Der Standardport für Microsoft SQL ist 1433 und der Standardport für PostgreSQL ist 5432.
   6. Geben Sie den Benutzernamen für den Datenbankadministrator ein.
   7. Geben Sie das Datenbankadministratorkennwort ein.
   8. Geben Sie den Namen der Datenbank ein.
   9. Drücken Sie die Eingabetaste, um die Datenbankeinstellungen zu übernehmen.
8. Optional können Siey eingeben, um das Clustering von XenMobile-Knoten oder Instanzen zu aktivieren.
   Wichtig: Wenn Sie einen XenMobile-Cluster aktivieren, öffnen Sie nach der Systemkonfiguration Port 80, um die Echtzeitkommunikation zwischen Clustermitgliedern zu aktivieren.
9. Geben Sie den vollqualifizierten Domänennamen (FQDN) des XenMobile-Servers ein. Der FQDN muss mit dem allgemeinen Namen im SSL Listener-Zertifikat übereinstimmen.

   Hinweis: Der FQDN des XenMobile-Servers ist die öffentliche DNS für die XenMobile-Registrierung.

10. Drücken Sie die Eingabetaste, um die Einstellungen zu übernehmen.
11. Geben Sie die Kommunikationsports an. Informationen über die Ports und ihre Verwendung finden Sie unter Portanforderungen für XenMobile.
    Hinweis: Zum Akzeptieren der Standardports drücken Sie die Eingabetaste.

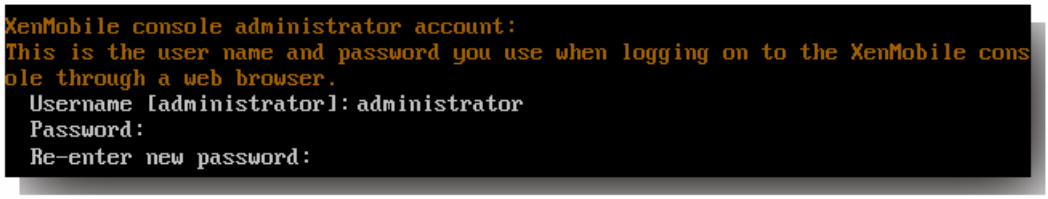
12. Überspringen Sie die nächste Frage zum Upgrade von einem vorherigen XenMobile-Release, da Sie XenMobile zum ersten Mal installieren.
13. Eingabey ein, wenn Sie dasselbe Kennwort für alle Public Key-Infrastruktur-Zertifikate verwenden möchten. Informationen zum XenMobile PKI-Feature finden Sie unter Hochladen von Zertifikaten in XenMobile.



Wichtig: Wenn Sie Knoten oder Instanzen von XenMobile in Clustern verwenden möchten, müssen Sie identische Kennwörter für die nachfolgenden Knoten angeben.

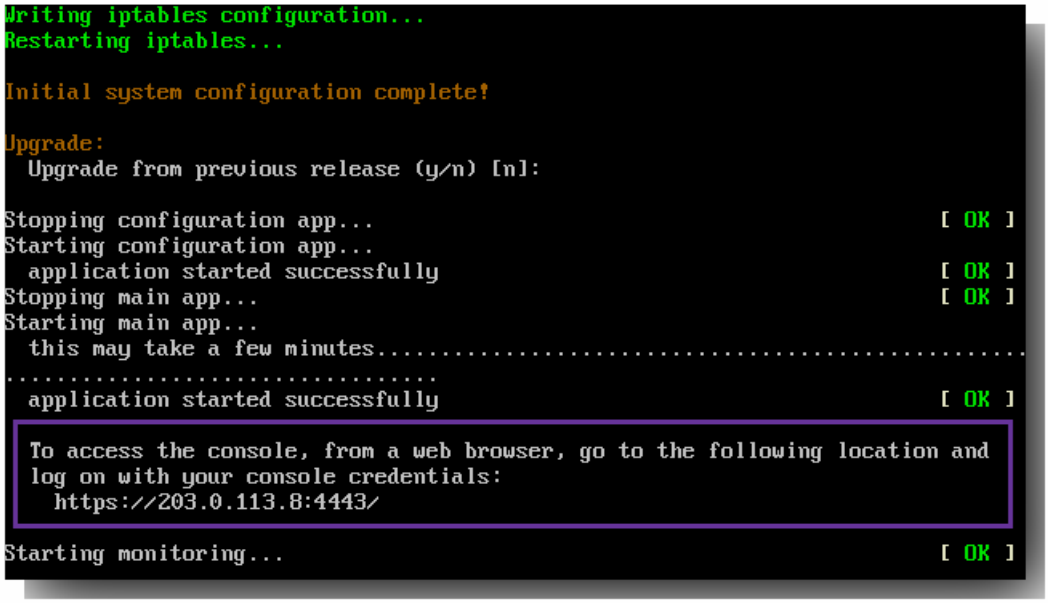
14. Geben Sie das neue Kennwort ein und geben Sie dann das neue Kennwort zur Bestätigung erneut ein.
    Hinweis: Bei der Eingabe des neuen Kennworts werden keine Zeichen (Sternchen o. Ä.) angezeigt. Es wird nichts angezeigt.

15. Drücken Sie die Eingabetaste, um die Einstellungen zu übernehmen.
16. Erstellen Sie ein Administratorkonto für die Anmeldung bei der XenMobile-Konsole mit einem Webbrowser. Diese Anmeldeinformationen sind zur späteren Verwendung aufzubewahren.



Hinweis: Bei der Eingabe des neuen Kennworts werden keine Zeichen (Sternchen o. Ä.) angezeigt. Es wird nichts angezeigt.

17. Drücken Sie die Eingabetaste, um die Einstellungen zu übernehmen. Die anfängliche Systemkonfiguration wird gespeichert.
18. Geben Sie zur Beantwortung der Frage, ob es sich um ein Upgrade handelt,n ein, da Sie eine Neuinstallation vornehmen.
19. Kopieren Sie die vollständige nun angezeigte URL und setzen Sie die Erstkonfiguration von XenMobile in Ihrem Webbrowser fort.



Konfigurieren von XenMobile in einem Webbrowser

-
-

Konfigurieren von FIPS mit XenMobile

-
-
-

Konfigurieren des FIPS-Modus

Voraussetzungen für SQL

Voraussetzungen für Internetinformationsdienste (IIS)

Hinweis

Importieren des Stammzertifikats während der FIPS-Erstkonfiguration

-
-
-
-
-
-
-
-
-

Aktualisieren von XenMobile

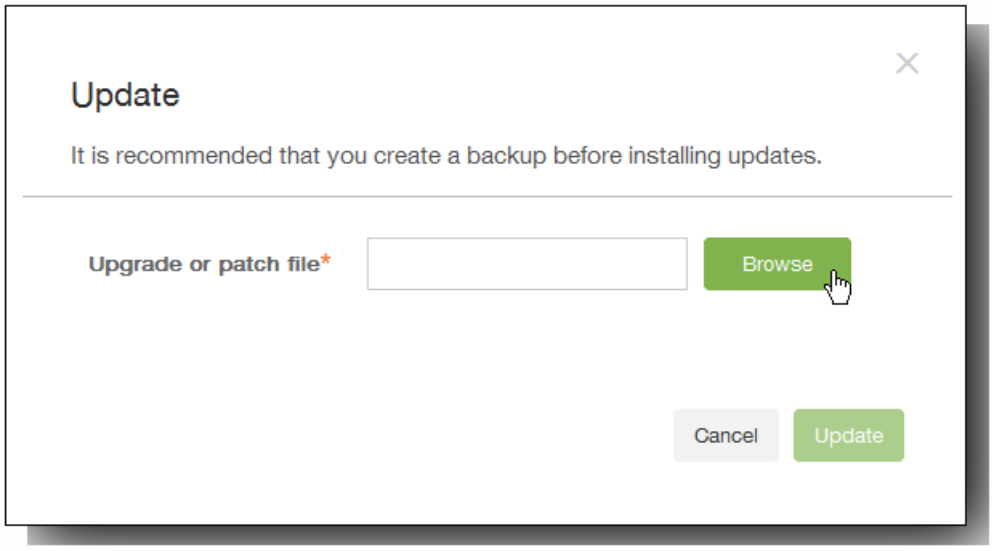
-
-

> Hinweis
> -
> -

> Important
> -
> -

So aktualisieren Sie XenMobile

-
-
-



-
-
-

Informationen zum Upgrade Tool

-
-

Upgradepfade

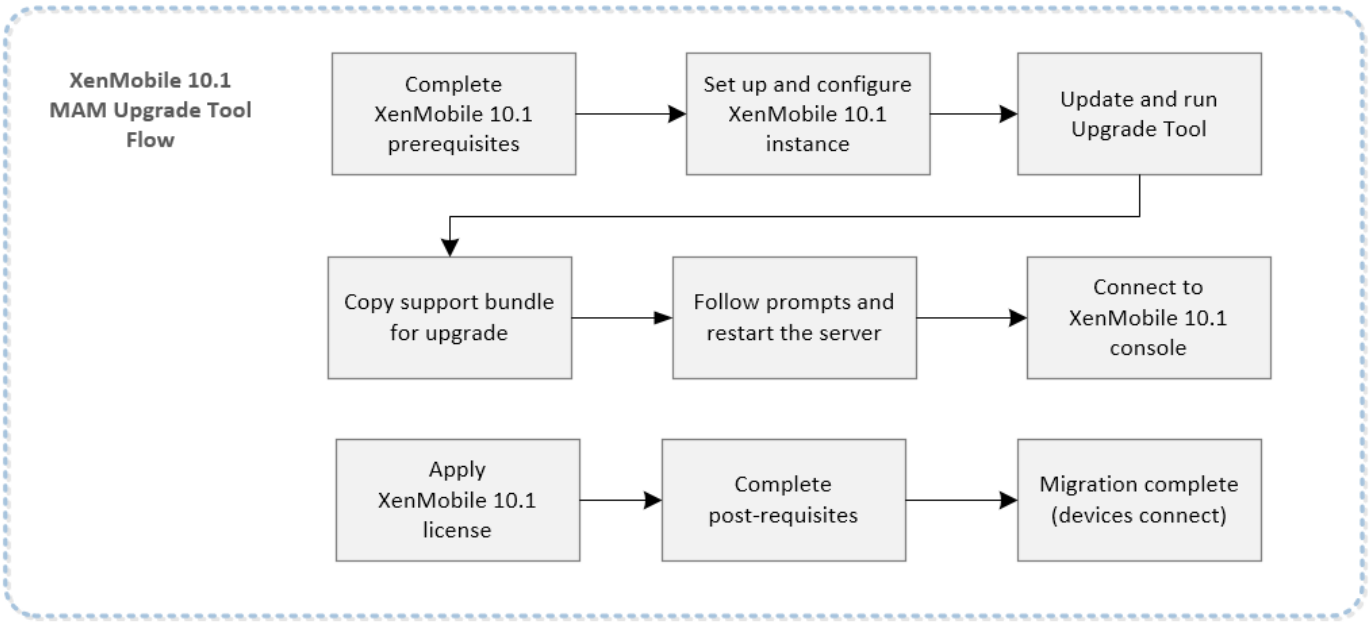
-
-

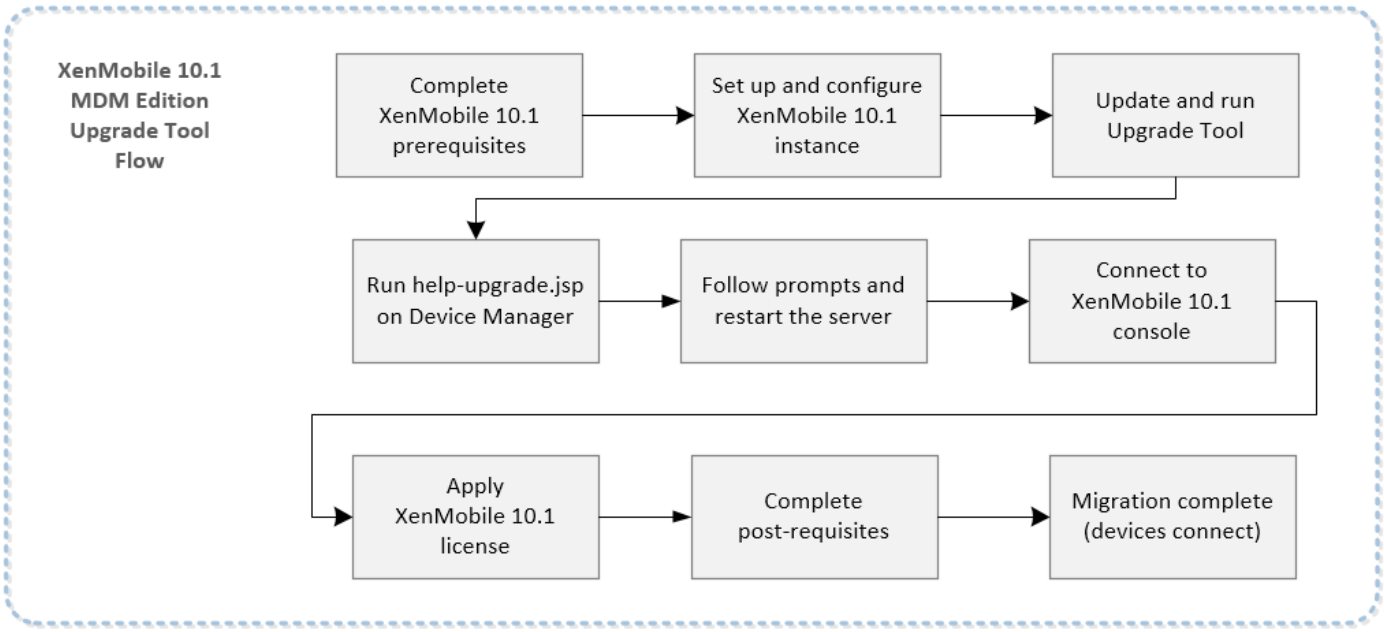
iOS- und Android-Geräte (alle Registrierungsmodi) und Windows Phones und Windows-Tablets (MDM)

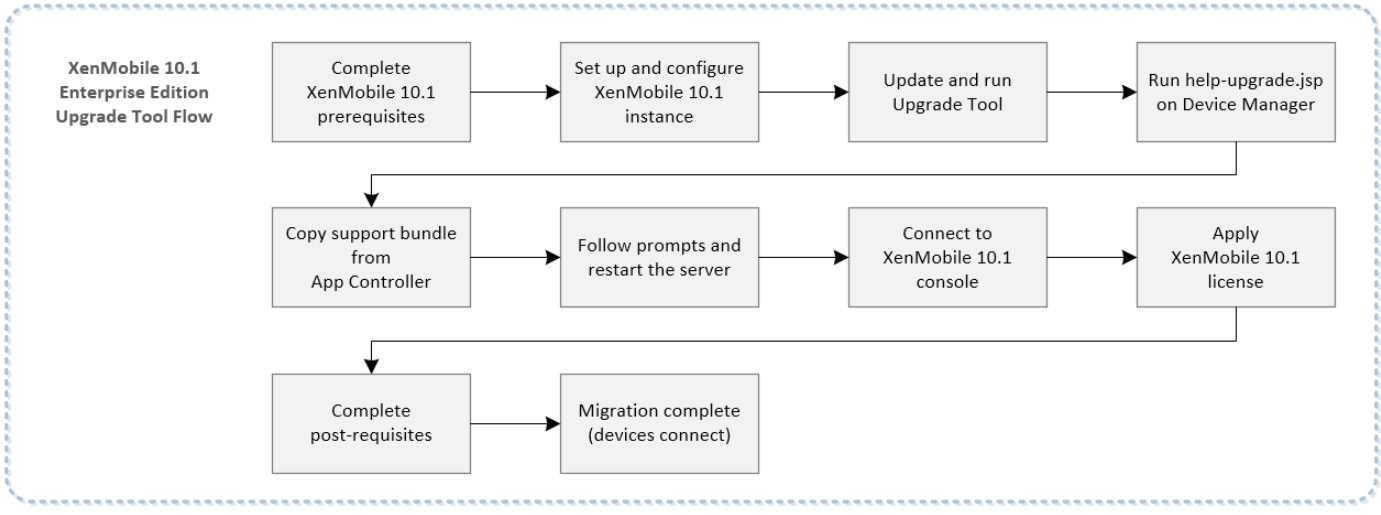
-
-

Windows Phones (Enterprise-Modus)

Übersicht über das Upgrade von XenMobile 9.0 auf 10.1







Upgrade Tool – behobene Probleme in diesem Release

> Hinweis

Upgrade Tool – bekannte Probleme in diesem Release

> Important
>
> •

•
•

•

-
-
-
-
-
-
-
-
-
-
-

-
-
-
-

Vom Upgrade Tool migrierte Elemente

-
-

-
-

Vom Upgrade Tool nicht migrierte Elemente

-
-
-
-
-
-
-
-
-
-
-

-

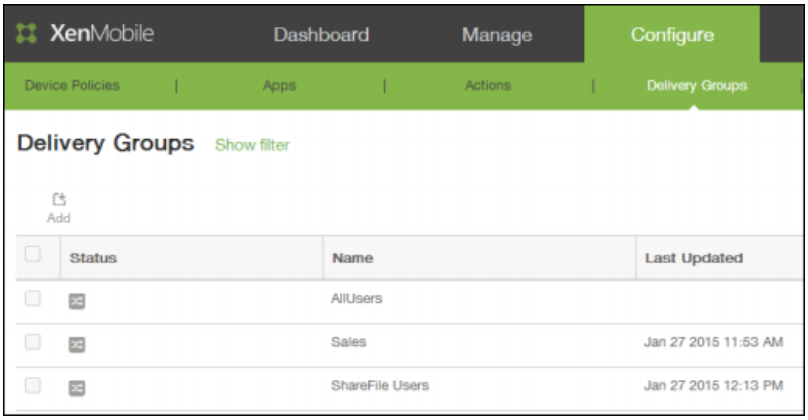
-
-

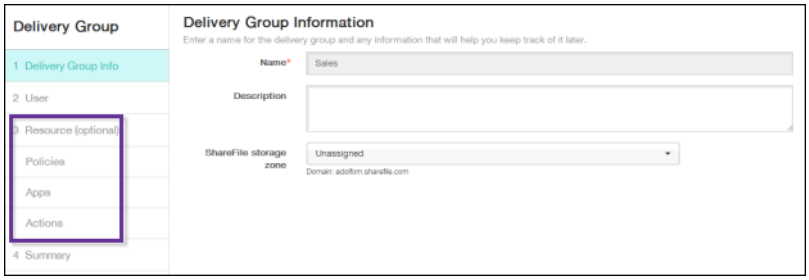
-
-

Planen des Upgrades

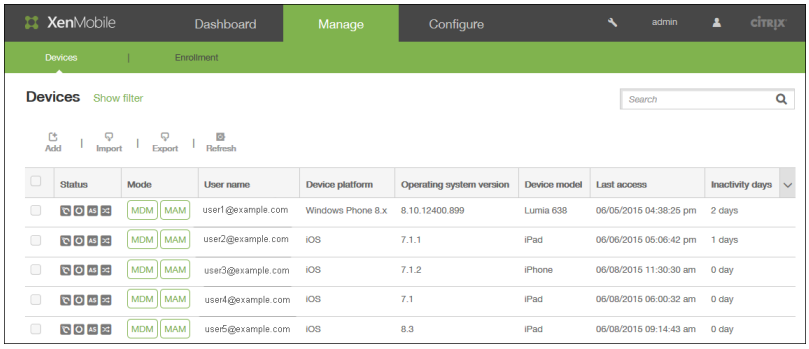
> **Important**

Geänderte Terminologie bei XenMobile 10.1





Geräteregistrierung in einer XenMobile Enterprise Edition-Bereitstellung nach einem Upgrade



Voraussetzungen

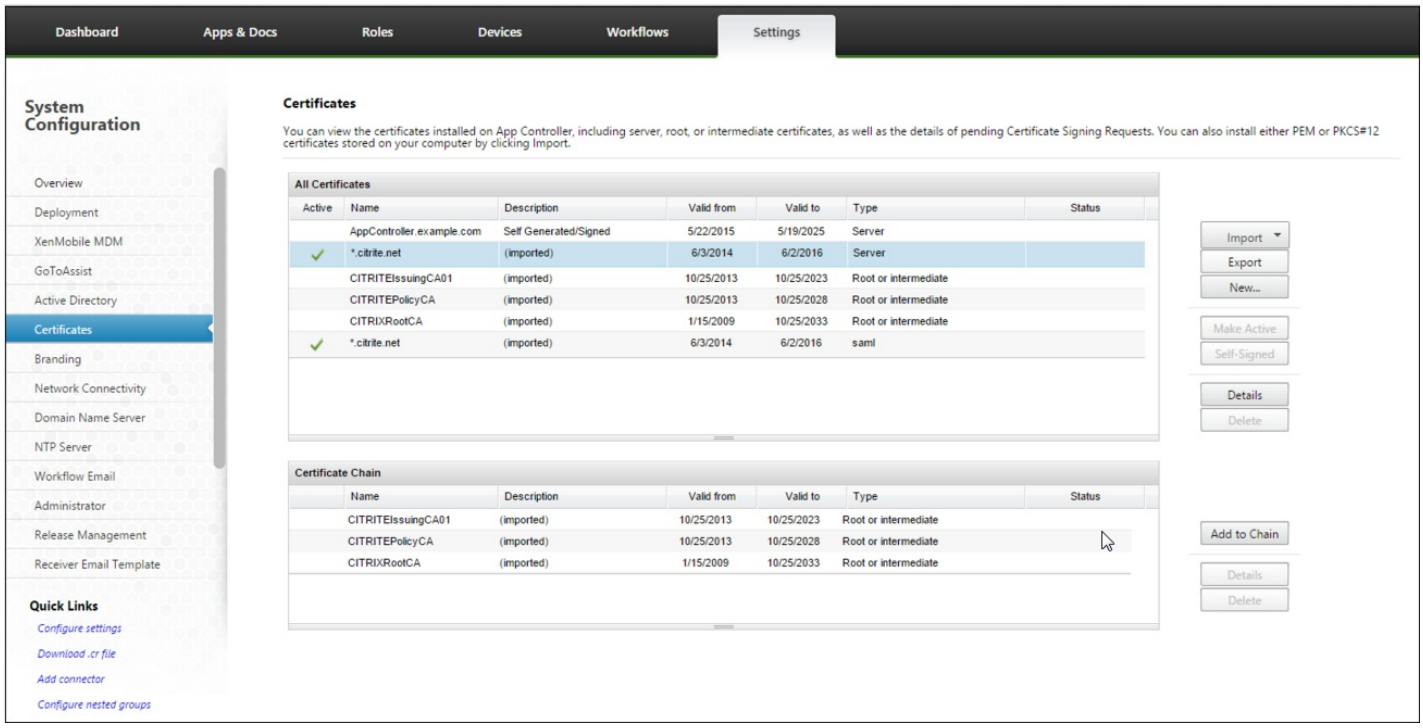
Important

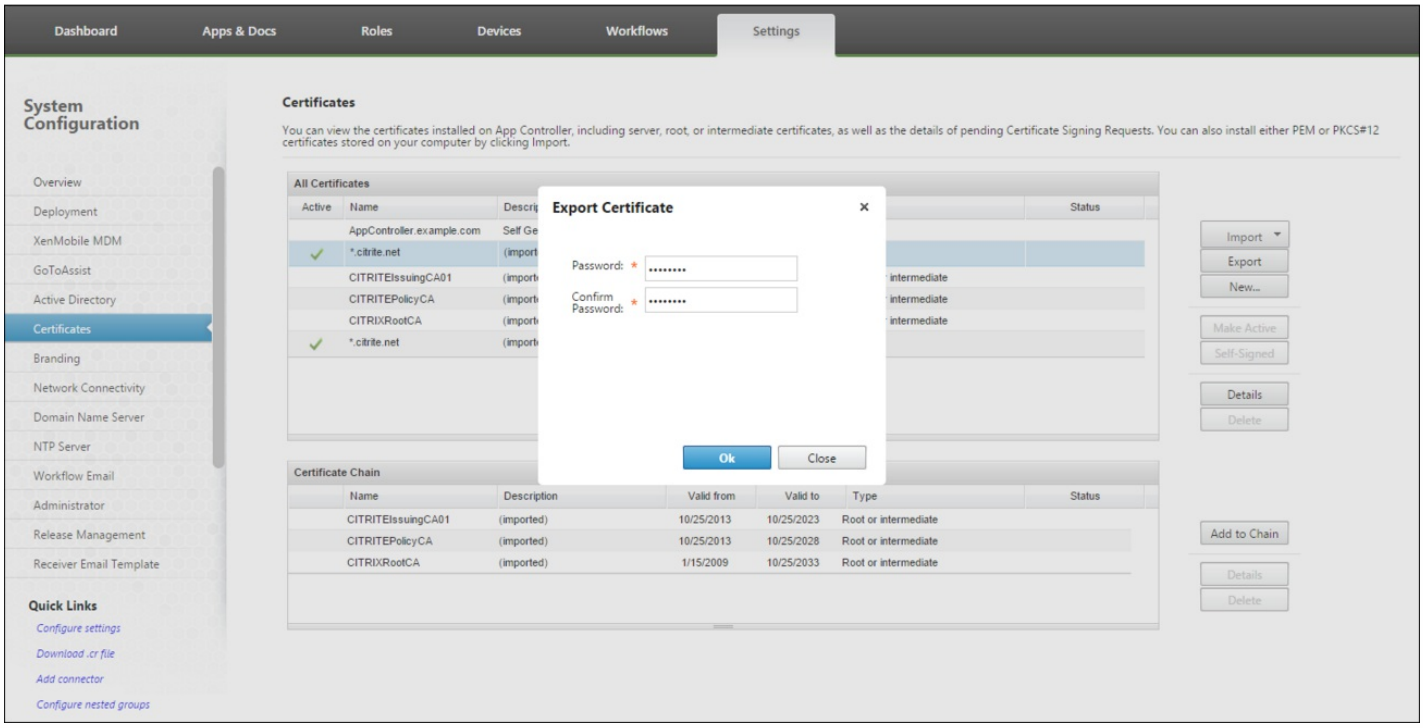
-

Hinweis

-
-

> Hinweis

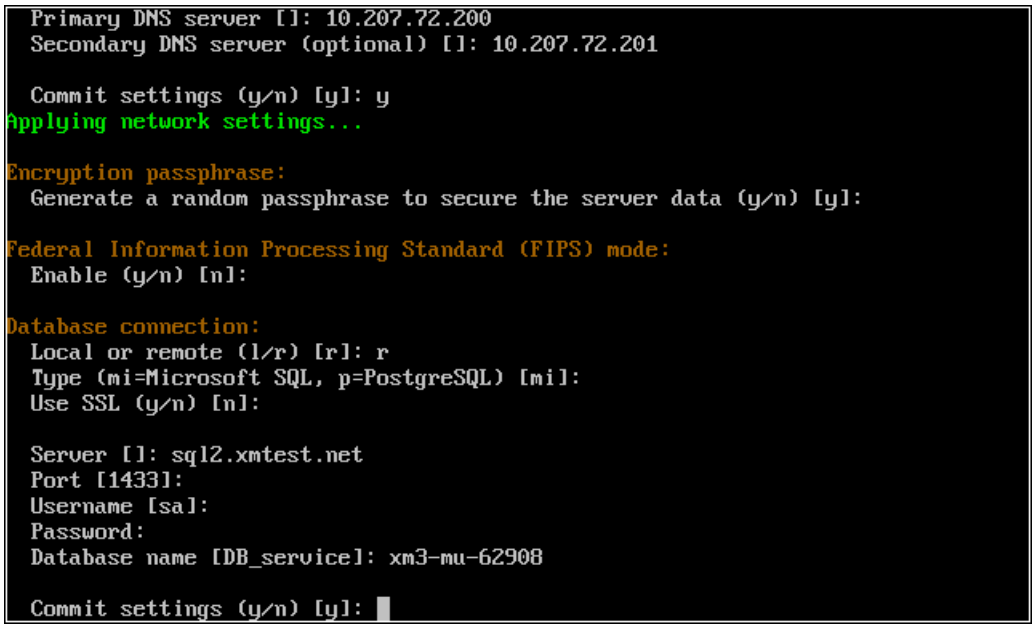


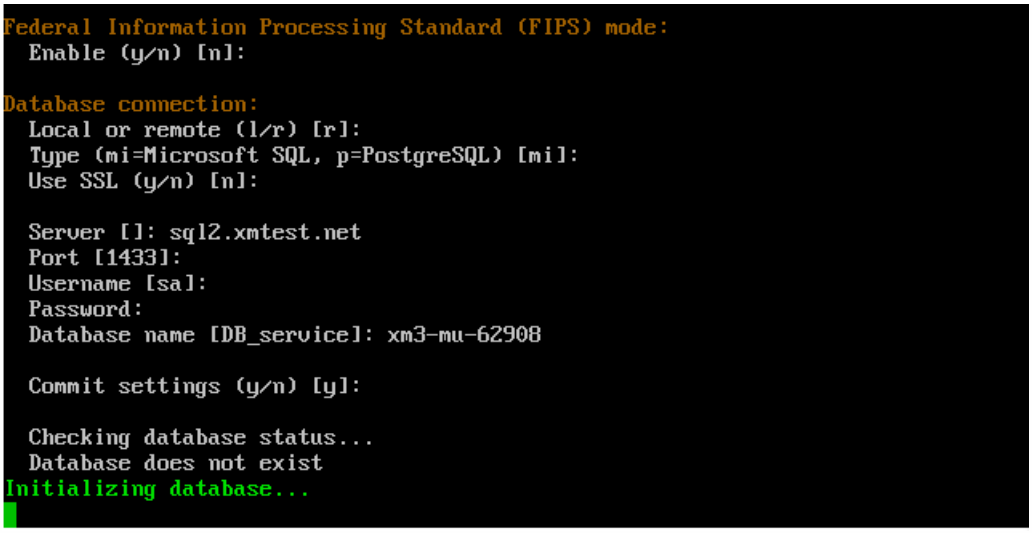


Aktivieren und Ausführen des XenMobile 10.1 Upgrade Tools

So installieren Sie eine Instanz von XenMobile 10.1 und aktivieren das Upgrade Tool

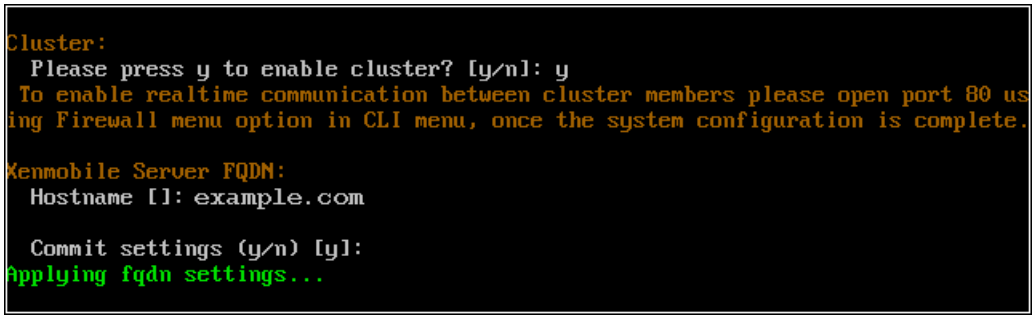
> Important

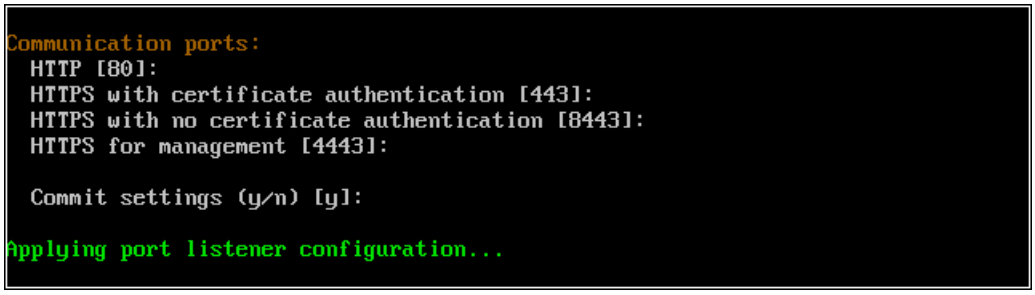


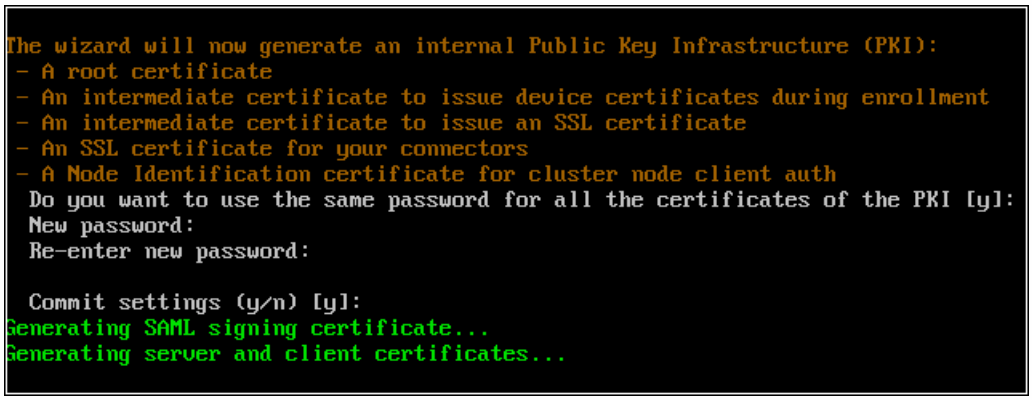


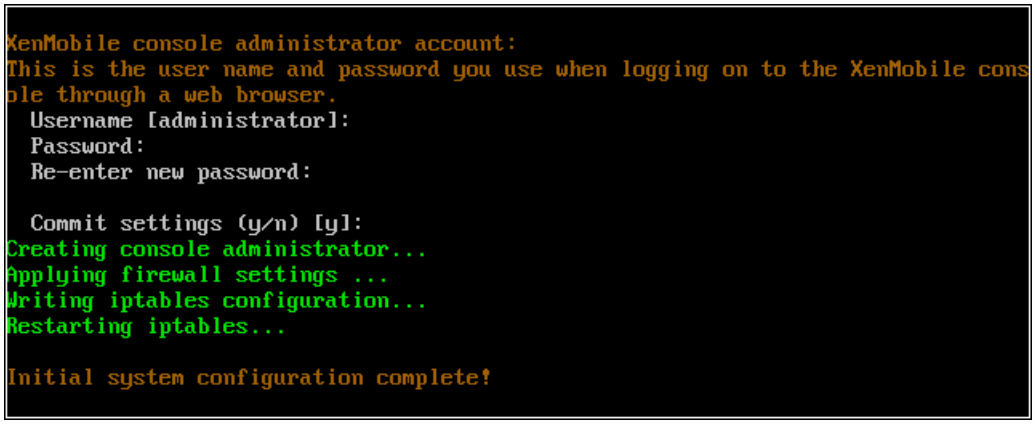
-
-
-

> **Important**

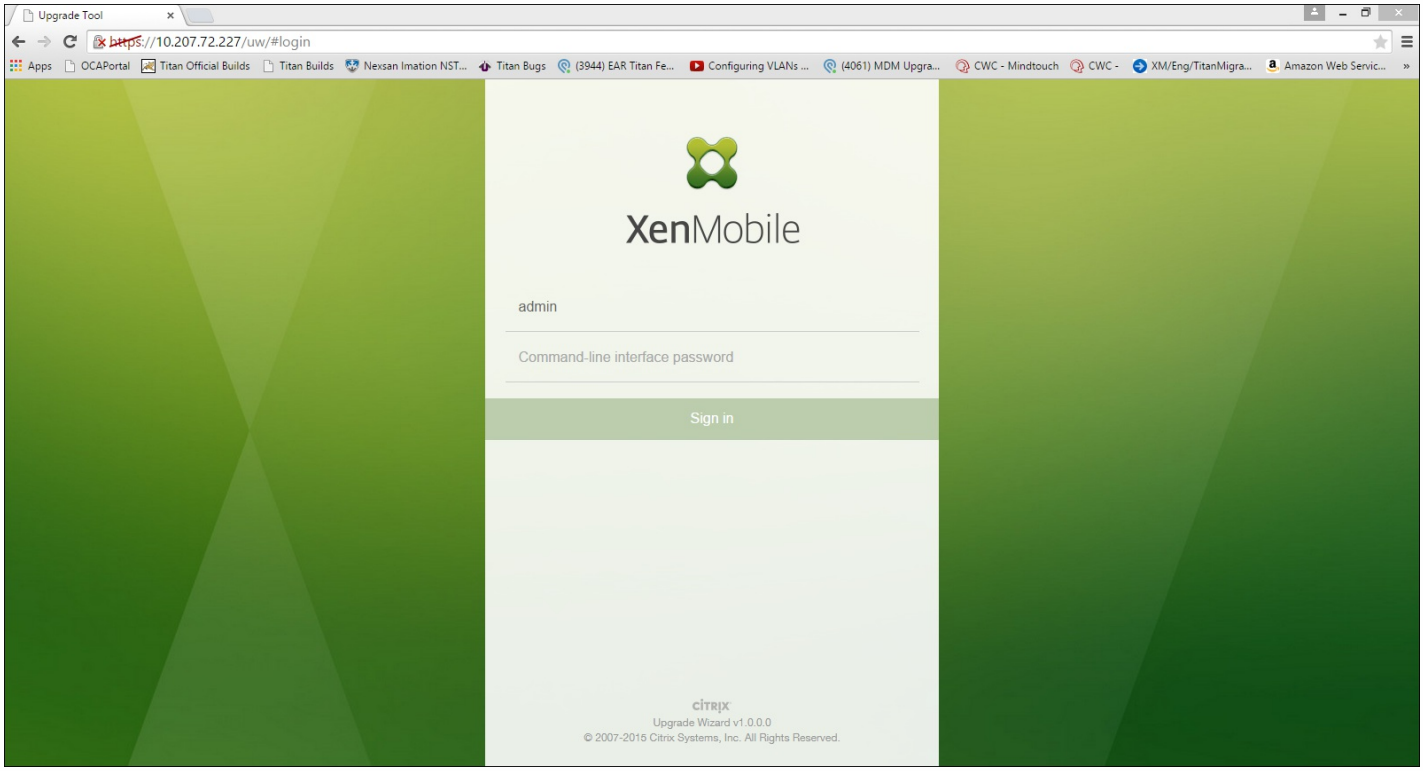


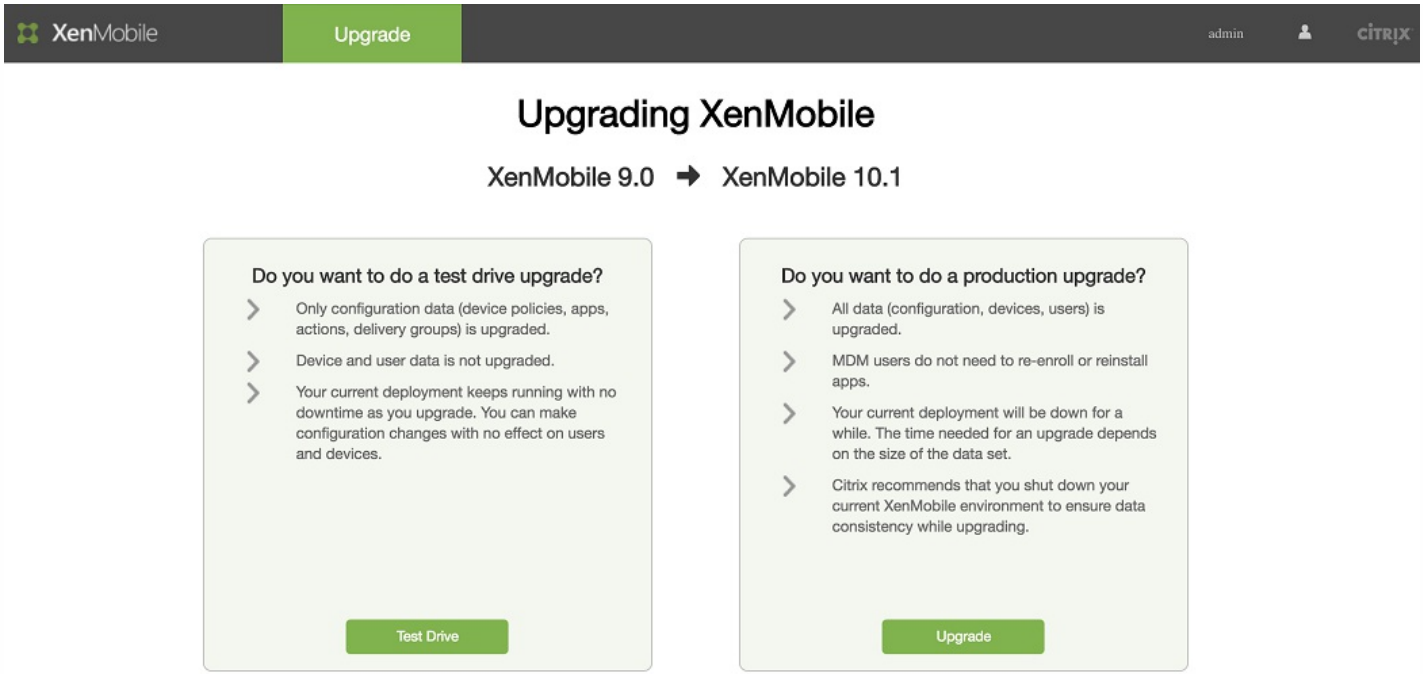


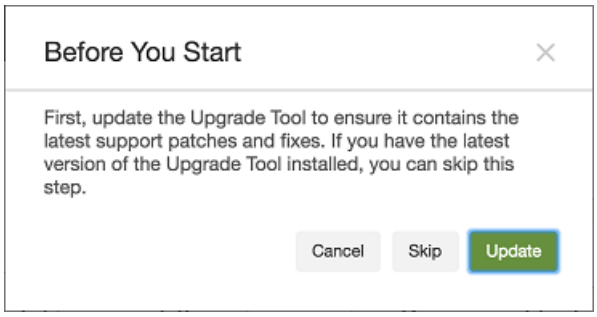


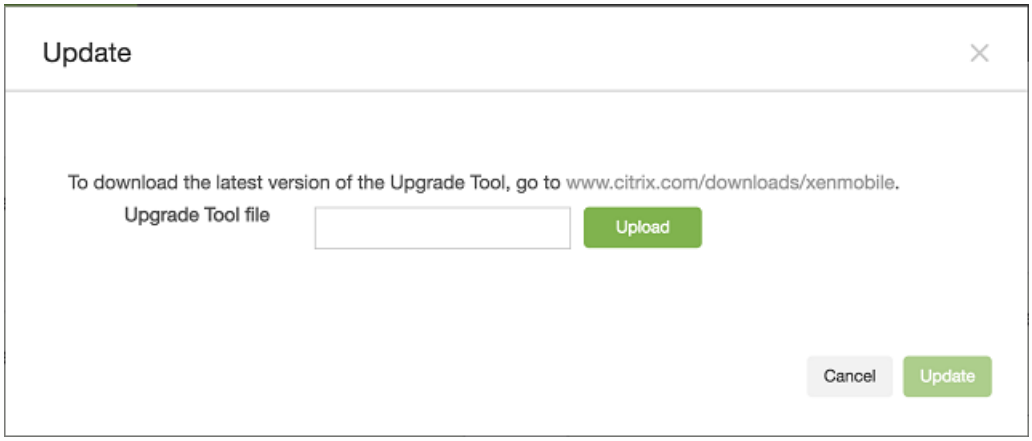


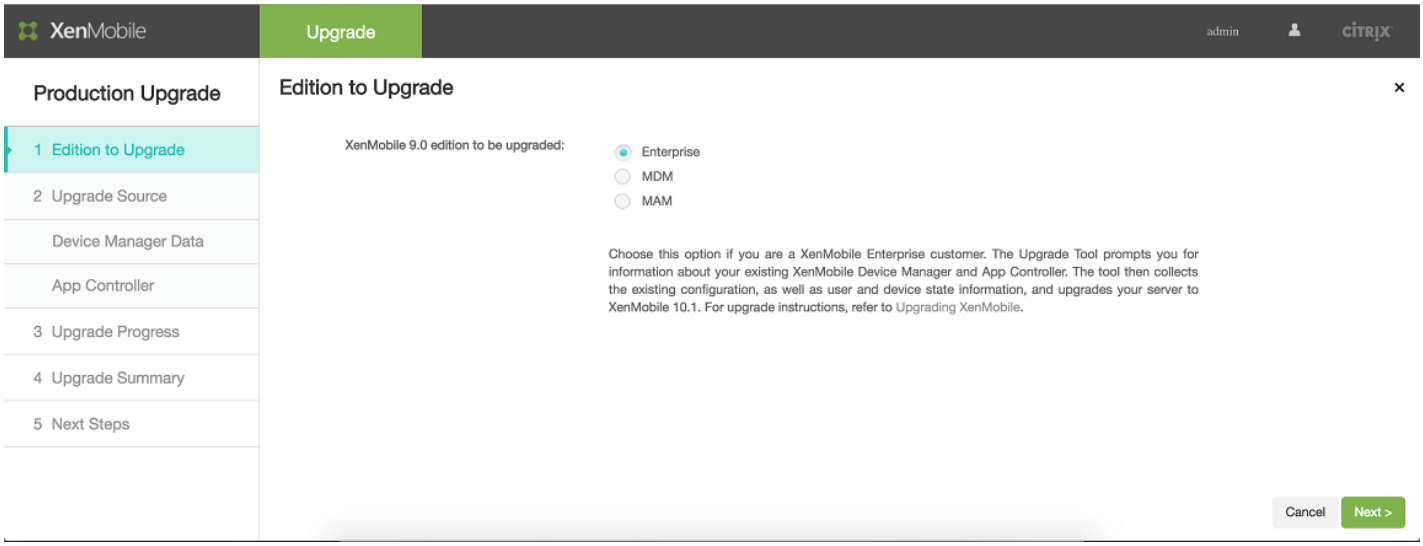
```
Upgrade:
  Upgrade from previous release (y/n) [n]: y

Stopping configuration app...                                    [ OK ]
Starting configuration app...
  this may take a few seconds........
  application started                                            [ OK ]
Stopping main app...                                             [ OK ]
Starting main app...
  not ready to start yet                                         [ OK ]

  To complete the upgrade process, from a web browser, go to the following
  location and log on with your command prompt credentials:
    https://198.51.100.1/uw/

Starting monitoring...                                           [ OK ]

enroll.example.com login:
```

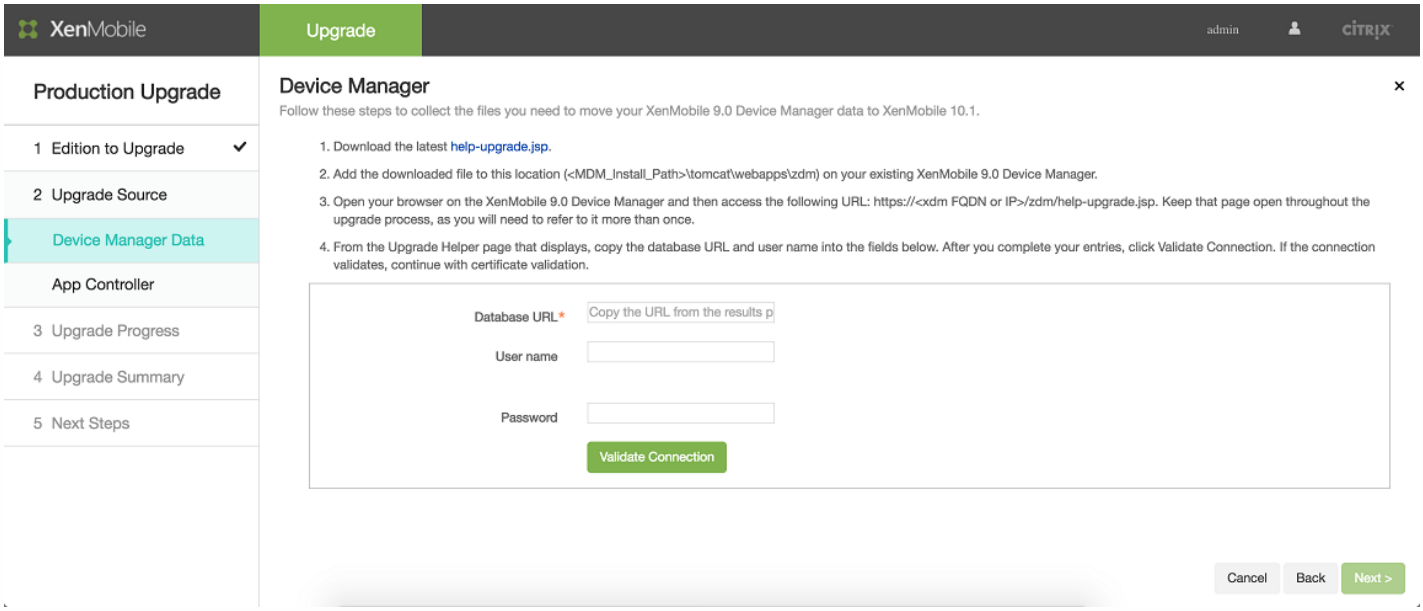


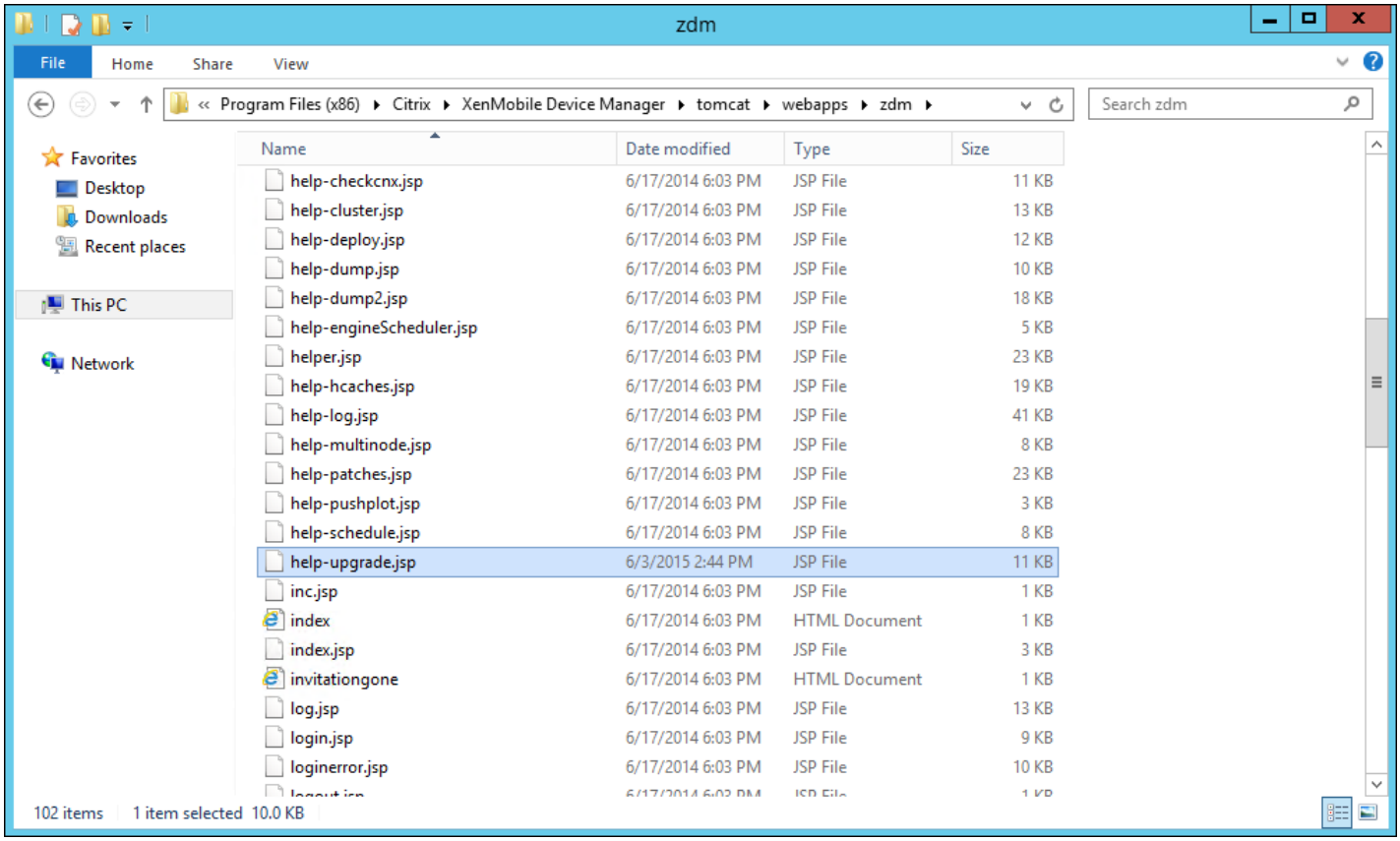


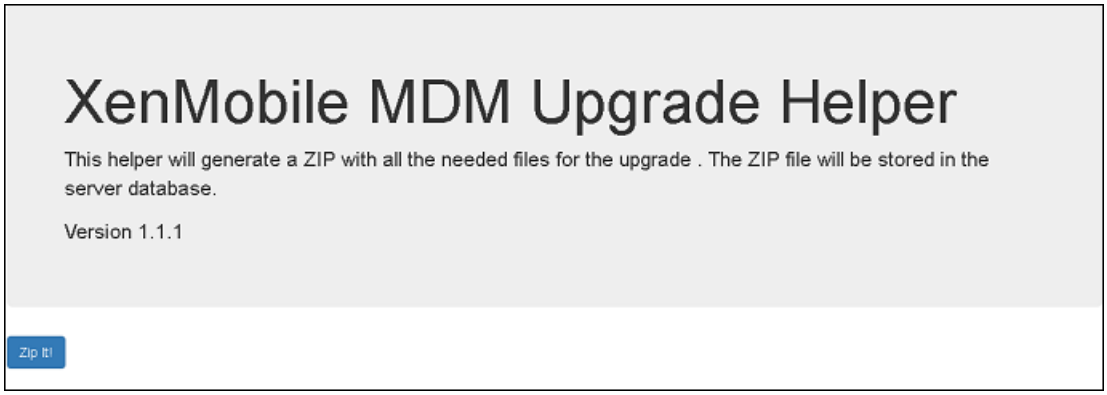


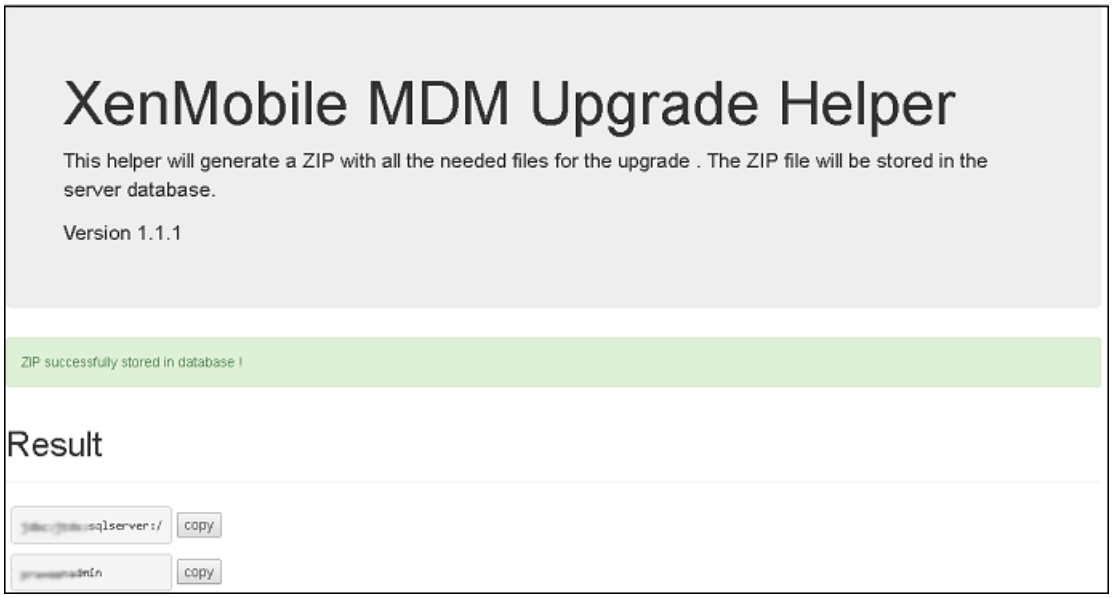


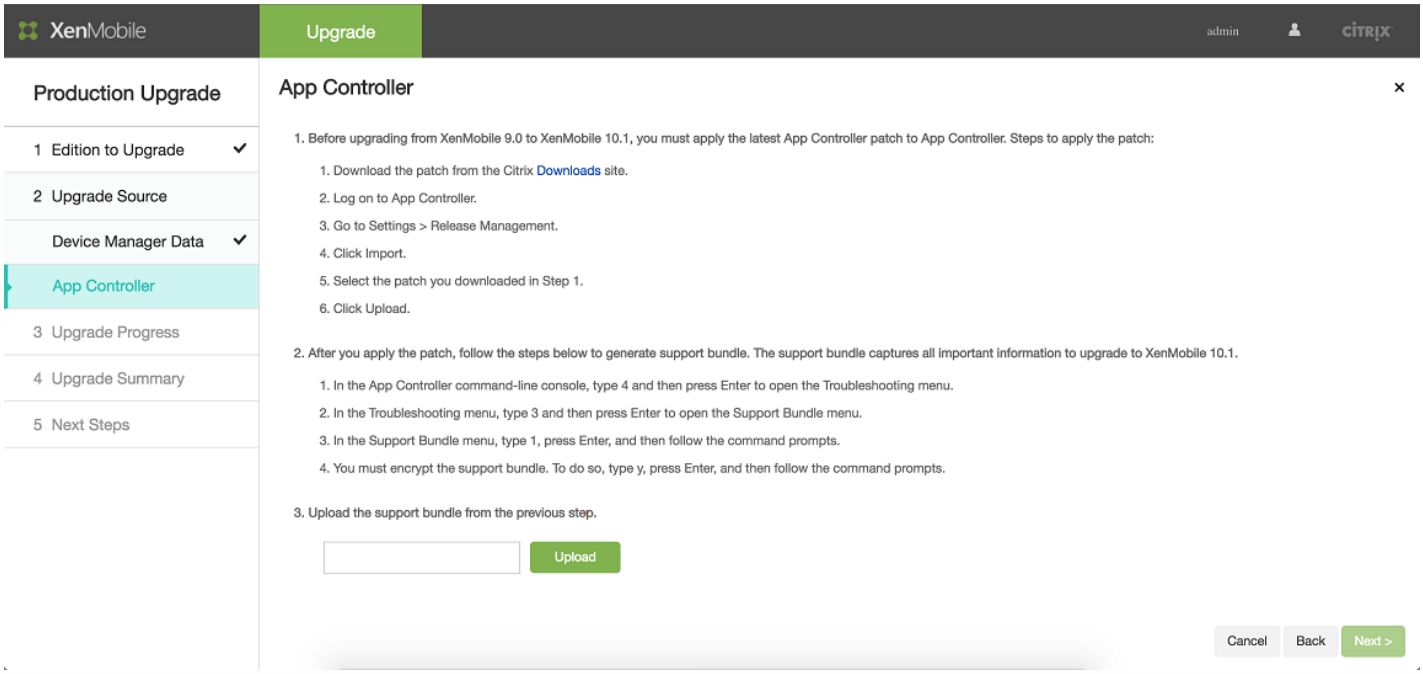










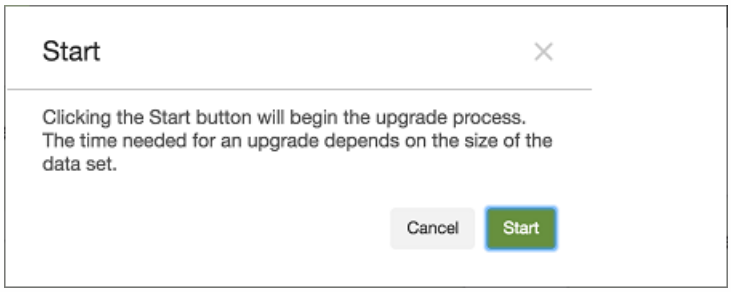


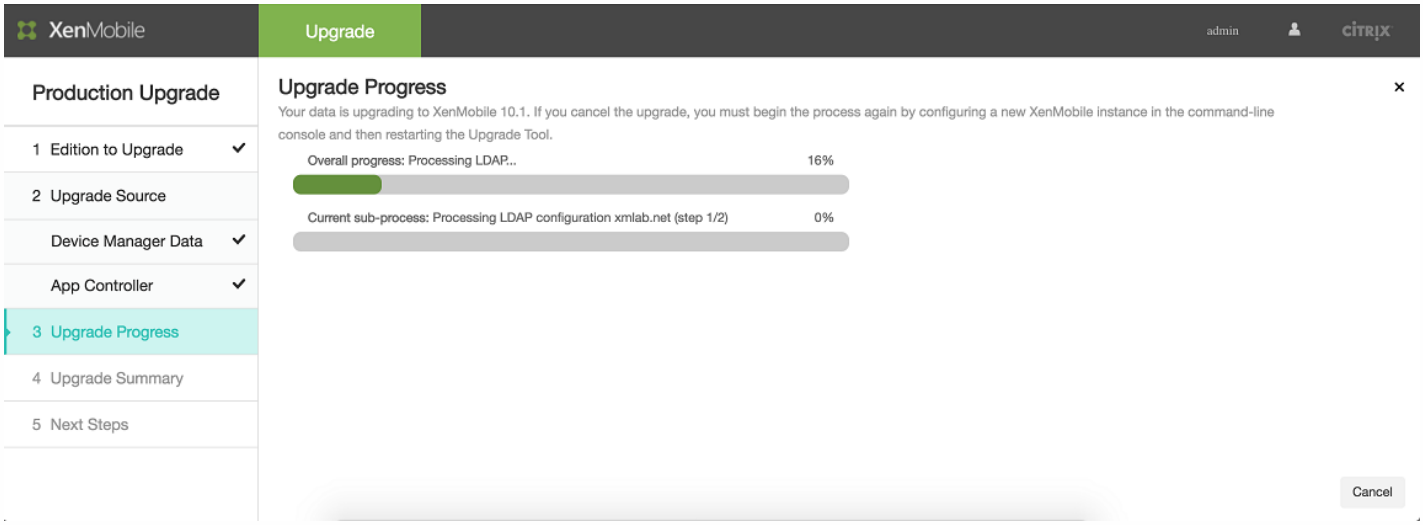
```
AppController 9.0.0.973502, 2015-06-26

---------------------------------
Main Menu
---------------------------------
[0] Express Setup
[1] High Availability
[2] Clustering
[3] System
[4] Troubleshooting
[5] Help
[6] Log Out
---------------------------------
Choice: [0 - 6] 4

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

```
[6] Log Out
---------------------------------
Choice: [0 - 6] 4

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

---------------------------------
Support Bundle Menu
---------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
---------------------------------
Choice: [0 - 4]
```

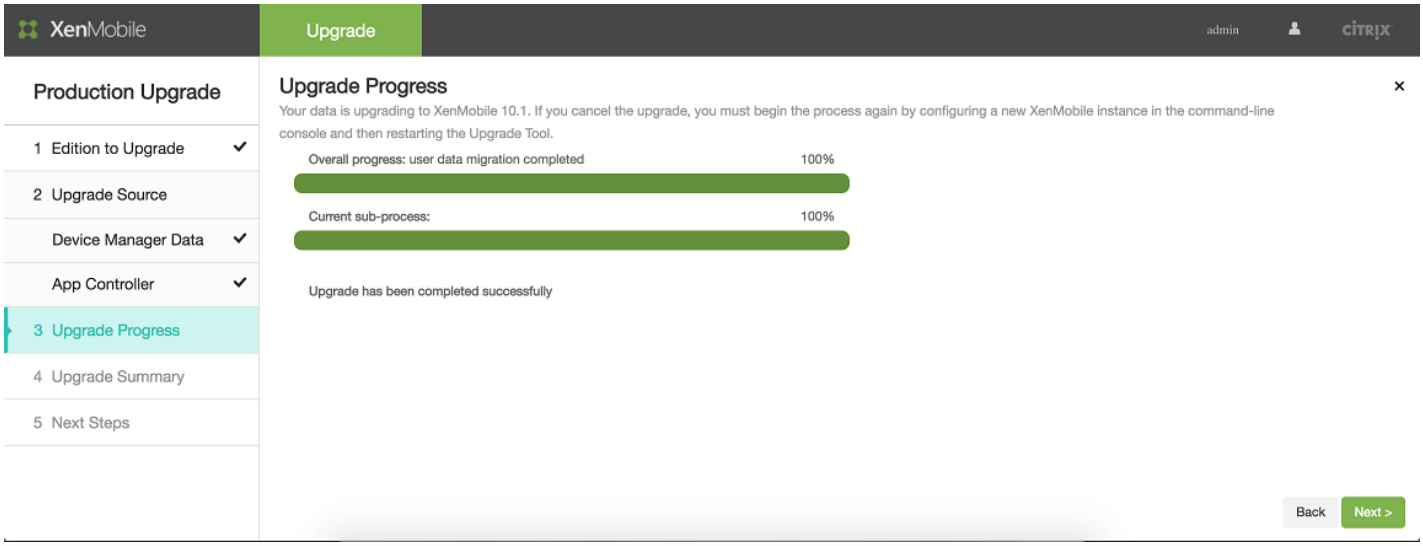
```
[6] Log Out
---------------------------------
Choice: [0 - 6] 4

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

---------------------------------
Support Bundle Menu
---------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
---------------------------------
Choice: [0 - 4] 1
```

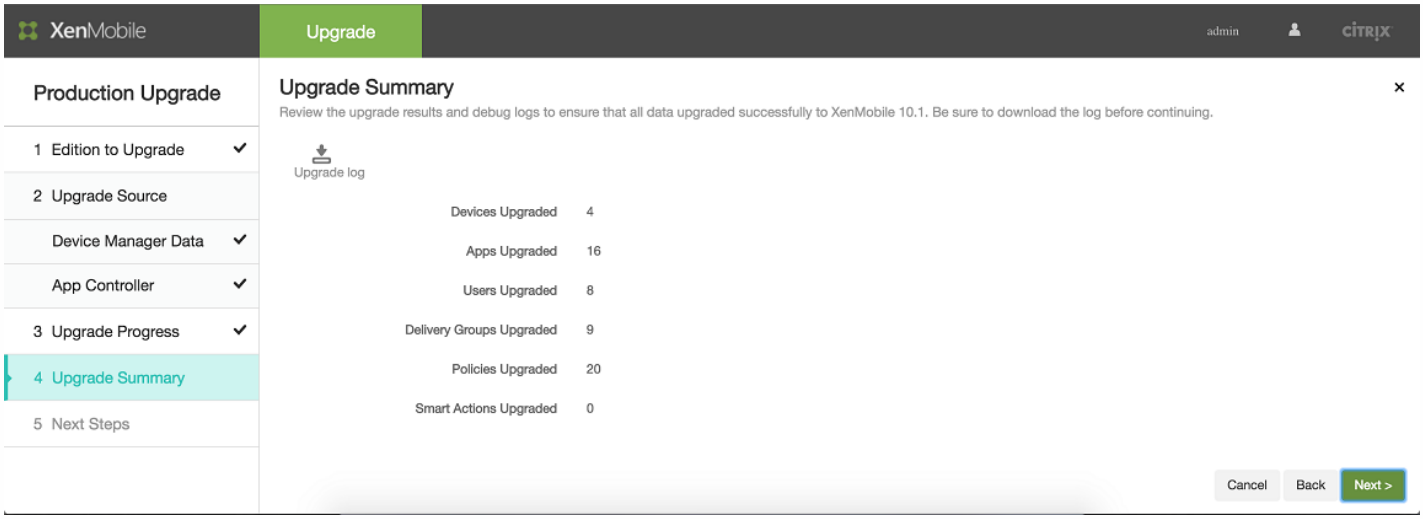
```
---------------------------------
Troubleshooting Menu
---------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
---------------------------------
Choice: [0 - 3] 3

---------------------------------
Support Bundle Menu
---------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
---------------------------------
Choice: [0 - 4] 1
Do you want to encrypt the support bundle? [y/n] y

Please wait while AppController creates the support bundle.
```

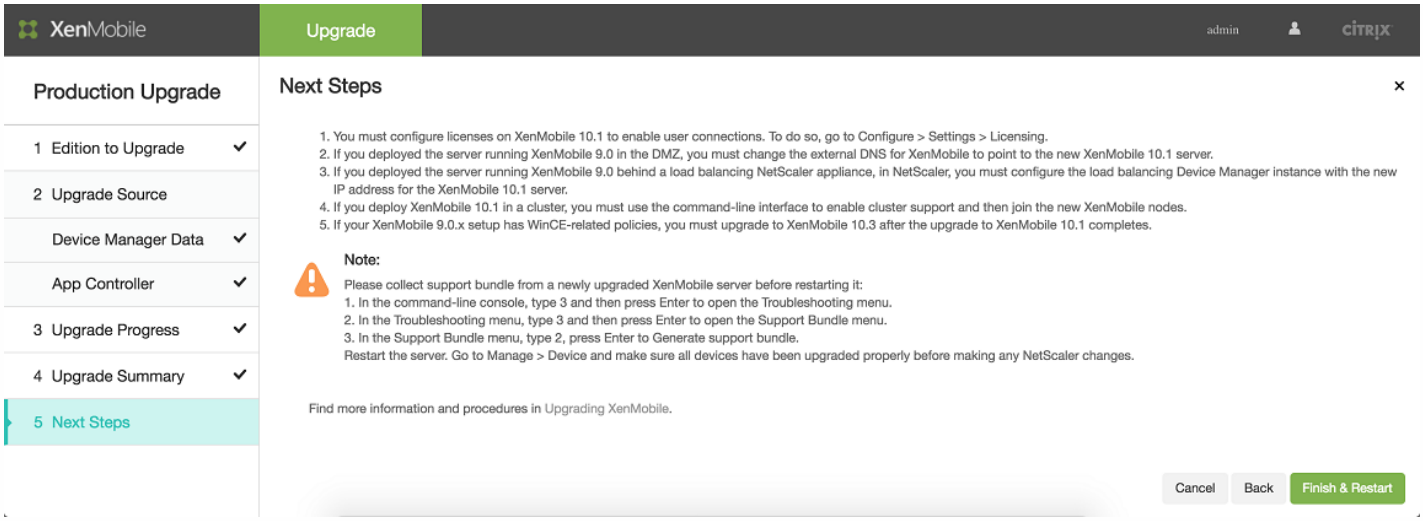




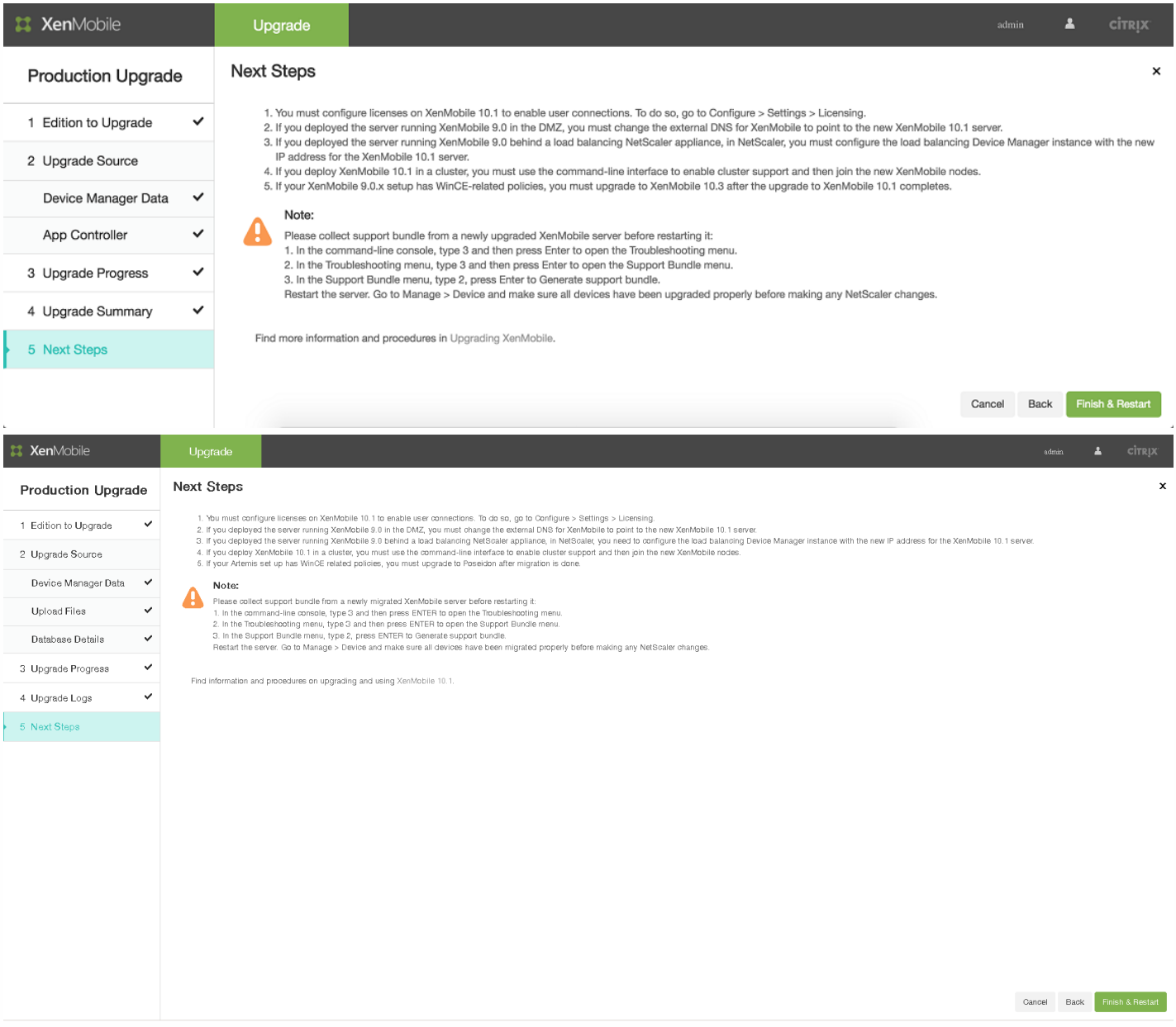
Hinweis

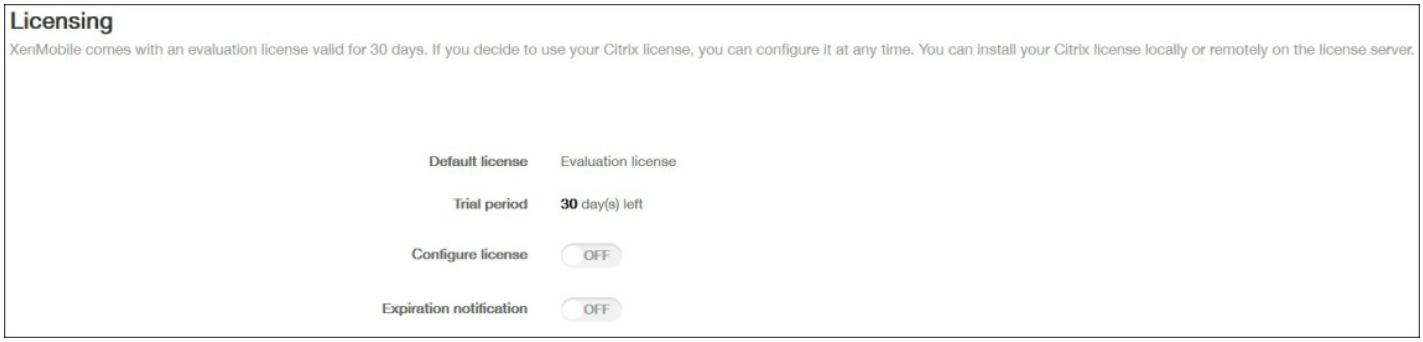




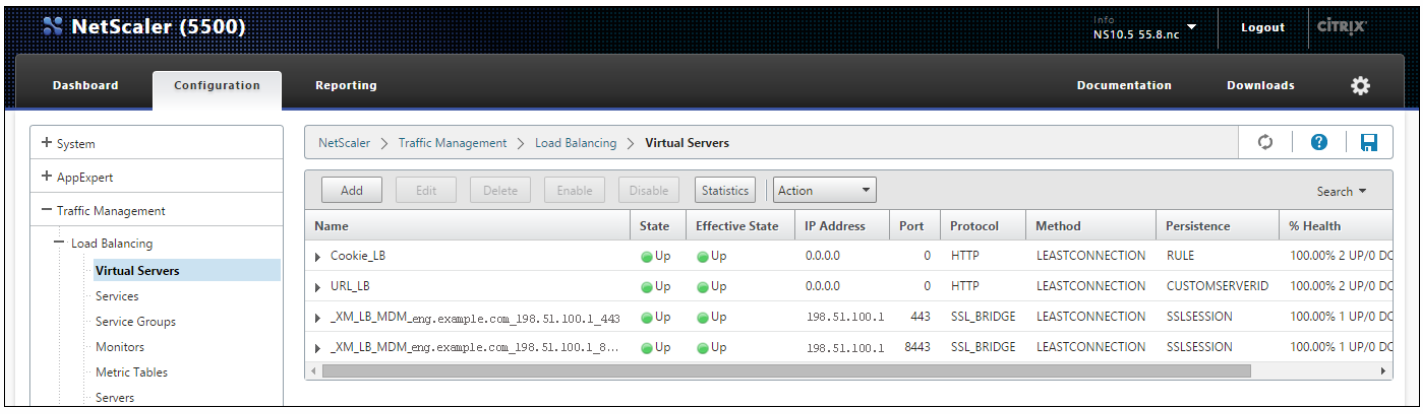


Nachbereitung eines Upgrades

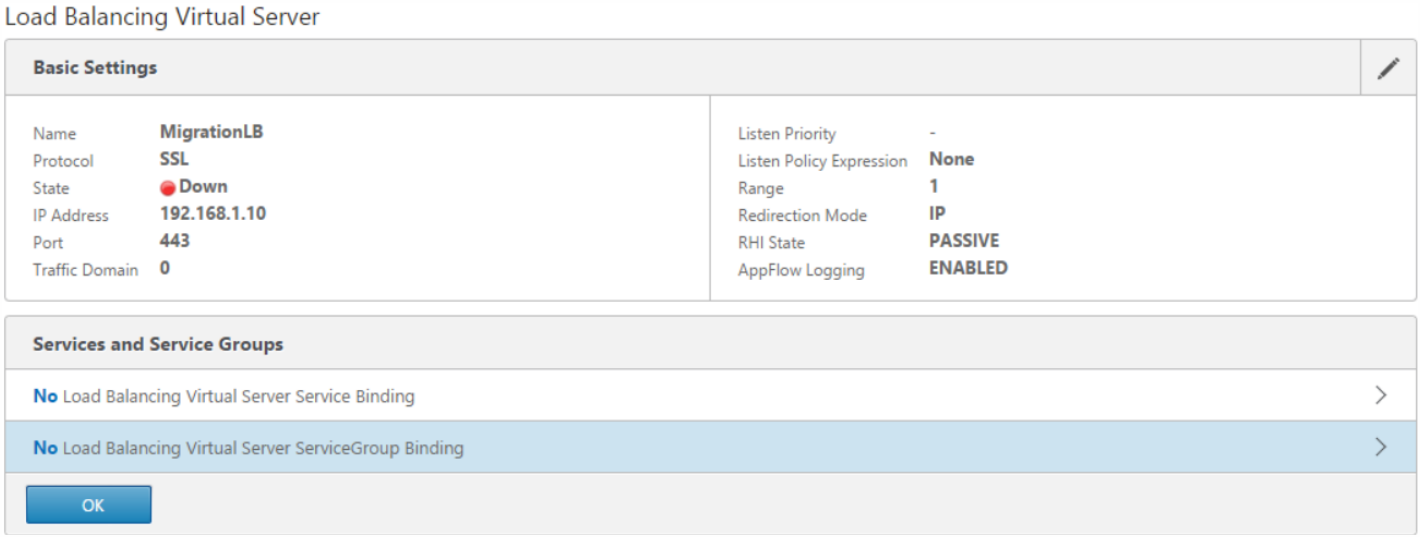


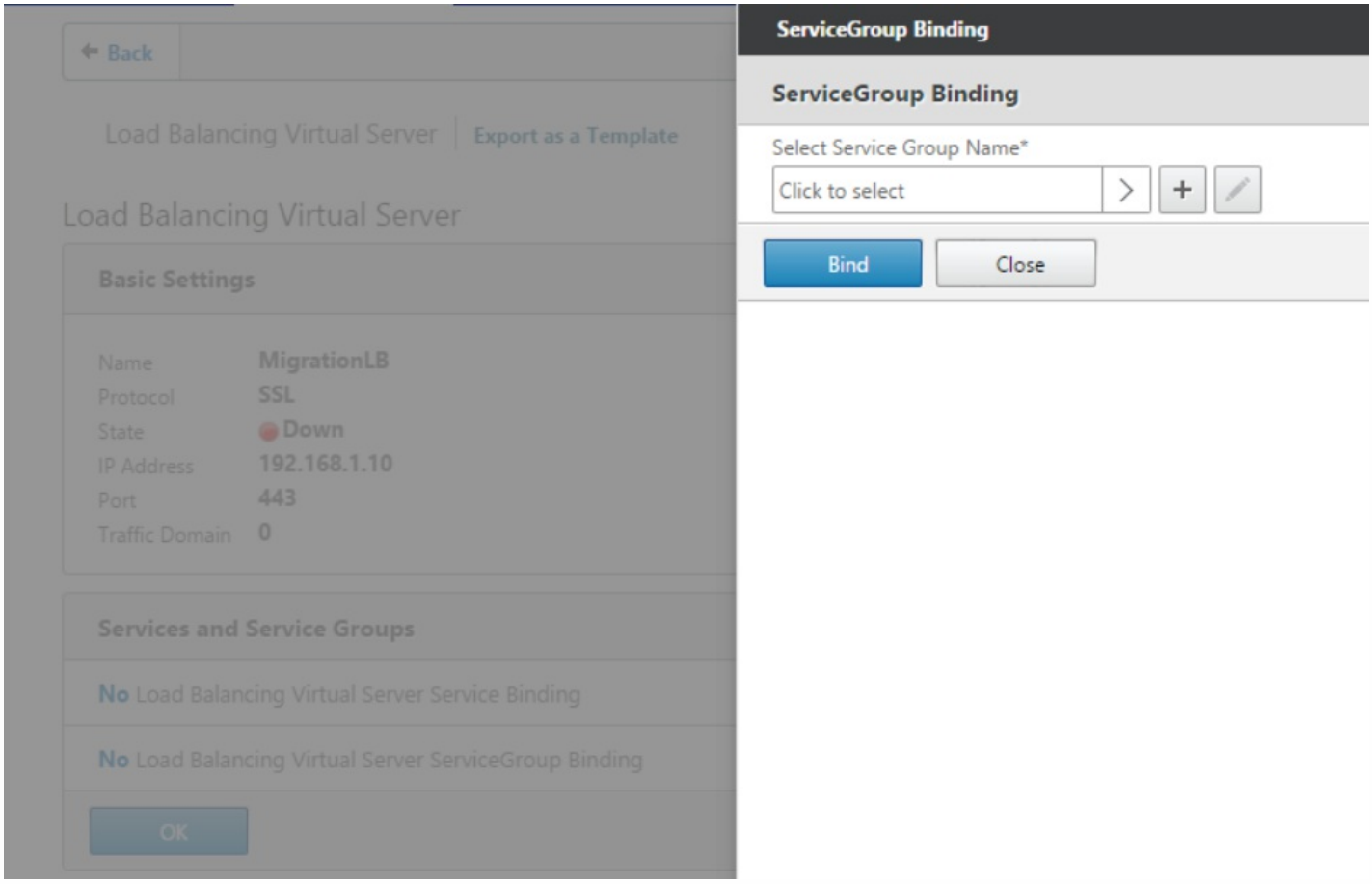


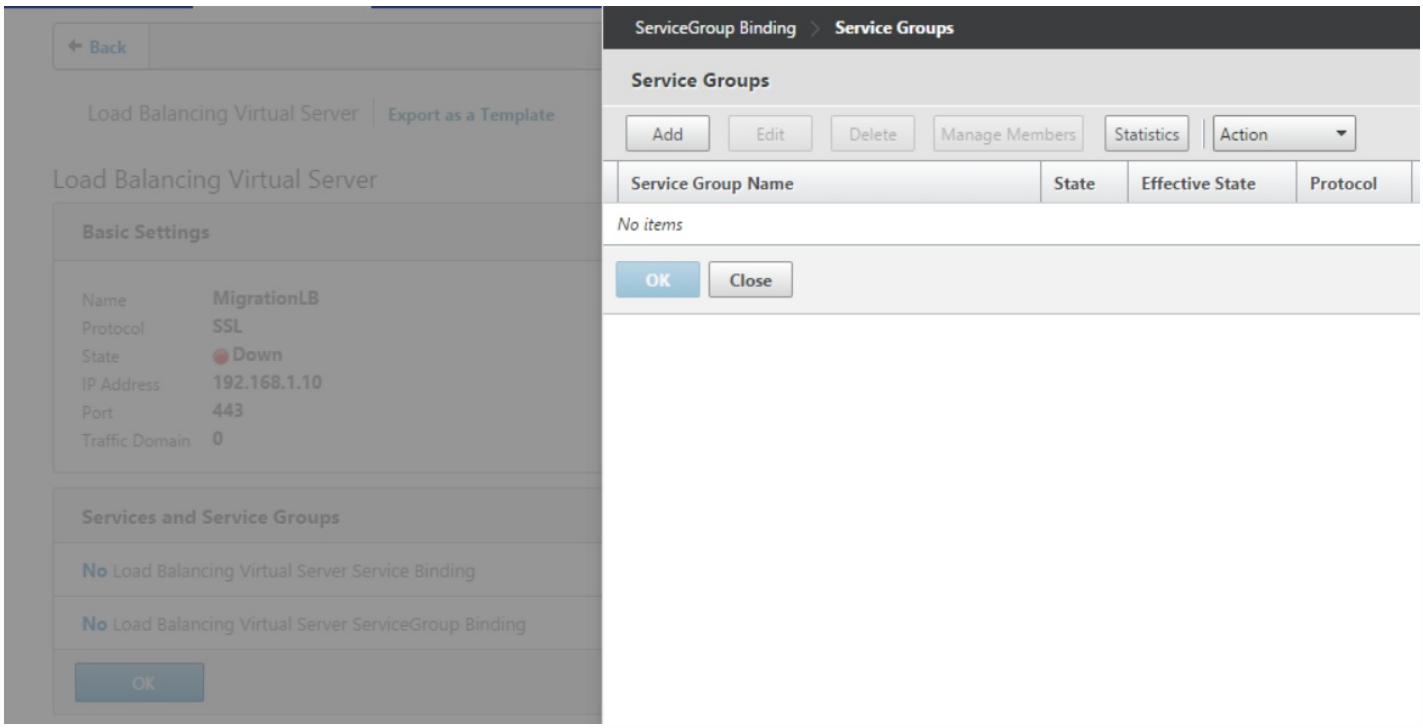
Hinweis

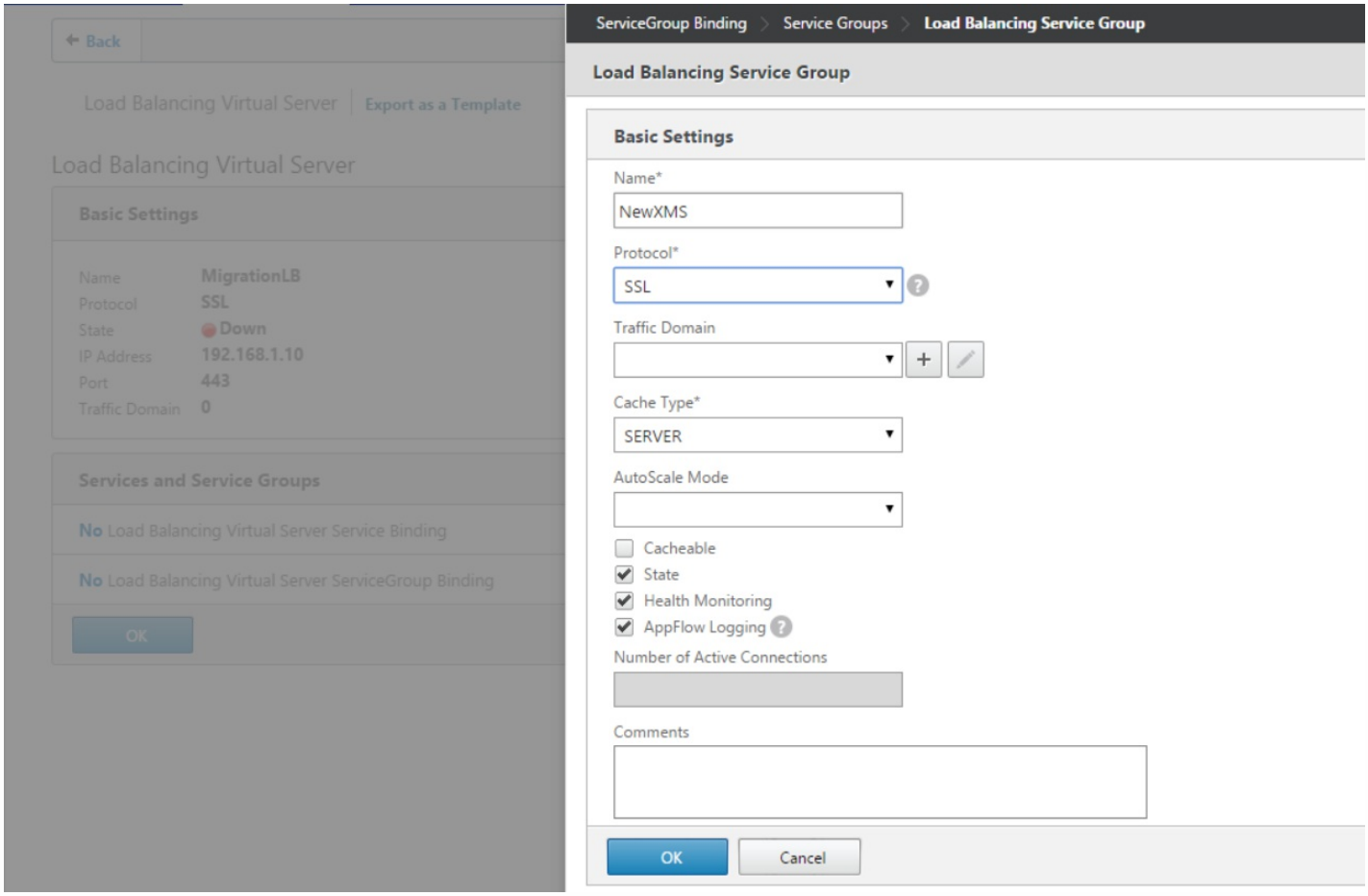


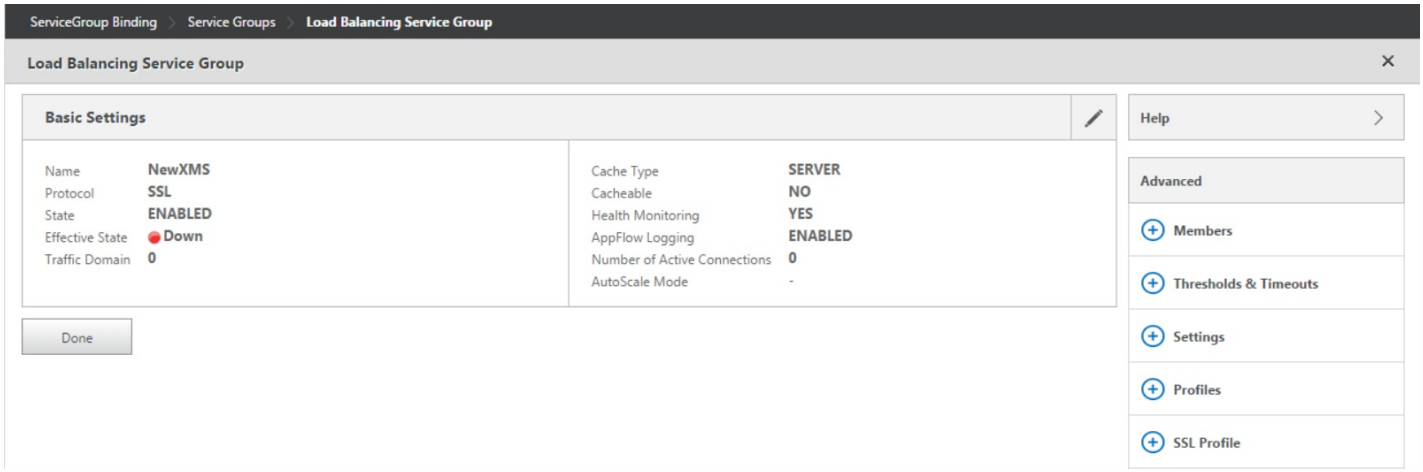
-
-
-
-

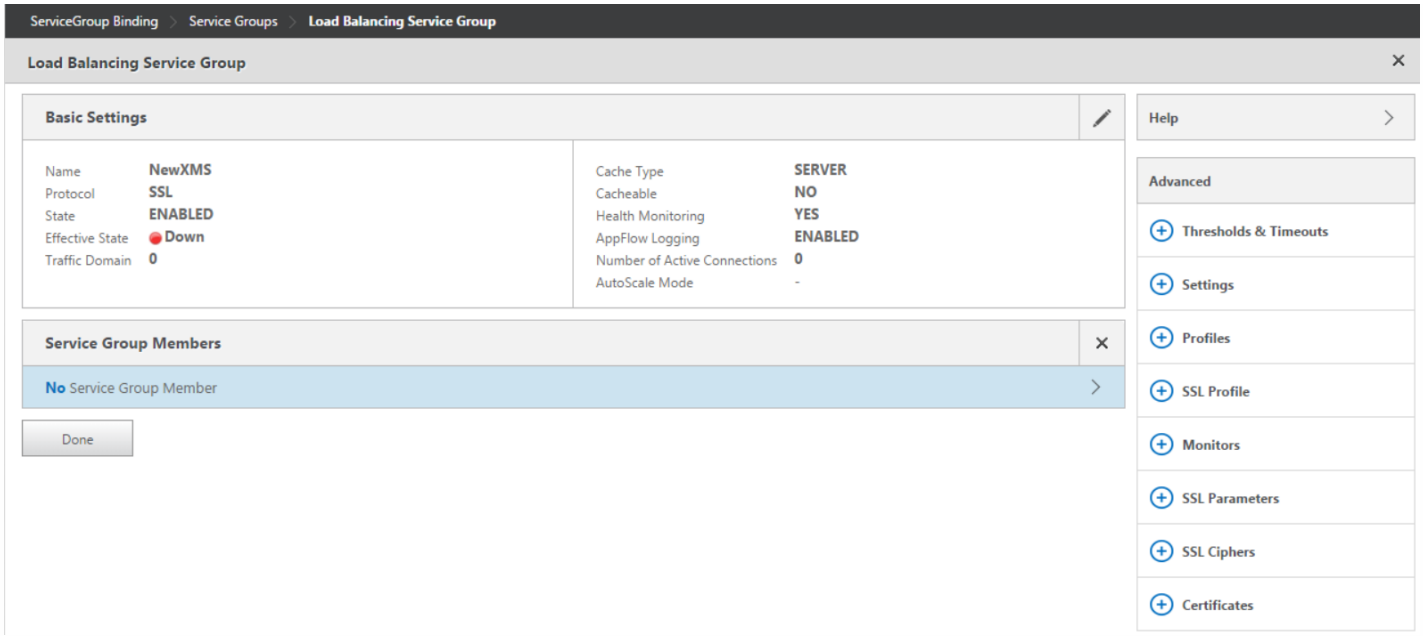








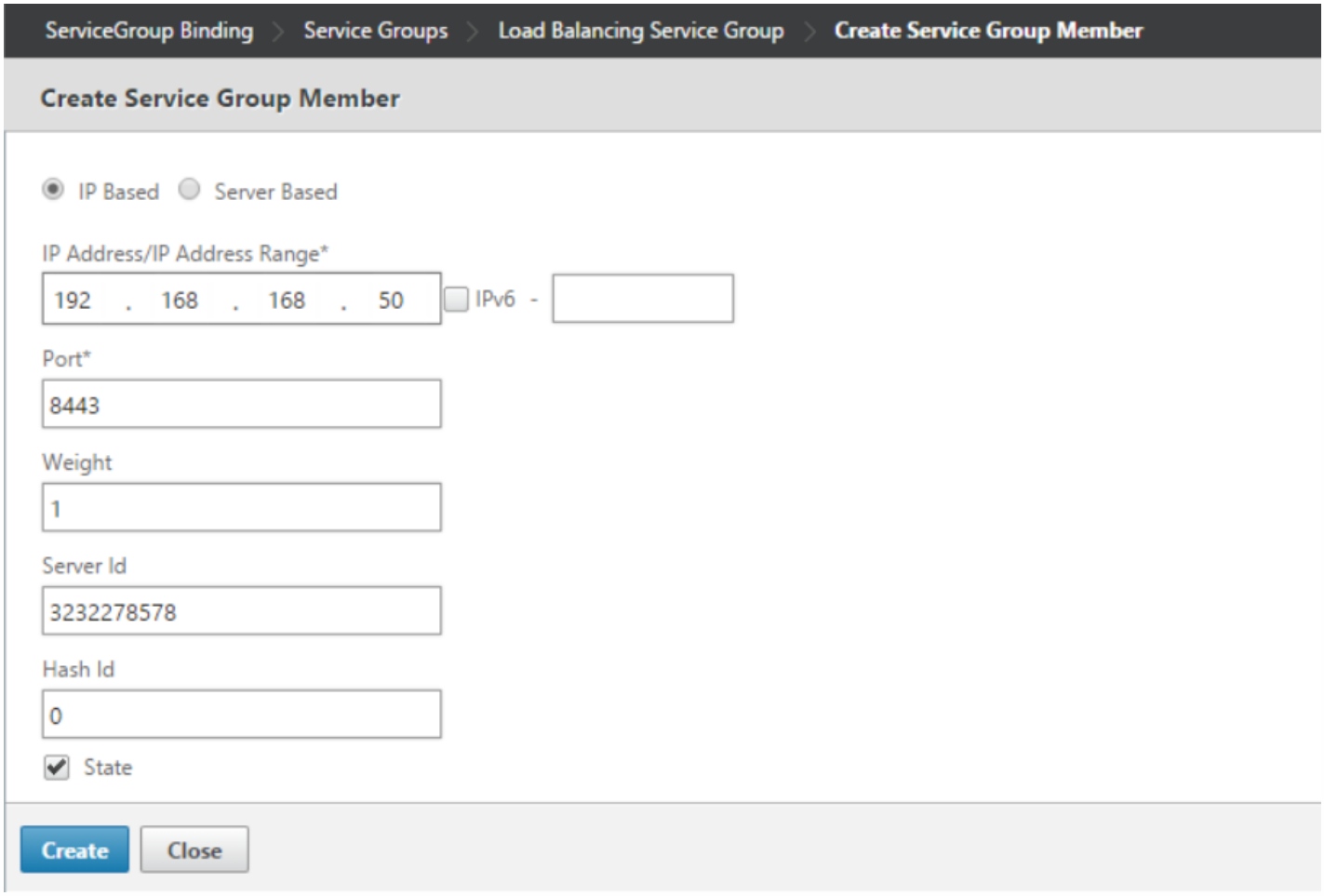


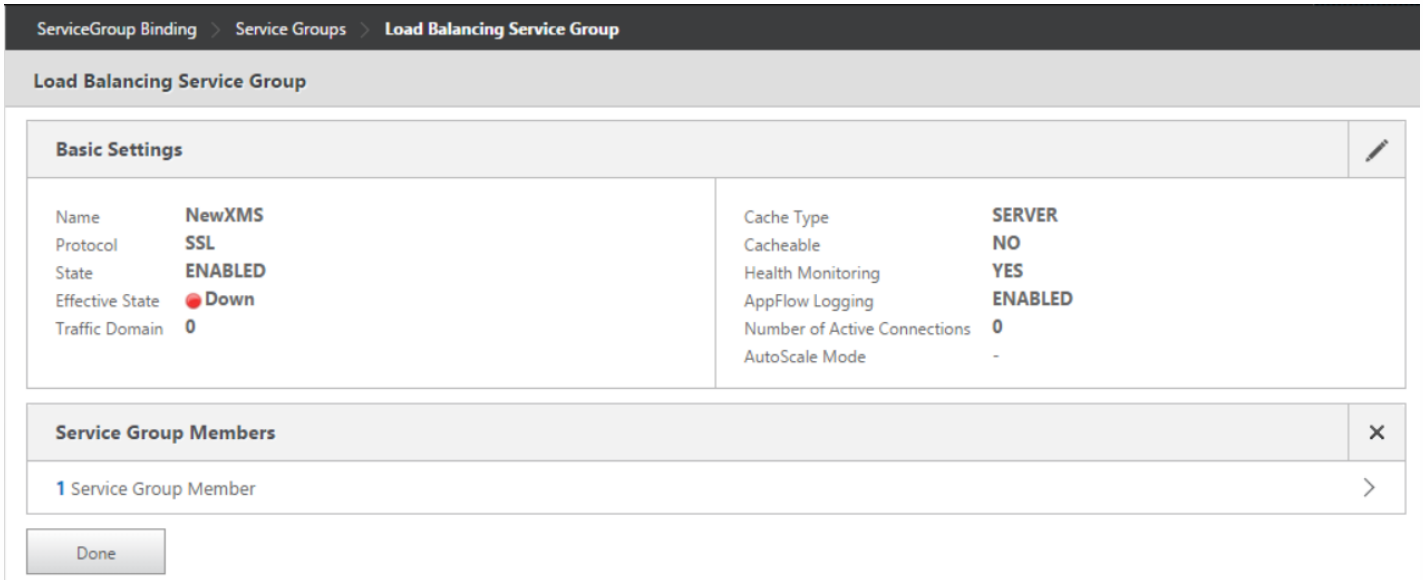


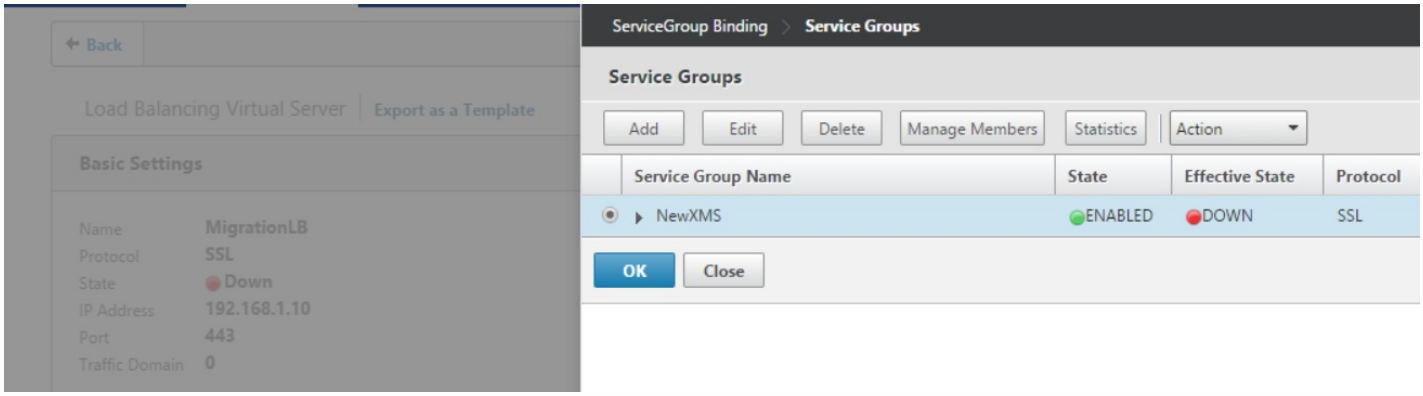
-
-
-

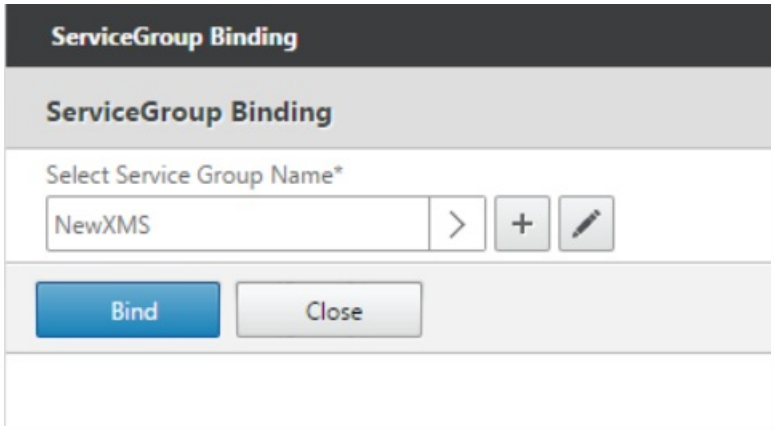
Hinweis

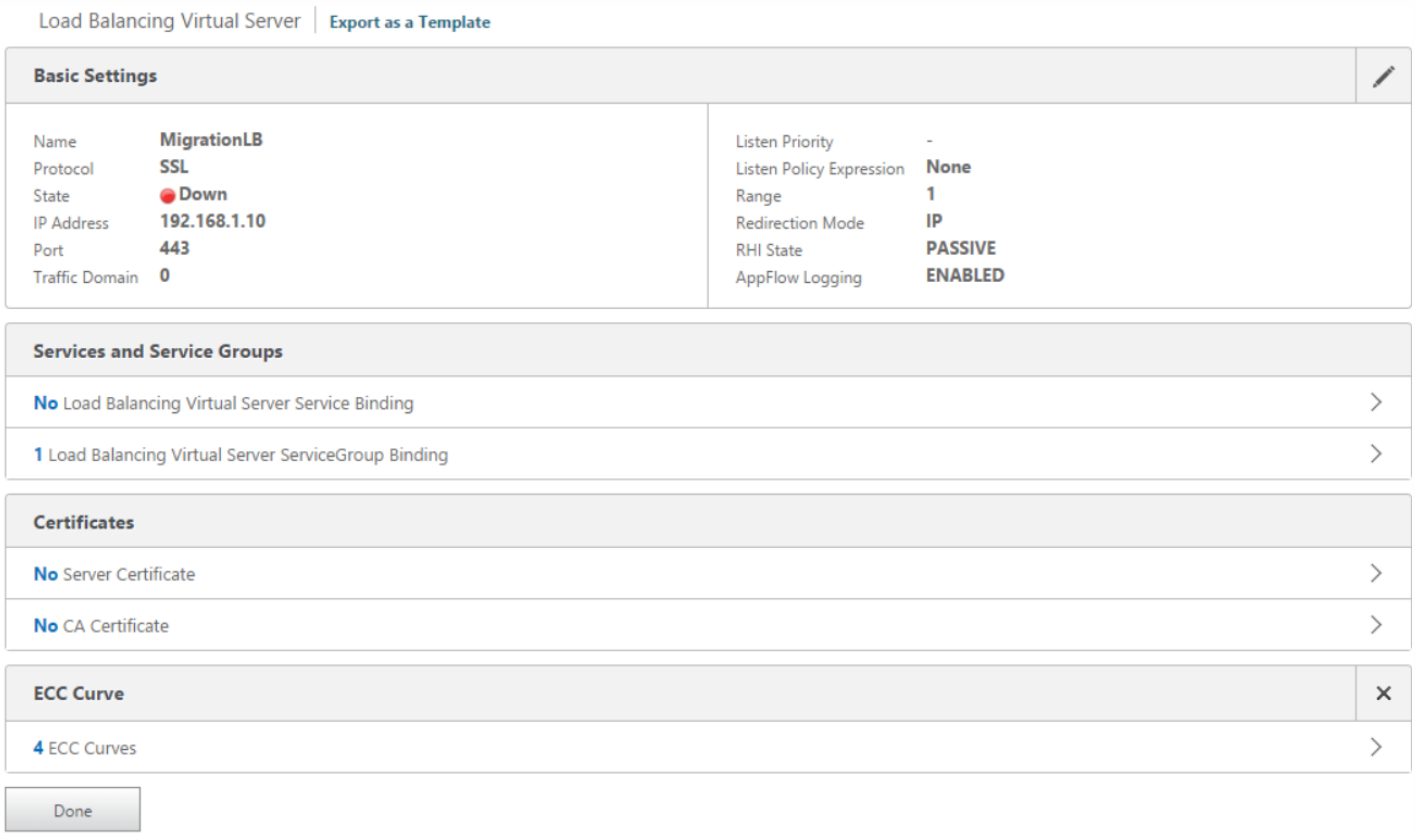
```
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----------------------------------
Choice: [0 - 5] 1

Current Node ID: 181356771

Cluster Members:
node: 192.0.2.0 status: ACTIVE  role: OLDEST


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

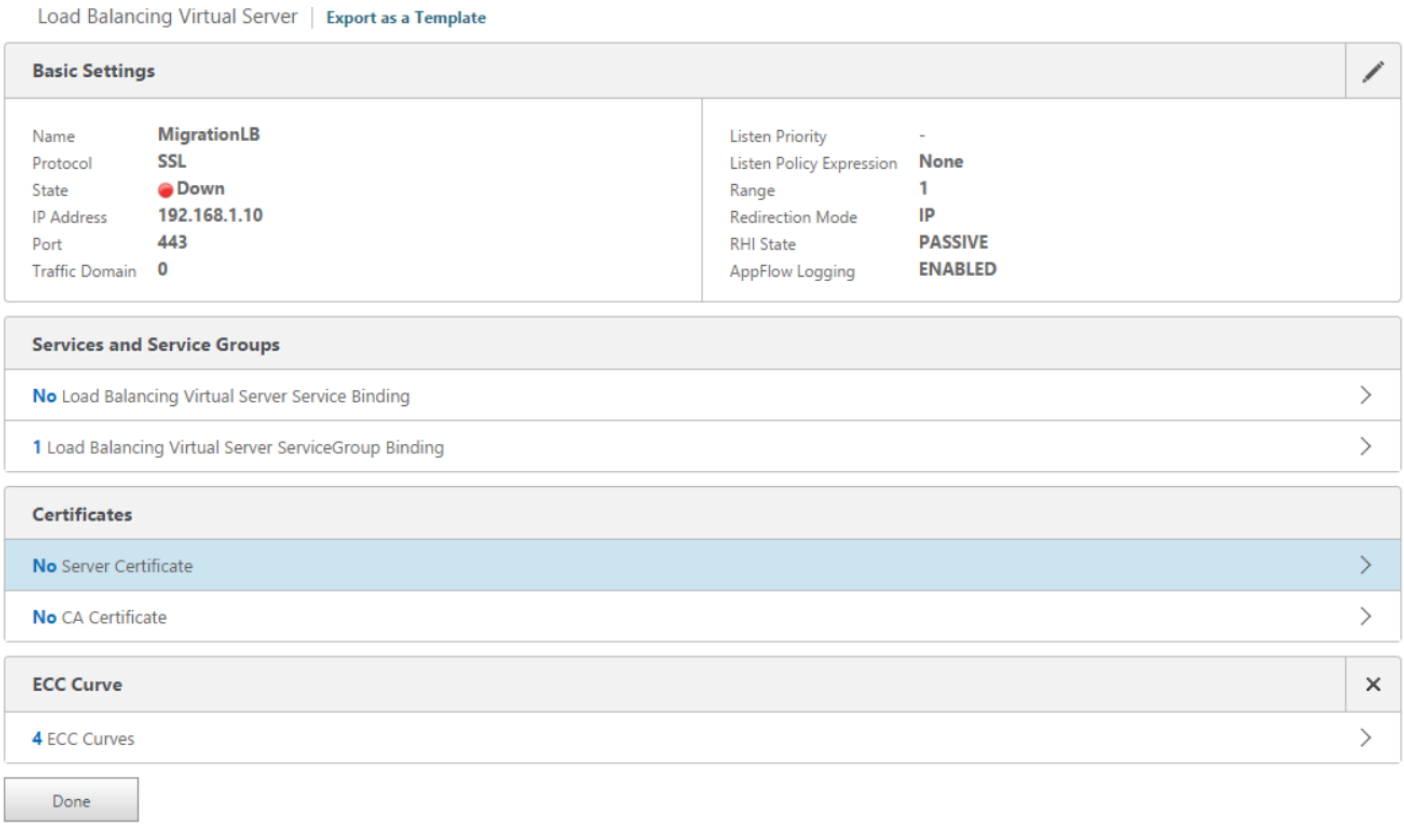


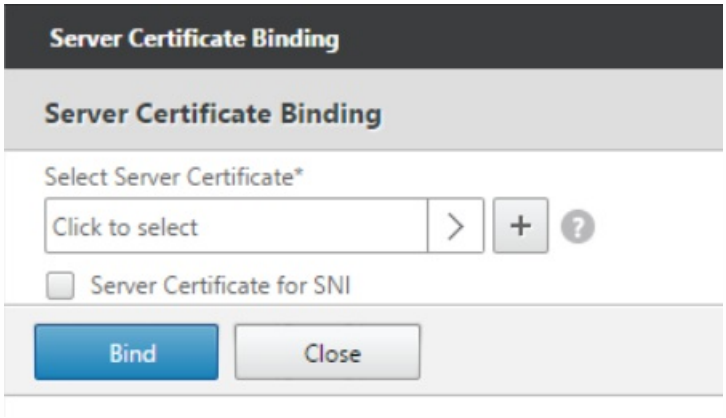


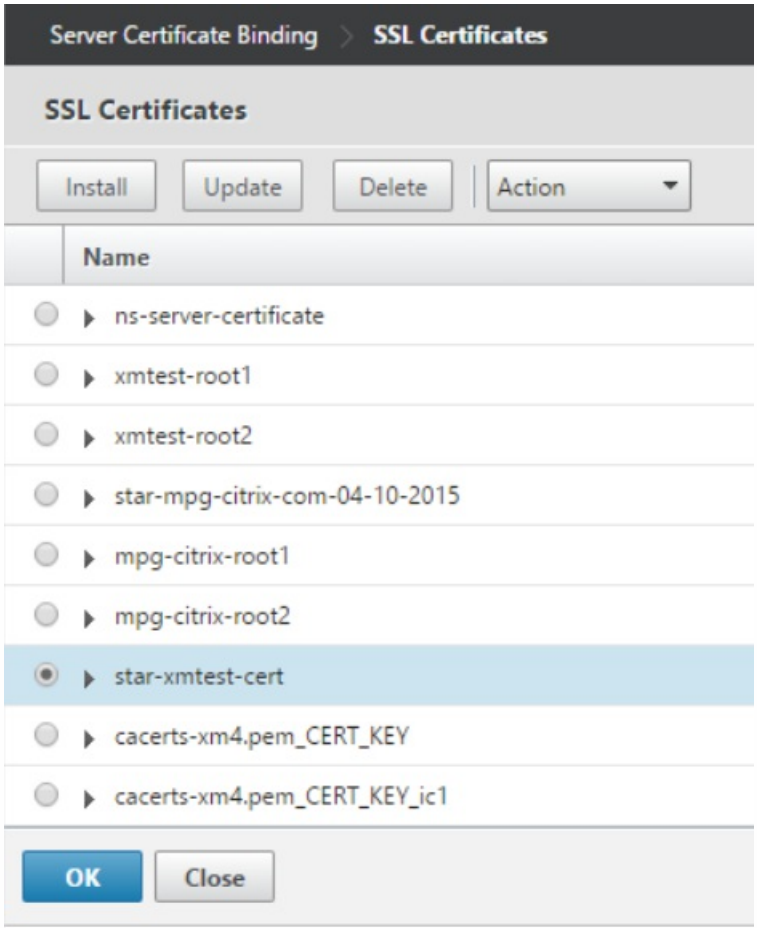


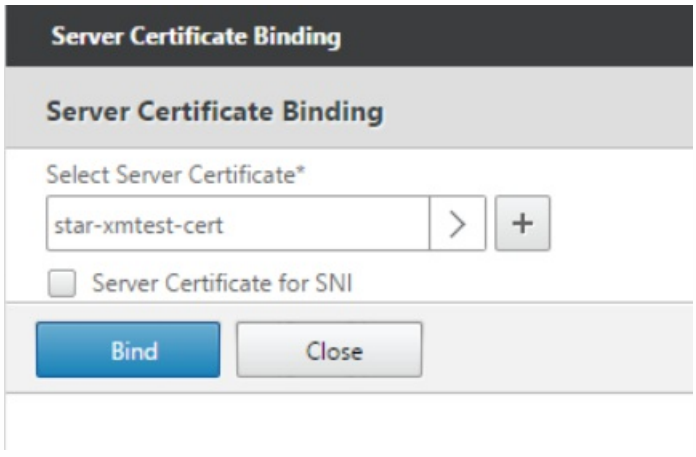












Load Balancing Virtual Server | Export as a Template

Basic Settings

Name	MigrationLB	Listen Priority	-
Protocol	SSL	Listen Policy Expression	None
State	Down	Range	1
IP Address	192.168.1.10	Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED

Services and Service Groups

No Load Balancing Virtual Server Service Binding

1 Load Balancing Virtual Server ServiceGroup Binding

Certificates

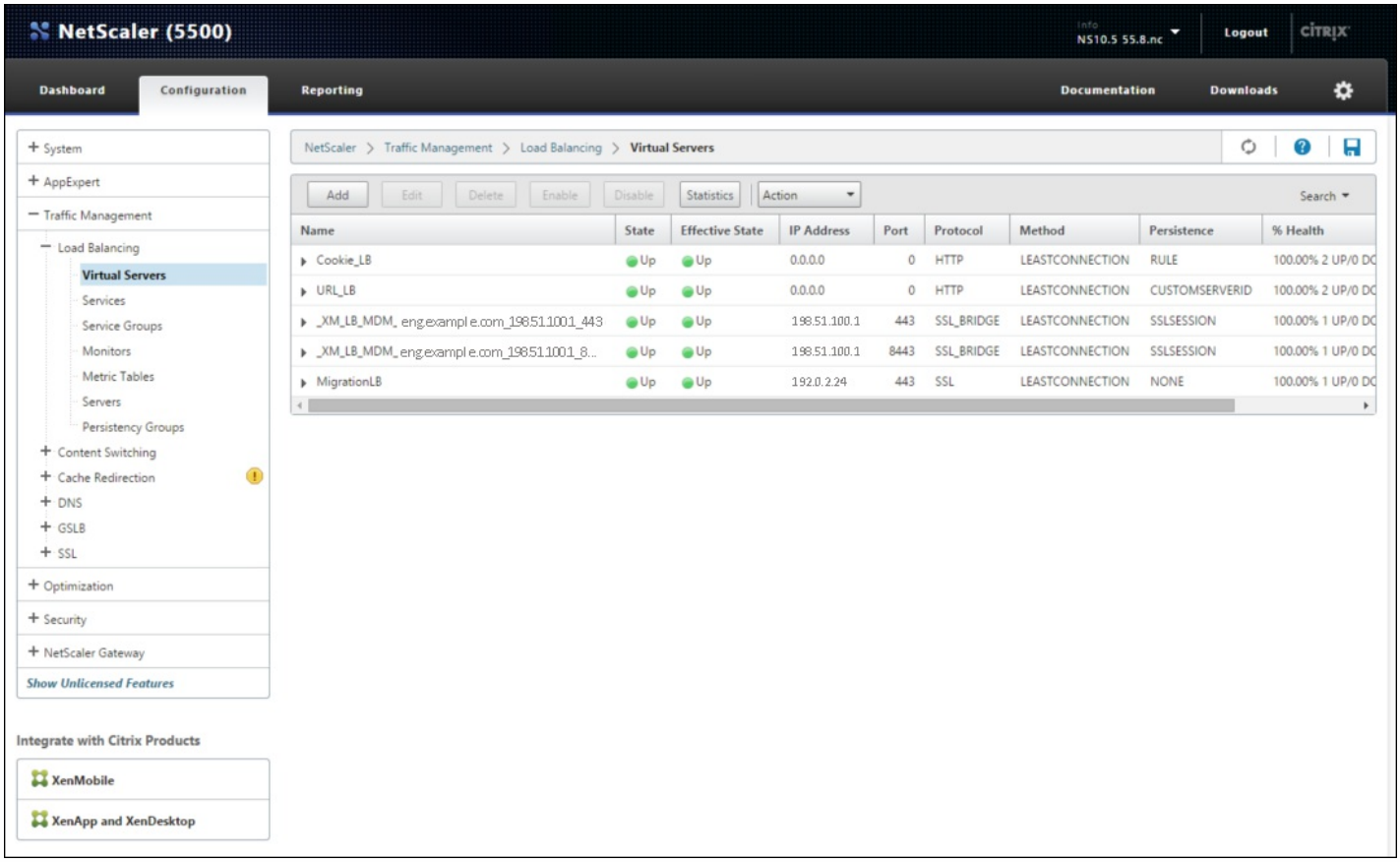
1 Server Certificate

No CA Certificate

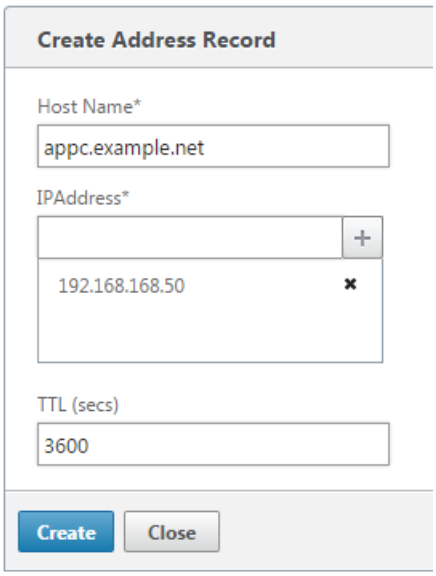
ECC Curve

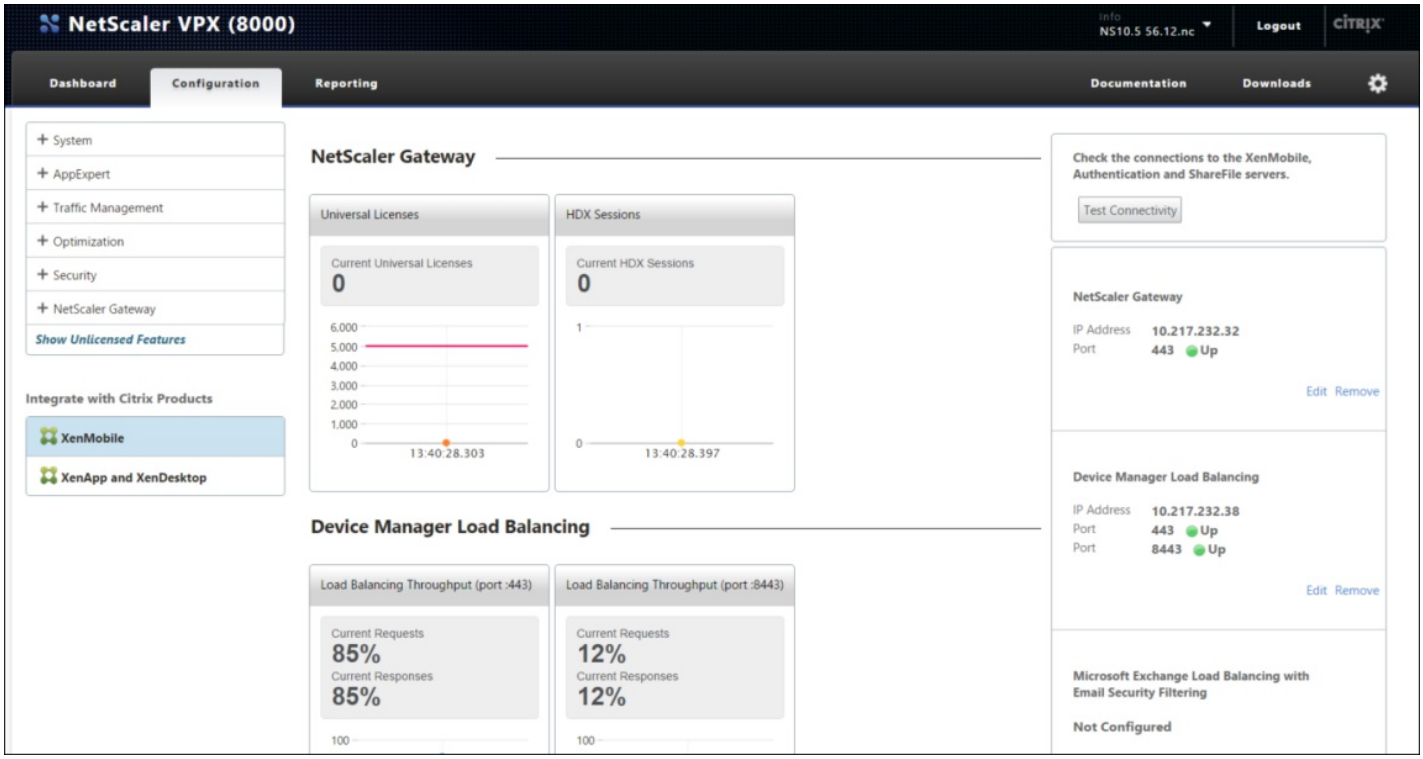
4 ECC Curves

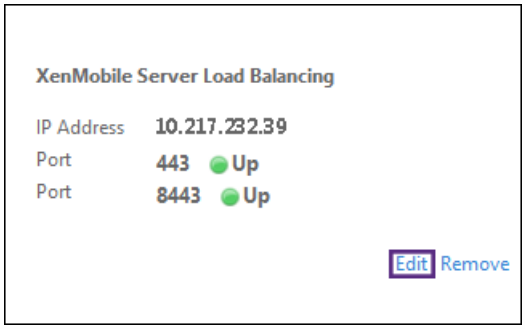
Done

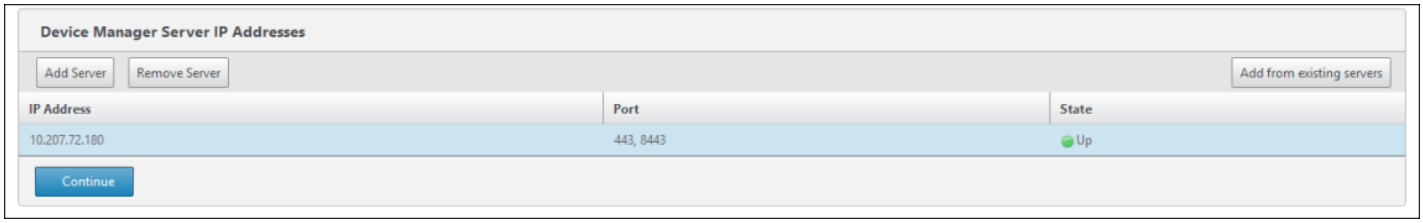


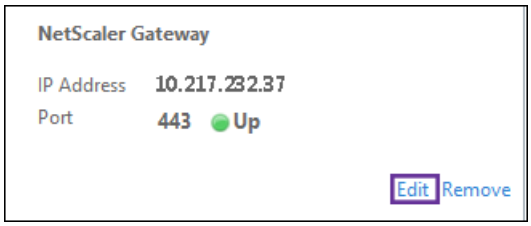
Hinweis

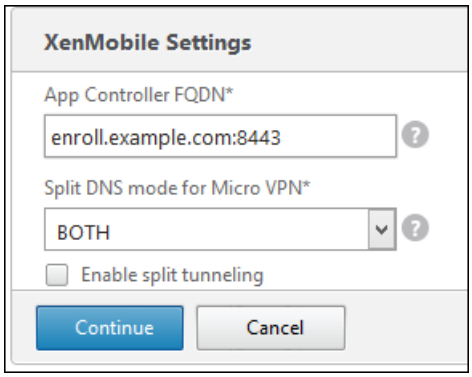


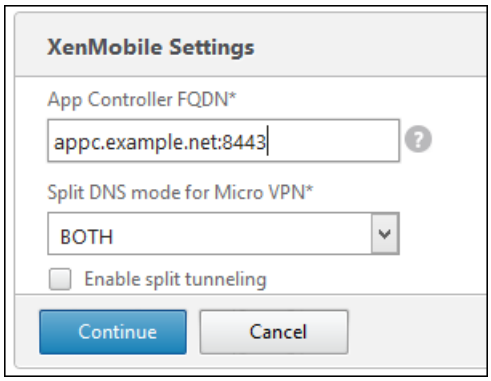


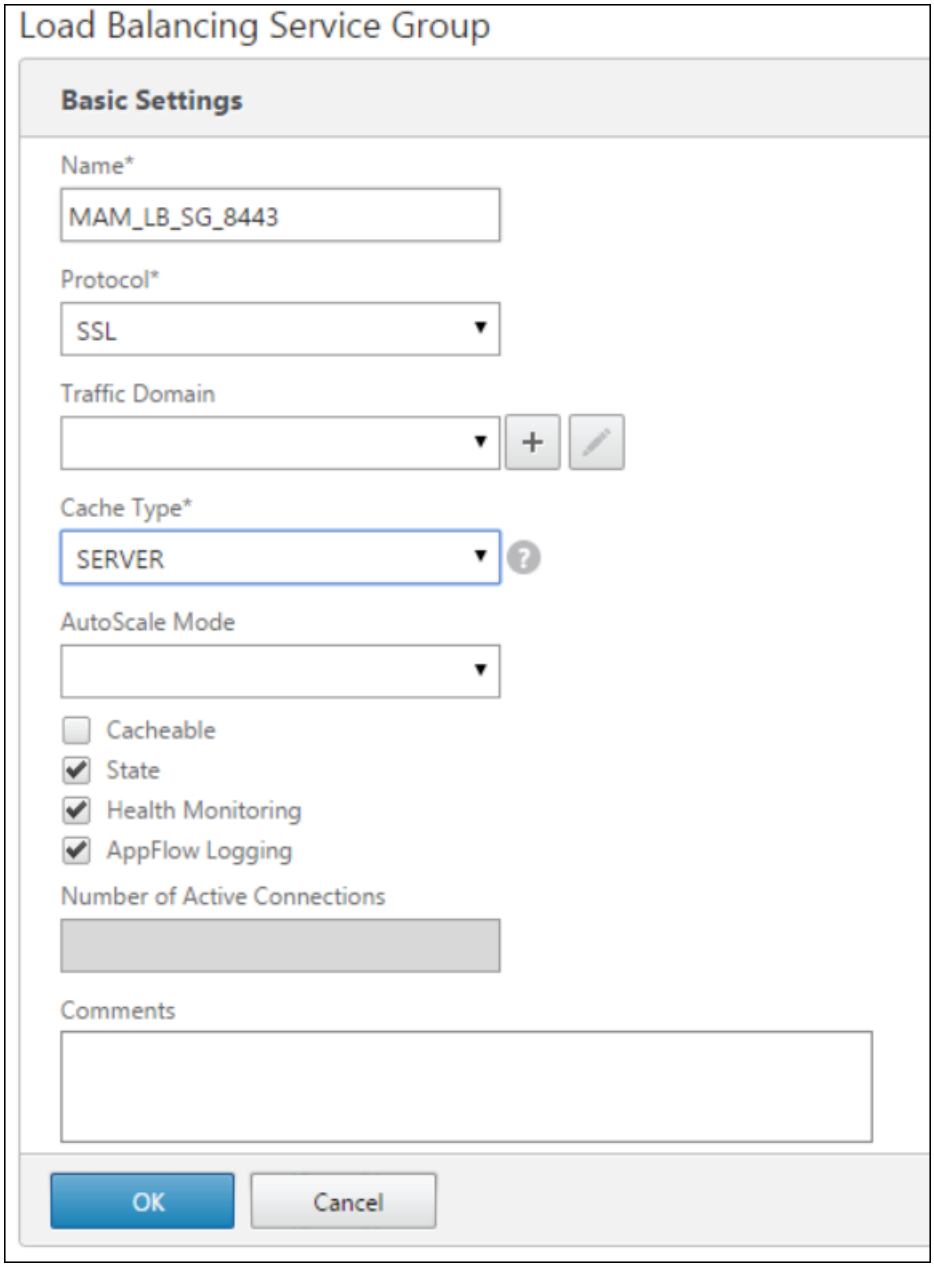


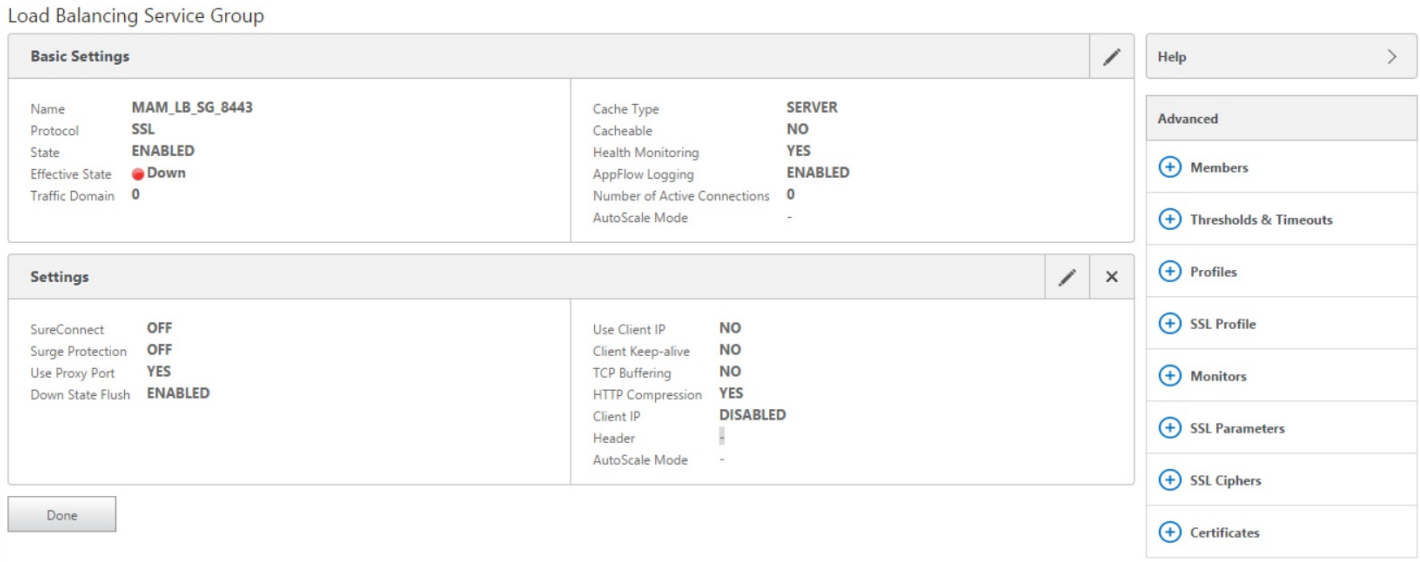


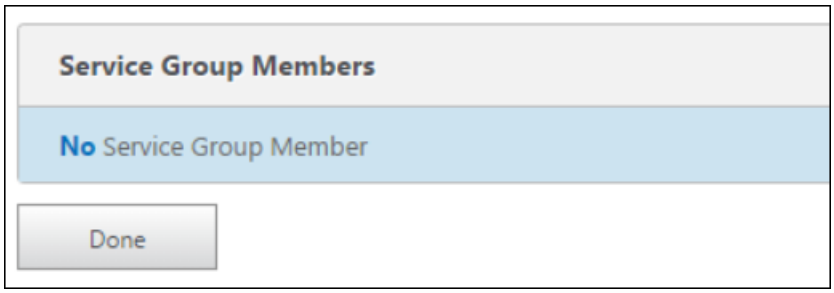


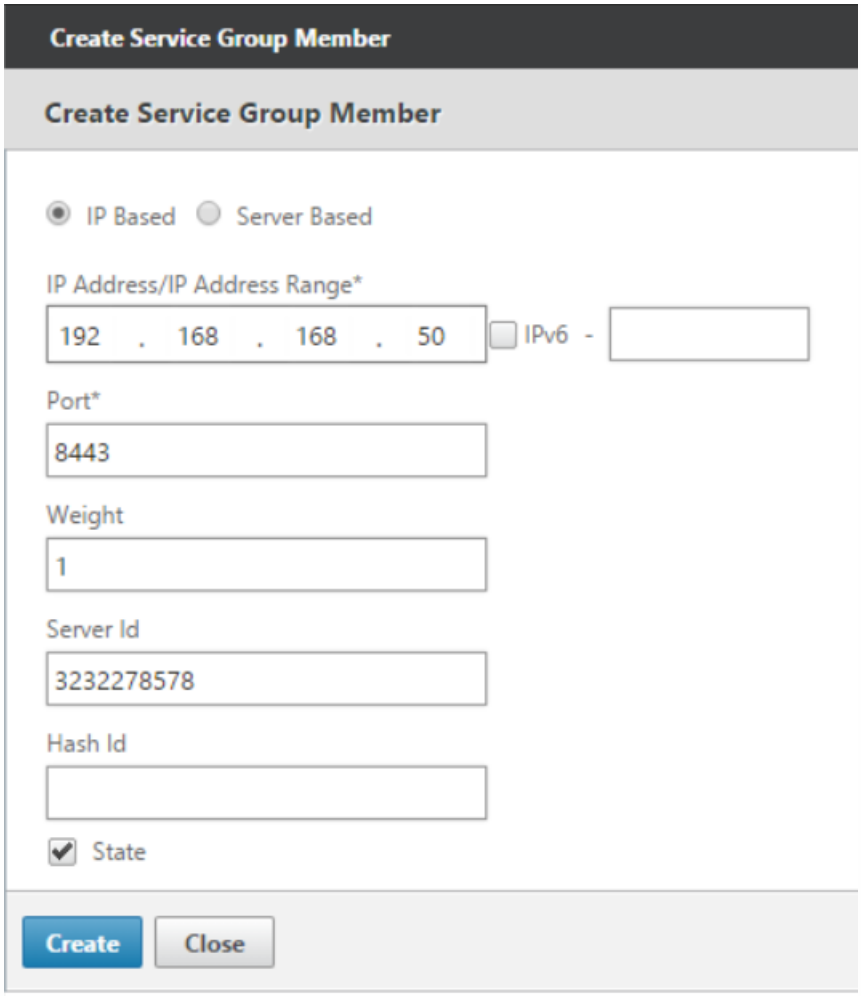






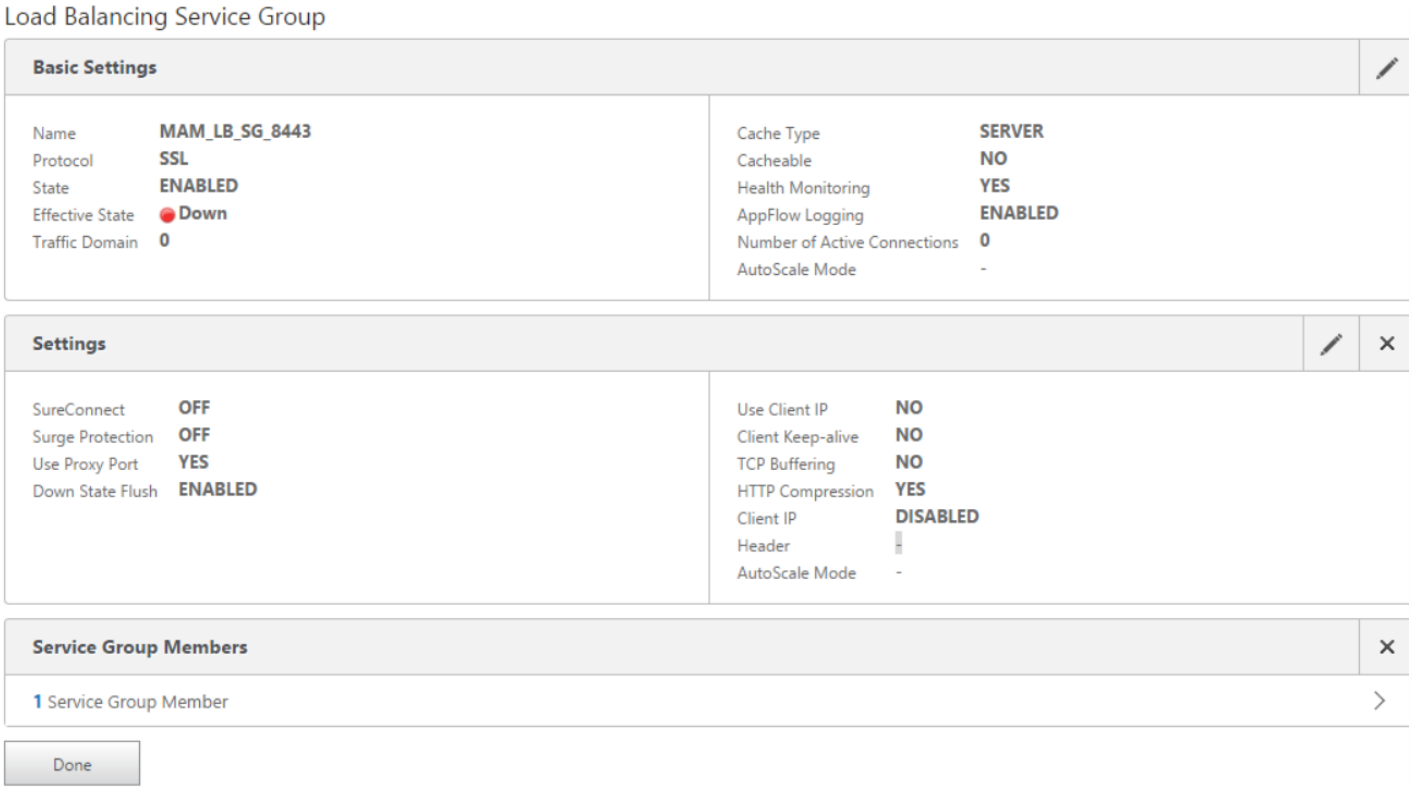




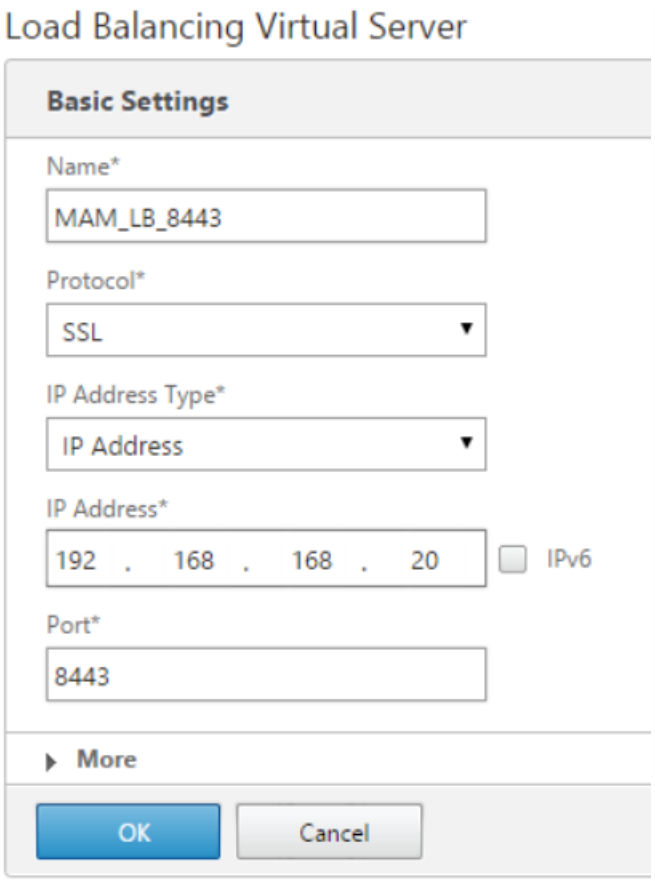


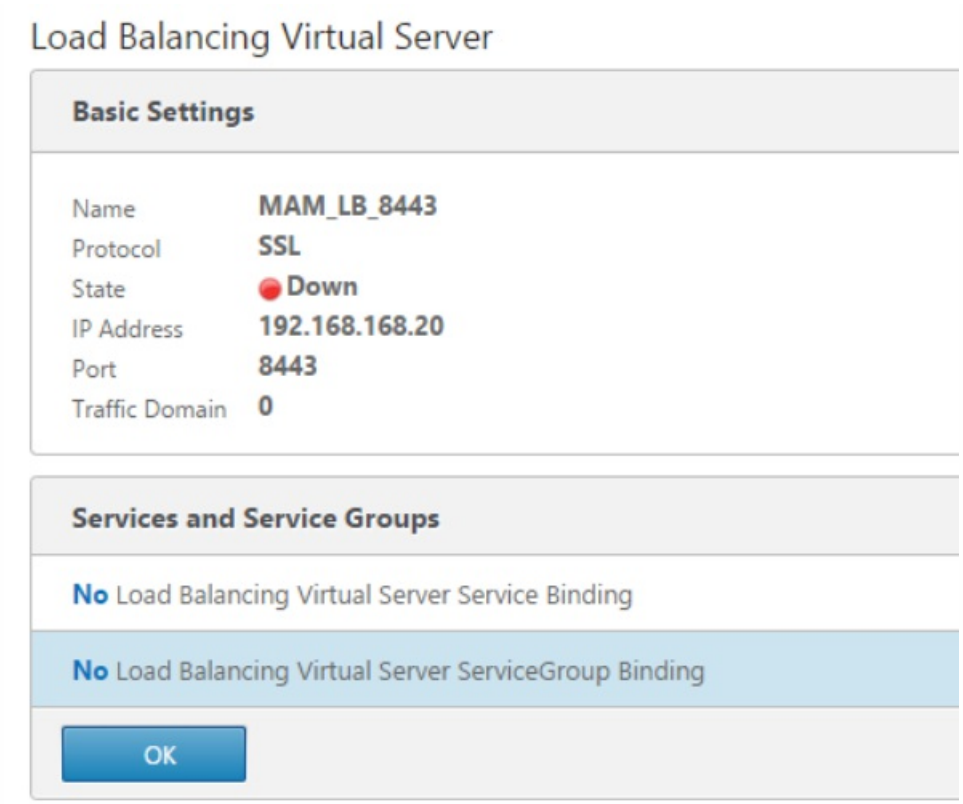
Hinweis

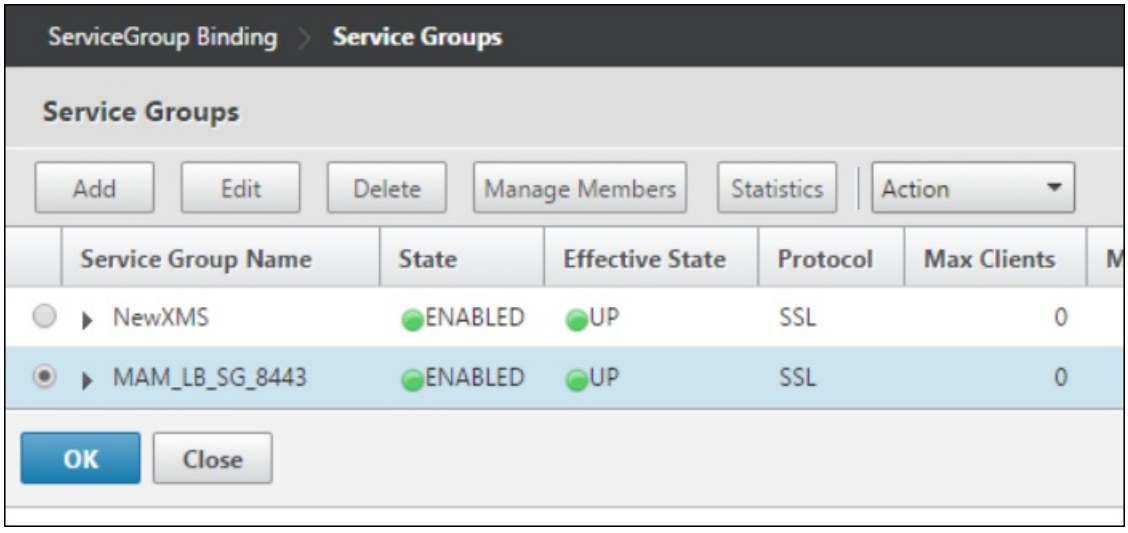
-
-

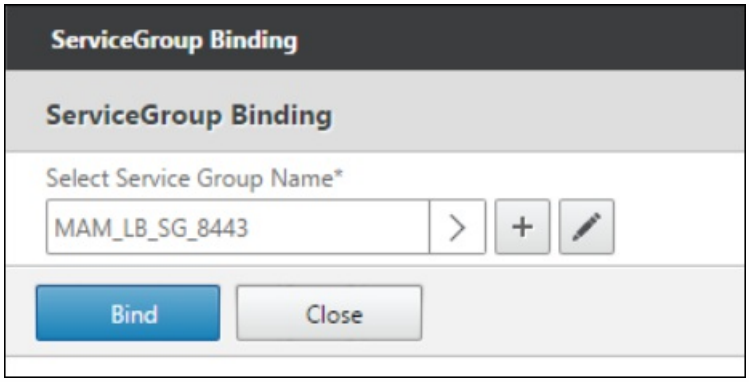


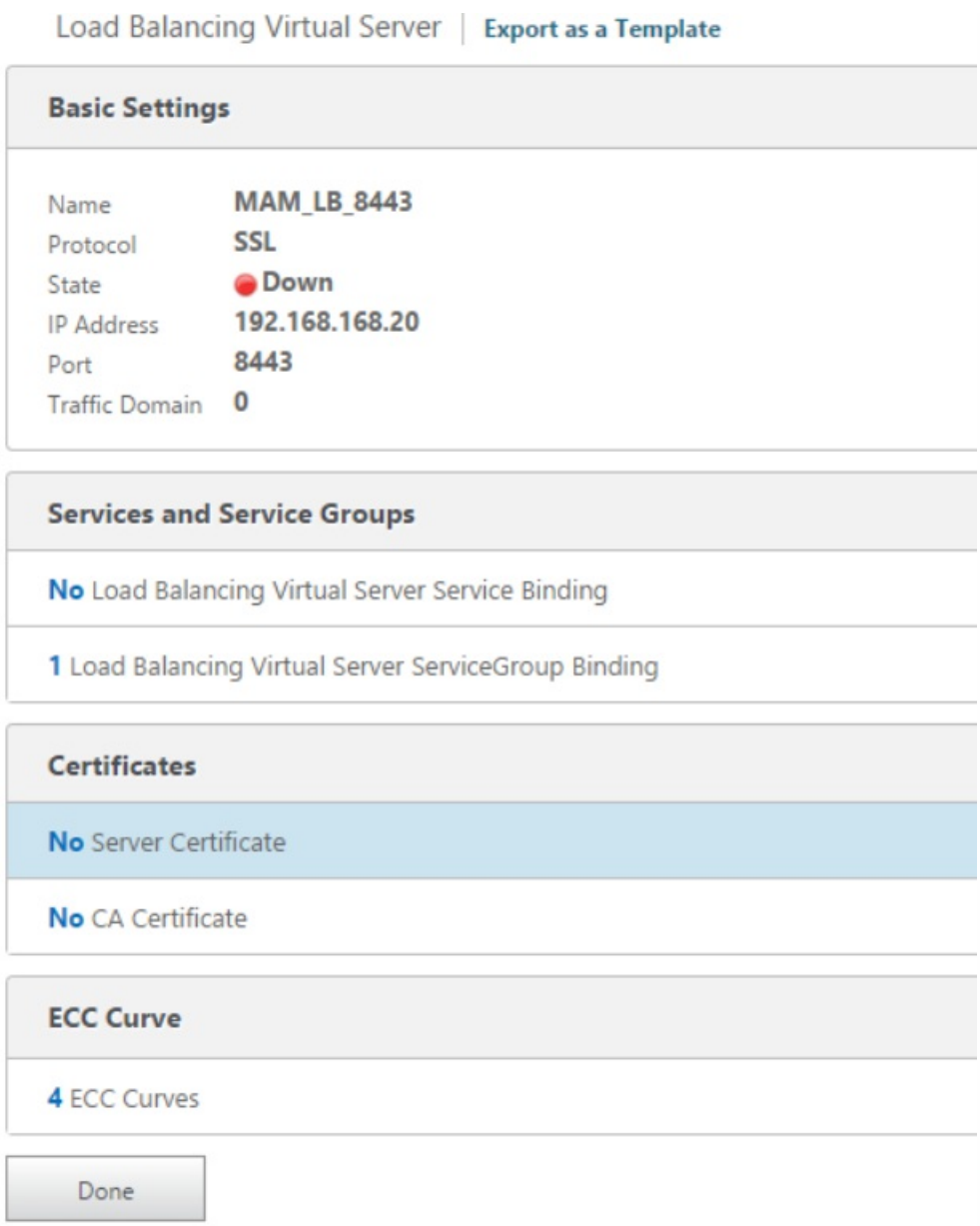
Hinweis

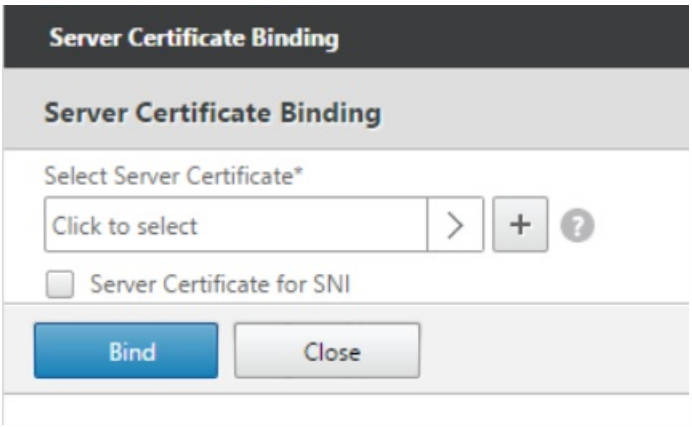


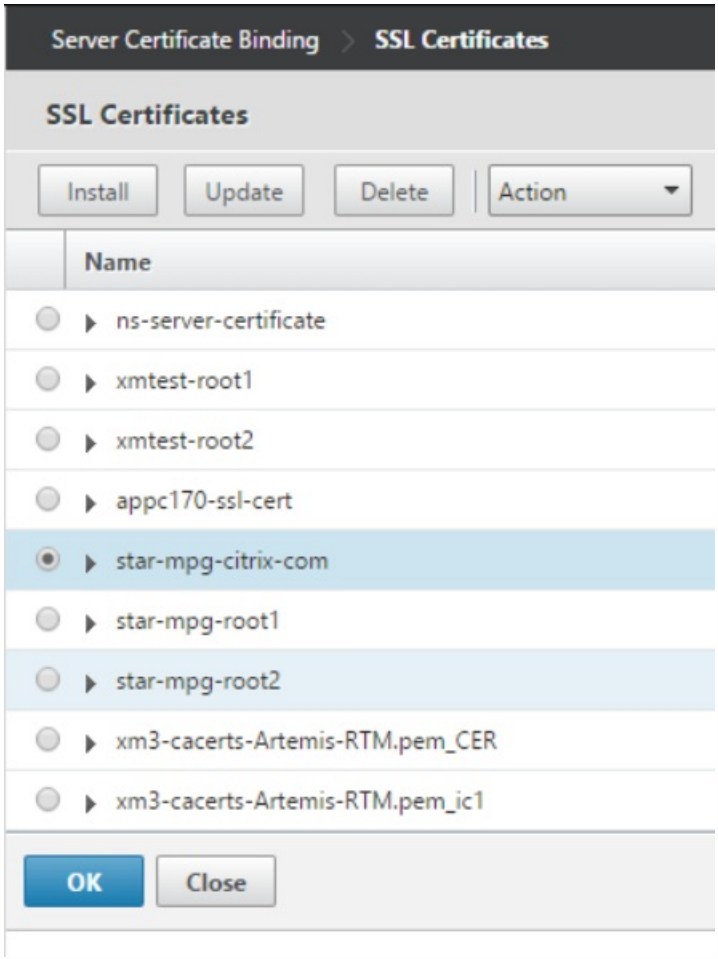


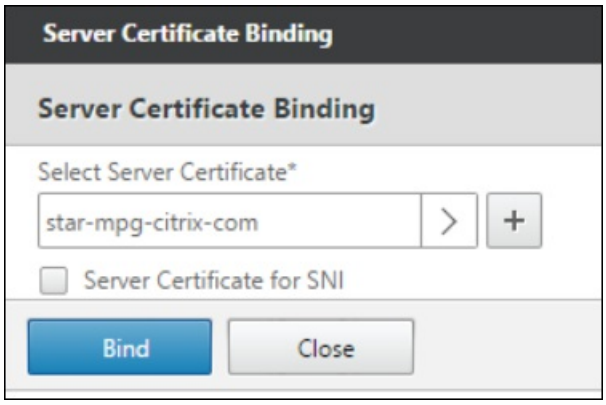


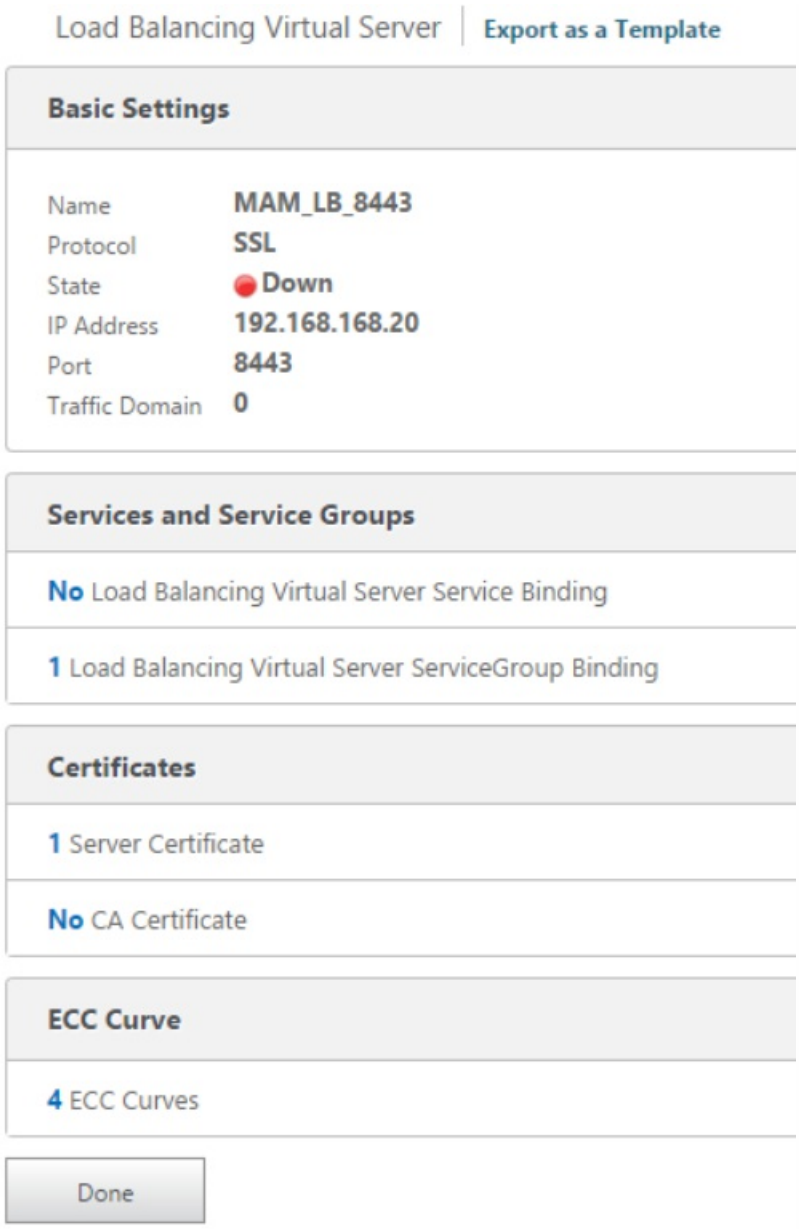


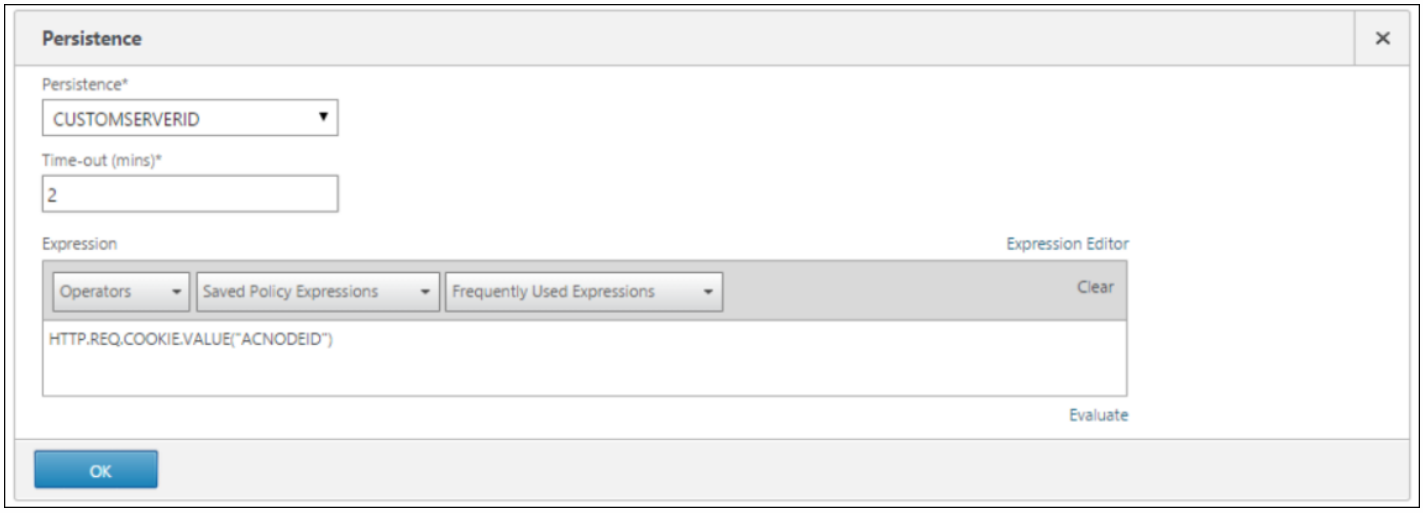




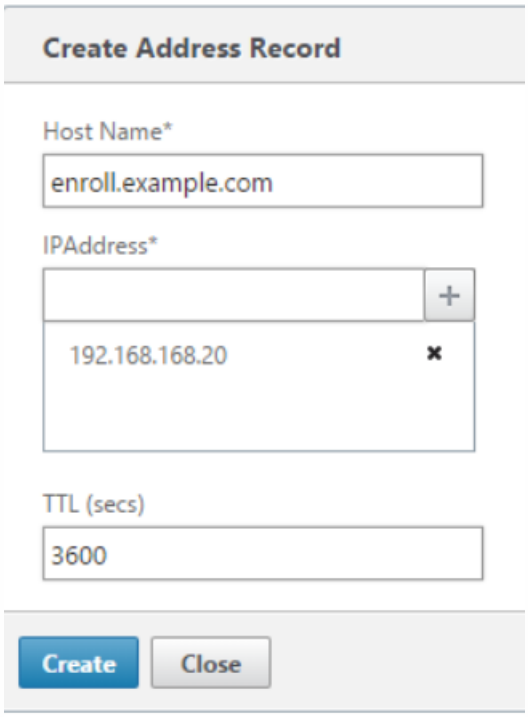


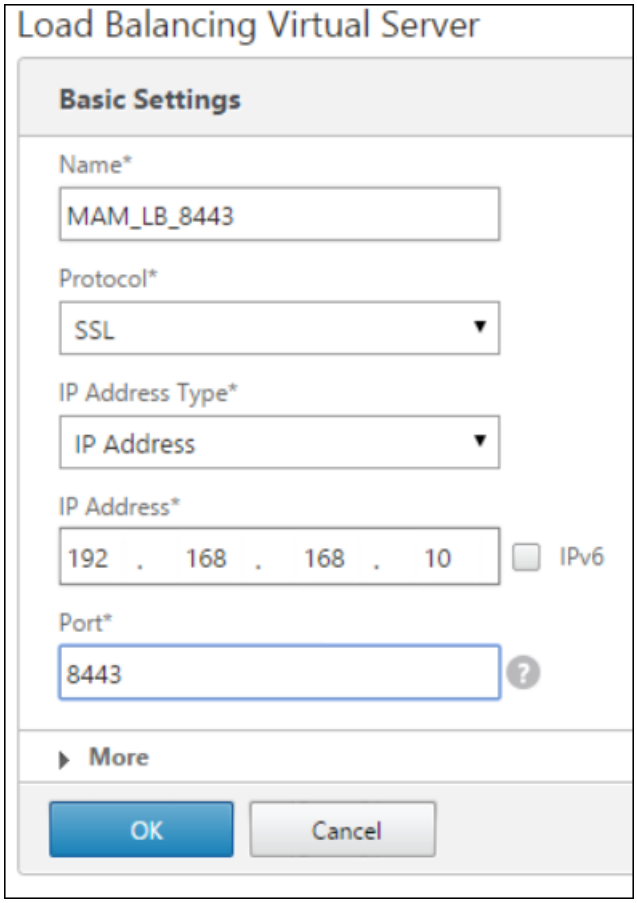


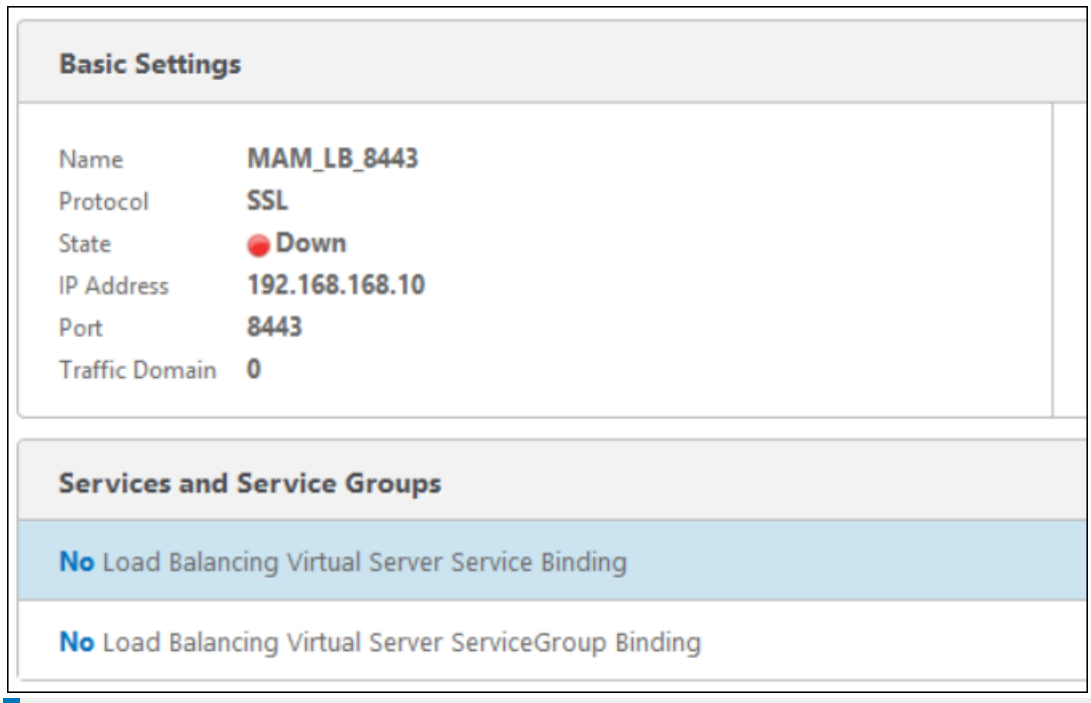




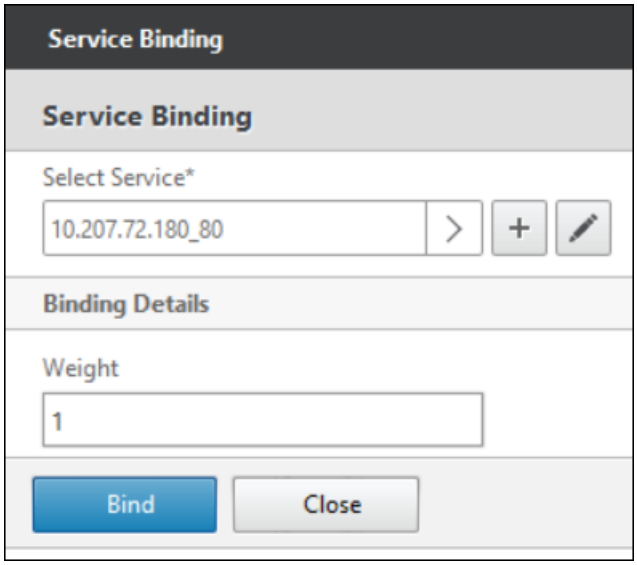
Hinweis

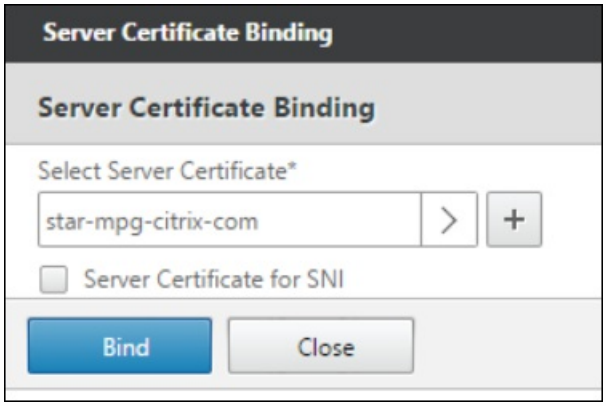


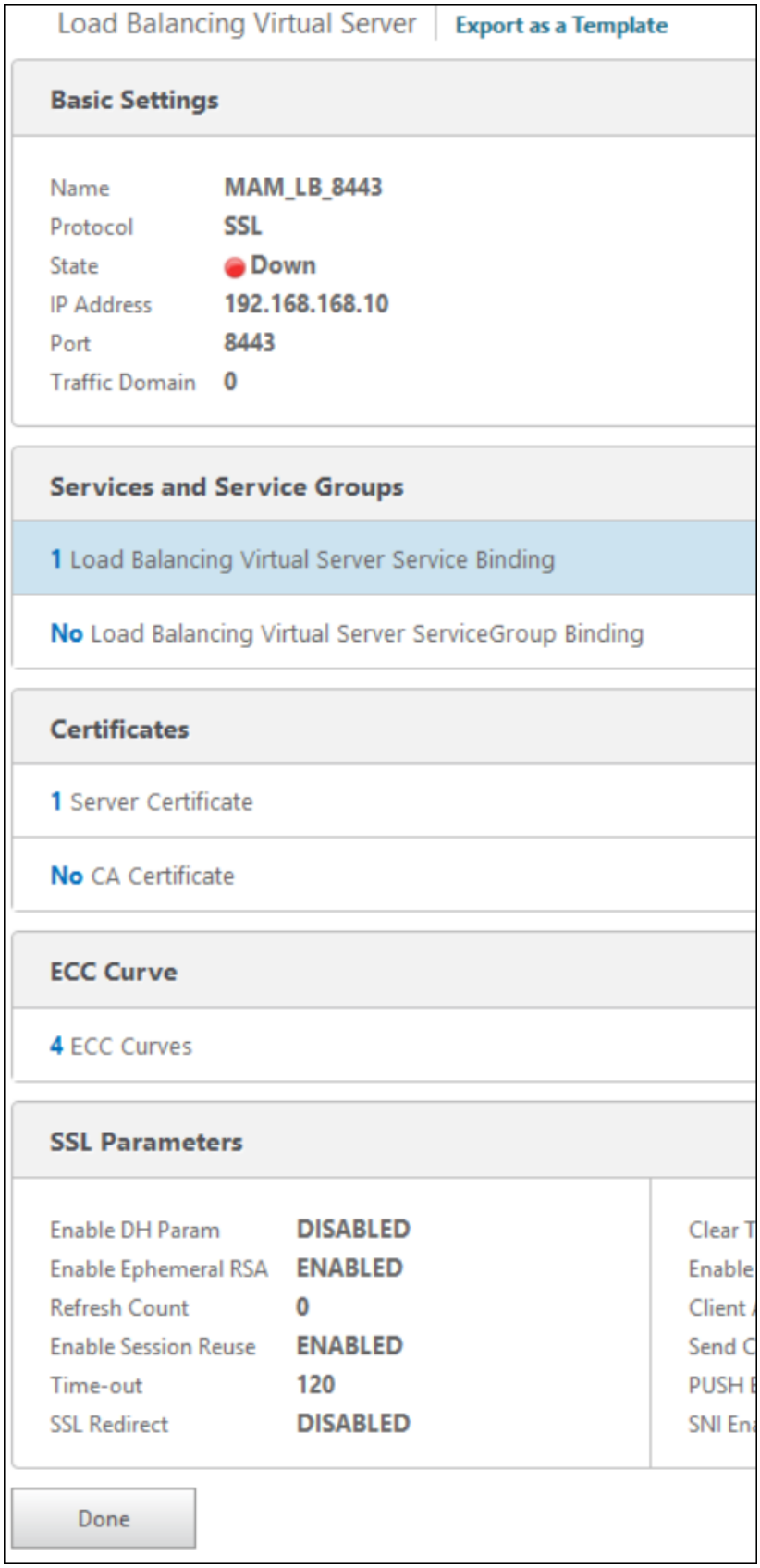


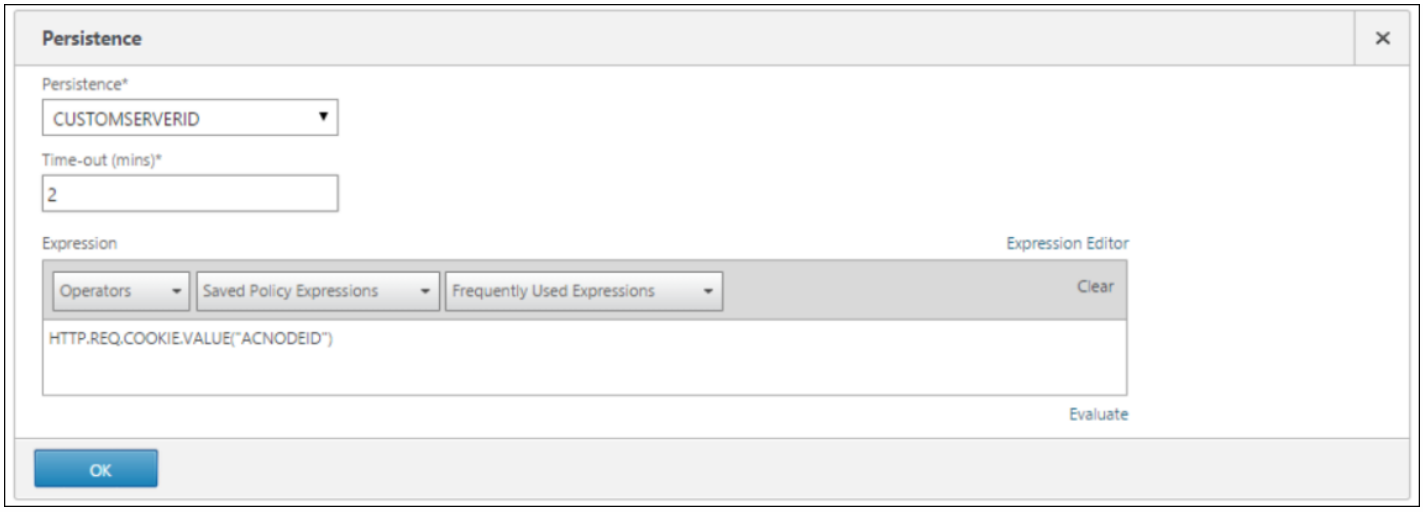


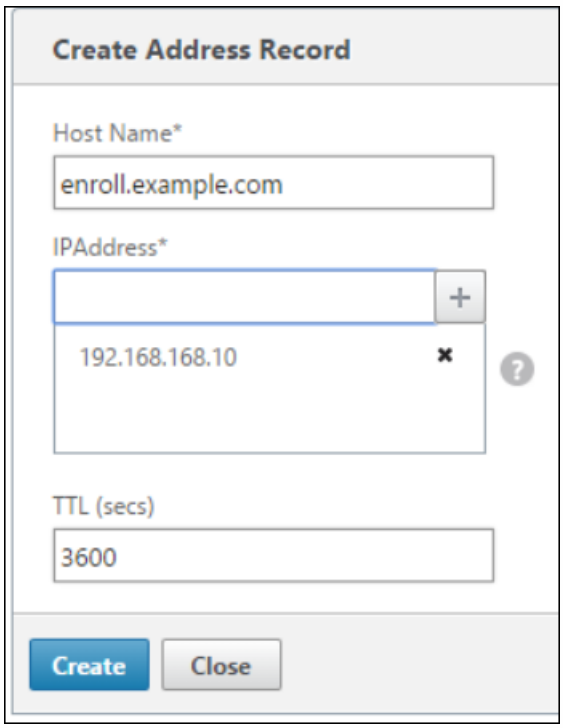
Hinweis



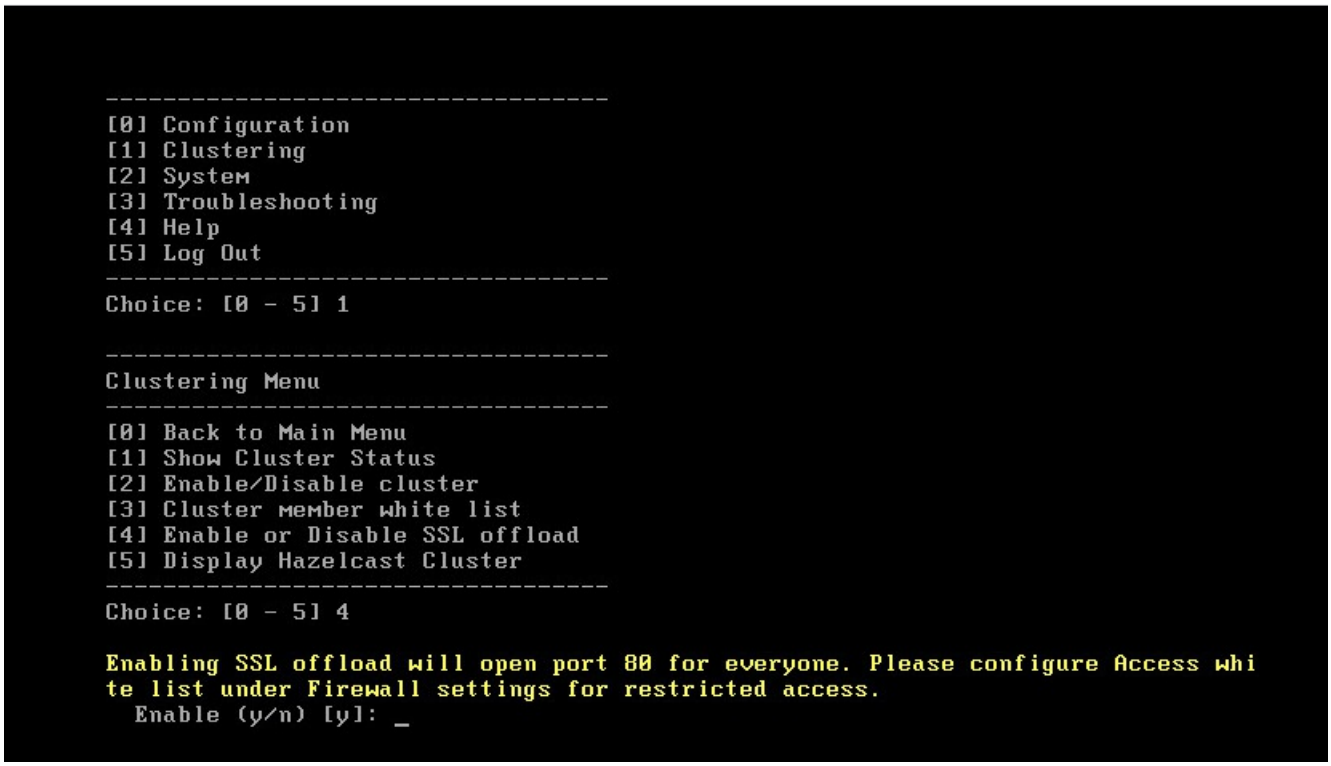








Hinweis



In NetScaler Gateway müssen Sie auch die IP-Adresse oder den FQDN des Servers hinzufügen, auf dem die Secure Ticket Authority ausgeführt wird. Führen Sie hierzu folgende Schritte aus:

1. Klicken Sie auf **NetScaler Gateway**.

2. Klicken Sie auf **Virtual Servers**.

3. Wählen Sie den konfigurierten virtuellen NetScaler Gateway-Server aus und klicken Sie auf **Edit**.

4. Klicken Sie unter **Published Applications** auf **STA server**.

5. Notieren Sie die URL und wählen Sie dann den Secure Ticket Authority-Server aus der Liste aus.

6. Klicken Sie auf **Unbind** und dann auf **Add Binding**.

7. Geben Sie im Feld **Secure Ticket Authority Server** die in Schritt 5 notierte URL ein.

8. Klicken Sie auf **Bind**, dann auf **Close** und dann auf **Done**.

Clustering

-
-
-
-
-
-
-

-
-

Rollback von XenMobile-Upgrades

Aktualisieren des MTC-Mandantenservers auf XenMobile 10.1

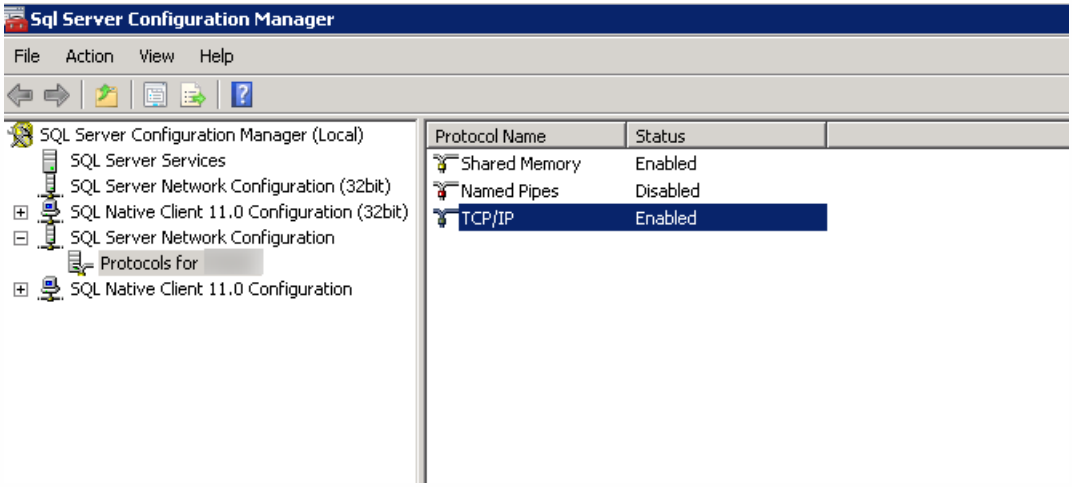
-
-
-

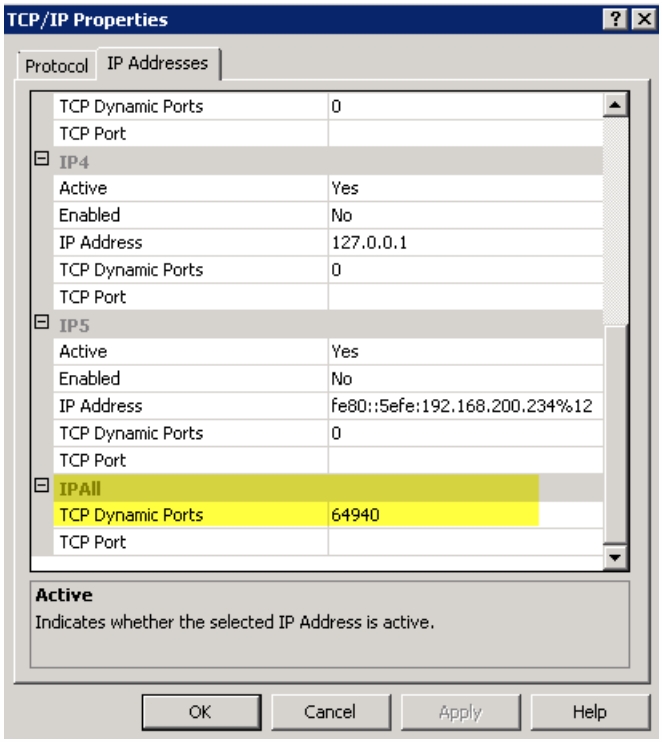
-
-
-
-
-

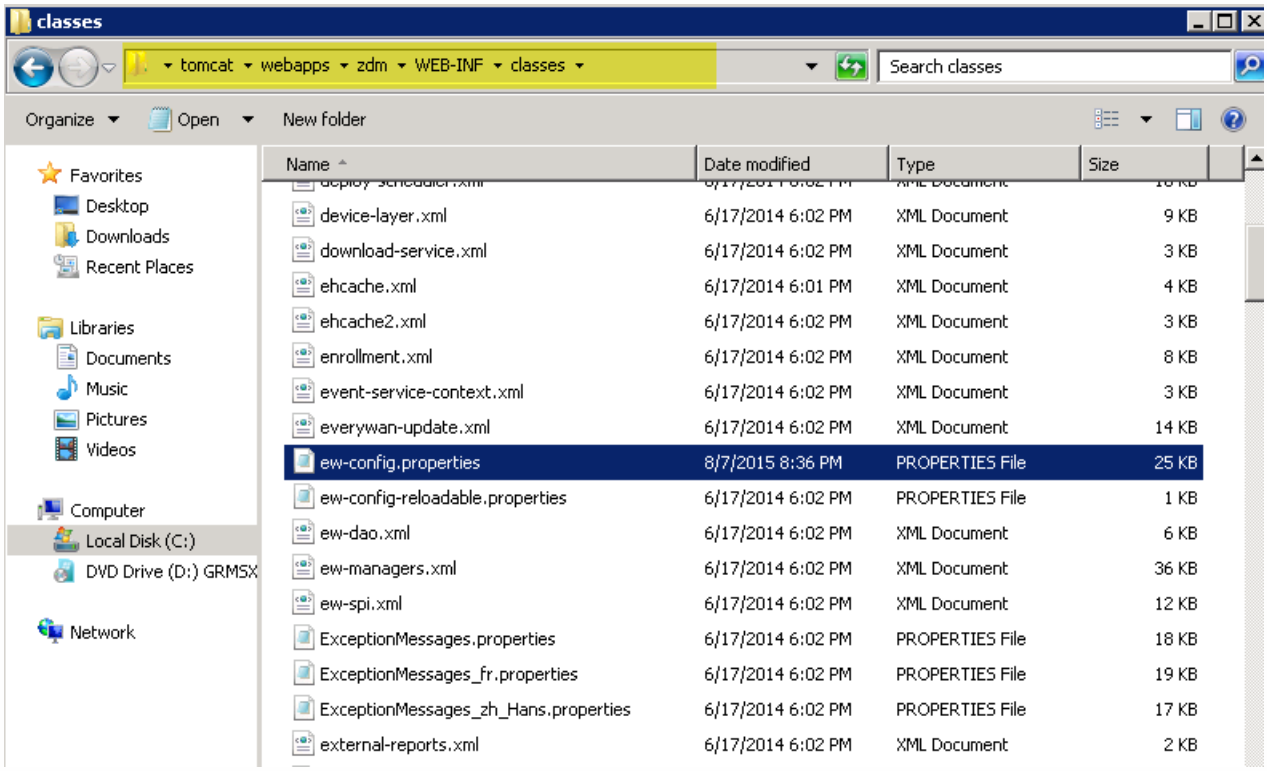
Unterstützung für benannte SQL-Instanzen

-
-
-

> Hinweis







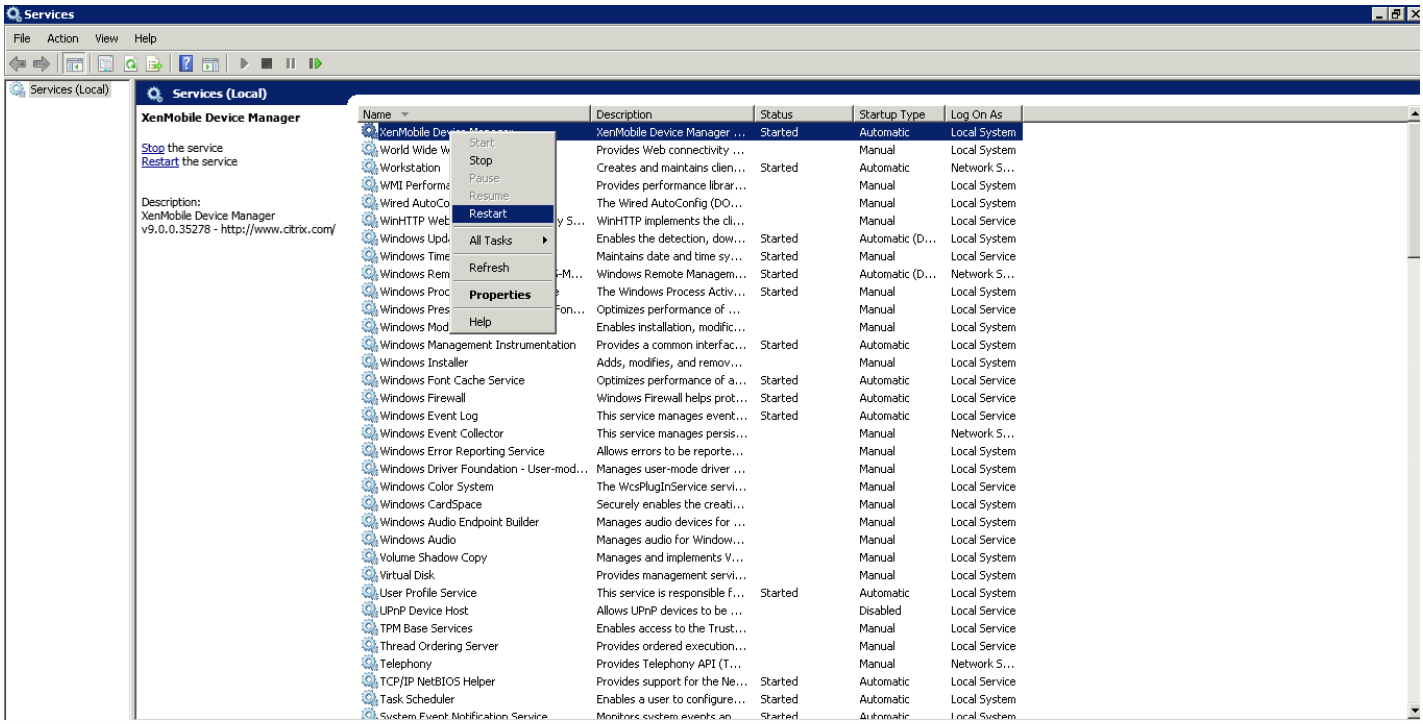
ew-config.properties

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

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

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

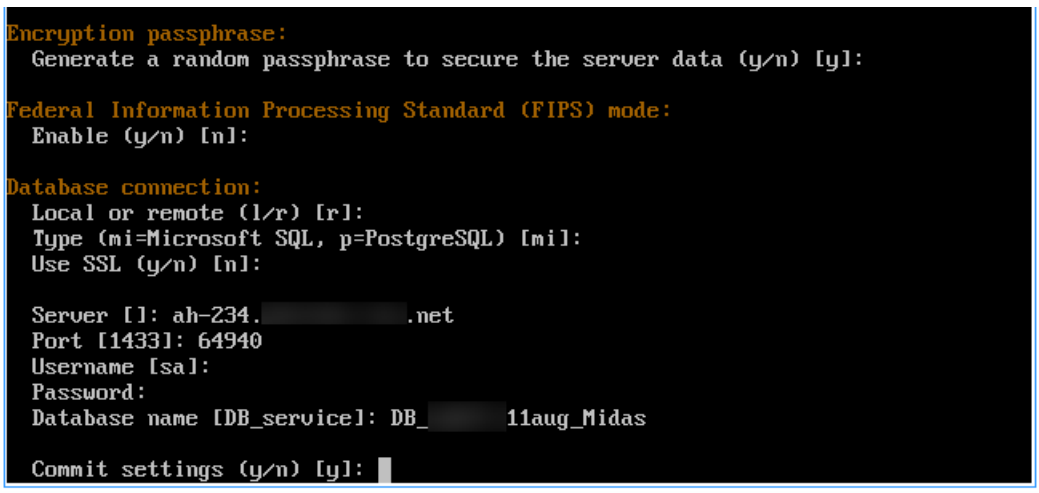
Hinweis

ew-config.properties

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

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

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



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

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

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

  Server []: ah-234.[redacted].net
  Port [1433]: 64940
  Username [sa]:
  Password:
  Database name [DB_service]: DB_[redacted]11aug_Midas

  Commit settings (y/n) [y]:
```



-
-

Konfigurieren von Clustering für XenMobile 10

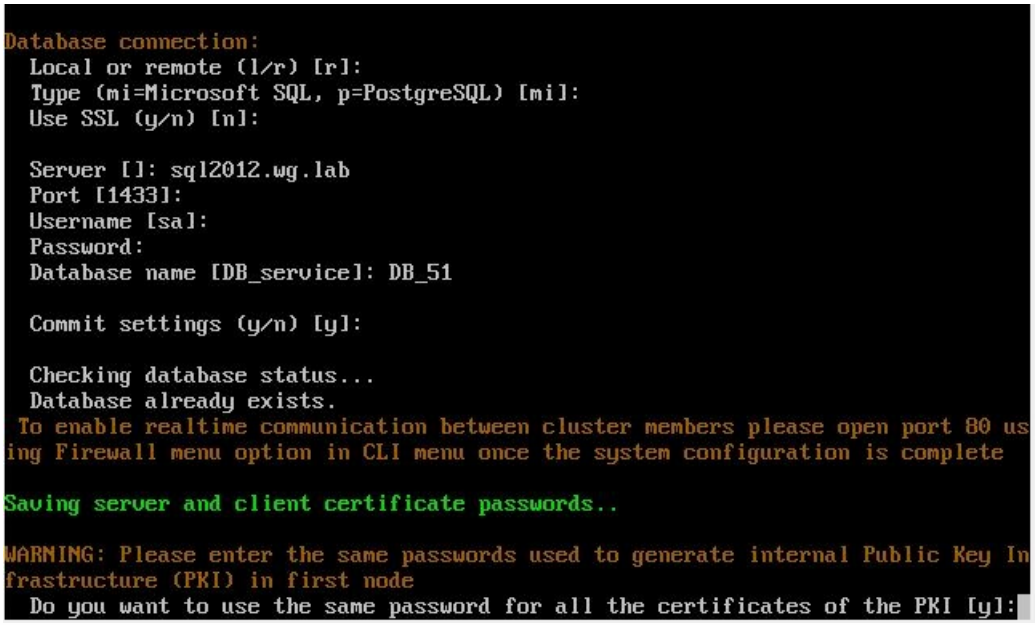
-
-
-
-
-

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

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

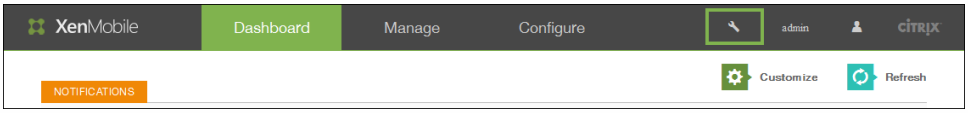
```
Encryption passphrase:
  Generate a random passphrase to secure the server data (y/n) [y]:
```

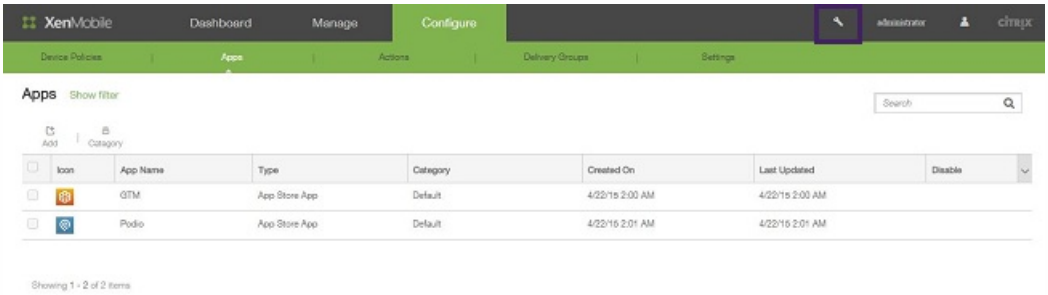
```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

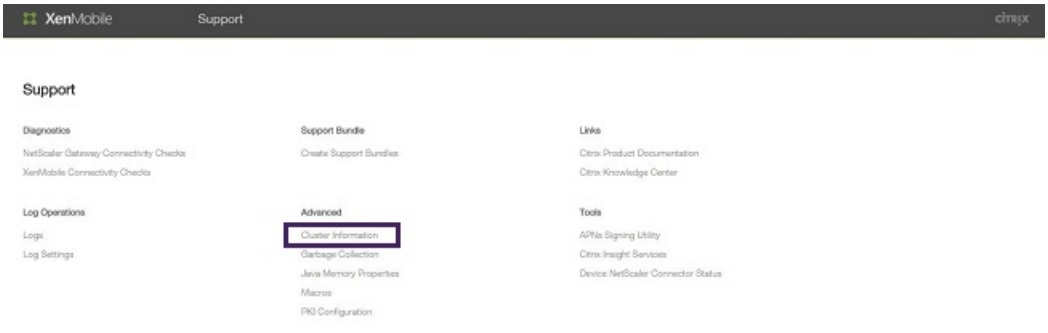
```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

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

  Commit settings (y/n) [y]:

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

Saving server and client certificate passwords..
```

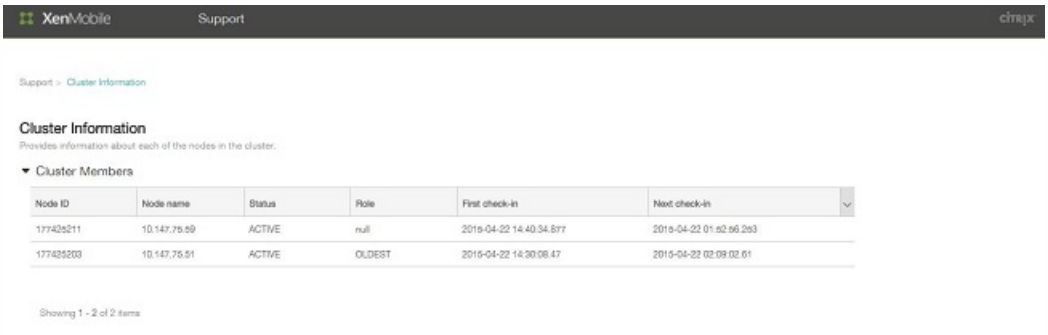


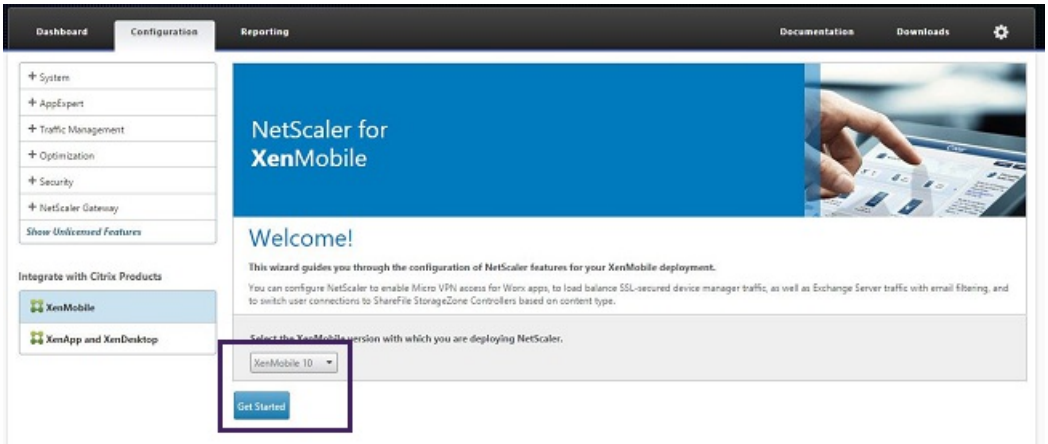
```
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

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

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

Starting monitoring...                                           [ OK ]

xms51.wg.lab login:
```

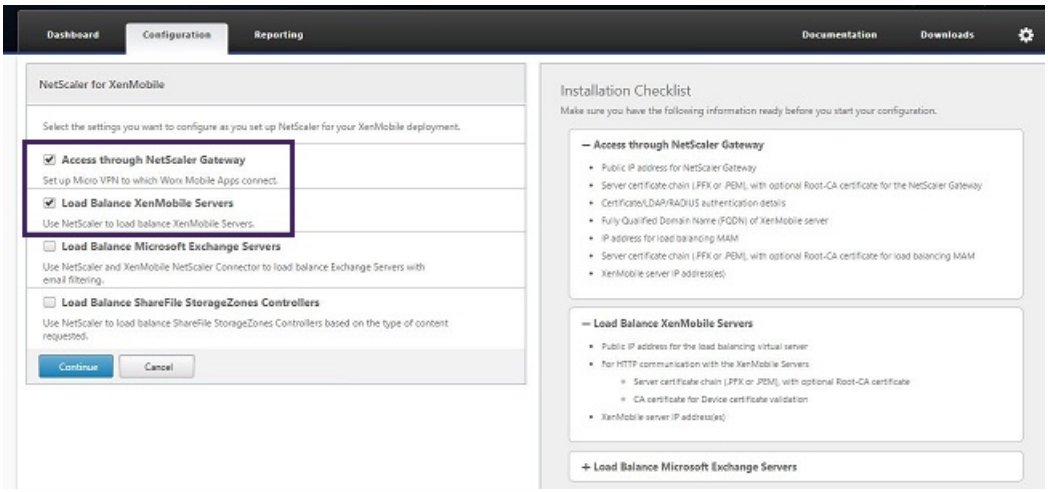


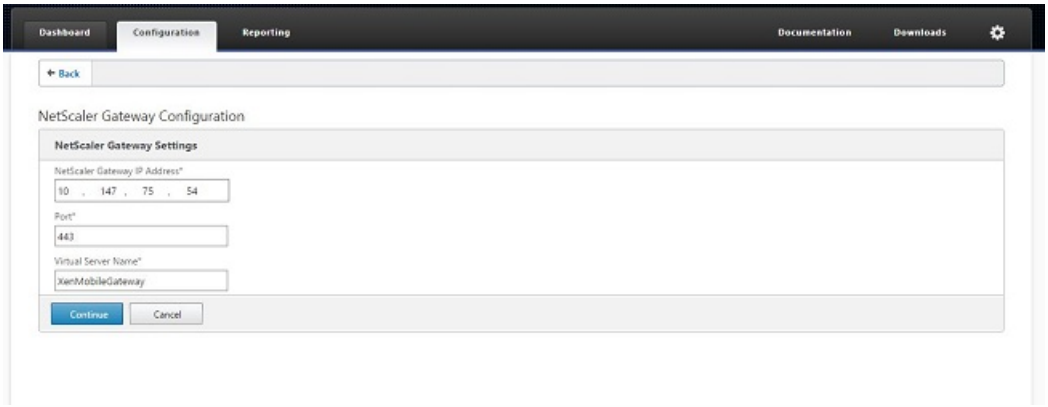




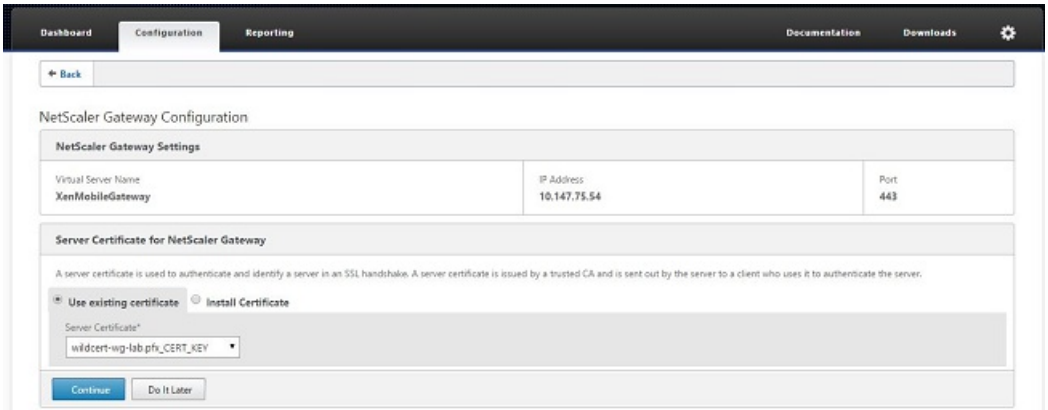


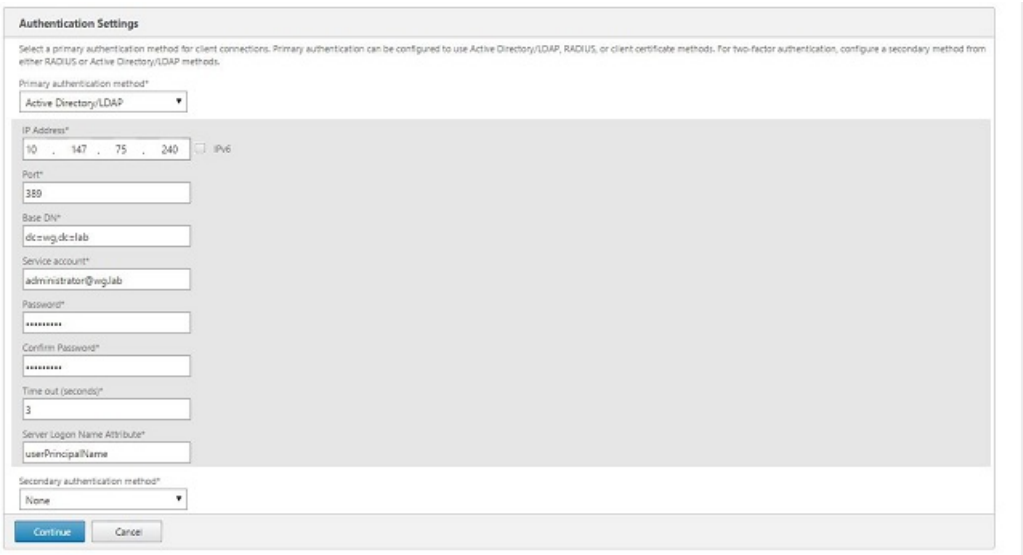


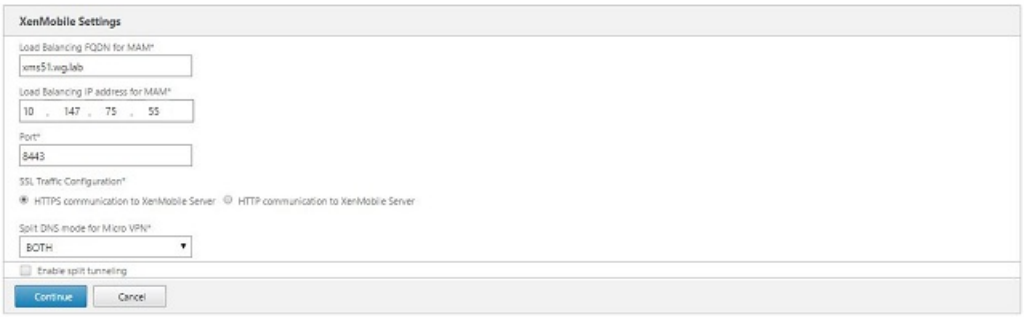


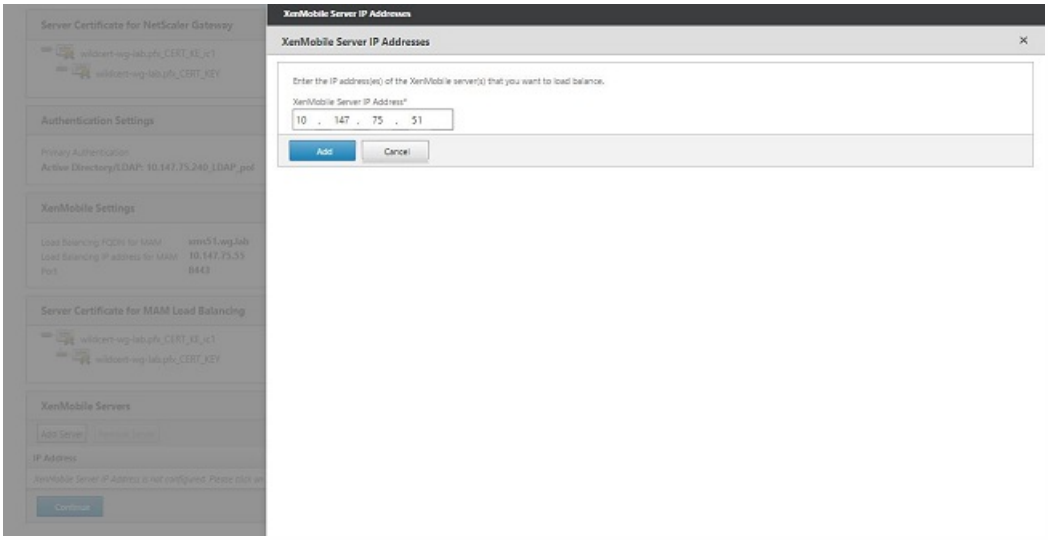


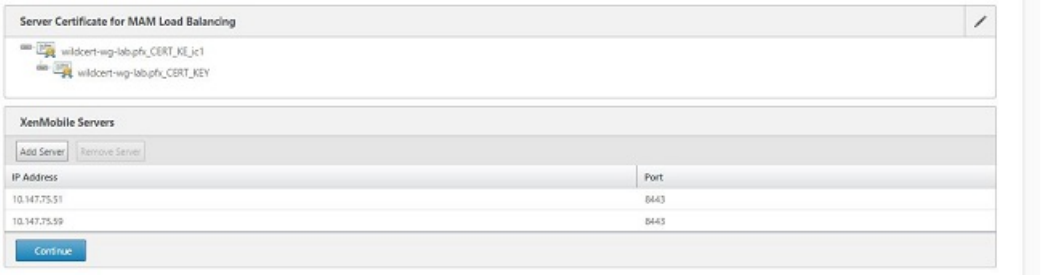
-
-

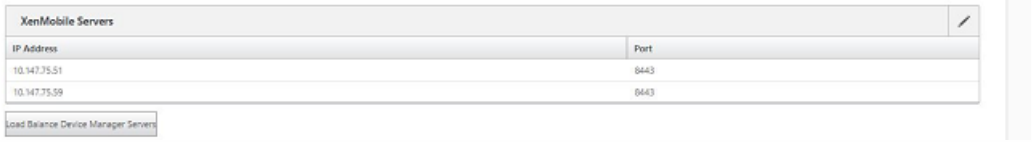


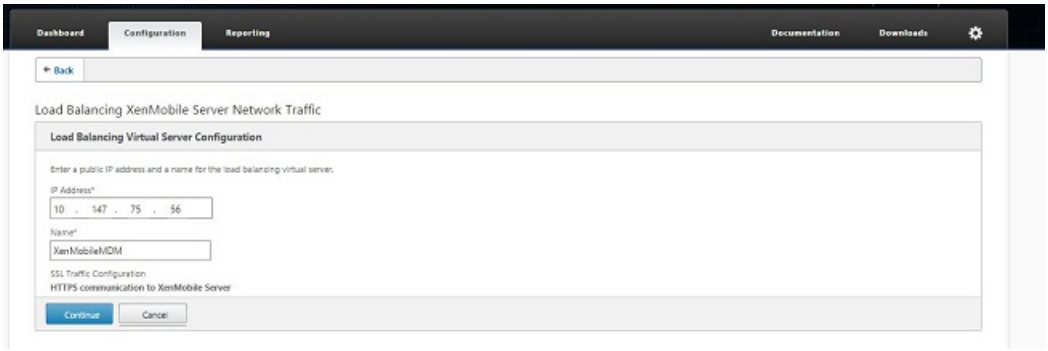


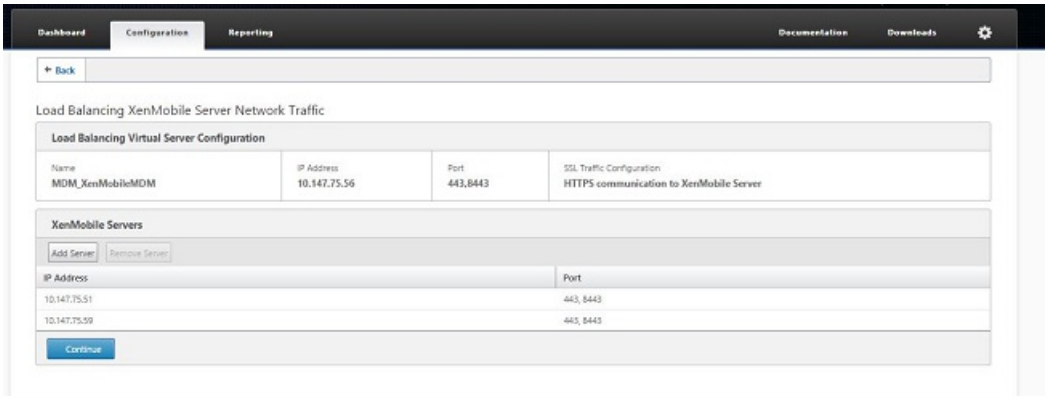


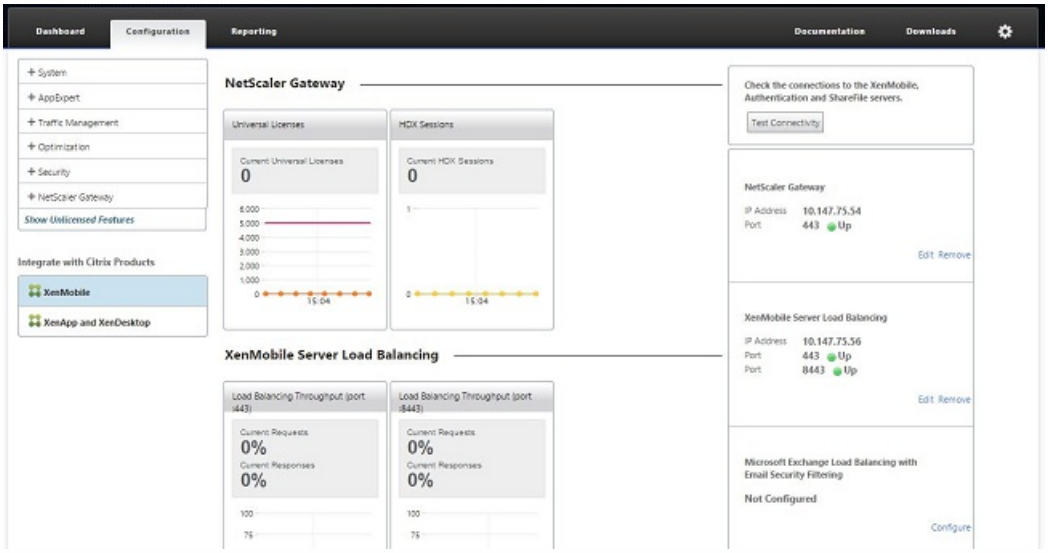


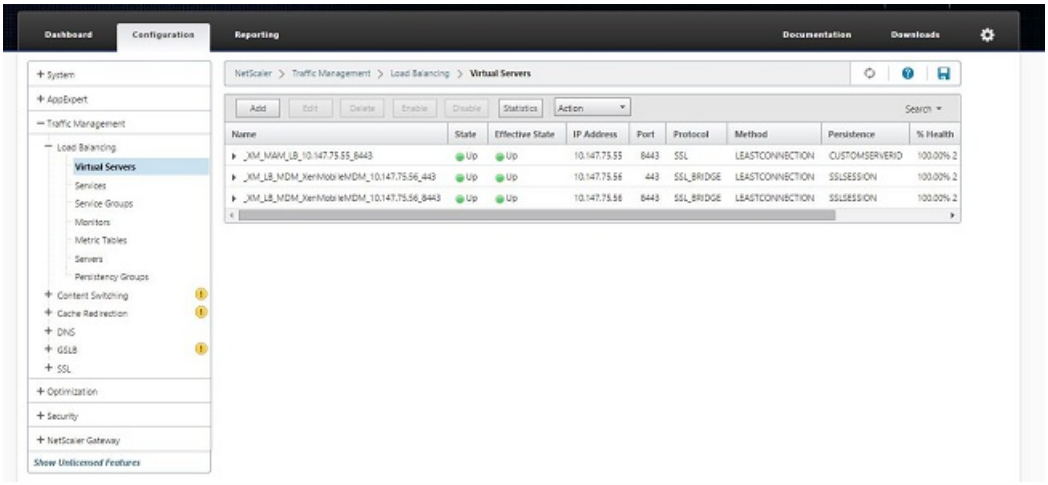


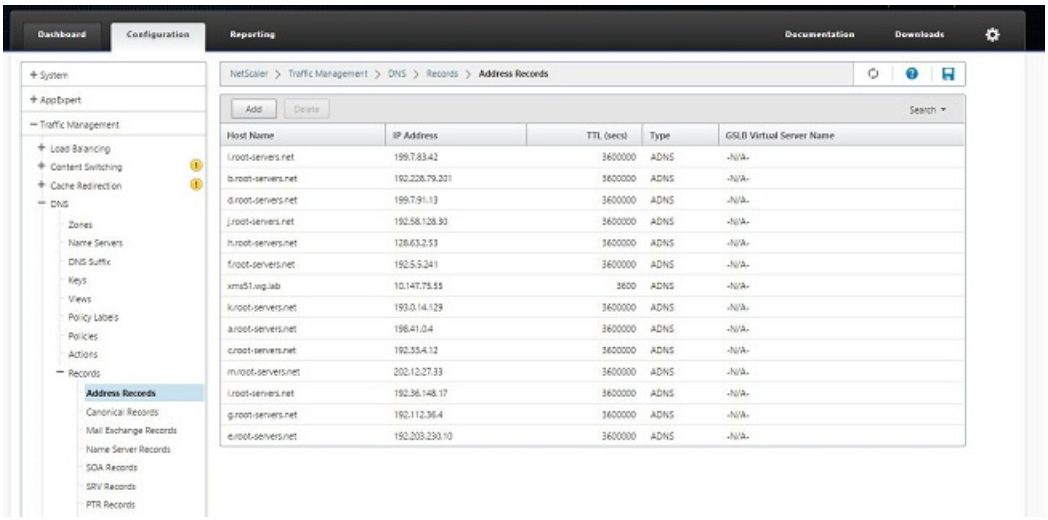




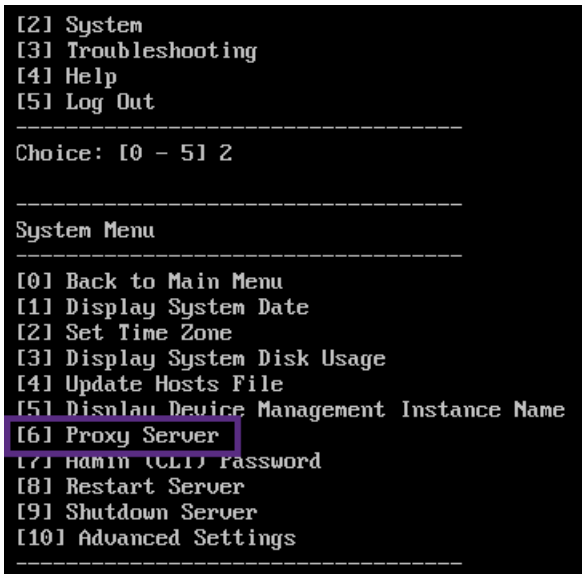


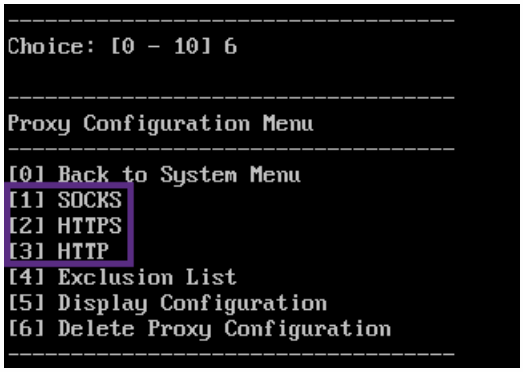


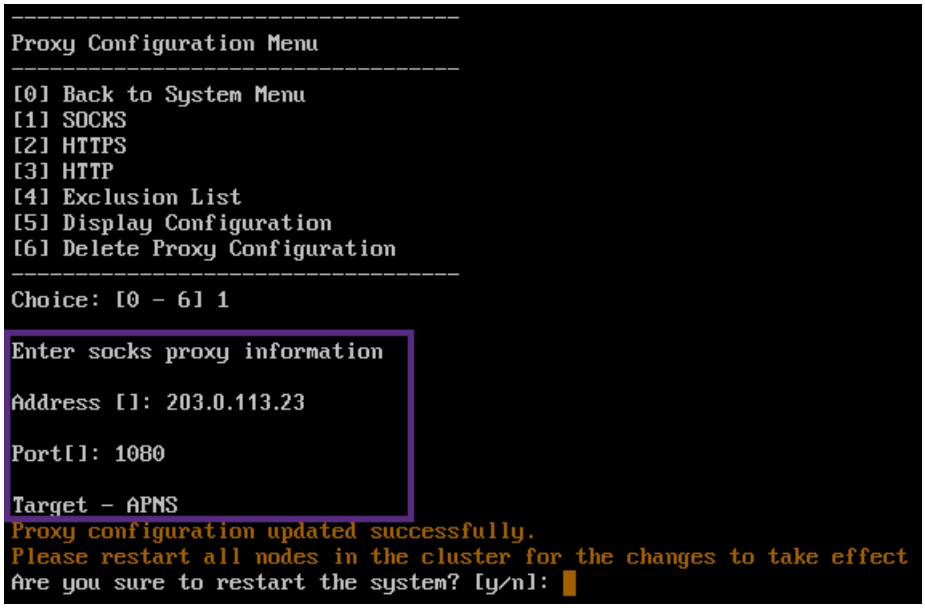


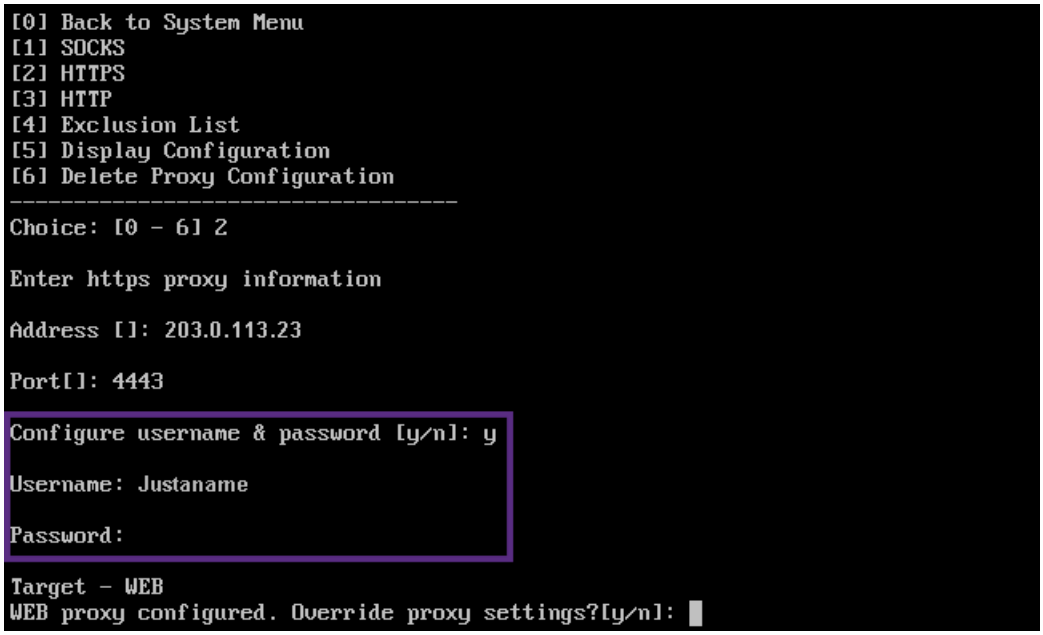


Aktivieren von Proxyservern in XenMobile









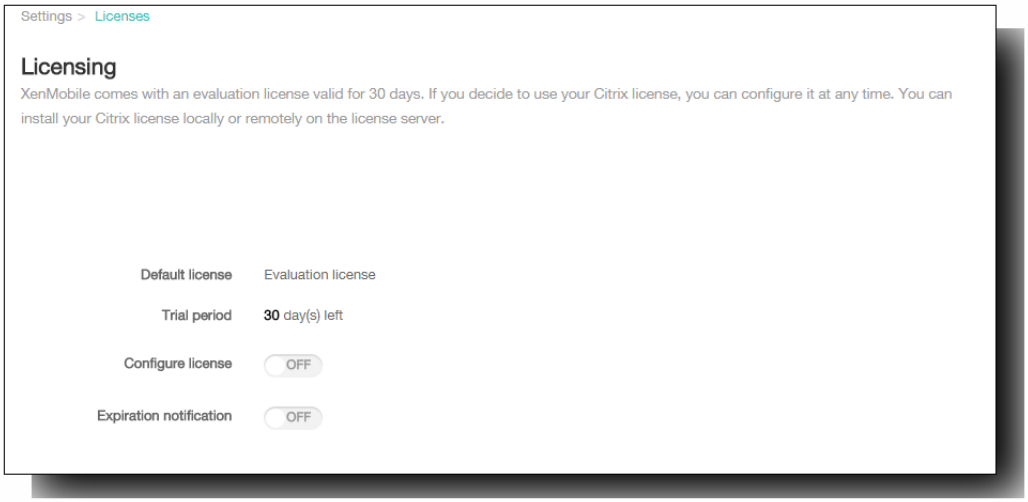
Lizenzierung

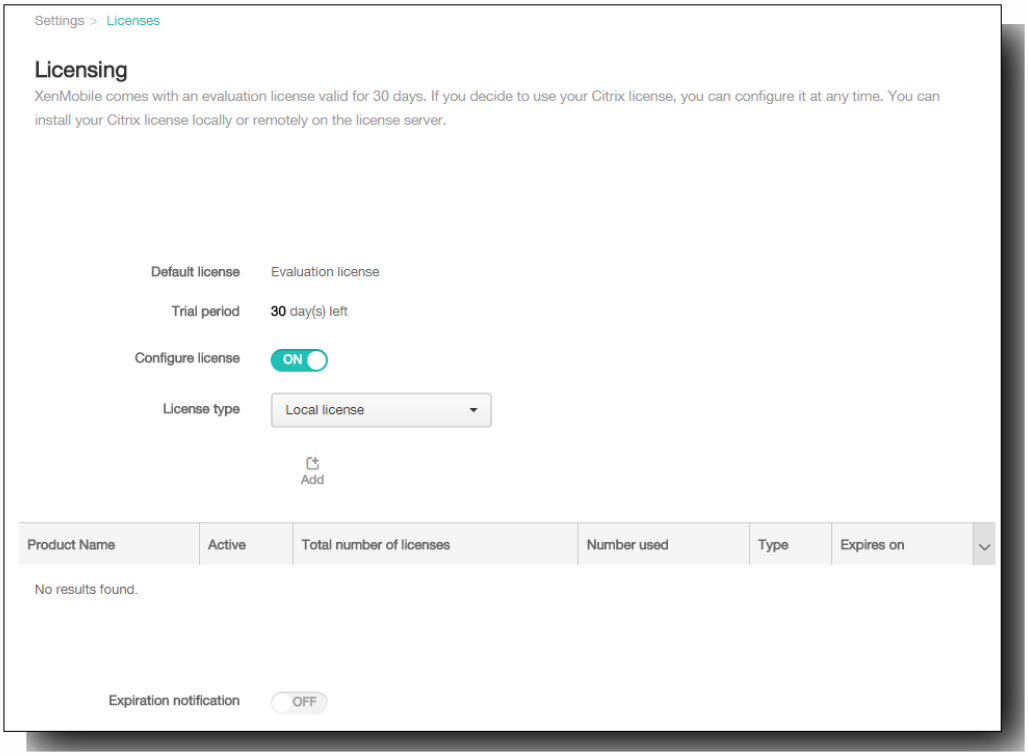
Hinweis

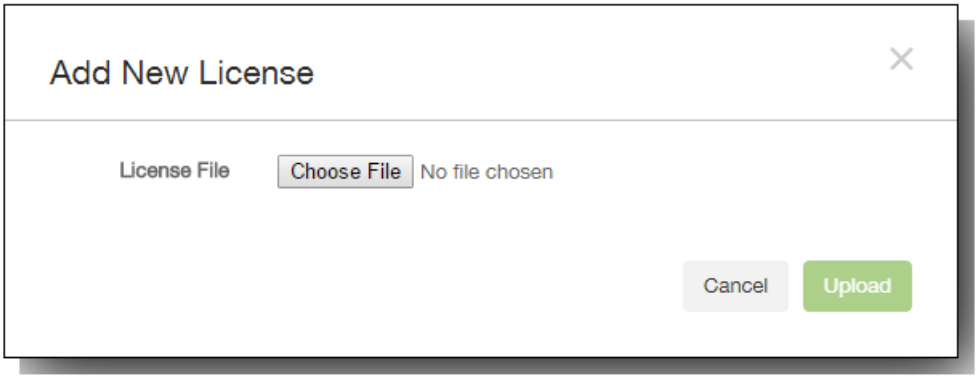
Important

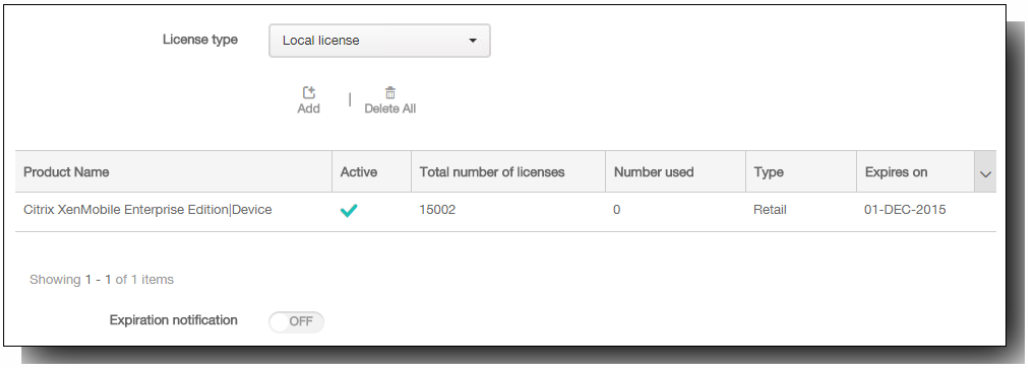
Informationen zur XenMobile-Lizenzierung

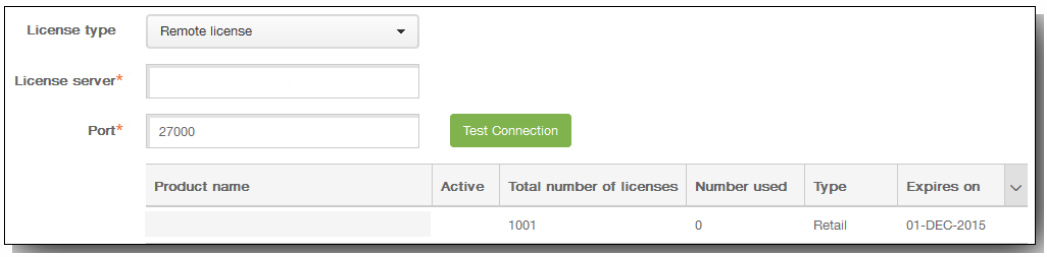
So finden Sie die Lizenzierungsseite in der XenMobile-Konsole

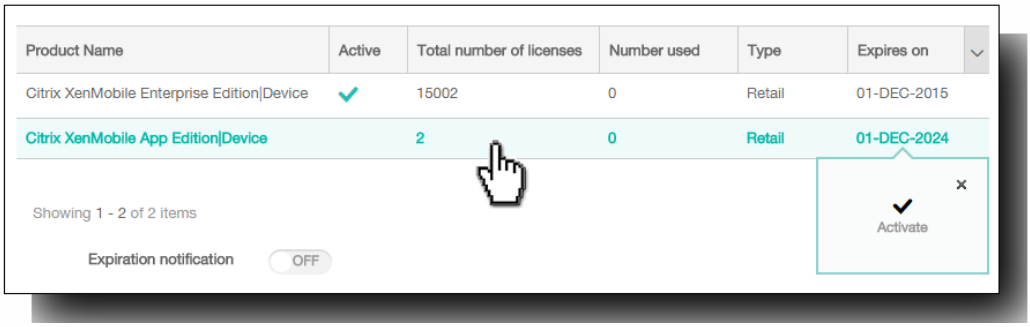


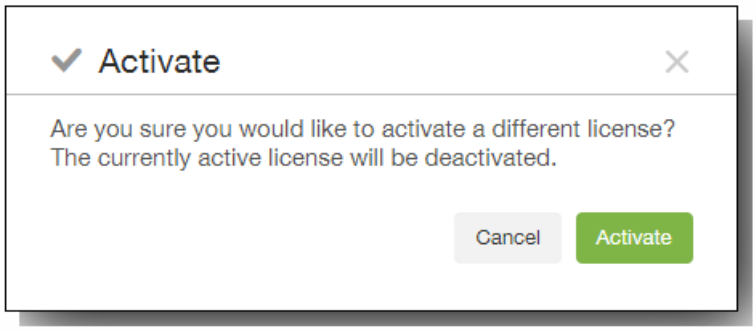


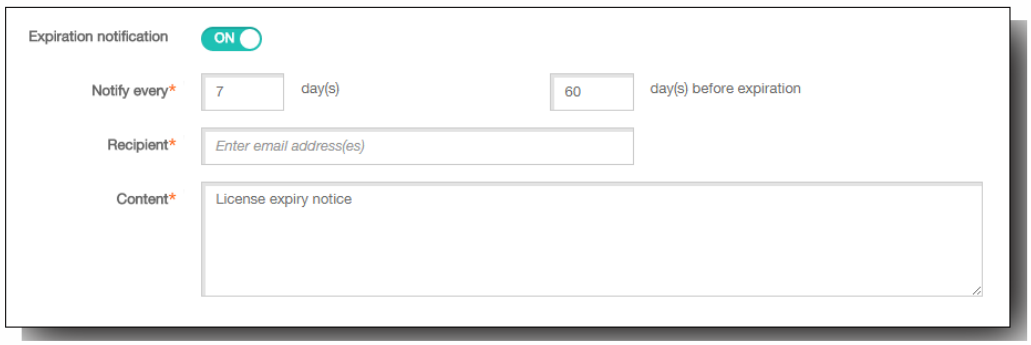






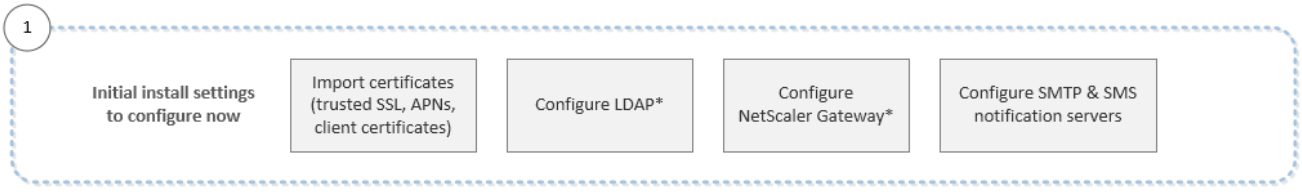


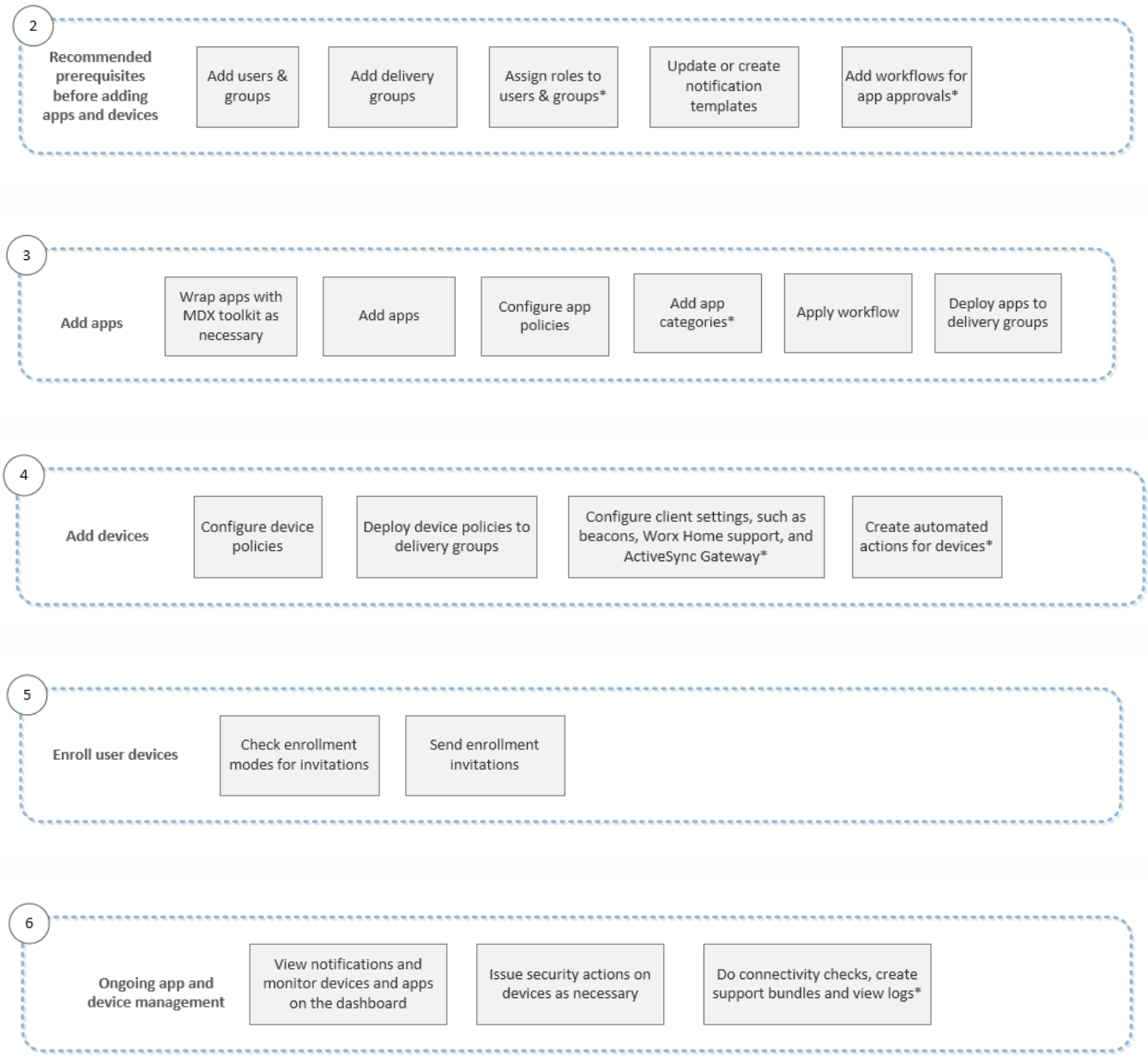




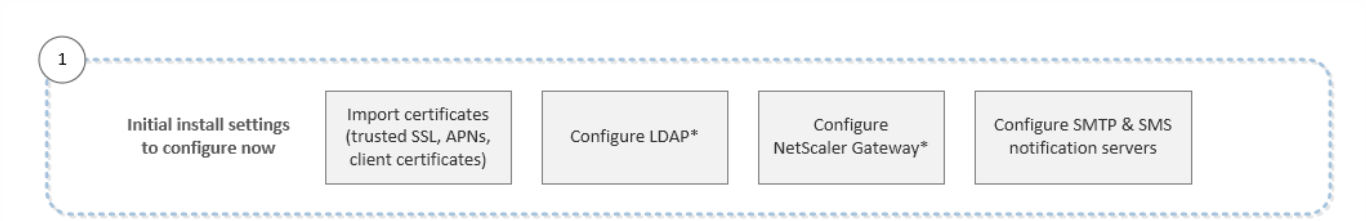
-
-

Erste Schritte mit der XenMobile-Konsole





Workflow für erste Einstellungen

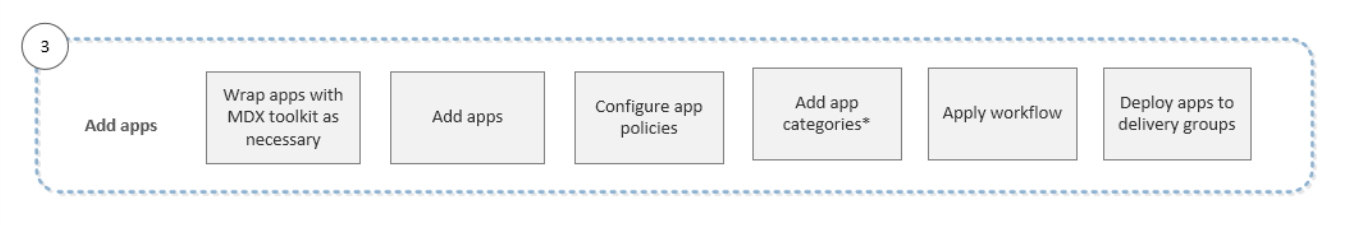


-
-
-
-

Workflow für Konsolenvoraussetzungen

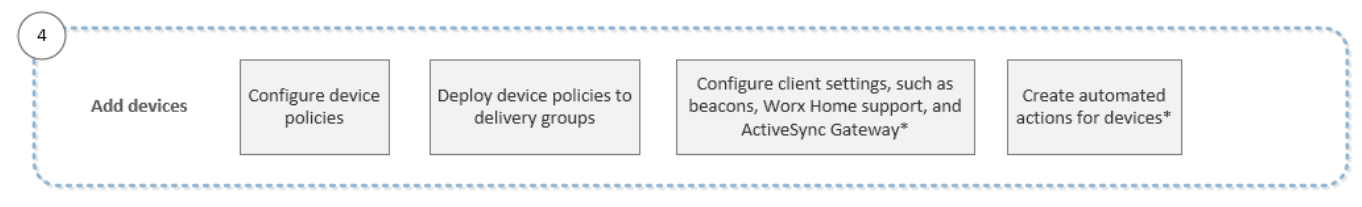
-
-
-
-
-
-

Workflow beim Hinzufügen von Apps



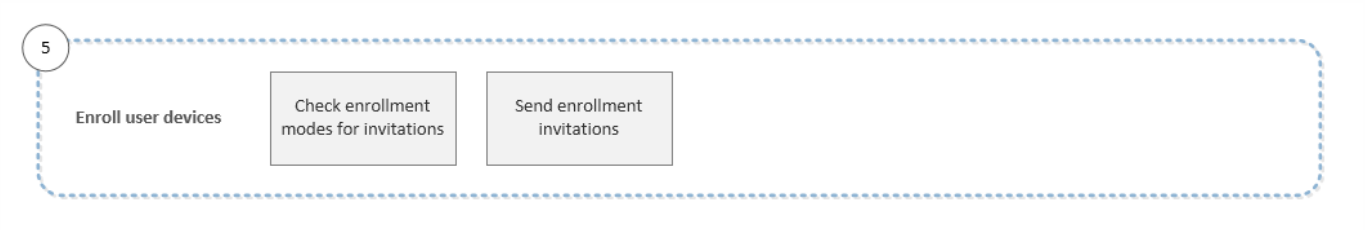
-
-
-
-
-
-

Workflow beim Hinzufügen von Geräten



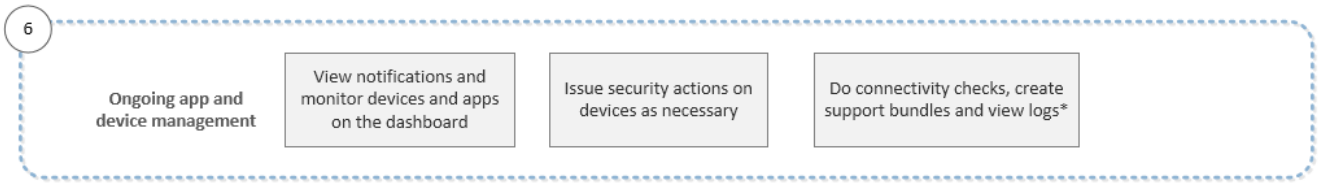
-
-
-
-
-

Workflow beim Registrieren von Benutzergeräten



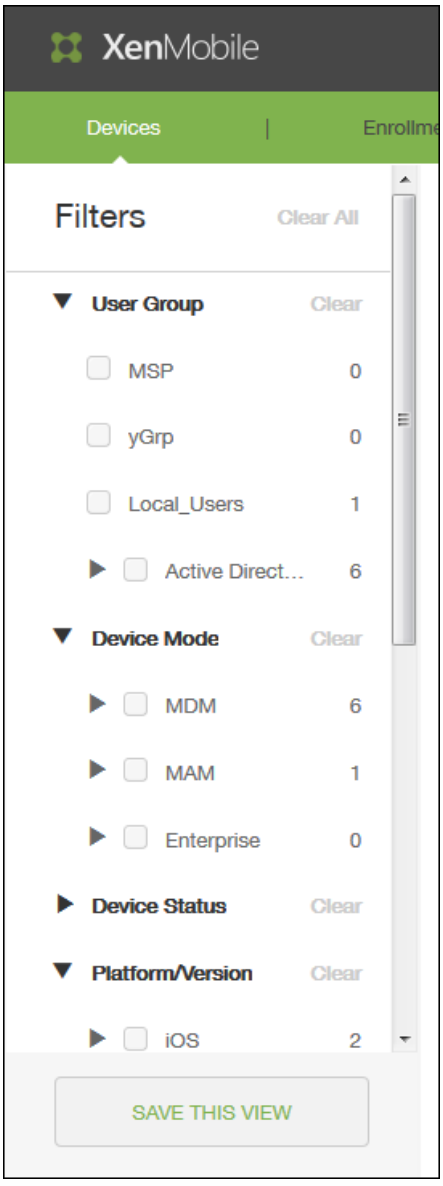
-
-

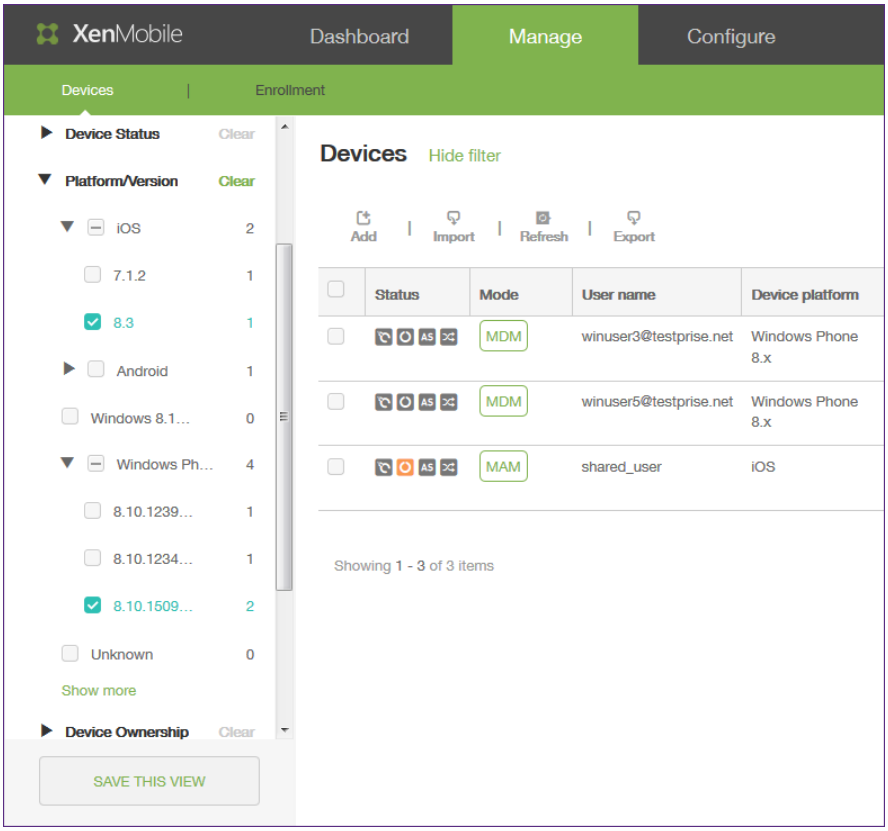
Workflow bei der Verwaltung von Apps und Geräten



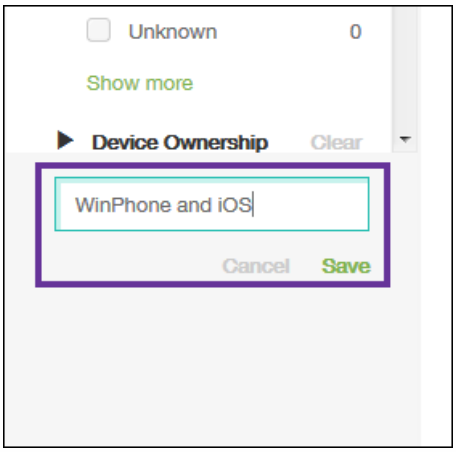
Filter und Tabellen in der XenMobile-Konsole

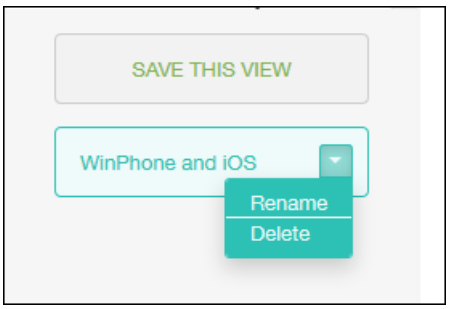
-
-
-
-



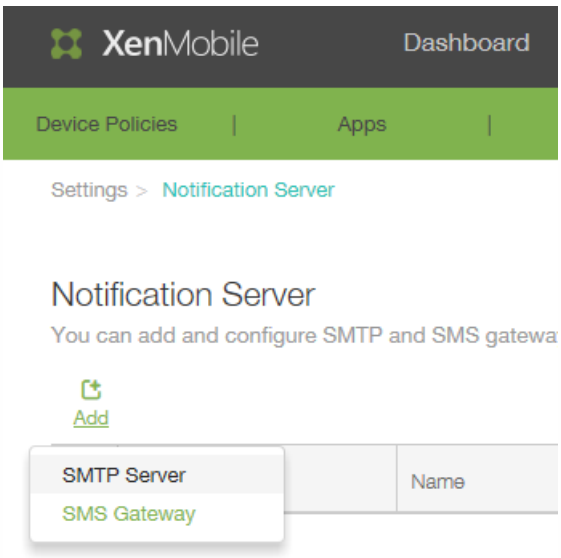


-
-
-

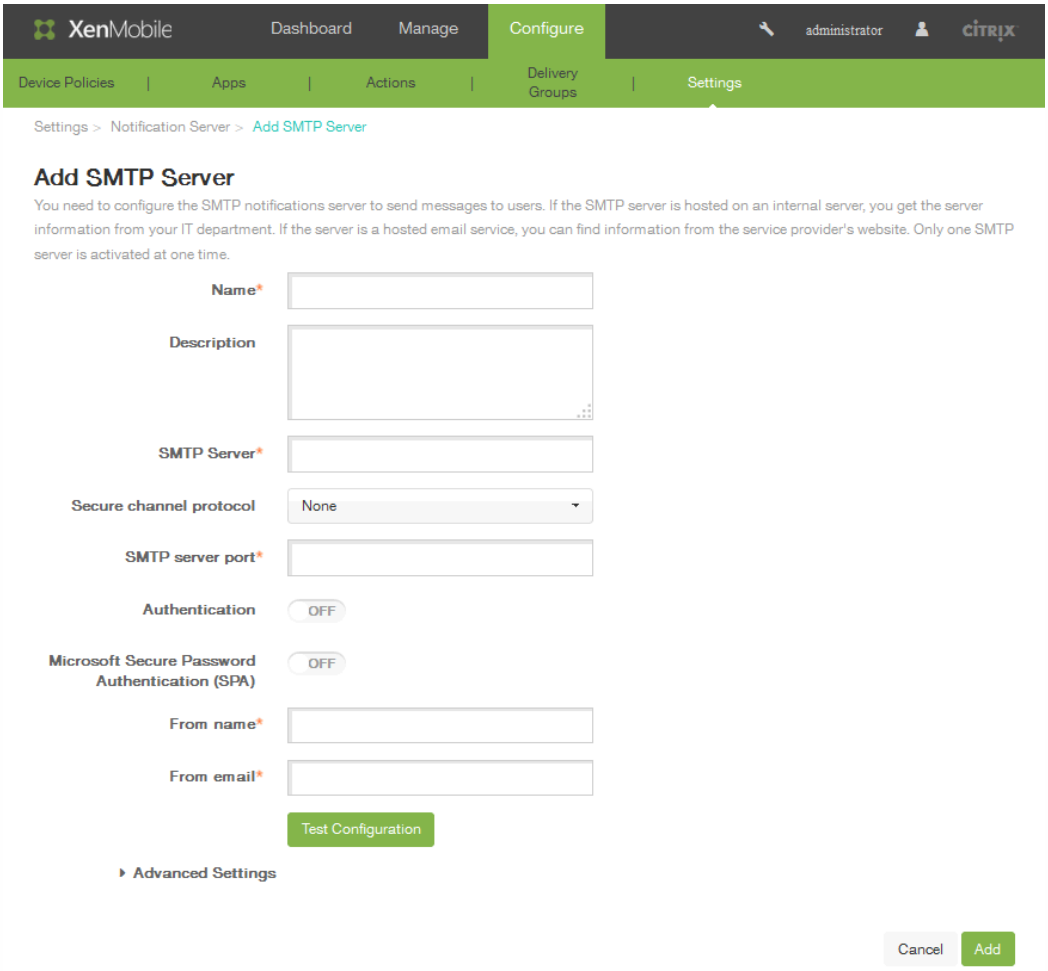




Benachrichtigungen

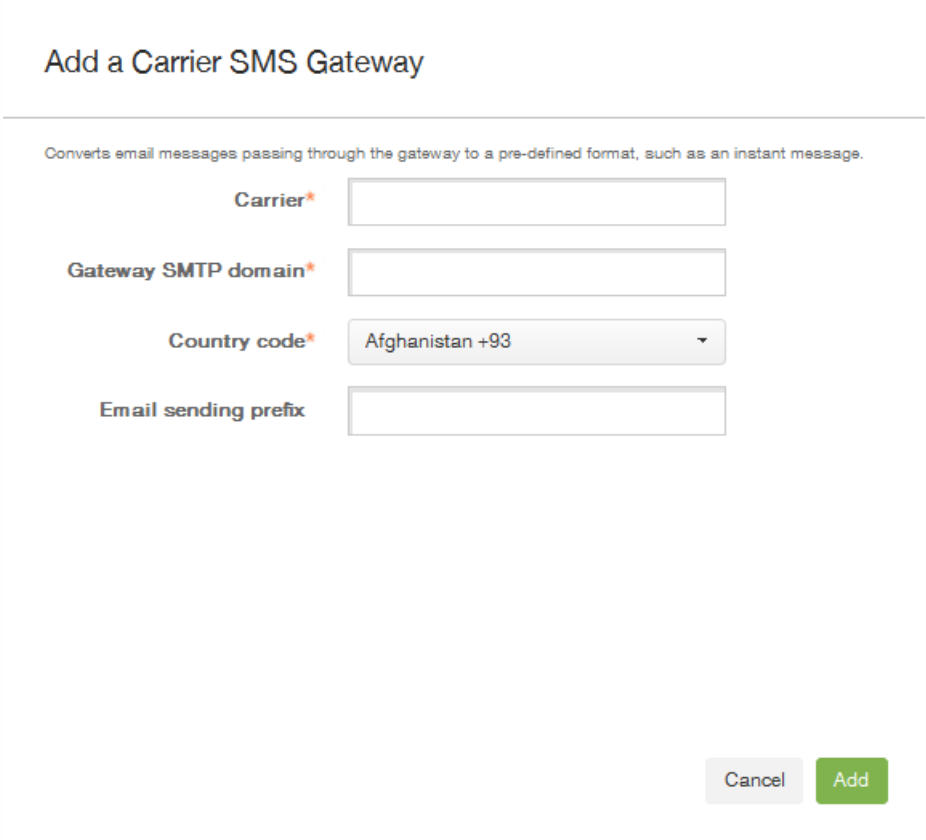


-
-



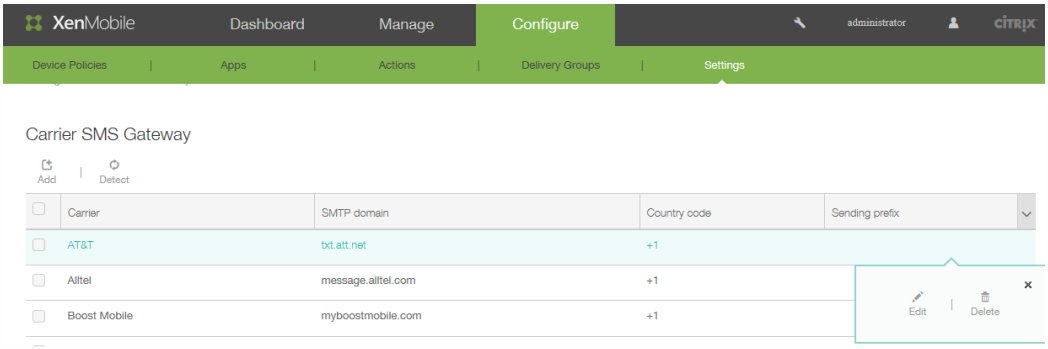
-
-
-
-
-
-
-
-
-
-
-

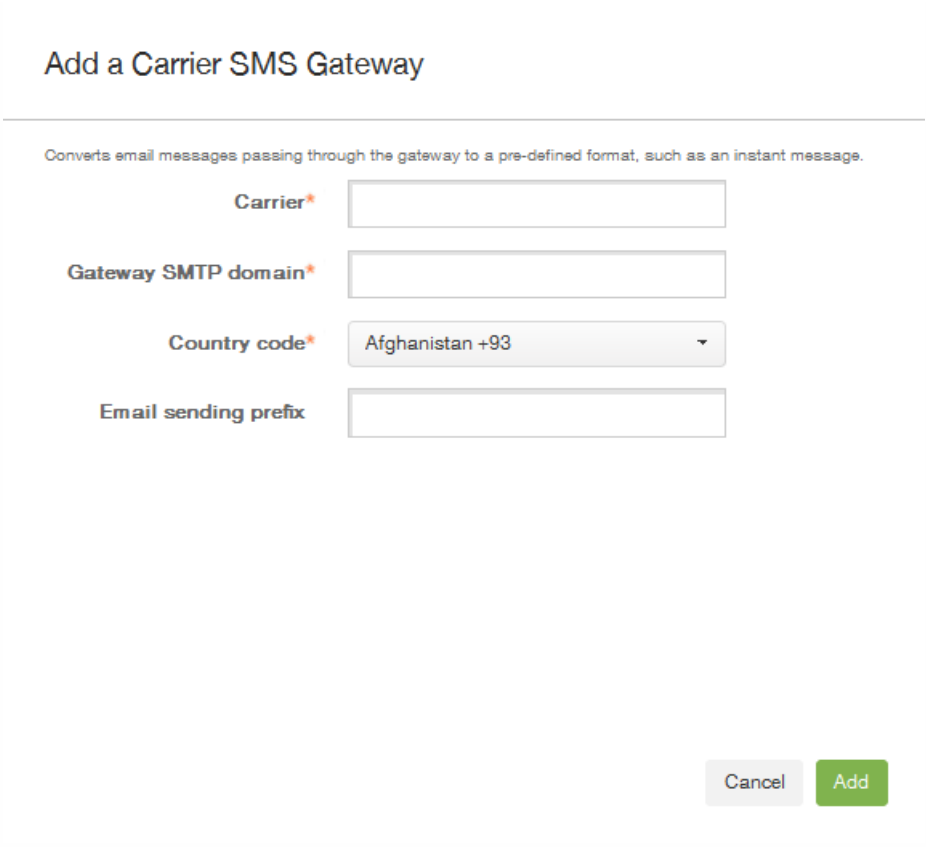
-
-



-
-
-
-
-
-
-

-





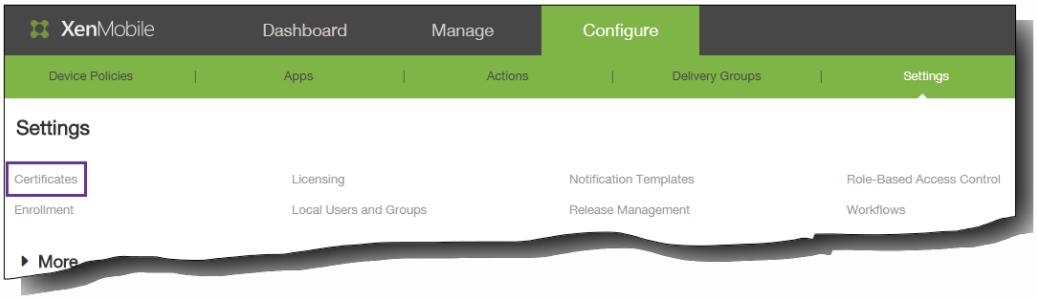
Zertifikate

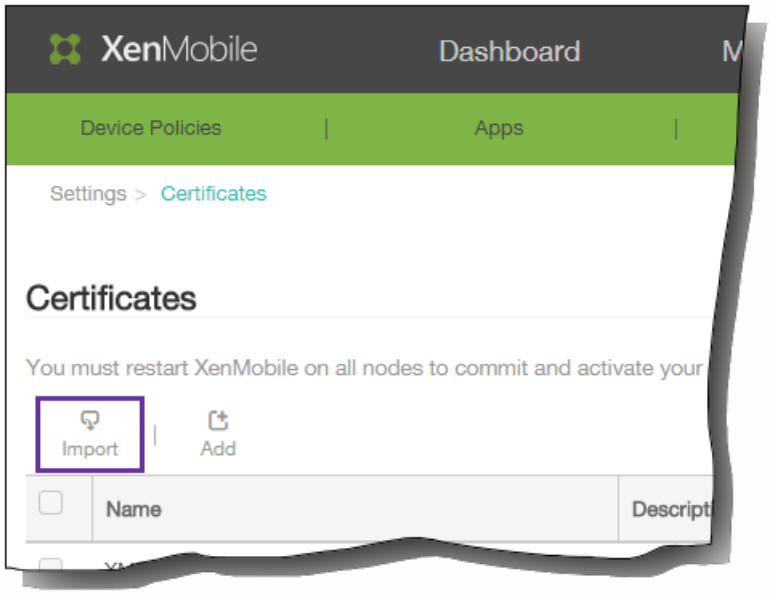
XenMobile-Zertifikatverwaltung

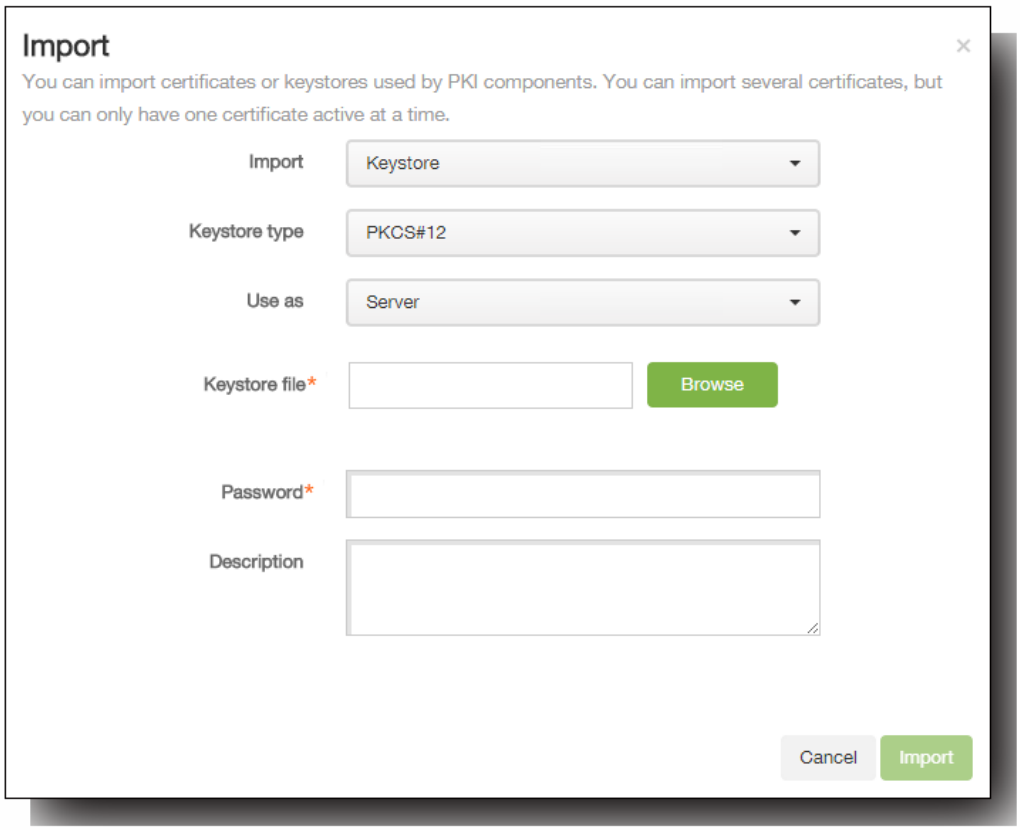
Hinweis

Hochladen von Zertifikaten in XenMobile

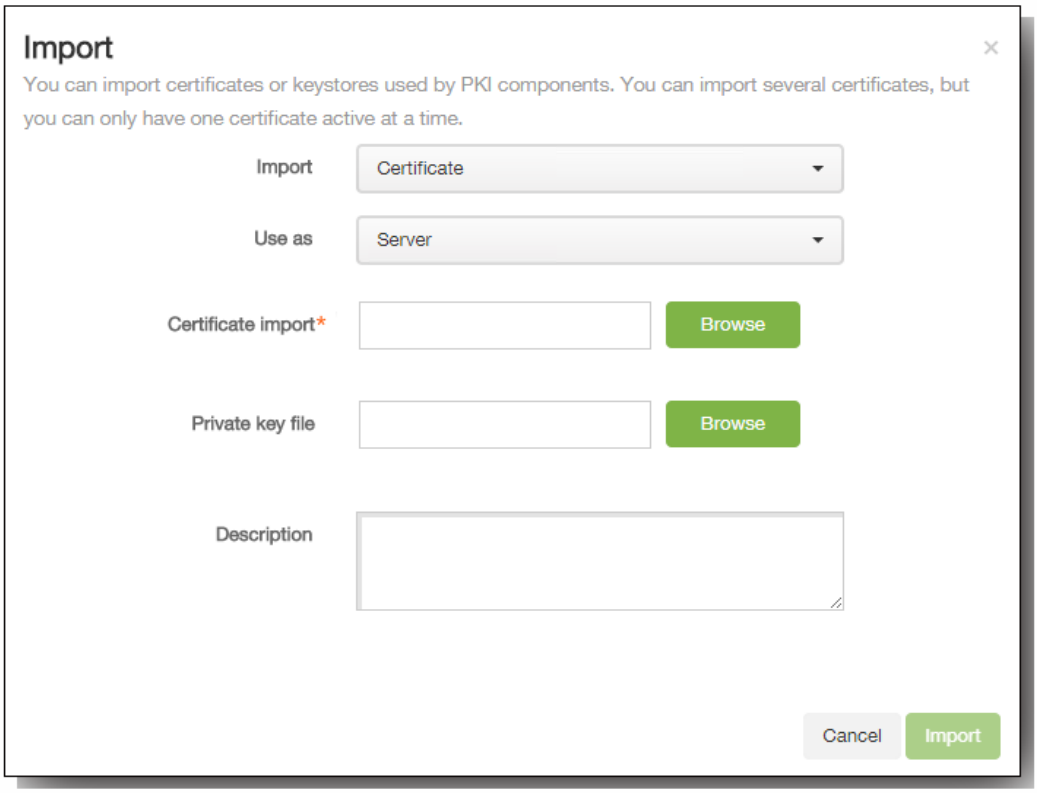
-
-
-







-
-
-
-



-
-
-

PKI-Entitäten

Apr 12, 2016

Eine XenMobile-PKI-Entität ist eine Komponente, die PKI-Vorgänge (Ausstellung, Sperrung und Statusinformationen) durchführt. Solche Komponenten können entweder XenMobile-intern (= eigenverwaltet) sein oder extern, wenn sie Teil der Unternehmensinfrastruktur sind.

XenMobile unterstützt folgende Arten von PKI-Entitäten:

- Eigenverwaltete CAs
- Allgemeiner PKIs (GPKIs)
- Microsoft Zertifikatdienste

XenMobile unterstützt die folgenden Zertifizierungsstellenserver:

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

Allgemeine PKI-Konzepte

Unabhängig von ihrem Typ umfasst jede PKI-Entität folgende Funktionen:

- sign: Ausstellung eines neuen Zertifikats nach Zertifikatsignieranforderung (CSR)
- fetch: Abruf eines vorhandenen Zertifikat-/Schlüsselpaars
- revoke: Sperre eines Clientzertifikats

Informationen über Zertifizierungsstellenzertifikate

Beim Konfigurieren einer PKI-Entität müssen Sie in XenMobile angeben, welches CA-Zertifikat die von dieser Entität ausgestellten bzw. gesperrten Zertifikate signiert. Dieselbe PKI-Entität kann abgerufene oder neu signierte Zertifikate, die von einer beliebigen Zahl verschiedener Zertifizierungsstellen signiert wurden, zurückgeben. Sie müssen das Zertifikat jeder dieser Zertifizierungsstellen als Teil der PKI-Entitätskonfiguration bereitstellen. Hierfür laden Sie die Zertifikate in XenMobile hoch und referenzieren sie dann in der PKI-Entität. Bei eigenverwalteten Zertifizierungsstellen ist das Zertifikat implizit das Zertifikat der signierenden Zertifizierungsstelle, bei externen Entitäten müssen Sie das Zertifikat jedoch manuell angeben.

Generic PKI

Das Protokoll Generic PKI (GPKI) ist ein XenMobile-eigenes Protokoll, das über eine SOAP-Webdienstschicht zur Vereinheitlichung der Schnittstelle mit verschiedenen PKI-Lösungen ausgeführt wird. GPKI definiert folgende grundlegenden PKI-Vorgänge:

- sign: Der Adapter kann Zertifikatsignieranforderungen an die PKI übertragen und neu signierte Zertifikate zurückgeben.
- fetch: Der Adapter kann vorhandene Zertifikate und Schlüsselpaare – je nach den Eingabeparametern – von der PKI abrufen (wiederherstellen).
- revoke: Die Adapter kann eine Sperre von Zertifikaten durch die PKI auslösen.

Empfänger der GPKI-Befehle ist der GPKI-Adapter. Der Adapter übersetzt die grundlegenden Vorgänge für den spezifischen PKI-Typ, für den er erstellt wurde. Es gibt also GPKI-Adapter für RSA, für EnTrust usw.

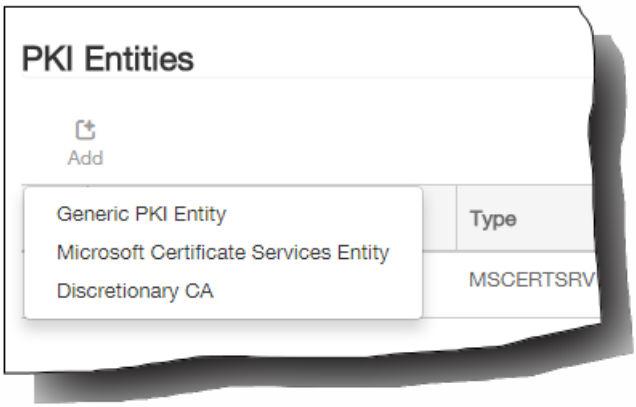
Der GPKI-Adapter veröffentlicht als SOAP-Webdienst-Endpunkt eine selbstbeschreibende WSDL-Definition (Web Services Description Language). Die Erstellung einer GPKI-PKI-Entität besteht in der Bereitstellung dieser WSDL-Definition für XenMobile über eine URL oder durch Hochladen der Datei selbst.

Unterstützung für die einzelnen PKI-Vorgänge ist bei einem Adapter optional. Wenn ein Adapter einen bestimmten Vorgang unterstützt, hat der Adapter die entsprechende Funktion (sign, fetch oder revoke). Jeder Funktion können diverse Benutzerparameter zugeordnet werden.

Benutzerparameter werden durch den GPKI-Adapter für einen bestimmten Vorgang definiert und erfordern die Bereitstellung von Werten an XenMobile. XenMobile ermittelt durch Analyse der WSDL, welche Vorgänge ein Adapter unterstützt (d. h. welche Funktionen er bietet) und welche Parameter er für diese Vorgänge jeweils benötigt. Bei entsprechender Auswahl verwenden Sie die SSL-Clientauthentifizierung zum Schützen der Verbindung zwischen XenMobile und dem GPKI-Adapter.

So fügen Sie eine GPKI-Entität hinzu

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > PKI Entities.
2. Klicken Sie auf der Seite PKI Entities auf Add.
   Eine Liste mit den Typen der PKI-Entitäten, die Sie hinzufügen können, wird angezeigt.



3. Klicken Sie auf Generic PKI Entity.
   Die Seite Generic PKI Entity: General Information wird angezeigt.

4. Führen Sie auf der Seite Generic PKI Entity: General Information folgende Schritte aus:
   1. Name: Geben Sie einen aussagekräftigen Namen für die PKI-Entität ein.

2. WSDL URL: Geben Sie den Speicherort der WSDL mit der Beschreibung des Adapters ein.
3. Authentication type: Klicken Sie auf die Authentifizierungsmethode, die Sie verwenden möchten.
   - Keine
   - HTTP Basic: Geben Sie den Benutzernamen und das Kennwort für die Verbindung mit dem Adapter ein.
   - Client certificate: Wählen Sie das richtige SSL-Clientzertifikat aus.
4. Klicken Sie auf Next.
   Die Seite Generic PKI Entity: Adapter Capabilities wird angezeigt.

5. Prüfen Sie auf der Seite Generic PKI Entity: Adapter Capabilities die Funktionen und Parameter des Adapters und klicken Sie dann auf Next.
   Die Seite Generic PKI Entity: Issuing CA Certificates wird angezeigt.

6. Wählen Sie auf der Seite Generic PKI Entity: Issuing CA Certificates die Zertifikate aus, die Sie für die Entität verwenden möchten.
   Hinweis: Obwohl Entitäten zwar von verschiedenen Zertifizierungsstellen signierte Zertifikate zurückgeben können, müssen alle von einem bestimmten Zertifikatanbieter abgerufenen Zertifikate von derselben Zertifizierungsstelle signiert sein. Wählen Sie analog dazu bei der Konfiguration des Anmeldeinformationsanbieters auf der Seite Distribution eines der hier konfigurierten Zertifikate aus.
7. Klicken Sie auf Speichern.
   Die Entität wird in der Tabelle der PKI-Entitäten angezeigt.

Microsoft Zertifikatdienste

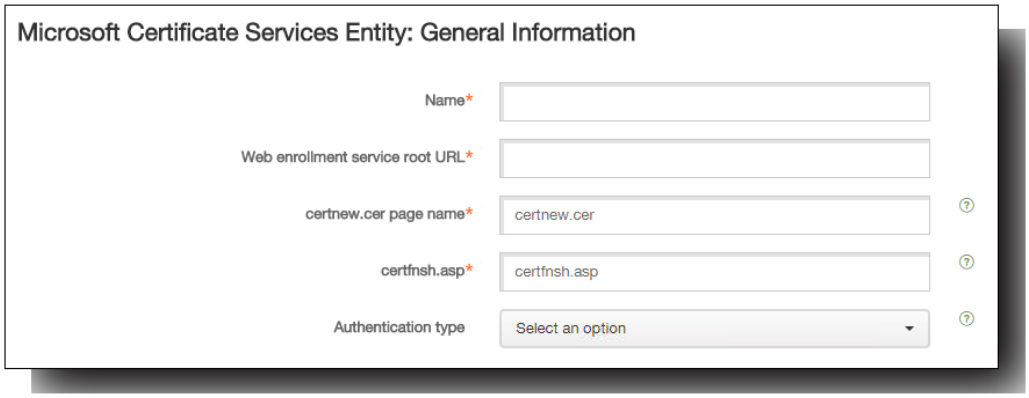
XenMobile interagiert mit Microsoft Zertifikatdiensten über seine Schnittstelle zur Webregistrierung. XenMobile unterstützt nur die Ausstellung neuer Zertifikate über diese Schnittstelle (entspricht der sign-Funktion von GPKI).

Zum Erstellen einer PKI-Entität für eine Microsoft-Zertifizierungsstelle in XenMobile müssen Sie die Basis-URL der Zertifikatdienste-Webschnittstelle angeben. Bei entsprechender Auswahl verwenden Sie die SSL-Clientauthentifizierung zum Schützen der Verbindung zwischen XenMobile und Zertifikatdienste-Webinterface.

So fügen Sie eine Microsoft-Zertifikatdienste-Entität hinzu

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > PKI Entities.
2. Klicken Sie auf der Seite "PKI Entities" auf Add.
   Eine Liste mit den Typen der PKI-Entitäten, die Sie hinzufügen können, wird angezeigt.

3. Klicken Sie auf Microsoft Certificate Services Entity.
   Die Seite Microsoft Certificate Services Entity: General Information wird angezeigt.



4. Führen Sie auf der Seite Microsoft Certificate Services Entity: General Information folgende Schritte aus:
   1. Name: Geben Sie einen Namen für die neue Entität ein. Der Name von Entitäten muss eindeutig sein.
   2. Web enrollment service root URL: Geben Sie die Basis-URL des Webregistrierungsdiensts für die Microsoft-Zertifizierungsstelle ein. Beispiel: https://192.0.2.13/certsrv/. Die URL darf HTTP oder HTTP über SSL verwenden.
   3. certnew.cer page name: Name der certnew.cer-Seite. Verwenden Sie den Standardnamen, es sei denn, Sie haben die Seite aus irgendeinem Grund umbenannt.
   4. certfnsh.asp: Der Name der certfnsh.asp-Seite. Verwenden Sie den Standardnamen, es sei denn, Sie haben die Seite aus irgendeinem Grund umbenannt.
   5. Authentication type: Klicken Sie auf die Authentifizierungsmethode, die Sie verwenden möchten.
      - Keine
      - HTTP Basic: Geben Sie den Benutzernamen und das Kennwort für die Verbindung ein.
      - Client certificate: Wählen Sie das richtige SSL-Clientzertifikat aus.
      - Klicken Sie auf Next.
        Die Seite Microsoft Certificate Services Entity: Templates wird angezeigt. Auf dieser Seite geben Sie die internen Namen der Vorlagen ein, die die Microsoft-Zertifizierungsstelle unterstützt. Beim Erstellen von Anmeldeinformationsanbietern wählen Sie eine Vorlage aus der hier definierten Liste aus. Jeder Anmeldeinformationsanbieter, der diese Entität verwendet, verwendet eine Vorlage.

5. Klicken Sie auf der Seite Microsoft Certificate Services Entity: Templates auf Add, geben Sie den Namen der Vorlage ein und klicken Sie auf Save. Wiederholen Sie diesen Schritt für jede Vorlage, die Sie hinzufügen möchten.
6. Klicken Sie auf Next.
   Die Seite Microsoft Certificate Services Entity: HTTP parameters wird angezeigt. Auf dieser Seite legen Sie benutzerdefinierte Parameter fest, die XenMobile in HTTP-Anforderungen an die Microsoft-Webregistrierungsschnittstelle einfügen soll. Dies ist nur nützlich, wenn auf der Zertifizierungsstelle angepasste Skripts ausgeführt werden.

7. Klicken Sie auf der Seite Microsoft Certificate Services Entity: HTTP parameters auf Add, geben Sie Namen und Wert der gewünschten HTTP-Parameter ein und klicken Sie auf Next.
   Die Seite Microsoft Certificate Services Entity: CA Certificates wird angezeigt. Auf dieser Seite müssen Sie die Signierer der Zertifikate angeben, die das System über diese Entität erhalten wird. Wenn Ihr Zertifizierungsstellenzertifikat verlängert wird, aktualisieren Sie es in XenMobile. Die Änderung wird dann transparent auf die Entität angewendet.

8. Wählen Sie auf der Seite Microsoft Certificate Services Entity: CA Certificates die Zertifikate aus, die Sie für die Entität verwenden möchten.
9. Klicken Sie auf Speichern.
   Die Entität wird in der Tabelle der PKI-Entitäten angezeigt.

Eigenverwaltete Zertifizierungsstellen

Eine eigenverwaltete Zertifizierungsstelle wird erstellt, wenn Sie in XenMobile ein Zertifizierungsstellenzertifikat mit zugehörigem privatem Schlüssel angeben. XenMobile wickelt Zertifikatausstellung, Sperrungen und Statusinformationen intern gemäß den von Ihnen gewählten Parametern ab.

Beim Konfigurieren einer eigenverwalteten Zertifizierungsstelle können Sie OCSP-Unterstützung (Online Certificate Status Protocol) für diese aktivieren. Wird die OCSP-Unterstützung aktiviert, fügt die Zertifizierungsstelle den von ihr ausgestellten Zertifikaten eine id-pe-authorityInfoAccess-Erweiterung hinzu, die auf den XenMobile-internen OCSP-Responder im folgenden Verzeichnis verweist:

https://server/instance/ocsp
Wenn Sie den OCSP-Dienst konfigurieren, müssen Sie ein OCSP-Signaturzertifikat für die eigenverwaltete Entität angeben. Sie das Zertifizierungsstellenzertifikat selbst als Signaturzertifikat verwenden. Wenn Sie eine unnötige Offenlegung des privaten Schlüssels Ihrer Zertifizierungsstelle vermeiden möchten (empfehlenswert), erstellen Sie ein von der eigenverwalteten Zertifizierungsstelle signiertes Delegate-OCSP-Signaturzertifikat und schließen Sie eine id-kp-OCSPSigning extendedKeyUsage-Erweiterung ein.

Der OCSP-Responder-Dienst von XenMobile unterstützt einfache OCSP-Antworten und folgende Hashalgorithmen in Anforderungen:

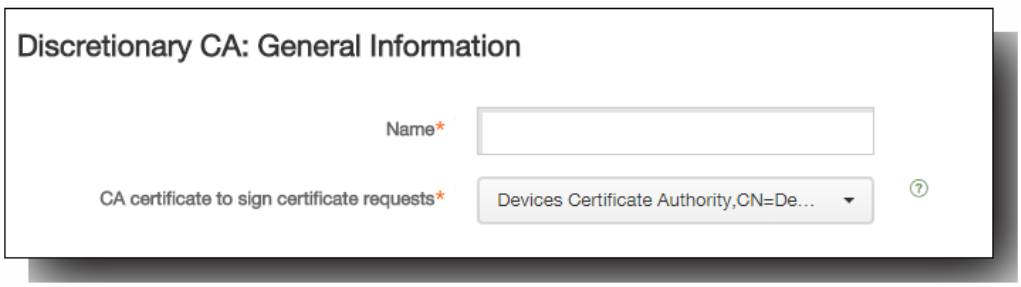
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Antworten werden mit SHA-256 und dem Signaturzertifikat-Schlüsselalgorithmus (DSA, RSA oder ECDSA) signiert.

So fügen Sie eigenverwaltete Zertifizierungsstellen hinzu

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > PKI Entities.
2. Klicken Sie auf der Seite PKI Entities auf Add.
   Eine Liste mit den Typen der PKI-Entitäten, die Sie hinzufügen können, wird angezeigt.

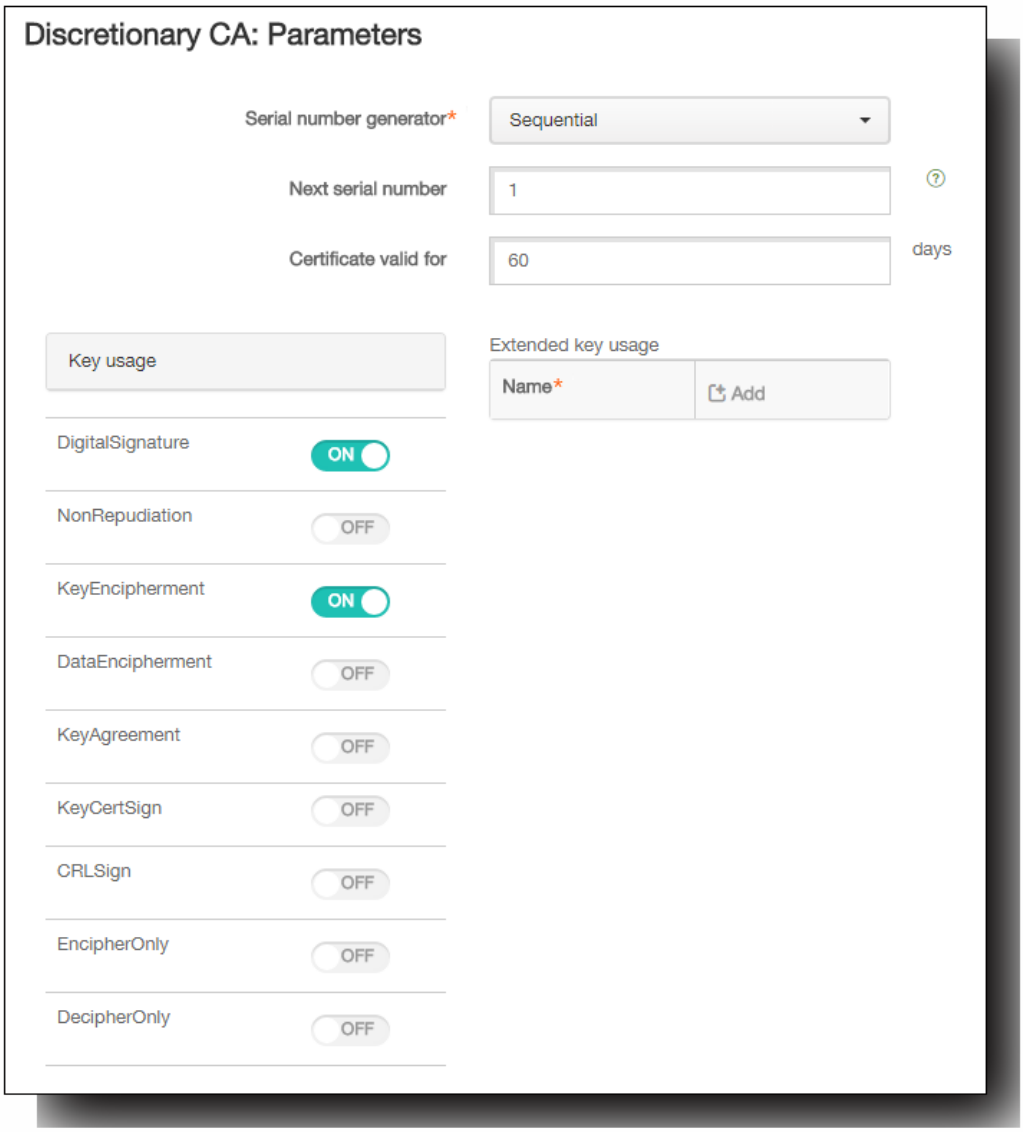
3. Klicken Sie auf Discretionary CA.
   Die Seite Discretionary CA: General Information wird angezeigt.



4. Führen Sie auf der Seite Discretionary CA: General Information folgende Schritte aus:
   1. Name: Geben Sie einen aussagekräftigen Namen für die eigenverwaltete CA ein.
   2. CA certificate to sign certificate requests: Klicken Sie auf das Zertifikat, das von der eigenverwalteten CA zum

Signieren von Zertifikatanforderungen verwendet werden soll. Die Liste der Zertifikate wird aus den von Ihnen über XenMobile at Configure > Settings > Certificates hochgeladenen Zertifizierungsstellenzertifikaten mit privatem Schlüssel generiert.

3. Klicken Sie auf Next.
   Die Seite Discretionary CA: Parameters wird angezeigt.



5. Führen Sie auf der Seite Discretionary CA: Parameters folgende Schritte aus:
   1. Serial number generator: Die eigenverwaltete CA generiert Seriennummern für die von ihr herausgegebenen Zertifikate. Klicken Sie in dieser Liste auf Sequential oder Non-sequential, um zu bestimmen, wie die Nummern generiert werden sollen.
   2. Next serial number: Geben Sie einen Wert für die nächste Seriennummer ein.
   3. Certificate valid for: Geben Sie die Anzahl der Tage ein, für die das Zertifikat gültig sein soll.
   4. Key usage: Legen Sie den Zweck der von der eigenverwalteten CA herausgegebenen Zertifikate fest, indem Sie die entsprechenden Schlüssel auf On setzen. Im Anschluss an diese Einstellung ist die Zertifizierungsstelle auf die Ausstellung von Zertifikaten für diese Zwecke beschränkt.
   5. Extended key usage: Zum Hinzufügen weiterer Parameter klicken Sie auf Add, geben Sie den Schlüsselnamen ein und

klicken Sie auf Save.

6. Klicken Sie auf Next.
   Die Seite Discretionary CA: Distribution wird angezeigt.

6. Wählen Sie auf der Seite Discretionary CA: Distribution einen Verteilungsmodus aus:
   - Centralized: server-side key generation: Citrix empfiehlt diese zentrale Verteilung. Die privaten Schlüssel werden auf dem Server generiert und gespeichert und auf die Benutzergeräte verteilt.
   - Distributed: device-side key generation: Die privaten Schlüssel werden auf den Benutzergeräten generiert und gespeichert. Beim verteilten Modus wird SCEP verwendet und es ist ein RA-Verschlüsselungszertifikat mit keyUsage "keyEncryption" sowie ein RA-Signaturzertifikat mit dem KeyUsage "digitalSignature" erforderlich. Das gleiche Zertifikat kann für Verschlüsselung und Signieren verwendet werden.
7. Klicken Sie auf Next.
   Die Seite Discretionary CA: Online Certificate Status Protocol (OCSP) wird angezeigt.

8. Führen Sie auf der Seite Discretionary CA: Online Certificate Status Protocol (OCSP) folgende Schritte aus:
   1. Wenn Sie den von dieser Zertifizierungsstelle signierten Zertifikaten eine AuthorityInfoAccess (RFC2459)-Erweiterung hinzufügen möchten, legen Sie Enable OCSP support for this CA auf On fest. Diese Erweiterung verweist auf den OCSP-Responder der Zertifizierungsstelle unter https://server/instance/ocsp.
   2. Wenn Sie OCSP-Unterstützung aktiviert haben, wählen Sie ein OSCP-Zertifizierungsstellenzertifikat aus. Die Liste der Zertifikate wird aus den von Ihnen über XenMobile at Configure > Settings > Certificates hochgeladenen Zertifizierungsstellenzertifikaten generiert.
9. Klicken Sie auf Speichern.
   Die eigenverwaltete CA wird in der Tabelle der PKI-Entitäten angezeigt.

Anmeldeinformationsanbieter

Apr 12, 2016

Anmeldeinformationsanbieter sind die Zertifikatkonfigurationen, die Sie in den verschiedenen Teilen des XenMobile-Systems verwenden. Sie definieren Quellen, Parameter und Lebenszyklus der Zertifikate und ob diese Teil der Gerätekonfigurationen oder eigenständig sind (d. h. per Push auf den Geräten bereitgestellt werden).

Die Geräteregistrierung schränkt den Lebenszyklus von Zertifikaten ein. Das bedeutet, dass vor einer Registrierung keine Zertifikate von XenMobile ausgegeben werden, allerdings eventuell im Rahmen der Registrierung. Außerdem werden Zertifikate, die von der internen PKI im Zusammenhang mit einer Registrierung ausgegeben wurden, gesperrt, wenn die Registrierung widerrufen wird. Nach dem Ende der Verwaltungsbeziehung verbleiben keine gültigen Zertifikate.

Sie können eine Anmeldeinformationsanbieter-Konfiguration an verschiedenen Stellen verwenden, eine Konfiguration kann daher beliebig viele Zertifikate zugleich steuern. Dies läuft dann bei der Bereitstellungsressource und der Bereitstellung zusammen. Wenn beispielsweise der Anmeldeinformationsanbieter P auf Gerät D im Rahmen der Konfiguration C bereitgestellt wird, gelten die Ausstellungseinstellungen von P für das auf Gerät D bereitgestellte Zertifikat. Gleichermaßen gelten die Verlängerungseinstellungen von D, wenn C aktualisiert wird, und die Sperreinstellungen für D gelten, wenn C gelöscht oder wenn D widerrufen wird.

Dies bedeutet, dass der Anmeldeinformationsanbieter in XenMobile folgende Aufgaben übernimmt:

- Festlegen der Quelle für Zertifikate
- Festlegen der Methode des Bezugs von Zertifikaten: Signieren eines neuen Zertifikats oder Abruf (Wiederherstellung) eines vorhandenen Zertifikat-/Schlüsselpaars
- Festlegen der Parameter für die Ausstellung/Wiederherstellung von Zertifikaten: beispielsweise CSR-Parameter wie Schlüssellänge, Schlüsselalgorithmus Distinguished Name, Zertifikaterweiterungen usw.
- Festlegen der Art und Weise, in der Zertifikate auf Geräten bereitgestellt werden
- Festlegen von Sperrbedingungen: Zwar werden alle Zertifikate bei Beenden der Verwaltungsbeziehung in XenMobile gesperrt, durch die Konfiguration kann jedoch auch eine frühere Sperrung, z. B. bei Löschen der Gerätekonfiguration, festgelegt sein. Außerdem kann unter bestimmten Bedingungen die Sperrung eines Zertifikats in XenMobile an die Back-End-PKI (Public Key-Infrastruktur) gesendet werden, d. h. die Sperrung in XenMobile kann zur Sperrung in der PKI führen.
- Festlegen der Verlängerungseinstellungen. Über einen bestimmten Anmeldeinformationsanbieter abgerufene Zertifikate können kurz vor ihrem Ablauf automatisch verlängert werden. Davon unabhängig können bei Anstehen des Ablaufs Benachrichtigungen gesendet werden.

Welche Konfigurationsoptionen verfügbar sind, hängt hauptsächlich davon ab, welche PKI-Entität und Ausstellungsmethode Sie für einen Anmeldeinformationsanbieter ausgewählt haben.

Methoden der Zertifikatausstellung

Beim Bezug von Zertifikaten stehen zwei Methoden der Zertifikatausstellung zur Verfügung:

- sign: Bei dieser Methode werden ein privater Schlüssel und eine Zertifikatsignieranforderung (CSR) erstellt und die CSR zum Signieren an eine Zertifizierungsstelle (ZS) übermittelt. XenMobile unterstützt die Methode "sign" für die drei PKI-Entitäten (MS Zertifikatdiensteentität, Generic PKI und Eigenverwaltete ZS).
- fetch: Bei dieser Methode wird ein – für XenMobile – vorhandenes Zertifikat und Schlüsselpaar wiederhergestellt. XenMobile unterstützt die Methode "fetch" nur für Generic PKI.

Ein Anmeldeinformationsanbieter verwendet entweder die Methode "sign" oder "fetch". Die ausgewählte Methode wirkt sich auf die verfügbaren Konfigurationsoptionen aus. CSR-Konfiguration und verteilte Bereitstellung sind nur verfügbar, wenn als Ausstellungsmethode "sign" ausgewählt wird. Bei der Methode "fetch" wird das Zertifikat immer als PKCS#12 an das Gerät gesendet (entspricht der zentralen Bereitstellung der Methode "sign").

Zertifikatbereitstellung

Es gibt zwei Arten der Zertifikatbereitstellung in XenMobile: zentral und verteilt. Im verteilten Modus wird Simple Certificate Enrollment Protocol (SCEP) verwendet. Dies ist nur möglich, wenn der Client das Protokoll unterstützt (nur iOS). Der verteilte Modus ist in manchen Situationen verbindlich.

Damit ein Anmeldeinformationsanbieter die verteilte Bereitstellung mit SCEP unterstützt, ist ein spezieller Konfigurationsschritt, nämlich das Einrichten von Registrierungsstellenzertifikaten (RA-Zertifikate), erforderlich. RA-Zertifikate sind erforderlich, weil XenMobile bei Verwendung von SCEP als Delegate (erweiterte Registrierungsstelle) für die tatsächliche Zertifizierungsstelle fungiert und beim Client nachweisen muss, dass es dazu berechtigt ist. Diese Berechtigung ist durch die Bereitstellung der o. g. Zertifikate für XenMobile gegeben.

Es sind zwei unterschiedliche Zertifikatrollen erforderlich (die allerdings durch ein einzelnes Zertifikat erfüllt werden können): RA-Signatur und RA-Verschlüsselung. Für diese Rollen gilt Folgendes:

- Das RA-Signaturzertifikat muss eine digitale Signatur mit X.509-Schlüsselverwendung haben.
- Das RA-Verschlüsselungszertifikat muss die X.509-Schlüsselchiffrierung haben.

Zum Konfigurieren von RA-Zertifikaten für einen Anmeldeinformationsanbieter müssen Sie die Zertifikate in XenMobile hochladen und dann mit dem Anmeldeinformationsanbieter verknüpfen.

Ein Anmeldeinformationsanbieter unterstützt die verteilte Bereitstellung nur, wenn er ein für Zertifikatrollen konfiguriertes Zertifikat hat. Jeder Anmeldeinformationsanbieter kann so konfiguriert werden, dass er den zentralen Modus oder den verteilten Modus bevorzugt oder den verteilten Modus erfordert. Das Resultat hängt vom Kontext ab: Unterstützt dieser den verteilten Modus nicht und der Modus wird vom Anmeldeinformationsanbieter erfordert, schlägt die Bereitstellung fehl. Erfordert der Kontext den verteilten Modus, aber der Anmeldeinformationsanbieter unterstützt diesen nicht, schlägt die Bereitstellung fehl. In allen anderen Fällen wird der als bevorzugt festgelegte Modus verwendet.

Die folgende Tabelle zeigt die SCEP-Verteilung in XenMobile:

Kontext	SCEP unterstützt	SCEP erforderlich
iOS-Profildienst	Ja	Ja
Registrierung für die iOS-Mobilgeräteverwaltung	Ja	Nein
iOS-Konfigurationsprofile	Ja	Nein
SHTP-Registrierung	Nein	Nein
Konfigurieren von SHTP	Nein	Nein
Windows Phone-Registrierung	Nein	Nein
Windows Phone-Konfiguration	Nein	Nein

Zertifikatsperre

Es gibt drei Arten der Sperre.

- **Interne Sperre**: Die interne Sperre wirkt sich auf den von XenMobile gepflegten Zertifikatstatus aus. Dieser Status wird

berücksichtigt, wenn XenMobile ein eingehendes Zertifikat auswertet oder OCSP-Statusinformationen für ein Zertifikat bereitstellen muss. Die Konfiguration des Anmeldeinformationsanbieters bestimmt, wie sich diverse Bedingungen auf diesen Status auswirken. Beispielsweise kann durch den Anmeldeinformationsanbieter festgelegt sein, dass über den Zertifikatanbieter abgerufene Zertifikate als gesperrt gekennzeichnet werden, wenn sie vom Gerät gelöscht wurden.

- **Extern weitergegebene Sperre**: Eine Sperrung dieser Art (auch "Revocation XenMobile") gilt für von einer externen PKI bezogene Zertifikate. Das Zertifikat wird in der PKI gesperrt, wenn es intern von XenMobile gesperrt wird, unter den in der Anmeldeinformationsanbieter-Konfiguration festgelegten Bedingungen. Der Aufruf zum Ausführen der Sperre erfordert eine Generic PKI-Entität (GPKI) mit Sperrfunktion.
- **Extern durchgeführte Sperre**: Eine Sperrung dieser Art (auch "Revocation PKI") gilt ebenfalls nur für von einer externen PKI bezogene Zertifikate. Beim Auswerten des Status von Zertifikaten fragt XenMobile diesen bei der PKI ab. Ist das Zertifikat gesperrt, wird es von XenMobile intern ebenfalls gesperrt. Bei diesen Methoden wird das OCSP-Protokoll verwendet.

Die drei Arten der Sperre schließen einander nicht aus, sondern gelten gemeinsam: Die interne Sperre wird entweder durch eine externe Sperre ausgelöst oder aber aufgrund anderer Ursachen und sie kann ihrerseits eine externe Sperre nach sich ziehen.

Zertifikatverlängerung

Bei einer Zertifikatverlängerung wird das vorhandene Zertifikat gesperrt und ein neues Zertifikat ausgestellt.

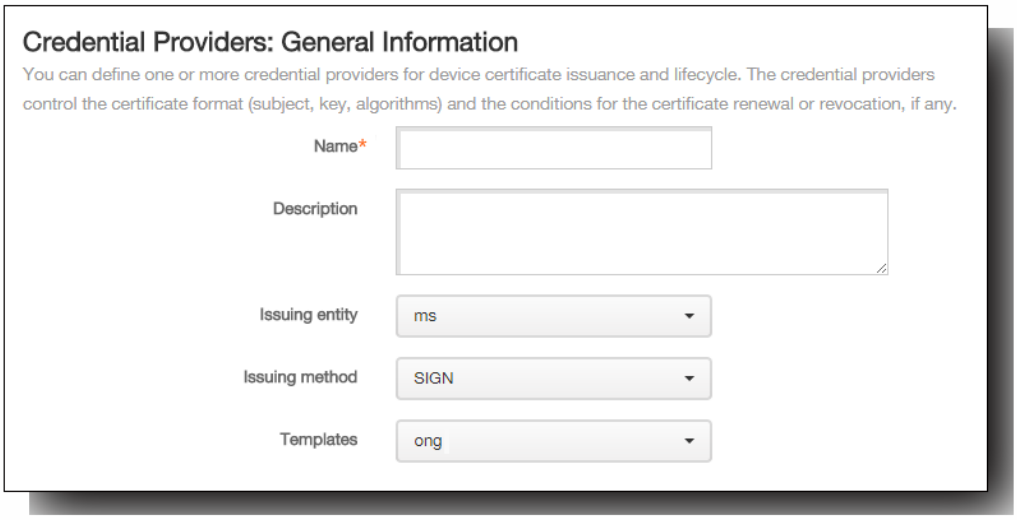
In XenMobile wird vor Sperrung des vorhandenen Zertifikats versucht, das neue Zertifikat abzurufen, um eine Dienstunterbrechung zu vermeiden, wenn die Ausstellung fehlschlägt. Wenn die verteilte (SCEP-unterstützte) Bereitstellung verwendet wird, erfolgt die Sperrung zudem erst, wenn das Zertifikat erfolgreich auf dem Gerät installiert wurde. Ansonsten erfolgt sie vor Senden des neuen Zertifikats an das Gerät und unabhängig von dem Erfolg der Installation.

Die Sperrungskonfiguration erfordert die Angabe eines bestimmten Zeitraums (in Tagen). Wenn ein Gerät eine Verbindung herstellt, wird vom Server geprüft, ob das Datum "NotAfter" für das Zertifikat nach dem aktuellen Datum minus dem angegebenen Zeitraum liegt. Wenn dies der Fall ist, wird eine Verlängerung versucht.

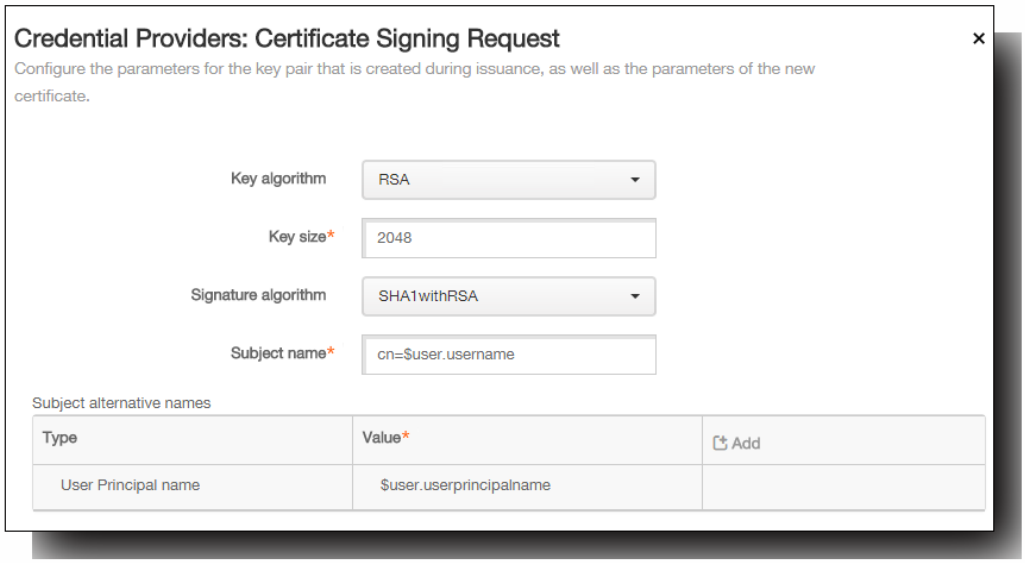
So erstellen Sie einen Anmeldeinformationsanbieter

Die Schritte beim Konfigurieren eines Anmeldeinformationsanbieters variieren hauptsächlich nach ausgewählter ausstellender Entität und Ausstellungsmethode. Man unterscheidet zwischen Anmeldeinformationsanbietern mit einer internen Entität, z. B. einer eigenverwalteten Zertifizierungsstelle, und solchen mit einer externen Entität wie etwa einer Microsoft-Zertifizierungsstelle oder GPKI. Die Ausstellungsmethode bei eigenverwalteten Zertifizierungsstellen ist immer "sign", d. h. bei jeder Ausstellung wird von XenMobile ein neues Schlüsselpaar mit dem für die Entität ausgewählten CA-Zertifikat signiert. Ob das Schlüsselpaar auf dem Gerät oder auf dem Server generiert wird, hängt von der ausgewählten Verteilungsmethode ab.

1. Klicken Sie in der XenMobile-Webkonsole auf Configure > Settings > More > Credential Providers.
2. Klicken Sie auf der Seite Credential Providers auf Add.
   Es wird die Seite Credential Providers: General Information angezeigt.



3. Führen Sie auf der Seite Credential Providers: General Infomation folgende Schritte aus:
    1. Name: Geben Sie einen eindeutigen Namen für die neue Anbieterkonfiguration ein. Unter diesem Namen wird die Konfiguration anschließend in anderen Teilen der XenMobile-Konsole angezeigt.
    2. Description: Geben Sie eine Beschreibung für den Anmeldeinformationsanbieter ein. Dies ist zwar ein optionales Feld, eine Beschreibung kann jedoch nützlich sein, um Ihnen später Details über den Anmeldeinformationsanbieter in Erinnerung zu rufen.
    3. Issuing entity: Klicken Sie auf die ausstellende Entität.
    4. Issuing method: Klicken Sie auf Sign oder Fetch zu Festlegen der Methode für den Bezug von Zertifikaten von der konfigurierten Entität.
    5. Wenn die Vorlagenliste verfügbar ist, wählen Sie eine Vorlage für den Anmeldeinformationsanbieter aus.
    Hinweis: Die Vorlagen werden verfügbar, wenn Microsoft-Zertifikatdienste-Entitäten über Configure > Settings > More > PKI Entities hinzugefügt werden.
    6. Klicken Sie auf Next.
    Es wird die Seite Credential Providers: Certificate Signing Request angezeigt.

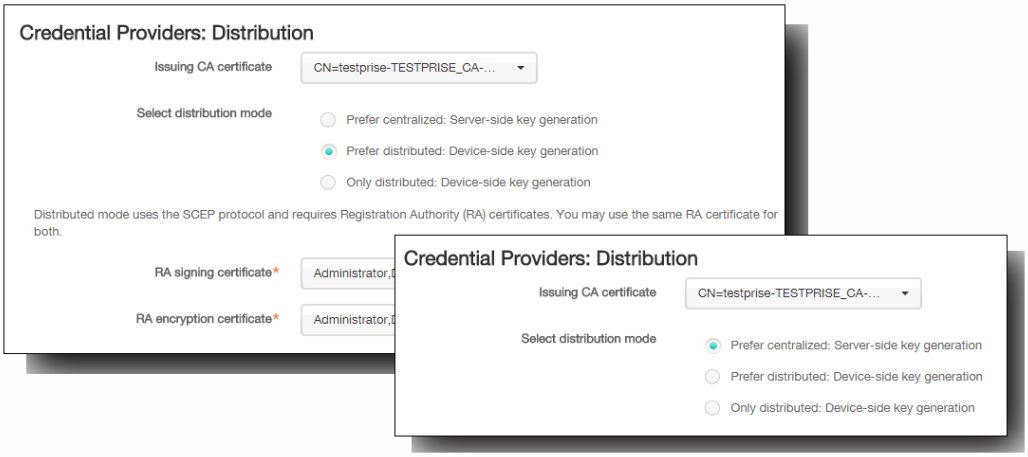


4. Führen Sie auf der Seite Credential Providers: Certificate Signing Request folgende Schritte aus:

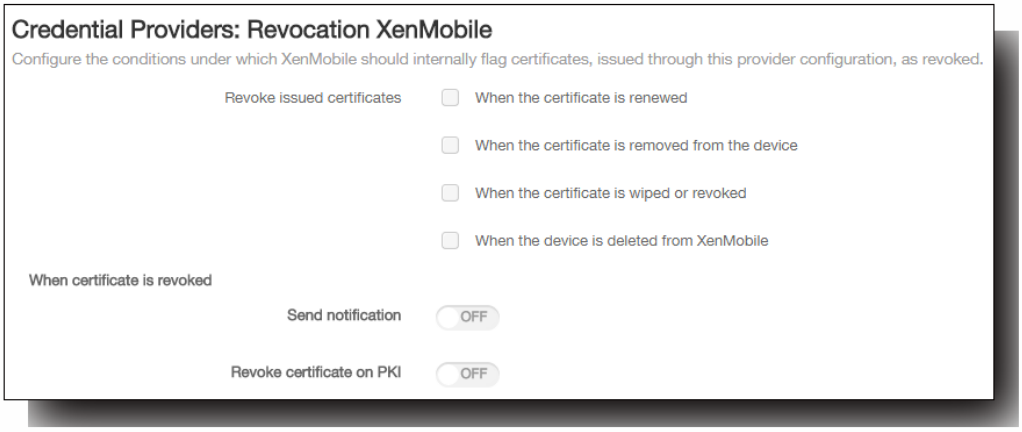
1. Key algorithm: Klicken Sie auf den Schlüsselalgorithmus für das neue Schlüsselpaar. Verfügbare Werte sind RSA, DSA und ECDSA.
2. Key size: Geben Sie Länge des Schlüsselpaars in Bits ein. Dies ist ein Pflichtfeld.
   Hinweis: Welche Werte zulässig sind, hängt von der Art des Schlüssels ab. Die maximale Länge eines DSA-Schlüssels ist beispielsweise 1024 Bit. Zur Vermeidung falscher Negative, die von der verwendeten Hardware oder Software abhängig sind, erzwingt XenMobile keine Schlüssellängen. Anmeldeinformationsanbieter sind vor Übernahme in die Produktionsumgebung immer in einer Testumgebung zu testen.
3. Signature algorithm: Klicken Sie auf einen Wert für das neue Zertifikat. Welche Werte zulässig sind, hängt vom Schlüsselalgorithmus ab.
4. Subject name: Geben Sie den Distinguished Name (DN) des Antragstellers für das neue Zertifikat ein. Beispiel: CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation. Dies ist ein Pflichtfeld.
5. Zum Hinzufügen eines neuen Eintrags zur Tabelle Subject alternative names klicken Sie auf Add. Wählen Sie den Typ des alternativen Namens aus und geben Sie einen Wert in der zweiten Spalte ein.
   Hinweis: Wie beim Antragstellernamen können Sie in dem Wertefeld XenMobile-Makros verwenden.
6. Klicken Sie auf Next.
   Es wird die Seite Credential Providers: Distribution angezeigt.

5. Führen Sie auf der Seite Credential Providers: Distribution folgende Schritte aus:
   1. Klicken Sie in der Liste Issuing CA certificate auf das angebotene ZS-Zertifikat. Da der Anmeldeinformationsanbieter eine eigenverwaltete Zertifizierungsstelle verwendet, erhält er immer das für die Entität selbst konfigurierte CA-Zertifikat. Die Aufführung hier erfolgt aus Gründen der Konsistenz mit Konfigurationen, in denen externe Entitäten verwendet werden.
   2. Wählen Sie für Select distribution mode eine der folgenden Methoden zum Generieren und Verteilen von Schlüsseln aus:
      - Prefer centralized: Server-side key generation: Citrix empfiehlt diese zentralisierte Option. Sie unterstützt alle von XenMobile unterstützten Plattformen und ist erforderlich, wenn die NetScaler Gateway-Authentifizierung verwendet wird. Die privaten Schlüssel werden auf dem Server generiert und gespeichert und auf die Benutzergeräte verteilt.
      - Prefer distributed: Device-side key generation: Die privaten Schlüssel werden auf den Benutzergeräten generiert und gespeichert. Beim verteilten Modus wird SCEP verwendet und es ist ein RA-Verschlüsselungszertifikat mit keyUsage "keyEncryption" sowie ein RA-Signaturzertifikat mit dem KeyUsage "digitalSignature" erforderlich. Das gleiche Zertifikat kann für Verschlüsselung und Signieren verwendet werden.
      - Only distributed: Device-side key generation: Diese Option funktioniert wie Prefer distributed: Device-side key generation, doch da sie anstelle einer Bevorzugung eine Ausschließlichkeit definiert, steht keine Option zur Verfügung, wenn die geräteseitige Schlüsselgenerierung fehlschlägt oder nicht verfügbar ist.

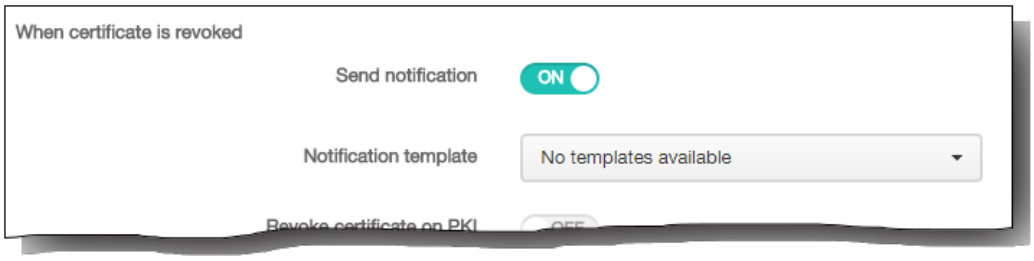
      Bei Auswahl von Prefer distributed: Device-side key generation oder Only distributed: Device-side key generation müssen Sie zusätzlich ein RA-Signaturzertifikat und ein RA-Verschlüsselungszertifikat auswählen. Es werden neue Felder für diese Zertifikate eingeblendet.



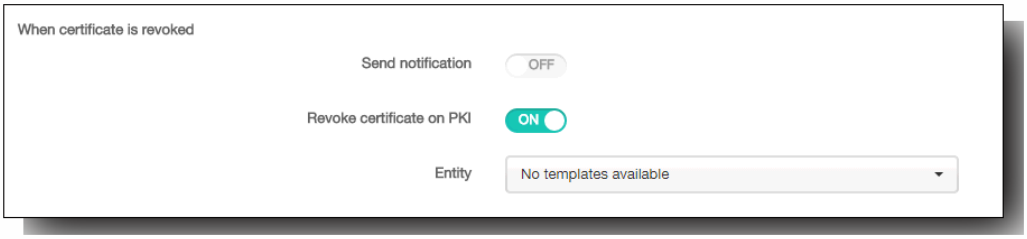
3. Wenn Sie Prefer distributed: Device-side key generation oder Only distributed: Device-side key generation ausgewählt haben, klicken Sie auf das gewünschte RA-Signaturzertifikat und das RA-Verschlüsselungszertifikat. Das gleiche Zertifikat kann für beides verwendet werden.
4. Klicken Sie auf Next.
   Es wird die Seite Credential Providers: Revocation XenMobile angezeigt. Auf dieser Seite konfigurieren Sie die Bedingungen, unter denen XenMobile Zertifikate, die über diese Anbieterkonfiguration ausgestellt wurden, intern als gesperrt kennzeichnet.



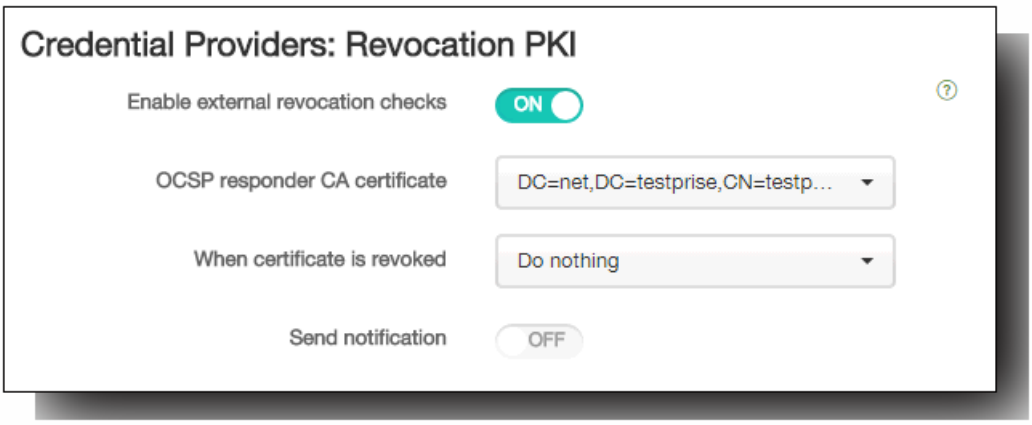
6. Führen Sie auf der Seite Credential Providers: Revocation XenMobile folgende Schritte aus:
   1. Wählen Sie für Revoke issued certificates aus, wann Zertifikate gesperrt werden sollen.
   2. Wenn XenMobile eine Benachrichtigung bei Sperrung des Zertifikats senden soll, legen Sie für Send notification die Einstellung On fest und wählen Sie eine Benachrichtigungsvorlage aus.



3. Wenn das Zertifikat bei Sperrung durch XenMobile in der PKI gesperrt werden soll, legen Sie für Revoke certificate on PKI die Option On fest und klicken Sie in der Liste Entity auf eine Vorlage. Die Liste Entity enthält alle verfügbaren GPKI-Entitäten mit Sperrfunktion. Wenn das Zertifikat von XenMobile gesperrt wird, wird ein Sperraufruf an die in der Liste Entity ausgewählte PKI gesendet.



4. Klicken Sie auf Next.
   Es wird die Seite Credential Providers: Revocation PKI angezeigt. Auf dieser Seite legen Sie fest, welche Aktionen in der PKI auszuführen sind, wenn das Zertifikat gesperrt wird. Darüber hinaus können Sie eine Benachrichtigung einrichten.



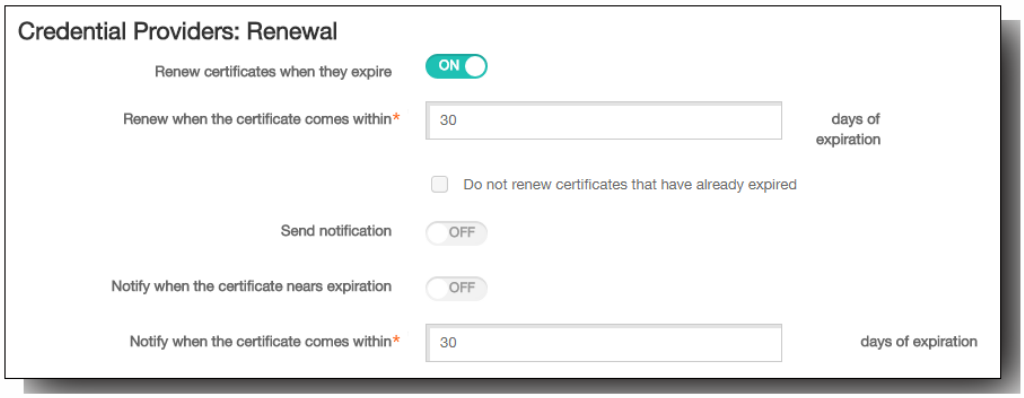
7. Führen Sie auf der Seite Credential Providers: Revocation PKI folgende Schritte aus, wenn Sie Zertifikate über die PKI sperren möchten:
   1. Ändern Sie die Einstellung für Enable external revocation checks in On.
      Zusätzliche Felder für die Sperrung werden angezeigt.
   2. Klicken Sie in der Liste OCSP responder CA certificate auf den Distinguished Name (DN) des Zertifikatantragstellers.
      Hinweis: Sie können XenMobile-Makros für Werte im DN-Feld verwenden. Beispiel: CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation
   3. Klicken Sie in der Liste When certificate is revoked auf eine der folgenden Optionen zum Festzulegen der in der PKI bei Sperrung des Zertifikats auszuführenden Aktionen:
      - Do nothing
      - Renew the certificate
      - Revoke and wipe the device

4. Wenn XenMobile eine Benachrichtigung bei Sperrung des Zertifikats senden soll, legen Sie für Send notification die Einstellung On fest.
   Sie können eine von zwei Benachrichtigungsoptionen auswählen:

   - Mit Select notification template können Sie einen vorhandenen Benachrichtigungstext auswählen und ggf. anpassen. Die entsprechenden Vorlagen sind in der Liste Notification template.
   - Mit Enter notification details können Sie einen eigenen Text eingeben. Neben der E-Mail-Adresse des Empfängers und dem Text können Sie festlegen, wie oft die Benachrichtigung gesendet wird.

5. Klicken Sie auf Next.
   Es wird die Seite Credential Providers: Renewal angezeigt. Auf dieser Seite können Sie für XenMobile die Ausführung folgender Schritte festlegen:
   - Verlängern des Zertifikats, optional Versand einer entsprechenden Benachrichtigung und optional Ausschließen bereits abgelaufener Zertifikate von diesem Vorgang
   - Versand einer Benachrichtigung für Zertifikate, deren Ablauf kurz bevorsteht

8. Führen Sie auf der Seite Credential Providers: Renewal folgende Schritte aus, wenn Zertifikate bei Ablauf verlängert werden sollen:
   1. Legen Sie für Renew certificates when they expire die Option On fest.
      Zusätzliche Felder werden eingeblendet.



   2. Geben Sie im Feld Renew when the certificate comes within die Zeit vor Ablauf des Zertifikats in Tagen ein, zu der die Verlängerung erfolgen soll.
   3. Wählen Sie optional Do not renew certificates that have already expired aus.
      Hinweis: In diesem Zusammenhang bedeutet "already expired", dass das NotAfter-Datum des Zertifikats in der Vergangenheit liegt, und nicht, dass das Zertifikat gesperrt wurde. XenMobile verlängert keine intern gesperrten Zertifikate.
   4. Wenn XenMobile eine Benachrichtigung bei Verlängerung des Zertifikats senden soll, legen Sie Send notification auf On fest.
      Sie können eine von zwei Benachrichtigungsoptionen auswählen:

      - Mit Select notification template können Sie einen vorhandenen Benachrichtigungstext auswählen und ggf. anpassen. Die entsprechenden Vorlagen sind in der Liste Notification template.
      - Mit Enter notification details können Sie einen eigenen Text eingeben. Neben der E-Mail-Adresse des Empfängers und dem Text können Sie festlegen, wie oft die Benachrichtigung gesendet wird.

   5. Wenn XenMobile eine Benachrichtigung bei anstehendem Ablauf des Zertifikats senden soll, legen Sie Notify when certificate nears expiration auf On fest.

Sie können eine von zwei Benachrichtigungsoptionen auswählen:

- Mit Select notification template können Sie einen vorhandenen Benachrichtigungstext auswählen und ggf. anpassen. Die entsprechenden Vorlagen sind in der Liste Notification template.
- Mit Enter notification details können Sie einen eigenen Text eingeben. Neben der E-Mail-Adresse des Empfängers und dem Text können Sie festlegen, wie oft die Benachrichtigung gesendet wird.

6. Geben Sie im Feld Notify when the certificate comes within die Zeit vor Ablauf des Zertifikats in Tagen ein, zu der die Benachrichtigung gesendet werden soll.

9. Klicken Sie auf Save.
   Der neue Anbieter wird der Tabelle der Anmeldeinformationsanbieter hinzugefügt.

Anfordern eines APNs-Zertifikats

Apr 12, 2016

Zum Registrieren und Verwalten von iOS-Geräten mit XenMobile müssen Sie ein Zertifikat von Apple für den Apple Dienst für Push-Benachrichtigungen (Apple Push Notification Service, APNS) erstellen und einrichten. In diesem Abschnitt werden die grundlegenden Schritte zum Anfordern eines APNs-Zertifikats aufgeführt:

- Verwenden eines Computers mit Windows Server 2012 R2 oder Windows Server 2008 R2 und Microsoft Internetinformationsdienste (IIS) oder eines Mac-Computers zum Generieren einer Zertifikatsignieranforderung (Certificate Signing Request, CSR)
- Die CSR muss von Citrix signiert werden.
- Anfordern eines APNs-Zertifikats bei Apple
- Importieren Sie das Zertifikat in XenMobile.

Hinweis:

- Das APNs-Zertifikat von Apple ermöglicht die Mobilgeräteverwaltung über das Apple Push-Netzwerk. Wenn Sie ein Zertifikat aus Versehen oder absichtlich widerrufen, können Sie die Geräte nicht mehr verwalten.
- Wenn Sie mit dem iOS Developer Enterprise Program ein Push-Zertifikat für die Mobilgeräteverwaltung erstellt haben, müssen Sie ggf. aufgrund der Migration vorhandener Zertifikate zum Apple Push Certificates Portal Schritte unternehmen.

Folgende Themen in der Reihenfolge ihrer Auflistung enthalten grundlegende Informationen zu den Verfahren:

Schritt 1	Erstellen einer Zertifikatsignieranforderung in IIS Erstellen einer Zertifikatsignieranforderung auf einem Mac	Generieren Sie eine Zertifikatsignieranforderung auf einem Computer mit Windows Server 2012 R2 oder Windows Server 2008 R2 und Microsoft IIS oder auf einem Mac Computer. Citrix empfiehlt diese Methode.
Schritt 2	Signieren der Zertifikatsignieranforderung (CSR)	Laden Sie die CSR auf die XenMobile APNs CSR Signing-Website von Citrix hoch (MyCitrix-ID erforderlich). Citrix signiert die Zertifikatsignieranforderung mit seinem Zertifikat für die Mobilgeräteverwaltung und sendet die signierte Datei im PLIST-Format zurück.
Schritt 3	Senden der signierten Zertifikatsignieranforderung an Apple	Senden Sie die signierte Zertifikatsignieranforderung an Apple über das Apple Push Certificate Portal (Apple-ID erforderlich) und laden Sie das APNs-Zertifikat von Apple herunter.
Schritt 4	Erstellen eines PFX-Zertifikats für APNs mit Microsoft IIS Erstellen eines PFX-Zertifikats für APNs auf einem Macintosh-Computer	Exportieren Sie das APNS-Zertifikat als PCKS#12-Zertifikat (PFS-Format) in IIS, Mac oder SSL.

	Erstellen eines PFX-Zertifikats für APNs mit OpenSSL	
Schritt 5	Importieren eines APNs-Zertifikats in XenMobile	Importieren Sie das Zertifikat in XenMobile.

Informationen zur Apple MDM-Pushzertifikatmigration

Im iOS Developer Enterprise Program erstellte MDM-Pushzertifikate wurden in das Apple Push Certificate Portal migriert. Diese Migration wirkt sich auf die Erstellung neuer MDM-Pushzertifikate und auf Verlängerung, Sperrung und Download bestehender MDM-Pushzertifikate aus. Die Migration hat keine Auswirkungen auf andere (nicht für MDM verwendete) APNs-Zertifikate.

Wurde Ihr MDM-Pushzertifikat im iOS Developer Enterprise Program erstellt, gilt Folgendes:

- Das Zertifikat wurde automatisch migriert.
- Sie können das Zertifikat über das Apple Push Certificate Portal verlängern, ohne dass dies Auswirkungen auf die Benutzer hat.
- Für die Sperrung oder den Download eines vorhandenen Zertifikats müssen Sie das iOS Developer Enterprise Program verwenden.

Steht bei keinem Ihrer MDM-Pushzertifikate ein Ablauf an, müssen Sie nichts tun. Wenn bei einem Ihrer MDM-Pushzertifikate der Ablauf ansteht, wenden Sie sich an Ihren MDM-Lösungsanbieter. Die bei Ihnen für das iOS Developer Program zuständige Person muss sich dann beim Apple Push Certificate Portal mit ihrer Apple-ID anmelden.

Alle neuen MDM-Pushzertifikate müssen über das Apple Push Certificate Portal erstellt werden. Im iOS Developer Enterprise Program ist keine weitere Erstellung einer App-ID mit Paketbezeichner (siehe Abschnitt "APNs"), die "com.apple.mgmt" enthält, mehr möglich.

Hinweis: Sie müssen die beim Erstellen des Zertifikats verwendete Apple-ID aufbewahren. Bei der Apple-ID muss es sich außerdem um eine Unternehmens-ID und nicht um eine private ID handeln.

Erstellen einer Zertifikatsignieranforderung mit Microsoft IIS

Der erste Schritt zum Generieren einer APNs-Zertifikatanforderung für iOS-Geräte ist das Erstellen einer Zertifikatsignieranforderung (Certificate Signing Request, CSR). Auf einem Computer mit Windows Server 2012 R2 oder Windows Server 2008 R2 können Sie eine CSR mit Microsoft IIS generieren.

1. Öffnen Sie Microsoft IIS.
2. Doppelklicken Sie auf das Serverzertifikatesymbol für IIS.
3. Klicken Sie im Fenster "Serverzertifikate" auf **Zertifikatanforderung erstellen**.
4. Geben Sie den richtigen Distinguished Name (DN) ein und klicken Sie auf **Weiter**.
5. Wählen Sie als Kryptografieanbieter **Microsoft RSA SChannel Cryptographic Provider** und als Bitlänge **2048** aus und klicken Sie auf **Weiter**.
6. Geben Sie einen speicherortspezifischen Dateinamen zum Speichern der CSR ein und klicken Sie dann auf **Fertig stellen**.

Erstellen einer Zertifikatsignieranforderung auf einem Macintosh-Computer

1. Starten Sie auf einem Computer mit Mac OS X unter **Anwendungen** > **Dienstprogramme** die Anwendung Keychain Access.
2. Öffnen Sie das Menü **Keychain Access** und klicken Sie auf **Preferences**.
3. Ändern Sie auf der Registerkarte **Certificates** die die Einstellung für **OCSP** und **CRL** in **Off** und schließen Sie das Fenster "Preferences".
4. Klicken Sie im **Keychain Access**-Menü auf **Certificate Assistant** > **Request a Certificate From a Certificate Authority**.
5. Der Zertifikatassistent fordert Sie zur Eingabe folgender Informationen auf:
   1. **Email Address**: E-Mail-Adresse des Benutzer- bzw. Rollenkontos, das zum Verwalten des Zertifikats verwendet wird.
   2. **Common Name**: allgemeiner Name des Benutzer- bzw. Rollenkontos, das zum Verwalten des Zertifikats verwendet wird.
   3. **CA Email Address**: E-Mail-Adresse der Zertifizierungsstelle.
6. Wählen Sie die Optionen **Saved to disk** und **Let me specify key pair information** und klicken Sie auf **Continue**.
7. Geben Sie einen Namen für die CSR-Datei ein, speichern Sie die Datei auf Ihrem Computer und klicken Sie dann auf **Save**.
8. Als Schlüsselpaarinformationen wählen Sie für **Key Size** den Wert "2048 bits" und unter **RSA algorithm** den RSA-Algorithmus aus. Klicken Sie dann auf **Continue**. Die CSR-Datei kann nun als Teil des APNs-Zertifikatverfahrens hochgeladen werden.
9. Klicken Sie auf **Done**, wenn die Erstellung der CSR durch den Zertifikatsassistenten abgeschlossen ist.

Erstellen einer Zertifikatsignieranforderung mit Open SSL

Wenn Sie keinen Computer mit Windows Server 2012 R2 oder Windows Server 2008 R2 und Microsoft Internetinformationsdiensten (IIS) oder keinen Mac-Computer zum Generieren einer Zertifikatsignieranforderung (Certificate Signing Request, CSR) für ein APNs-Zertifikat verwenden können, können Sie OpenSSL verwenden.

Hinweis: Für die CSR-Erstellung mit OpenSSL müssen Sie zuerst OpenSSL von der OpenSSL-Website herunterladen und installieren.

1. Führen Sie auf dem Computer, auf dem Sie OpenSSL installiert haben, folgenden Befehl an einer Eingabeaufforderung oder Shell aus.
   openssl req -new -keyout Customer.key.pem –out CompanyAPNScertificate.csr -newkey rsa:2048

2. Die folgende Meldung bezüglich der Informationen für die Zertifikatbenennung wird angezeigt. Geben Sie die Informationen wie angefordert ein.
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.

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

3. Geben Sie bei der nächsten Meldung ein Kennwort für den privaten CSR-Schlüssel ein.
   Please enter the following 'extra' attributes
   to be sent with your certificate request
   A challenge password []:
   An optional company name []:

4. Senden Sie die CSR an Citrix.

Citrix erstellt die signierte CSR und sendet sie per E-Mail an Sie zurück.

Signieren der Zertifikatsignieranforderung (CSR)

Bevor Sie das Zertifikat an Apple senden können, muss dieses von Citrix signiert werden, damit es mit XenMobile verwendet werden kann.

1. Rufen Sie im Browser die Website XenMobile APNs CSR Signing auf.
2. Klicken Sie auf **Upload the CSR**.
3. Navigieren Sie zu dem Zertifikat und wählen Sie es aus.
   Hinweis: Das Zertifikat muss im PEM/TXT-Format vorliegen.

4. Klicken Sie auf der Seite"XenMobile APNs CSR Signing" auf **Sign**. Die CSR wird signiert und automatisch im konfigurierten Downloadordner gespeichert.

Übermitteln der signierten CSR an Apple für den Erhalt eines APNs-Zertifikats

Nach Erhalt der signierten CSR von Citrix müssen Sie diese an Apple senden, um das APNs-Zertifikat zu erhalten.

Hinweis: Es gibt Berichte über Probleme mit der Anmeldung beim Apple Push Certificate Portal. Alternativ können Sie sich beim Apple Developer Portal anmelden (http://developer.apple.com/devcenter/ios/index.action), bevor Sie den Link "identity.apple.com" in Schritt 1 aufrufen.

1. Rufen Sie in einem Browser https://identity.apple.com/pushcert auf.
2. Klicken Sie auf **Create a Certificate**.
3. Wenn Sie zum ersten Mal ein Zertifikat von Apple anfordern, aktivieren Sie das Kontrollkästchen **I have read and agree to these terms and conditions** und klicken Sie auf **Accept**.
4. Klicken Sie auf **Choose File**, navigieren Sie auf Ihrem Computer zu der signierten CSR und klicken Sie auf **Upload**. Es müsste eine Bestätigungsmeldung angezeigt werden, dass der Upload erfolgreich war.
5. Klicken Sie auf **Download**, um das Zertifikat (PEM-Datei) herunterzuladen.
   Hinweis: Wenn Sie Internet Explorer verwenden und die Dateinamenerweiterung fehlt, klicken Sie zwei Mal auf **Cancel** und führen Sie den Download über das nächste Fenster aus.

Erstellen eines PFX-Zertifikats für APNs mit Microsoft IIS

Zum Verwenden eines APNS-Zertifikats von Apple in XenMobile müssen Sie die Zertifikatanforderung in Microsoft IIS abschließen, das Zertifikat als PCKS#12-Datei (.pfx) exportieren und dann das APNS-Zertifikat in XenMobile importieren.

Wichtig: Für diese Aufgabe müssen Sie den gleichen IIS-Server verwenden wie für die Erstellung der Zertifikatsignieranforderung.

1. Öffnen Sie Microsoft IIS.
2. Klicken Sie auf das Serverzertifikatesymbol.
3. Klicken Sie im Fenster **Serverzertifikate** auf **Zertifikatanforderung abschließen**.

4. Navigieren Sie zu der Datei Certificate.pem von Apple. Geben dann Sie einen Anzeigenamen oder den Zertifikatnamen ein und klicken Sie auf **OK**.
5. Wählen Sie das in Schritt 4 angegebene Zertifikat aus und klicken Sie dann auf **Exportieren**.
6. Geben Sie einen Speicherort und Dateinamen für die PFX-Zertifikatdatei sowie ein Kennwort ein und klicken Sie dann auf **OK**.
   Hinweis: Sie benötigen das Kennwort für das Zertifikat während der Installation von XenMobile.
7. Kopieren Sie die PFX-Zertifikatdatei auf den Server, auf dem XenMobile installiert werden soll.
8. Melden Sie sich an der XenMobile-Konsole als Administrator oder als Benutzer mit Zugriff auf die Registerkarte **Info** an.
9. Klicken Sie auf die Registerkarte **Info** und dann auf **Update APNs Certificate**.
10. Navigieren Sie im Dialogfeld **Update APNs Certificate** zu der PFX-Datei des APNs-Zertifikats und geben Sie ein neues Kennwort ein.
11. Klicken Sie auf **Load APNs Certificate**.
12. Klicken Sie auf **Update**.

Erstellen eines PFX-Zertifikats für APNs auf einem Macintosh-Computer

1. Suchen Sie auf dem Macintosh-Computer mit Mac OS X, auf dem Sie die Zertifikatsignieranforderung erstellt haben, das von Apple erhaltene PEM-Zertifikat.
2. Doppelklicken Sie auf die Zertifikatdatei, um sie in die Schlüsselsammlung zu importieren.
3. Wenn Sie aufgefordert werden, das Zertifikat einer bestimmten Schlüsselsammlung hinzuzufügen, lassen Sie die Standardanmelde-Schlüsselsammlung ausgewählt und klicken Sie dann auf **OK**. Das neu hinzugefügte Zertifikat wird nun in der Liste der Zertifikate angezeigt.
4. Klicken Sie im Menü **Datei** auf das Zertifikat und dann auf **Exportieren**, um es in ein PCKS#12-Zertifikat (PFX-Datei) zu exportieren.
5. Legen Sie einen eindeutigen Namen für die Zertifikatdatei zur Verwendung auf dem XenMobile-Server fest, wählen Sie einen Ordner als Speicherort für das Zertifikat aus, wählen Sie die PFX-Datei und klicken Sie auf **Speichern**.
6. Geben Sie ein Kennwort zum Exportieren des Zertifikats ein. Citrix empfiehlt die Verwendung eines eindeutigen sicheren Kennworts. Bewahren Sie außerdem Zertifikat und Kennwort zur späteren Verwendung auf.
7. Keychain Access fordert Sie zur Eingabe des Anmeldekennworts oder der ausgewählten Schlüsselsammlung auf. Geben Sie das Kennwort ein und klicken Sie dann auf **OK**. Das gespeicherte Zertifikat kann nun auf dem XenMobile-Server verwendet werden.
   Hinweis: Wenn Sie den Computer und das Benutzerkonto, den bzw. das Sie zum Generieren der Zertifikatsignieranforderung und zum Exportieren des Zertifikats verwendet haben, nicht behalten möchten, empfiehlt Citrix, den privaten und den öffentlichen Schlüssel aus dem lokalen System zu speichern oder zu exportieren. Ansonsten wird der Zugriff auf APNs-Zertifikate zur Wiederverwendung ungültig und Sie müssen das gesamte Verfahren zum Erstellen von Zertifikatsignieranforderung und APNs-Zertifikat wiederholen.

Erstellen eines PFX-Zertifikats für APNs mit OpenSSL

Nachdem Sie mit OpenSSL eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) erstellt haben, können Sie mit OpenSSL auch ein PFX-Zertifikat für APNs erstellen.

1. Führen Sie an einer Eingabeaufforderung oder Shell folgenden Befehl aus:
   openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12
2. Geben Sie ein Kennwort für die PFX-Datei ein. Merken Sie sich das Kennwort, denn Sie benötigen es erneut, wenn Sie das Zertifikat in XenMobile hochladen.
3. Notieren Sie den Speicherort der PFX-Zertifikatdatei und kopieren Sie die Datei auf den XenMobile-Server, damit Sie sie

mit der XenMobile-Konsole hochladen können.

Importieren eines APNs-Zertifikats in XenMobile

Nachdem Sie ein neues APNS-Zertifikat angefordert und empfangen haben, importieren Sie das APNS-Zertifikat in XenMobile – entweder als erstes Zertifikat oder als Ersatz für ein vorhandenes Zertifikat.

1. Melden Sie sich an der XenMobile-Konsole als Administrator an.
2. Klicken Sie auf **Configure** > **Settings** > **Certificates**.
3. Klicken Sie auf der Seite **Certificates** auf **Import**. Das Dialogfeld **Import** wird angezeigt.
4. Navigieren Sie zu der P12-Datei auf Ihrem Computer.
5. Geben Sie ein Kennwort ein und klicken Sie auf **Import**.

Weitere Informationen über Zertifikate in XenMobile finden Sie im Abschnitt Zertifikate.

Erneuern eines APNs-Zertifikats

Zum Erneuern eines APNs-Zertifikats führen Sie dieselben Schritte aus wie beim Erstellen eines Zertifikats. Anschließend laden Sie das Zertifikat im Apple Push Certificates Portal hoch. Nach der Anmeldung wird Ihr vorhandenes Zertifikat oder ein aus Ihrem vorherigen Apple Developer-Konto importiertes Zertifikat angezeigt. Der einzige Unterschied beim Erneuern eines Zertifikats im Portal besteht darin, dass Sie auf **Renew** klicken. Sie müssen ein Developer-Konto für das Portal haben, um auf die Website zugreifen zu können.

Hinweis: Um herauszufinden, wann Ihr APNs-Zertifikat abläuft, klicken Sie in der XenMobile-Konsole auf **Configure** > **Settings** > **Certificates**. Ist das Zertifikat abgelaufen, müssen Sie es nicht widerrufen.

1. Generieren Sie eine Zertifikatsignieranforderung mit Microsoft Internetinformationsdienste (IIS).
2. Laden Sie die neue CSR auf die XenMobile APNs CSR Signing-Website hoch und klicken Sie dann auf **Sign**.
3. Senden Sie die signierte Zertifikatsignieranforderung im Apple Push Certificate Portal an Apple.
4. Klicken Sie auf **Renew**.
5. Generieren Sie ein PCKS#12-APNs-Zertifikat (PFX-Datei) mit Microsoft IIS.
6. Aktualisieren Sie das neue APNs-Zertifikat in XenMobile, indem Sie auf **Configure** > **Settings** > **Certificates** klicken.
7. Importieren Sie das neue Zertifikat im Dialogfeld **Import**.

NetScaler Gateway und XenMobile

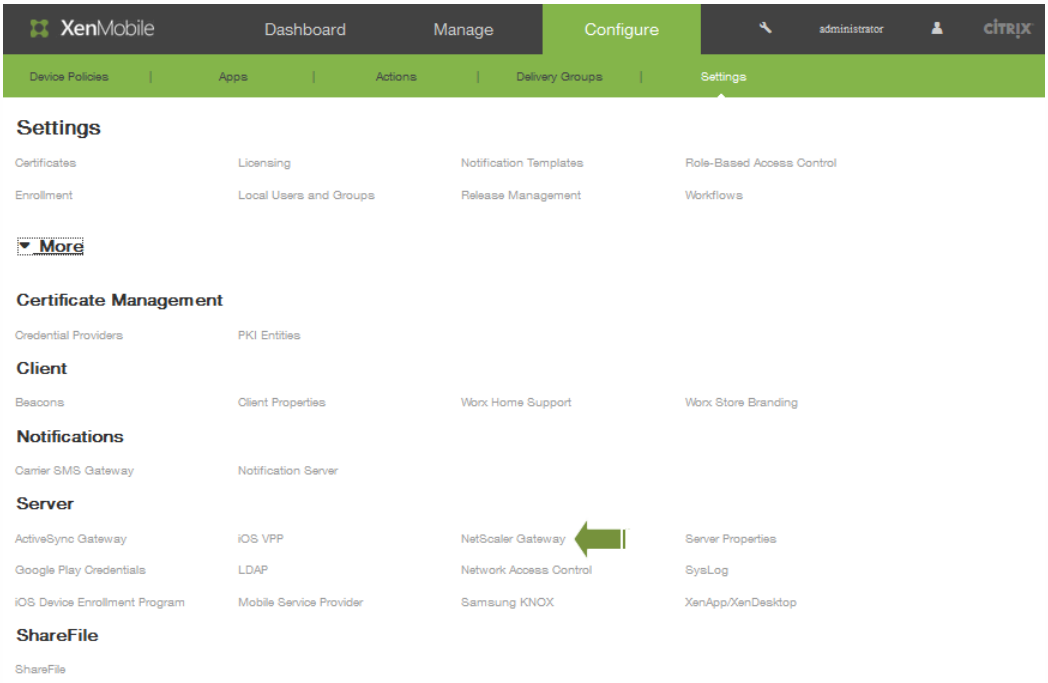
Apr 12, 2016

Bei der Konfiguration von NetScaler Gateway mit XenMobile erstellen Sie die Authentifizierungsmethode für den Remote-Gerätezugriff auf das interne Netzwerk. Mit dieser Funktionalität können Apps auf einem Mobilgerät auf Unternehmensserver im Intranet zugreifen, indem ein Micro VPN von den Apps zu NetScaler Gateway erstellt wird. Sie konfigurieren NetScaler Gateway in der XenMobile-Konsole.

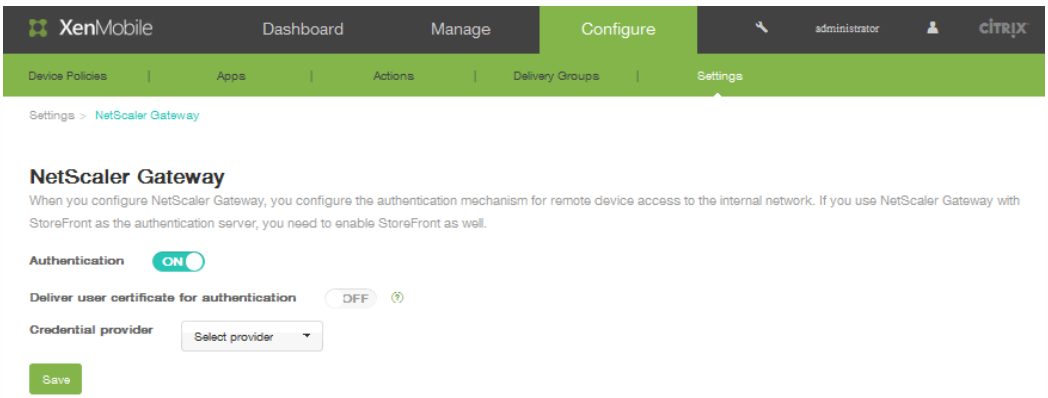
Hinweis: Informationen zum Einrichten von NetScaler Gateway für XenMobile in NetScaler finden Sie unter Configuring Settings for Your XenMobile Environment.

So konfigurieren Sie NetScaler Gateway

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > NetScaler Gateway.



2. Legen Sie für Authentication die Einstellung ON fest.



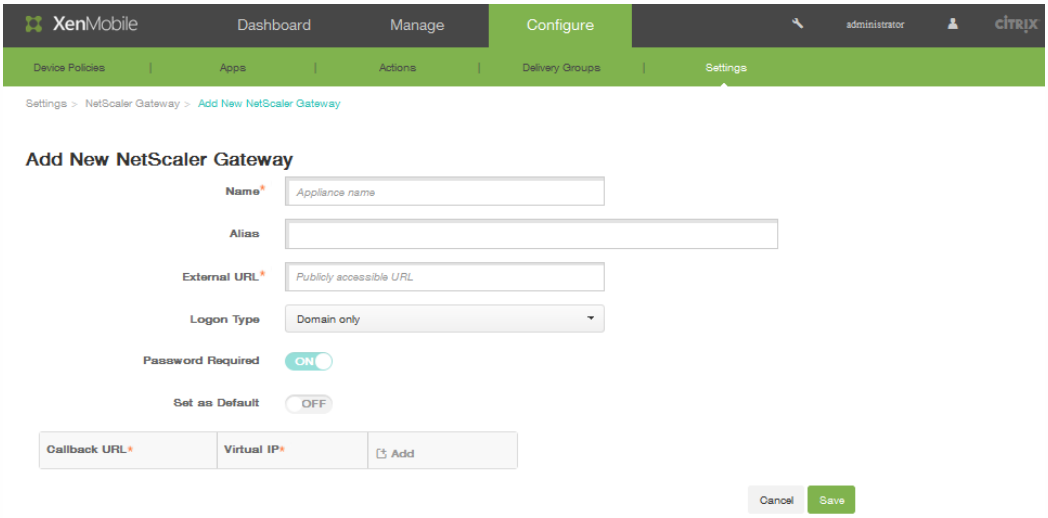
3. Wenn Sie möchten, dass XenMobile das Authentifizierungszertifikat mit Worx Home gemeinsam verwendet, sodass

NetScaler Gateway die Clientzertifikatauthentifizierung abwickelt, wählen Sie für Deliver user certificate for authentication die Einstellung ON.

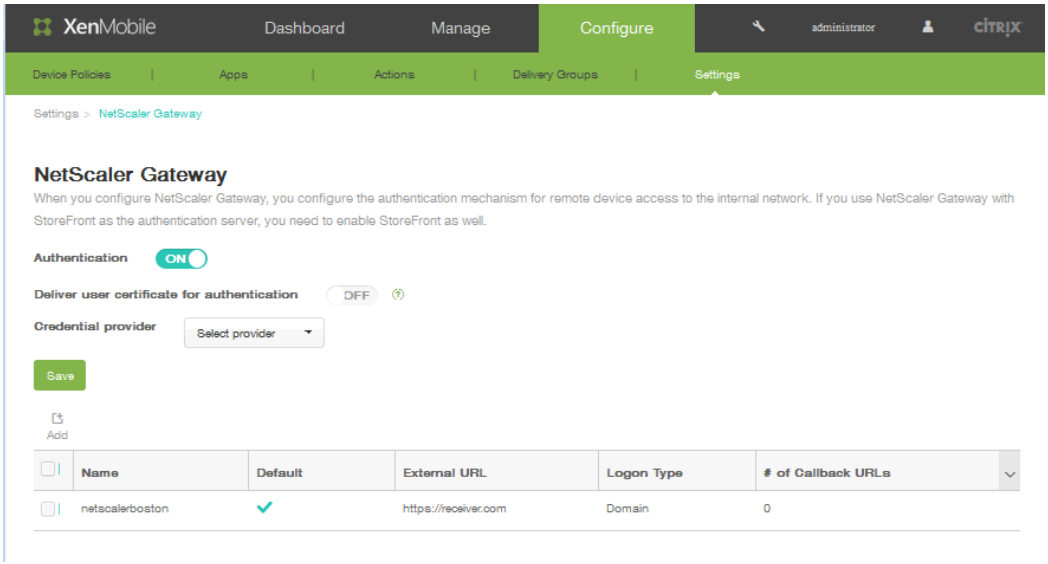
4. Klicken Sie in der Liste Credential Provider auf den Anmeldeinformationsanbieter. Weitere Informationen finden Sie unter Anmeldeinformationsanbieter.
5. Klicken Sie auf Speichern.

So fügen Sie eine neue NetScaler Gateway-Instanz hinzu

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > NetScaler Gateway.
2. Klicken Sie oberhalb der Tabelle auf Add. Die Seite Add New NetScaler Gateway wird angezeigt.

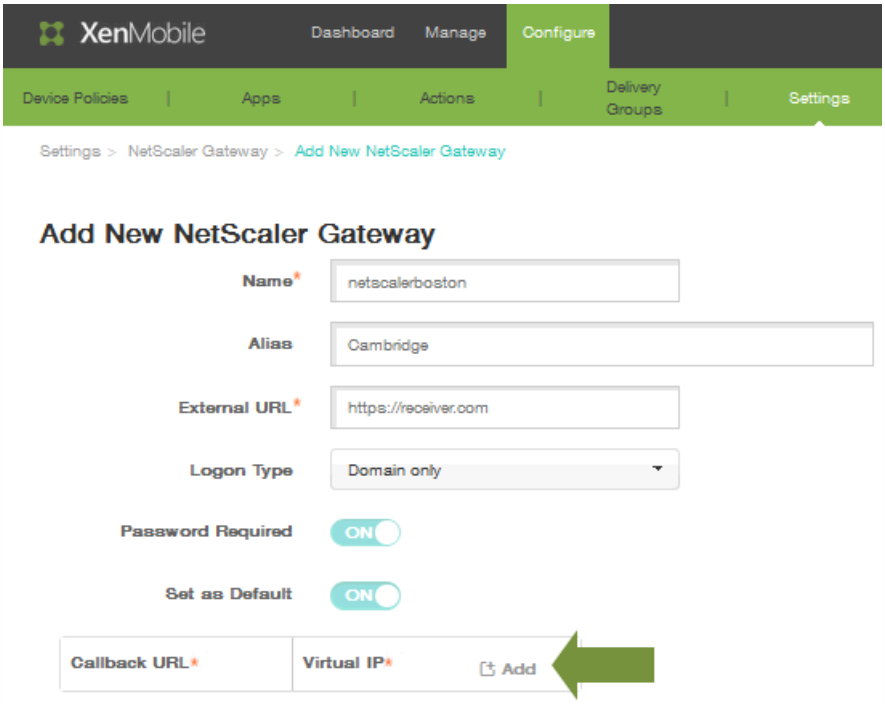


3. Geben Sie unter Name einen Namen für die NetScaler Gateway-Instanz ein.
4. Geben Sie optional unter Alias ein Alias ein.
5. Geben Sie unter External URL die öffentlich zugängliche URL für NetScaler Gateway ein. Beispiel: https://receiver.com.
6. Klicken Sie in der Liste Logon Type auf einen Anmeldetyp. Zur Auswahl stehen Domain only, Security token only, Domain and security token, Certificate, Certificate and domain und Certificate and security token. Standardmäßig ist der Anmeldetyp auf **Domain only** eingestellt. Wenn Sie mehrere Domänen haben, funktioniert **Domain only** nicht, sondern Sie müssen **Certificate and domain** verwenden. Bei einigen Optionen, z. B. Domain only, können Sie das Feld Password nicht ändern. Bei diesem Anmeldetyp gilt für das Feld immer die Einstellung ON. Außerdem ändern sich die Standardwerte des Felds Password Requiredje nach der Auswahl unter Logon Type.
7. Wählen Sie für **Password Required** die Einstellung ON, wenn Sie eine Kennwortauthentifizierung erzwingen möchten.
8. Wählen Sie für **Set as Default** die Einstellung ON, um diese NetScaler Gateway-Instanz als Standard zu verwenden.
9. Klicken Sie auf **Save**. Die neue NetScaler Gateway-Instanz wird hinzugefügt und in der Tabelle angezeigt. Sie können eine Instanz bearbeiten oder löschen, indem Sie auf deren Namen in der Liste klicken.



Nach dem Hinzufügen der NetScaler Gateway-Instanz können Sie eine Callback-URL hinzufügen und eine virtuelle IP-Adresse für das NetScaler Gateway VPN angeben. **Hinweis**: Dies ist optional, kann aber für zusätzliche Sicherheit konfiguriert werden, insbesondere dann, wenn der XenMobile-Server in der DMZ ist.

1. Wählen Sie auf der Seite "NetScaler Gateway" die NetScaler Gateway-Instanz in der Tabelle aus und klicken Sie auf **Add**.
2. Klicken Sie auf der Seite Add New NetScaler Gateway in der Tabelle mit den Callback-URLs auf Add.



3. Geben Sie die **Callback-URL** ein. Das Feld enthält den vollqualifizierten Domänennamen (FQDN) und prüft, ob die Anforderung von NetScaler Gateway stammt.

4. Geben Sie die virtuelle IP-Adresse für NetScaler Gateway ein und klicken Sie auf **Save**.

Konfigurieren von LDAP

Oct 29, 2015

Sie können in XenMobile eine Verbindung mit einem oder mehreren Verzeichnissen, z. B. Active Directory, konfigurieren. Sie verwenden dann die LDAP-Konfiguration für den Import von Gruppen, Benutzerkonten und zugehörigen Eigenschaften. LDAP ist ein herstellerneutrales Open-Source-Anwendungsprotokoll zur Verwaltung eines verteilten Verzeichnisinformationsdiensts über ein Internet Protocol-Netzwerk. Verzeichnisinformationsdienste werden verwendet, um Informationen zu Benutzern, Systemen, Netzwerken, Diensten und Anwendungen über das Netzwerk zu teilen. Häufig wird LDAP zur Bereitstellung von Single Sign-On (SSO) für Benutzer verwendet. Beim SSO wird ein Kennwort pro Benutzer für mehrere Dienste gemeinsam verwendet, sodass sich der Benutzer einmal bei einer Unternehmens-Website anmelden kann und dann automatisch im Intranet des Unternehmens angemeldet wird.

Funktionsweise von LDAP

Ein Client beginnt eine LDAP-Sitzung durch Herstellen einer Verbindung mit einem LDAP-Server (dem Directory System Agent, DSA). Der Client sendet eine Vorgangsanforderung an den Server, der die entsprechende Authentifizierung zurückgibt.

So konfigurieren Sie LDAP-Verbindungen in XenMobile

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > LDAP.
   Die Seite LDAP wird angezeigt.

2. Klicken Sie auf Add.
   Die Seite Add LDAP wird angezeigt.

3. Konfigurieren Sie die folgenden Einstellungen:
   - Directory type: Klicken Sie auf den verwendeten Verzeichnistyp. Standardmäßig ist Microsoft Active Directory ausgewählt.
   - Primary server: Geben Sie den für LDAP verwendeten primären Server an. Sie können die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) eingeben.
   - Secondary server: Geben Sie optional die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) für den sekundären Server (sofern konfiguriert) ein.
   - Port: Geben Sie die Portnummer des LDAP-Servers ein. Die Standardeinstellung für unsichere LDAP-Verbindungen ist 389. Verwenden Sie Port 636 für sichere LDAP-Verbindungen, 3268 für unsichere Microsoft-LDAP-Verbindungen oder 3269 für sichere Microsoft-LDAP-Verbindungen.
   - Domain name: Geben Sie den Domänennamen ein.
   - User base DN: Geben Sie den Speicherort von Benutzern in Active Directory über einen eindeutigen Bezeichner ein. Syntaxbeispiele: ou=users, dc=example oder dc=com.
   - Group base DN: Geben Sie den Gruppen-Basis-DN-Namen gemäß dem Muster cn=Gruppenname ein. Beispiel: cn=users, dc=servername, dc=net, wobei "cn=users" der Gruppenname ist und "DN" und "servername" den Namen des Servers, auf dem Active Directory ausgeführt wird, angeben.
   - User ID: Geben Sie die dem Active Directory-Konto zugeordnete Benutzer-ID ein.
   - Password: Geben Sie das dem Benutzer zugeordnete Kennwort ein.
   - Domain alias: Geben Sie ein Alias für den Domänennamen ein.
   - XenMobile Lockout Limit: Geben Sie eine Zahl zwischen 0 und 999 für die Anzahl zulässiger fehlgeschlagener Anmeldeversuche ein. Wenn Sie 0 festlegen, wird der Benutzer nie aufgrund fehlgeschlagener Anmeldeversuche aus XenMobile ausgesperrt.

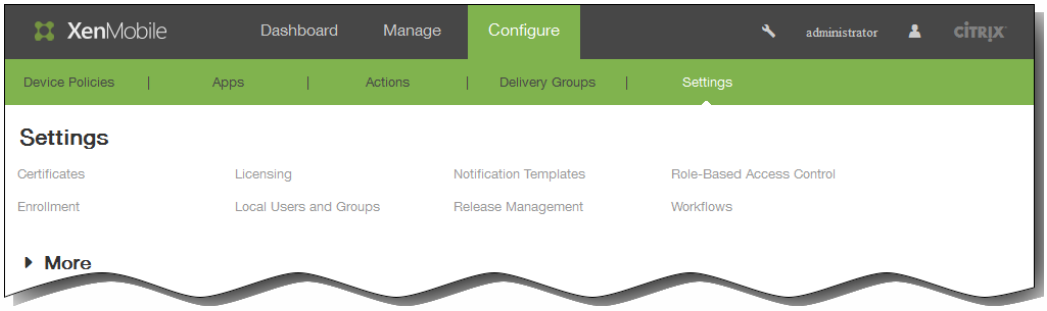
- XenMobile Lockout Time: Geben Sie eine Zahl zwischen 0 und 99999 für den Zeitraum in Minuten ein, den ein Benutzer nach einer Überschreitung des Sperrlimits abwarten muss. Wenn Sie 0 festlegen, muss der Benutzer nach einer Sperrung nicht warten.
- Global Catalog TCP Port: Geben Sie die TCP-Portnummer des Servers für den globalen Katalog ein. Die Standard-TCP-Portnummer ist 3268. Verwenden Sie für SSL-Verbindungen die Portnummer 3269.
- Global Catalog Root Context: Geben Sie optional den Stammkontext für den globalen Katalog ein, der eine Suche im globalen Katalog von Active Directory ermöglicht. Diese Suchfunktion existiert zusätzlich zu der Standard-LDAP-Suche und ermöglicht die Suche in jeder Domäne ohne Angabe des Domänennamens.
- User search by: Klicken Sie in der Liste auf userPrincipalName oder sAMAccountName.
- Use secure connection: Klicken Sie auf YES, um sichere Verbindungen zu aktivieren.

4. Klicken Sie auf Save.

Benutzerkonten, Rollen und Registrierungseinstellungen

Oct 29, 2015

In XenMobile konfigurieren Sie Benutzer und Gruppen, Rollen für Benutzer und Gruppen sowie den Registrierungsmodus und Einladungen auf der Seite Settings der XenMobile-Konsole.



Auf der Seite Settings können Sie folgende Einstellungen ändern:

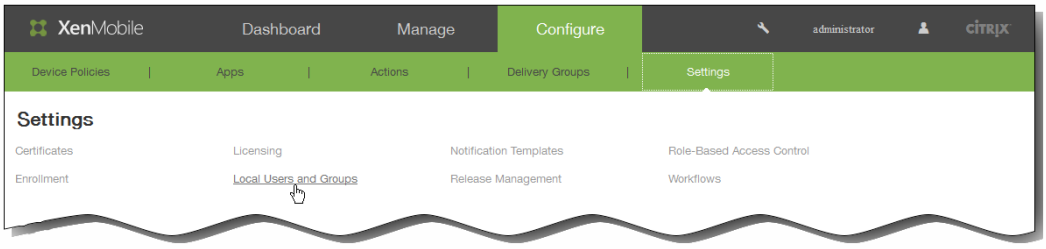
- Klicken Sie auf Local Users and Groups, um Benutzerkonten manuell oder unter Verwendung einer CSV-Provisioningdatei für den Import hinzuzufügen und lokale Gruppen zu verwalten. Weitere Informationen:
  - So erstellen, bearbeiten oder löschen Sie lokale Benutzer in XenMobile
  - So importieren Sie Benutzerkonten über eine CSV-Provisioningdatei und Provisioningdateiformate.
  - So erstellen oder entfernen Sie Gruppen in XenMobile
- Klicken Sie auf Enrollment zum Konfigurieren von bis zu sieben Registrierungsmodi mit jeweils eigener Sicherheitsstufe und Anzahl der Schritte, die Benutzer zur Geräteregistrierung durchführen müssen, und zum Senden von Registrierungseinladungen. Weitere Informationen:
  - So konfigurieren Sie Registrierungsmodi und aktivieren das Selbsthilfeportal
  - So aktivieren Sie in XenMobile Autodiscovery für die Benutzerregistrierung
- Klicken Sie auf Role-Based Access Control, um Benutzern und Gruppen vordefinierte Rollen bzw. Berechtigungssätze zuzuweisen. Diese Berechtigungen steuern den Zugriff der Benutzer auf Systemfunktionen. Weitere Informationen:
  - Erstellen und Aktualisieren benutzerdefinierter Rollen in XenMobile mit der rollenbasierten Zugriffssteuerung
- Klicken Sie auf Notification Templates, um Benachrichtigungsvorlagen zur Verwendung in automatisierten Aktionen, bei der Registrierung und für Standardbenachrichtigungen an Benutzer einzurichten. Sie können Benachrichtigungsvorlagen zum Senden von Nachrichten über drei verschiedene Kanäle konfigurieren: Worx Home, SMTP oder SMS. Weitere Informationen:
  - So erstellen oder aktualisieren Sie Benachrichtigungsvorlagen in XenMobile

Erstellen, Bearbeiten oder Löschen lokaler Benutzer in XenMobile

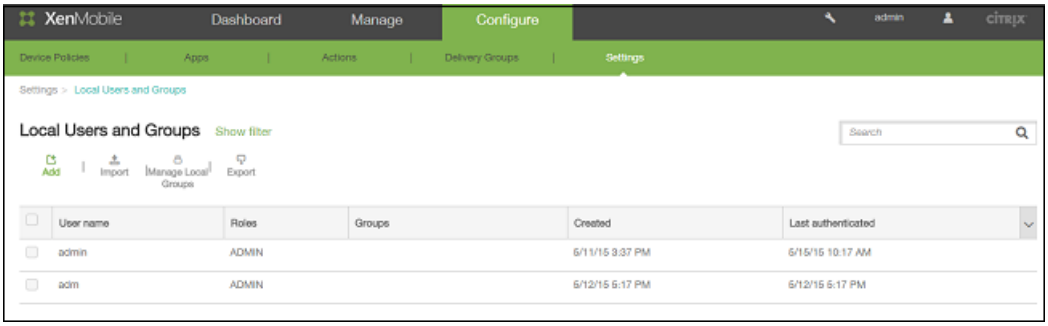
Nov 12, 2015

Sie können lokale Benutzerkonten in XenMobile manuell hinzufügen oder mit einer Provisioningdatei importieren. Schritte für das Importieren von Benutzern aus einer Provisioningdatei finden Sie unter So importieren Sie Benutzerkonten über eine CSV-Provisioningdatei.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Local Users and Groups.



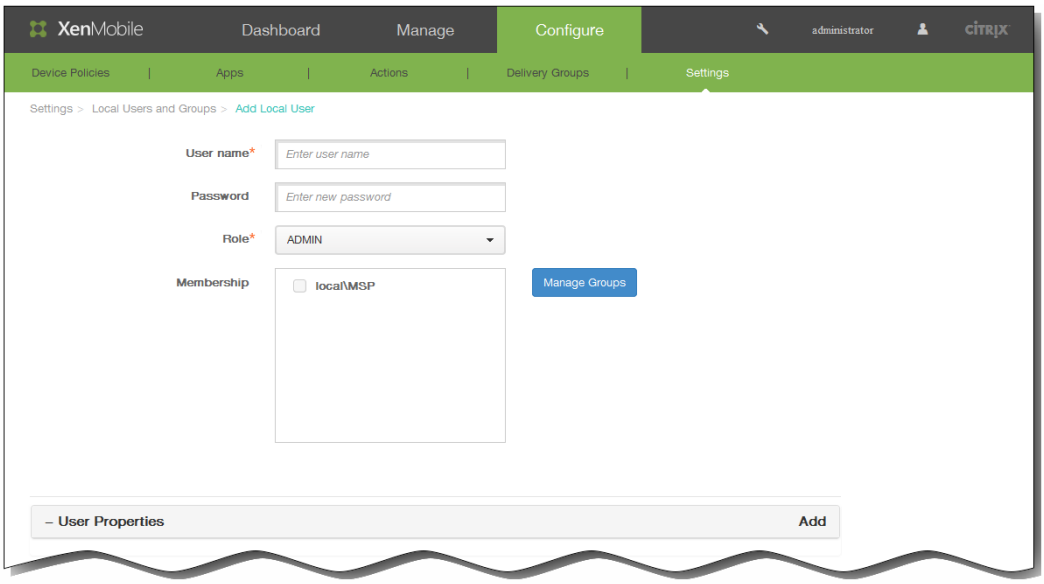
Die Seite Local Users and Groups wird angezeigt.



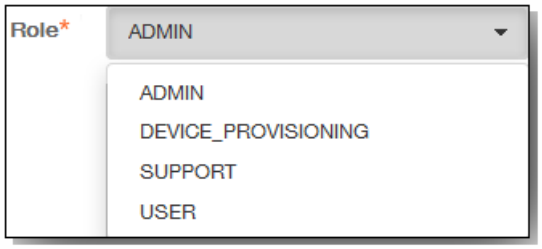
So fügen Sie einen lokalen Benutzer hinzu

Mit diesem Verfahren werden XenMobile Benutzer einzeln hinzugefügt. Zum Hinzufügen mehrerer Benutzer siehe So importieren Sie Benutzerkonten über eine CSV-Provisioningdatei.

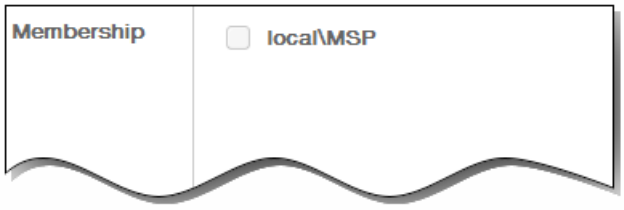
1. Klicken Sie auf der Seite Local Users and Groups auf Add. Die Seite Add Local User wird angezeigt.



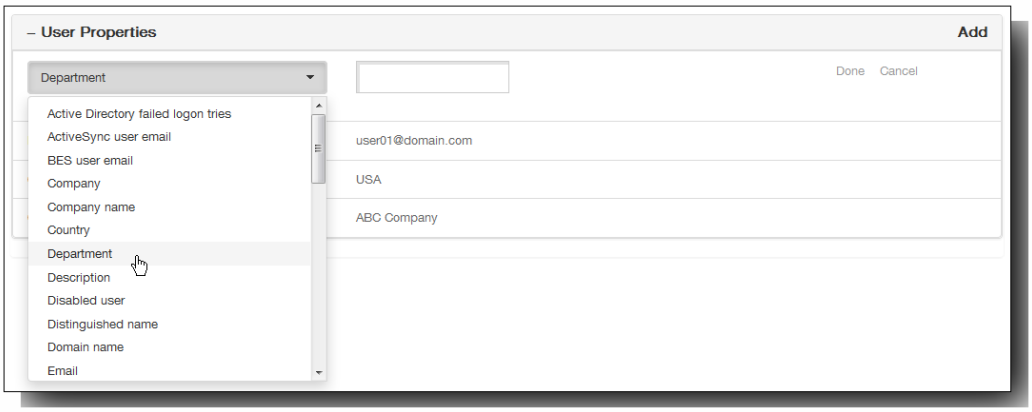
2. Geben Sie zum Hinzufügen des lokalen Benutzers die folgenden Informationen ein:
   1. User name: Geben Sie den Benutzernamen ein. Dies ist ein Pflichtfeld.
   2. Password: Geben Sie ein optionales Benutzerkennwort ein.
   3. Role: Klicken Sie in der Liste Role auf die Rolle des Benutzers. Weitere Informationen über Rollen finden Sie unter Erstellen und Aktualisieren benutzerdefinierter Rollen in XenMobile mit der rollenbasierten Zugriffssteuerung (RBAC).



   4. Membership: Klicken Sie in der Liste Membership auf die Gruppen, zu denen der Benutzer gehören soll.

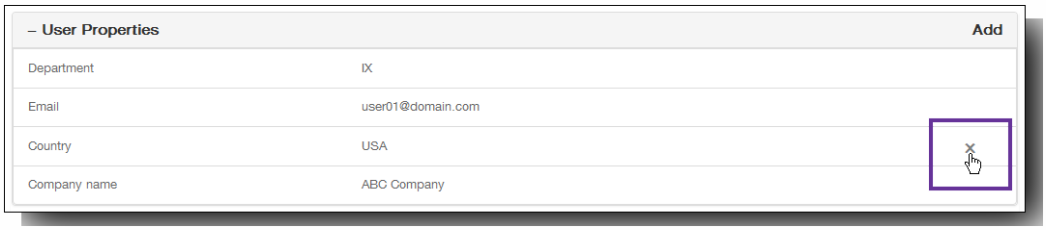


3. Wenn Sie (optional) Eigenschaften hinzufügen möchten, führen Sie die folgenden Schritte aus:
   1. Klicken Sie neben User Properties auf Add.
   2. Klicken Sie in der Liste User Properties auf eine Eigenschaft.
   3. Geben Sie das zugehörige Attribut in das Feld neben der Liste ein.



4. Klicken Sie auf Done, um die Eigenschaft zu speichern, oder auf Cancel, um den Vorgang abzubrechen.
5. Wiederholen Sie die Schritte b und c für jede Eigenschaft, die Sie hinzufügen möchten.

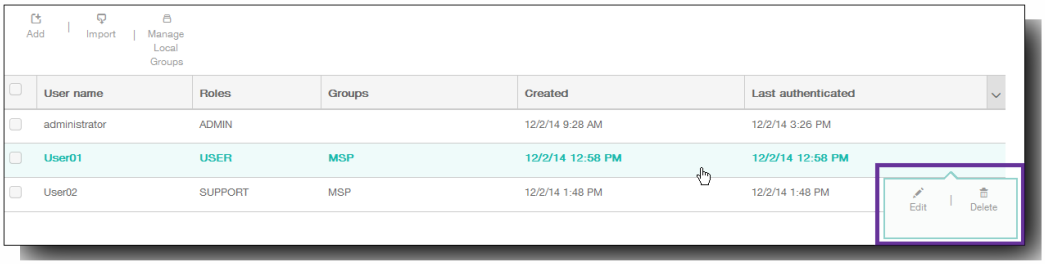
4. Optional können Sie Benutzereigenschaften bearbeiten. Führen Sie hierfür folgende Schritte aus:
   1. Klicken Sie auf die Eigenschaft, die Sie bearbeiten möchten.
   2. Ändern Sie das zugehörige Attribut.
   3. Klicken Sie auf Done, um die Bearbeitung zu speichern, oder auf Cancel, um den Vorgang abzubrechen.
5. Optional können Sie Benutzereigenschaften löschen. Führen Sie hierfür folgende Schritte aus:
   1. Zeigen Sie auf die Zeile mit der Benutzereigenschaft, die Sie löschen möchten.
   2. Klicken Sie auf das X, das rechts neben der Zeile angezeigt wird.



   Die Eigenschaft wird sofort gelöscht.
6. Klicken Sie auf Save, um den neuen Benutzer zu speichern.

So bearbeiten Sie einen lokalen Benutzer

1. Wählen Sie auf der Seite Local Users and Groups den Benutzer in der Liste der Benutzer aus.



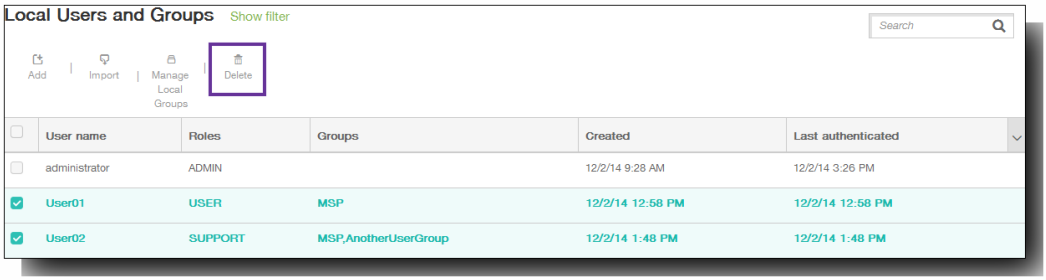
   Die Seite Edit Local User wird angezeigt.
2. Ändern Sie nach Bedarf die folgenden Informationen:
   1. User name: Geben Sie den Benutzernamen ein. Dies ist ein Pflichtfeld.
   2. Password: Geben Sie ein optionales Benutzerkennwort ein.

3. Role: Klicken Sie in der Liste Role auf die Rolle des Benutzers.
4. Membership: Klicken Sie in der Liste Membership auf die Gruppen, zu denen der Benutzer gehören soll.
5. User properties: Fügen Sie neue Benutzereigenschaften hinzu oder bearbeiten Sie vorhandene.

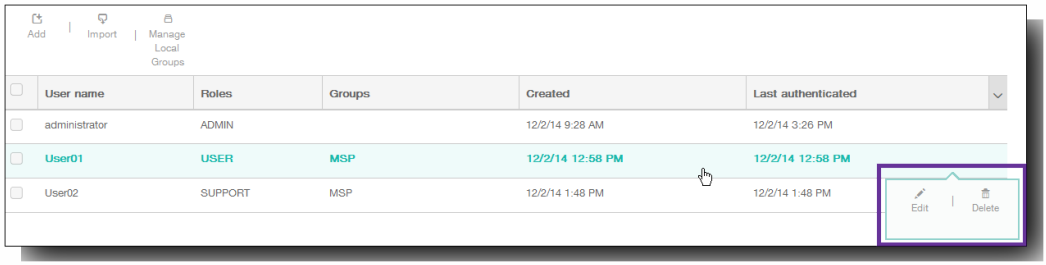
3. Klicken Sie auf Save, um die Änderungen zu speichern.

So löschen Sie einen lokalen Benutzer

1. Führen Sie auf der Seite Local Users and Groups in der Liste der Benutzer einen der folgenden Schritte aus:
   - Aktivieren Sie die Kontrollkästchen neben dem Benutzer (ggf. neben mehreren Benutzern), den Sie löschen möchten, und klicken Sie dann auf Delete.



   - Klicken Sie auf die Zeile des Benutzers und in dem nun rechts angezeigten Menü auf Delete.



Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf Delete, um den Vorgang zu bestätigen und den oder die Benutzer zu löschen.
Wichtig: Sie können diesen Vorgang nicht rückgängig machen.

Importieren von Benutzerkonten

Nov 12, 2015

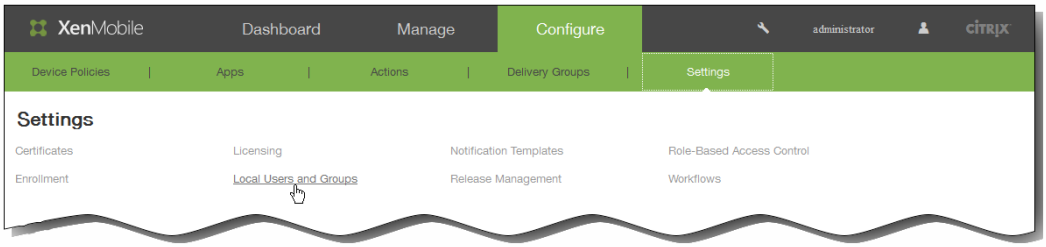
Sie können Benutzerkonten und Eigenschaften aus einer CSV-Datei, einer so genannten Provisioningdatei importieren, die Sie manuell erstellen können. Informationen zur Formatierung von Provisioningdateien finden Sie unter Provisioningdateiformate.

Hinweis:

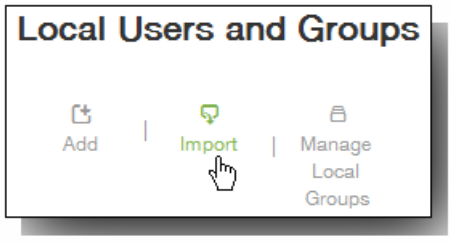
- Wenn Sie Benutzer aus einem LDAP-Verzeichnis importieren, verwenden Sie den Domänennamen zusammen mit dem Benutzernamen in der Importdatei. Beispiel: username@domain.com. Diese Syntax vermeidet zusätzliche Nachschlagevorgänge, die den Import verlangsamen.
- Beim Import von Benutzerkonten in das interne Benutzerverzeichnis von XenMobile deaktivieren Sie die Standarddomäne, um den Importvorgang zu beschleunigen. Sie können die Standarddomäne nach dem Import wieder aktivieren.
- Lokale Benutzer können im UPN-Format (Benutzerprinzipalname) angegeben werden. Allerdings empfiehlt Citrix, nicht die verwaltete Domäne zu verwenden. Ist beispielsweise example.com verwaltet, erstellen Sie keinen lokalen Benutzer mit diesem UPN-Format: Benutzer@example.com.

Nach dem Erstellen einer Provisioningdatei führen Sie folgende Schritte für den Import der Datei in XenMobile durch.

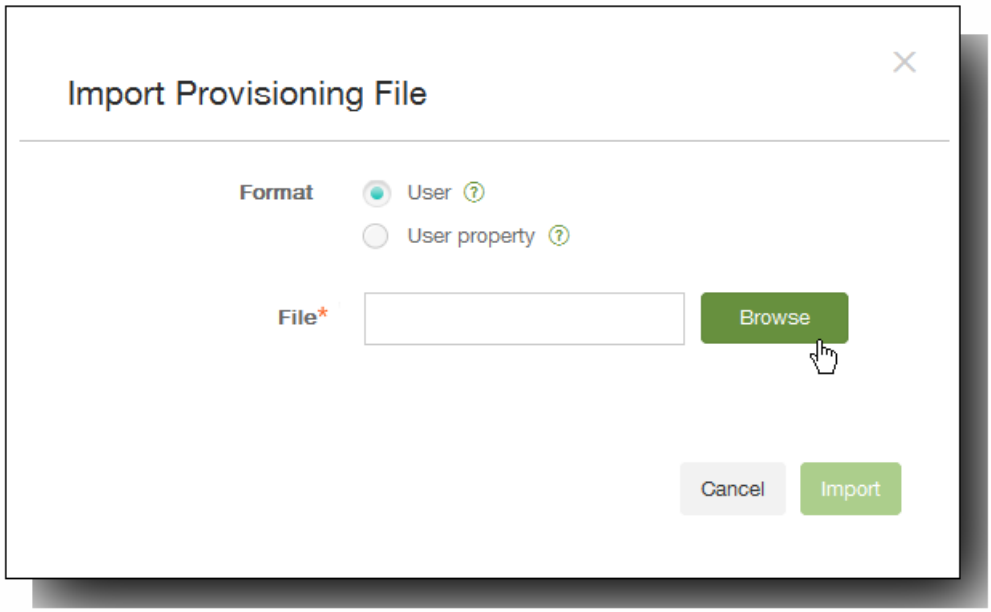
1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Local Users and Groups.



2. Klicken Sie auf der Seite Local Users and Groups auf Import.



   Das Dialogfeld Import Provisioning File wird angezeigt.
3. Wählen Sie im Dialogfeld Import Provisioning File das Format der Provisioningdatei, die Sie importieren.



4. Klicken Sie neben File auf Browse, navigieren Sie zu dem Speicherort der Provisioningdatei und klicken Sie auf Import.

Provisioningdateiformate

Nov 12, 2015

Eine manuell erstellte Provisioningdatei zum Importieren von Benutzerkonten und -eigenschaften in XenMobile muss folgendes Format haben:

- Felder der Provisioningdatei: user;password;role;group1;group2
- Felder für Benutzerattribute in der Provisioningdatei: user;propertyName1;propertyValue1;propertyName2;propertyValue2

Hinweis:

- Die Felder in der Provisioningdatei werden durch Semikola (;) getrennt. Wenn ein Feld ein Semikolon enthält, muss dieses mit einem umgekehrten Schrägstrich (\) geschützt werden. Beispiel: Eigenschaft propertyV;test;1;2 würde eingegeben als propertyV\;test\;1\;2 in der Provisioningdatei.
- Gültige Werte für "Role" sind die vordefinierten Rollen USER, ADMIN, SUPPORT und DEVICE_PROVISIONING sowie alle zusätzlich von Ihnen definierten Rollen.
- Der Punkt (.) wird als Trennzeichen zum Erstellen von Gruppenhierarchien verwendet und kann daher nicht in Gruppennamen verwendet werden.
- Eigenschaftsattribute in Attributprovisioningdateien müssen in Kleinbuchstaben geschrieben werden. Bei der Datenbank wird zwischen Groß- und Kleinschreibung unterschieden.

Beispiel für Benutzerprovisioninginhalt

Der Eintrag: user01;pwd\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01Bedeutet:

- Benutzer: user01
- Kennwort: pwd;01
- Rolle: USER
- Gruppen:
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

Beispiel für Benutzerattribut-Provisioninginhalt

Der Eintrag: user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 valueBedeutet:

- Benutzer: user01
- Eigenschaft 1:
  - Name: propertyN
  - Wert: propertyV;test;1;2
- Eigenschaft 2:
  - Name: prop 2
  - Wert: prop 2 value

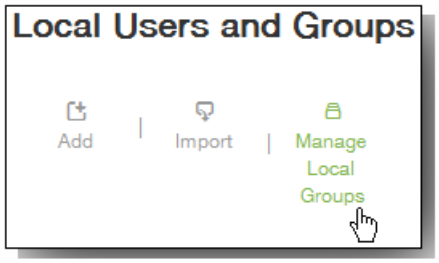
Hinzufügen oder Entfernen von Gruppen

Nov 12, 2015

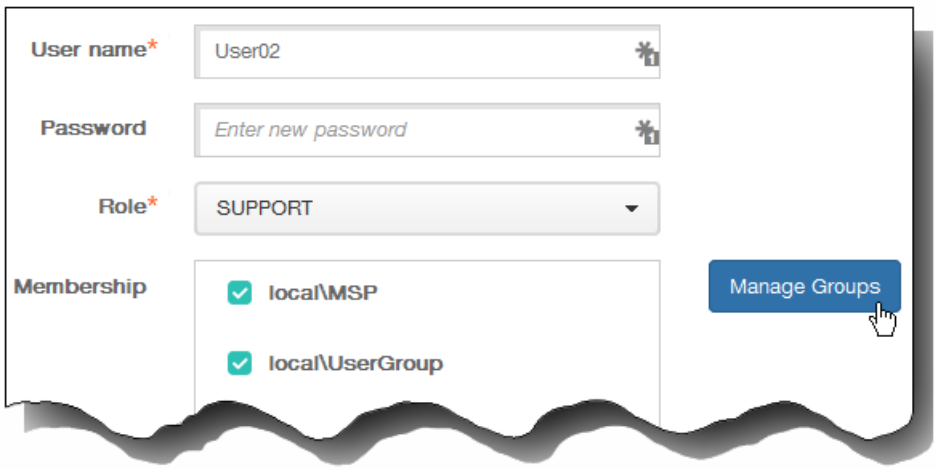
Gruppen werden im Dialogfeld Manage Groups in der XenMobile-Konsole verwaltet. Dieses kann über die Seite Local Users and Groups, Add Local User oder Edit Local User aufgerufen werden. Es gibt keinen "Edit"-Befehl zum Bearbeiten von Gruppen. Das Entfernen einer Gruppe hat keine Auswirkungen auf die Benutzerkonten. Beim Entfernen einer Gruppe wird lediglich die Zuordnung von Benutzern zu der Gruppe aufgehoben. Die Benutzer verlieren zudem den Zugriff auf Apps und Profile, die über Bereitstellungsgruppen bereitgestellt werden, die der gelöschten Gruppe zugeordnet sind. Sämtliche anderen Gruppenzuordnungen bleiben jedoch intakt. Wenn Benutzer keiner anderen lokalen Gruppen zugeordnet sind, werden sie auf oberster Ebene zugeordnet.

So fügen Sie eine lokale Gruppe hinzu

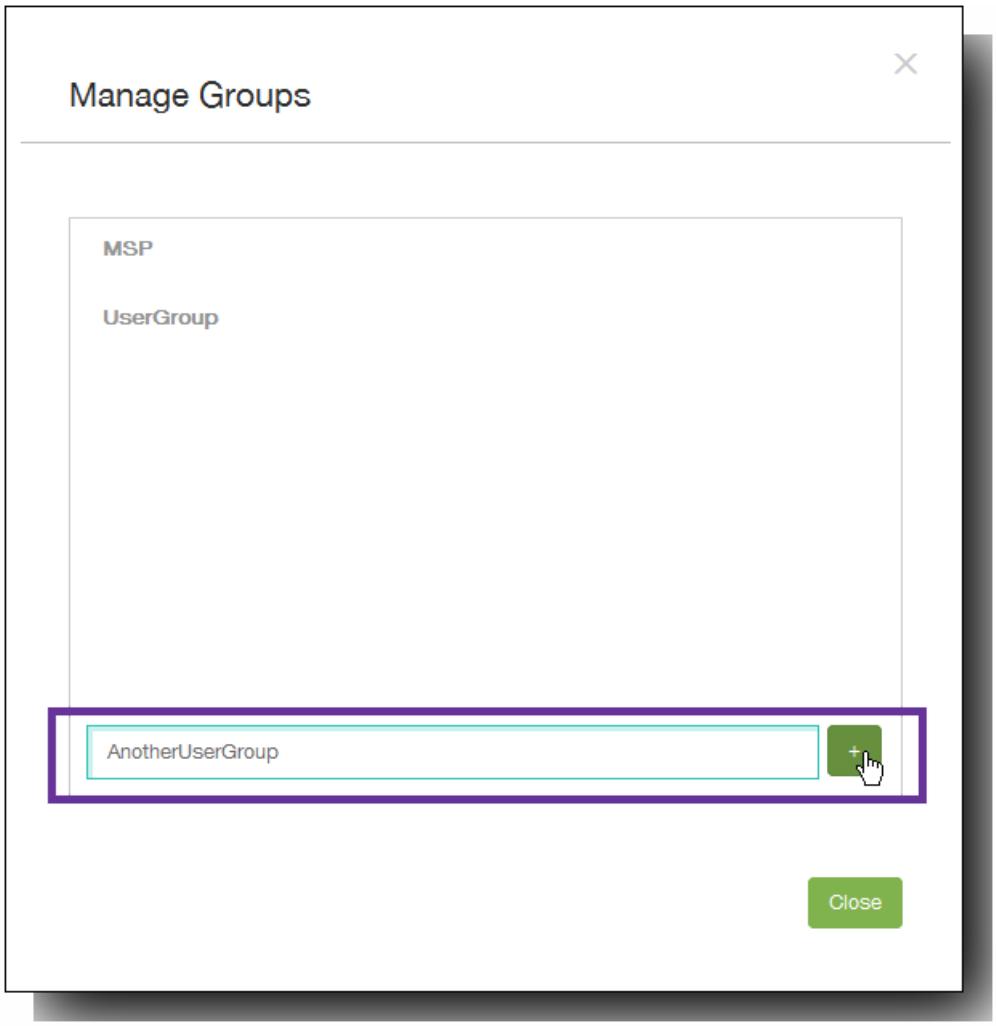
1. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf der Seite Local Users and Groups auf Manage Local Groups.



   - Klicken Sie auf der Seite Add Local User oder Edit Local User auf Manage Groups.



   Das Dialogfeld Manage Groups wird angezeigt.
2. Geben Sie unterhalb der Gruppenliste einen Namen für die neue Gruppe ein und klicken Sie auf das Pluszeichen (+).



Die Benutzergruppe wird der Liste hinzugefügt.

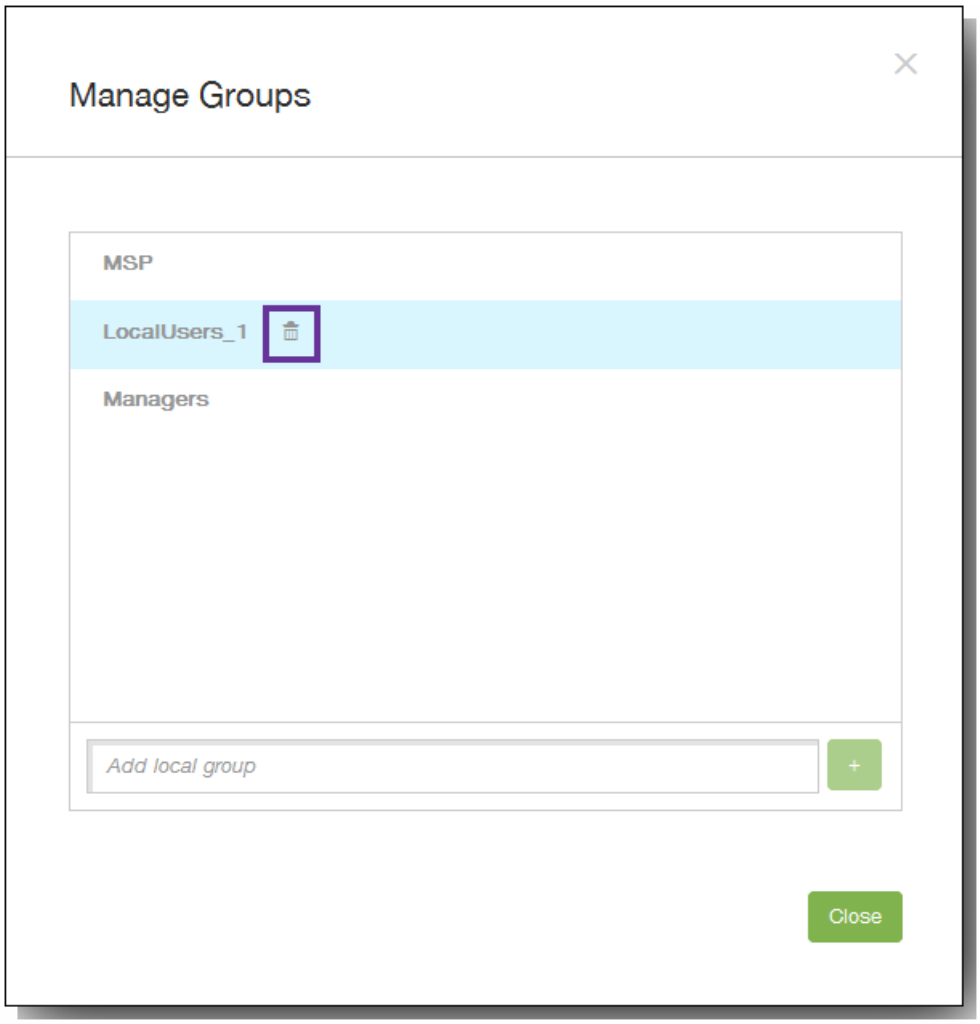
3. Klicken Sie auf Close.

So entfernen Sie eine Gruppe

Hinweis: Das Entfernen einer Gruppe hat keine Auswirkungen auf die Benutzerkonten. Beim Entfernen einer Gruppe wird lediglich die Zuordnung von Benutzern zu der Gruppe aufgehoben. Die Benutzer verlieren zudem den Zugriff auf Apps und Profile, die über Bereitstellungsgruppen bereitgestellt werden, die der gelöschten Gruppe zugeordnet sind. Sämtliche anderen Gruppenzuordnungen bleiben jedoch intakt. Wenn Benutzer keiner anderen lokalen Gruppen zugeordnet sind, werden sie auf oberster Ebene zugeordnet.

1. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf der Seite Local Users and Groups auf Manage Local Groups.
   - Klicken Sie auf der Seite Add Local User oder Edit Local User auf Manage Groups.

   Das Dialogfeld Manage Groups wird angezeigt.
2. Klicken Sie im Dialogfeld Manage Groups auf die Gruppe, die Sie löschen möchten.



3. Klicken Sie auf das Papierkorbsymbol rechts neben dem Gruppennamen. Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf Delete, um den Vorgang zu bestätigen und die Gruppe zu entfernen.
   Wichtig: Sie können diesen Vorgang nicht rückgängig machen.
5. Klicken Sie im Dialogfeld Manage Groups auf Close.

Konfigurieren der Registrierungsmodi und Aktivieren des Selbsthilfeportals

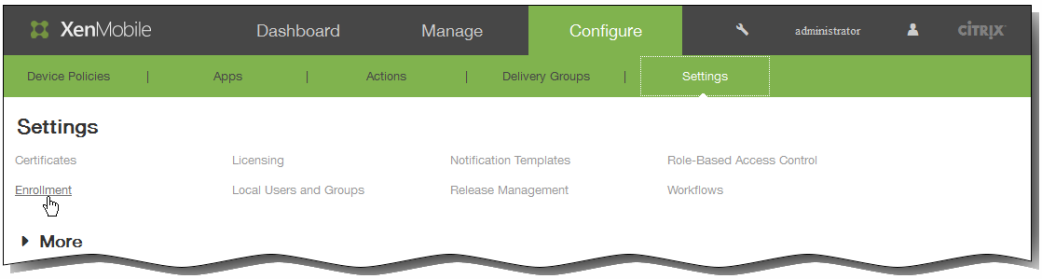
Nov 12, 2015

Sie konfigurieren Geräteregistrierungsmodi, damit Benutzer ihre Geräte in XenMobile registrieren können. XenMobile bietet sieben Modi mit verschiedenen Sicherheitsstufen und Schritten, die die Benutzer zum Registrieren von Geräten ausführen müssen. Sie können einige Modi auf dem Selbsthilfeportal zur Verfügung stellen, mit denen Benutzer nach Anmeldung Registrierungslinks generieren oder eine Registrierungseinladung an das eigene E-Mail-Konto senden können.

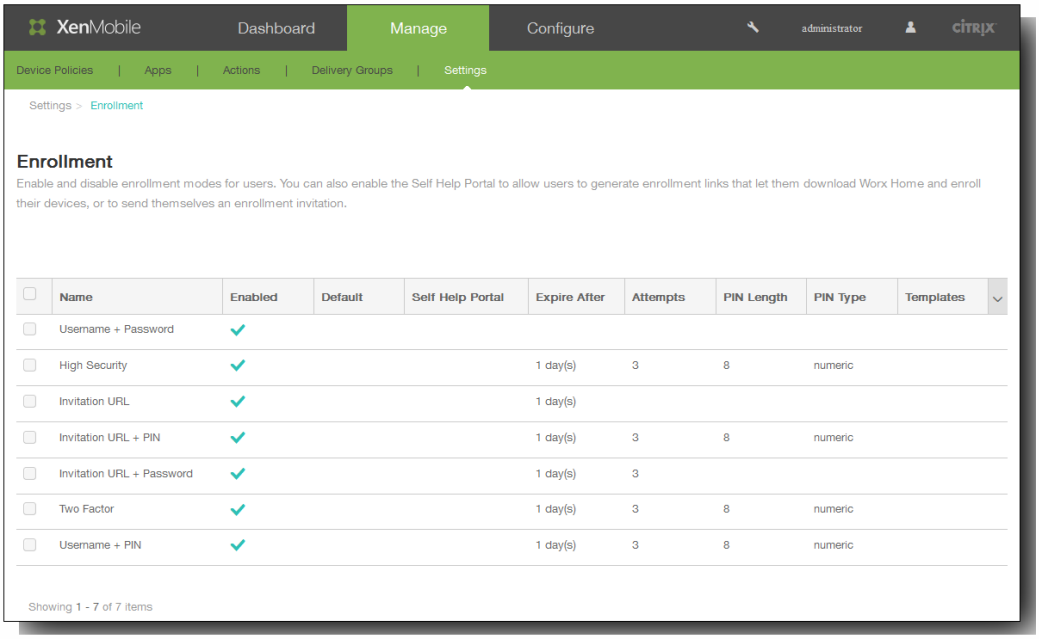
Zum Konfigurieren von Registrierungsmodi verwenden Sie in der XenMobile-Konsole die Seite Settings > Enrollment. Zum Senden von Registrierungseinladungen verwenden Sie in der XenMobile-Konsole die Seite Manage > Enrollment (siehe Registrieren von Benutzern und Geräten in XenMobile).

Hinweis: Wenn Sie benutzerdefinierte Benachrichtigungsvorlagen verwenden möchten, müssen Sie diese vor dem Konfigurieren der Registrierungsmodi erstellen. Weitere Informationen über Benachrichtigungen finden Sie unter So erstellen oder aktualisieren Sie Benachrichtigungsvorlagen in XenMobile.

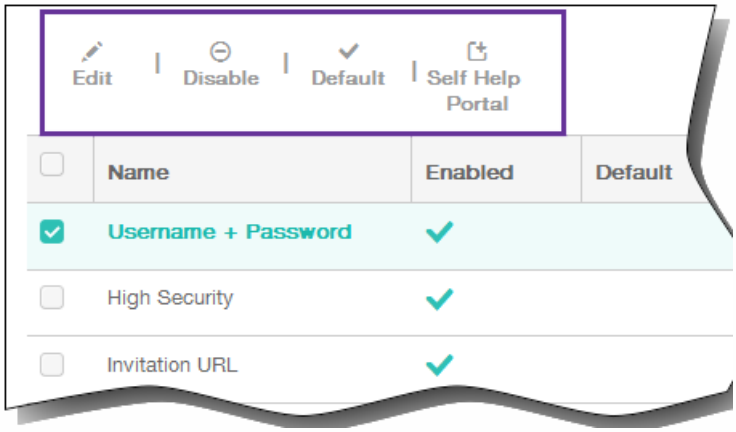
1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Enrollment.

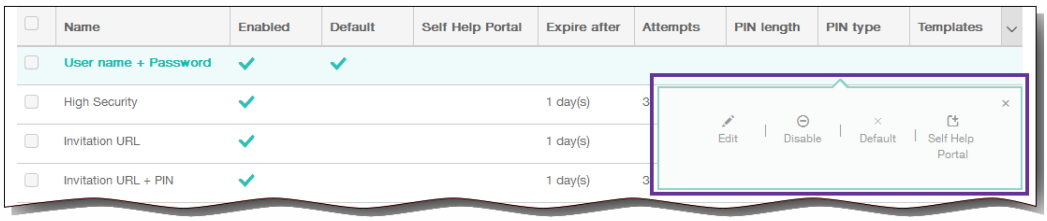


Die Seite Enrollment wird angezeigt. Sie enthält eine Tabelle aller verfügbaren Registrierungsmodi.



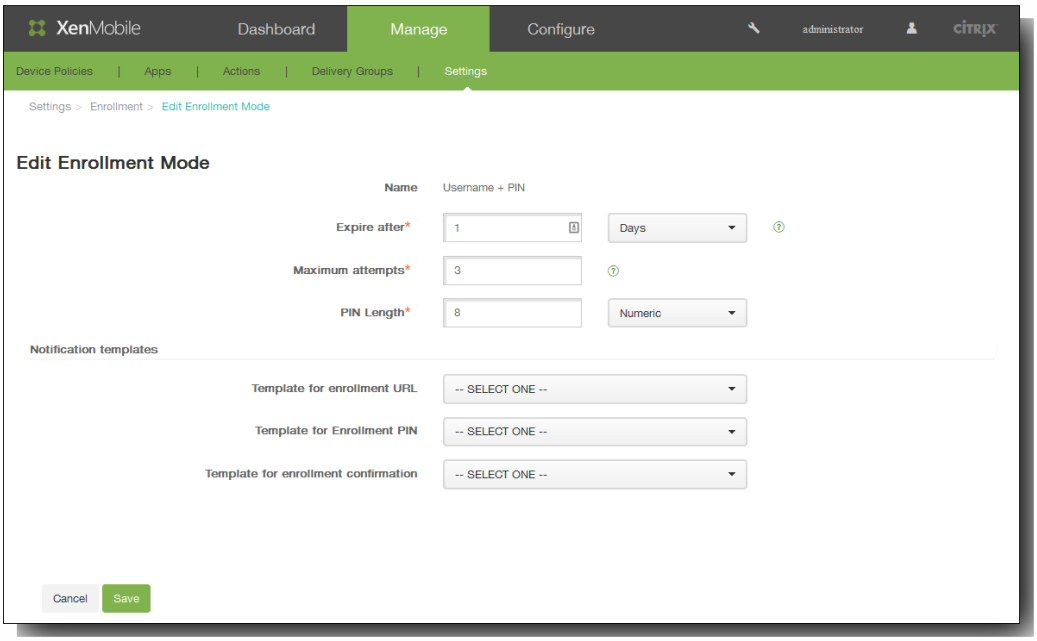
2. Wählen Sie einen Registrierungsmodus in der Liste zur Bearbeitung aus und legen Sie diesen als Standard fest, löschen Sie ihn oder erteilen Sie Benutzern Zugriff darauf über das Selbsthilfeportal.
   Hinweis: Wenn Sie das Kontrollkästchen neben einem Registrierungsmodus auswählen, wird das Menü mit den Optionen oberhalb der Liste der Registrierungsmodi eingeblendet. Wenn Sie auf eine andere Stelle im Eintrag klicken, wird es rechts neben dem Eintrag eingeblendet.



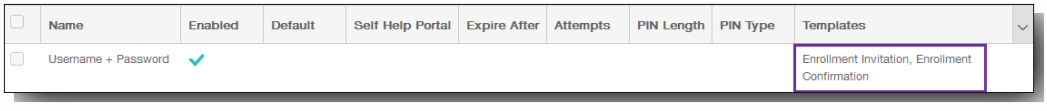


So bearbeiten Sie einen Registrierungsmodus

1. Wählen Sie in der Liste Enrollment einen Registrierungsmodus aus und klicken Sie dann auf Edit. Abhängig vom ausgewählten Modus werden ggf. andere Optionen angezeigt, als die in der folgenden Abbildung dargestellten.



2. Ändern Sie nach Bedarf die folgenden Informationen:
    1. Expire after: Geben Sie einen Zeitraum ein, nach dem die Benutzer ihre Geräte nicht mehr registrieren können.
    Hinweis: Geben Sie 0 ein, wenn die Einladung nicht ablaufen soll.
    2. Days: Wählen Sie Days oder Hours zur Bestimmung der Maßeinheit für den unter Expire after eingegebenen Zeitraum aus.
    3. Maximum attempts: Geben Sie die Anzahl der Registrierungsversuche ein, die ein Benutzer machen darf, bevor die Registrierung für ihn gesperrt wird.
    Hinweis: Geben Sie 0 ein, um eine unbegrenzte Anzahl von Versuchen zuzulassen.
    4. PIN length: Geben Sie eine Zahl für die Länge der generierten PIN in Ziffern/Zeichen ein.
    5. Numeric: Wählen Sie als PIN-Typ Numeric oder Alphanumeric aus.
3. Ändern Sie nach Bedarf unter Notification templates folgende Einstellungen:
    1. Template for enrollment URL: Wählen Sie eine Vorlage für die Registrierungs-URL aus. Über die Registrierungseinladungsvorlage wird beispielsweise den Benutzern eine E-Mail oder SMS gesendet, je nachdem, wie Sie die Vorlage für die Geräteregistrierung in XenMobile konfiguriert haben. Weitere Informationen über Benachrichtigungen finden Sie unter So erstellen oder aktualisieren Sie Benachrichtigungsvorlagen in XenMobile.
    2. Template for enrollment confirmation: Wählen Sie eine Vorlage für die Benachrichtigung der Benutzer über eine erfolgreiche Registrierung aus.
4. Klicken Sie auf Save, um die Änderungen zu übergeben.



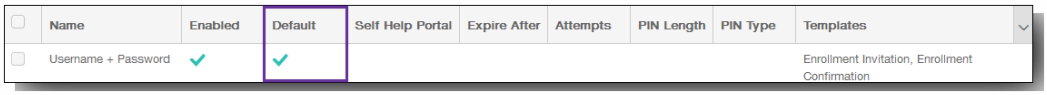
So legen Sie einen Registrierungsmodus als Standard fest

Wenn Sie einen Registrierungsmodus als Standard festlegen, wird er für alle Geräteregistrierungsanfragen verwendet, wenn kein anderer Registrierungsmodus ausgewählt wird. Wenn kein Registrierungsmodus als Standard festgelegt wird, muss für

jede Geräteregistrierung eine eigene Registrierungsanforderung erstellt werden.

Hinweis: Nur Username + Passwords, Two Factor oder Username + PIN können als Standardregistrierungsmodus festgelegt werden.

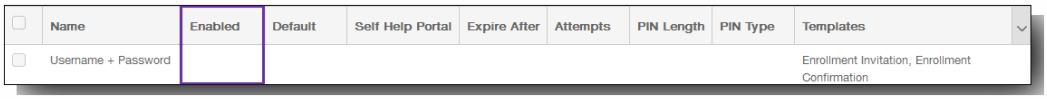
1. Wählen Sie Username + Passwords, Two Factor oder Username + PIN zum Festlegen als Standardregistrierungsmodus aus.
   Hinweis: Der ausgewählte Modus muss aktiviert sein, um als Standard festgelegt werden zu können.
2. Klicken Sie auf Default. Der ausgewählte Modus ist jetzt der Standardmodus. War zuvor ein anderer Registrierungsmodus als Standard eingestellt, ist dieser Modus nun nicht mehr Standardmodus.



So deaktivieren Sie einen Registrierungsmodus

Wenn Sie einen Registrierungsmodus deaktivieren, ist er sowohl für Gruppenregistrierungseinladungen als auch auf dem Selbsthilfeportal nicht mehr verfügbar. Sie können die Art und Weise der Geräteregistrierung durch die Benutzer ändern, indem Sie einen Registrierungsmodus deaktivieren und einen anderen aktivieren.

1. Wählen Sie einen Registrierungsmodus aus.
   Hinweis: Den Standardregistrierungsmodus können Sie nicht deaktivieren. Wenn Sie den Standardregistrierungsmodus deaktivieren möchten, müssen Sie zunächst dessen Einstellung als Standard aufheben.
2. Klicken Sie auf Disable. Der Registrierungsmodus ist nicht mehr aktiviert.



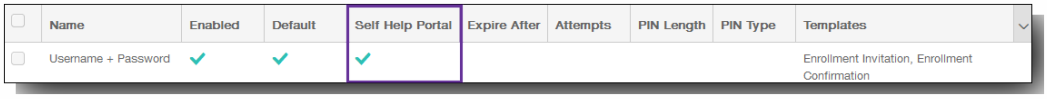
So aktivieren Sie einen Registrierungsmodus auf dem Selbsthilfeportal

Durch Aktivieren eines Registrierungsmodus auf dem Selbsthilfeportal können Benutzer ihre Geräte in XenMobile selbst registrieren.

Hinweis:

- Der Registrierungsmodus muss aktiviert und an Benachrichtigungsvorlagen gebunden sein, damit er auf dem Selbsthilfeportal zur Verfügung gestellt werden kann.
- Sie können auf dem Selbsthilfeportal nur jeweils einen Registrierungsmodus aktivieren.

1. Wählen Sie einen Registrierungsmodus aus.
2. Klicken Sie auf Self Help Portal. Der ausgewählte Registrierungsmodus steht Benutzern jetzt auf dem Selbsthilfeportal zur Verfügung. Andere für das Selbsthilfeportal aktivierte Modi sind nicht mehr verfügbar.



Konfigurieren von Rollen mit RBAC

Nov 12, 2015

Mit der rollenbasierten Zugriffssteuerung (RBAC) in XenMobile können Sie Benutzern und Gruppen vordefinierte Rollen bzw. Berechtigungssätze zuweisen. Diese Berechtigungen steuern den Zugriff der Benutzer auf Systemfunktionen.
In XenMobile sind vier Standardbenutzerrollen für die logische Trennung des Zugriffs auf Systemfunktionen implementiert:

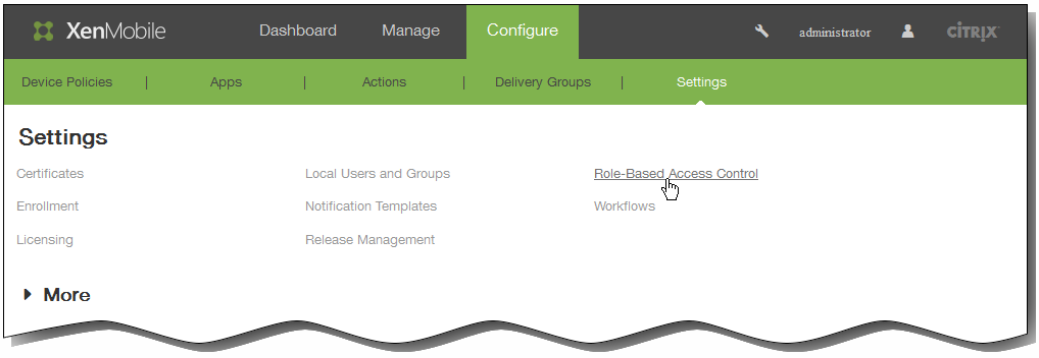
- **Administrator**: besitzt Vollzugriff auf das System.
- **Support**: besitzt Zugriff auf den Remotesupport.
- **User**: von Benutzern verwendete Rolle für die Registrierung von Geräten und den Zugriff auf das Selbsthilfeportal.

Zusätzlich zu den Standardrollen können Sie auch neue Benutzerrollen mit Berechtigungen für spezifische Systemfunktionen erstellen. Hierfür verwenden Sie die Standardrollen als Vorlagen, die Sie dann anpassen.

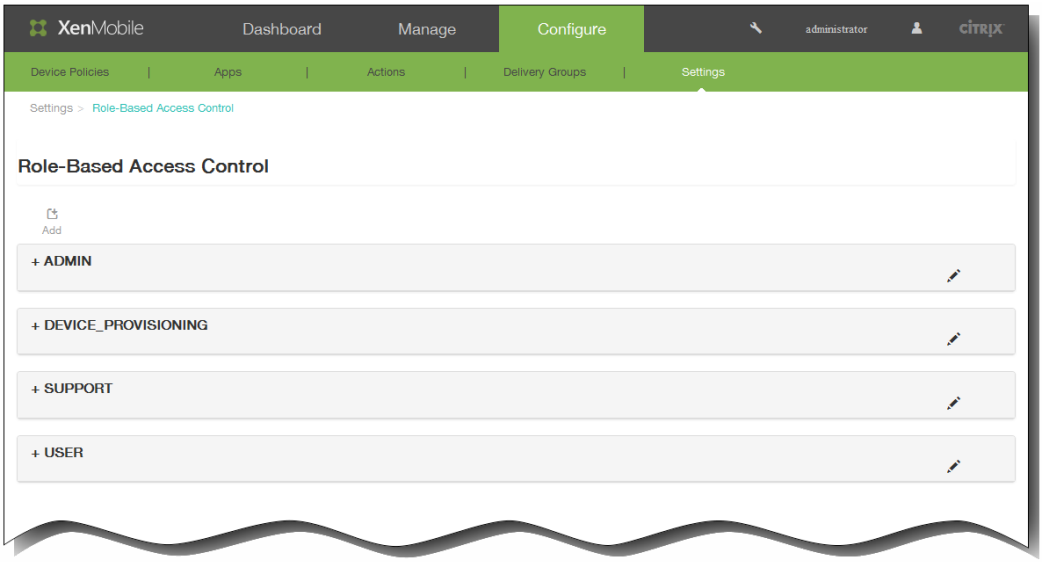
Rollen können lokalen Benutzern (auf Benutzerebene) oder Active Directory-Gruppen (alle Benutzer in der Gruppe haben dieselben Berechtigungen) zugewiesen werden. Gehört ein Benutzer mehreren Active Directory-Gruppen an, werden alle entsprechenden Berechtigungen zu einem für diesen Benutzer spezifischen Satz zusammengeführt. Beispiel: Wenn Benutzer der Active Directory-Gruppe A Geräte von Managern suchen und Benutzer der Active Directory-Gruppe B eine Datenlöschung auf Mitarbeitergeräten durchführen können, dann können Benutzer, die beiden Gruppen angehören, Geräte von Managern *und* Mitarbeitern suchen und eine Datenlöschung darauf durchführen.
Hinweis: Lokalen Benutzern kann bei Bedarf nur eine Rolle zugewiesen werden.
Mit dem RBAC-Feature in XenMobile ist Folgendes möglich:

- Erstellen einer Regel
- Hinzufügen von Gruppen zu einer Rolle
- Zuweisen von Rollen an lokale Benutzer

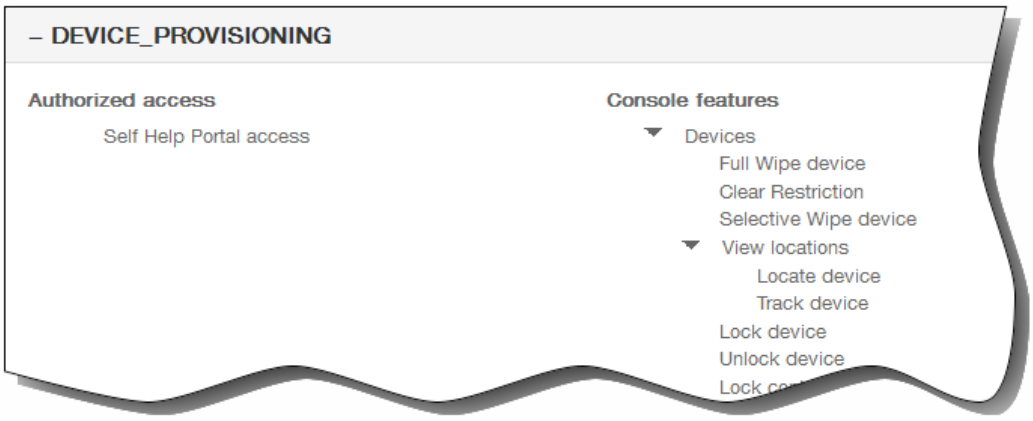
1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Role-Based Access Control.



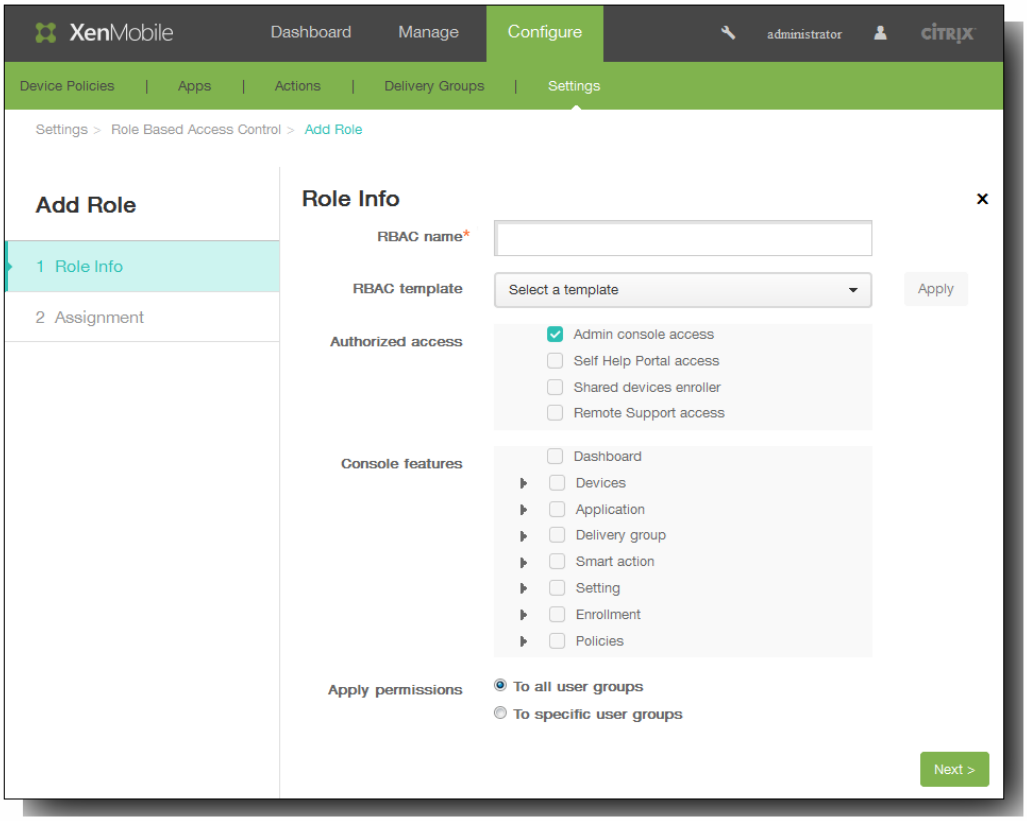
Die Seite Role mit den vier Standardbenutzerrollen und allen von Ihnen zuvor hinzugefügten Rollen wird angezeigt.



Hinweis: Wenn Sie auf das Pluszeichen (+) neben einer Rolle klicken, wird diese erweitert, sodass alle zugehörigen Berechtigungen zu sehen sind (siehe folgende Abbildung).

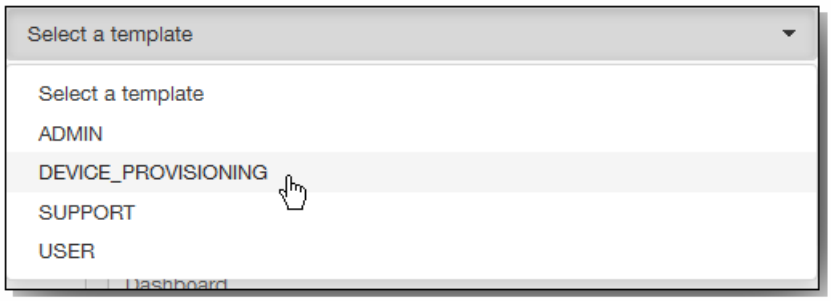


2. Klicken Sie auf Add, um eine neue Benutzerrolle hinzuzufügen, klicken Sie auf das Stiftsymbol rechts neben einer vorhandenen Rolle, um diese zu bearbeiten, oder klicken Sie auf das Papierkorbsymbol rechts neben einer von Ihnen hinzugefügten Rolle, um sie zu löschen. Sie können die Standardbenutzerrollen nicht löschen.
   - Wenn Sie auf Add oder das Stiftsymbol klicken, wird die Seite Add Role bzw. Edit Role angezeigt.

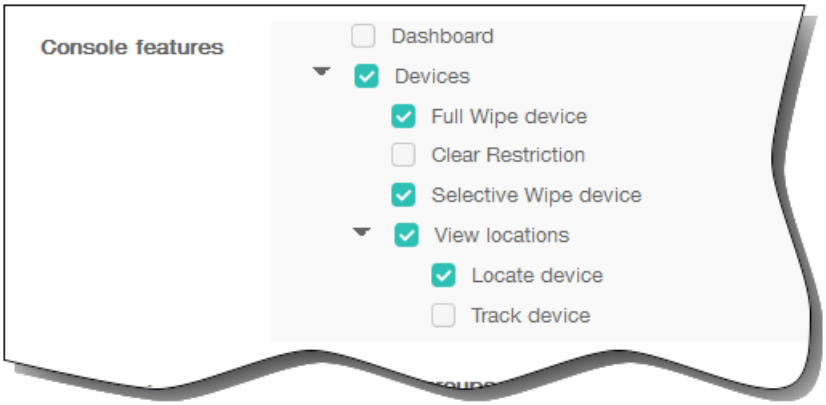


- Wenn Sie auf das Papierkorbsymbol klicken, wird ein Bestätigungsdialogfeld angezeigt. Klicken Sie auf Delete, um die ausgewählte Rolle zu entfernen.

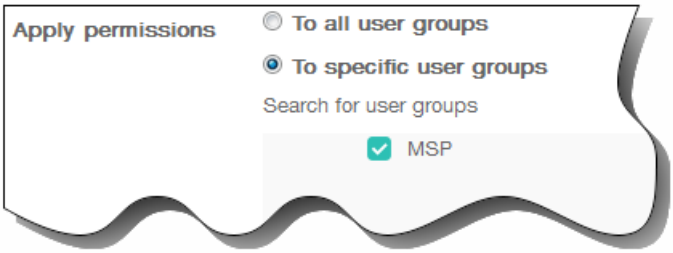
3. Geben Sie die folgenden Informationen zum Erstellen einer neuen Benutzerrolle bzw. zum Bearbeiten einer vorhandenen Benutzerrolle ein:
   1. RBAC name: Geben Sie einen aussagekräftigen Namen für die neue Benutzerrolle ein. Sie können den Namen vorhandener Rollen nicht ändern.
   2. RBAC template: Klicken Sie auf eine Vorlage als Ausgangspunkt für eine neue Rolle oder auf eine neue Vorlage für eine vorhandene Rolle.
      Hinweis: RBAC-Vorlagen sind die Standardbenutzerrollen sowie alle Rollen, die Sie selbst definiert haben. Sie definieren Sie den Zugriff auf Systemfunktionen für die Benutzer, denen die Rolle zugewiesen ist. Nach der Auswahl einer RBAC-Vorlage werden alle zu der Rolle gehörenden Berechtigungen in den Feldern Authorized Access und Console Features angezeigt. Die Verwendung von Vorlagen ist optional. Sie können die Berechtigungen auch direkt in den Feldern Authorized Access und Console Features auswählen.



- Klicken Sie auf Apply, um die Kontrollkästchen unter Authorized access und Console features gemäß den Berechtigungen der ausgewählten Vorlage einzustellen.
- Aktivieren bzw. deaktivieren Sie die Kontrollkästchen unter Authorized access und Console features, um die Rolle anzupassen.
  Hinweis: Wenn Sie auf das Dreieck neben einem Konsolenfeature klicken, werden featurespezifische Berechtigungen angezeigt, die Sie aktivieren und deaktivieren können. Wenn Sie auf das oberste Kontrollkästchen eines Konsolenbereichs klicken, erteilen Sie nur Lesezugriff für den Konsolenbereich. Zum Aktivieren von Schreib- und Aktualisierungszugriff für spezifische Optionen müssen Sie das Kontrollkästchen der jeweiligen Option aktivieren. In der folgenden Abbildung ist für die Option Clear Restrictions beispielsweise nur Lesezugriff aktiviert.

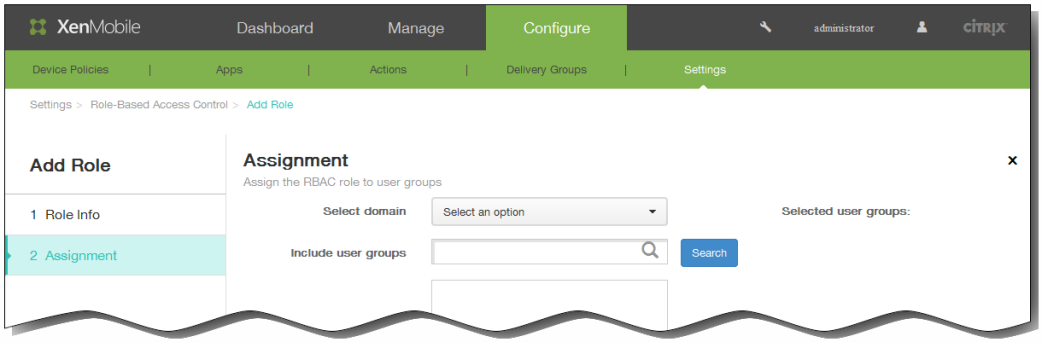


3. Apply permissions: Wählen Sie die Gruppen aus, denen Sie die ausgewählten Berechtigungen erteilen möchten.

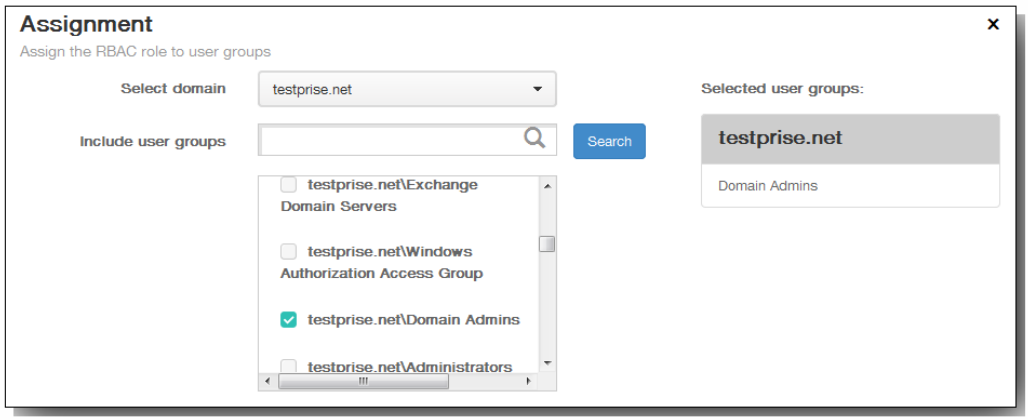


Wenn Sie auf To specific user groups klicken, wird eine Liste mit Gruppen angezeigt, in der Sie eine oder mehrere Gruppen auswählen können.

4. Klicken Sie auf Next. Die Seite Assignment wird angezeigt.



5. Geben Sie die folgenden Informationen zum Zuweisen der Rolle zu Gruppen ein und klicken Sie dann auf Save.
   1. Select domain: Klicken Sie in der Liste auf eine Domäne.
   2. Include user groups: Klicken Sie auf Search, um eine Liste aller verfügbaren Gruppen aufzurufen, oder geben Sie einen Gruppennamen vollständig oder teilweise ein, um die Liste auf Gruppen des entsprechenden Namens zu beschränken.
   3. Wählen Sie in der nun angezeigten Liste die Benutzergruppen aus, denen Sie die Rolle zuweisen möchten. Wenn Sie eine Benutzergruppe auswählen, wird die Gruppe in der Liste Selected user groups angezeigt.



Zum Entfernen einer Benutzergruppe aus der Liste Selected user groups führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf Search, um eine Liste aller Benutzergruppen in der ausgewählten Domäne anzuzeigen.
- Geben Sie den Gruppennamen vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf Search, um die Liste der Benutzergruppen einzuschränken.

Die Namen der Benutzergruppen in der Liste sind in der nun angezeigten Liste mit einem Häkchen gekennzeichnet. Navigieren Sie durch die Liste und deaktivieren Sie die Kontrollkästchen aller Gruppen, die Sie entfernen möchten.

RBAC-Rollen und -Berechtigungen

Nov 12, 2015

Jeder vordefinierten Rolle für die rollenbasierte Zugriffssteuerung (RBAC) sind bestimmte Zugriffs- und Featureberechtigungen zugewiesen. In diesem Artikel werden die einzelnen Berechtigungen erläutert. Weitere Informationen über das Konfigurieren von RBAC-Rollen finden Sie unter Konfigurieren von Rollen mit RBAC.

So aktivieren Sie in XenMobile Autodiscovery für die Benutzerregistrierung

Jul 27, 2016

Autodiscovery vereinfacht den Registrierungsvorgang für Benutzer. Diese können bei der Geräteregistrierung dann ihren Netzwerkbenutzernamen und ihr Active Directory-Kennwort verwenden, statt Angaben zum XenMobile-Server eingeben zu müssen. Der Benutzername wird im Benutzerprinzipalnamensformat (UPN) eingegeben, z. B. user@mycompany.com.

Autodiscovery können Sie über das zugehörige Dienstportal auf https://xenmobiletools.citrix.com aktivieren. Weitere Informationen zum Autodiscovery-Dienstportal finden Sie unter XenMobile Autodiscovery-Dienst.

In manchen Fällen muss zum Aktivieren von Autodiscovery der Citrix Support kontaktiert werden. Sie können hierfür die Schritte unten befolgen, um dem technischen Support von Citrix Ihre Bereitstellungsinformationen und – für Windows-Geräte – ein SSL-Zertifikat zukommen zu lassen. Wenn Citrix diese Informationen erhalten hat, werden bei der Geräteregistrierung die Domäneninformationen extrahiert und einer Serveradresse zugeordnet. Diese Informationen werden in der XenMobile-Datenbank gepflegt, sodass sie bei jeder Registrierung durch einen Benutzer verfügbar und zugänglich sind.

1. Wenn Sie Autodiscovery über das Autodiscovery-Dienstportal auf https://xenmobiletools.citrix.com nicht aktivieren können, öffnen Sie über das Citrix Supportportal einen Supportfall und geben Sie folgende Informationen an:
   - Die Domäne mit den Konten, mit denen Benutzer Geräte registrieren.
   - Vollqualifizierter Domänenname (FQDN) des XenMobile-Servers.
   - XenMobile-Instanzname. Standardmäßig lautet der Instanzname (Groß-/Kleinschreibung beachten) zdm.
   - Benutzer-ID-Typ (entweder UPN oder E-Mail). Standardeinstellung ist UPN.
   - Der für die iOS-Registrierung verwendete Port, wenn Sie die standardmäßige Portnummer 8443 geändert haben.
   - Der Port, über den der XenMobile-Server Verbindungen annimmt, wenn Sie die standardmäßige Portnummer 443 geändert haben.
   - E-Mail-Adresse des XenMobile-Administrators (optional).
2. Wenn Windows-Geräte registriert werden sollen, führen Sie die folgenden Schritte aus:
   1. Beschaffen Sie ein öffentlich signiertes SSL-Zertifikat (kein Wildcard-Zertifikat) für enterpriseenrollment.mycompany.com, wobei mycompany.com die Domäne mit den Konten ist, die die Benutzer bei der Registrierung verwenden. Senden Sie das SSL-Zertifikat in PFX-Format und das zugehörige Kennwort im Anhang Ihrer Anforderung.
   2. Erstellen Sie einen Datensatz mit einem kanonischen Namen (CNAME) im DNS und weisen Sie die Adresse des SSL-Zertifikats (enterpriseenrollment.mycompany.com) der Adresse autodisc.zc.zenprise.com zu. Wenn ein Benutzer ein Windows-Gerät unter Angabe des UPNs und der Details des XenMobile-Servers registriert, weist der Citrix Registrierungsserver das Gerät an, ein gültiges Zertifikat vom XenMobile-Server anzufordern.

Ihr Supportfall wird aktualisiert, sobald Ihre Daten und ggf. das Zertifikat den Citrix Servern hinzugefügt wurden. Nun ist eine Registrierung mit Autodiscovery möglich.

Hinweis: Für eine Registrierung mit mehreren Domänen können Sie auch ein Multidomänenzertifikat verwenden. Das Multidomänenzertifikat muss folgende Struktur haben:

- SubjectDN mit einem CN, der die primäre Domäne für das Zertifikat angibt (z. B. enterpriseenrollment.mycompany1.com)
- SANs der restlichen Domänen (z. B. enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com usw.)

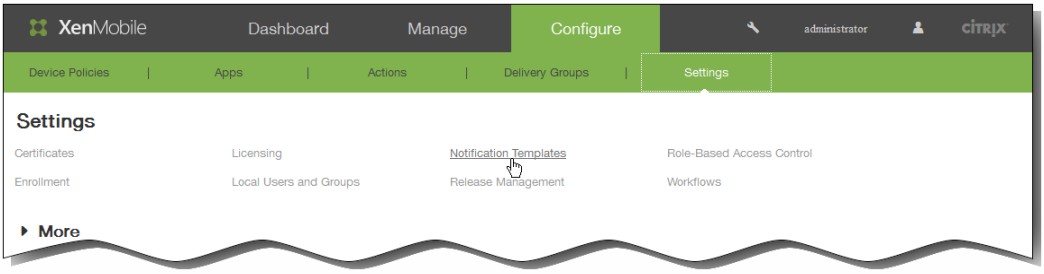
Erstellen und Aktualisieren von Benachrichtigungsvorlagen

Nov 12, 2015

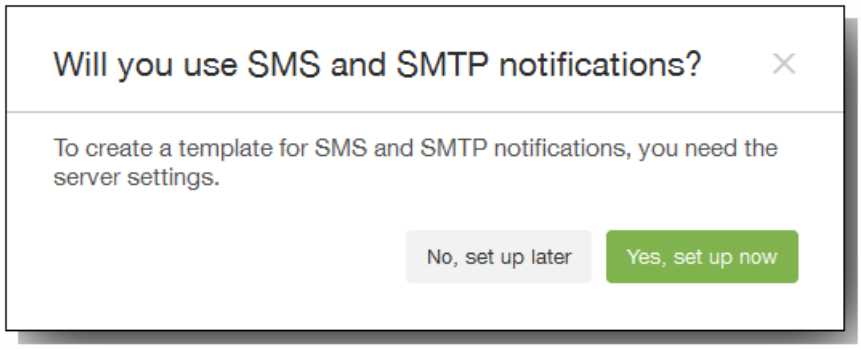
Sie können Benachrichtigungsvorlagen zur Verwendung in automatisierten Aktionen, bei der Registrierung und für Standardbenachrichtigungen an Benutzer erstellen und aktualisieren. Sie können Benachrichtigungsvorlagen zum Senden von Nachrichten über drei verschiedene Kanäle konfigurieren: Worx Home, SMTP oder SMS.

Hinweis: Für die Verwendung von SMTP oder SMS als Kanal für den Versand von Benachrichtigungen müssen Sie diese vor dem Aktivieren zunächst einrichten. XenMobile fordert Sie beim Hinzufügen von Benachrichtigungsvorlagen zum Einrichten der Kanäle auf, wenn dies nicht bereits geschehen ist. Weitere Informationen finden Sie unter Benachrichtigungen in XenMobile.

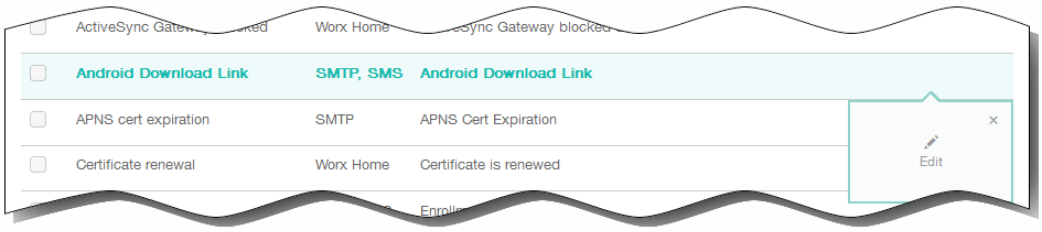
1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Notification Templates.



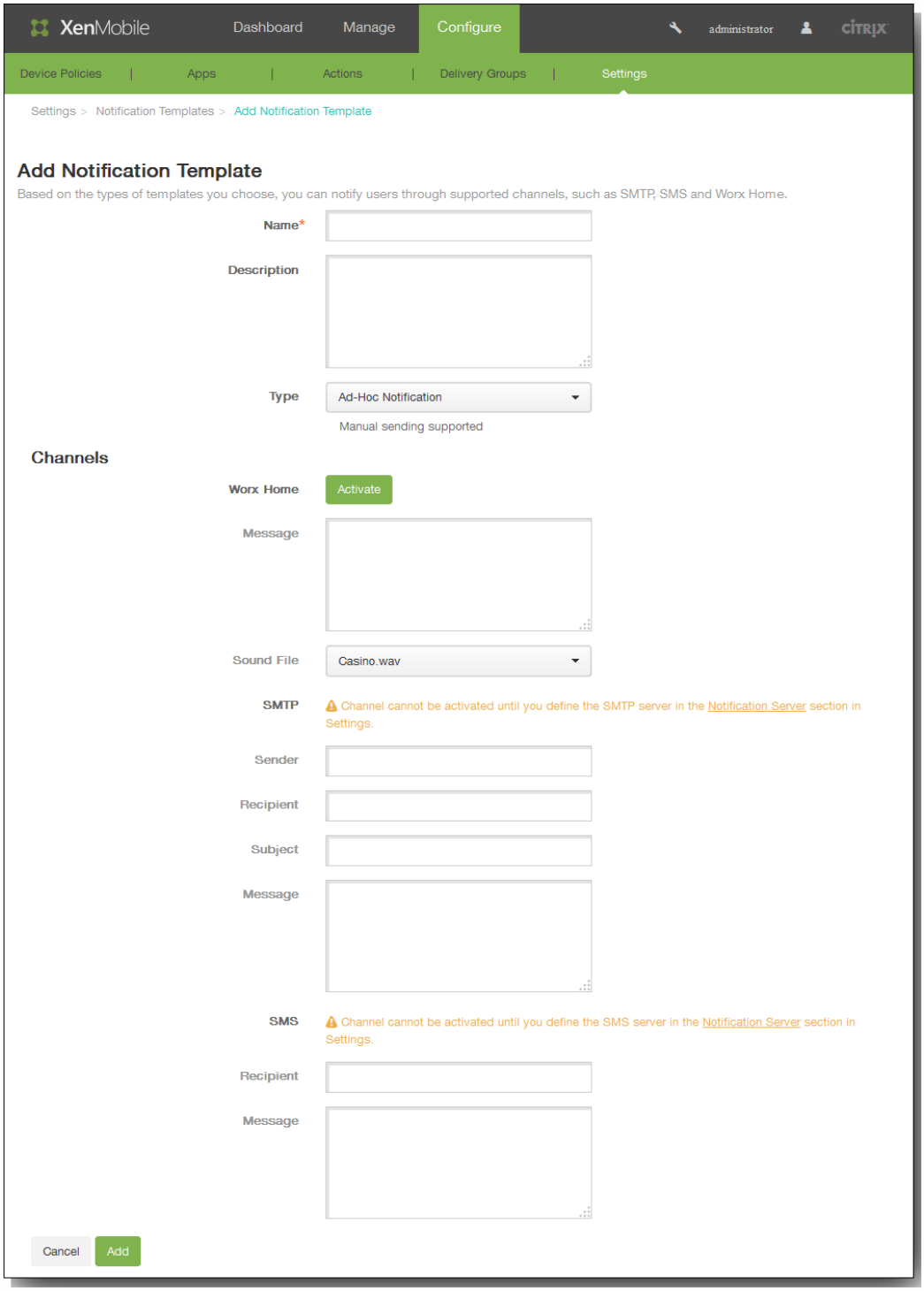
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf Add, um eine neue Benachrichtigungsvorlage hinzuzufügen. Wenn kein SMS-Gateway oder SMTP-Server eingerichtet wurde, wird eine Meldung bezüglich der Verwendung von SMS- und SMTP-Benachrichtigungen angezeigt. Sie können wählen, ob Sie SMTP-Server oder SMS-Gateway sofort oder später einrichten möchten. Weitere Informationen finden Sie unter Benachrichtigungen in XenMobile.
     Hinweis: Wenn Sie sich für eine sofortige Einrichtung entschieden haben, werden Sie zu der Seite Configure > Settings > Notification Server geleitet. Nach der Einrichtung der gewünschten Kanäle können Sie zur Seite Configure > Settings > Notification Template zurückkehren, um mit dem Hinzufügen bzw. Ändern von Benachrichtigungsvorlagen fortzufahren.
     Wichtig: Wenn Sie entscheiden, die SMS- oder SMTP-Server-Einstellungen später einzurichten, können Sie diese Kanäle beim Hinzufügen oder Bearbeiten einer Benachrichtigungsvorlage nicht aktivieren, d. h. die Kanäle sind nicht zum Senden von Benutzerbenachrichtigungen verfügbar.



- Wählen Sie eine vorhandene Vorlage zum Bearbeiten oder Löschen aus. Klicken Sie auf die gewünschte Option.
  Hinweis:
  - Sie können nur Benachrichtigungsvorlagen löschen, die Sie selbst hinzugefügt haben, nicht aber vordefinierte Vorlagen.
  - Wenn Sie das Kontrollkästchen neben einer Benachrichtigungsvorlage auswählen, wird das Menü mit den Optionen oberhalb der Liste der Benachrichtigungsvorlagen eingeblendet. Wenn Sie auf eine andere Stelle im Eintrag klicken, wird es rechts neben dem Eintrag eingeblendet.
  - XenMobile umfasst viele vordefinierte Vorlagen für die diversen Ereignisse, auf die XenMobile automatisch für jedes Gerät im System reagiert.



Wenn Sie eine Benachrichtigungsvorlage hinzufügen, wird die Seite Add Notification Template angezeigt.



3. Konfigurieren Sie auf der Seite Add Notification Template (bzw. Edit Notification Template, wenn Sie eine vorhandene Benachrichtigungsvorlage bearbeiten) folgende Informationen:
   1. Name: Geben Sie einen aussagekräftigen Namen für die Vorlage ein.
   2. Description: Geben Sie eine Beschreibung für die Vorlage ein.
   3. Type: Wählen Sie den Benachrichtigungstyp aus. Es werden nur für den ausgewählten Typ unterstützte Kanäle angezeigt.
      Hinweis: Unterhalb einiger Vorlagentypen wird Manual sending supported angezeigt. Solche Vorlagen sind in der Liste Notifications im Dashboard und auf der Seite "Devices" verfügbar und können manuell an Benutzer versendet werden. Manuelles Senden ist bei Vorlagen, bei denen für das Betreffs- oder Nachrichtenfeld die folgenden Makros verwendet

werden, über keinen Kanal möglich:

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

Achtung: Es ist nur eine APNs Cert Expiration-Vorlage zulässig und zwar die vordefinierte Vorlage. Sie können also keine Vorlage dieses Typs hinzufügen.

4. Channels: Konfigurieren Sie die Informationen für jeden Kanal, der für die Benachrichtigung verwendet werden soll. Sie können einen beliebigen oder alle Kanäle auswählen. Welche Kanäle Sie wählen, hängt davon ab, wie Sie Benachrichtigungen senden möchten:

- Wenn Sie Worx Home auswählen, erhalten nur iOS- und Android-Geräte Benachrichtigungen. Diese werden im Infobereich des Geräts angezeigt.
- Wenn Sie SMS auswählen, empfangen nur Geräte mit einer SIM-Karte Benachrichtigungen.
- Wenn Sie SMTP auswählen, sollten die meisten Benutzer Benachrichtigungen empfangen, da sie sich mit ihrer E-Mail-Adresse registriert haben.

Worx Home

1. Activate: Klicken Sie hier zum Aktivieren dieses Benachrichtigungskanals.
2. Message: Geben Sie die Nachricht ein, die an Benutzer gesendet werden soll. Dieses Feld ist erforderlich, wenn Sie Worx Home verwenden.
3. Sound File: Wählen Sie den Benachrichtigungston aus, der bei Empfang einer Benachrichtigung ausgegeben werden soll.

SMTP

1. Klicken Sie auf Activate, um den Benachrichtigungskanal zu aktivieren.
   Wichtig: Sie können den SMTP-Kanal nur aktivieren, wenn Sie bereits den SMTP-Server eingerichtet haben. Weitere Informationen finden Sie unter Benachrichtigungen in XenMobile.
2. Sender: Geben Sie optional einen Absender für die Benachrichtigung an (Name, E-Mail-Adresse oder beides).
3. Recipient: Dieses Feld enthält ein vordefiniertes Makro für alle Benachrichtigungen mit Ausnahme von Ad-hoc-Benachrichtigungen, um sicherzustellen, dass sie an die richtige SMTP-Empfängeradresse gesendet werden. Citrix empfiehlt, Makros in Vorlagen nicht zu ändern. Sie können auch Empfänger hinzufügen (z. B. den Administrator des Unternehmens), indem Sie deren Adressen getrennt durch Semikola (;) eingeben. Zum Senden von Ad-hoc-Benachrichtigungen können Sie Empfänger auf dieser Seite eingeben oder Geräte auf der Seite Manage > Devices auswählen und die Benachrichtigungen von dort aus senden. Weitere Informationen finden Sie unter Hinzufügen von Geräten und Anzeigen von Gerätedetails in XenMobile
4. Subject: Geben Sie einen aussagekräftigen Betreff für die Benachrichtigung ein. Dieses Feld ist erforderlich, wenn Sie SMTP verwenden.
5. Message: Geben Sie die Nachricht ein, die an Benutzer gesendet werden soll.

SMS

1. Klicken Sie auf Activate, um den Benachrichtigungskanal zu aktivieren.
   Wichtig: Sie können den SMTP-Kanal nur aktivieren, wenn Sie bereits den SMTP-Server eingerichtet haben. Weitere Informationen finden Sie unter Benachrichtigungen in XenMobile.
2. Recipient: Dieses Feld enthält ein vordefiniertes Makro für alle Benachrichtigungen mit Ausnahme von Ad-hoc-Benachrichtigungen, um sicherzustellen, dass sie an die richtige SMTP-Empfängeradresse gesendet werden. Citrix empfiehlt, Makros in Vorlagen nicht zu ändern. Zum Senden von Ad-hoc-Benachrichtigungen können Sie Empfänger

eingeben oder Geräte auf der Seite Manage > Devices auswählen. Weitere Informationen finden Sie unter Hinzufügen von Geräten und Anzeigen von Gerätedetails in XenMobile

3. Message: Geben Sie die Nachricht ein, die an Benutzer gesendet werden soll. Dieses Feld ist erforderlich, wenn Sie SMS verwenden.
   Wichtig: Sie können den SMS-Kanal nur aktivieren, wenn Sie bereits das SMS-Gateway eingerichtet haben. Weitere Informationen finden Sie unter Benachrichtigungen in XenMobile.

5. Klicken Sie auf Add, um die neue Vorlage hinzuzufügen, bzw. auf Save, um Ihre Änderungen zu speichern. Wenn alle Kanäle richtig konfiguriert sind, werden sie in dieser Reihenfolge auf der Seite Notification Templates angezeigt: SMTP, SMS und Worx Home. Falsch konfigurierte Kanäle werden nach den richtig konfigurierten Kanälen angezeigt.

Verwalten von Bereitstellungsgruppen

Jul 27, 2016

Die Gerätekonfiguration und -verwaltung umfasst üblicherweise das Erstellen von Ressourcen (Richtlinien und Apps) und Aktionen in der XenMobile-Konsole und anschließend das Verpacken dieser Ressourcen für die Verwendung mit Bereitstellungsgruppen. Die Reihenfolge, in der XenMobile Ressourcen und Aktionen in einer Bereitstellungsgruppe per Push auf Geräten bereitstellt, wird als Bereitstellungsreihenfolge bezeichnet. In diesem Abschnitt wird beschrieben, wie Sie Bereitstellungsgruppen hinzufügen, verwalten und bereitstellen, wie Sie die Bereitstellungsreihenfolge der Ressourcen und Aktionen in Bereitstellungsgruppen ändern, und wie XenMobile die Bereitstellungsreihenfolge ermittelt, wenn ein Benutzer in mehreren Bereitstellungsgruppen ist und es duplizierte oder widersprüchlichen Richtlinien gibt

Bereitstellungsgruppe sind Kategorien von Benutzern, für deren Geräte Sie Kombinationen aus Richtlinien, Apps und Aktionen bereitstellen. Die Aufnahme in einer Bereitstellungsgruppe basiert normalerweise auf Benutzermerkmalen wie Unternehmen, Land, Abteilung, Bürostandort usw. Mit Bereitstellungsgruppen haben Sie mehr Kontrolle darüber, wem welche Ressourcen wann zur Verfügung stehen. Sie können eine Bereitstellungsgruppe allen Benutzern oder einer enger spezifizierten Benutzergruppe bereitstellen.

Beim Bereitstellen von Ressourcen für eine Bereitstellungsgruppe wird eine Pushbenachrichtigung an alle Benutzer mit iOS- und Windows Phone- oder Windows Tablet-Geräte gesendet, eine Verbindung mit XenMobile herzustellen, sodass Sie die Geräte neu auswerten und Apps, Richtlinien und Aktionen bereitstellen können. Benutzer mit anderen Geräten erhalten die Ressourcen sofort, sofern bereits eine Verbindung besteht, oder – basierend auf der für sie eingerichteten Planungsrichtlinie – wenn sie das nächste Mal eine Verbindung herstellen.

Die Standardbereitstellungsgruppe "AllUsers" wird bei der Installation und Konfiguration von XenMobile erstellt. Sie enthält alle lokalen und Active Directory-Benutzer. Die Gruppe "AllUsers" kann nicht gelöscht werden, Sie können die Gruppe jedoch deaktivieren, wenn Sie Ressourcen nicht per Push für alle Benutzer bereitstellen möchten.

Bereitstellungsreihenfolge

Die Bereitstellungsreihenfolge ist die Reihenfolge, in der XenMobile Ressourcen per Push auf den Geräten bereitstellt. Beim Ermitteln der Bereitstellungsreihenfolge wendet XenMobile Filter- und Steuerungskriterien für Richtlinien, Apps, Aktionen und Bereitstellungsgruppen an, z. B. Bereitstellungsregeln und Bereitstellungszeitpläne. Vor dem Hinzufügen von Bereitstellungsgruppen, beachten Sie, wie sich die Informationen in diesem Abschnitt mit Ihren Bereitstellungszielsetzungen zusammenhängen.

Hier ist eine Zusammenfassung der grundlegende Konzepte für die Bereitstellungsreihenfolge:

- **Bereitstellungsreihenfolge:** Die Reihenfolge, in der XenMobile Ressourcen (Richtlinien und Apps) und Aktionen per Push auf einem Gerät bereitstellt.
- **Bereitstellungsregeln:** XenMobile verwendet die Bereitstellungsregeln, die Sie für Geräteigenschaften angeben, zum Filtern von Richtlinien, Apps, Aktionen und Bereitstellungsgruppen. Beispiel: Eine Bereitstellungsregel könnte angeben, dass eine Bereitstellungspaket per Push bereitgestellt wird, wenn ein Domänenname einen bestimmten Wert hat.
- **Bereitstellungszeitplan:** XenMobile verwendet den Bereitstellungszeitplan, den Sie für Aktionen, Apps und Geräterichtlinien angeben, um die Bereitstellung dieser Elemente zu steuern. Sie können festlegen, dass eine Bereitstellung sofort, zu einem bestimmten Datum und einer bestimmten Uhrzeit oder basierend auf Bereitstellungsbedingungen stattfindet.

Die folgende Tabelle zeigt diese und weitere Kriterien, die Sie bestimmten Objekten oder Ressourcen zuordnen können, um sie zu filtern oder um deren Bereitstellung zu steuern.

Objekt/Ressource	Filter/Steuerungskriterien
Geräterichtlinie	Geräteplattform Bereitstellungsregeln (basierend auf Geräteeigenschaften) Bereitstellungszeitplan
App	Geräteplattform Bereitstellungsregeln (basierend auf Geräteeigenschaften) Bereitstellungszeitplan
Aktion	Bereitstellungsregeln (basierend auf Geräteeigenschaften) Bereitstellungszeitplan
Bereitstellungsgruppe	Benutzer/Gruppen Bereitstellungsregeln (basierend auf Geräteeigenschaften)

Es ist in einer typischen Umgebung wahrscheinlich, dass mehrere Bereitstellungsgruppen einem einzelnen Benutzer zugewiesen werden. Das hat die folgenden möglichen Auswirkungen:

- In den Bereitstellungsgruppen sind duplizierte Objekte.
- Eine bestimmte Richtlinie ist anders konfiguriert in mehr als einer Bereitstellungsgruppe, die einem Benutzer zugewiesen ist.

Tritt eine der beiden Situationen ein, berechnet XenMobile die Bereitstellungsreihenfolge für alle Objekte, die es an ein Gerät liefern muss oder für die Aktionen ausgeführt werden sollen. Die Berechnungsschritte sind unabhängig von der Geräteplattform.

Berechnungsschritte:

1. Alle Bereitstellungsgruppen für einen bestimmten Benutzer ermitteln, basierend auf den Filtern für Benutzer/Gruppen und den Bereitstellungsregeln.
2. Erstellen einer sortierten Liste mit allen Ressourcen (Richtlinien, Aktionen und Apps) in den ausgewählten Bereitstellungsgruppen, die basierend auf den Filtern für Geräteplattform, Bereitstellungsregeln und Bereitstellungszeitplan gelten. Der Sortieralgorithmus ist wie folgt:

a. Ressourcen von Bereitstellungsgruppen, eine benutzerdefinierte Bereitstellungsreihenfolge haben, werden vor die Bereitstellungsgruppen ohne Bereitstellungsreihenfolge gestellt. Die Begründung wird nach diesen Schritten beschrieben.

b. Bei einem Gleichstand zwischen Bereitstellungsgruppen werden Ressourcen von Bereitstellungsgruppen nach dem

Bereitstellungsgruppennamen sortiert. Beispiel: Ressourcen von Bereitstellung Gruppe A werden vor denen aus Bereitstellungsgruppe B einsortiert.

c. Wurde eine benutzerdefinierte Bereitstellungsreihenfolge für Ressourcen in einer Bereitstellungsgruppe angegeben, muss sie beim Sortieren erhalten bleiben. Sonst die Ressourcen in der Bereitstellungsuppe nach Ressourcenname sortieren.

d. Erscheint dieselbe Ressource mehr als einmal, wird das Duplikat der Ressource entfernt.

Ressourcen, denen eine benutzerdefinierte Reihenfolge zugeordnet ist, werden vor Ressourcen bereitgestellt, für die keine benutzerdefinierte Reihenfolge festgelegt wurde. Eine Ressource kann in mehreren dem Benutzer zugewiesenen Bereitstellungsgruppen sein. Wie in den Schritte oben beschrieben, entfernt der Berechnungsalgorithmus redundante Ressourcen und stellt nur die erste Ressource in dieser Liste bereit. Dadurch, dass die Ressourcenduplikate auf diese Weise entfernt werden, setzt XenMobile die Reihenfolge durch, die vom XenMobile-Administrator festgelegt wurde.

Beispiel: Angenommen, Sie haben zwei Bereitstellungsgruppen:

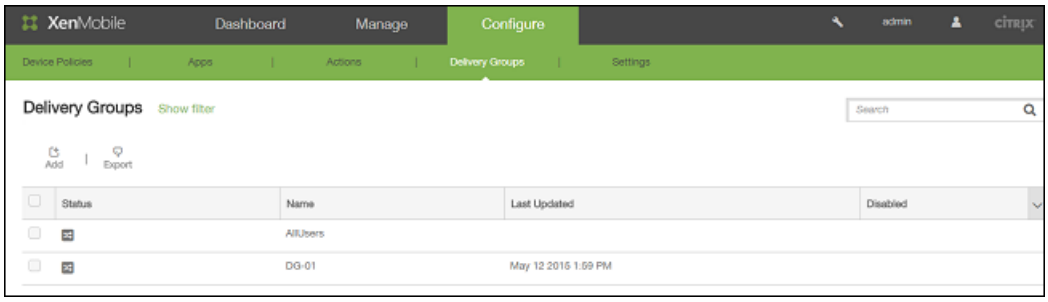
- Bereitstellungsgruppe A: Reihenfolge für die Ressourcen (RES) RES1 und RES2 wurde **nicht angegeben**.
- Bereitstellungsgruppe B: Reihenfolge für die Ressourcen (RES) RES3 und RES2 wurde **angegeben**. In diesem Fall sollte RES3 vor RES2 bereitgestellt werden.

Sortierte der Berechnungsalgorithmus die Bereitstellungsgruppen nur nach Name, würde XenMobile die Bestellung in dieser Reihenfolge durchführen: RES1, RES2, RES3. XenMobile würde RES2, ein Duplikat, aus Bereitstellungsgruppe B ignorieren.

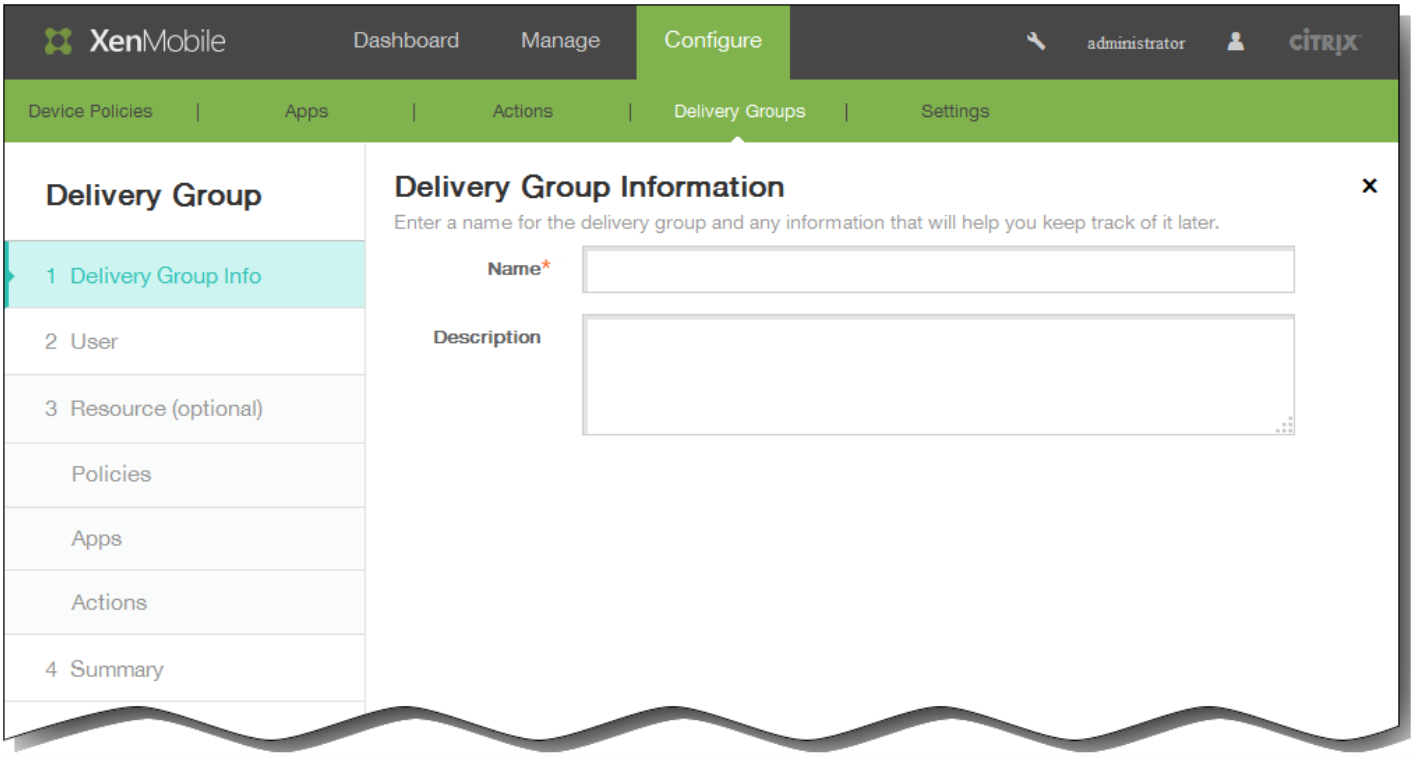
Tatsächlich stellt der Berechnungsalgorithmus aber die Ressourcen aus Bereitstellungsgruppe B vor die Ressourcen aus Bereitstellungsgruppe A, sodass XenMobile die Bereitstellung in dieser Reihenfolge durchführt: RES3, RES2, RES1. RES2 aus Bereitstellungsgruppe A wird als Duplikat ignoriert. Dieser Algorithmus wendet daher die vom XenMobile-Administrator festgelegte Reihenfolge an.

So fügen Sie eine Bereitstellungsgruppe hinzu

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Bereitstellungsgruppen**. Die Seite **Geräterichtlinien** wird angezeigt.



2. Klicken Sie auf der Seite **Bereitstellungsgruppen** auf **Hinzufügen**. Die Seite **Bereitstellungsgruppeninformationen** wird angezeigt.

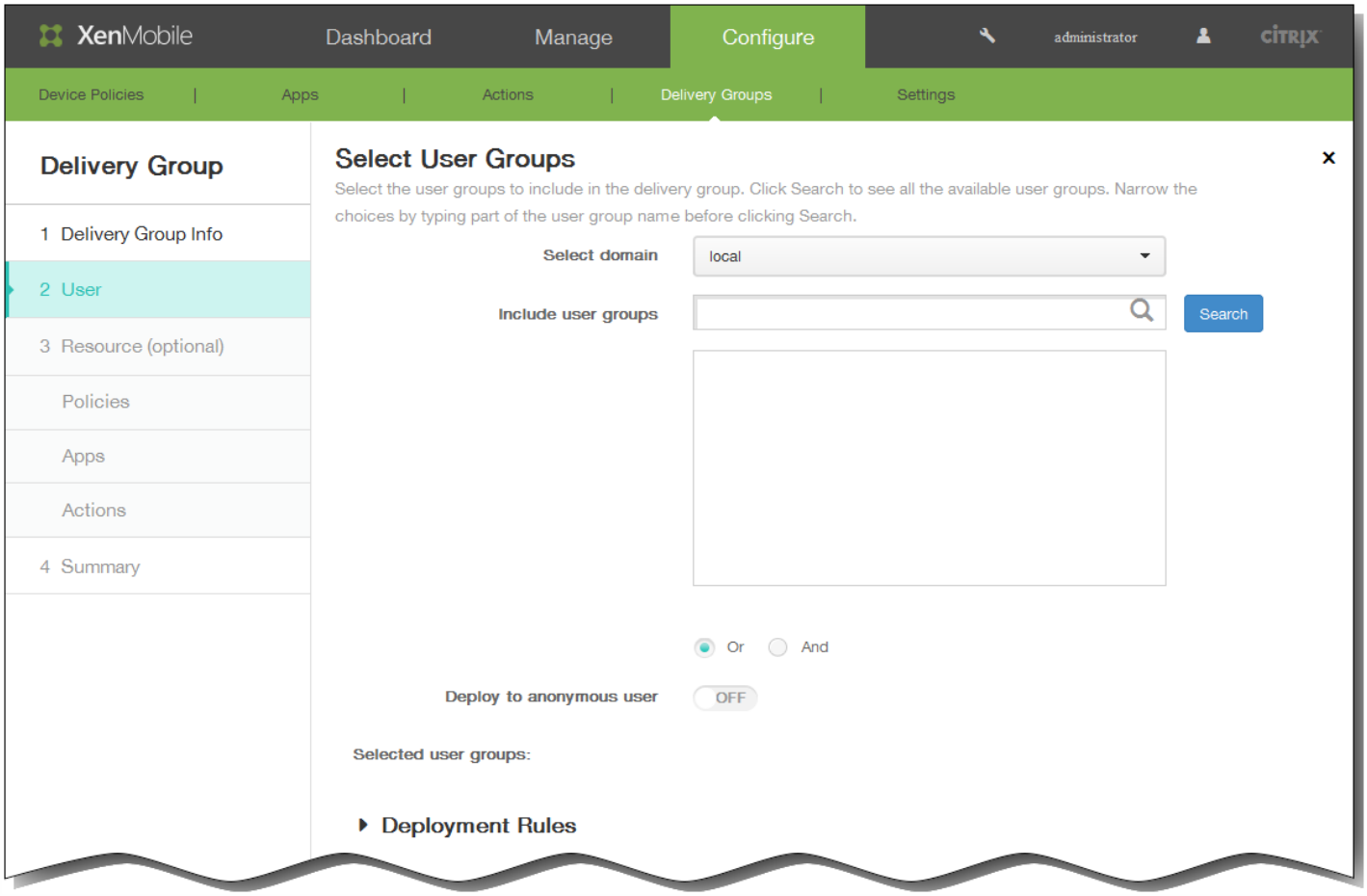


3. Geben Sie auf der Seite **Bereitstellungsgruppeninformationen** die folgenden Informationen ein:

   Name: Geben Sie einen aussagekräftigen Namen für die Bereitstellungsgruppe ein.

   Beschreibung: Geben Sie optional eine Beschreibung der Bereitstellungsgruppe ein.

4. Klicken Sie auf **Weiter**. Die Seite zur Auswahl der Benutzer wird angezeigt.



5. Geben Sie im Bereich **Benutzergruppen auswählen** die folgenden Informationen ein:

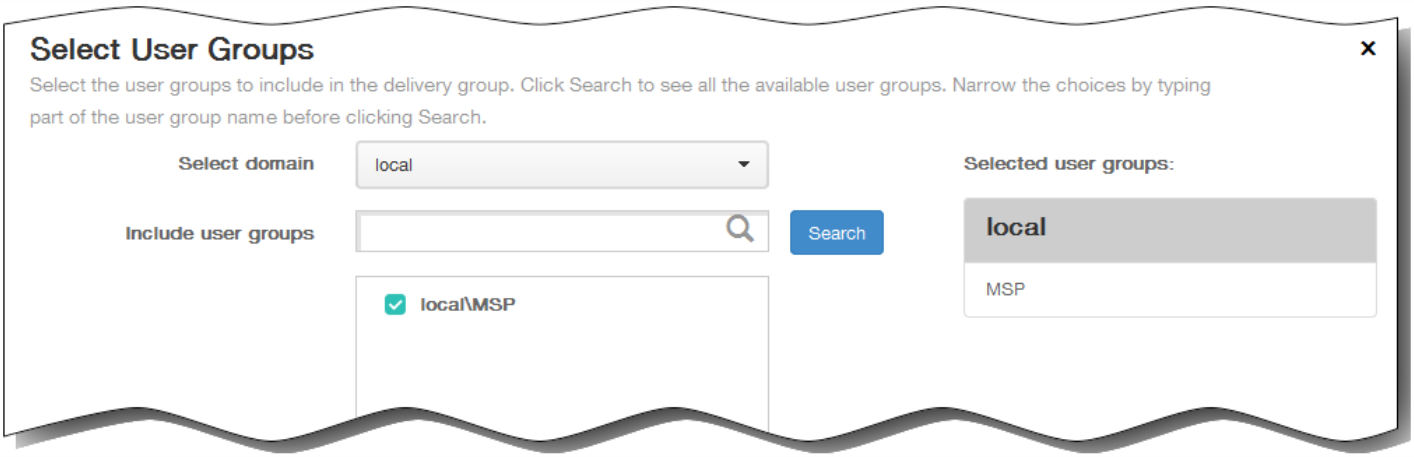
a. **Domäne auswählen**: Wählen Sie in der Liste die Domäne aus, in der Sie Benutzer auswählen möchten.

b. **Benutzergruppen einschließen**: Führen Sie einen der folgenden Schritte aus:

Klicken Sie auf **Suchen**, um eine Liste aller Benutzergruppen in der ausgewählten Domäne anzuzeigen.

Geben Sie den Gruppennamen vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf **Suchen**, um die Liste der Benutzergruppen einzuschränken.

c. Klicken Sie in der Liste der Benutzergruppen auf die Gruppen, die Sie hinzufügen möchten. Die ausgewählten Gruppen werden in der Liste **Ausgewählte Benutzergruppen** angezeigt.



Zum Entfernen einer Benutzergruppe aus der Liste **Ausgewählte Benutzergruppen** führen Sie einen der folgenden Schritte aus:

Klicken Sie auf **Suchen**, um eine Liste aller Benutzergruppen in der ausgewählten Domäne anzuzeigen.

Geben Sie den Gruppennamen vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf **Suchen**, um die Liste der Benutzergruppen einzuschränken.

Die Namen der ausgewählten Benutzergruppen sind in der nun angezeigten Liste mit einem Häkchen gekennzeichnet. Navigieren Sie durch die Liste und deaktivieren Sie die Kontrollkästchen aller Gruppen, die Sie entfernen möchten.

d. **Oder/Und**: Wählen Sie aus, ob Benutzer für die bereitzustellende Ressource nur einer Gruppe angehören dürfen (Oder) oder ob sie allen Gruppen angehören müssen (Und).

e. **Für anonyme Benutzer bereitstellen**: Wählen Sie aus, ob die Bereitstellung auch für nicht authentifizierte Benutzer in der Bereitstellungsgruppe erfolgen soll.

Hinweis: Nicht authentifizierte Benutzer sind Benutzer, bei denen keine Authentifizierung erfolgen konnte, denen jedoch dennoch eine Verbindung mit XenMobile gestattet wurde.

6. Erweitern Sie **Bereitstellungsregeln** und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte **Basis** wird standardmäßig angezeigt.

a. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.

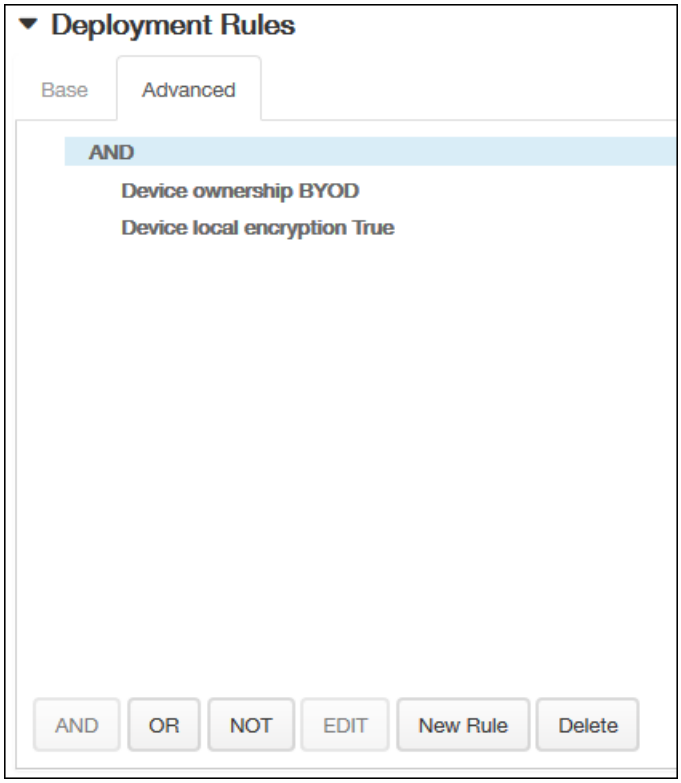
(1) Sie können die Richtlinie bereitstellen, wenn alle oder spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist **Alle**.

(2) Klicken Sie auf **Neue Regel**, um Bedingungen zu definieren.

(3) Klicken Sie in der Liste auf Bedingungen wie **Gerätebesitz** oder **BYOD** (siehe Abbildung oben).

(4) Klicken Sie erneut auf **Neue Regel**, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.

b. Klicken Sie auf die Registerkarte **Erweitert**, um die Regeln mit booleschen Optionen zu kombinieren.



Die Bedingungen, die Sie auf der Registerkarte **Basis** ausgewählt haben, werden angezeigt.

c. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.

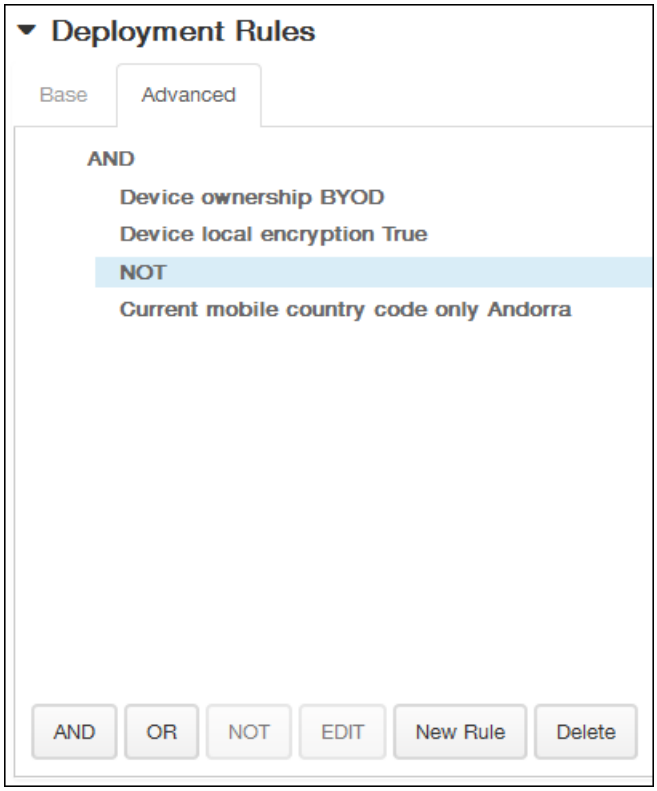
(1) Klicken Sie auf **UND**, **ODER** oder **NICHT**.

(2) Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.

Sie können jederzeit auf eine Bedingung und dann auf **BEARBEITEN** klicken, um die Bedingung zu ändern, oder auf **Löschen**, um die Bedingung zu löschen.

(3) Klicken Sie erneut auf **Neue Regel**, wenn Sie weitere Bedingungen hinzufügen möchten.

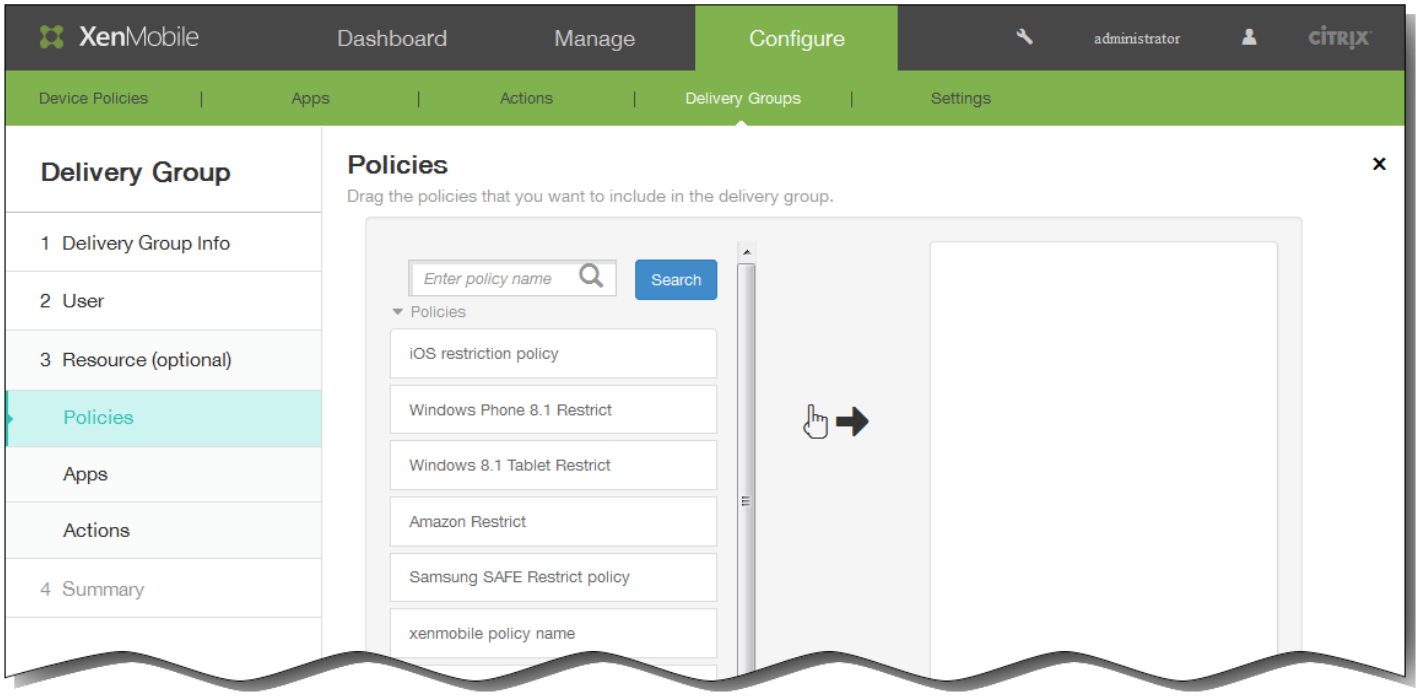
In diesem Beispiel wurde für "Gerätebesitz" **BYOD**, für "Lokale Verschlüsselung des Geräts" und "Passcode richtlinientreu" **Wahr** eingestellt und "Aktueller Ländercode für mobiles Gerät" auf **Andorra** eingeschränkt.



7. Klicken Sie auf **Weiter**. Die Seite zur Auswahl der Ressourcen wird angezeigt. Hier können Sie für die Bereitstellungsgruppe optional Richtlinien, Apps oder Aktionen hinzufügen. Zum Überspringen dieses Schritts klicken Sie unter **Bereitstellungsgruppe** auf **Zusammenfassung**, um eine Zusammenfassung der Bereitstellungsgruppenkonfiguration anzuzeigen, oder führen Sie einen der folgenden Schritte aus:

Hinweis: Zum Überspringen einer Ressource klicken Sie unter **Ressource (optional)** auf die Ressource, die Sie hinzufügen möchten, und folgen Sie den Schritten für diese Ressource.

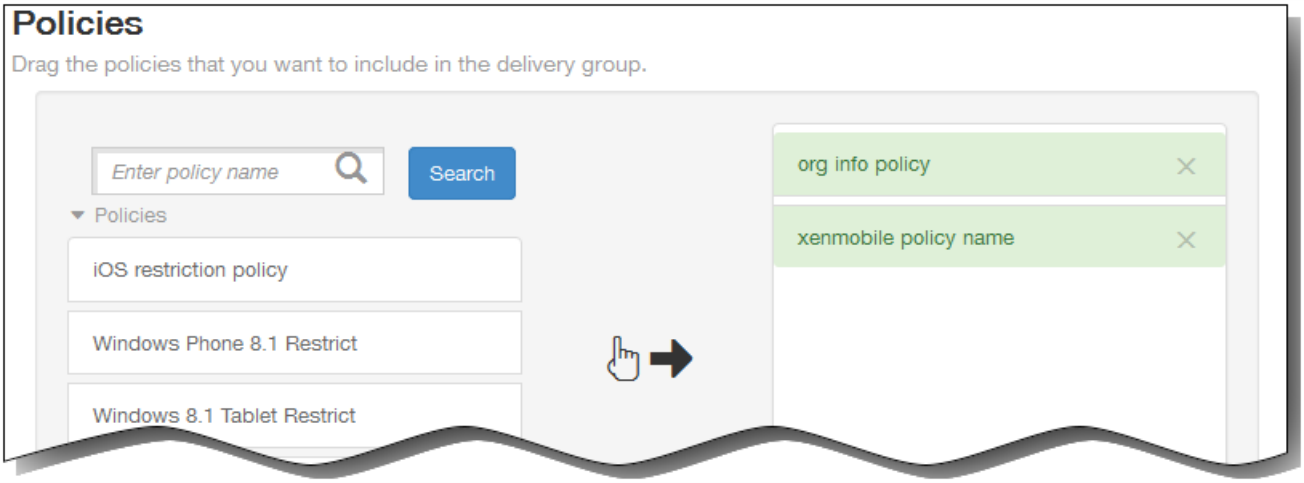
So fügen Sie Richtlinien hinzu



a. Navigieren Sie in der Liste der verfügbaren Richtlinien zu der gewünschten Richtlinie oder geben Sie zum Einschränken der Richtlinienliste in das Suchfeld einen Richtlinienamen vollständig oder teilweise ein und klicken Sie dann auf **Suchen**.

b. Klicken Sie auf eine Richtlinie und ziehen Sie sie in das Feld auf der rechten Seite.

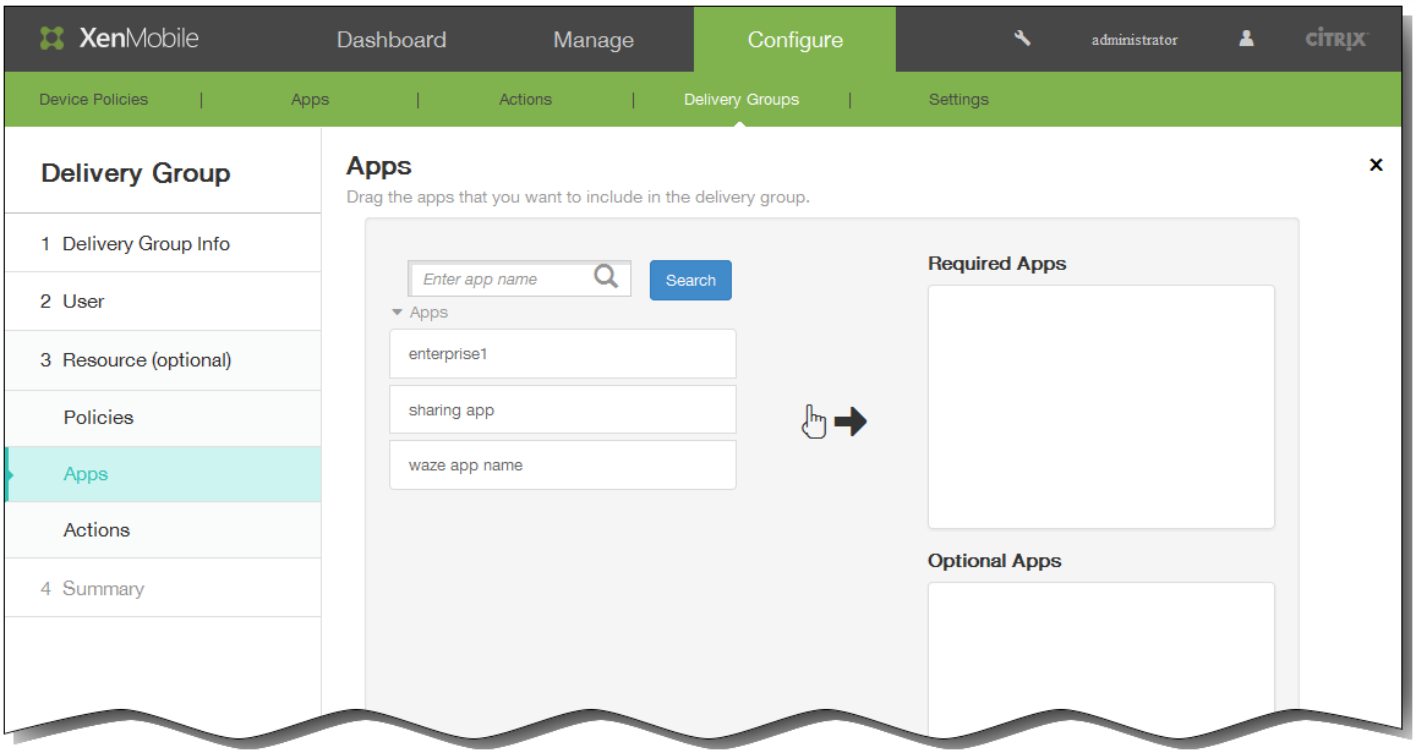
c. Wiederholen Sie die Schritte a und b zum Hinzufügen weiterer Richtlinien.



d. Zum Entfernen einer Richtlinienressource klicken Sie auf das X neben deren Namen.

e. Klicken Sie auf **Weiter**, um die Seite **Apps** aufzurufen. Wenn Sie keine weiteren Ressourcen hinzufügen möchten, klicken Sie unter **Bereitstellungsgruppe** auf **Zusammenfassung**. Daraufhin wird entweder die Seite zur Auswahl der Ressource oder die Seite **Zusammenfassung** angezeigt.

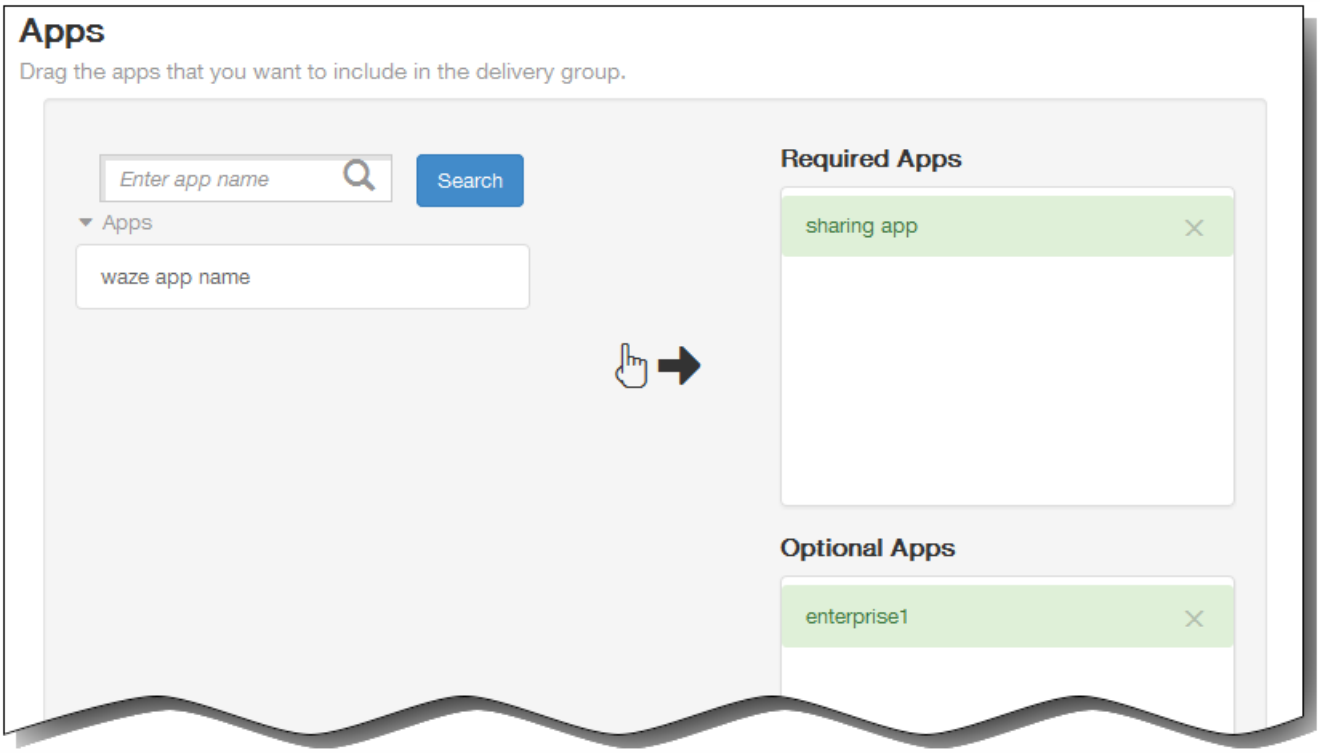
So fügen Sie Apps hinzu



a. Navigieren Sie in der Liste der verfügbaren Apps zu der gewünschten App oder geben Sie zum Einschränken der App-Liste in das Suchfeld einen App-Namen vollständig oder teilweise ein und klicken Sie dann auf **Suchen**.

b. Klicken Sie auf eine App und ziehen Sie sie entweder in das Feld **Erforderliche Apps** oder in das Feld **Optionale Apps**.

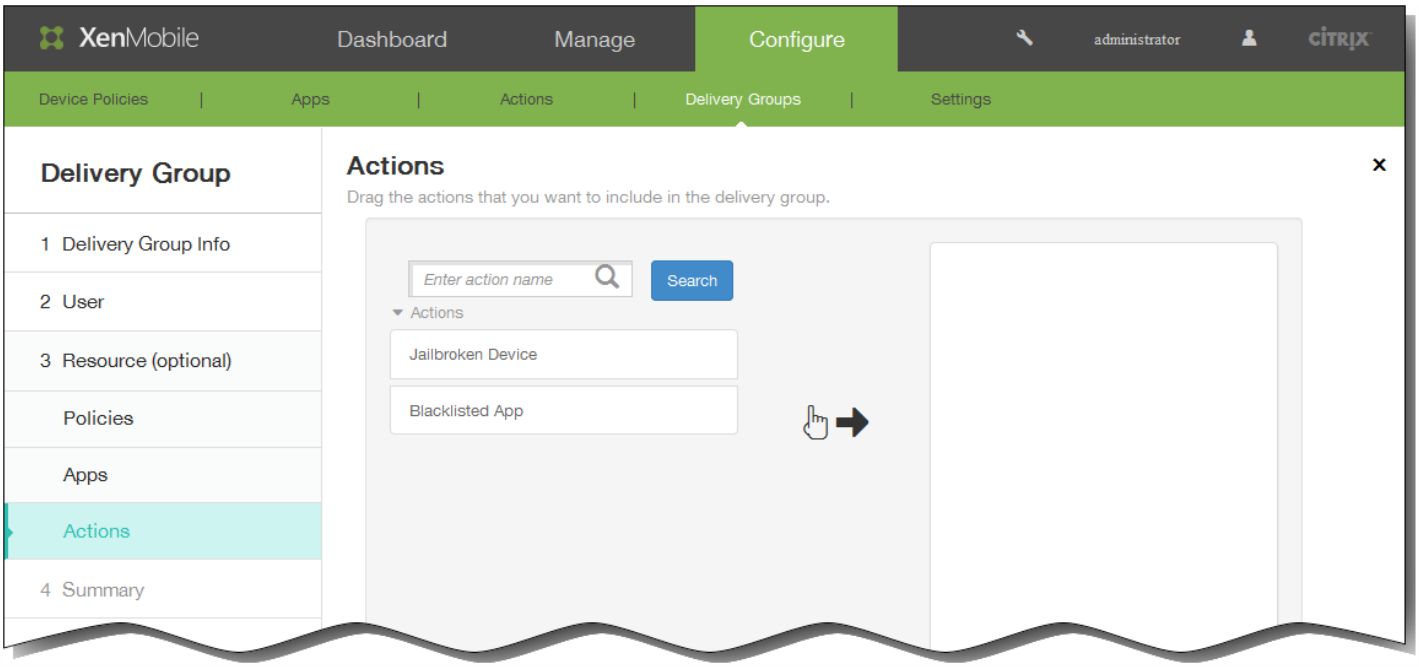
c. Wiederholen Sie die Schritte a und b zum Hinzufügen weiterer Apps.



d. Zum Entfernen einer App-Ressource klicken Sie auf das X neben deren Namen.

e. Klicken Sie auf **Weiter**, um die Seite **Aktionen** aufzurufen. Wenn Sie keine weiteren Ressourcen hinzufügen möchten, klicken Sie unter **Bereitstellungsgruppe** auf **Zusammenfassung**. Daraufhin wird entweder die Seite zur Auswahl der Ressource oder die Seite **Zusammenfassung** angezeigt.

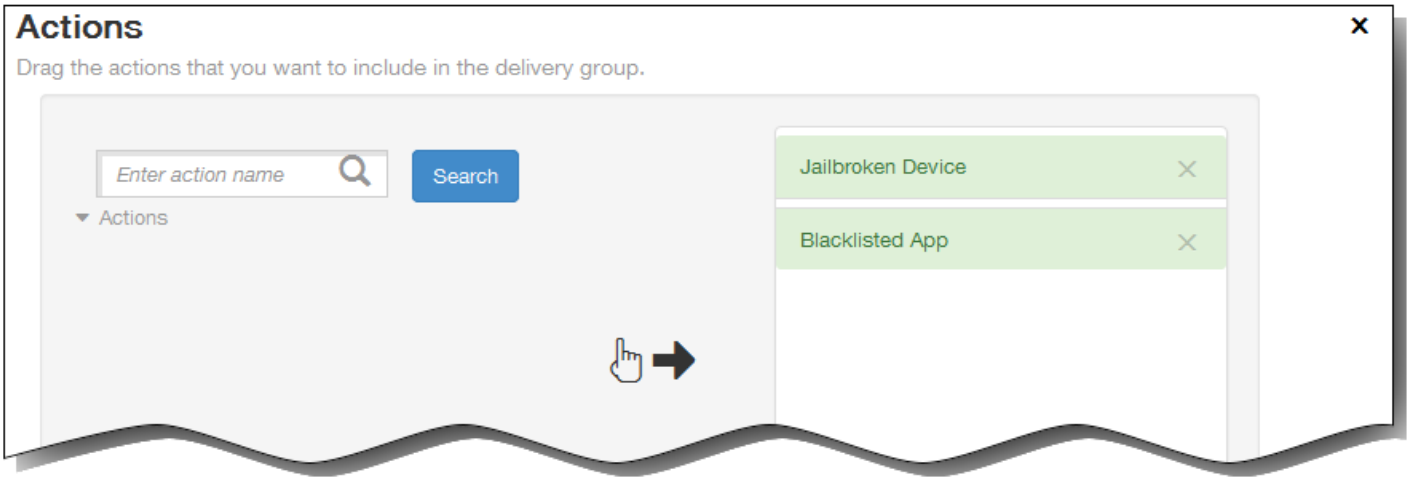
So fügen Sie Aktionen hinzu



a. Navigieren Sie in der Liste der verfügbaren Aktionen zu der gewünschten Aktion oder geben Sie zum Einschränken der Liste der Aktionen in das Suchfeld einen Aktionsnamen vollständig oder teilweise ein und klicken Sie dann auf **Suchen**.

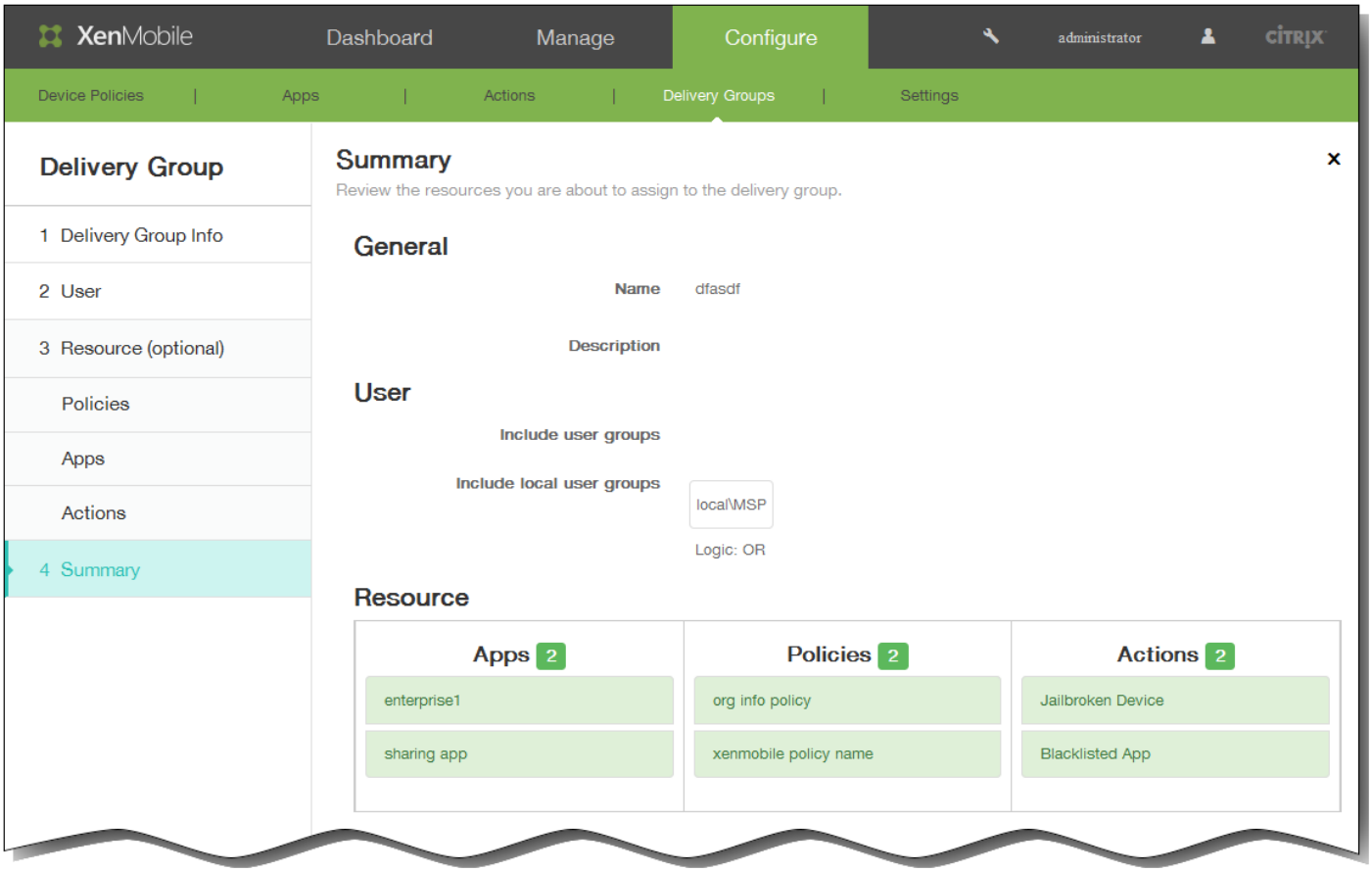
b. Klicken Sie auf eine Aktion und ziehen Sie sie in das Feld auf der rechten Seite.

c. Wiederholen Sie die Schritte a und b zum Hinzufügen weiterer Aktionen.



d. Zum Entfernen einer Aktionsressource klicken Sie auf das X neben deren Namen.

e. Klicken Sie auf **Weiter**. Die Seite **Zusammenfassung** wird angezeigt.



8. Auf der Seite **Zusammenfassung** können Sie die Optionen überprüfen, die Sie für die Bereitstellungsgruppe konfiguriert haben, und die Bereitstellungsreihenfolge der Ressourcen ändern. Klicken Sie auf **Zurück**, um auf vorherige Seiten aufzurufen, wenn Sie Änderungen vornehmen müssen. Klicken Sie auf **Bereitstellungsreihenfolge**, um die Bereitstellungsreihenfolge der Ressourcen zu ändern. Weitere Informationen zum Ändern der Bereitstellungsreihenfolge finden Sie unter Ändern der Bereitstellungsreihenfolge.

9. Klicken Sie auf **Speichern**, um die Bereitstellungsgruppe zu speichern.

So ändern Sie die Bereitstellungsreihenfolge

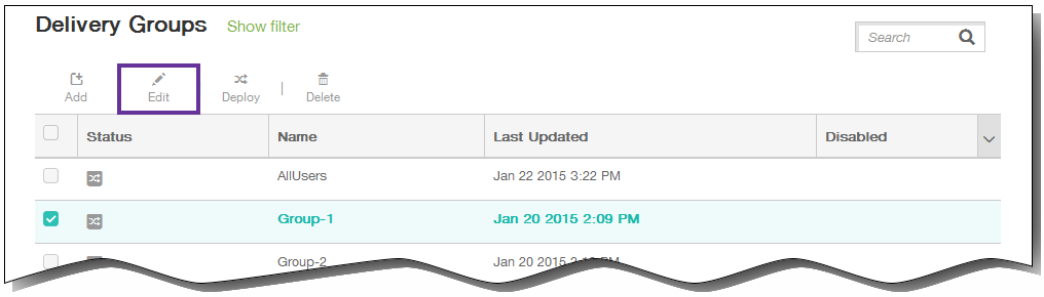
1. Klicken Sie auf die Schaltfläche **Bereitstellungsreihenfolge**. Das Dialogfeld **Bereitstellungsreihenfolge** wird angezeigt.

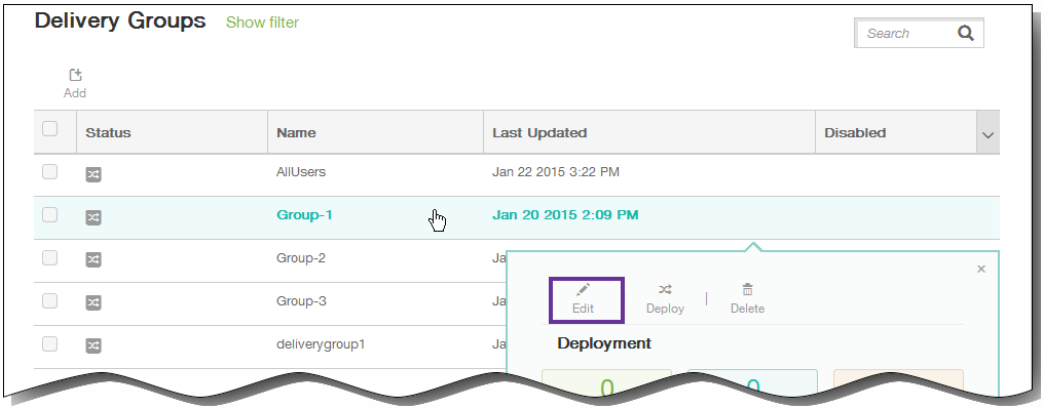
2. Klicken Sie auf eine Ressource und ziehen Sie sie auf die Position, von der aus sie bereitgestellt werden soll. Nachdem Sie die Bereitstellungsreihenfolge geändert haben, stellt XenMobile die Ressourcen in der Liste von oben nach unten bereit.

3. Klicken Sie auf **Speichern**, um die Bereitstellungsreihenfolge zu speichern.

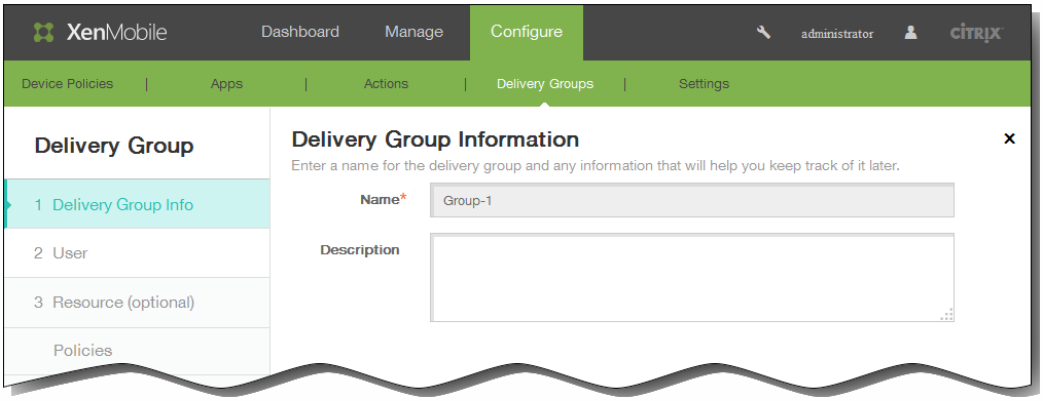
So bearbeiten Sie eine Bereitstellungsgruppe

1. Wählen Sie auf der Seite Delivery Groups die gewünschte Bereitstellungsgruppe aus, indem Sie auf das Kontrollkästchen neben ihrem Namen oder auf die Zeile mit ihrem Namen klicken.
2. Klicken Sie auf Edit.
   Hinweis: Der Befehl Edit wird, je nachdem wie Sie die Bereitstellungsgruppe ausgewählt haben, oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.

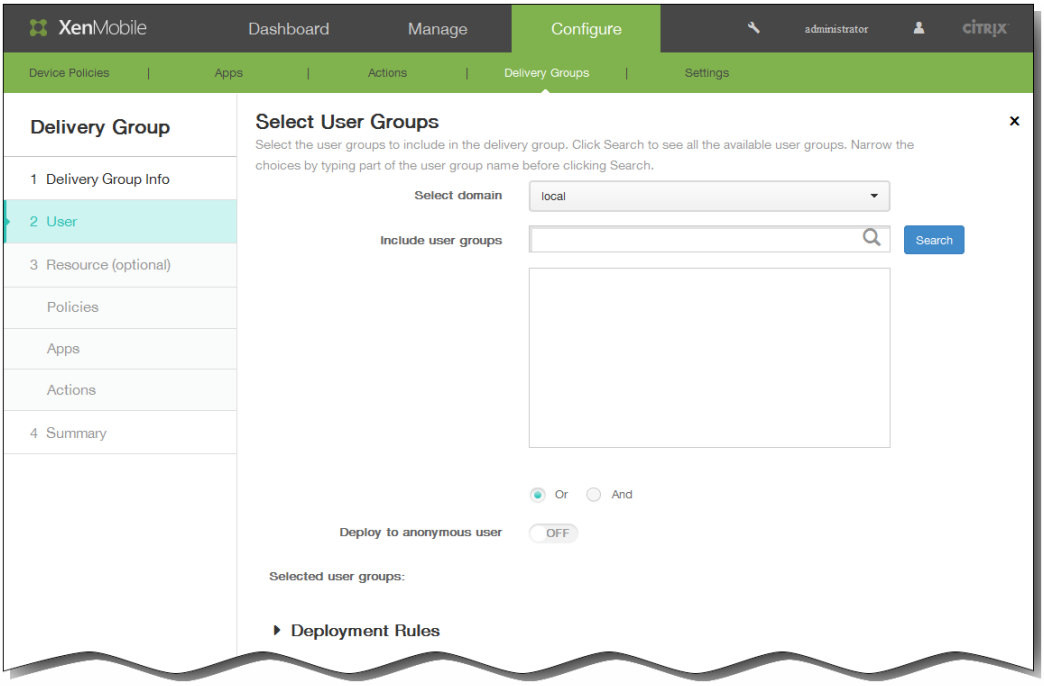




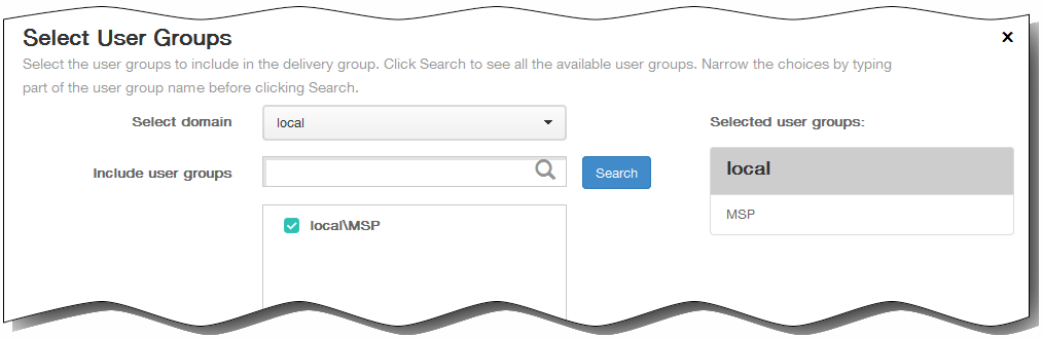
Die Seite Delivery Group Information wird zur Bearbeitung angezeigt.



3. Ändern Sie unter Description die Beschreibung, bzw. fügen Sie eine Beschreibung hinzu.
   Hinweis: Sie können den Namen einer vorhandenen Gruppe nicht ändern.
4. Klicken Sie auf Next. Die Seite Select User Groups wird angezeigt.



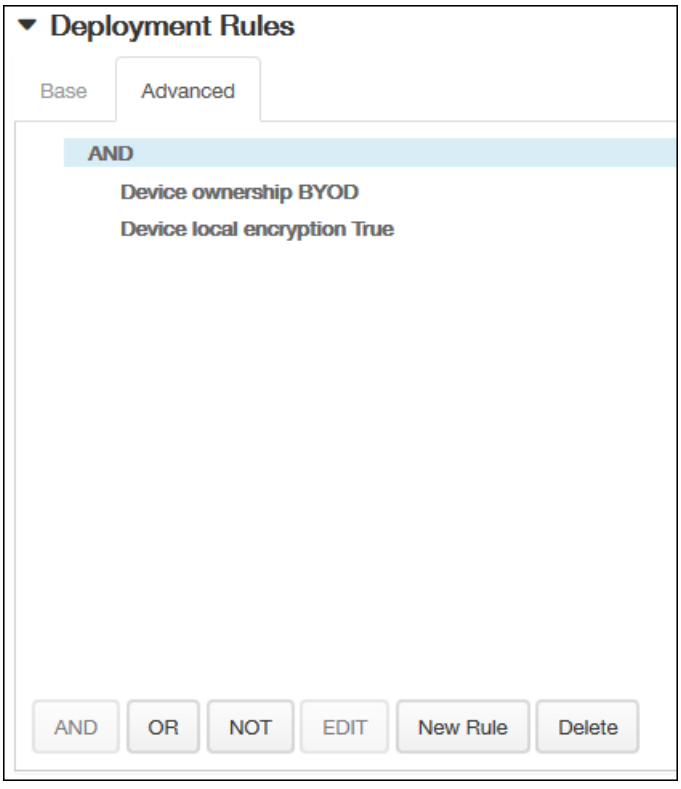
5. Geben Sie im Bereich Select User Groups die folgenden Informationen ein, bzw. ändern Sie sie:
   1. Select domain: Wählen Sie in der Liste die Domäne aus, in der Sie Benutzer auswählen möchten.
   2. Include user groups: Führen Sie einen der folgenden Schritte aus:
      - Klicken Sie auf Search, um eine Liste aller Benutzergruppen in der ausgewählten Domäne anzuzeigen.
      - Geben Sie den Gruppennamen vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf Search, um die Liste der Benutzergruppen einzuschränken.
   3. Klicken Sie in der Liste der Benutzergruppen auf die Gruppen, die Sie hinzufügen möchten. Die ausgewählten Gruppen werden in der Liste Selected user groups angezeigt.



   Hinweis: Zum Entfernen von Benutzergruppen klicken Sie auf Search und deaktivieren Sie in der Liste der Benutzergruppen die Kontrollkästchen der Gruppen, die Sie entfernen möchten. Sie können den Gruppennamen vollständig oder teilweise in das Suchfeld eingeben und auf Search klicken, um die Liste der Benutzergruppen einzuschränken.
   4. Or/And: Wählen Sie aus, ob Benutzer für die Bereitstellung nur einer Gruppe angehören dürfen (Or) oder ob sie allen Gruppen angehören müssen (And).

5. Deploy to anonymous user: Wählen Sie aus, ob die Bereitstellung auch für nicht authentifizierte Benutzer in der Bereitstellungsgruppe erfolgen soll.
   Hinweis: Nicht authentifizierte Benutzer sind Benutzer, bei denen keine Authentifizierung erfolgen konnte, für deren Geräte jedoch dennoch eine Verbindung mit XenMobile gestattet wurde.
6. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

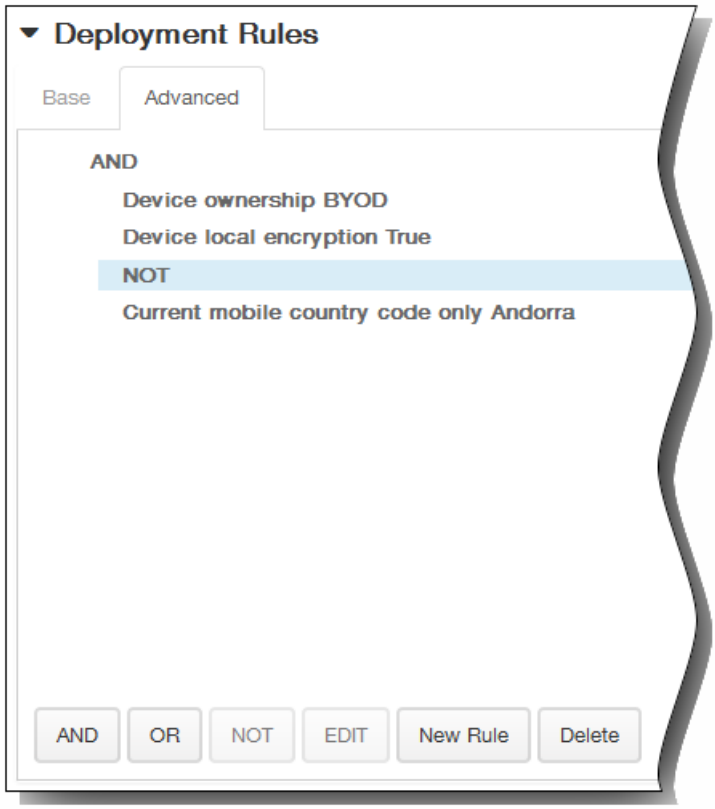
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
   3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
   4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

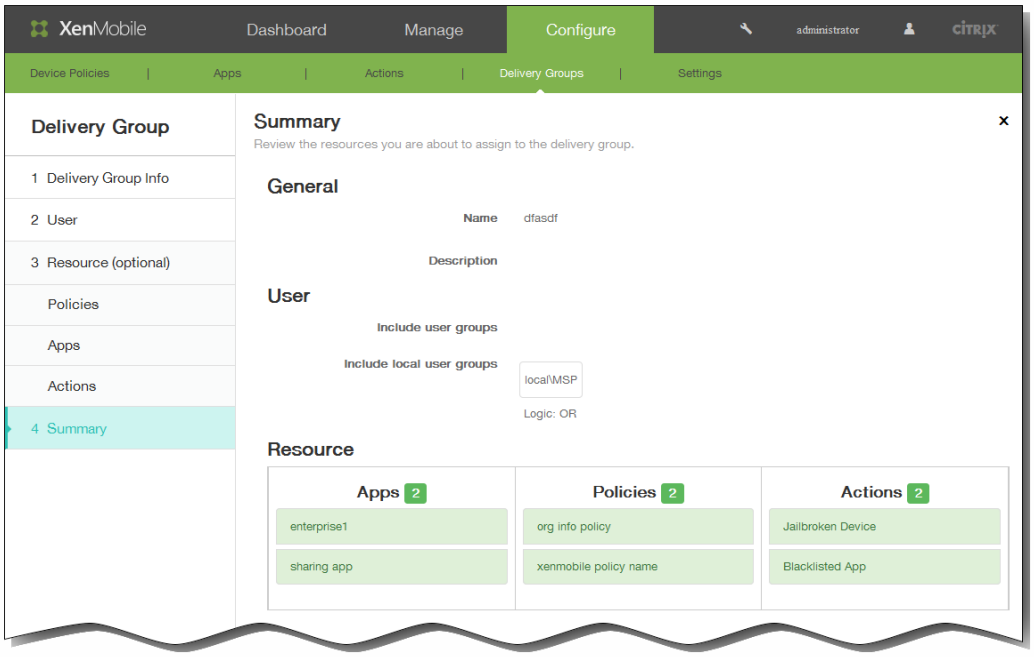
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



7. Klicken Sie auf Next. Die Seite Delivery Group Resources wird angezeigt. Hier können Sie Richtlinien, Apps oder Aktionen hinzufügen oder löschen. Zum Überspringen dieses Schritts klicken Sie unter Delivery Group auf Summary, um eine Zusammenfassung der Bereitstellungsgruppenkonfiguration anzuzeigen.
   Wenn Sie eine Ressource modifiziert haben, klicken Sie auf Next oder unter Delivery Group auf Summary.

   Es wird die nächste Seite für die Ressource bzw. die Seite Summary angezeigt.

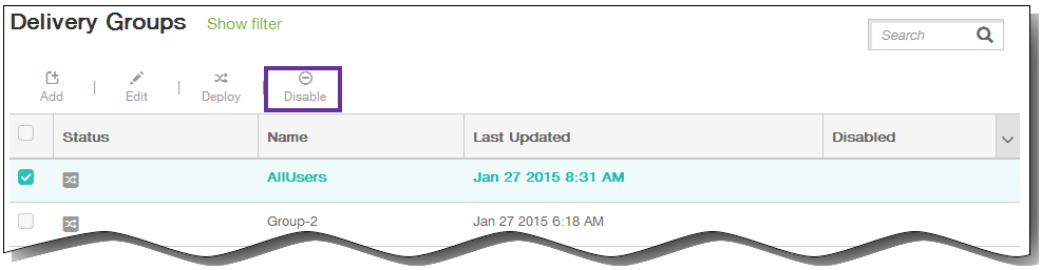


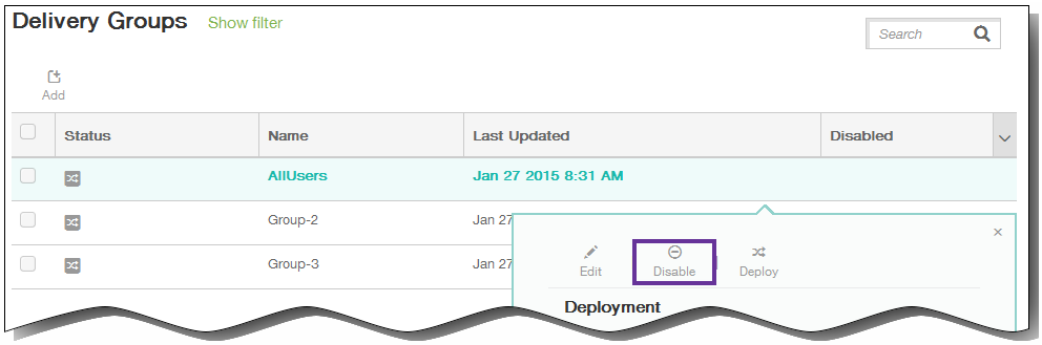
8. Auf der Seite Summary können Sie die Optionen überprüfen, die Sie für die Bereitstellungsgruppe konfiguriert haben, und Sie können die Bereitstellungsreihenfolge der Ressourcen ändern. Klicken Sie auf Back, um auf vorherige Seiten aufzurufen, wenn Sie Änderungen vornehmen müssen. Klicken Sie auf Deployment Order, um die Bereitstellungsreihenfolge der Ressourcen zu ändern. Weitere Informationen zum Ändern der Bereitstellungsreihenfolge finden Sie unter So ändern Sie die Bereitstellungsreihenfolge.
9. Klicken Sie auf Save, um die Änderungen zu speichern.

So aktivieren oder deaktivieren Sie die Bereitstellungsgruppe "AllUsers"

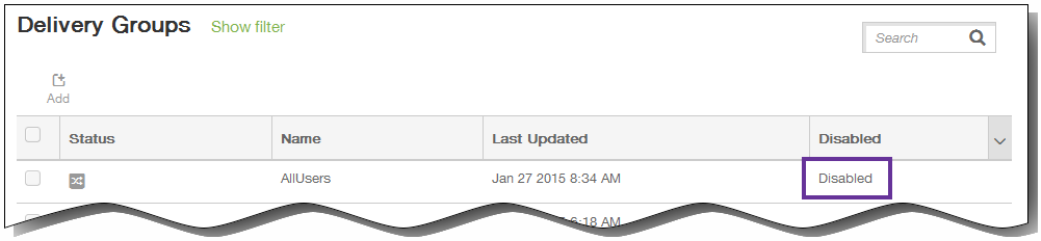
Hinweis: "AllUsers" ist die einzige Bereitstellungsgruppe, die Sie aktivieren oder deaktivieren können.

1. Wählen Sie auf der Seite Delivery Groups die Bereitstellungsgruppe "AllUsers" aus, indem Sie auf das Kontrollkästchen neben AllUsers oder auf die Zeile AllUsers klicken. Führen Sie einen der folgenden Schritte aus:
   Hinweis: Der Befehl Enable bzw. Disable wird, je nachdem wie Sie die Bereitstellungsgruppe AllUsers ausgewählt haben, oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.





- Klicken Sie auf Disable, um die Bereitstellungsgruppe "AllUsers" zu deaktivieren. Dieser Befehl ist nur verfügbar, wenn AllUsers aktiviert ist (= Standardeinstellung).
  Disabled wird unter der gleichnamigen Spaltenüberschrift in der Tabelle angezeigt.



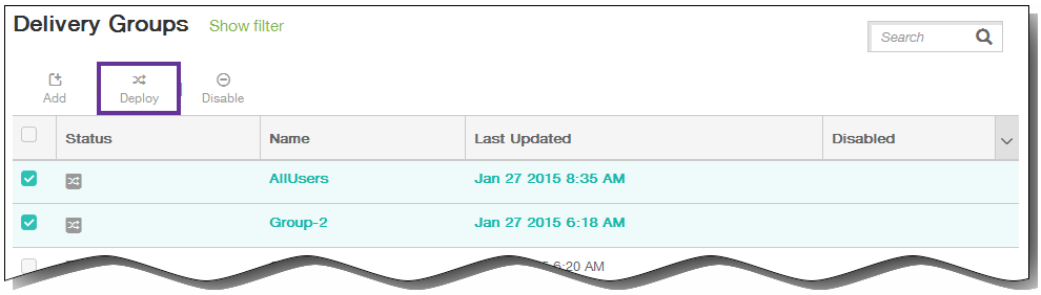
- Klicken Sie auf Enable, um die Bereitstellungsgruppe "AllUsers" zu aktivieren. Dieser Befehl ist nur verfügbar, wenn AllUsers deaktiviert ist.
  Disabled wird unter der gleichnamigen Spaltenüberschrift in der Tabelle ausgeblendet.

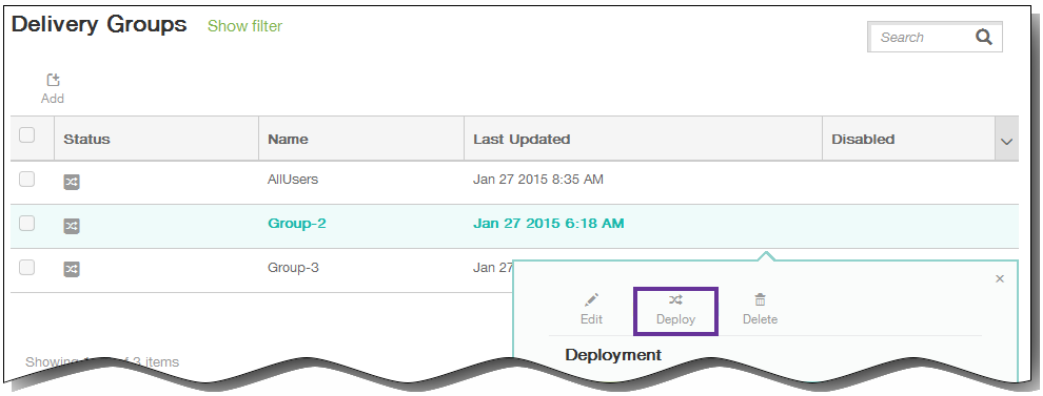
So stellen Sie Bereitstellungsgruppen bereit

Beim Bereitstellen von Ressourcen für eine Bereitstellungsgruppe wird eine Pushbenachrichtigung an alle Benutzer mit iOS- und Windows Phone 8.1-Smartphones und Windows 8.1-Tablets gesendet, eine Verbindung mit XenMobile herzustellen, sodass Sie die Geräte neu auswerten und Apps, Richtlinien und Aktionen bereitstellen können. Benutzer mit Geräten einer anderen Plattform erhalten die Ressourcen sofort, sofern bereits eine Verbindung besteht, oder – basierend auf der für sie eingerichteten Planungsrichtlinie – wenn sie das nächste Mal eine Verbindung herstellen.

Hinweis: Damit aktualisierte Apps in der Liste der verfügbaren Updates im Worx Store auf Android-Geräten angezeigt werden, müssen Sie auf den Geräten eine App-Bestandsrichtlinie bereitstellen.

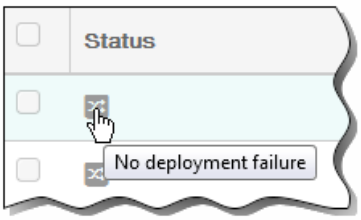
1. Führen Sie auf der Seite Delivery Groups einen der folgenden Schritte aus:
   - Zur Bereitstellung für mehrere Bereitstellungsgruppen aktivieren Sie die Kontrollkästchen neben den gewünschten Gruppen.
   - Zur Bereitstellung für eine einzelne Bereitstellungsgruppe klicken Sie auf das Kontrollkästchen neben ihrem Namen oder auf die Zeile mit ihrem Namen.
2. Klicken Sie auf Deploy.
   Hinweis: Der Befehl Deploy wird, je nachdem wie Sie die einzelne Bereitstellungsgruppe ausgewählt haben, oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.



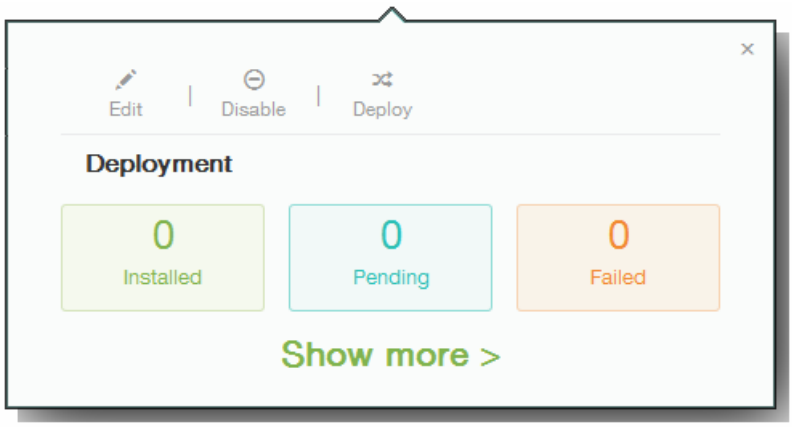


Das Dialogfeld Deploy Devices wird geöffnet.

3. Vergewissern Sie sich, dass die Gruppen, für die Sie Apps, Richtlinien und Aktionen bereitstellen möchten, aufgelistet sind, und klicken Sie dann auf Deploy. Die Bereitstellung von Apps, Richtlinien und Aktionen für die ausgewählten Gruppen erfolgt basierend auf Geräteplattform und Planungsrichtlinie.
   Sie können den Bereitstellungsstatus auf der Seite Delivery Groups mit einer der folgenden Methoden prüfen:
   - Prüfen Sie das Bereitstellungssymbol in der Spalte "Status" für die Bereitstellungsgruppe. Es zeigt eventuelle Bereitstellungsfehler an.



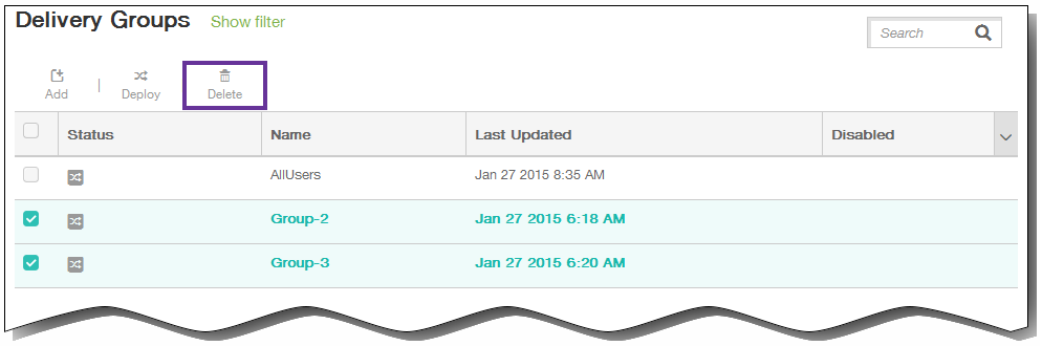
   - Klicken Sie auf der Zeile mit der Bereitstellungsgruppe, um eine Überlagerung einzublenden, in der der Status "Installed", "Pending" oder "Failed" angezeigt wird.

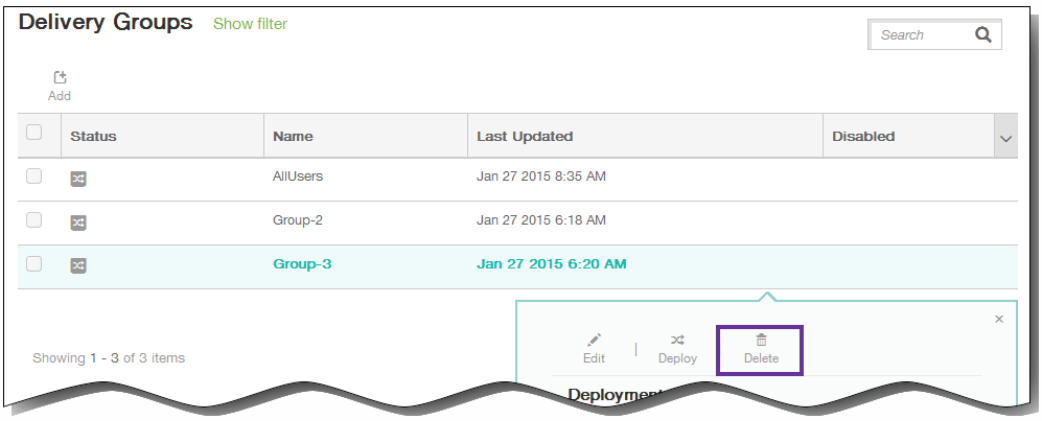


So löschen Sie Bereitstellungsgruppen

Hinweis: Die Bereitstellungsgruppe "AllUsers" kann nicht gelöscht werden, Sie können die Gruppe jedoch deaktivieren, wenn Sie Ressourcen nicht per Push für alle Benutzer bereitstellen möchten.

1. Führen Sie auf der Seite Delivery Groups einen der folgenden Schritte aus:
   - Zum Löschen mehrerer Bereitstellungsgruppen aktivieren Sie die Kontrollkästchen neben den gewünschten Gruppen.
   - Zum Löschen einer einzelnen Bereitstellungsgruppe klicken Sie auf das Kontrollkästchen neben ihrem Namen oder auf die Zeile mit ihrem Namen.
2. Klicken Sie auf Delete.
   Hinweis: Der Befehl Delete wird, je nachdem wie Sie die einzelne Bereitstellungsgruppe ausgewählt haben, oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.





Das Dialogfeld Delete wird angezeigt.

3. Klicken Sie auf Delete.
   Wichtig: Sie können diese Aktion nicht rückgängig machen.

Registrieren von Benutzern und Geräten

Oct 29, 2015

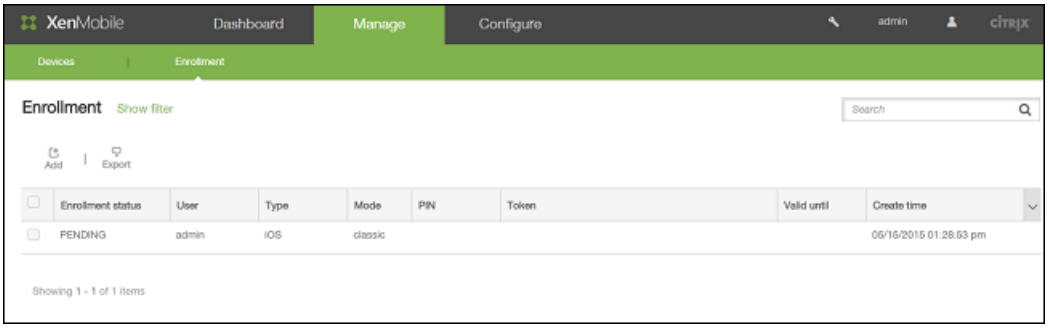
Für die sichere Remote-Verwaltung von Benutzergeräten müssen diese bei XenMobile registriert werden. Die XenMobile-Clientsoftware wird auf dem Benutzergerät installiert, die Identität des Benutzers wird authentifiziert und anschließend werden XenMobile und das Profil des Benutzers installiert. Nachdem die Geräte in der XenMobile-Konsole registriert wurden, können Sie Verwaltungsaufgaben daran ausführen, z. B. Anwenden von Richtlinien, Bereitstellen von Apps, Bereitstellen von Daten auf Geräten per Push, Sperren, Löschen und Suchen von verlorenen oder gestohlenen Geräten.

Zum Registrieren von Benutzern müssen Sie diese zunächst XenMobile hinzufügen, sofern Sie noch keine Active Directory-Verbindung hergestellt haben. In den Themen in diesem Abschnitt werden die anschließend erforderlichen Schritte für die Registrierung von Benutzern erläutert:

- Konfigurieren von Registrierungsmodi (Standard, SHP)
- Konfigurieren von Benachrichtigungsservern (SMTP und SMS)
- Konfigurieren der Benachrichtigungsvorlage für die Registrierung
- Senden der Registrierungsbenachrichtigung

Hinweis: Vor dem Registrieren von iOS-Geräten müssen Sie ein APNS-Zertifikat anfordern. Weitere Informationen finden Sie unter Zertifikate in XenMobile.

Für den Zugriff auf die Konfigurationsoptionen für Benutzer und Geräte klicken Sie in der XenMobile-Konsole auf **Manage > Enrollment**:



Android-Geräte

Nov 12, 2015

1. Rufen Sie auf dem Android-Gerät Google Play oder den Amazon App-Shop auf, laden Sie die Citrix Worx Home-App herunter und tippen Sie dann auf die App.
2. Wenn Sie zum Installieren der App aufgefordert werden, klicken Sie auf Next und dann auf Install.
3. Nach der Installation von Worx Home tippen Sie auf Öffnen.
4. Geben Sie Ihre geschäftlichen Anmeldeinformationen ein, z. B. den Namen des XenMobile-Servers in Ihrem Unternehmen, Ihren Benutzerprinzipalnamen oder Ihre E-Mail-Adresse, und klicken Sie dann auf Weiter.
5. Tippen Sie im Bildschirm Geräteadministrator aktivieren auf Aktivieren.
6. Geben Sie Ihr geschäftliches Kennwort ein und tippen Sie dann auf Anmelden.
7. Je nach XenMobile-Konfiguration müssen Sie möglicherweise eine Worx-PIN zur Anmeldung bei Worx Home und anderen Worx-aktivierten Apps (WorxMail, WorxWeb, ShareFile usw.) einrichten. Sie müssen die Worx-PIN zweimal eingeben. Geben Sie im Bildschirm Worx-PIN erstellen eine PIN aus sechs beliebigen Zahlen ein.
8. Geben Sie die PIN erneut ein. Worx Home wird geöffnet. Sie können nun auf den Worx Store zugreifen und Apps für die Installation auf dem Android-Gerät anzeigen.
9. Wenn Sie XenMobile so konfiguriert haben, dass Apps nach der Registrierung automatisch per Push auf Benutzergeräten bereitgestellt werden, werden Meldungen angezeigt, durch die die Benutzer zur Installation der Apps aufgefordert werden. Tippen Sie auf Installieren, um die Apps zu installieren.

So heben Sie die Registrierung eines Android-Geräts auf und registrieren es erneut

Aktualisiert: 2015-02-12

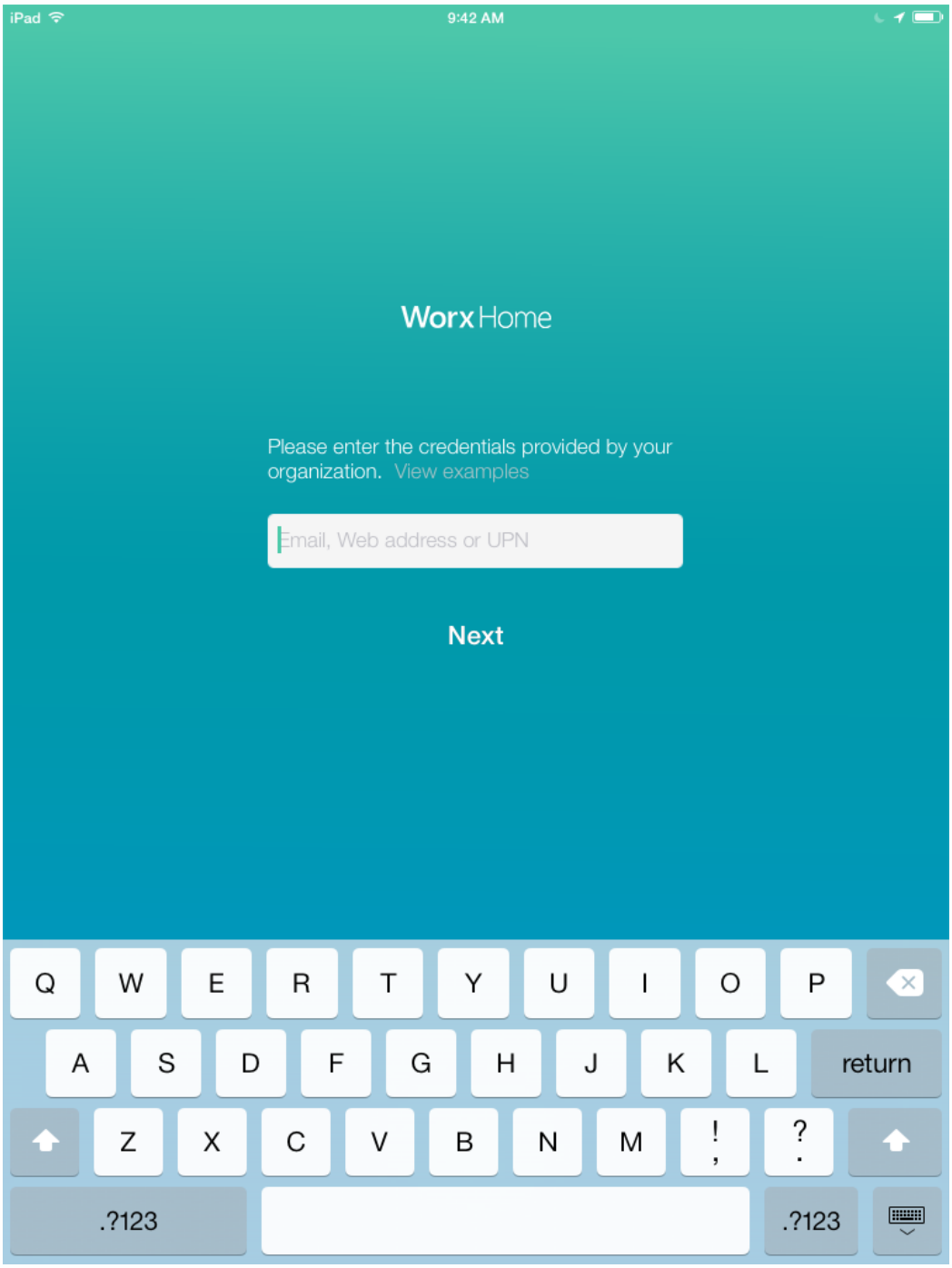
Bevor Sie ein Gerät erneut registrieren können, müssen Sie seine Registrierung aufheben. Nachdem die Registrierung des Geräts aufgehoben wurde und bevor eine erneute Registrierung erfolgt ist, wird das Gerät nicht von XenMobile verwaltet, obwohl es weiterhin in der Gerätebestandsliste angezeigt wird. Sie können Geräte nicht verfolgen und ihre Richtlinientreue nicht überwachen, wenn diese nicht von XenMobile verwaltet werden.

1. Tippen Sie auf die Worx Home-App.
2. Tippen Sie auf das Einstellungssymbol oben links im App-Fenster.
3. Tippen Sie auf Re-Enroll. Eine Meldung wird zur Bestätigung, dass Sie das Gerät erneut registrieren möchten, angezeigt.
4. Tippen Sie auf OK. Die Registrierung des Geräts wird aufgehoben.
5. Folgen Sie dann den Anweisungen auf dem Bildschirm, um das Gerät erneut zu registrieren.

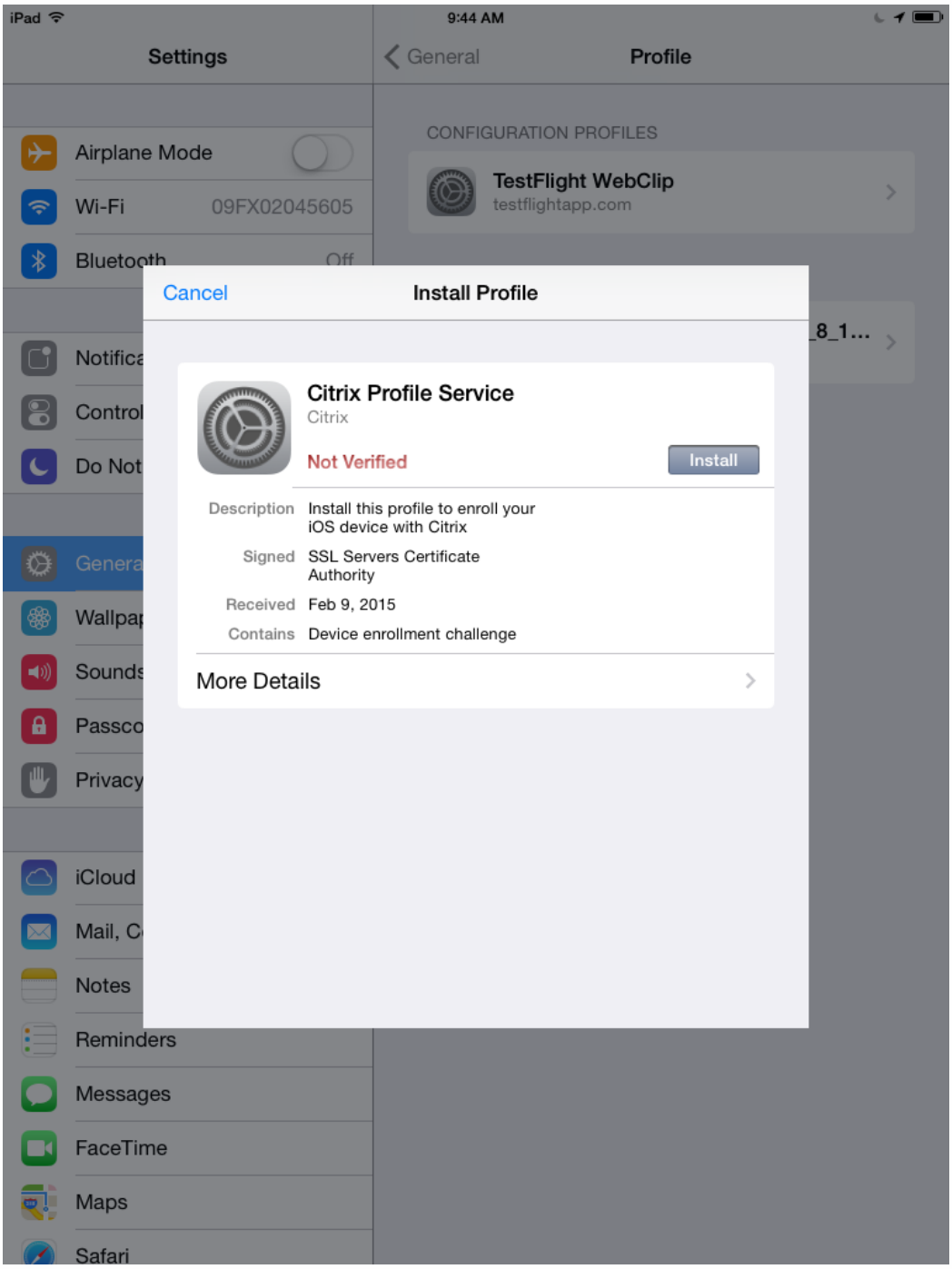
iOS-Geräte

Nov 12, 2015

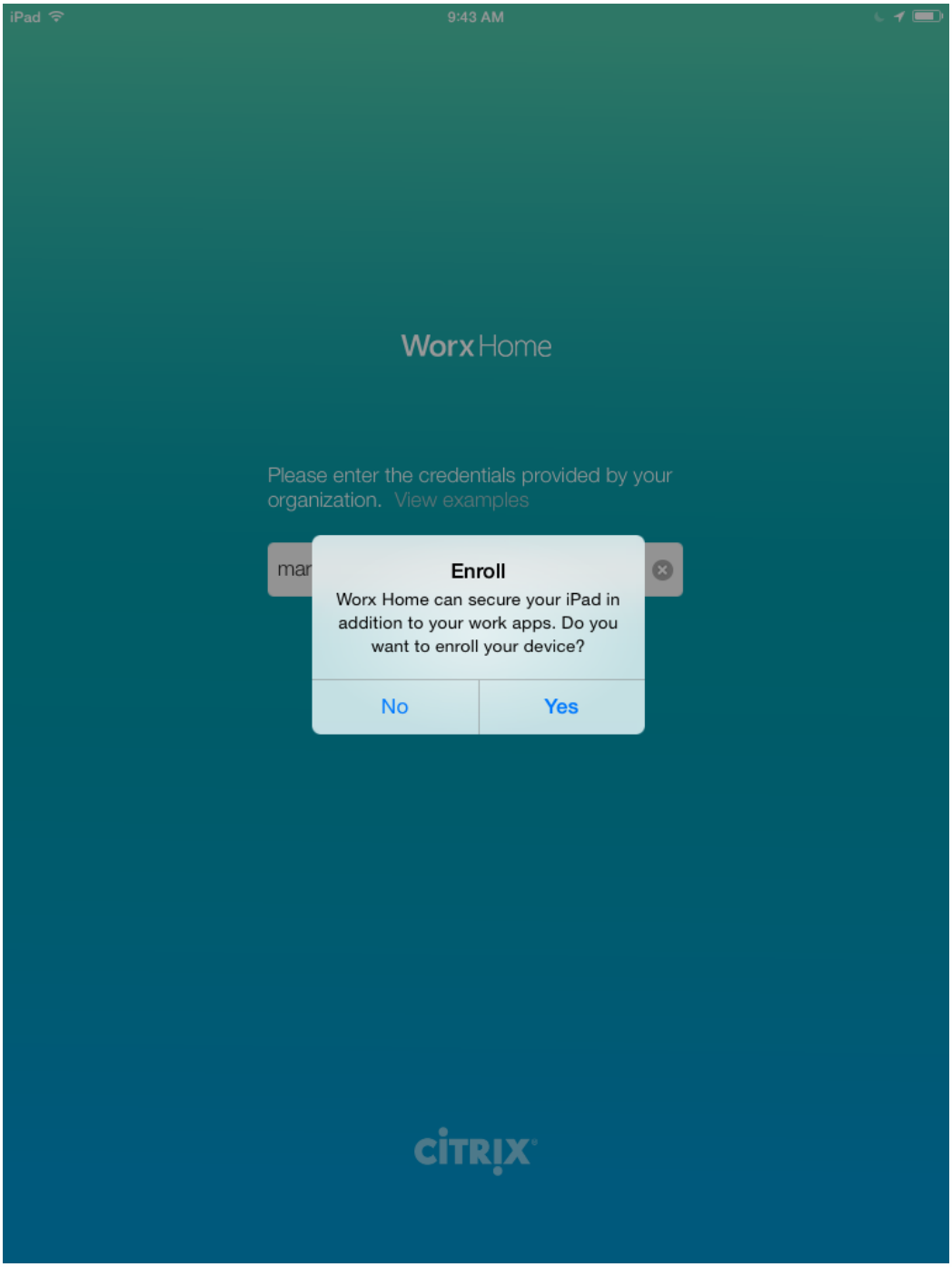
1. Laden Sie die Worx Home-App aus dem Apple iTunes-App Store auf das Gerät herunter und installieren Sie sie auf dem Gerät.
2. Tippen Sie auf dem Homebildschirm des iOS-Geräts auf die Worx Home-App.
3. Wenn die Worx Home-App sich öffnet, geben Sie Ihre geschäftlichen Anmeldeinformationen ein, z. B. den Namen des XenMobile-Servers in Ihrem Unternehmen, Ihren Benutzerprinzipalnamen oder Ihre E-Mail-Adresse, und tippen Sie dann auf Weiter.



4. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Ein Browser wird für die Registrierung geöffnet.
5. Tippen Sie auf Installieren, um den Citrix Profildienst zu installieren.



6. Tippen Sie auf Jetzt installieren, wenn eine Warnmeldung angezeigt wird.
7. Wenn das Gerät mit einem Passcode konfiguriert ist, werden Sie zu dessen Eingabe aufgefordert, um das Profil zu installieren.
8. Tippen Sie auf Installieren.
9. Wenn die Profilinstallation abgeschlossen ist, tippen Sie auf Fertig, um den Vorgang abzuschließen.
10. Wenn Worx Home angezeigt wird, tippen Sie auf Ja, damit Worx Home den aktuellen Standort verwenden kann.



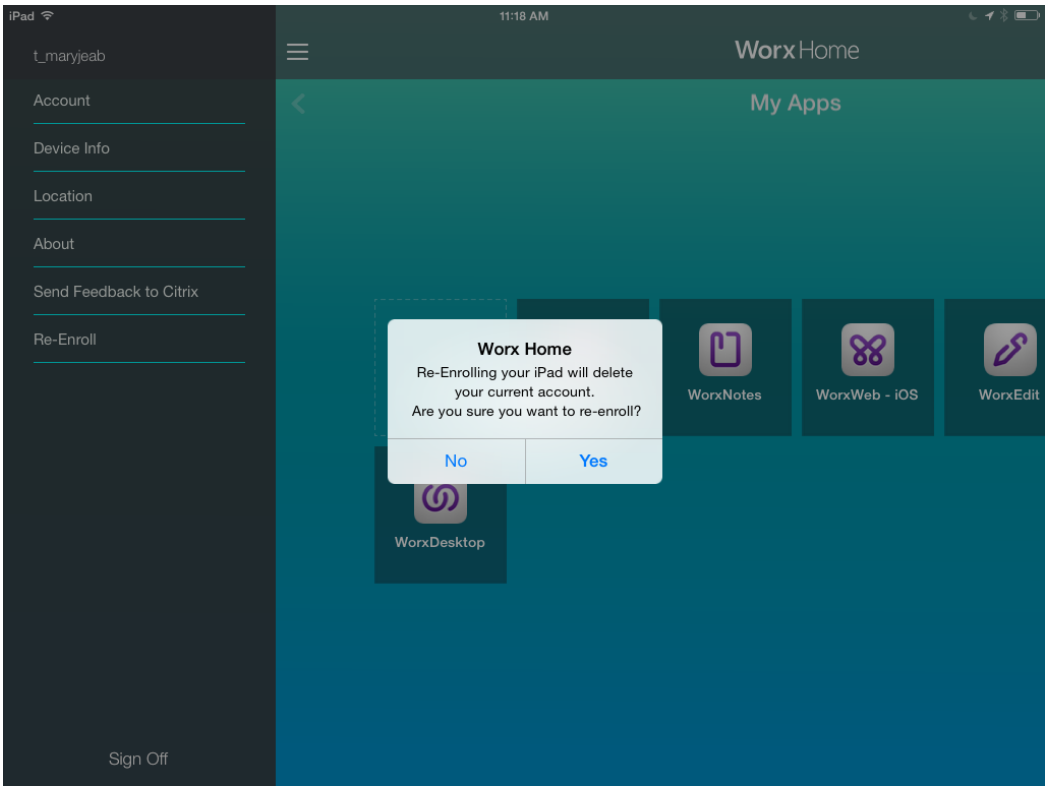
11. Je nach XenMobile-Konfiguration müssen Sie möglicherweise eine Worx-PIN zur Anmeldung bei Worx Home und anderen Worx-aktivierten Apps (WorxMail, WorxWeb, ShareFile usw.) einrichten. Sie müssen die Worx-PIN zweimal eingeben. Worx Home wird geöffnet. Sie können nun auf den Worx Store zugreifen und Apps für die Installation auf dem iOS-Gerät anzeigen.
12. Tippen Sie auf Worx Store, um den firmeninternen App-Store zu öffnen.
13. Wenn Sie XenMobile so konfiguriert haben, dass Apps nach der Registrierung automatisch per Push auf Benutzergeräten bereitgestellt werden, werden Meldungen angezeigt, durch die die Benutzer zur Installation der Apps aufgefordert werden. Tippen Sie auf Installieren, um die Apps zu installieren.

So registrieren Sie ein iOS-Gerät erneut

Aktualisiert: 2015-02-13

Zum erneuten Registrieren eines Geräts müssen Sie seine Registrierung zunächst aufheben. Nachdem die Registrierung des Geräts aufgehoben wurde und bevor eine erneute Registrierung erfolgt ist, wird das Gerät nicht von XenMobile verwaltet, obwohl es weiterhin in der Gerätebestandsliste angezeigt wird. Sie können Geräte nicht verfolgen und ihre Richtlinientreue nicht überwachen, wenn diese nicht von XenMobile verwaltet werden.

1. Tippen Sie auf die Worx Home-App.
2. Tippen Sie auf das Einstellung oben links im App-Fenster.
3. Tippen Sie auf Neu registrieren. Eine Meldung wird zur Bestätigung, dass Sie das Gerät erneut registrieren möchten, angezeigt.



4. Tippen Sie auf Ja. Die Registrierung des Geräts wird aufgehoben.
5. Folgen Sie dann den Anweisungen auf dem Bildschirm, um das Gerät erneut zu registrieren.

Windows-Geräte

Apr 12, 2016

XenMobile unterstützt die Registrierung von Geräten mit folgenden Windows-Betriebssystemen:

- Windows
- Windows Phone

Benutzer von Windows- und Windows Phone-Geräten registrieren diese direkt über das Gerät.

Sie müssen Autodiscovery für die Registrierung aktivieren, um die Verwaltung von Windows- und Windows Phone-Geräten zu ermöglichen.

> **Hinweis**
>
> Das SSL-Listenerzertifikat muss ein öffentliches Zertifikat sein, damit Windows-Geräte sich registrieren können. Bei einem selbstsignierten SSL-Zertifikat schlägt die Registrierung fehl.

So registrieren Sie Windows 8.1-Geräte mit Autodiscovery

Benutzer können Geräte mit Windows RT 8.1 und mit der 32-Bit- und der 64-Bit-Version von Windows 8.1 Pro oder Windows 8.1 Enterprise registrieren. Um die Verwaltung von Windows 8.1-Geräten zu ermöglichen, empfiehlt Citrix das Konfigurieren von Autodiscovery. Weitere Informationen finden Sie unter So aktivieren Sie in XenMobile Autodiscovery für die Benutzerregistrierung.

1. Prüfen Sie auf dem Gerät auf Updates und installieren Sie alle verfügbaren Windows-Updates. Dieser Schritt ist besonders wichtig beim Upgrade von Windows 8 auf Windows 8.1, da die Benutzer möglicherweise nicht automatisch über alle verfügbaren Updates benachrichtigt werden.
2. Tippen Sie im Charms-Menü auf Einstellungen und dann auf PC-Einstellungen > Netzwerk > Unternehmensbereich.
3. Geben Sie Ihre geschäftliche E-Mail-Adresse ein und tippen Sie dann auf Einschalten. Zur Registrierung als lokaler Benutzer geben Sie eine nicht vorhandene E-Mail-Adresse mit dem richtigen Domänennamen (z. B. foo@mydomain.com) ein. Dies ermöglicht die Umgehung einer bekannten Microsoft-Einschränkung. Geben Sie im Dialogfeld Mit einem Dienst verbinden den Benutzernamen und das Kennwort des lokalen Benutzers ein. Das Gerät sucht automatisch einen XenMobile-Server und startet die Registrierung.
4. Geben Sie Ihr Kennwort ein. Verwenden Sie das Kennwort eines Kontos, das zu einer Benutzergruppe in XenMobile gehört.
5. Geben Sie im Dialogfeld Apps und Dienste des IT-Administrators zulassen an, dass Sie der Verwaltung Ihres Geräts zustimmen, und tippen Sie auf Einschalten.

So registrieren Sie Windows 8.1-Geräte ohne Autodiscovery

Windows 8.1-Geräte können ohne Autodiscovery registriert werden. Citrix empfiehlt jedoch die Verwendung von Autodiscovery. Da bei einer Registrierung ohne Autodiscovery ein Aufruf an Port 80 erfolgt, bevor eine Verbindung mit der gewünschten URL hergestellt wird, ist sie kein optimales Verfahren bei einer Produktionsbereitstellung. Citrix empfiehlt die Verwendung dieses Verfahrens nur in Bereitstellungen für Testzwecke und Machbarkeitsstudien.

1. Prüfen Sie auf dem Gerät auf Updates und installieren Sie alle verfügbaren Windows-Updates. Dieser Schritt ist

besonders wichtig beim Upgrade von Windows 8 auf Windows 8.1, da die Benutzer möglicherweise nicht automatisch über alle verfügbaren Updates benachrichtigt werden.
2. Tippen Sie im Charms-Menü auf Einstellungen und dann auf PC-Einstellungen > Netzwerk > Unternehmensbereich.
3. Geben Sie Ihre geschäftliche E-Mail-Adresse ein.
4. Wenn die Option Automatisch erkennen für die Serveradresse aktiviert ist, tippen Sie darauf, um sie zu deaktivieren.
5. Geben Sie im Feld Enter server die Serveradresse in folgendem Format ein: https://*serverfqdn:8443/serverInstance*/Discovery.svc. Wenn für SSL-Verbindungen ohne Authentifizierung eine andere Portnummer als 8443 verwendet wird, geben Sie die verwendete Portnummer mit der Adresse ein.
6. Geben Sie Ihr Kennwort ein.
7. Geben Sie im Dialogfeld Apps und Dienste des IT-Administrators zulassen an, dass Sie der Verwaltung Ihres Geräts zustimmen, und tippen Sie auf Einschalten.

So registrieren Sie Windows Phone 8.1-Geräte

Für die Registrierung von Windows Phone 8.1-Geräten in XenMobile benötigen die Benutzer ihre Active Directory- oder netzwerkinterne E-Mail-Adresse und ihr Kennwort. Ist Autodiscovery nicht eingerichtet, benötigen die Benutzer zudem die Serverwebadresse des XenMobile-Servers. Sie folgen dann den nachfolgenden Anweisungen zur Registrierung ihres Geräts.

Hinweis: Wenn Sie Apps über den Windows Phone-Unternehmens-Store vor der Registrierung der Benutzer bereitstellen möchten, müssen Sie vorher eine Enterprise Hub-Richtlinie erstellen (mit einer signierten Windows Phone 8.x-App für Citrix Worx Home).

1. Tippen Sie auf der Hauptseite des Windows Phone 8.1-Geräts auf das Symbol Einstellungen.
2. Tippen Sie auf Arbeitsplatz.
3. Tippen Sie auf dem Bildschirm Arbeitsplatz auf Konto hinzufügen.
4. Geben Sie im nächsten Bildschirm eine E-Mail-Adresse und ein Kennwort ein und tippen Sie dann auf Anmelden. Wenn Autodiscovery für die Domäne konfiguriert ist, werden die in den nächsten Schritten angeforderten Informationen automatisch eingetragen. Gehen Sie zu Schritt 8. Wenn Autodiscovery für die Domäne nicht konfiguriert ist, fahren Sie mit dem nächsten Schritt fort. Zur Registrierung als lokaler Benutzer geben Sie eine nicht vorhandene E-Mail-Adresse mit dem richtigen Domänennamen (z. B. foo@mydomain.com) ein. Dies ermöglicht die Umgehung einer bekannten Microsoft-Einschränkung. Geben Sie im Dialogfeld Mit einem Dienst verbinden den Benutzernamen und das Kennwort des lokalen Benutzers ein.
5. Geben Sie im nächsten Bildschirm die Webadresse des XenMobile-Servers ein. Beispiel: https://://wpe. Beispiel: https://mycompany.mdm.com:8443/zdm/wpe. **Hinweis**: Die Portnummer muss gemäß der vorliegenden Implementierung angepasst werden, es muss jedoch derselbe Port sein, der für eine iOS-Registrierung verwendet wird.
6. Geben Sie den Benutzernamen und die Domäne ein, sofern die Authentifizierung über einen Benutzernamen und eine Domäne erfolgt und tippen Sie auf Anmelden.
7. Wenn ein Problem mit dem Zertifikat gemeldet wird, ist dieser Fehler auf die Verwendung eines selbstsignierten Zertifikats zurückzuführen. Wird der Server als vertrauenswürdig eingestuft, tippen Sie auf Fortfahren. Andernfalls tippen Sie auf Abbrechen.
8. Wenn das Konto hinzugefügt wurde, wird die Option Unternehmens-App installieren angeboten. Wenn der Administrator einen Unternehmens-App-Store konfiguriert hat, wählen Sie diese Option aus und tippen Sie dann auf Fertig. Wenn Sie diese Option deaktivieren, müssen Sie sich erneut registrieren, um den Unternehmens-App-Store zu erhalten.
9. Tippen Sie im Bildschirm Konto hinzugefügt auf Fertig.
10. Zum Erzwingen einer Verbindung mit dem Server tippen Sie auf das Symbol zum Aktualisieren. Wenn das Gerät nicht manuell eine Verbindung mit Server herstellt, versucht XenMobile, die Verbindung wiederherzustellen. XenMobile versucht 5 Mal alle 3 Minuten eine Verbindung herzustellen, anschließend alle 2 Stunden. Sie können diese Verbindungsrate unter Server properties über die Option Windows WNS Heartbeat Interval ändern. Nach Abschluss der Registrierung wird Worx Home im Hintergrund registriert. Der Abschluss der Installation wird nicht angezeigt. Öffnen Sie Worx Home über den

Bildschirm Alle Apps.

Symbian-Geräte

Nov 12, 2015

1. Navigieren Sie zu der XenMobile-Webadresse für Ihr Unternehmen. Die Webadresse hat folgendes Format: https://.domain.com//setup
   Hinweis: Sie können das Präfix "HTTPS" nur verwenden, wenn Sie ein von einer vertrauenswürdigen Zertifizierungsstelle wie VeriSign oder Thawte herausgegebenes Zertifikat haben.
2. Tippen Sie im Bildschirm Installieren auf OK.
3. Tippen Sie auf Phone Memory als Speicherort für die Installation des XenMobile-Agents.
4. Wenn die Installation abgeschlossen ist, tippen Sie auf Ja, um XenMobile zu öffnen.
5. Klicken Sie auf dem Bildschirm Sicherheitsdetails auf OK, um XenMobile den Zugriff auf das Telefon zu ermöglichen.
6. Geben Sie als erste vier Zahlen des Servercodes 2831 ein und tippen Sie dann auf OK.
7. Klicken Sie im Bildschirm Steuerungsanforderung akzeptiert auf OK.
8. Geben Sie Benutzernamen, Kennwort, Servernamen, Port und Instanznamen für den XenMobile-Server ein und tippen Sie dann auf OK. Die Verbindungsinformationen werden angezeigt.
9. Tippen Sie auf Optionen, um die Server-Verbindungsinformationen zu prüfen und dann auf Schließen, um die Einrichtung zu beenden.

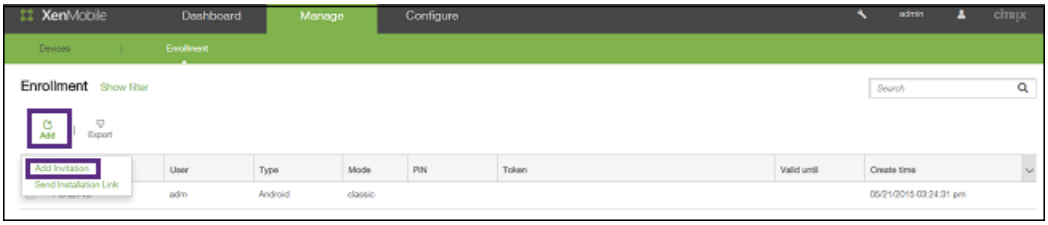
Senden einer Registrierungseinladung in XenMobile

Apr 12, 2016

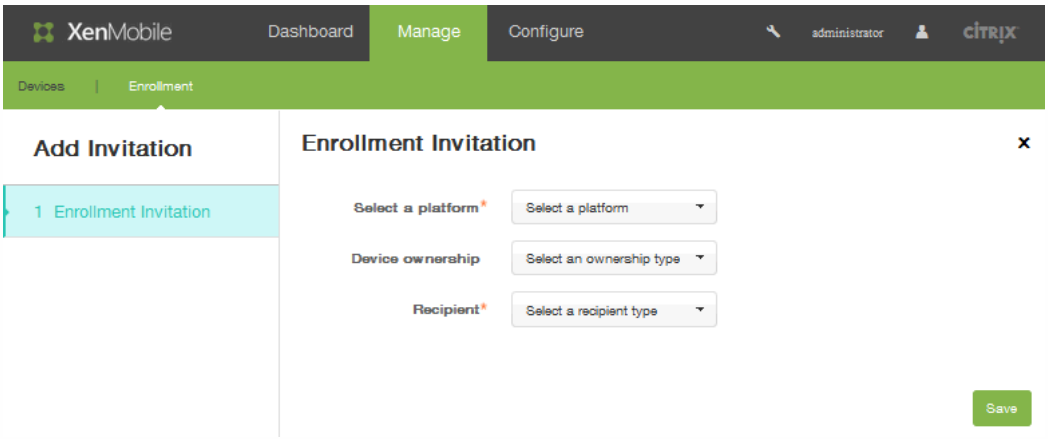
In der XenMobile-Konsole können Sie Registrierungseinladungen an Benutzer mit iOS-, Android- und Windows-Geräten senden.

1. Klicken Sie in der XenMobile-Konsole auf Manage > Enrollment.

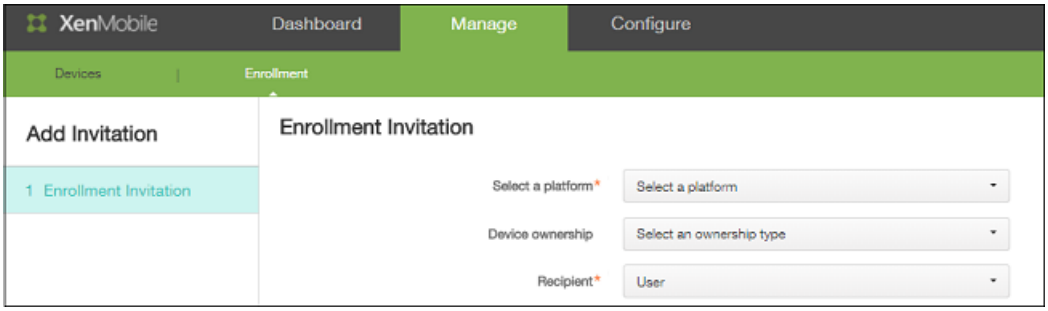
2. Klicken Sie auf der Seite Enrollment auf Add. Ein Menü wird eingeblendet, das Optionen zum Hinzufügen einer Einladung und zum Senden eines Installationslinks enthält.
3. Klicken Sie auf Add Invitation.



Die Seite Enrollment Invitation wird angezeigt.



4. Klicken Sie in der Liste Select a platform auf iOS oder Android.
5. Klicken Sie in der Liste Device ownership auf Corporate oder Employee.
6. Klicken Sie in der Liste Recipient auf User oder Group.



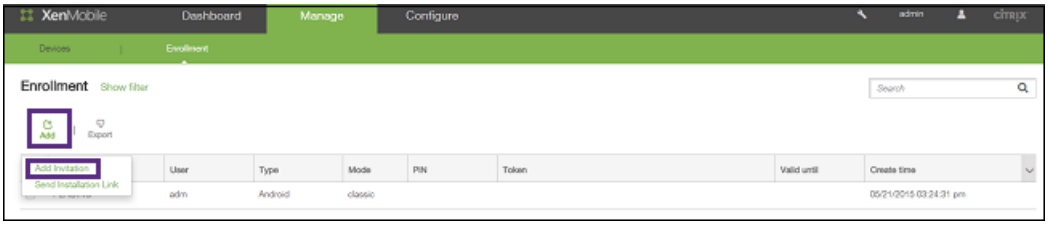
Wenn Sie einen Benutzer als Empfänger auswählen, werden zusätzliche Konfigurationsoptionen angezeigt. Folgen Sie den Schritten im entsprechenden Abschnitt zum Festlegen der Einladungseinstellungen nach Empfängertyp.

So senden Sie eine Registrierungseinladung an einen Benutzer

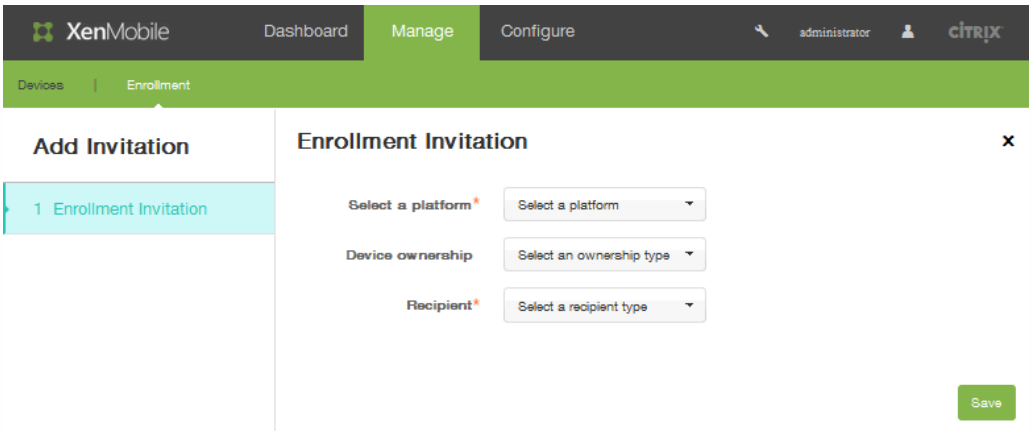
1. Klicken Sie in der XenMobile-Konsole auf Manage > Enrollment.

2. Klicken Sie auf der Seite Enrollment auf Add. Ein Menü wird eingeblendet, in dem Sie die Option zum Hinzufügen einer Einladung oder zum Senden eines Installationslinks auswählen können.

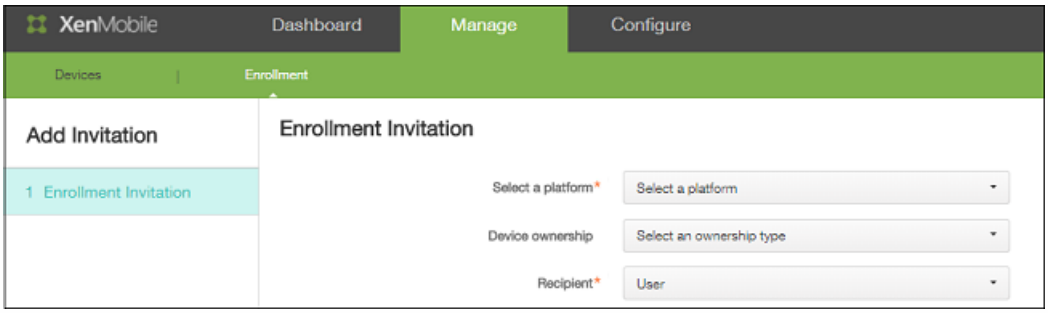
3. Klicken Sie auf Add Invitation.



Die Seite Enrollment Invitation wird angezeigt.

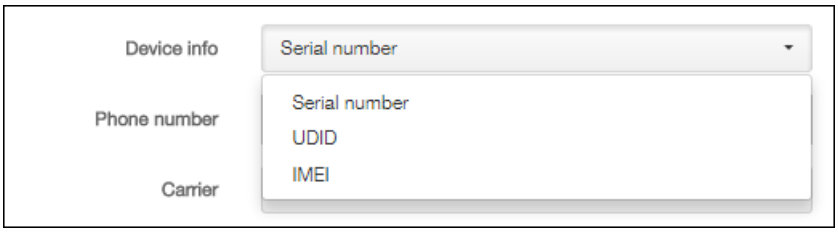


4. Klicken Sie in der Liste Select a platform auf iOS oder Android.
5. Klicken Sie in der Liste Device ownership auf Corporate oder Employee.
6. Klicken Sie in der Liste Recipient auf User.



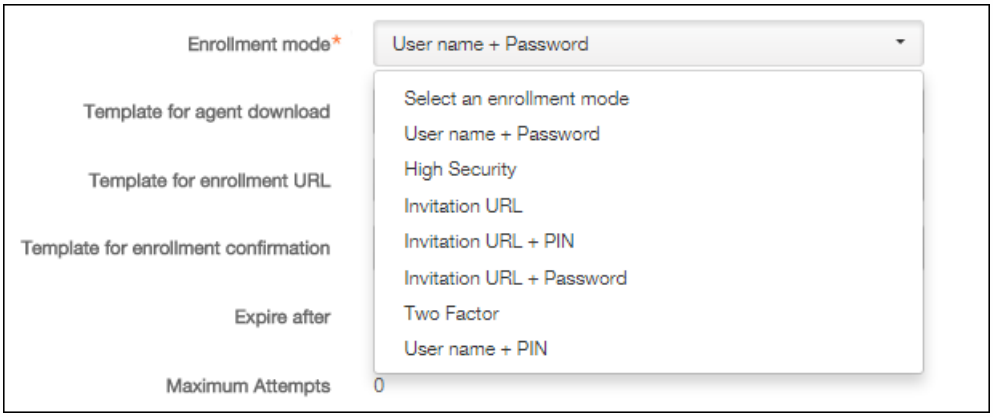
Zusätzliche Konfigurationsoptionen werden für die Benutzerregistrierung angezeigt.

7. Geben Sie in das Feld Username einen Benutzernamen ein.
   Hinweis: Der Benutzer muss als lokaler Benutzer auf dem XenMobile-Server oder als Active Directory-Benutzer vorliegen. Stellen Sie bei lokalen Benutzern sicher, dass deren E-Mail Eigenschaft eingestellt ist, damit Benachrichtigungen gesendet werden können. Bei Active Directory-Benutzern muss LDAP konfiguriert sein.
8. Klicken Sie in der Liste Device info auf Serial number, UDID oder IMEI.

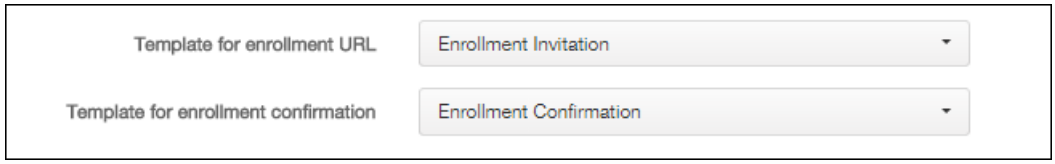


Wenn Sie eine Option auswählen, wird ein Feld angezeigt, in das Sie den entsprechenden Wert für das Gerät eingeben können.

9. Geben Sie für Phone number optional eine Telefonnummer für den Benutzer ein.
10. Wählen Sie in der Liste Carrier den Netzbetreiber aus, der der Telefonnummer zugeordnet werden soll.
11. Wählen Sie in der Liste Enrollment mode die Option User name + Password (the default), High Security, Invitation URL, Invitation URL + PIN, Invitation URL + Password, Two Factor oder User name + PIN aus.

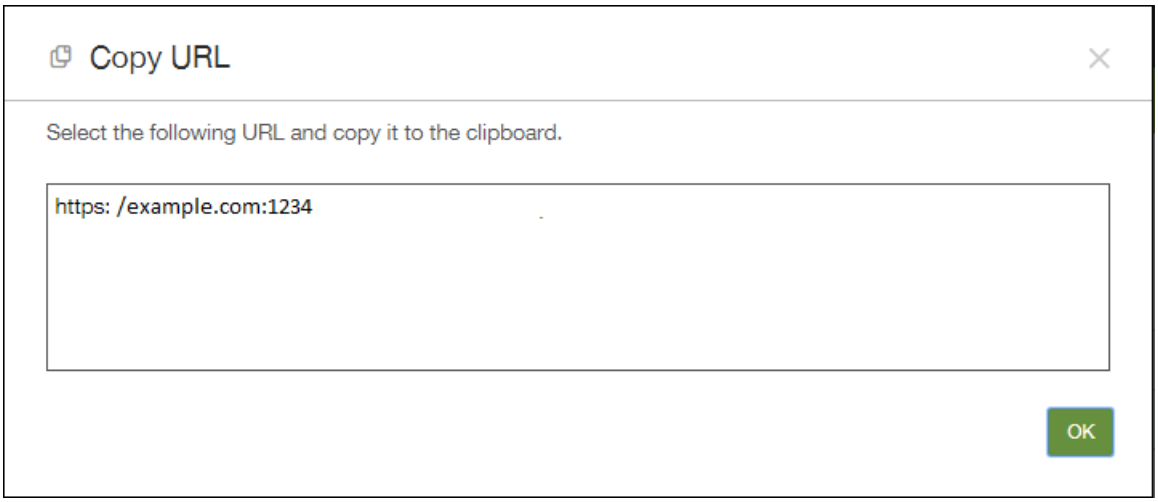


12. Die Optionen in der Liste Template for agent download hängen vom Plattformtyp ab. Beispielsweise wird iOS Download Link angezeigt, wenn Sie in Schritt 1 als Plattform iOS ausgewählt haben.



13. Klicken Sie in der Liste Template for enrollment URL auf Enrollment Invitation.
14. Klicken Sie in der Liste Template for enrollment confirmation auf Enrollment Confirmation. Die Registrierungseinladung läuft nach einem bestimmten Zeitraum ab. Dieser Zeitraum wird im Feld Expire after angezeigt. Im Feld Maximum Attempts wird die Höchstanzahl der Registrierungsversuche angezeigt.
15. Führen Sie in Send invitation eine der folgenden Aktionen durch:
    - Klicken Sie auf ON und klicken Sie dann auf Save & Send.
    - Lassen Sie die Option als Off und klicken Sie auf Save.
16. Die Einladung, die Sie hinzugefügt haben, wird in der Tabelle auf der Seite für die Registrierung angezeigt. Wenn Sie jetzt auf eine Einladung klicken und sie auswählen, werden zahlreiche neue Optionen über der Tabelle angezeigt: Notify, Copy URL und Delete.

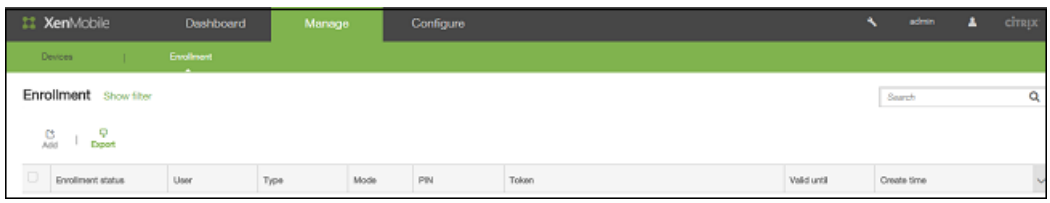
1. Klicken Sie auf Notify, um eine ausstehende Einladung zu senden.
2. Klicken Sie auf Copy URL, um die Einladungs-URL zu kopieren, falls Sie die Einladung per E-Mail senden möchten. Wenn die Benachrichtigung angezeigt wird, wählen Sie die URL aus, kopieren Sie sie und klicken Sie dann auf OK.



3. Klicken Sie auf Delete, um die Einladung zu löschen.

So senden Sie eine Registrierungseinladung an eine Gruppe

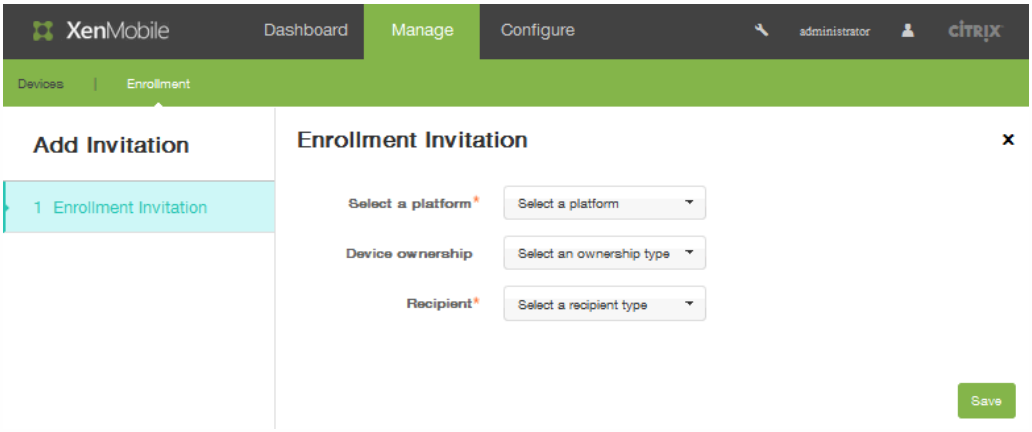
1. Klicken Sie in der XenMobile-Konsole auf Manage > Enrollment.



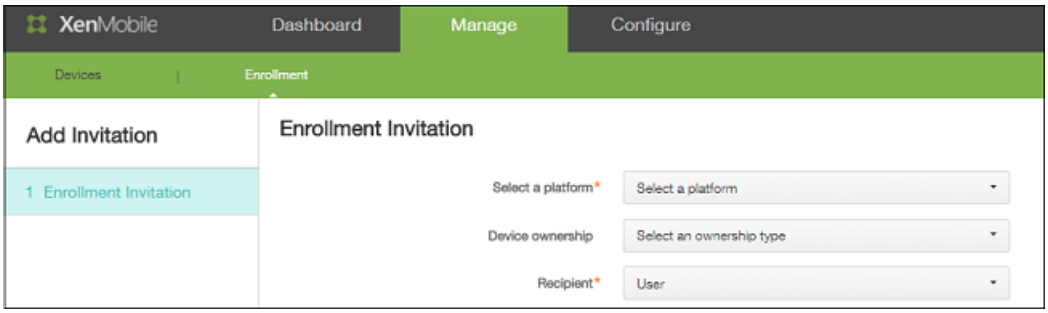
2. Klicken Sie auf der Seite Enrollment auf Add. Ein Menü wird eingeblendet, in dem Sie die Option zum Hinzufügen einer Einladung oder zum Senden eines Installationslinks auswählen können.

3. Klicken Sie auf Add Invitation.

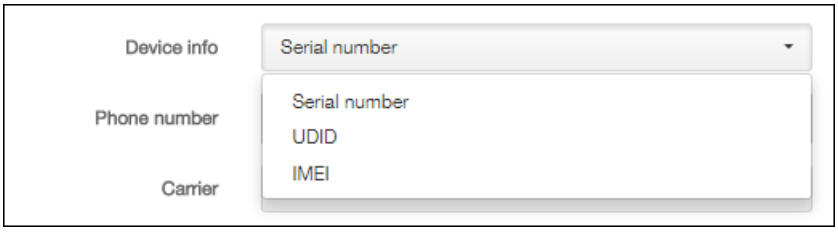
Die Seite Enrollment Invitation wird angezeigt.



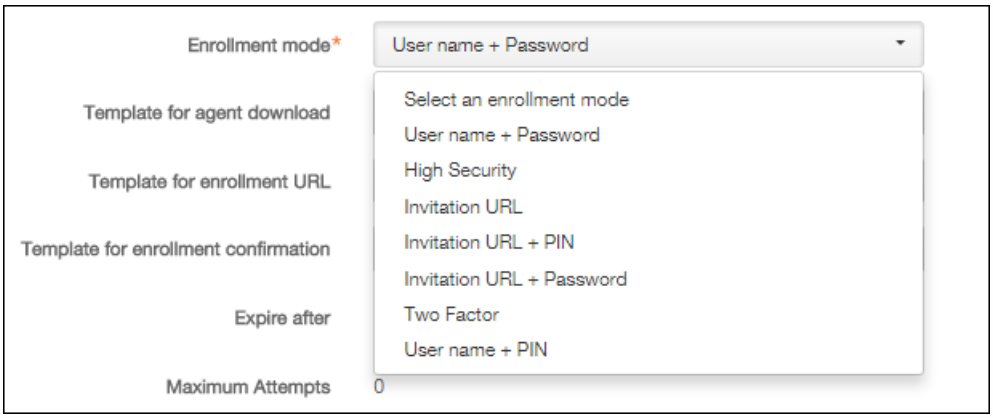
4. Wählen Sie in der Liste Select a platform die Option iOS oder Android aus.
5. Wählen Sie in der Liste Device ownership die Option Corporate oder Employee aus.
6. Wählen Sie in der Liste Recipient die Option Group aus. Konfigurationsoptionen für die Gruppenregistrierung werden angezeigt.



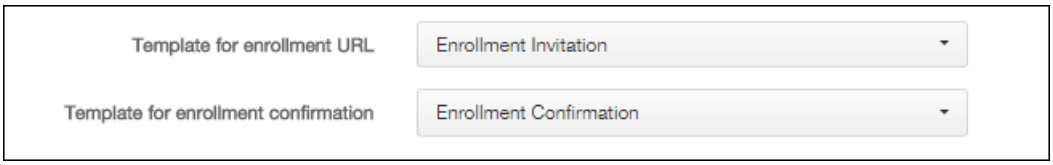
7. Geben Sie in das Feld Username einen Benutzernamen ein.
   Hinweis: Der Benutzer muss als lokaler Benutzer auf dem XenMobile-Server oder als Active Directory-Benutzer vorliegen. Stellen Sie bei lokalen Benutzern sicher, dass deren E-Mail Eigenschaft eingestellt ist, damit Benachrichtigungen gesendet werden können. Bei Active Directory-Benutzern muss LDAP konfiguriert sein.
8. Klicken Sie in der Liste Device info auf Serial number, UDID oder IMEI. Wenn Sie eine Option auswählen, wird ein Feld angezeigt, in das Sie den entsprechenden Wert für das Gerät eingeben können.



9. Geben Sie für Phone number optional eine Telefonnummer für den Benutzer ein.
10. Wählen Sie in der Liste Carrier den Netzbetreiber aus, der der Telefonnummer zugeordnet werden soll.
11. Wählen Sie für Enrollment mode die Option User name + Password (Standardeinstellung), High Security, Invitation URL + PIN, Invitation URL + Password, Two Factor oder User name + PIN aus.



12. Die Optionen in der Liste Template for agent download hängen vom Plattformtyp ab. Beispielsweise wird iOS Download Link angezeigt, wenn Sie in Schritt 1 iOS ausgewählt haben.



13. Wählen Sie für Template for enrollment URL die Option Enrollment Invitation aus.
14. Wählen Sie für Template for enrollment confirmation die Option Enrollment Invitation aus. Die Registrierungseinladung läuft nach einem bestimmten Zeitraum ab. Dieser Zeitraum wird im Feld Expire after angezeigt. Im Feld Maximum Attempts wird die Höchstanzahl der Registrierungsversuche angezeigt.
15. Klicken Sie unter Send invitation auf ON und dann auf Save & Send.

So senden Sie einen Installationslink für die Registrierung

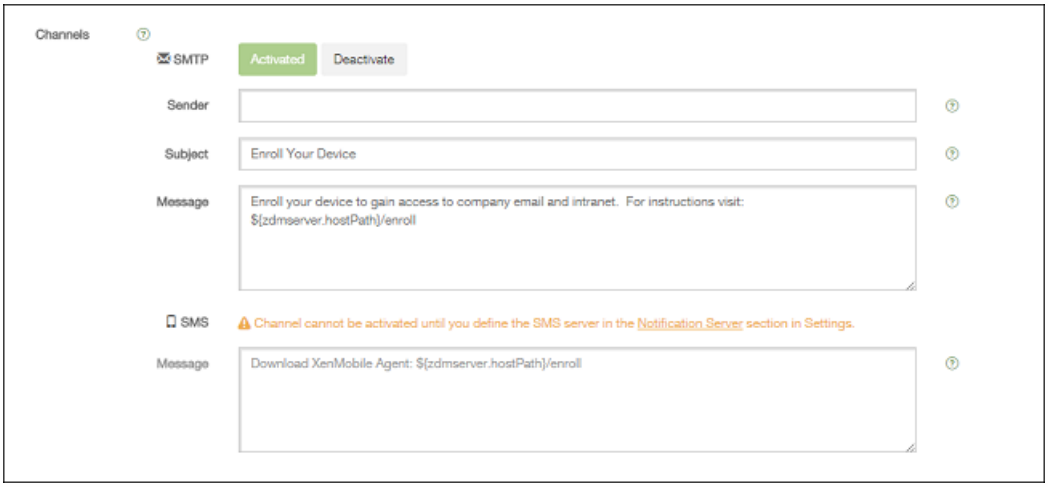
Zum Senden von Installationslinks für die Registrierung müssen Sie Kanäle (SMTP oder SMS) auf dem Benachrichtigungsserver konfigurieren: Configure > Settings > Notification Server. Weitere Informationen finden Sie unter Benachrichtigungen in XenMobile.

1. Klicken Sie in der XenMobile-Konsole auf Manage > Enrollment.

2. Klicken Sie auf der Seite Enrollment auf Add. Ein Menü wird eingeblendet, in dem Sie die Option zum Hinzufügen einer Einladung oder zum Senden eines Installationslinks auswählen können.

3. Klicken Sie auf Send Installation Link. Die Option Send Installation Link wird angezeigt.

4. Klicken Sie unter Recipient auf Add, um die E-Mail-Adresse und Telefonnummer eines Empfängers hinzuzufügen, dem Sie einen Installationslink für die Registrierung senden möchten, und klicken Sie dann auf Save. Wiederholen Sie diesen Schritt zum Hinzufügen einzelner weiterer Empfänger.
5. Wählen Sie unter Channelsden Kanal zum Senden des Installationslinks aus. Benachrichtigungen werden über SMTP oder SMS gesendet.



Hinweis: Diese Kanäle werden erst aktiviert, wenn Sie die Servereinstellungen unter Configure > Settings > Notification Server konfigurieren. Weitere Informationen finden Sie unter Benachrichtigungen in XenMobile.

6. Wenn Sie das Feld SMTP konfigurieren, geben Sie unter Sender den Absender ein. Dies ist ein optionales Feld, das im Formularfeld einer SMTP-Nachricht verwendet wird. Wenn Sie hier keinen Absender angeben, wird der unter Settings > Notification Server angegebene Wert verwendet.
7. Für SMTP-Benachrichtigungen können Sie den Betreff der Nachricht im Feld Subject angeben. Beispiel: "Registrieren Sie Ihr Gerät".
8. Unter Message können Sie den Inhalt der Nachricht an den Empfänger eingeben. Beispiel: "Registrieren Sie Ihr Gerät für den Zugriff auf Unternehmens-Apps und -E-Mail".
9. Zum Senden von Benachrichtigungen per SMS geben Sie eine Nachricht ein, die an den Empfänger gesendet wird. Dieses Feld ist für die Benachrichtigung per SMS erforderlich.
   Hinweis: In Nordamerika werden SMS-Nachrichten mit mehr als 160 Zeichen in mehrere Nachrichten aufgeteilt.
10. Klicken Sie auf Senden.

Hinweis

Wenn die Umgebung SAMAccountName verwendet, müssen Benutzer nach dem Erhalt der Einladung auf den Link klicken und dann den Benutzernamen ändern, um die Authentifizierung abzuschließen. Sie müssen beispielsweise "domainname" aus SAMAccountName@domainname.com entfernen.

Verwalten von Geräten mit Android for Work in XenMobile

Dec 01, 2015

Android for Work ist ein sicherer Arbeitsbereich auf Geräten mit Android 5.0 und höher, durch den geschäftliche Konten, Apps und Daten von persönlichen Konten, Apps und Daten getrennt werden. In XenMobile 10.1 verwalten Sie Privatgeräte (BYOD) und unternehmenseigene Android-Geräte, indem Sie veranlassen, dass die Benutzer ein separates Arbeitsprofil auf ihren Geräten erstellen, durch das in Kombination mit der Hardwareverschlüsselung und den von Ihnen bereitgestellten Richtlinien der geschäftliche und der persönliche Bereich voneinander sicher getrennt werden. Sie können alle Unternehmensrichtlinien, -Apps und -daten remote verwalten und löschen, ohne dass dies Auswirkungen auf den privaten Bereich der Benutzer hat. Weitere Informationen zu den unterstützten Android-Geräten finden Sie auf der Geräteseite von Google.

In XenMobile 10.1 können Sie auch Geräte mit Android 4.0-4.4 verwalten. Dazu müssen Benutzer die Android for Work-App herunterladen und installieren. Diese App bietet den gleichen sicheren Arbeitsbereich, der bei Geräten mit Android 5.0 und höher integriert ist.

Sie verwenden Google Play for Work zum Hinzufügen, Erwerben und Genehmigen von Apps für die Bereitstellung in dem Android for Work-Arbeitsbereich von Geräten. Über Google Play for Work können Sie private Android-Apps sowie öffentliche Apps und solche von Drittanbietern bereitstellen.

Anforderungen für Android for Work:

- Öffentlich zugängliche Domäne
- Google-Administratorkonto
- Geräte mit Android 5.0+ (Lollipop) mit Unterstützung für verwaltete Profile sowie Geräte mit Android 4.0-4.4 (Ice Cream Sandwich, Jelly Bean und KitKat) mit der Android for Work-App
- Google-Konto und Google Play im persönlichen Profil der Benutzer installiert
- Geschäftliches Profil auf den Geräten eingerichtet

Bevor Sie Android for Work-App-Einschränkungen festlegen können, müssen Sie die folgenden Schritte ausführen:

- Einrichtung von Android for Work auf Google
- Erstellen einer Reihe von Google Play-Anmeldeinformationen
- Konfigurieren der Android for Work-Servereinstellungen
- Erstellen Sie mindestens eine Android for Work Richtlinie.
- Hinzufügen, Erwerben und Genehmigen von Android for Work-Apps im Google Play for Work-Store

Bei der Verwaltung von Android for Work können Sie die folgenden Links verwenden:

- Google-Verwaltungskonsole: https://admin.google.com/AdminHome
- Play for Work-Verwaltungskonsole: https://play.google.com/work/apps
- Google Play zur Veröffentlichung für private Kanäle und selbstgehostete Apps: https://play.google.com/apps/publish
- Google Developer-Konsole zur Erstellung des Dienstkontos: https://console.developers.google.com

Voraussetzungen für Android for Work

Bevor Sie Android for Work in XenMobile verwalten können, müssen Sie die folgenden Schritte ausführen:

- Erstellen eines Android for Work-Kontos
- Einrichten eines Dienstkontos
- Herunterladen eines Android for Work-Zertifikats
  Aktivieren und Autorisieren des Google Admin-SDKs und der MDM-APIs
- Autorisieren des Dienstkontos zur Verwendung des Verzeichnisses und von Google Play
- Abrufen eines Bindungstokens

In den folgenden Abschnitten werden diese Arbeitsgänge erläutert. Nachdem Sie diese Aufgaben erledigt haben, können Sie eine Reihe von Google Play-Anmeldeinformationen erstellen, Android for Work-Einstellungen konfigurieren und Android for Work-Apps in XenMobile verwalten.

Erstellen eines Android for Work-Kontos

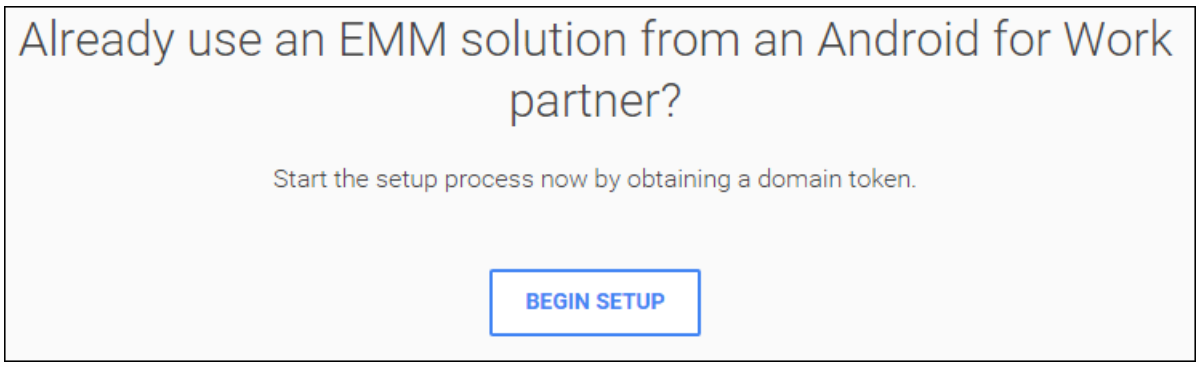
Die folgenden Voraussetzungen müssen erfüllt sein, damit Sie ein Android for Work-Konto erstellen können:

- Sie müssen eine Domäne haben (z. B. example.com).
- Sie müssen zulassen, dass Google prüft, ob Sie Eigentümer der Domäne sind.
- Sie müssen Android for Work über einen Enterprise Mobility Management (EMM)-Anbieter (XenMobile 10.1 oder höher) aktivieren und verwalten.

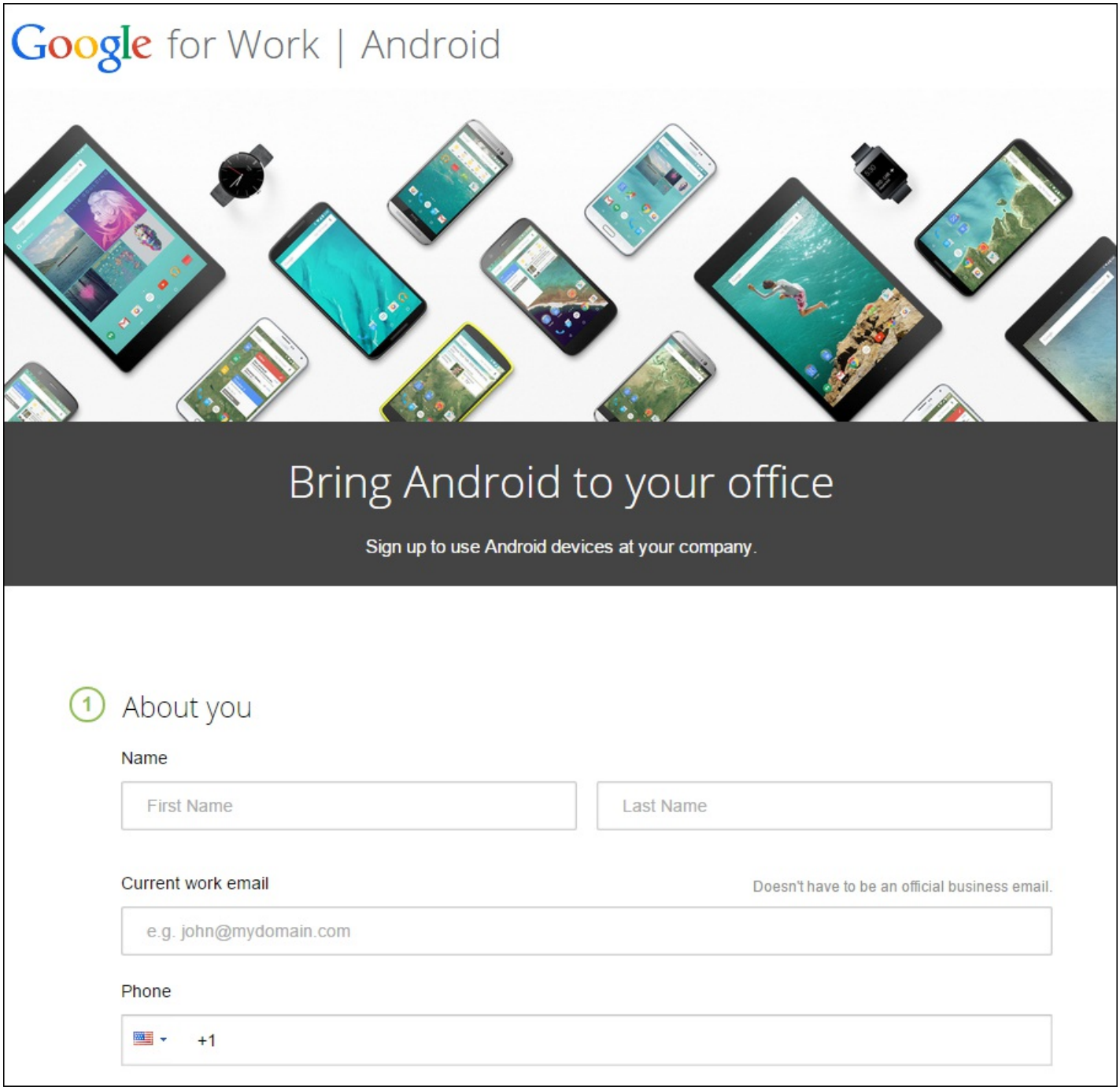
Wenn Ihr Domänenname bei Google bereits verifiziert wurde, können Sie mit dem Schritt Einrichten eines Android for Work-Dienstkontos und Download eines Android for Work-Zertifikats fortfahren.

1. Rufen Sie die Seite Partners des Android for Work-Portals von Google auf (**https://www.google.com/work/android/partners/**).

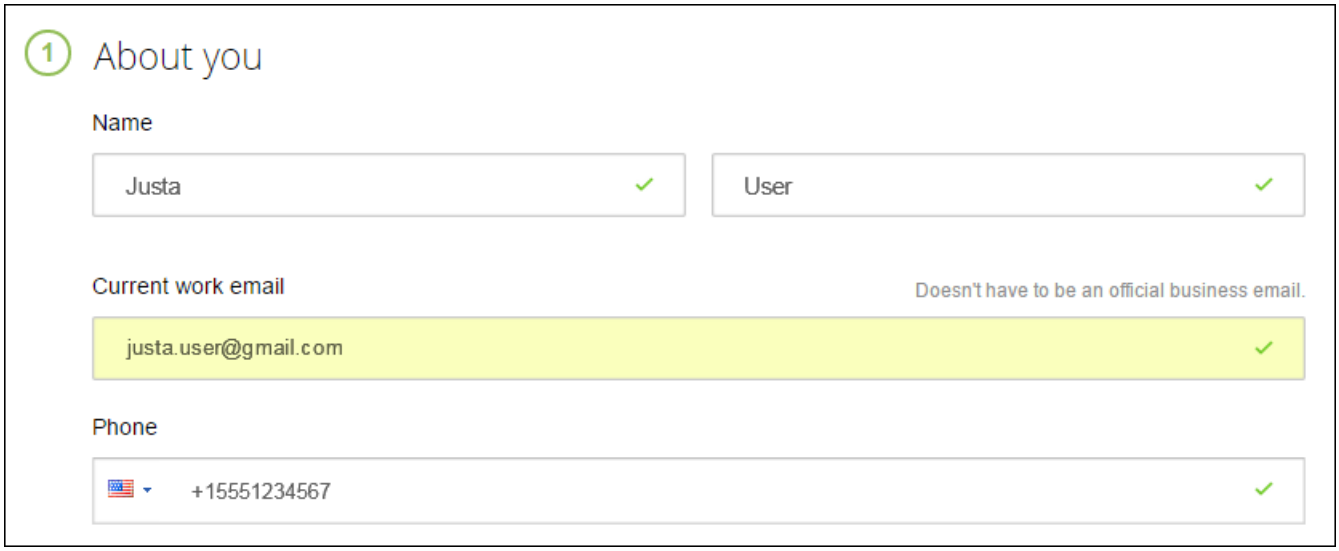
2. Klicken Sie auf **Begin Setup**.



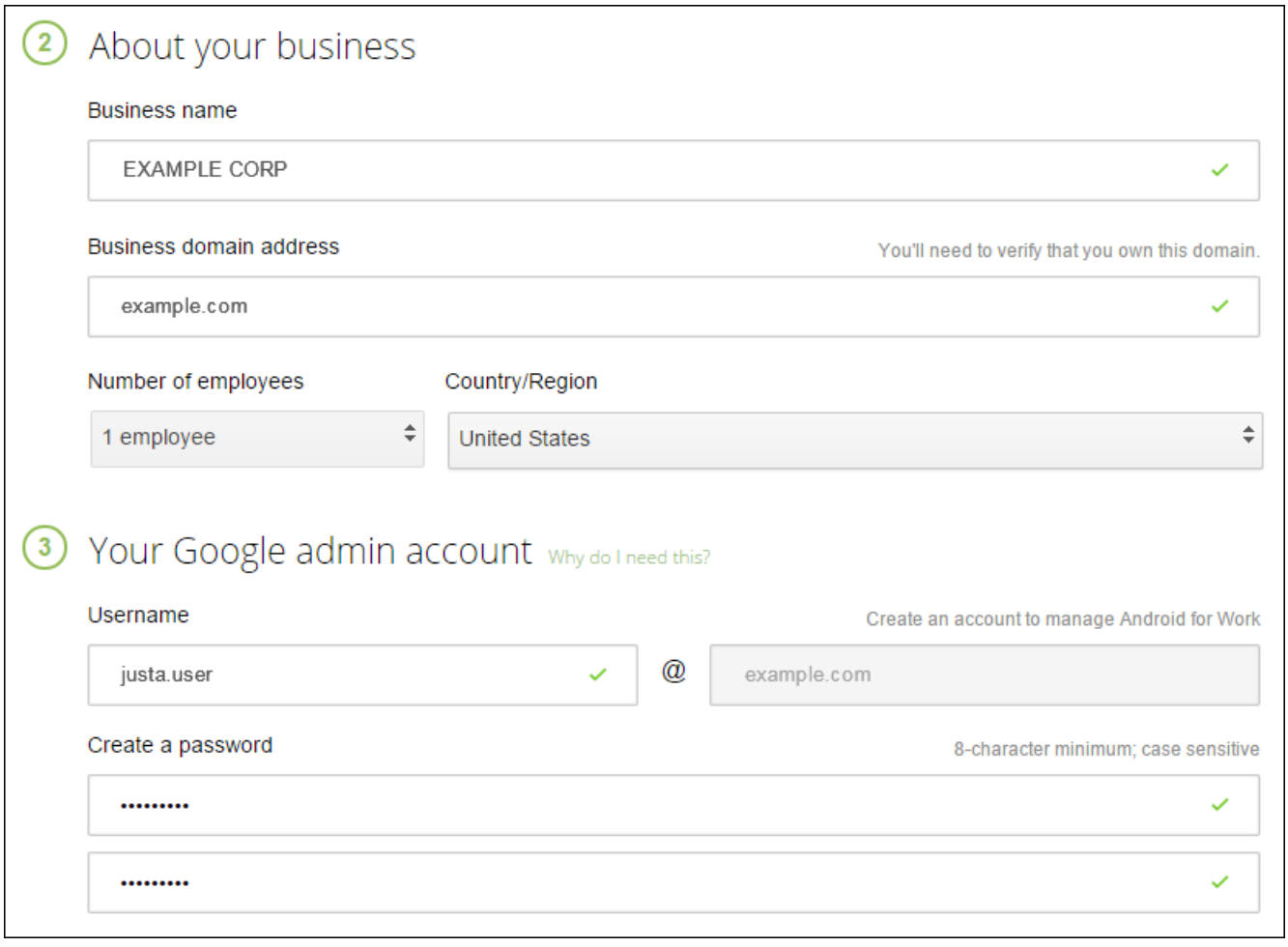
Sie werden auf die folgende Seite umgeleitet, auf der Sie die Administrator- und Unternehmensinformationen eingeben müssen.



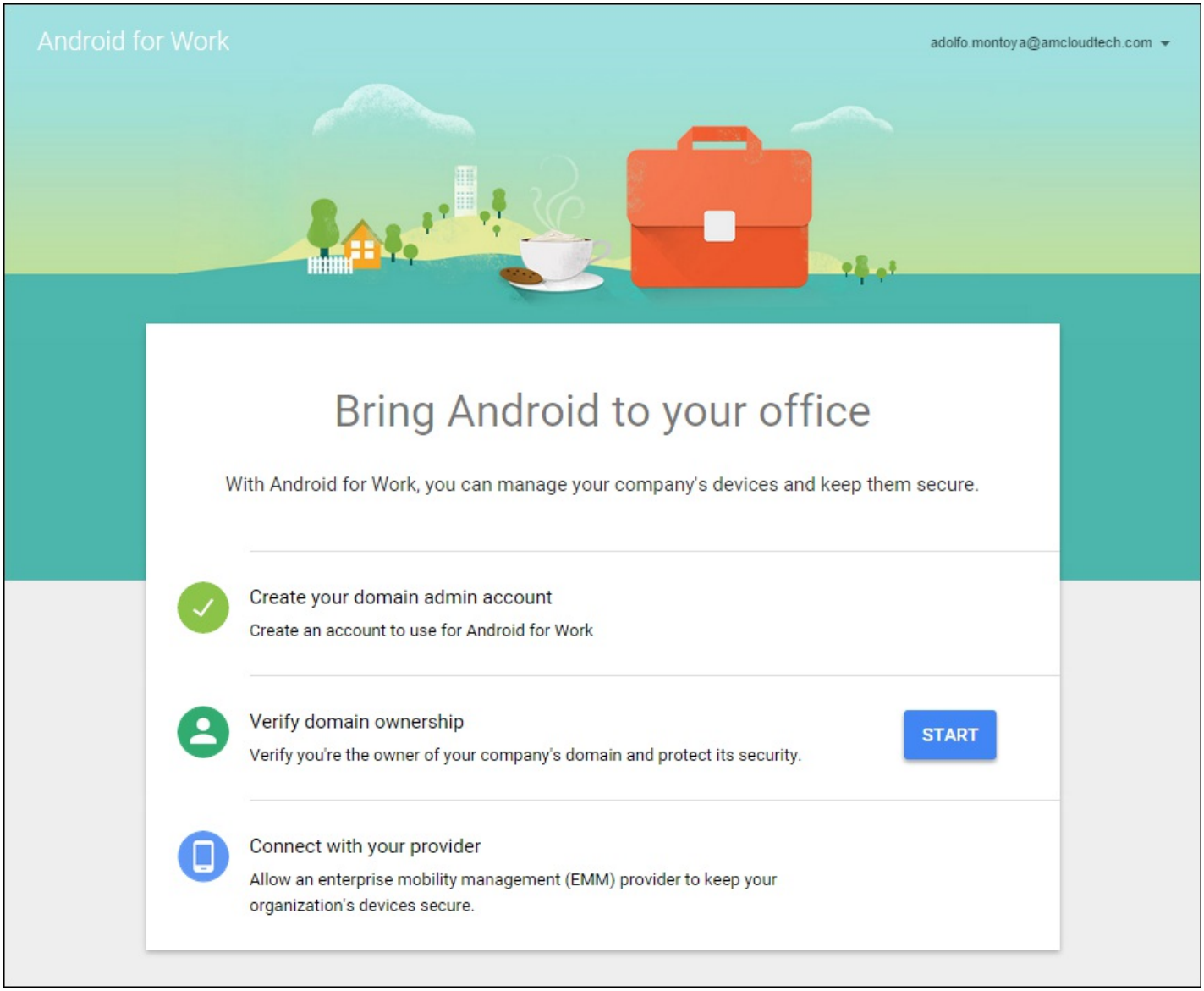
2. Geben Sie die Administratorinformationen ein.



3. Geben Sie Ihre Unternehmensinformationen sowie die Administratorkonteninformationen ein.



Der erste Schritt des Prozesses ist abgeschlossen und es wird die folgende Seite angezeigt.

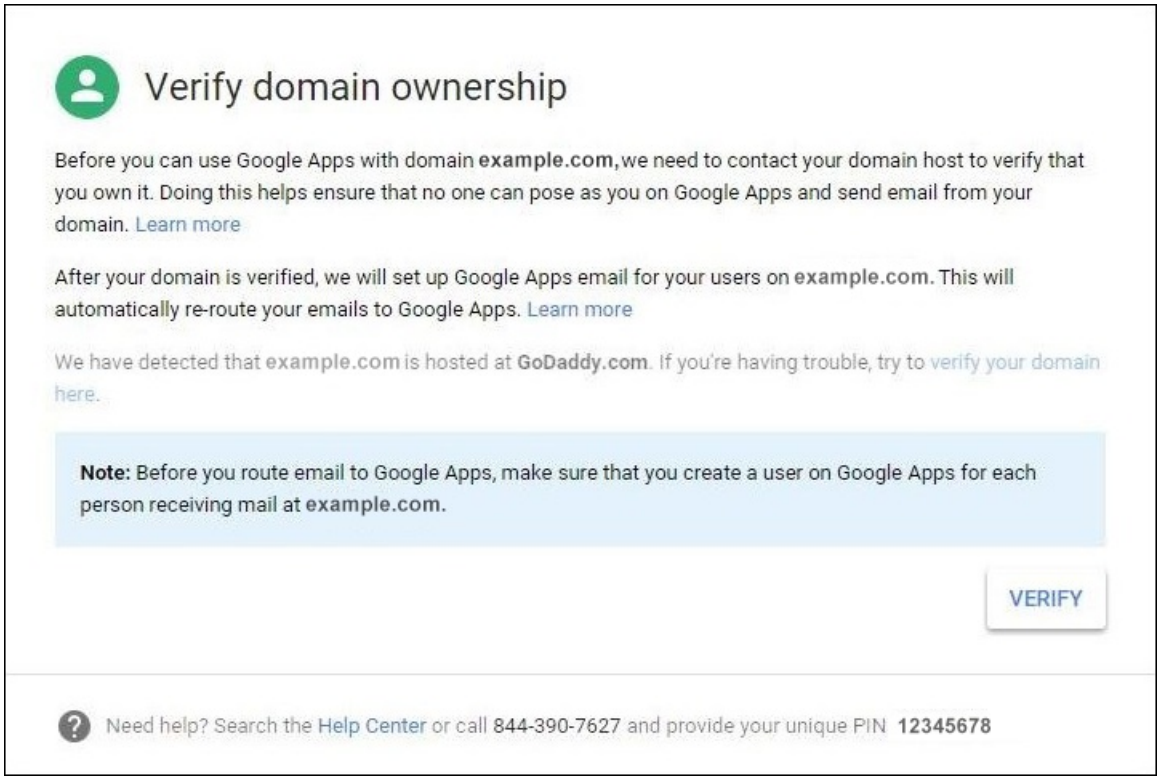


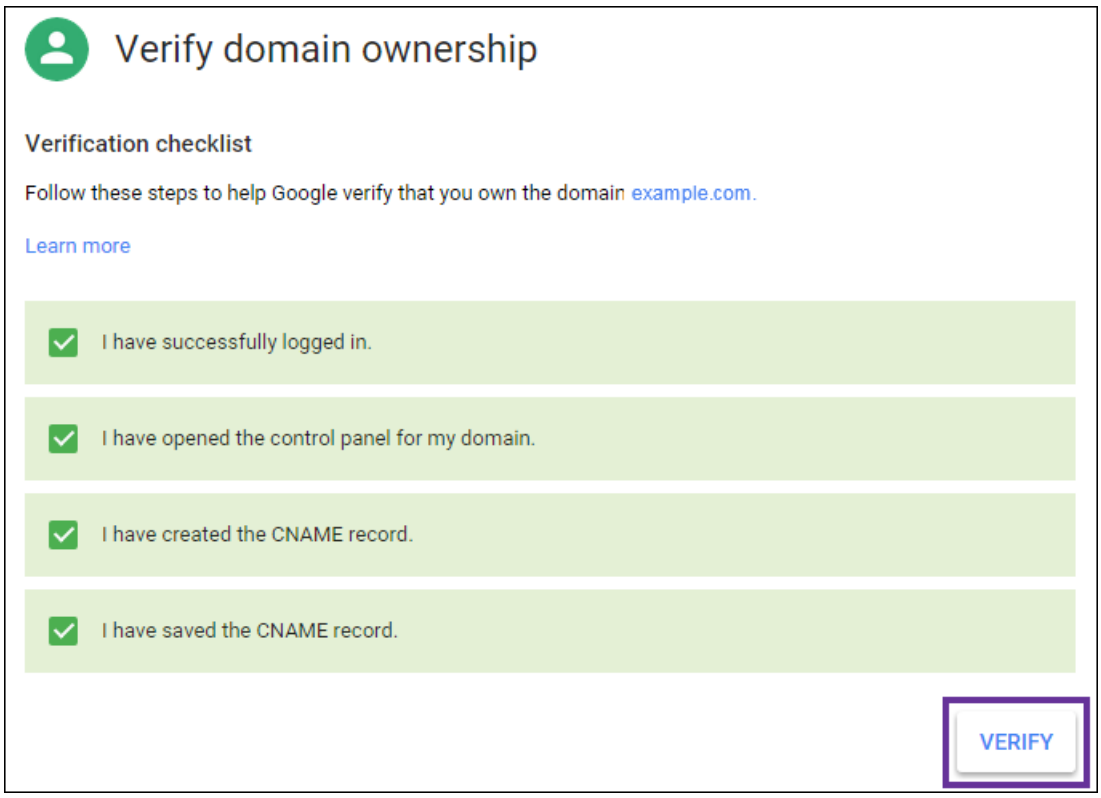
Überprüfen der Domäneneigentümerschaft

Sie müssen jetzt zulassen, dass Google Ihre Domäne überprüft. Die Domäne kann auf dreierlei Weise überprüft werden: Hinzufügen eines TXT- oder CNAME-Eintrags zur Website Ihres Domänenhosts, Hochladen einer HTML-Datei auf den Webserver Ihrer Domäne oder Hinzufügen eines -Tags zu Ihrer Homepage. Google empfiehlt die Verwendung der ersten Methode. Die Schritte zum Überprüfen Ihrer Domäneneigentümerschaft werden in diesem Artikel nicht behandelt, Informationen finden Sie unter https://support.google.com/a/answer/6095407/.

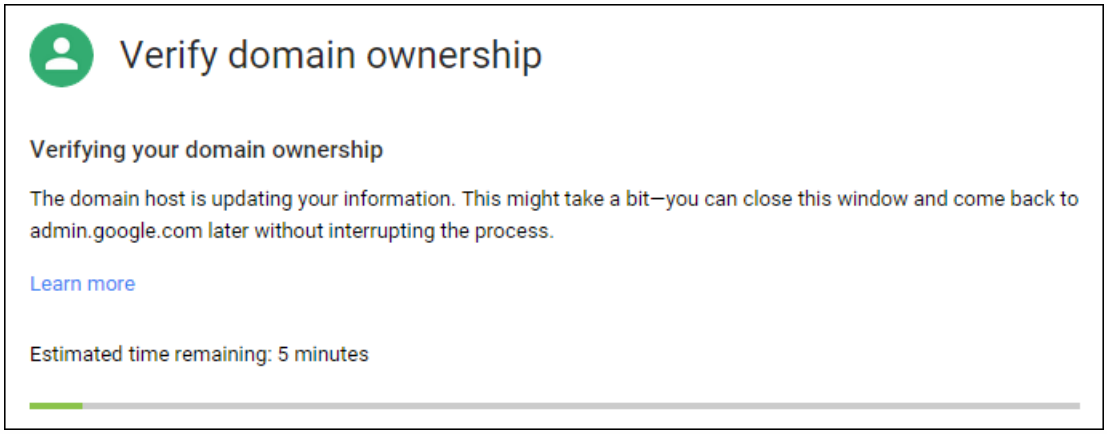
1. Klicken Sie auf **Start**, um die Domänenüberprüfung zu beginnen. Die Seite **Verify domain ownership** wird angezeigt. Folgen Sie den angezeigten Anweisungen zum Überprüfen Ihrer Domäne.

2. Wenn Sie fertig sind, klicken Sie auf **Verify**.

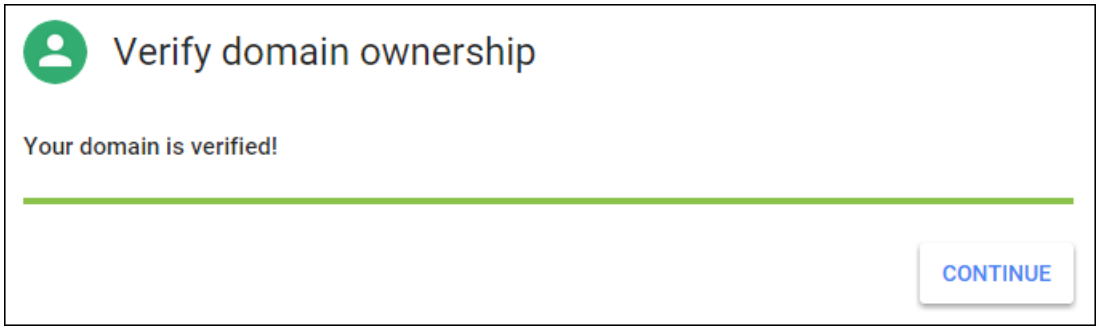




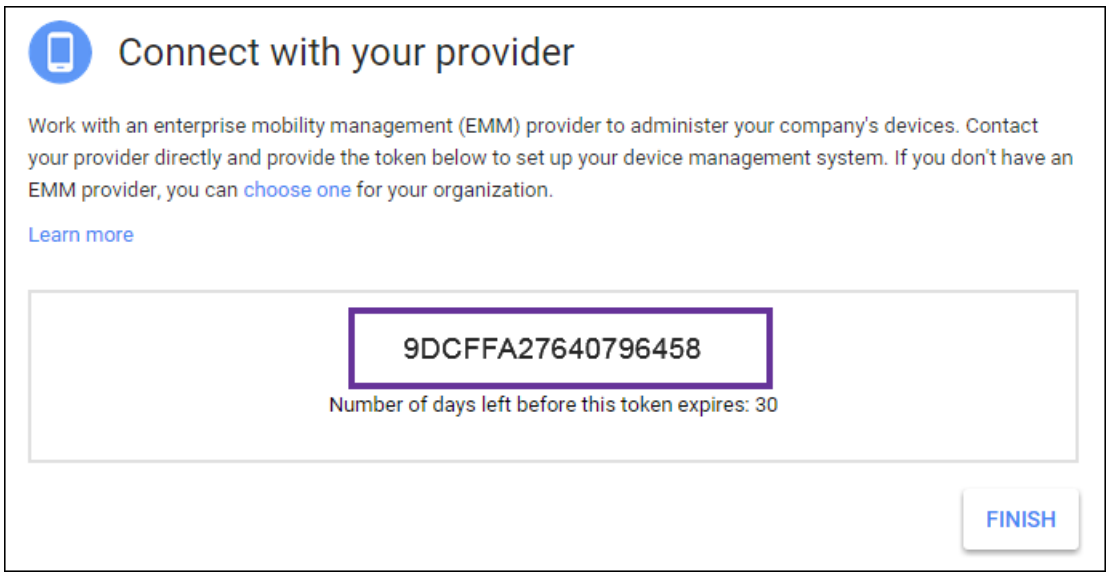
7. Google überprüft die Eigentümerschaft der Domäne.



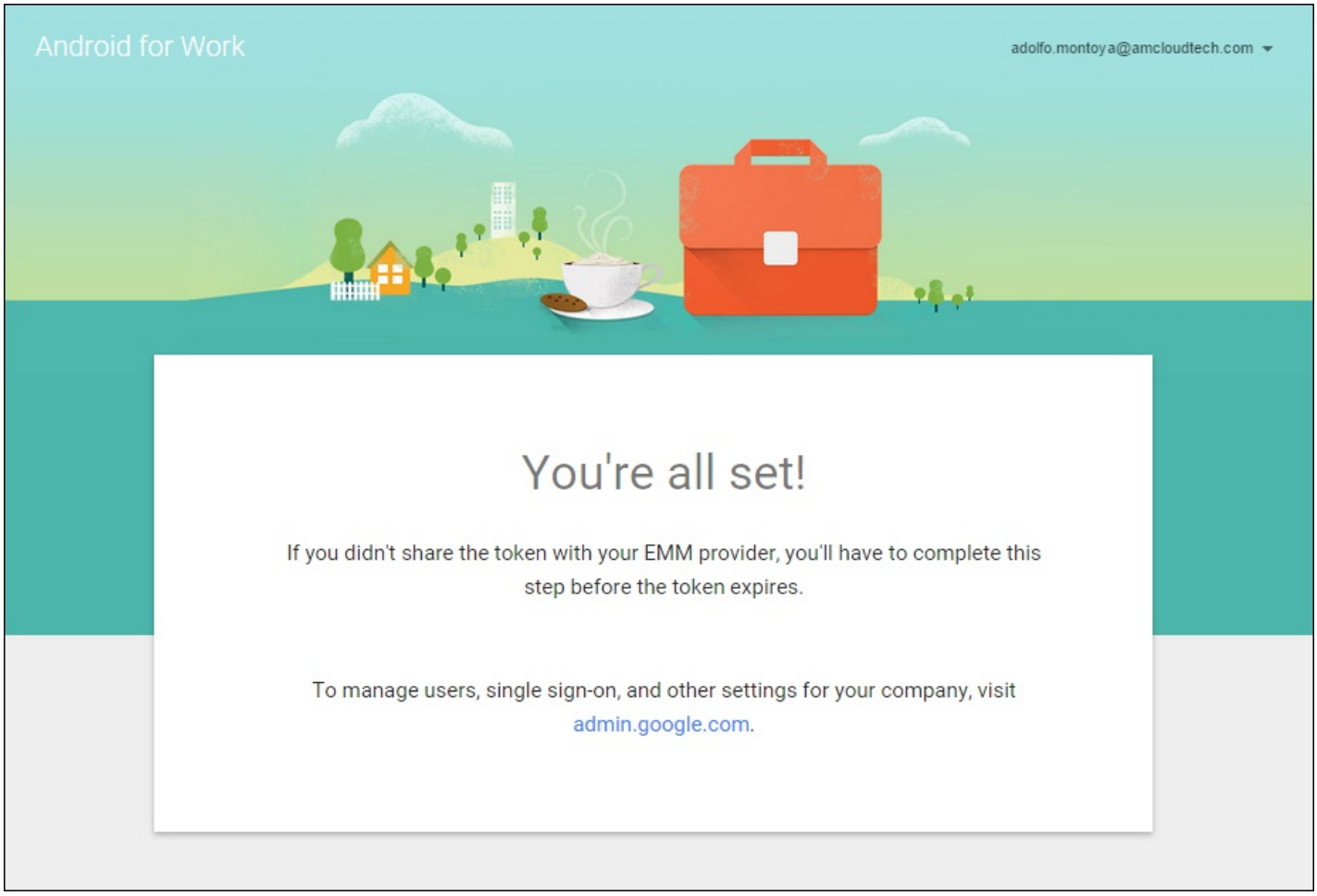
8. Nach Bestehen der Prüfung wird die folgende Seite angezeigt. Klicken Sie auf **Continue**.



9. Google erstellt ein EMM-Bindungstoken, das Sie Citrix zur Verfügung stellen und beim Konfigurieren der Android for Work-Einstellungen verwenden. Kopieren und speichern Sie das Token zur späteren Verwendung beim Setup.



10. Klicken Sie auf **Finish**, um die Einrichtung von Android for Work abzuschließen.

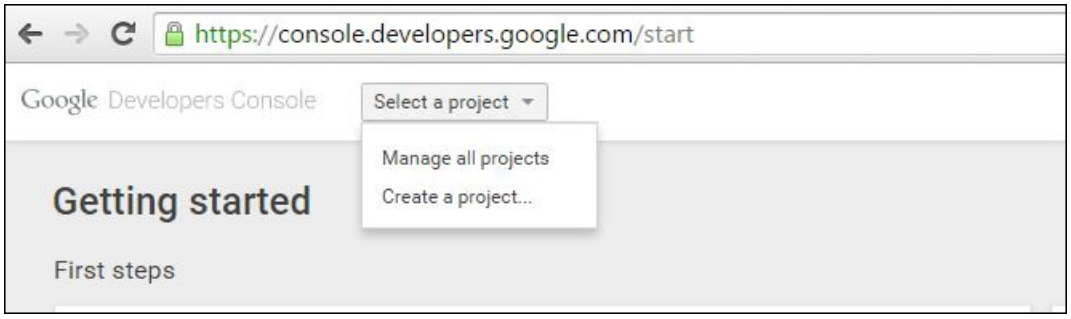


Nach dem Erstellen eines Android for Work-Dienstkontos können Sie sich bei der Google-Verwaltungskonsole zum Verwalten der Android for Work-Mobility Management-Einstellungen anmelden.

Einrichten eines Android for Work-Dienstkontos und Download eines Android for Work-Zertifikats

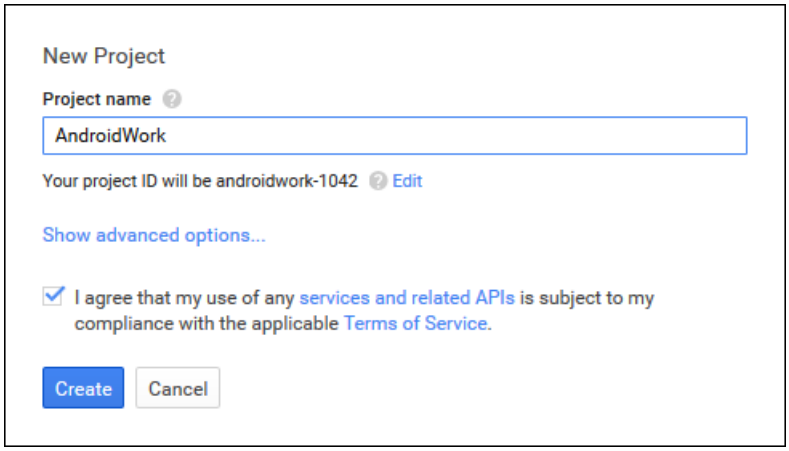
Damit XenMobile Google Play und Verzeichnisdienste kontaktieren kann, müssen Sie ein neues Dienstkonto mit dem Projektportal für Entwickler von Google erstellen. Das Dienstkonto wird für die Server-Kommunikation zwischen XenMobile und den Google-Diensten für Android for Work verwendet. Weitere Informationen zum verwendeten Authentifizierungsprotokoll finden Sie unter https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

1. Rufen Sie in einem Webbrowser https://console.developers.google.com/project auf und melden Sie sich mit Ihren Anmeldeinformationen als Google-Administrator an.

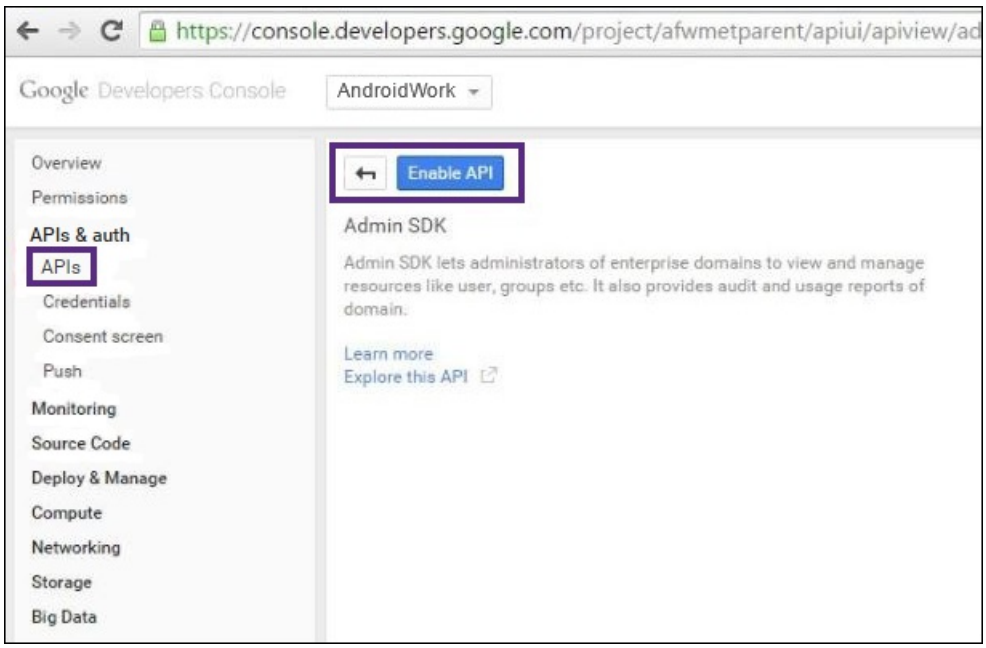


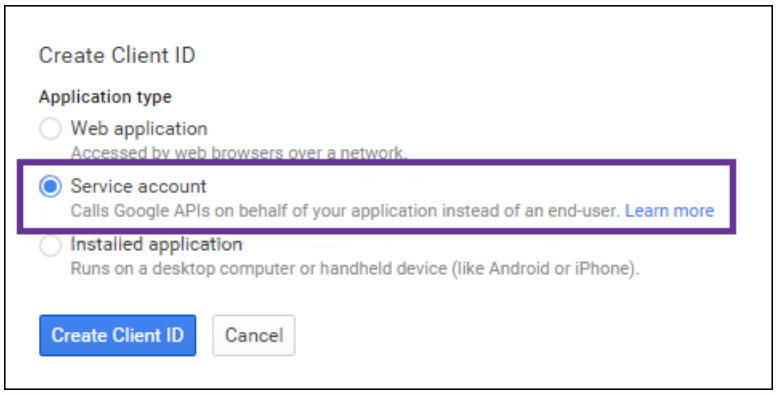
3. Klicken Sie in der Liste **Select a project** auf **Create a Project**.

4. Geben Sie einen Projektnamen ein. Klicken Sie auf das Kontrollkästchen um den Nutzungsbedingungen zuzustimmen, und klicken Sie dann auf **Create**.



5. Klicken Sie links auf **APIs & auth** und anschließend auf **APIs**.

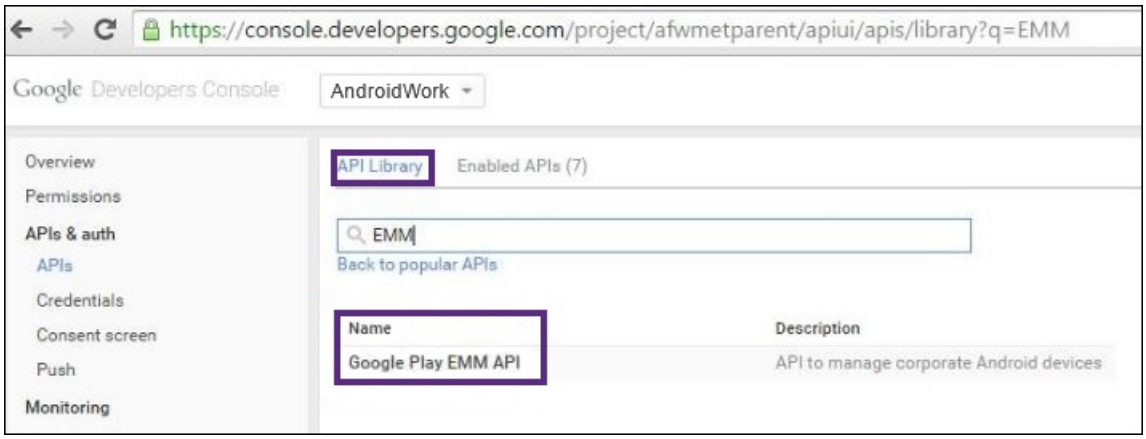




6. Klicken Sie unter **Google Apps APIs** auf **Admin SDK**. Alternativ geben Sie "Admin SDK" in das Suchfeld ein und klicken Sie anschließend im Suchergebnis auf **Admin SDK**.

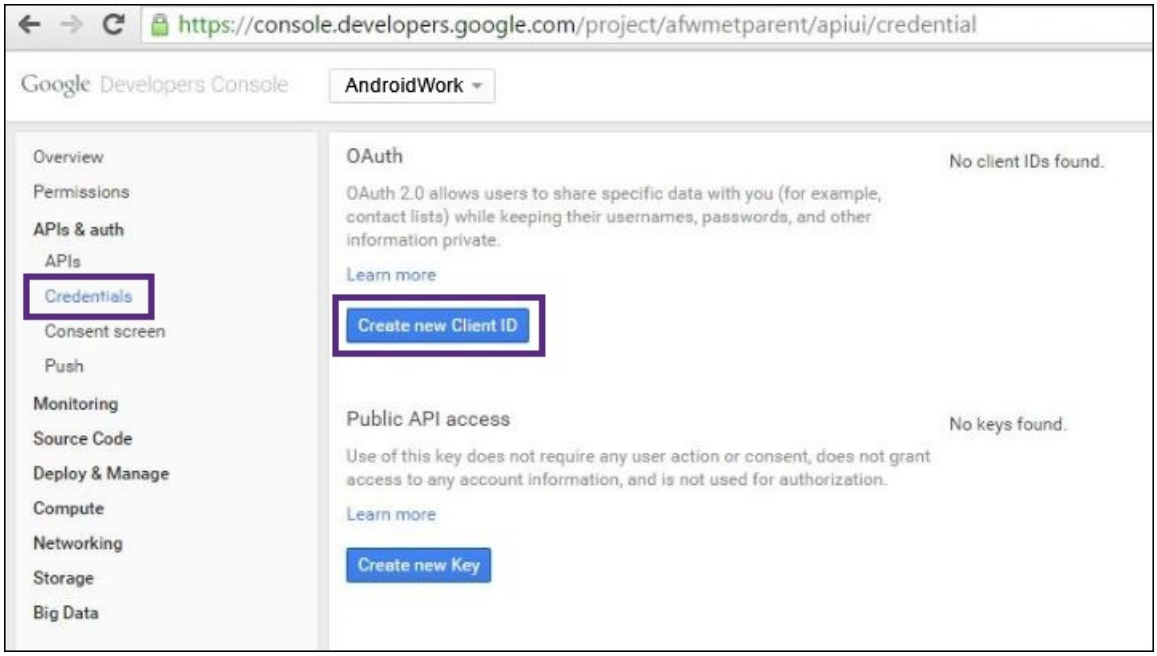
7. Klicken Sie auf **Enable API**.

8. Suchen Sie unter **API Library** den Eintrag **EMM** und wählen Sie **Google Play EMM API** aus.

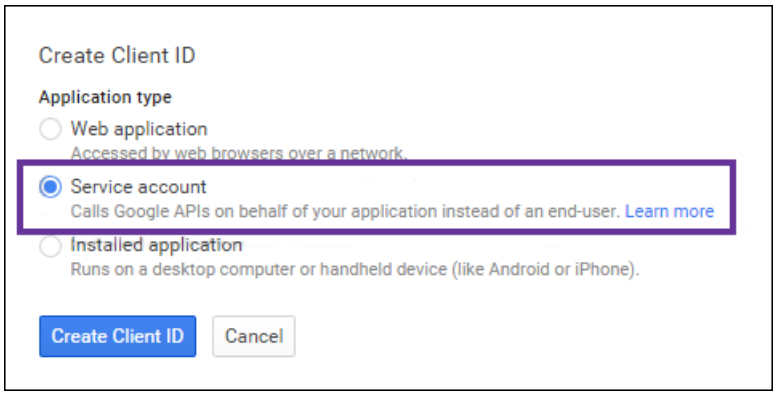


9. Klicken Sie auf **Enable API**.

10. Klicken Sie auf der gleichen Seite links unter **APIs & auth** auf **Credentials**.



11. Wählen Sie rechts **Create new Client ID** aus. Das Dialogfeld **Create Client ID** wird angezeigt.



12. Wählen Sie **Service account** aus und klicken Sie auf **Create Client ID**.

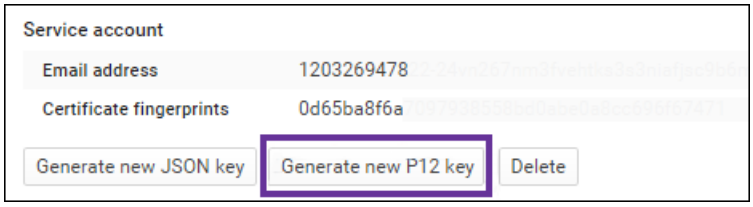
13. Klicken Sie auf **Okay, got it**. Nachdem Sie auf "Okay, got it" geklickt haben, wird eine JSON-Datei auf Ihren Computer

heruntergeladen. Speichern Sie die Datei an einem sicheren Ort.

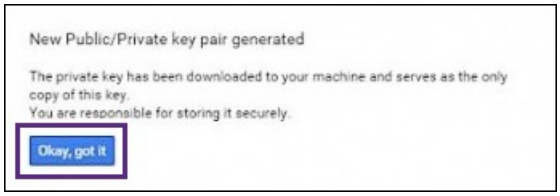
Notieren Sie die unter **Service account** angegebene E-Mail-Adresse und die Zertifikatfingerabdrücke (Kennwort). Sie benötigen diese später.

Die E-Mail-Adresse ist das Dienstkonto, das Sie für die Bindung von XenMobile als EMM-Anbieter und zum Aktivieren des API-Clientzugriffs verwenden.

14. Klicken Sie unter **Service account** auf **Generate new P12 key**. Die Zertifikatdatei (P12-Datei) wird auf Ihren Computer heruntergeladen. Speichern Sie das Zertifikat an einem sicheren Ort.

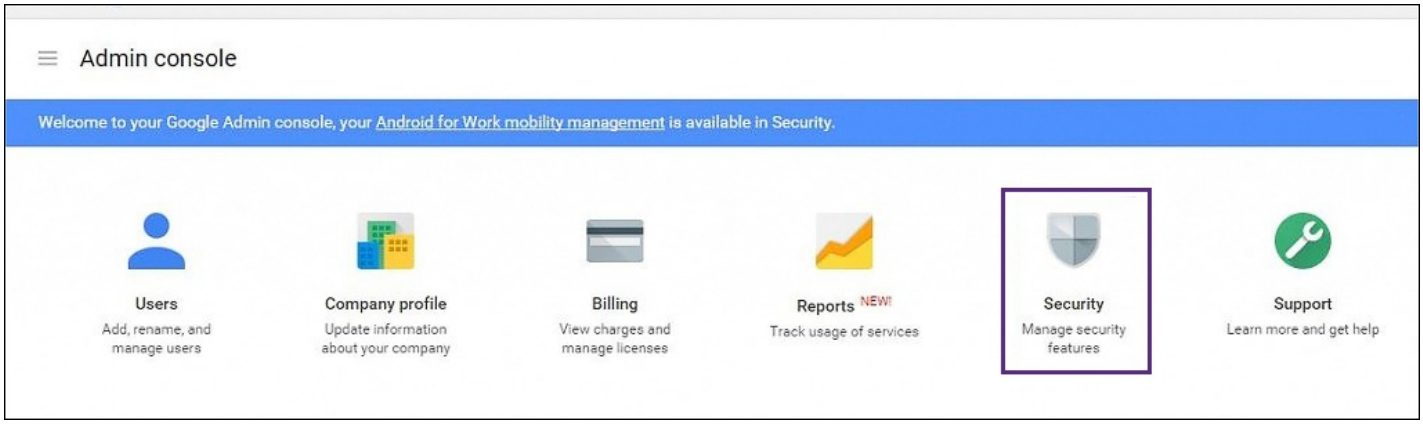


15. Klicken Sie auf **Okay, got it**.

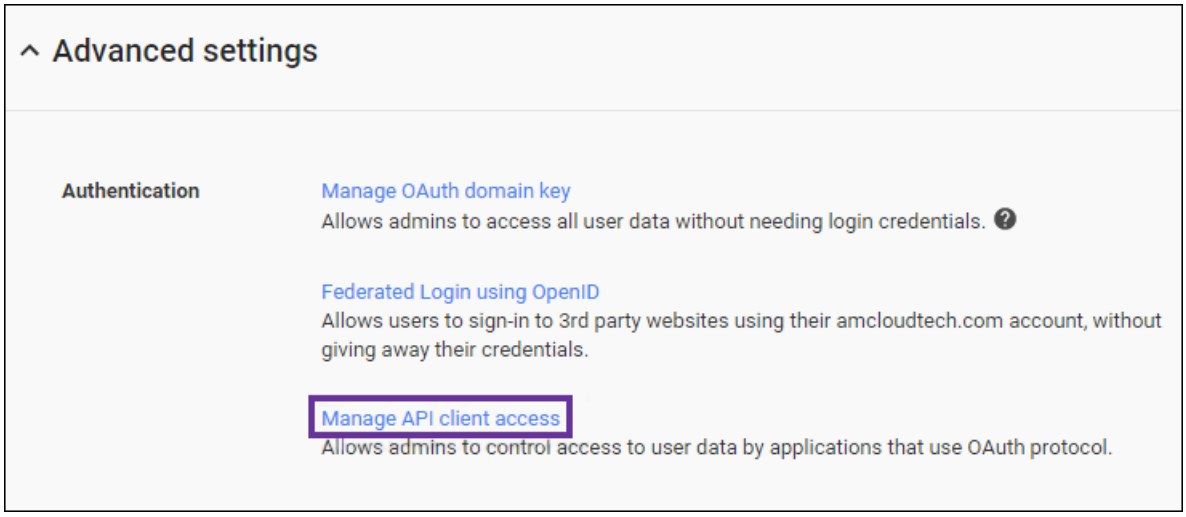


16. Melden Sie sich mit Ihren Administratoranmeldeinformationen für Android for Work beim Google-Verwaltungsportal unter https://admin.google.com an.

17. Klicken Sie auf **Security**.



18. Klicken Sie auf **Advanced Settings** und anschließend auf **Manage API client access**.

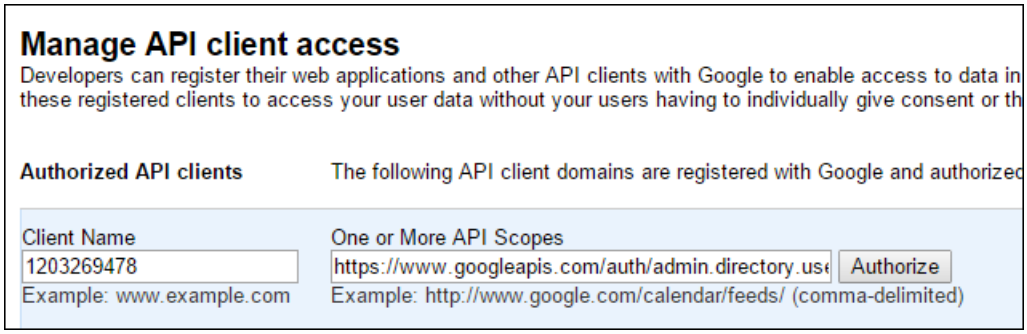


19. Klicken Sie auf **Authorized API clients**. Die Seite **Manage API client access** wird angezeigt.

20. Geben Sie unter **Client Name** die in Schritt 14 generierte Client-ID ein.

21. Geben Sie unter **One or More API Scopes** die URL https://www.googleapis.com/auth/admin.directory.user ein.

22. Klicken Sie auf **Authorize**.

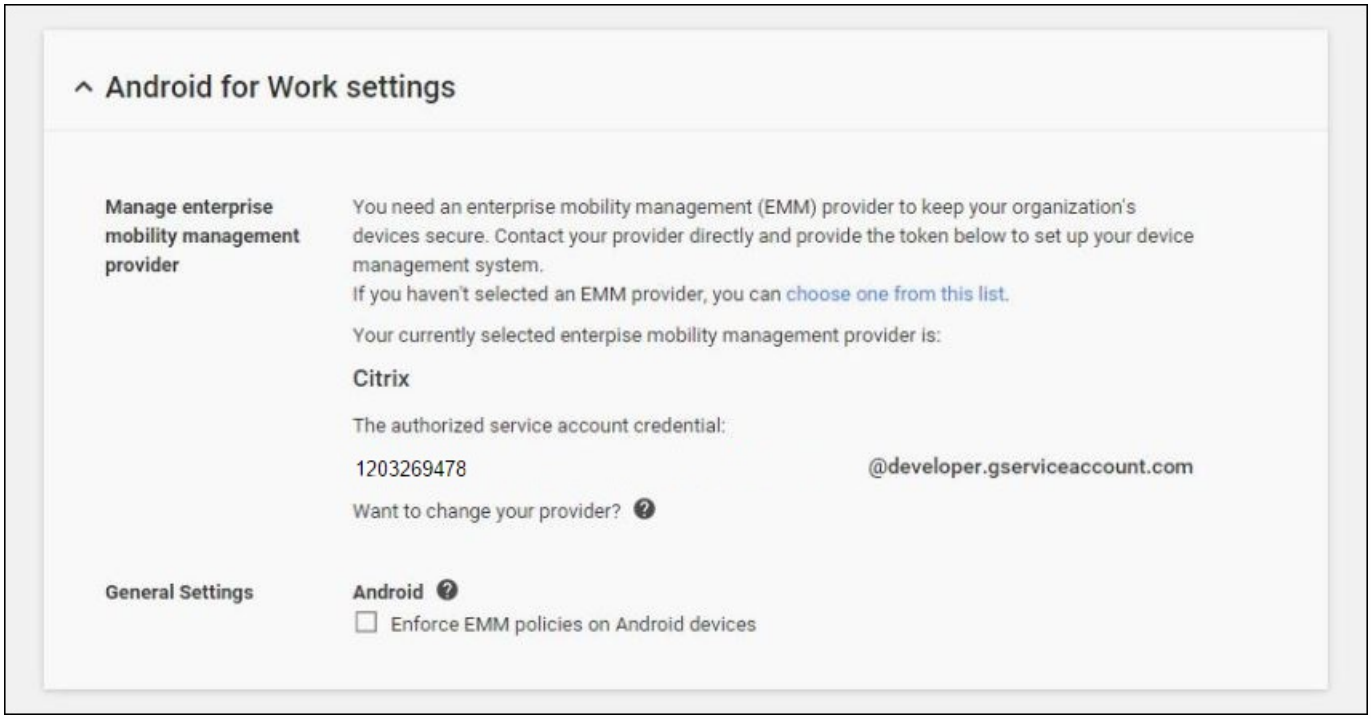


Binden an EMM

Bevor Sie Android for Work-Geräte mit XenMobile verwalten können, müssen Sie dem technischen Support von Citrix (https://www.citrix.com/contact/technical-support.html) den Namen Ihrer Domäne, das Dienstkonto und das Bindungstoken zukommen lassen. Citrix bindet das Token dann an XenMobile zur Verwendung als Enterprise Mobility Management-Anbieter (EMM).

1. Zum Überprüfen der Bindung melden Sie sich beim Google-Verwaltungsportal an und klicken Sie auf **Security**.

2. Klicken Sie auf **Android for Work settings**. Sie sehen dann, dass Ihr Android for Work-Konto bei Google nun an Citrix als EMM-Anbieter gebunden ist.



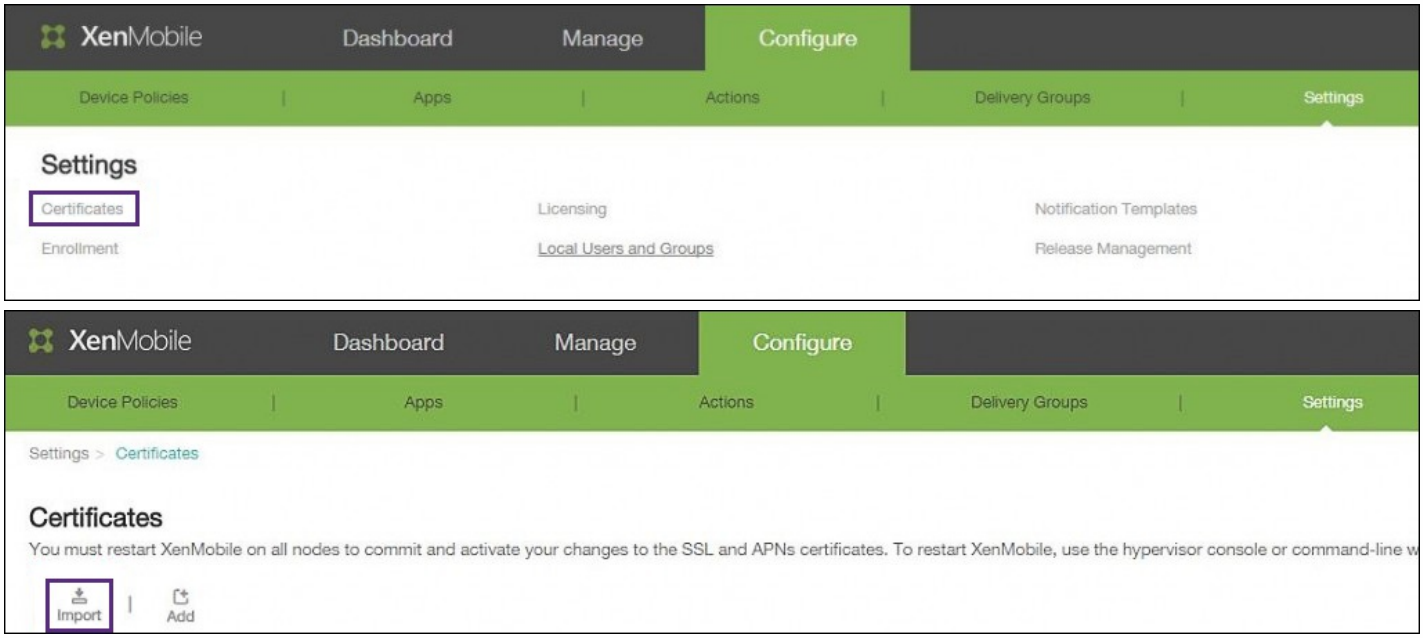
Nach der Prüfung der Tokenbindung können Sie XenMobile zum Verwalten der Android for Work-Geräte verwenden. Sie müssen das in Schritt 14 generierte P12-Zertifikat importieren, den Android for Work-Server einrichten, das SAML-basierte Single Sign-On aktivieren und mindestens eine Android for Work-Richtlinie definieren.

Importieren des P12-Zertifikats

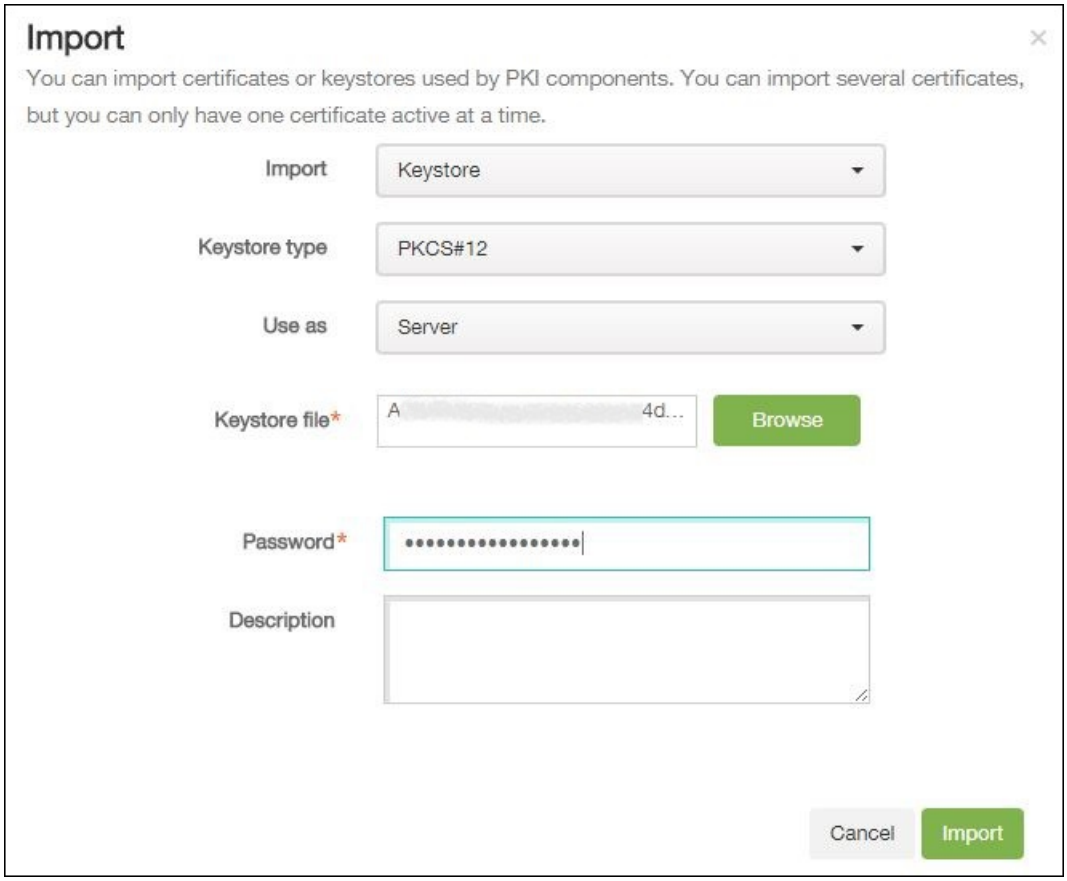
Führen Sie die folgenden Schritte zum Importieren des Android for Work-P12-Zertifikats aus:

1. Melden Sie sich bei der XenMobile 10.1-Konsole an.

2. Klicken Sie auf **Configure->Settings->Certificate**. Die Seite **Certificates** wird angezeigt.



3. Klicken Sie auf **Import**. Das Dialogfeld **Import** wird angezeigt. Konfigurieren Sie die folgenden Einstellungen:

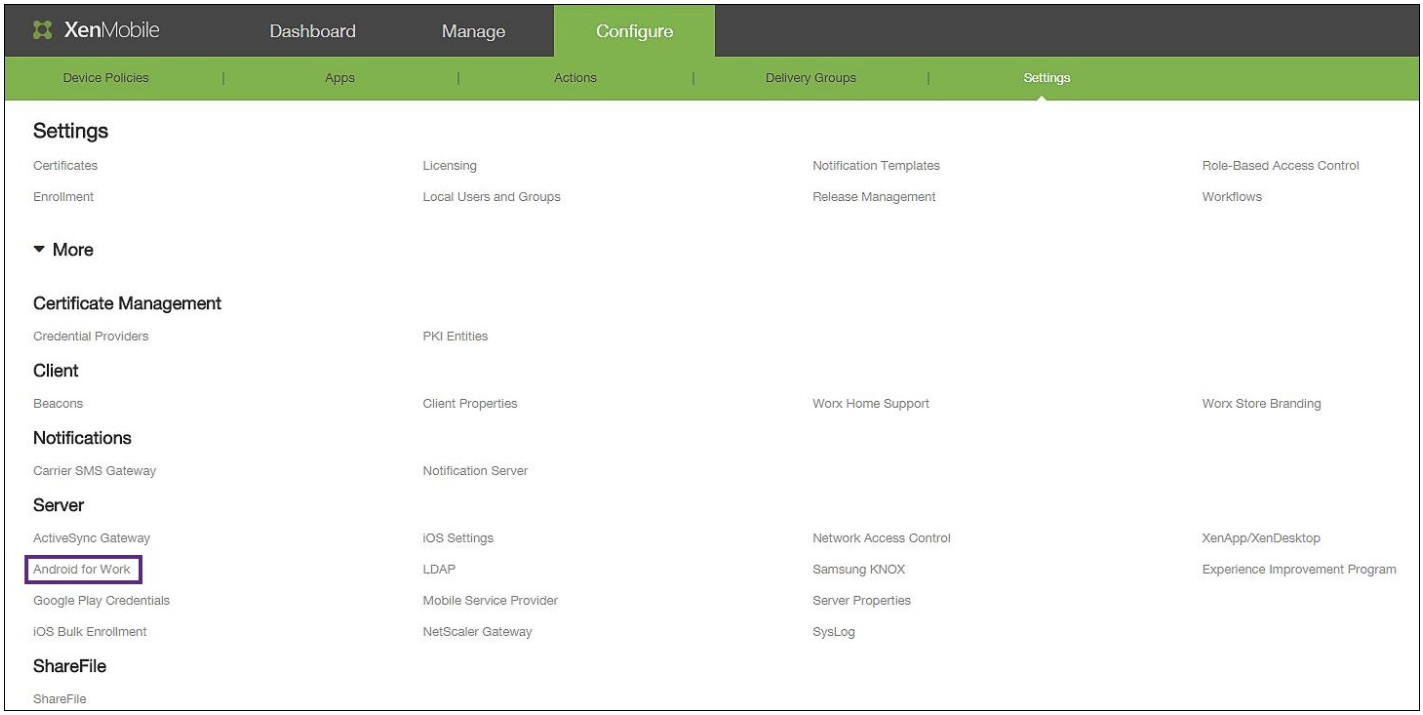


- **Import**: Klicken Sie in der Liste auf "Keystore".
- **Keystore type**: Klicken Sie in der Liste auf "PKCS#12".
- **Use as**: Klicken Sie in der Liste auf "Server".
- **Keystore file**: Klicken Sie auf "Browse" und navigieren Sie zu dem P12-Zertifikat.
- **Password**: Geben Sie das Keystore-Kennwort ein.
- **Description**: Geben Sie optional eine Beschreibung des Zertifikats ein.

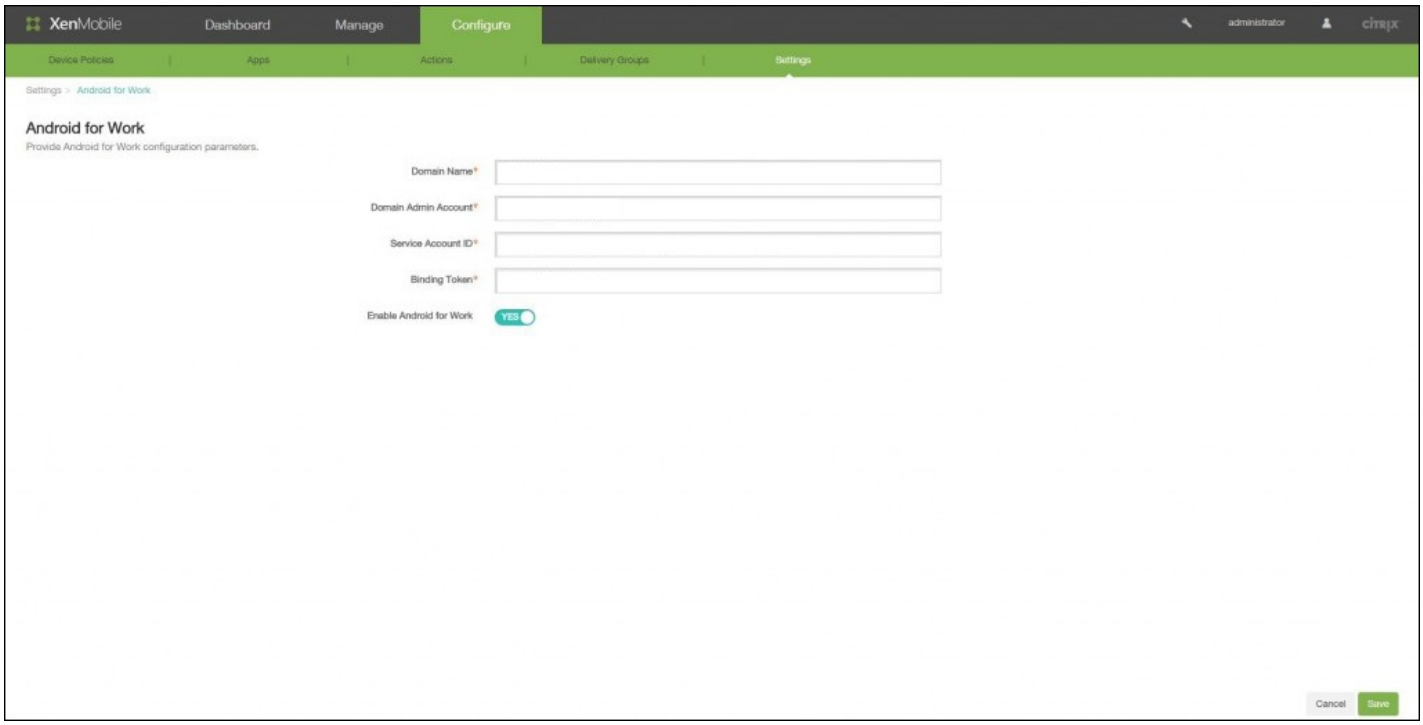
4. Klicken Sie auf **Import**.

Einrichten des Android for Work-Servers

1. Klicken Sie auf **Configure->Settings** und erweitern Sie **More**.



2. Klicken Sie unter **Server** auf **Android for Work**. Die Seite **Android for Work** wird angezeigt. Konfigurieren Sie die folgenden Einstellungen:



- **Domain name**: Geben Sie den Namen der Android for Work-Domänen ein.
- **Domain Admin Account**: Geben Sie Ihren Domänenadministrator-Benutzernamenein.
- **Service Account ID**: Geben Sie die ID Ihres Dienstkontos ein.
- **Binding Token**: Geben Sie das Bindungstoken ein oder kopieren Sie es in das Feld.
- **Enable Android for Work**: Klicken Sie zum Aktivieren oder Deaktivieren auf diese Option.

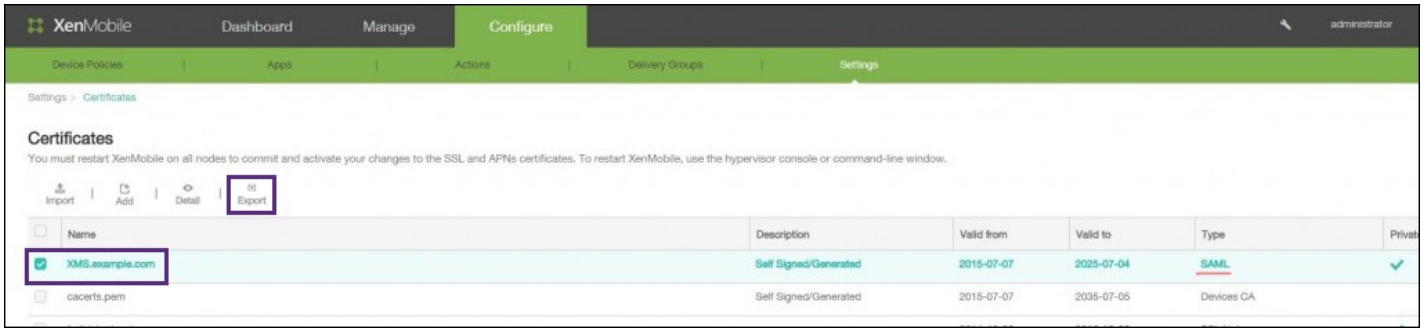
3. Klicken Sie auf **Save**.

Aktivieren des SAML-basierten Single Sign-Ons

1. Melden Sie sich bei der XenMobile 10.1-Konsole an.

2. Klicken Sie auf **Configure->Settings->Certificate**. Die Seite **Certificates** wird angezeigt.

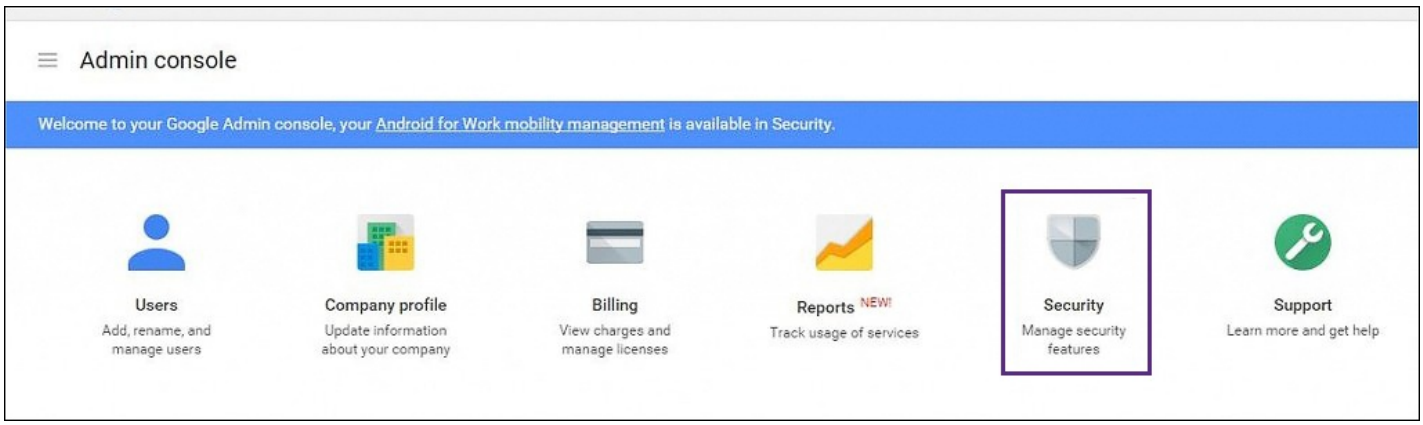
3. Klicken Sie auf der Seite **Certificates** in der Liste der Zertifikate auf das SAML-Zertifikat.



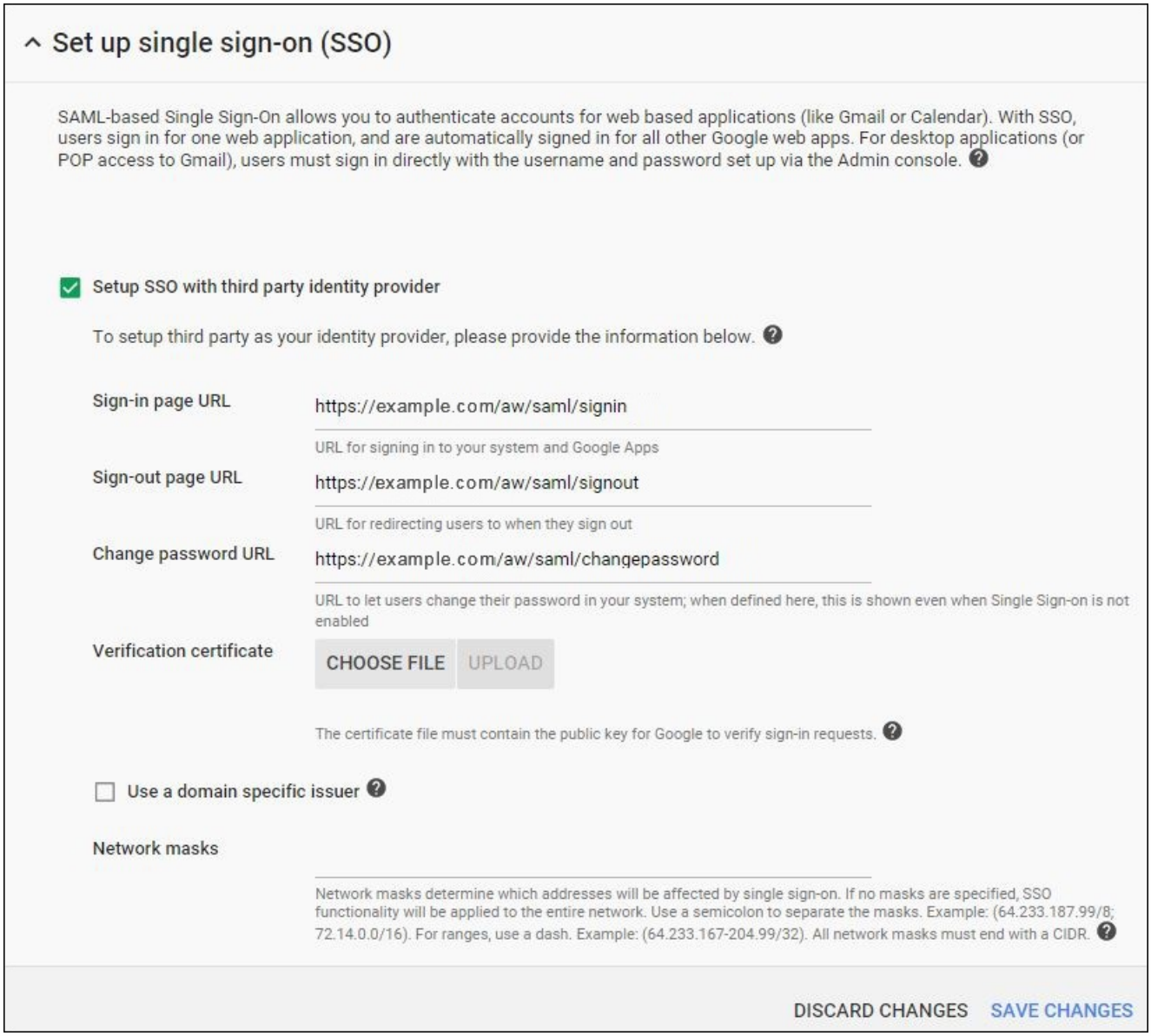
4. Klicken Sie auf **Export** und speichern Sie das Zertifikat auf Ihrem Computer.

5. Melden Sie sich mit Ihren Administratoranmeldeinformationen für Android for Work beim Google-Verwaltungsportal unter https://admin.google.com an.

6. Klicken Sie auf **Security**.



7. Klicken Sie unter **Security** auf **Set up single sign-on (SSO)** und konfigurieren Sie die folgenden Einstellungen:

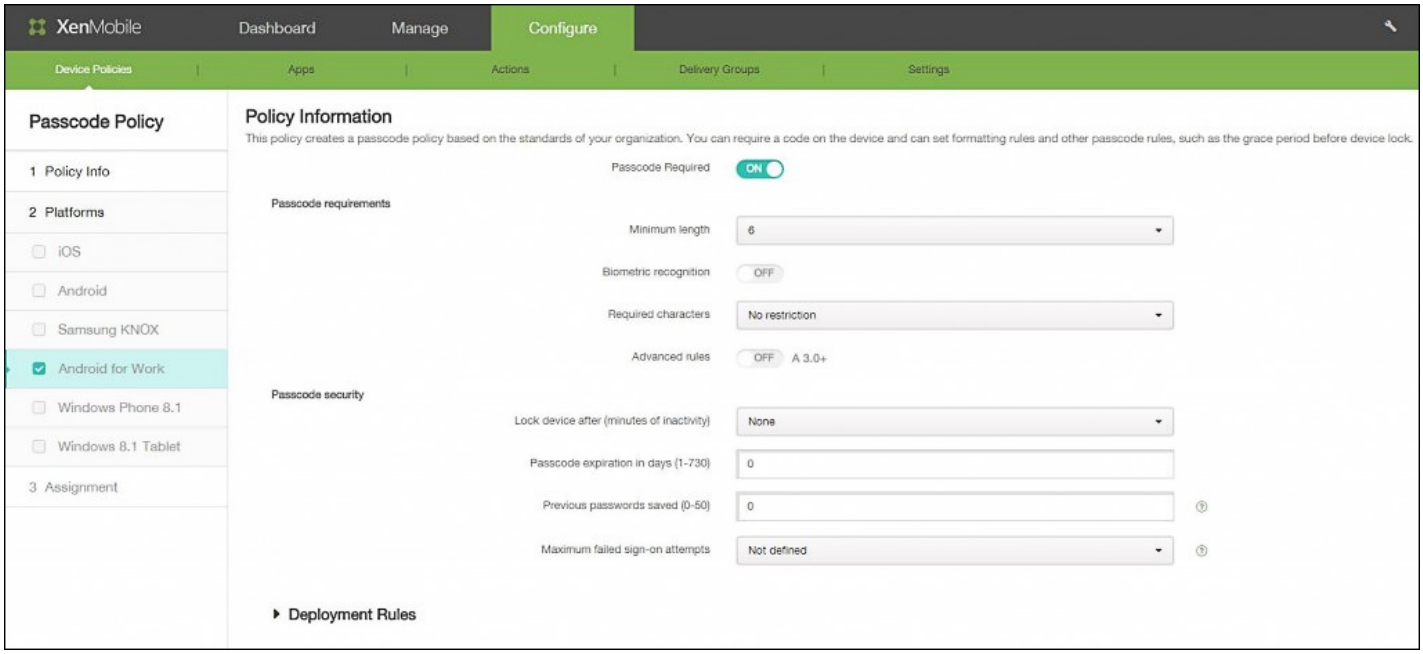


- **Sign-in page URL** Geben Sie die URL der Seite an, auf der sich die Benutzer bei Ihrem System und Google-Apps anmelden. Beispiel: https:///aw/saml/signin.
- **Sign-out page URL**: Geben Sie die URL an, an die die Benutzer weitergeleitet werden, wenn sie sich abmelden. Beispiel: https:///aw/saml/signout.
- **Change password URL**: Geben Sie die URL der Seite an, auf der die Benutzer ihr Kennwort in Ihrem System ändern können. Beispiel: https:///aw/saml/changepassword. Wenn dies hier definiert wird, können Benutzer es sehen, selbst wenn Single Sign-On nicht verfügbar ist.
- **Verification certificate**: Klicken Sie auf CHOOSE FILE und navigieren Sie zu dem aus XenMobile exportierten SAML-Zertifikat.

8. Klicken Sie auf **SAVE CHANGES**.

Einrichten einer Android for Work-Richtlinie

Sie können eine beliebige Richtlinie einrichten, empfehlenswert ist jedoch die Einrichtung einer Passcode-Richtlinie, sodass Benutzer bei der ersten Registrierung einen Passcode auf ihrem Gerät festlegen müssen.



Die grundlegenden Schritte zum Einrichten einer Geräterichtlinie sind folgende:

1. Melden Sie sich bei der XenMobile 10.1-Konsole an.

2. Klicken Sie auf **Configure->Device Policies**.

3. Klicken Sie auf **Add** und wählen Sie dann im Dialogfeld **Add a New Policy** die Richtlinie, die Sie hinzufügen möchten, aus (z. B. **Passcode**).

4. Füllen Sie die Seite **Policy Information** aus.

5. Klicken Sie auf **Android for Work** und konfigurieren Sie die Einstellungen für die Richtlinie.

6. Weisen Sie die Richtlinie einer Bereitstellungsgruppe zu.

Weitere Informationen zum Einrichten von Geräterichtlinien finden Sie unter Geräterichtlinien.

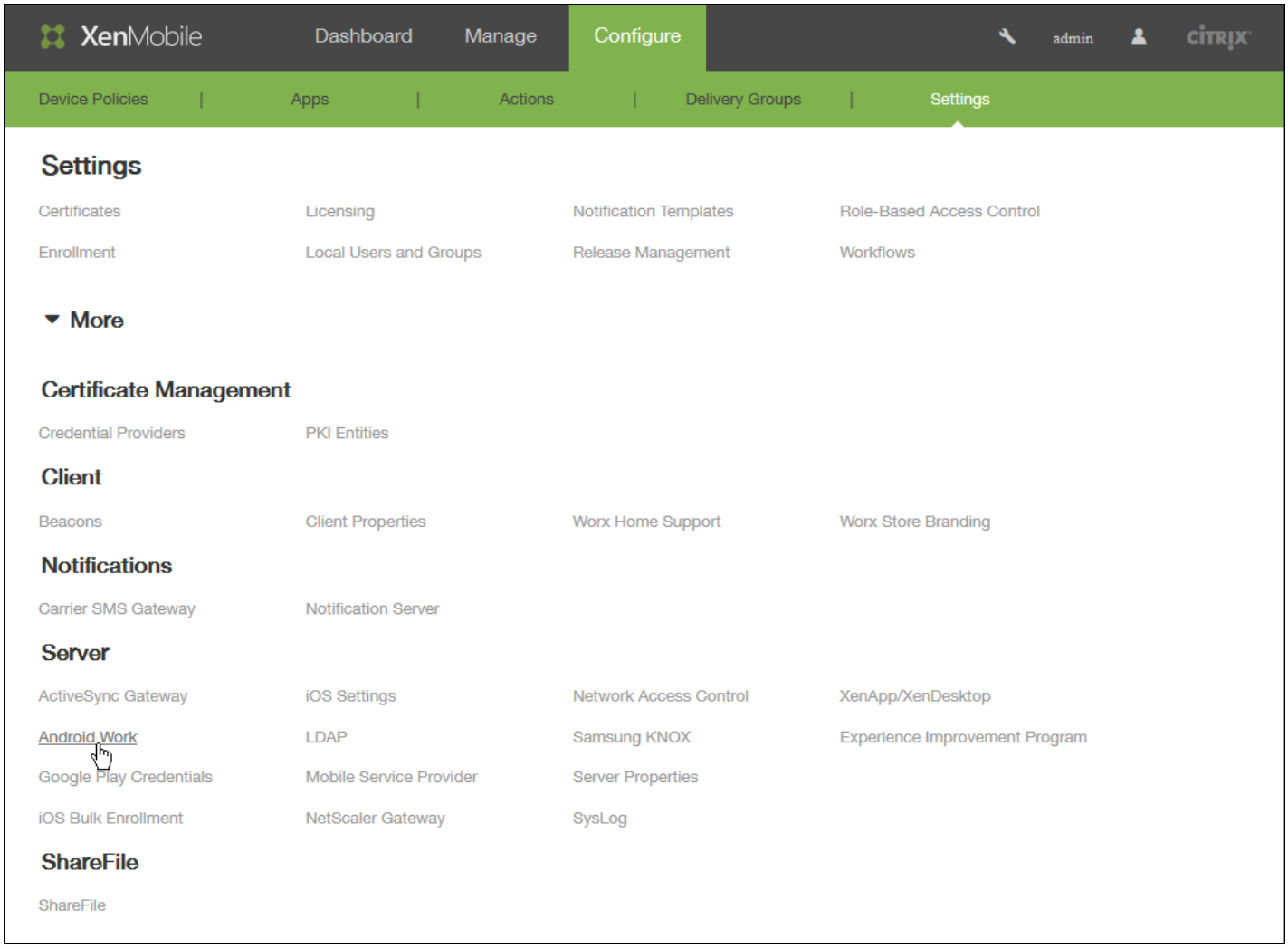
Die Benutzer können nun die Worx Home-App aus dem Google Play Store laden und ihre Geräte bei XenMobile registrieren (stellen Sie sicher, dass der Benutzerprinzipalname für die Registrierung verwendet wird). Nach erfolgter Geräteregistrierung installiert Worx Home das Android for Work-Profil, sodass die Benutzer auf ihre Android for Work-Apps zugreifen können. Die Benutzer werden u. U. aufgefordert, ihre Geräte während dieses Vorgangs zu verschlüsseln, bevor sie fortfahren können.

Konfigurieren von Android for Work-Kontoeinstellungen

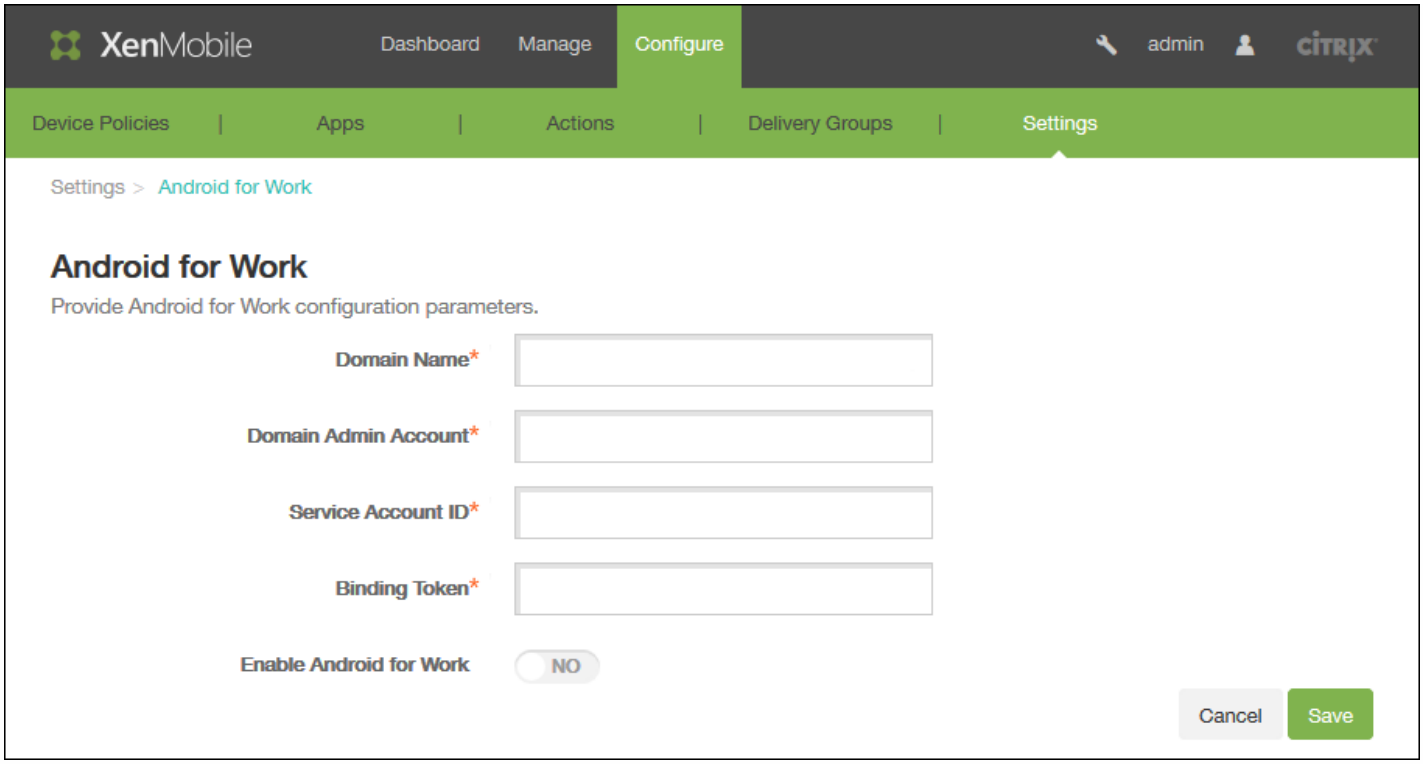
Nov 12, 2015

Bevor Sie Android for Work-Apps und Richtlinien auf Benutzergeräten verwalten können, müssen Sie eine Android for Work-Domäne und Kontoinformationen in XenMobile einrichten. Zunächst müssen Sie Android for Work-Einrichtungsaufgaben auf Google zum Einrichten eines Domänenadministrators erledigen und eine Dienstkonten-ID sowie ein Bindungstoken anfordern. Weitere Informationen zu den Android for Work-Einrichtungsaufgaben auf Google finden Sie unter Verwalten von Geräten mit Android for Work.

1. Klicken Sie in der XenMobile-Konsole auf **Configure > Settings**.



2. Erweitern Sie **More** und klicken Sie unter **Server** auf **Android for Work**. Die Seite **Android for Work** wird angezeigt.



3. Konfigurieren Sie auf der Seite **Android for Work** die folgenden Einstellungen:

- **Domain Name**: Geben Sie Ihren Domänennamen ein.
- **Domain Admin Account**: Geben Sie Ihren Domänenadministrator-Benutzernamen ein.
- **Service Account ID**: Geben Sie die ID Ihres Google-Dienstkontos ein.
- **Binding Token**: Geben (oder fügen) Sie das Bindungstoken ein, das Sie von Google bei der Einrichtung Ihres Android for Work-Kontos erhalten haben.
- **Enable Android for Work**: Wählen Sie aus, ob Android for Work aktiviert werden soll.

4. Klicken Sie auf **Save**.

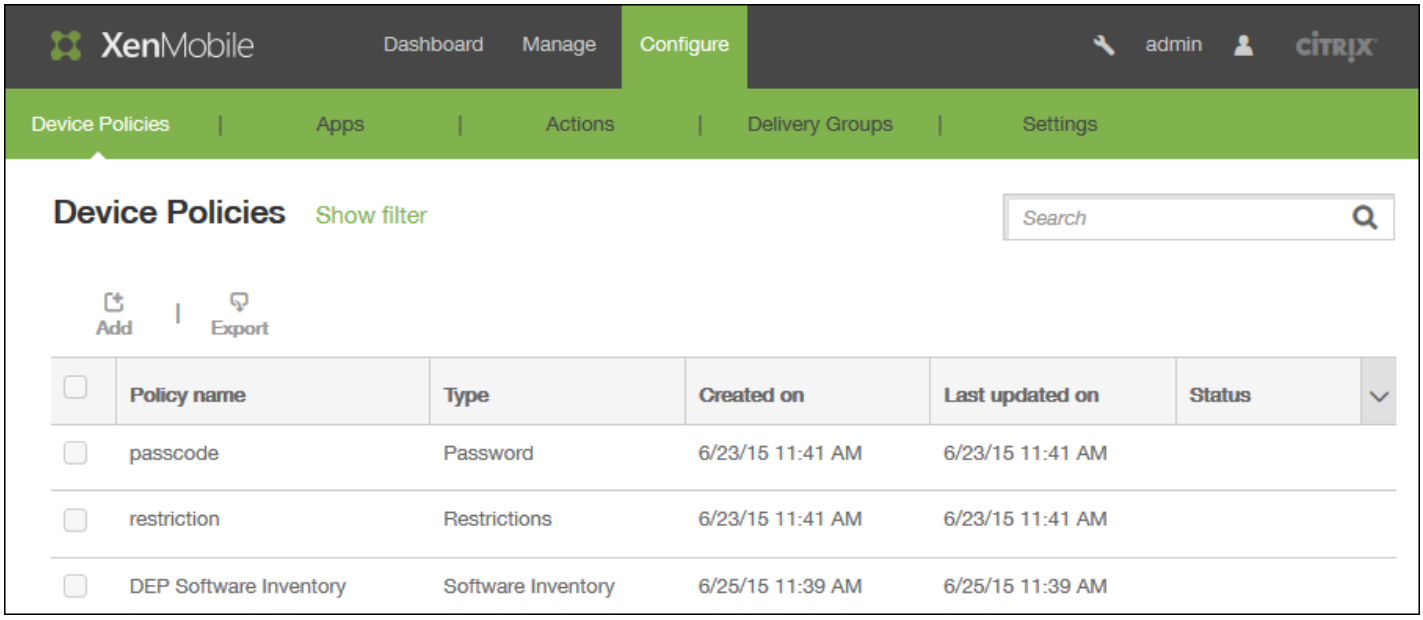
Einschränkungsrichtlinie für Android for Work-Apps

Nov 12, 2015

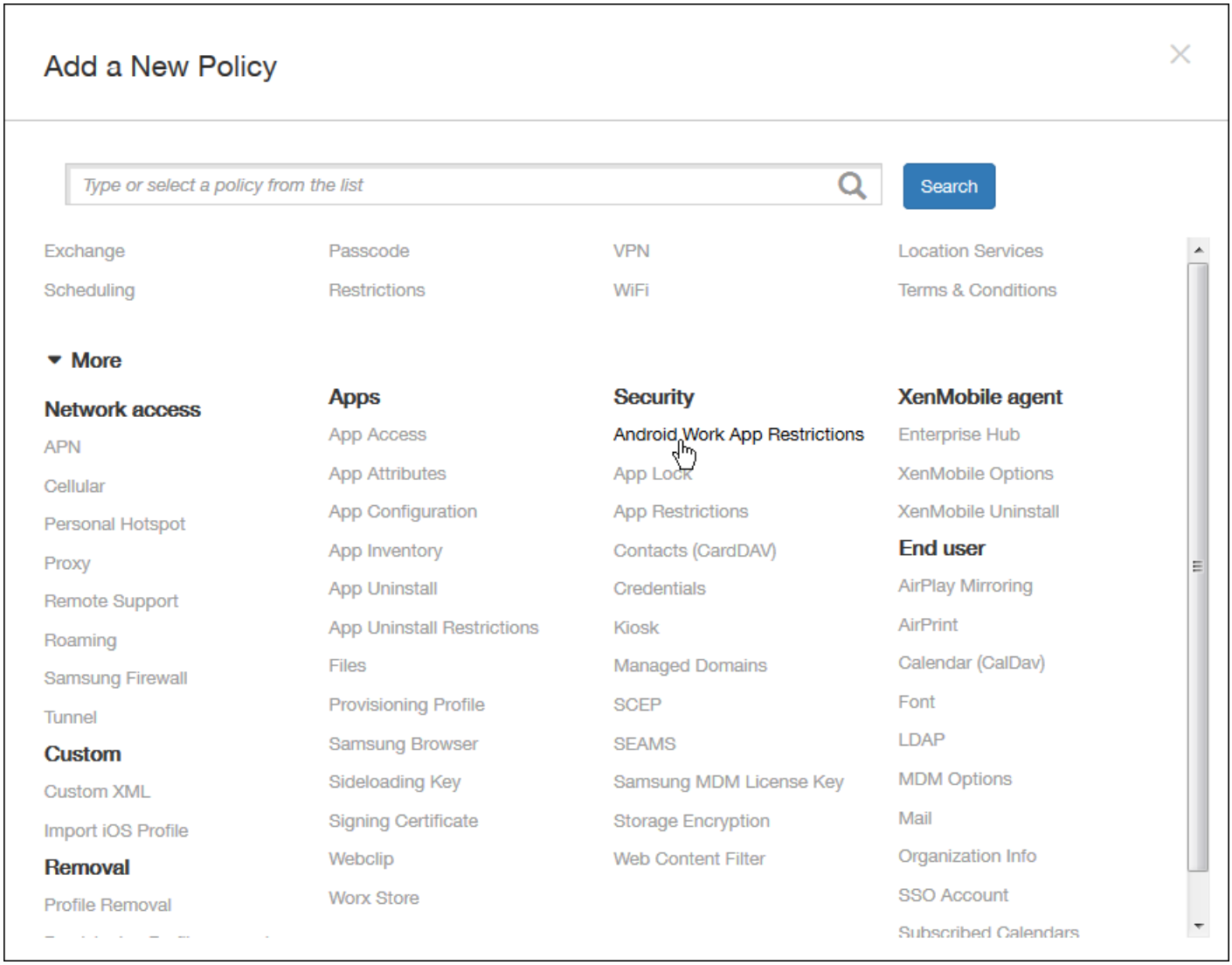
Sie können Einschränkungen für Android for Work-Apps ändern. Hierfür müssen jedoch die folgenden Vorbereitungen getroffen werden:

- Einrichtung von Android for Work auf Google Weitere Informationen finden Sie unter Verwalten von Geräten mit Android for Work.
- Erstellen einer Reihe von Google Play-Anmeldeinformationen Weitere Informationen finden Sie unter Google Play-Anmeldeinformationen.
- Konfigurieren der Android for Work-Kontoeinstellungen Weitere Informationen finden Sie unter Konfigurieren der Android for Work-Kontoeinstellungen.
- Hinzufügen von Android for Work-Apps in XenMobile Weitere Informationen finden Sie unter Hinzufügen von Apps in XenMobile.

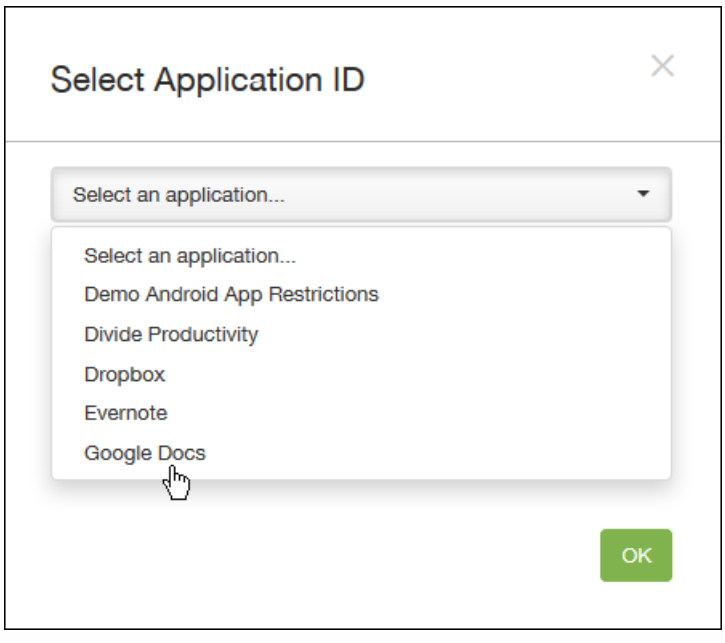
1. Klicken Sie in der XenMobile-Konsole auf **Configure > Device Policies**. Die Seite **Device Policies** wird angezeigt.



2. Klicken Sie auf **Add**, um eine neue Richtlinie hinzuzufügen. Die Seite **Add a New Policy** wird angezeigt.

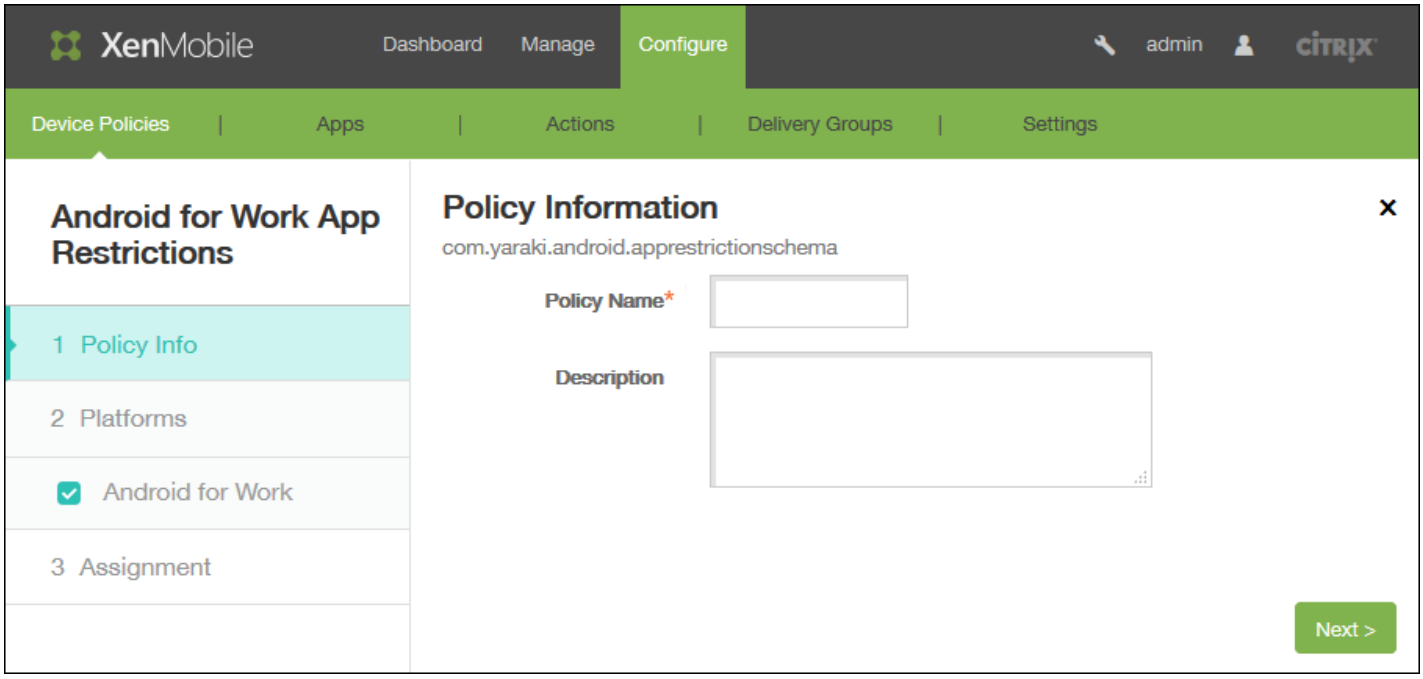


3. Klicken Sie auf der Seite **Add a New Policy** auf **More** und dann unter **Security** auf **Android for Work App Restrictions**. Ein Dialogfeld wird angezeigt, in dem Sie zum Auswählen der App aufgefordert werden.



4. Wählen Sie in der Liste die App aus, auf die Sie Einschränkungen anwenden möchten, und klicken Sie dann auf **OK**.

- Wenn XenMobile keine Android for Work-Apps hinzugefügt wurden, können Sie nicht fortfahren. Weitere Informationen zum Hinzufügen von Apps in XenMobile finden Sie unter Hinzufügen von Apps in XenMobile.
- Wenn der App keine Einschränkungen zugeordnet sind, wird eine entsprechende Benachrichtigung angezeigt. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.
- Wenn der App Einschränkungen zugeordnet sind, wird die Seite **Android for Work App Restrictions Policy** angezeigt.

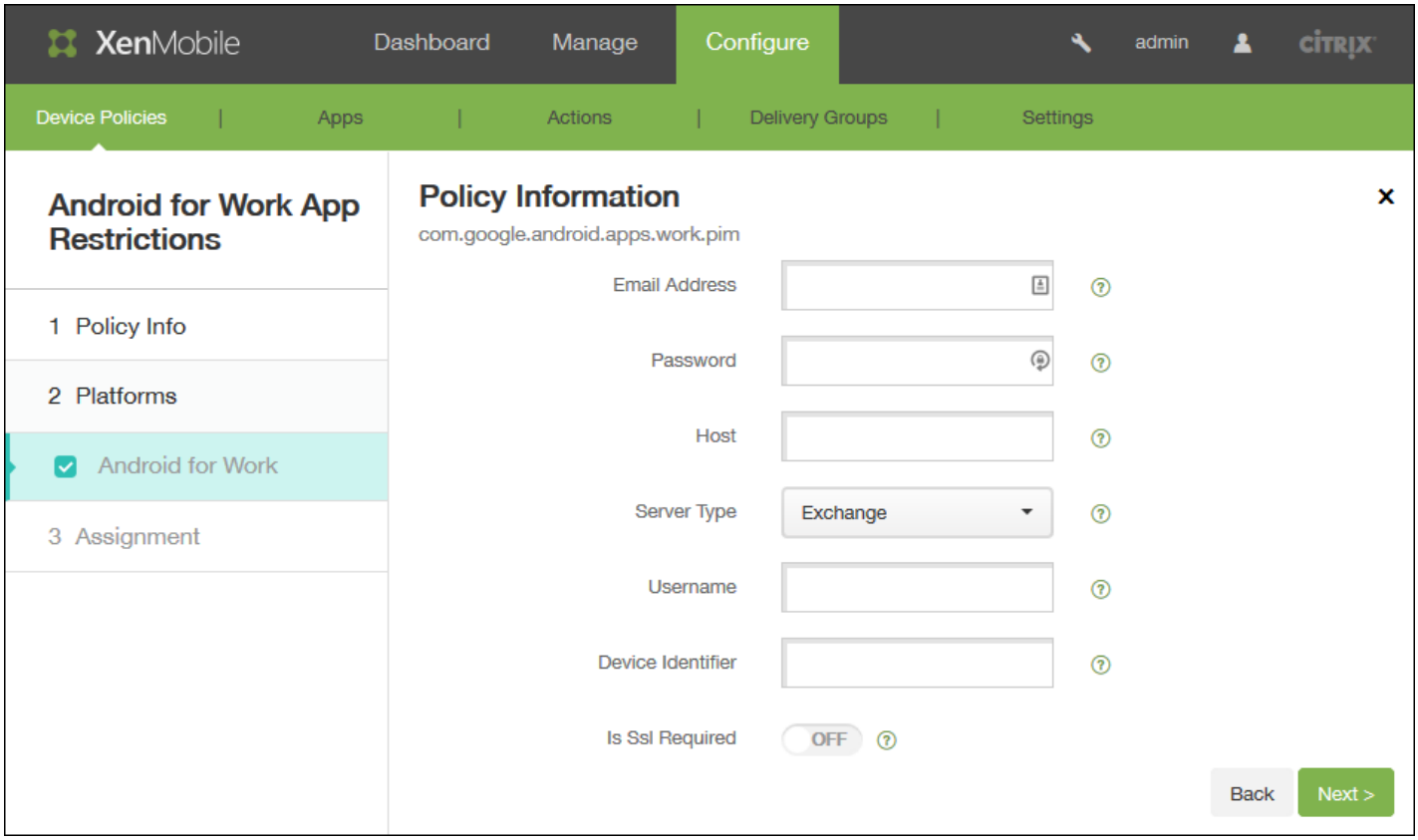


Geben Sie im Bereich **Policy Information** die folgenden Informationen ein:

- **Policy Name**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Description**: Geben Sie optional eine Beschreibung der Richtlinie ein.

6. Klicken Sie auf **Next**. Die Seite **Policy Platforms** wird angezeigt.

7. Konfigurieren Sie unter **Platforms** im Bereich **Android for Work** die Einstellungen für die ausgewählte App. Welche Einstellungen angezeigt werden, hängt von den Einschränkungen ab, die der ausgewählten App zugeordnet sind. Die folgende Abbildung zeigt einige der für die Google Docs-App verfügbaren Optionen.



Erweitern Sie **Deployment Rules** und konfigurieren Sie folgende Einstellungen:

Standardmäßig wird die Registerkarte **Base** angezeigt.

- Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.

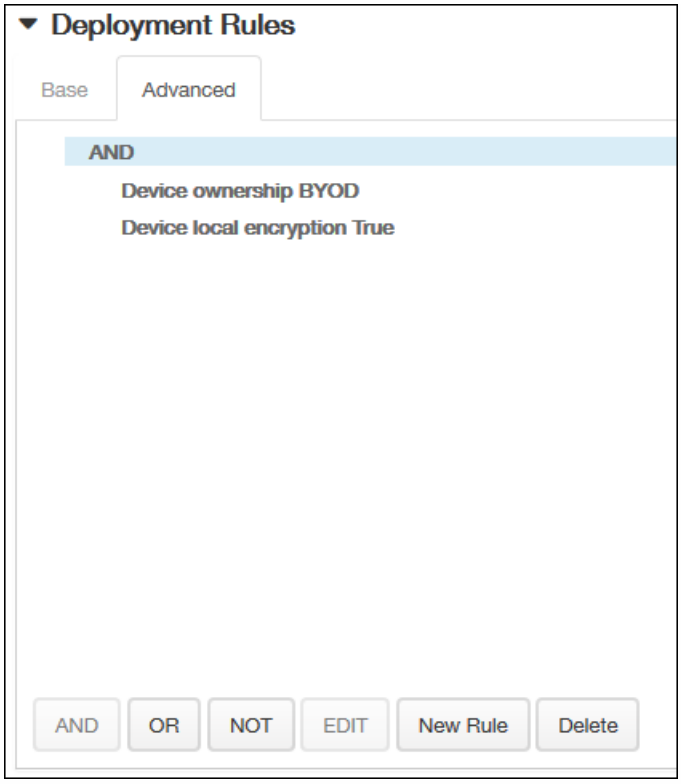
i. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist **All**.

ii. Klicken Sie auf **New Rule**, um Bedingungen zu definieren.

iii. Klicken Sie in der Liste auf Bedingungen wie **Device ownership** oder **BYOD** (siehe Abbildung oben).

iv. Klicken Sie erneut auf **New Rule**, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.

- Klicken Sie auf die Registerkarte **Advanced**, um die Regeln mit booleschen Optionen zu kombinieren.



Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

- Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.

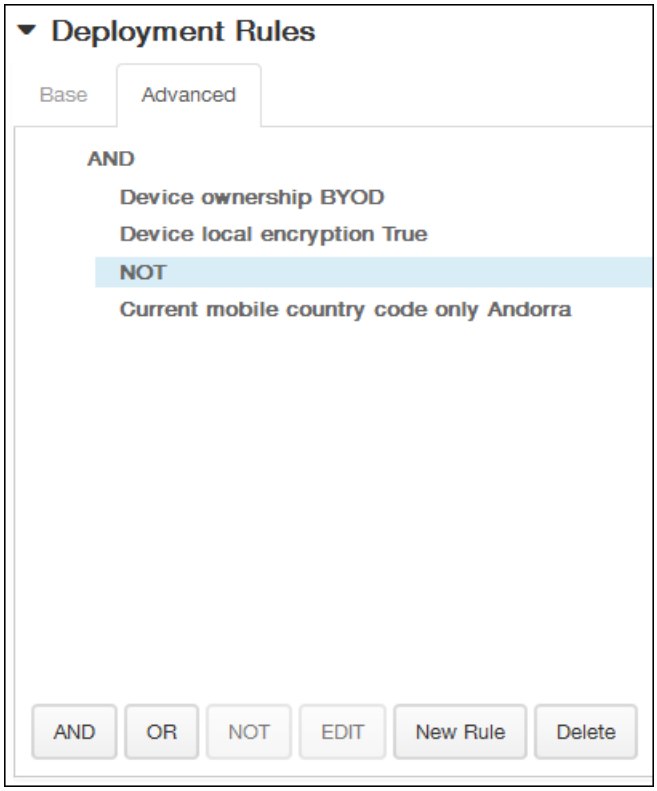
i. Klicken Sie auf **AND**, **OR** oder **NOT**.

ii. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.

Sie können jederzeit auf eine Bedingung und dann auf **EDIT** klicken, um die Bedingung zu ändern, oder auf **Delete**, um die Bedingung zu löschen.

iii. Klicken Sie erneut auf **New Rule**, wenn Sie weitere Bedingungen hinzufügen möchten.

In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.

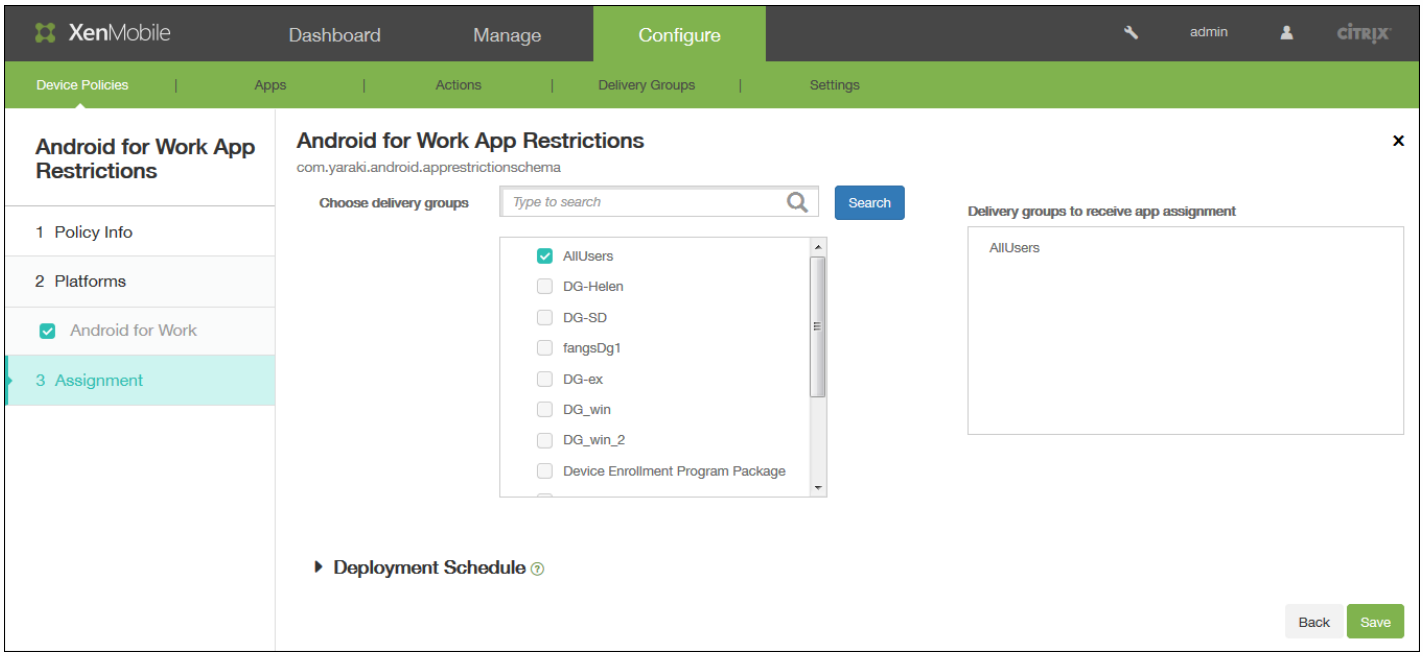


9. Klicken Sie auf **Next**.

Die Seite **Zuweisung** für die App-Einschränkungsrichtlinie für Android for Work wird angezeigt.

Machen Sie neben **Choose delivery groups** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus.

Diese ausgewählten Gruppen werden in der Liste **Delivery groups to receive app assignment** angezeigt.



Erweitern Sie **Deployment Schedule** und konfigurieren Sie folgende Einstellungen:

- Klicken Sie neben **Deploy** auf **ON**, um die Bereitstellung zu planen, oder auf **OFF**, um die Bereitstellung zu verhindern. Die

Standardeinstellung ist **ON**. Wenn Sie **OFF** auswählen, müssen keine anderen Optionen konfiguriert werden.

- Klicken Sie neben **Deployment schedule** auf **Now** oder **Later**. Die Standardeinstellung ist **Now**.
- Wenn Sie **Later** auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Deployment condition** auf **On every connection** oder auf **Only when previous deployment has failed**. Die Standardeinstellung ist **On every connection**.
- Klicken Sie neben **Deploy for always-on connection** auf **ON** oder **OFF**. Die Standardeinstellung ist **OFF**.

Hinweis

Diese Option gilt, wenn Sie unter "Settings > Server Properties" den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von "Deploy for always-on connection", denn diese Option gilt nicht für iOS.

Konfigurieren von Bereitstellungsregeln

Jul 27, 2016

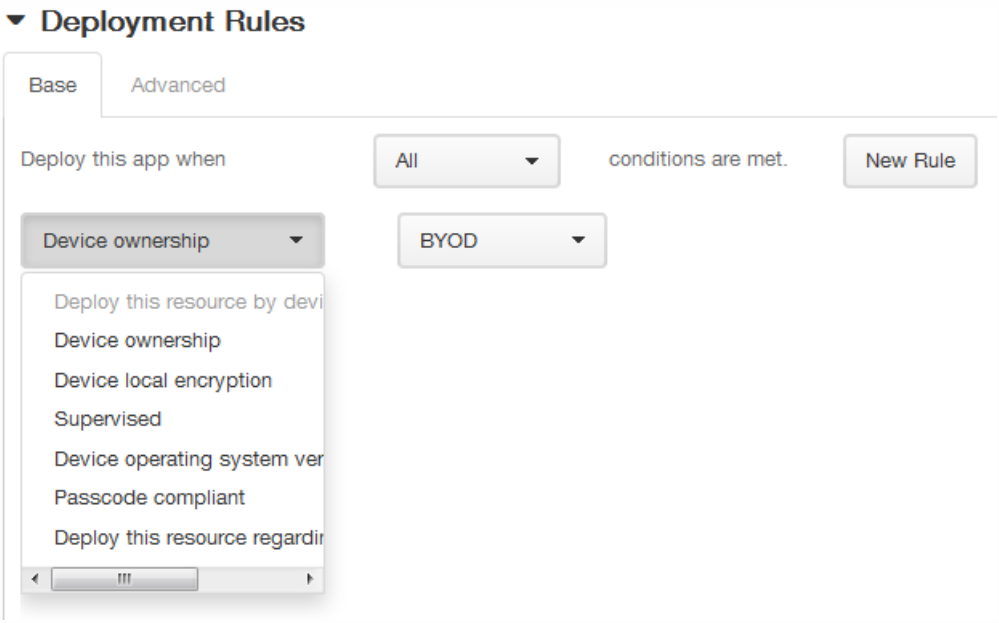
In diesem Abschnitt wird Folgendes beschrieben:

- Bereitstellungsregeln sind Parameter, die Auswirkungen auf das Bereitstellungsergebnis eines Pakets haben.
- Bereitstellungszeitpläne umfassen Optionen, die bestimmen, wann XenMobile Pakete auf einem Gerät per Push bereitstellt.

Konfigurieren von Bereitstellungsregeln

Bereitstellungsregeln sind Parameter, die Auswirkungen auf das Bereitstellungsergebnis eines Pakets haben. Sie können Bereitstellungsregeln für Geräteeigenschaften, Apps und Aktionen angeben. XenMobile verwendet die Bereitstellungsregeln, die Sie für Geräteigenschaften angeben zum Filtern von Richtlinien, Apps, Aktionen und Bereitstellungsgruppen beim Bestimmen die Bereitstellungsreihenfolge für ein Paket. Weitere Informationen finden Sie unter Bereitstellungsreihenfolge.

Sie können eine Paketbereitstellung basierend auf einer bestimmten Betriebssystemversion, auf einer bestimmten Hardwareplattform oder einer anderen Kombination durchführen. Dieser Assistent zum Hinzufügen und Bearbeiten von Geräteeigenschaften, Apps und Aktionen hat einen einfachen und einen erweiterten Editor für Regeln. Der erweiterte Editor ist ein formfreier Editor. Die Abbildung unten zeigt den Bildschirm mit den Bereitstellungsregeln, den Sie beim Hinzufügen oder Bearbeiten einer App aufrufen können:



Einfache Bereitstellungsregeln

Einfache Bereitstellungsregeln bestehen aus vordefinierten Tests und daraus hervorgehenden Aktionen. Soweit möglich sind die Ergebnisse in die Mustertests integriert. Basiert beispielsweise eine Paketbereitstellung auf einer Hardwareplattform, werden alle vorhandenen bekannten Plattformen in den entsprechenden Test eingetragen, sodass Zeitaufwand und mögliche Fehlerquellen bei der Regelerstellung deutlich reduziert werden.

Klicken Sie auf **Neue Regel**, um einem Paket eine Regel hinzuzufügen.

Hinweis: Der Regelassistent enthält weitere testspezifische Informationen.

Zum Erstellen einer Regel wählen Sie eine Regelvorlage und eine Bedingungsart aus und passen die Regel dann an. Zum Anpassen der Regel gehört das Ändern der Beschreibung. Wenn Sie die Einstellungen konfiguriert haben, fügen Sie die Regel dem Paket hinzu.

Sie können beliebig viele Regeln hinzufügen. Das Paket wird bereitgestellt, wenn alle Regeln erfüllt sind.

Erweiterte Bereitstellungsregeln

Wenn Sie auf die Registerkarte **Erweitert** klicken, wird der Editor für erweiterte Regeln angezeigt.

In diesem Modus können Sie die Beziehung zwischen den Regeln festlegen. Die Operatoren **UND**, **ODER** und **NICHT** sind verfügbar.

Konfigurieren von Bereitstellungszeitplänen

XenMobile verwendet den Bereitstellungszeitplan, den Sie für Aktionen, Apps und Geräterichtlinien angeben, um die Bereitstellung dieser Elemente zu steuern. Sie können festlegen, dass eine Bereitstellung sofort, zu einem bestimmten Datum und einer bestimmten Uhrzeit oder basierend auf Bereitstellungsbedingungen stattfindet. Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

Wenn Sie die Optionen für den Bereitstellungszeitplan nicht ändern, werden Bereitstellungen auf allen Verbindungen sofort durchgeführt. Die Bereitstellungszeitplanoptionen:

Bereitstellen: Der Standardwert ist **EIN**. Wenn Sie die Bereitstellung verhindern möchten, legen Sie die Einstellung auf **AUS** fest.

Bereitstellungszeitplan: Der Standardwert ist **Jetzt**. Um eine Bereitstellungzeit anzugeben, wählen Sie **Später** und legen Sie ein Datum und eine Uhrzeit fest.

Bereitstellungsbedingung: Der Standardwert ist **Bei jeder Verbindung**. Zum Beschränken von Bereitstellungen legen Sie diese Einstellung auf **Nur bei Fehler in der vorherigen Bereitstellung** fest.

Bereitstellen für immer aktive Verbindungen: Der Standardwert ist **AUS**. Bei iOS- und Windows Mobile-Geräten: Wenn Sie auf dem Gerät für **Verbindungszeitplan** die Option **Immer** festlegen, müssen Sie die Einstellung für **Bereitstellen für immer aktive Verbindungen** in **EIN** ändern. Bei Android-Geräten: Für die XenMobile-Servereigenschaft **Hintergrundbereitstellung** muss **Bereitstellen für immer aktive Verbindungen** für jede auf Android-Geräten bereitgestellte Richtlinie auf **EIN** festgelegt werden.

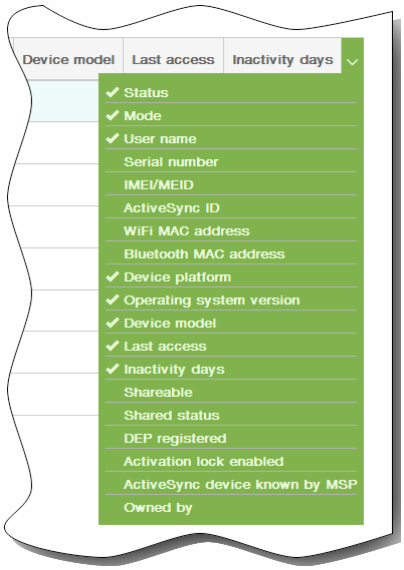
Hinzufügen von Geräten und Anzeigen von Gerätedetails

Oct 29, 2015

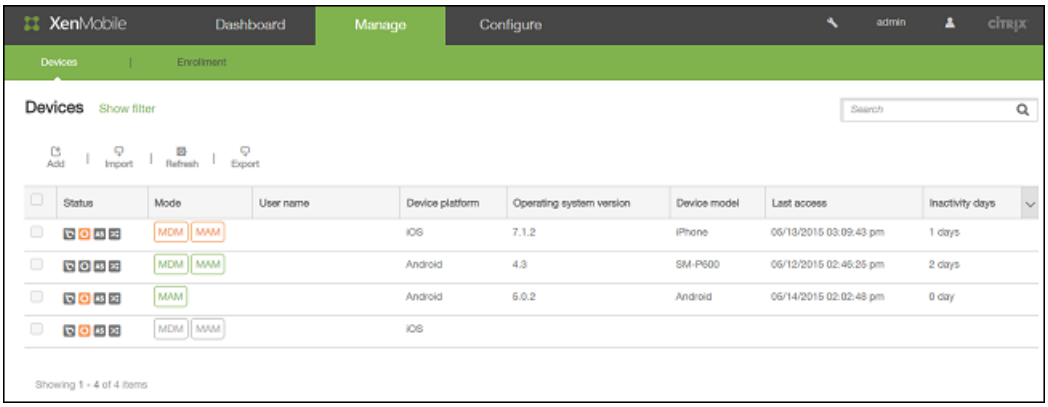
In der Repositorydatenbank auf dem XenMobile-Konsolenserver wird eine Liste der Mobilgeräte gespeichert. Jedes Mobilgerät ist durch eine eindeutige Seriennummer und/oder eine IMEI (International Mobile Station Equipment Identity) bzw. einen MEID (Mobile Equipment Identifier) gekennzeichnet. Sie können der XenMobile-Konsole Geräte manuell hinzufügen oder eine Liste mit Geräten aus einer Datei importieren. Siehe Geräte-Provisioningdateiformate.

Die Seite Devices der Konsole enthält eine Tabelle der Geräte mit folgenden Informationen: Status (Gerät ohne Jailbreak, Gerät nicht verwaltet, Active Sync-Gateway nicht verfügbar, kein Bereitstellungsfehler), Modus (MDM, MAM), Benutzername, Geräteplattform, Betriebssystemversion, Gerätemodell, letzter Zugriff und Inaktivität in Tagen.

Hinweis: Die oben genannten Tabellenspalten sind die Standardspalten. Sie können die Tabelle anpassen, indem Sie auf den Pfeil nach unten in der letzten Spaltenüberschrift klicken und dann die Spaltenüberschriften aktivieren, die in der Tabelle angezeigt werden sollen, bzw. diejenigen, die nicht angezeigt werden sollen, deaktivieren.

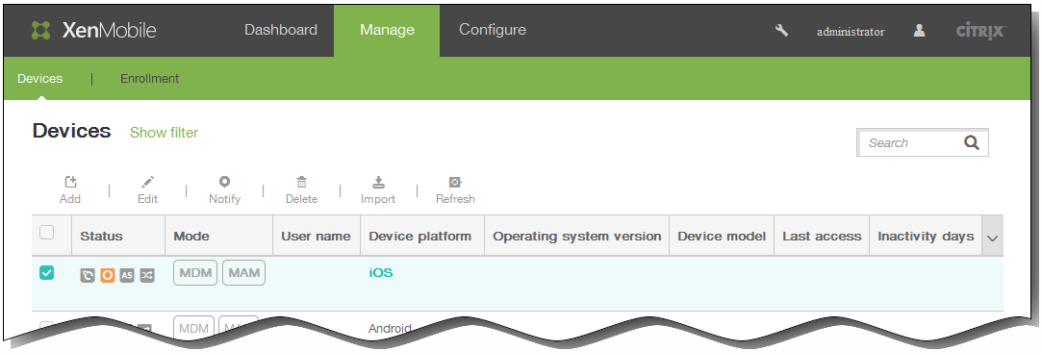


Sie können ein neues Gerät manuell durch Klicken auf Add oder per Import einer Provisioningdatei durch Klicken auf Import hinzufügen. Zum Aktualisieren der Tabelle klicken Sie auf Refresh.

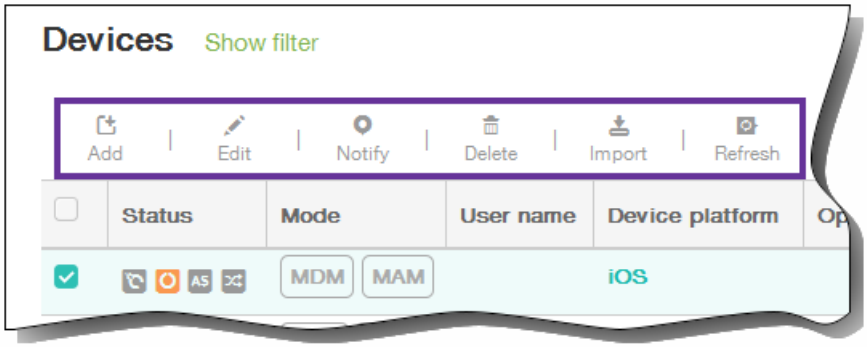


So fügen Sie Geräte manuell hinzu

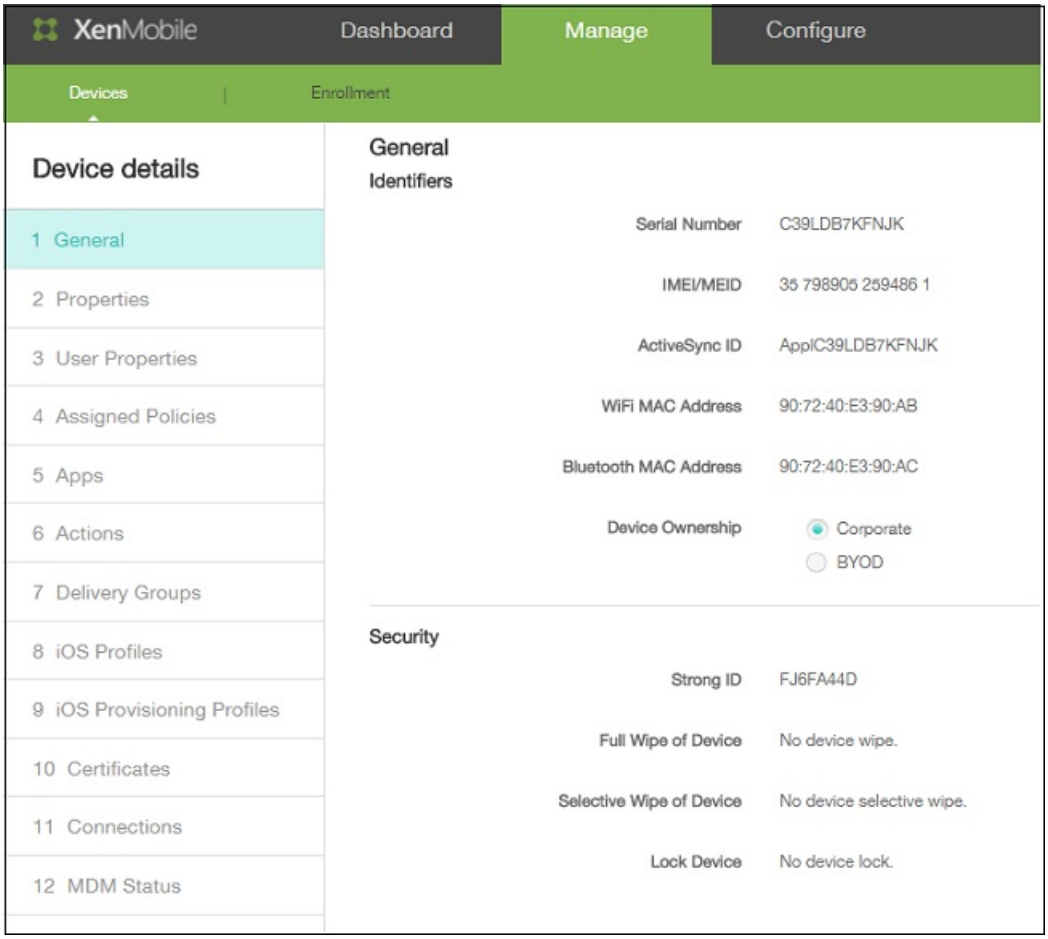
1. Klicken Sie in der XenMobile-Konsole auf ManageDevices und dann auf Add. Die Seite Add Device wird angezeigt.
2. Klicken Sie unter Select platform auf iOS, Android oder Symbian.
3. Geben Sie die folgenden Informationen ein:
   1. iOS: Geben Sie unter Serial Number die Seriennummer ein.
   2. Android: Geben Sie unter Serial Number die Seriennummer und die IMEI/MEID ein.
   3. Symbian: Geben Sie die IMEI/MEID ein.
4. Klicken Sie auf Add. Die Tabelle Devices wird angezeigt. Das hinzugefügte Gerät befindet sich am Ende der Liste.
5. Wählen Sie in der Liste das hinzugefügte Gerät aus und klicken Sie in dem nun angezeigten Menü auf Edit, um die Gerätedetails zu überprüfen.



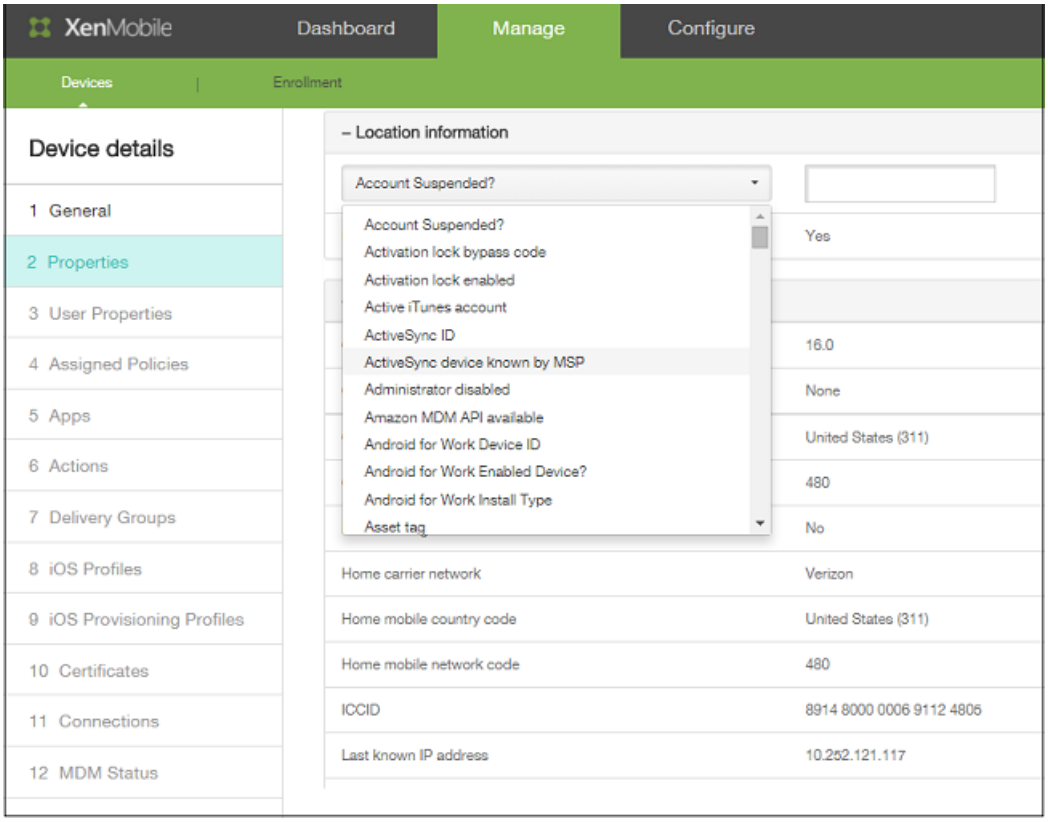
Hinweis: Wenn Sie das Kontrollkästchen neben einem Gerät auswählen, wird das Menü mit den Optionen oberhalb der Geräteliste eingeblendet. Wenn Sie auf eine andere Stelle im Eintrag klicken, wird es rechts neben dem Eintrag eingeblendet.



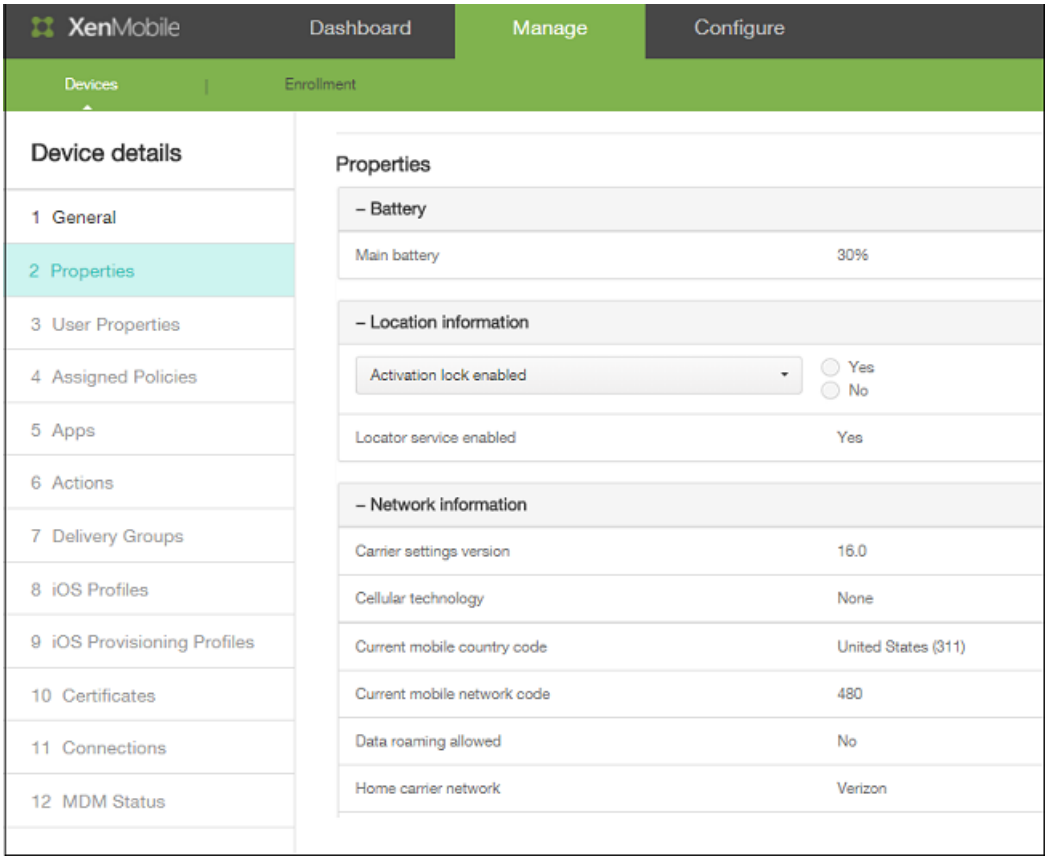
6. Prüfen Sie unter General Identifiers die angezeigten Informationen (welche Parameter angezeigt werden, hängt vom Plattformtyp ab): Seriennummer, IMEI/MEID, ActiveSync-ID, WiFi-MAC-Adresse, Bluetooth-MAC-Adresse, Geräteeigentümer: Corporate oder BYOD.



7. Prüfen Sie unter Security die angezeigten Informationen (welche Parameter angezeigt werden, hängt vom Plattformtyp ab): Strong ID, vollständige/selektive Datenlöschung, Gerätesperrung, Geräteentsperrung, Aufhebung der Eigentümerschaft, Umgehung der Aktivierungssperre, Einschränkungen für Löschen.
8. Klicken Sie auf Next, um Eigenschaften hinzuzufügen.
9. Klicken Sie auf der Seite Properties auf Add, um eine Liste der Eigenschaften anzuzeigen, die Sie für das Gerät bereitstellen können. Eine Liste der verfügbaren Eigenschaften wird angezeigt.



10. Wählen Sie in der Liste die gewünschte Eigenschaft aus und legen Sie deren Wert fest. Wählen Sie beispielsweise Activation lock enabled aus und legen Sie Yes oder No fest.
11. Nachdem Sie eine Eigenschaft konfiguriert haben, klicken Sie auf Done.
12. Wiederholen Sie die Schritte 9 bis 11 für jede Eigenschaft, die Sie bereitstellen möchten, und klicken Sie dann auf Next. Hinweis: Hinzugefügte Eigenschaften werden unter Properties angezeigt. Wenn Sie anschließend zur Seite Properties zurückkehren, werden die Eigenschaften separat in verschiedenen Kategorien angezeigt.



Der Bereich **Assigned Policies** und die nachfolgenden Bereiche enthalten zusammengefasste Informationen zu dem Gerät.

- Assigned Policies: zeigt die Anzahl der zugewiesenen bereitgestellten, ausstehenden und fehlgeschlagenen Richtlinien an. Für die einzelnen Richtlinien werden zudem Name, Typ und letzte Bereitstellung angezeigt
- Apps: zeigt die Anzahl der installierten, ausstehenden und fehlerhaften Apps im letzten Bestand an.
  - Für installierte Apps werden die folgenden Informationen angezeigt: Name, Eigentümerschaft, Version, Autor, Größe, installiert, ID und Typ.
  - Für ausstehende und fehlerhafte Apps werden die folgenden Informationen angezeigt: Name, letzte Bereitstellung, ID und Typ.
- Actions: zeigt die Anzahl der zugewiesenen bereitgestellten, ausstehenden und fehlgeschlagenen Aktionen an. Für jede Aktion werden Name und Datum der letzten Bereitstellung angezeigt.
- Delivery Groups: zeigt die Anzahl der erfolgreichen, ausstehenden und fehlerhaften Bereitstellungsgruppen an. Für jede Aktion werden Informationen zu Bereitstellungsgruppen und Zeit angezeigt. Außerdem werden detailliertere Informationen zur Bereitstellungsgruppe angezeigt, einschließlich Status, Aktion, Eigentümer und Datum.
- iOS Profiles (nur iOS-Geräte): zeigt den letzten iOS Profilbestand mit Namen, Typ, Unternehmen und Beschreibung an.
- Certificates: zeigt die Anzahl der gültigen, abgelaufenen und gesperrten Zertifikate mit Typ, Anbieter, Herausgeber, Seriennummer und Gültigkeitszeitraum an.
- Connections: zeigt den ersten und letzten Verbindungsstatus an. Für jede Verbindung werden zudem der Benutzername, die vorletzte Authentifizierung und die letzte Authentifizierung angezeigt.
- TouchDown (nur Android-Geräte): zeigt die letzte Geräteauthentifizierung und die letzte Benutzerauthentifizierung an. Es werden Name und Wert jeder angewendeten Richtlinie angezeigt.

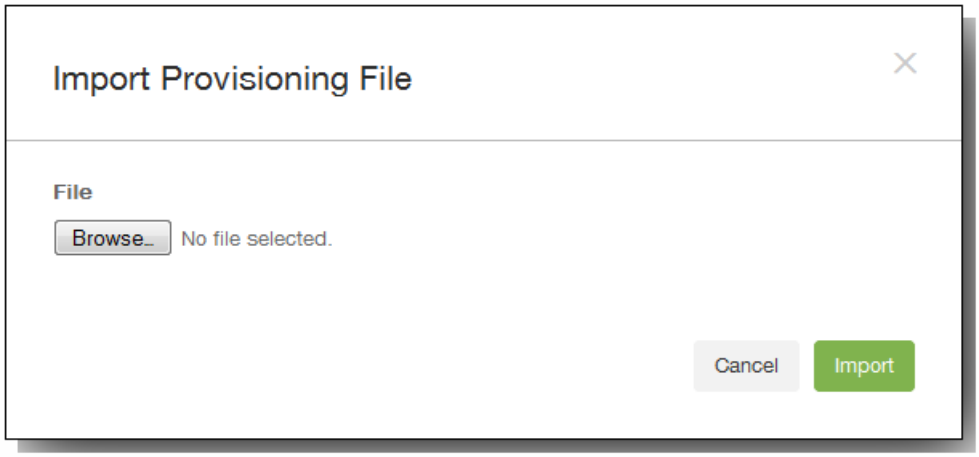
13. Klicken Sie auf Save.

So importieren Sie Geräte aus einer Provisioningdatei

Sie können die Datei eines Mobilfunkanbieters oder Geräteherstellers oder Ihre eigene Provisioningdatei importieren. Siehe

Geräte-Provisioningdateiformate.

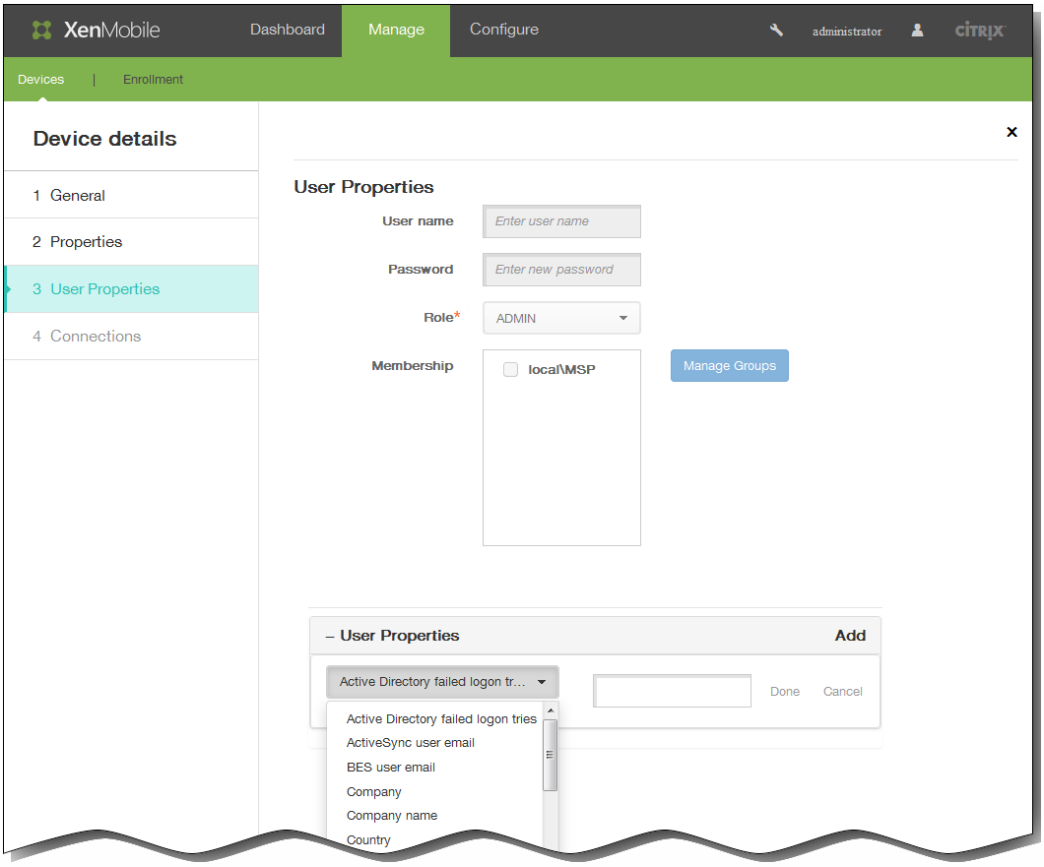
1. Klicken Sie im Menü oberhalb der Tabelle Devices auf Import. Das Dialogfeld Import Provisioning File wird angezeigt.



2. Klicken Sie zur Auswahl der zu importierenden Datei auf Browse und navigieren Sie zum Speicherort der Datei.
3. Klicken Sie auf Import. Die importierten Dateien werden der Tabelle Devices hinzugefügt.

So bearbeiten Sie Geräte

1. Wählen Sie das Gerät, das Sie bearbeiten möchten, aus und klicken Sie auf Edit. Die Seite Device Details wird angezeigt.
2. Das einzige Feld unter General Identifiers, das Sie ändern können, ist Device Ownership. Sie können Corporate oder BYOD auswählen.
3. Klicken Sie auf Next. Die Seite Properties wird angezeigt.
4. Verwenden Sie die Seite Properties zum Hinzufügen, Bearbeiten und Löschen von Geräten nach Bedarf.
   - Zum Bearbeiten klicken Sie auf die gewünschte Eigenschaft, ändern Sie deren Einstellungen und klicken Sie dann auf Done oder auf Cancel.
   - Zum Löschen einer Eigenschaft zeigen Sie auf die Auflistung und klicken Sie dann auf das X auf der rechten Seite. Das Element wird sofort gelöscht.
5. Klicken Sie auf Next. Die nächste Seite hängt von dem ausgewählten Gerät ab. Bei einigen Geräten wird User Properties, bei anderen Assigned Properties angezeigt.
6. Wird User Properties angezeigt, gehen Sie zum Hinzufügen, Bearbeiten oder Löschen der Benutzereigenschaften wie nachfolgend beschrieben vor. Die restlichen Seiten enthalten zusammengefasste Informationen für das Gerät. Eine Beschreibung dieser Seiten finden Sie unter So fügen Sie Geräte manuell hinzu.



Hinweis: Der obere Teil der Seite User Properties kann nicht bearbeitet werden.

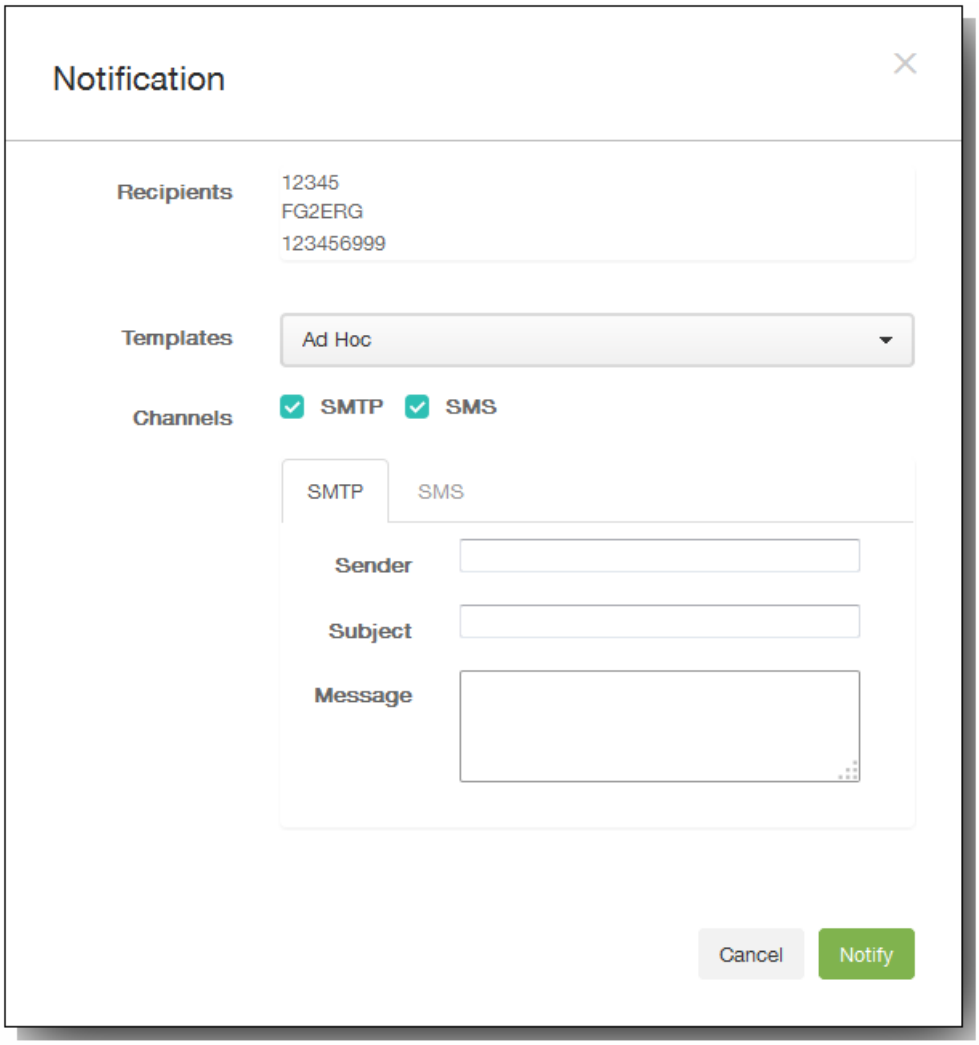
- Um eine Benutzereigenschaft hinzuzufügen, klicken Sie auf Add.
  - Klicken Sie in der Liste auf die gewünschte Eigenschaft, geben Sie den Wert ein und klicken Sie auf Done oder auf Cancel. Wiederholen Sie diese Schritte für jede Eigenschaft, die Sie hinzufügen möchten.
- Zum Bearbeiten klicken Sie auf die gewünschte Eigenschaft, ändern Sie deren Einstellungen und klicken Sie dann auf Done oder auf Cancel.
- Zum Löschen einer Eigenschaft zeigen Sie auf die Auflistung und klicken Sie dann auf das X auf der rechten Seite. Das Element wird sofort gelöscht.

7. Klicken Sie auf den folgenden Seiten mit zusammengefassten Informationen jeweils auf Next.
8. Klicken Sie auf der letzten Seite auf Save, um die Änderungen für das Gerät zu speichern.

So senden Sie eine Benachrichtigung an Geräte

Sie können Benachrichtigungen an Geräte über die Seite Devices senden. Weitere Informationen über Benachrichtigungen finden Sie unter So erstellen oder aktualisieren Sie Benachrichtigungsvorlagen in XenMobile.

1. Wählen Sie das oder die Geräte aus, an die Sie Benachrichtigung senden möchten.
2. Klicken Sie auf Notify. Das Dialogfeld Notification wird angezeigt. Unter Recipients sind alle Geräte aufgeführt, die die Benachrichtigung erhalten.



3. Konfigurieren Sie die folgenden Einstellungen:
   1. Templates: Klicken Sie in der Liste auf den gewünschten Benachrichtigungstyp.
      Die Felder Subject und Message werden mit den vorkonfigurierten Angaben aus der ausgewählten Vorlage (Ausnahme: Ad Hoc) ausgefüllt.

   2. Channels: Wählen Sie aus, wie die Benachrichtigung gesendet werden soll. Standardwert ist SMTP
      — und
      SMS.
      Sie können auf die Registerkarten SMTP und SMS klicken, um das jeweilige Nachrichtenformat anzuzeigen.

   3. Sender: Geben Sie optional eine Absender ein.
   4. Subject: Geben Sie für eine Ad Hoc-Nachricht einen Betreff ein.
   5. Message: Geben Sie für eine Ad Hoc-Nachricht einen Text ein.
4. Klicken Sie auf Notify.

So löschen Sie Geräte

1. Wählen Sie in der Tabelle Devices die Geräte aus, die Sie löschen möchten.
2. Klicken Sie auf Delete. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie noch einmal auf Delete.
   Wichtig: Sie können diesen Vorgang nicht rückgängig machen.

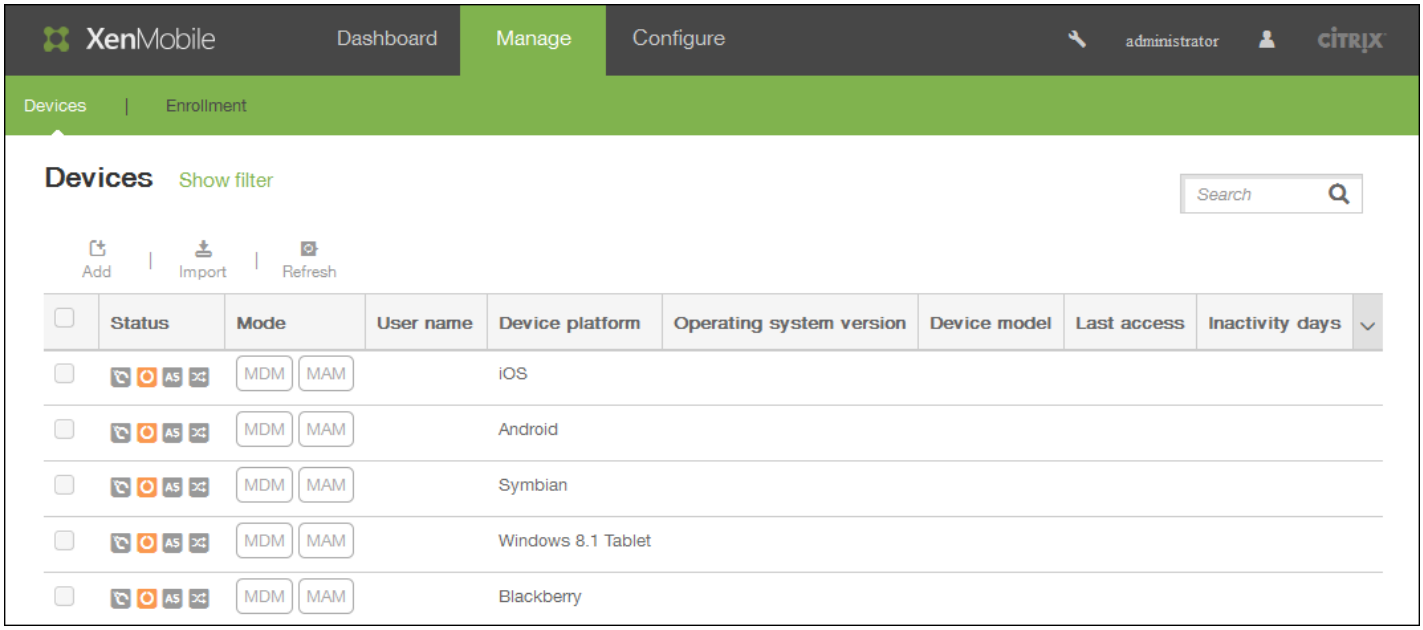
So sperren Sie ein iOS-Gerät

Nov 20, 2015

Sie können ein iOS-Gerät sperren und eine entsprechende Nachricht und Telefonnummer auf dem Sperrbildschirm anzeigen lassen. Dieses Feature wird für iOS 7- und iOS 8-Geräte unterstützt.

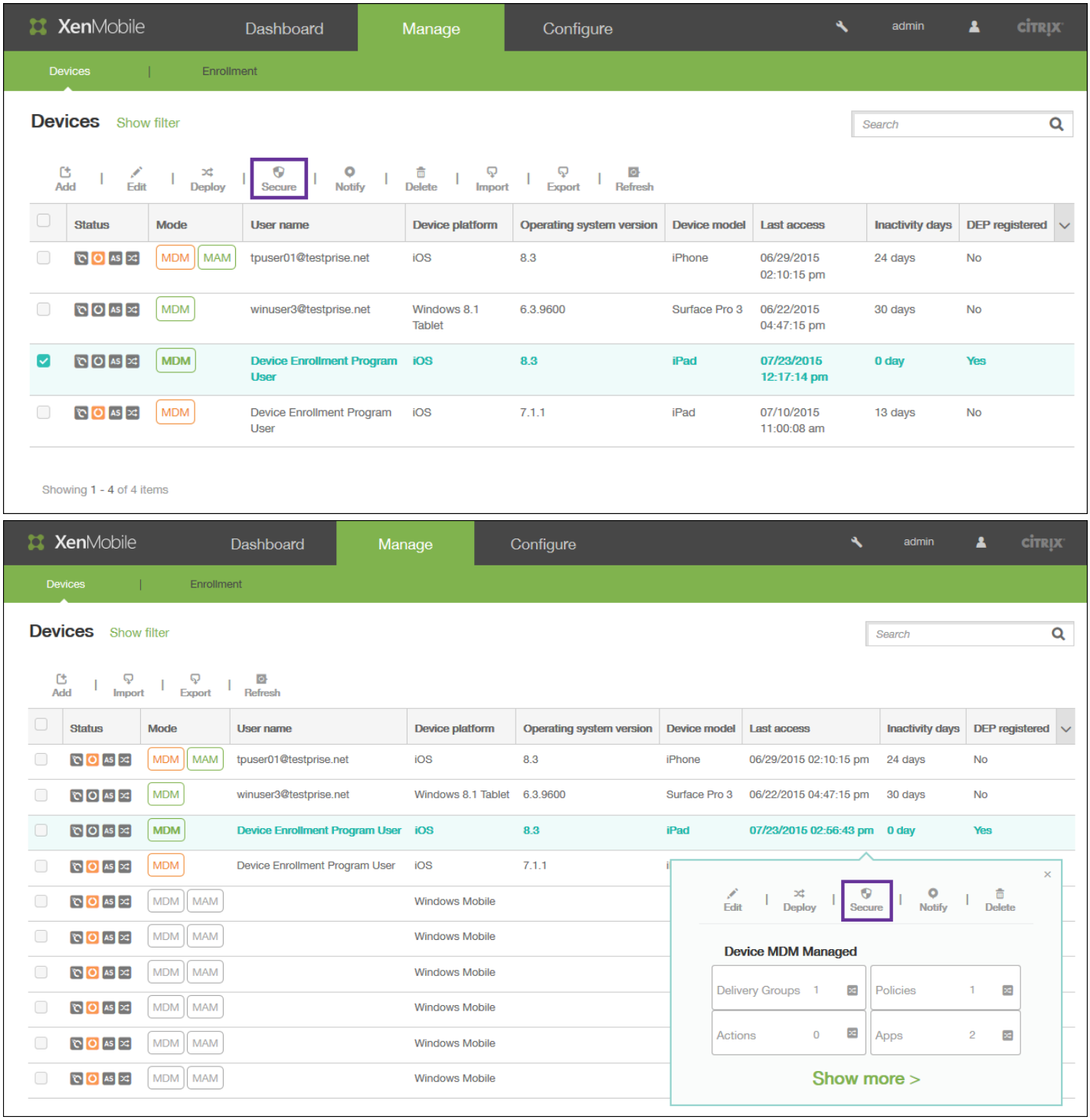
Wenn Sie sich für die Anzeige einer Nachricht und Telefonnummer auf dem Sperrbildschirm entscheiden, werden diese nur dann angezeigt, wenn Sie die Passcode-Richtlinie in der XenMobile-Konsole festgelegt oder wenn Benutzer den Passcode manuell auf Geräten aktiviert haben.

1. Klicken Sie in der XenMobile-Konsole auf **Manage > Devices**. Die Seite **Devices** wird angezeigt.

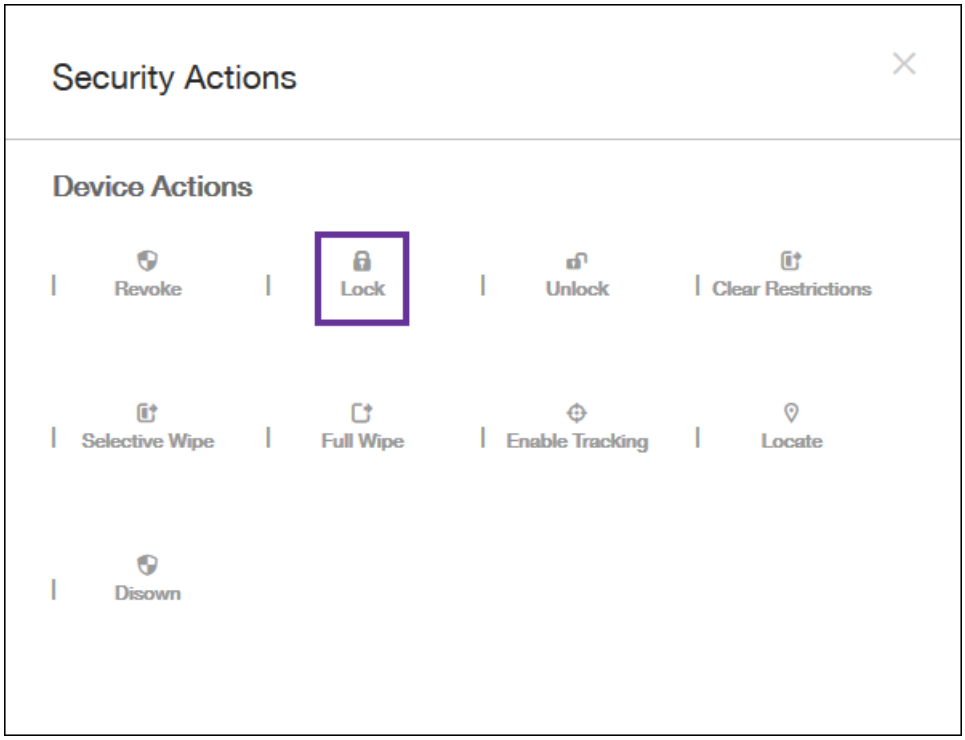


2. Wählen Sie das iOS-Gerät aus, das Sie sperren möchten.

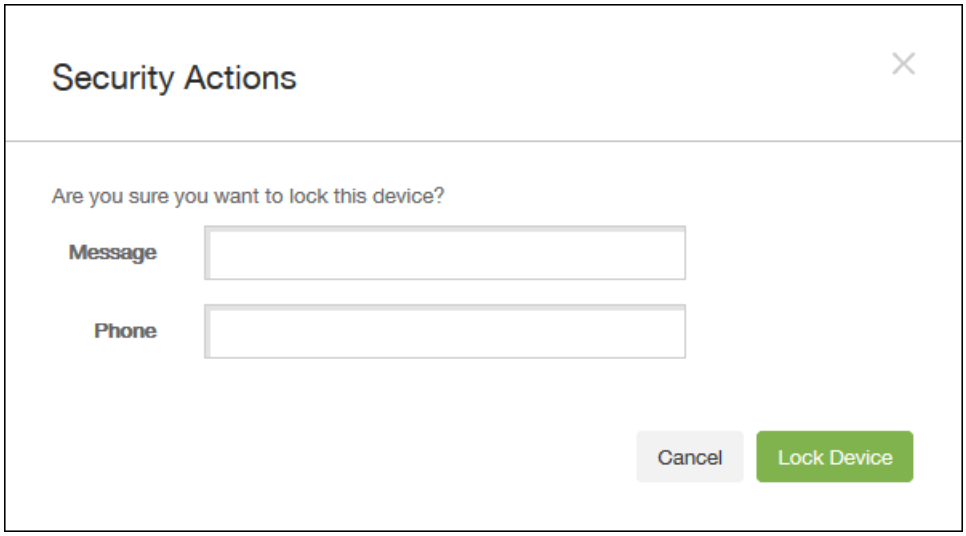
Wenn Sie das Kontrollkästchen neben einem Gerät auswählen, wird das Menü mit den Optionen oberhalb der Geräteliste eingeblendet. Wenn Sie auf eine andere Stelle im Eintrag klicken, wird es rechts neben dem Eintrag eingeblendet.



3. Wählen Sie im Menü "Options" **Secure**. Das Dialogfeld **Security Actions** wird angezeigt.



4. Wählen Sie **Lock**. Das Bestätigungsdialogfeld **Security Actions** wird angezeigt.



5. Geben Sie optional eine Meldung und Telefonnummer ein, die auf dem Sperrbildschirm des Geräts angezeigt werden sollen.

6. Klicken Sie auf **Lock Device**.

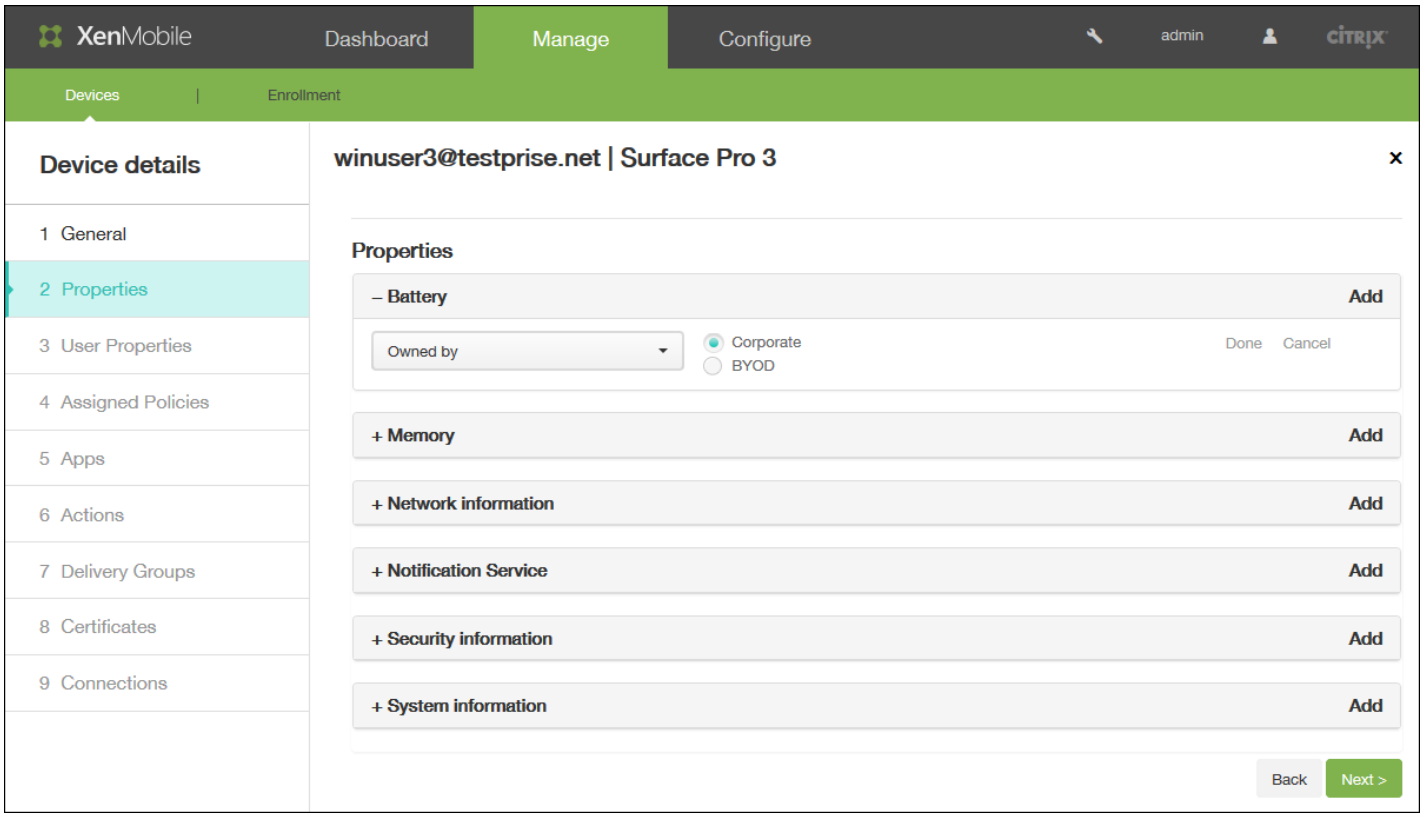
Manuelles Kennzeichnen von Benutzergeräten

Nov 12, 2015

Sie können Geräte in XenMobile auf dreierlei Weise manuell kennzeichnen:

- Kennzeichnen des Geräts bei der Registrierung nach Einladung
- Kennzeichnen des Geräts bei der Registrierung über das Selbsthilfeportal.
- Kennzeichnen des Geräts durch Hinzufügen einer Geräteeigenschaft

Sie können Geräte als Unternehmens- oder Privatgeräte kennzeichnen. Bei der Registrierung eines Geräts über das Selbsthilfeportal können Sie dieses ebenfalls als Unternehmens- oder Privatgerät kennzeichnen. Wie in der folgenden Abbildung dargestellt können Sie ein Gerät auch manuell kennzeichnen, indem Sie ihm auf der Registerkarte **Devices** in der XenMobile-Konsole eine Eigenschaft hinzufügen, die Eigenschaft **Owned by** hinzufügen und dann entweder **Corporate** oder **BYOD** (privat) auswählen.



Geräte-Provisioningdateiformate

Nov 12, 2015

Viele Mobilfunkanbieter und Mobilgerätehersteller stellen Listen autorisierter Mobilgeräte bereit, die Sie verwenden können, um die manuelle Erstellung einer langen Liste zu vermeiden. XenMobile unterstützt ein für alle drei unterstützten Gerätetypen – Android, iOS und Windows – geeignetes Importdateiformat.

Eine manuell erstellte Provisioningdatei zum Importieren von Geräten in XenMobile muss folgendes Format haben:

- SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2; ... propertyNameN;propertyValueN

Hinweis:

- Der Zeichensatz der Datei muss UTF-8 sein.
- Die Felder in der Provisioningdatei werden durch Semikola (;) getrennt. Wenn ein Feld ein Semikolon enthält, muss dieses mit einem umgekehrten Schrägstrich (\) geschützt werden. Beispiel: Eigenschaft propertyV;test;1;2 würde eingegeben als propertyV\;test\;1\;2 in der Provisioningdatei.
- SerialNumber ist erforderlich, wenn IMEI nicht angegeben wurde.
- SerialNumber ist für iOS-Geräte erforderlich, da die Seriennummer bei iOS als Geräte-ID verwendet wird.
- IMEI ist erforderlich, wenn SerialNumber nicht angegeben wurde.
- Gültige Werte für: OperatingSystemFamily sind: WINDOWS, ANDROID, or iOS.

Beispiel einer Geräteprovisioningdatei

Die folgenden Zeilen beschreiben ein Gerät in einer Geräteprovisioningdatei.

1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;propertyV$*&&éééétest

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;

Der erste Eintrag bedeutet Folgendes:

- Seriennummer: 1050BF3F5173010816100655105903 91
- IMEI: 15244201625379901
- Betriebssystemfamilie: WINDOWS
- Eigenschaftsname: propertyN
- Eigenschaftswert: propertyV\;test\;1\;2;prop 2

Makros in XenMobile

Apr 12, 2016

XenMobile bietet leistungsstarke Makros zum Eintragen von Benutzer- oder Geräteeigenschaftsdaten in die Textfelder von Profilen, Richtlinien, Benachrichtigungen, Registrierungsvorlagen (für einige Aktionen) und anderen. Mit Makros können Sie eine einzelne Richtlinie konfigurieren und einer großen Benutzergruppe bereitstellen, wobei für jeden Zielbenutzer benutzerspezifische Werte angezeigt werden. Sie können beispielsweise den Postfachwert in einem Exchange-Profil für tausende Benutzer vorab eingeben.

Dieses Feature ist zurzeit nur für Konfiguration und Vorlagen für iOS- und Android-Geräte verfügbar.

Definieren von Benutzermakros

Folgende Benutzermakros sind immer verfügbar:

- loginname (Benutzername und Domänenname)
- username (Anmeldename minus Domäne, falls vorhanden)
- domainname (Domänenname oder Standarddomäne)

Folgende vom Administrator definierte Eigenschaften stehen u. U. zur Verfügung:

- c
- cn
- company
- companyname
- department
- description
- displayname
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- ipphone
- l
- mail
- middleinitial
- mobile
- officestreetaddress
- pager
- physicaldeliveryofficename
- postalcode

- postofficebox
- telephonenumber
- samaccountname
- sn
- st
- streetaddress
- title
- userprincipalname
- domainname (hat Vorrang vor o. a. Eigenschaft)

Wenn der Benutzer mit einem Authentifizierungsserver (z. B. LDAP) authentifiziert wird, sind zusätzlich alle dem Benutzer in diesem Speicher zugeordneten Eigenschaften verfügbar.

Makrosyntax

Ein Makro kann folgendes Format haben:

- ${type.PROPERTYNAME}
- ${type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]}

Generell muss der gesamte Teil nach dem Dollarzeichen ($) in geschweiften Klammern ({}) stehen.

- Qualifizierte Eigenschaftsnamen verweisen entweder auf eine Benutzereigenschaft, eine Geräteeigenschaft oder eine benutzerdefinierte Eigenschaft.
- Qualifizierte Eigenschaftsnamen bestehen aus einem Präfix gefolgt von dem eigentlichen Eigenschaftsnamen.
- Benutzereigenschaften haben das Format ${user.[PROPERTYNAME] (prefix="user.")}.
- Geräteeigenschaften haben das Format ${device.[PROPERTYNAME] (prefix="device.")}.

Mit ${user.username} wird beispielsweise der Wert "Benutzername" im Textfeld einer Richtlinie eingetragen. Dies ist nützlich beim Konfigurieren von Exchange ActiveSync-Profilen und anderen Profilen, die von mehreren Benutzern verwendet werden.

Bei benutzerdefinierten (von Ihnen erstellten) Makros lautet das Präfix ${custom}. Sie können das Präfix auslassen.

Hinweis: Bei Eigenschaftennamen wird zwischen Groß- und Kleinschreibung unterschieden.

Geräterichtlinien

Jul 27, 2016

Durch Erstellen von Richtlinien können Sie konfigurieren, wie XenMobile mit Geräten interagiert. Obwohl viele Richtlinien für alle Geräte gelten, gibt es für jedes Gerät einen betriebssystemspezifischen Richtliniensatz. Daher gibt es möglicherweise Unterschiede zwischen iOS-, Android- und Windows-Geräten und sogar zwischen Android-Geräten verschiedener Hersteller.

Führen Sie vor dem Erstellen einer neuen Richtlinie die folgenden Schritte aus:

- Erstellen Sie alle Bereitstellungsgruppen, die Sie verwenden möchten.
- Installieren Sie alle erforderlichen Zertifizierungsstellenzertifikate.

Das Erstellen einer Geräterichtlinie besteht im Wesentlichen aus folgenden Schritten:

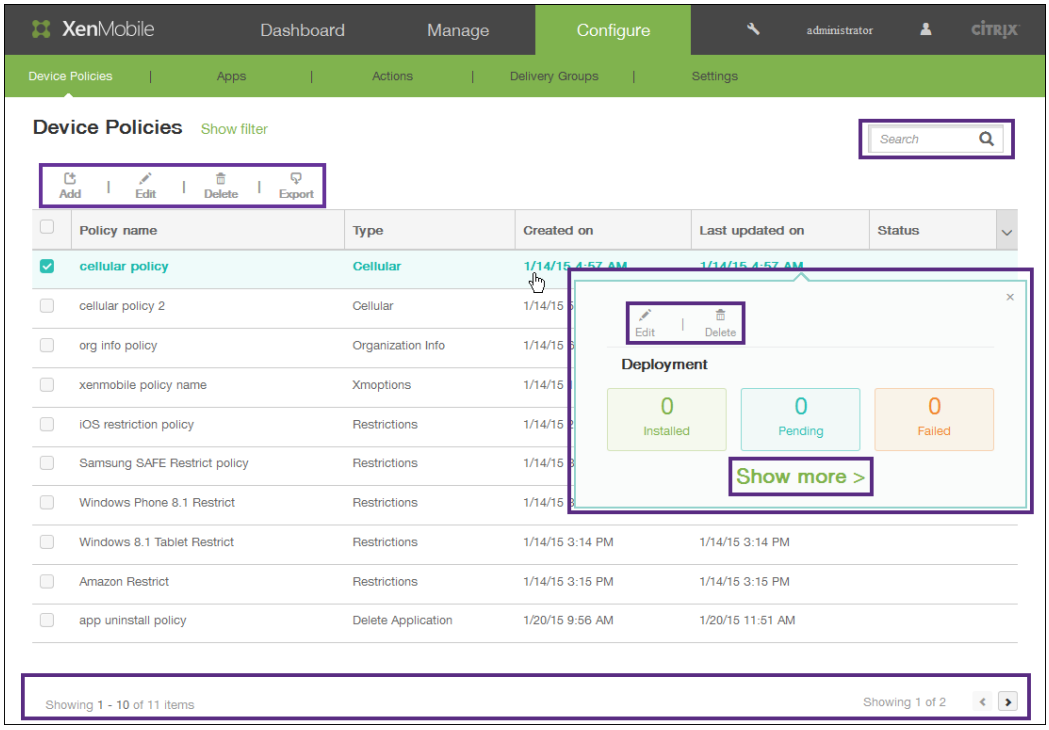
1. Benennen und Beschreiben Sie der Richtlinie
2. Konfigurieren einer oder mehrerer Plattformen
3. Erstellen von Bereitstellungsregeln (optional)
4. Zuweisen der Richtlinie zu Bereitstellungsgruppen
5. Konfigurieren des Bereitstellungszeitplans (optional)

Geräterichtlinienseite in der Konsole

Die Arbeit mit Geräterichtlinien erfolgt in der XenMobile-Konsole auf der Seite Device Policies. Zum Aufrufen der Seite Device Policies klicken Sie auf Configure > Device Policies. Auf dieser Seite können Sie neue Richtlinien hinzufügen, den Status vorhandener Richtlinien prüfen und Richtlinien bearbeiten oder löschen.

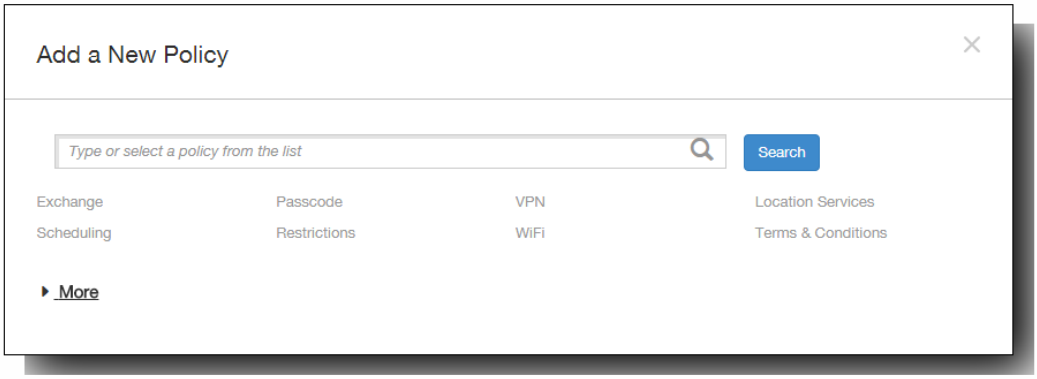
Die Seite Device Policies enthält eine Tabelle aller aktuellen Richtlinien.

Zum Bearbeiten oder Löschen einer Richtlinie auf der Seite Device Policies können Sie das Kontrollkästchen neben der Richtlinie auswählen, um das Menü mit den Optionen oberhalb der Liste einzublenden, oder auf eine Richtlinie in der Liste klicken, um das Menü rechts neben dem Eintrag einzublenden. Wenn Sie auf Show More klicken, werden die Richtliniendetails angezeigt.

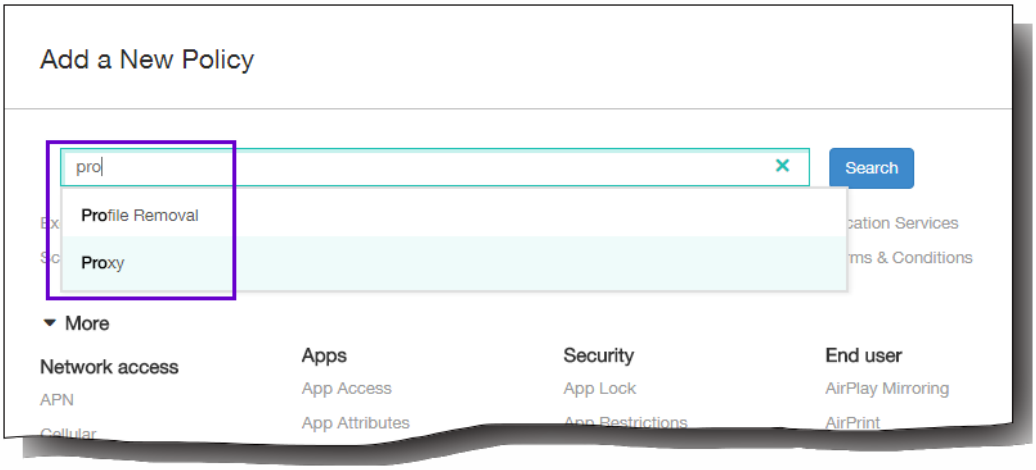


So fügen Sie eine Geräterichtlinie hinzu

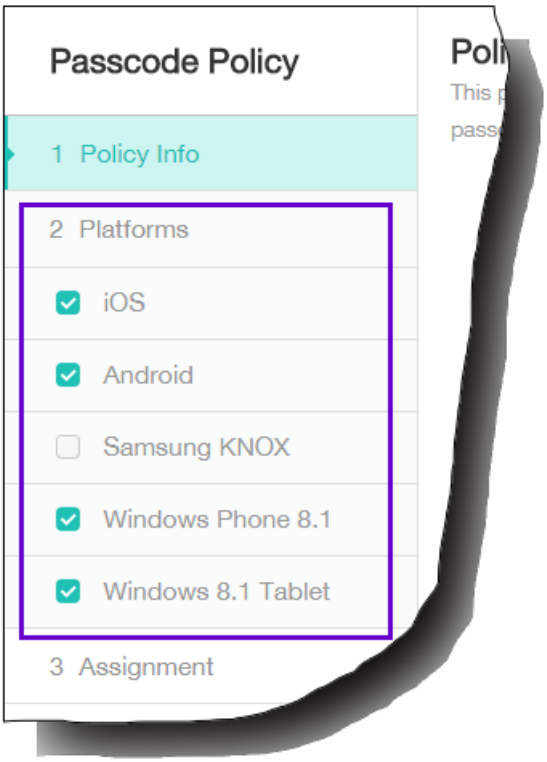
1. Klicken Sie auf der Seite Device Policies auf Add.
   Das Dialogfeld Add a New Policy wird angezeigt. Mit More können Sie weitere Richtlinien einblenden.



2. Zur Auswahl der gewünschten Richtlinie haben Sie folgende Möglichkeiten:
   - Klicken Sie auf die Richtlinie.
     Die Seite Policy Information für die ausgewählte Richtlinie wird angezeigt.
   - Geben Sie den Namen der Richtlinie in das Suchfeld ein. Während der Eingabe werden die möglichen Treffer eingeblendet. Wenn die Richtlinie in der Liste ist, klicken Sie darauf. Nur die ausgewählte Richtlinie verbleibt im Dialogfeld. Klicken Sie darauf, um die zugehörige Seite Policy Information zu öffnen.
     Wichtig: Wenn die ausgewählte Richtlinie im Bereich More ist, wird sie nur angezeigt, wenn Sie More erweitern.

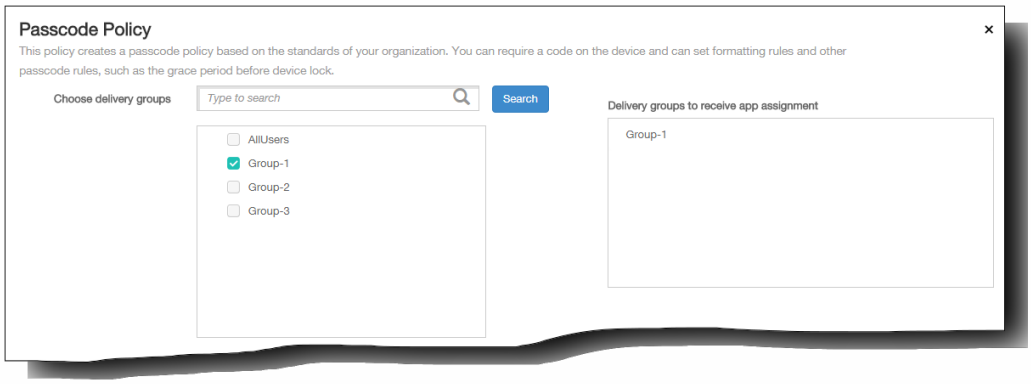


3. Wählen Sie die Plattformen aus, die Sie in die Richtlinie einschließen möchten. Die Seiten zur Konfiguration für die ausgewählten Plattformen werden in Schritt 5 angezeigt.
   Hinweis: Nur die von der Richtlinie unterstützten Plattformen werden aufgelistet.



4. Geben Sie die erforderlichen Informationen auf der Seite Policy Information ein und klicken Sie dann auf Next. Die Seite Policy Information enthält Informationen zum Identifizieren und Verfolgen von Richtlinien (z. B. Richtlinienname). Diese Seite ist bei allen Richtlinien ähnlich.
5. Füllen Sie die Plattformseiten aus. Plattformseiten werden für jede Plattform, die Sie in Schritt 3 ausgewählt haben, angezeigt. Diese Seiten unterscheiden sich für die einzelnen Richtlinien. Jede Richtlinie kann plattformabhängig anders sein. Nicht alle Richtlinien werden von allen Plattformen unterstützt. Klicken Sie auf Next, um zur nächsten Plattformseite oder, wenn alle Plattformseiten ausgefüllt sind, zur Seite Assignment zu gehen.
6. Wählen Sie auf der Seite Assignments die Bereitstellungsgruppen aus, auf die die Richtlinie angewendet werden soll. Wenn Sie auf eine Bereitstellungsgruppe klicken, wird deren Name im Feld Delivery groups to receive app assignment

angezeigt.
Hinweis: Das Feld Delivery groups to receive app assignment wird erst eingeblendet, wenn Sie auf eine Bereitstellungsgruppe klicken.



7. Klicken Sie auf Speichern.
   Die Richtlinie wird der Tabelle der Geräterichtlinien hinzugefügt.

So bearbeiten oder löschen Sie eine Geräterichtlinie

1. Aktivieren Sie in der Tabelle **Device Policies** das Kontrollkästchen neben die Richtlinie, die Sie bearbeiten oder löschen möchten.
2. Klicken Sie auf Edit oder Delete.
   - Wenn Sie auf Edit klicken, bearbeiten Sie beliebige Einstellungen nach Bedarf.
   - Wenn Sie auf Delete klicken, wird ein Bestätigungsdialogfeld angezeigt. Klicken Sie darin erneut auf Delete.

XenMobile-Geräterichtlinien nach Plattform

Nov 12, 2015

Sie können in XenMobile Geräterichtlinien für Amazon-, iOS-, Android-, Android for Work-, Samsung SAFE-, Samsung KNOX-, Symbian-, Windows Phone 8.1-Geräte und Windows 8.1-Tablets erstellen. Zum Hinzufügen und Konfigurieren von Geräterichtlinien verwenden Sie die Optionen Configure > Device Policies der XenMobile-Konsole.

Hinweis: Android Sony unterstützt nur die Speicherverschlüsselungsrichtlinie. Android HTC unterstützt nur der Exchange-Richtlinie.

Geräterichtlinie	**Amazon**	**iOS**	**Android**	**Android for Work**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Windows 8.1-Tablet**
Allgemeines									
Exchange		X	X	X	X	X		X	
Planung			X	X			X		
Passcode		X	X	X		X		X	X
Einschränkungen	X	X			X			X	X
VPN	X	X	X		X	X			X
WiFi		X	X					X	X
Ortungsdienste		X	X						
Nutzungsbedingungen	X	X	X		X	X	X		
Network access									
APN		X	X			X			
Mobilfunk		X	X						
Persönlicher Hotspot		X							
Proxy		X							
Remote Support						X			
Roaming		X							

Samsung-Firewall					X				
Tunnel			X						
	Amazon	**iOS**	**Android**	**Android for Work**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Windows 8.1-Tablet**
Benutzerdefiniert									
Benutzerdefinierte XML							X	X	X
iOS-Profil importieren		X							
Entfernen									
Profilentfernung		X							
Provisioningprofilentfernung		X							
Apps									
App-Zugriff		X	X				X		
App-Attribute		X							
App-Konfiguration		X							
App-Bestand		X	X			X	X	X	X
App-Deinstallation		X	X	X		X			X
Einschränkungen für App-Deinstallation	X				X				
Dateien			X						
Browser				X	X	X			
Provisioningprofil		X							
Sideloading-Schlüssel									X

Signaturzertifikat									X
Webclip		X	X						X
Worx Store		X	X						X
	Amazon	**iOS**	**Android**	**Android for Work**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Windows 8.1-Tablet**
Security									
Android for Work-App-Einschränkungen				X					
App-Sperre		X	X						
App-Einschränkungen						X			
Kontakte (CardDAV)		X							
Anmeldeinformationen		X	X	X					X
Kiosk					X				
Verwaltete Domänen		X							
SCEP		X							
Samsung MDM-Lizenzschlüssel					X	X			
Speicherverschlüsselung			X		X			X	
Webinhaltsfilterung		X							
XenMobile-Agent									
Enterprise Hub								X	
XenMobile-Optionen			X				X		

XenMobile-Deinstallation			X						
Endbenutzer									
AirPlay-Spiegelung		X							
AirPrint		X							
Kalender (CalDav)		X							
Schriftart		X							
LDAP		X							
MDM-Optionen		X							
E-Mail		X							
Informationen zum Unternehmen		X							
SSO-Konto		X							
Abonnierte Kalender		X							

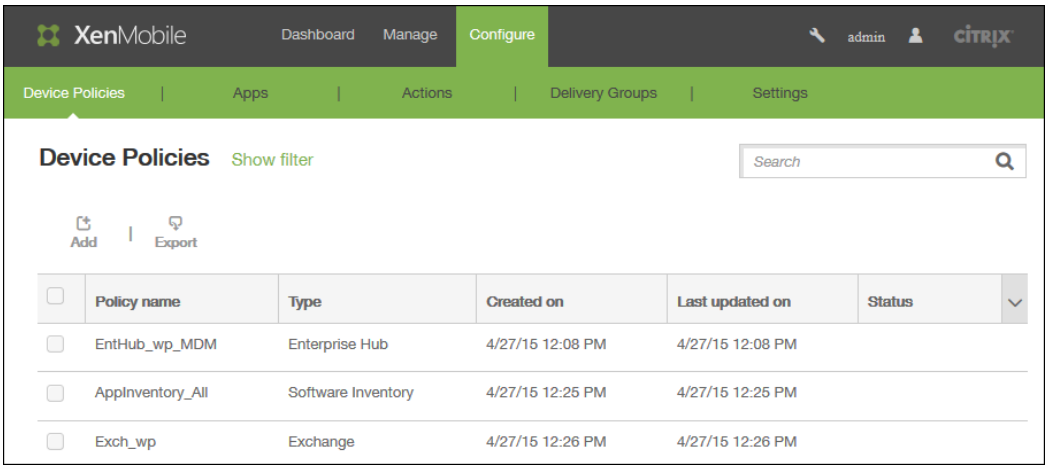
So fügen Sie eine App-Zugriffsrichtlinie für Geräte hinzu

Nov 12, 2015

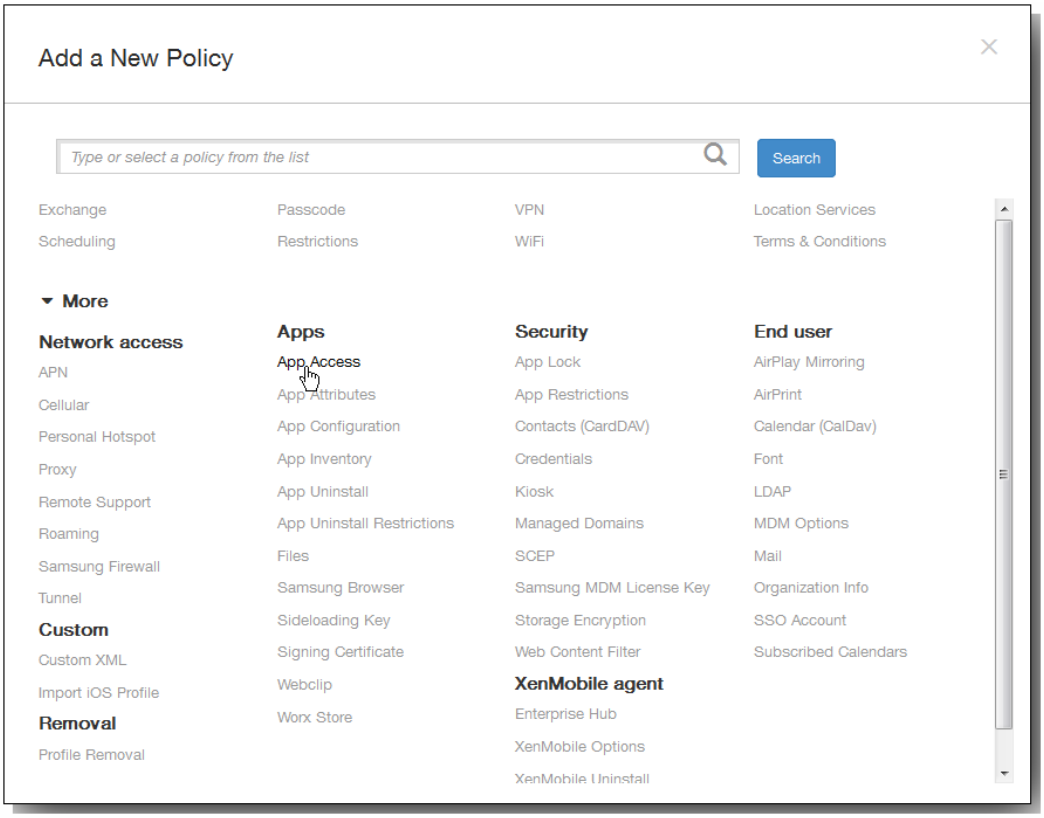
Über eine App-Zugriffsrichtlinie für Geräte können Sie in XenMobile eine Liste der Apps definieren, die auf Geräten installiert werden müssen, nach Wahl installiert werden können oder nicht installiert werden dürfen. Sie können dann eine automatisierte Aktion erstellen, mit der die Reaktion auf die Richtlinientreue von Geräten gesteuert wird. Sie können App-Zugriffsrichtlinien für iOS-, Android- und Symbian-Geräte erstellen.

Sie können in einem Arbeitsgang nur eine Zugriffsrichtlinie konfigurieren. Eine Richtlinie darf eine Liste der erforderlichen Apps, der empfohlenen Apps oder der verbotenen Apps, jedoch nicht eine Mischung aus allen drei Gruppen enthalten. Wenn Sie eine Richtlinie für jeden Listentyp erstellen, empfiehlt sich eine sorgfältige Wahl des Namens für die Richtlinien, damit Sie wissen, welche für welche Apps-Liste gilt.

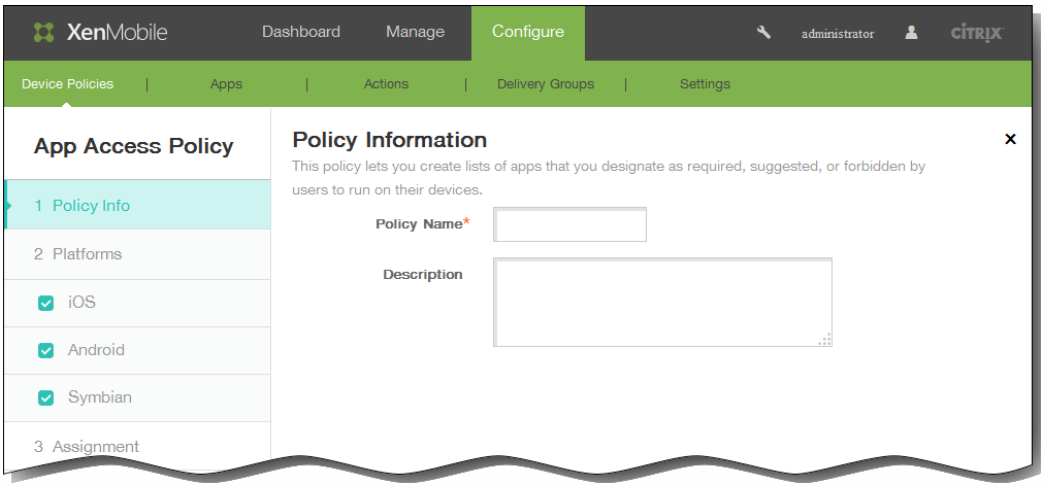
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies.



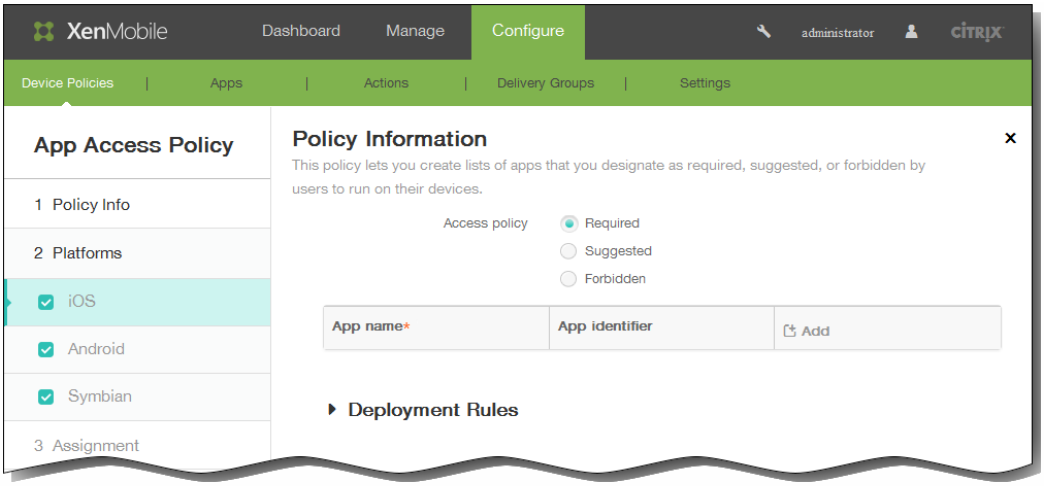
2. Klicken Sie auf Add. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More > App Access. Die Seite App Access Policy wird angezeigt.



4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Policy Platforms wird angezeigt.
   Hinweis: Auf der Seite Policy Platforms sind alle Plattformen ausgewählt, die Konfigurationsseite für die iOS-Plattform wird als erste angezeigt.

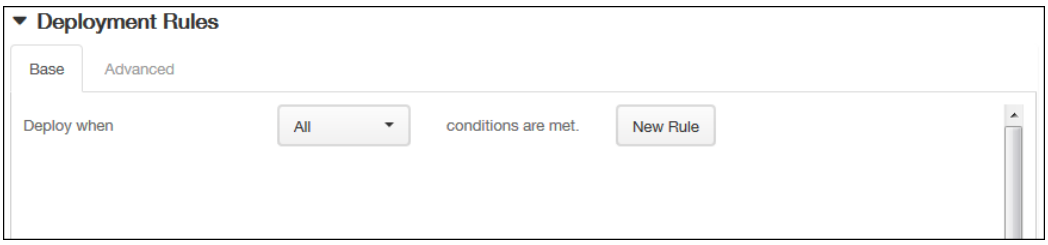


6. Wählen Sie unter Platforms die gewünschten Plattformen aus und führen Sie für jede Plattform die folgenden Schritte durch:
   1. Access policy: Klicken Sie auf Required, Suggested oder Forbidden. Der Standardwert ist Required.
   2. Zum Hinzufügen von Apps zu der Liste klicken Sie auf Add und führen Sie die folgenden Schritte aus:
      1. App name: Geben Sie einen App-Namen ein.
      2. App Identifier: Geben Sie optional eine App-ID ein.
      3. Klicken Sie auf Save oder Cancel.
      4. Wiederholen Sie die Schritte i bis iii für jede App, die Sie hinzufügen möchten.

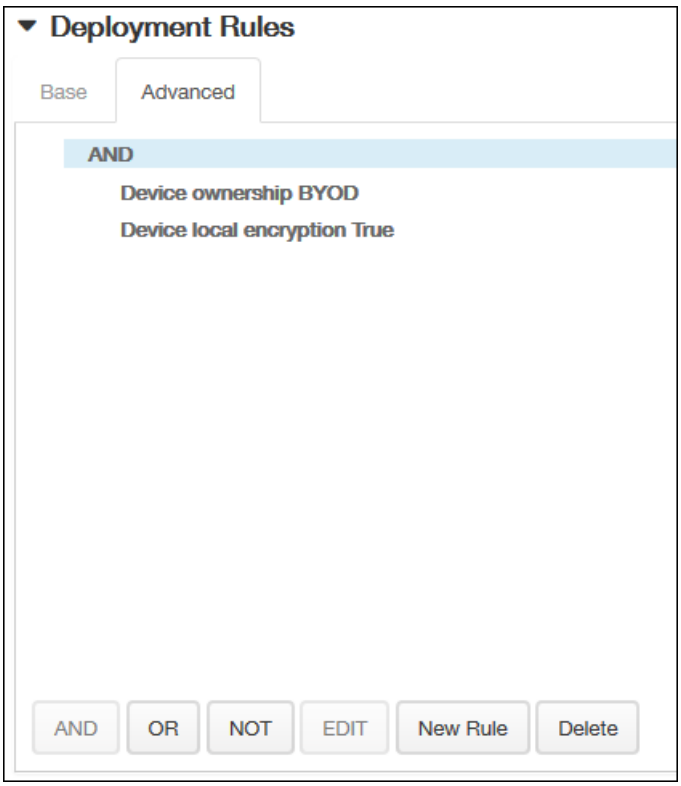
      Hinweis: Zum Löschen einer vorhandenen App zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf Delete zum Löschen des Eintrags oder auf Edit, um ihn beizubehalten.

      Zum Bearbeiten einer App zeigen Sie auf deren Zeile und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf Save, um die Änderungen zu speichern oder auf Cancel, um den Vorgang abzubrechen.

7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

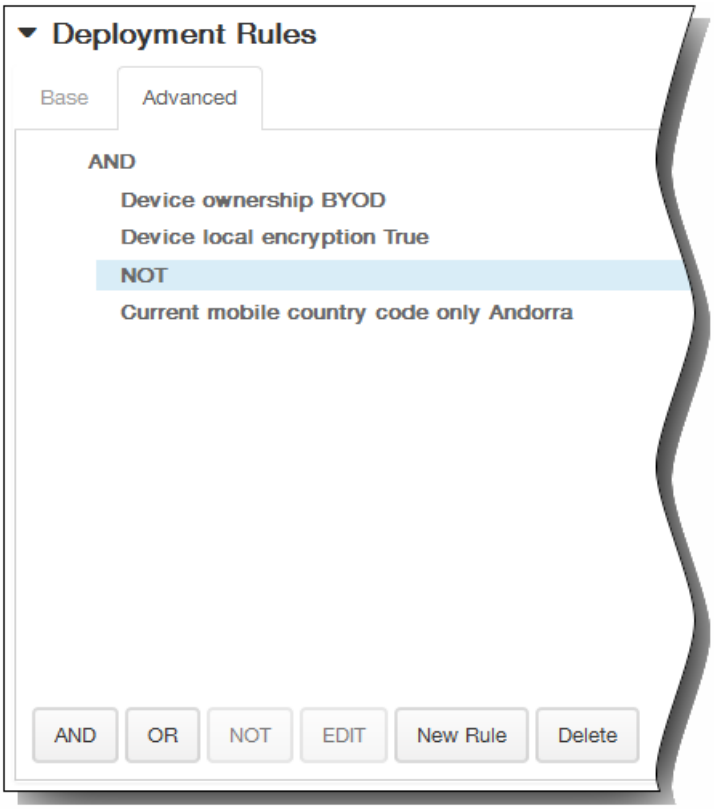


   1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
      1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
      2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
      3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
      4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
   2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.

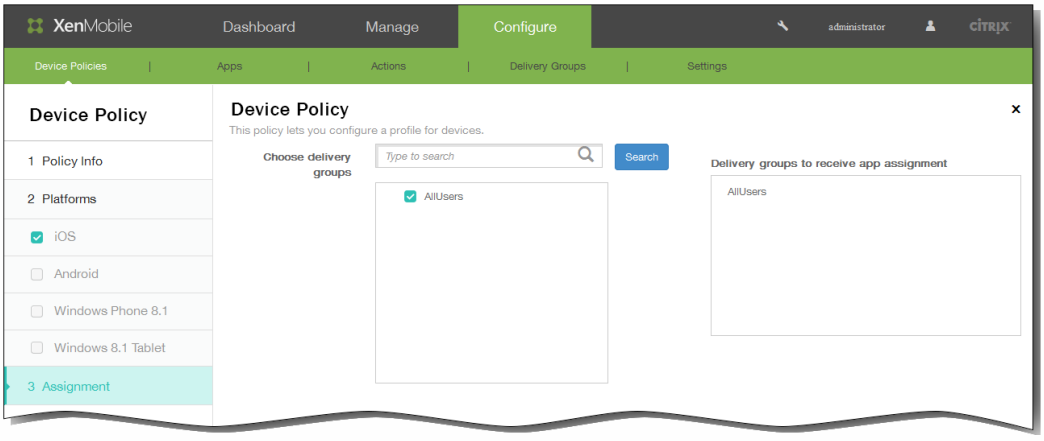


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.
   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



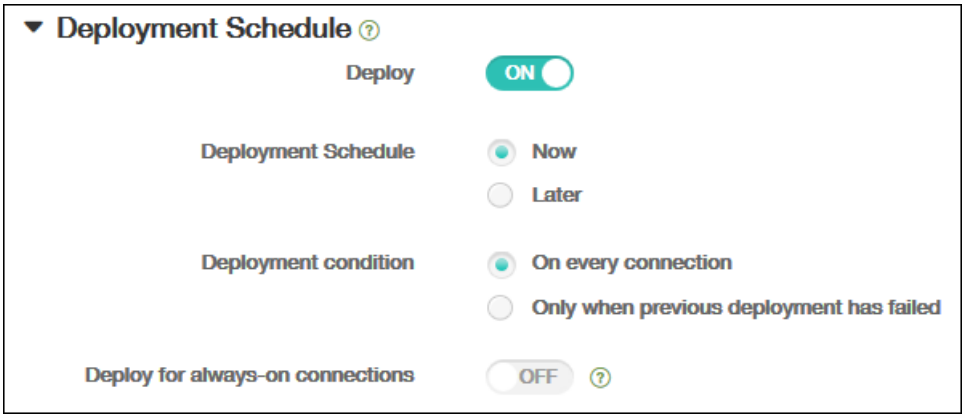
8. Klicken Sie auf Next. Die nächste Plattformseite oder die Zuweisungsseite App Access Policy wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



11. Klicken Sie auf Save, um die Richtlinie zu speichern.

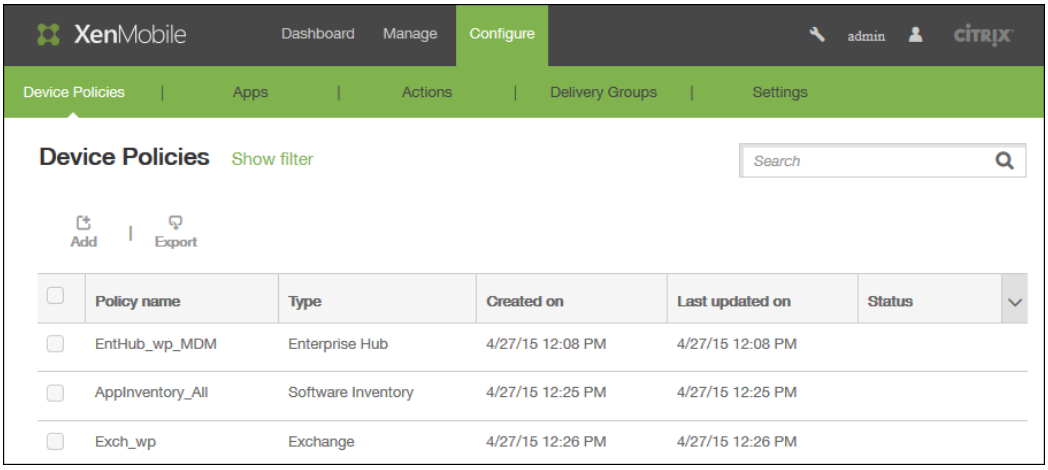
So fügen Sie eine App-Bestandsrichtlinie für Geräte hinzu

Nov 12, 2015

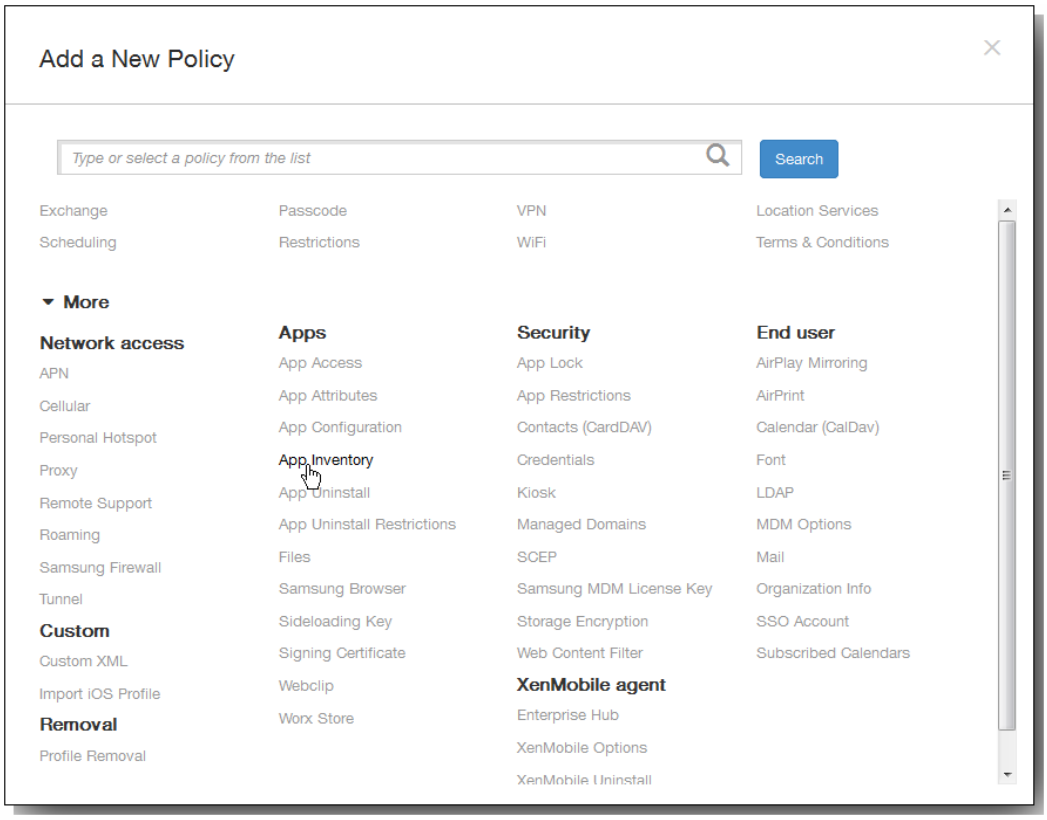
Mit einer App-Bestandsrichtlinie können Sie in XenMobile einen Bestand der Apps auf verwalteten Geräten sammeln und dann mit allen auf diesen Geräten bereitgestellten App-Zugriffsrichtlinien vergleichen. Auf diese Weise können Sie Apps erkennen, die in einer App-Sperrliste (d. h. in einer App-Zugriffsrichtlinie verboten) oder einer App-Positivliste (d. h. gemäß einer App-Zugriffsrichtlinie erforderlich) sind, und entsprechende Maßnahmen ergreifen.

Wichtig: Damit aktualisierte Apps in der Liste der verfügbaren Updates im Worx Store auf Android-Geräten angezeigt werden, müssen Sie auf den Geräten diese Richtlinie bereitstellen.

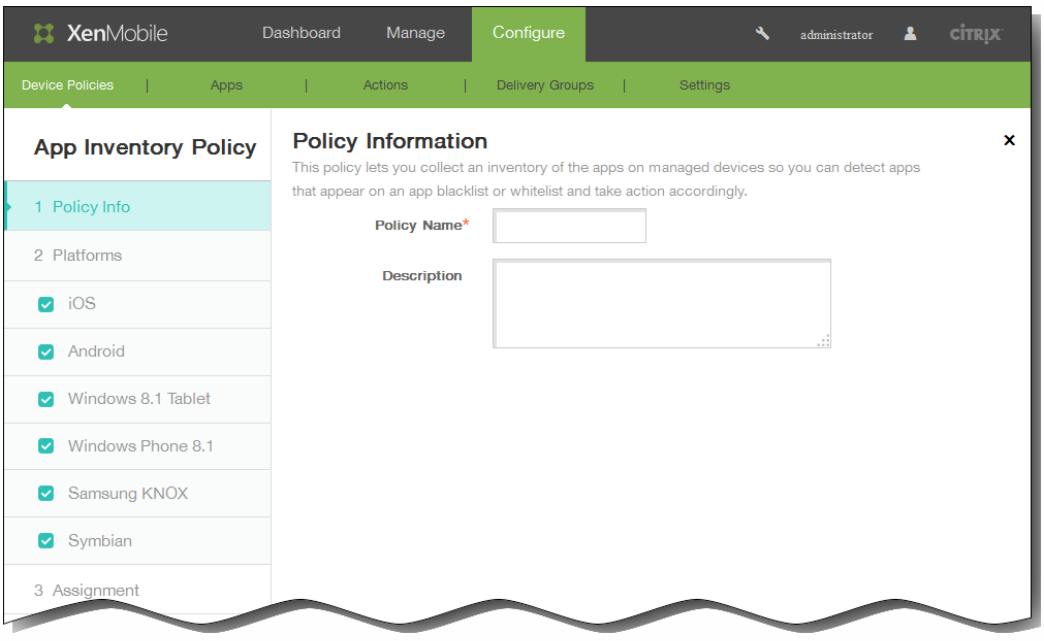
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



2. Klicken Sie auf Add. Die Seite Add a New Policy wird angezeigt.

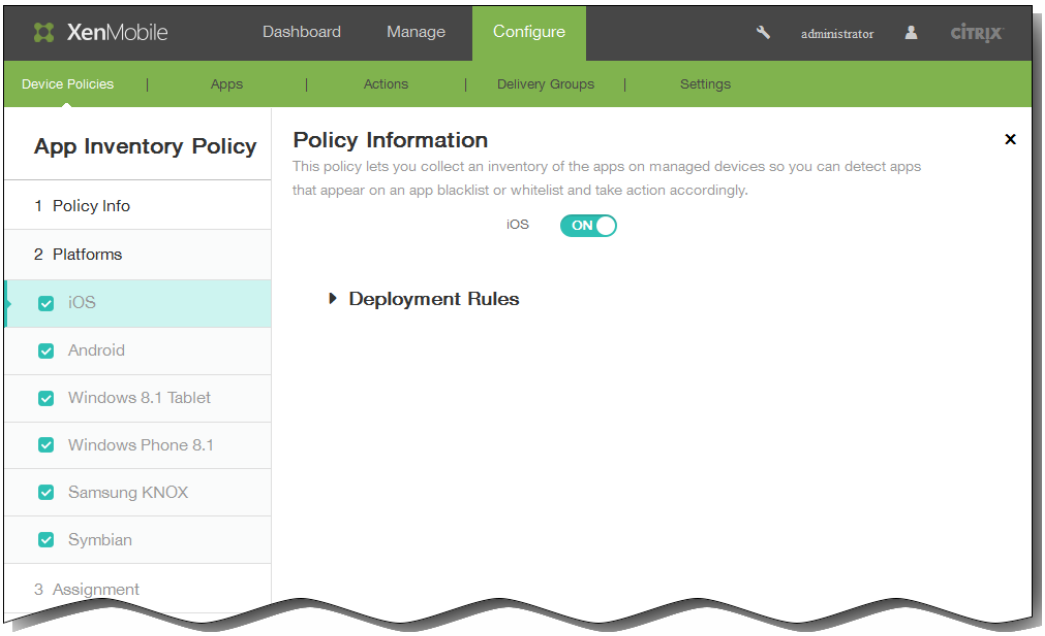


3. Klicken Sie auf More > App Inventory. Die Seite App Inventory Policy wird angezeigt.



4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Policy Platforms wird angezeigt.

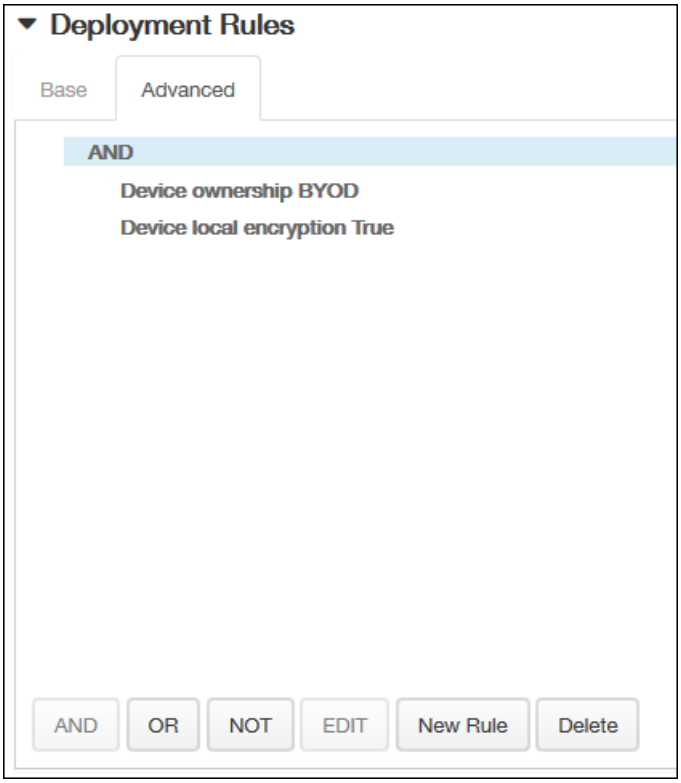
Hinweis: Auf der Seite Policy Platforms sind alle Plattformen ausgewählt, der Konfigurationsbereich für die iOS-Plattform wird als erstes angezeigt.



Wählen Sie die gewünschten Plattformen aus und führen Sie dann für jede Plattform die folgenden Schritte aus:

6. Behalten Sie die Standardeinstellung bei oder ändern Sie sie in OFF. Die Standardeinstellung ist ON.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

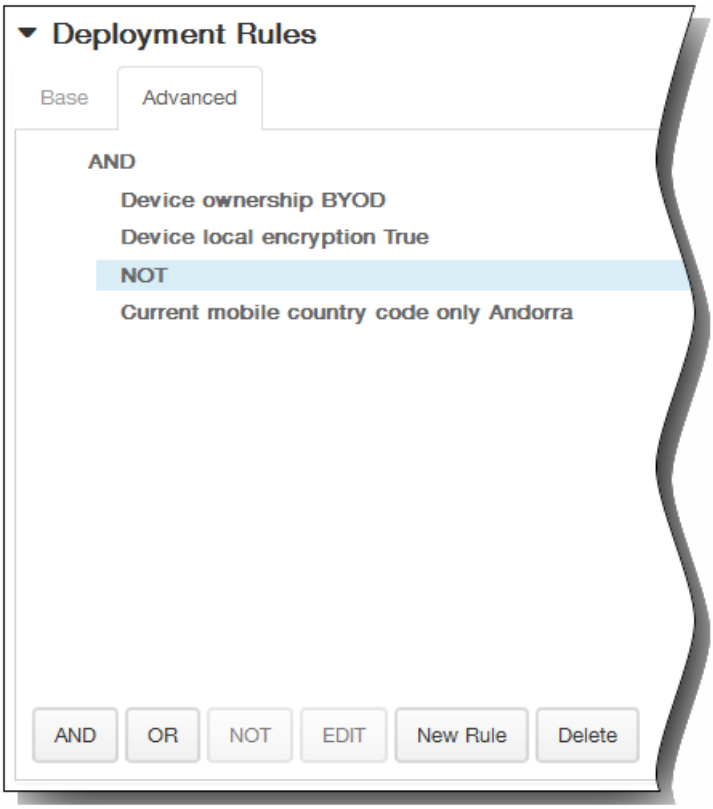
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



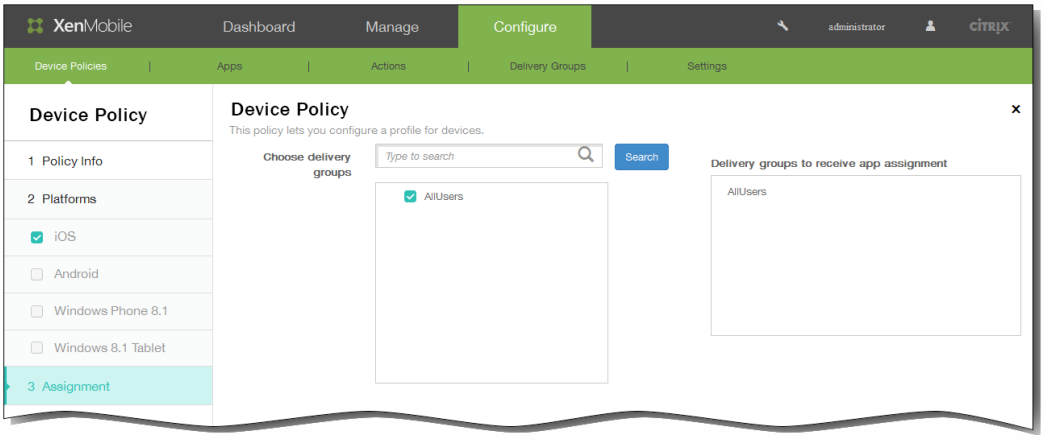
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



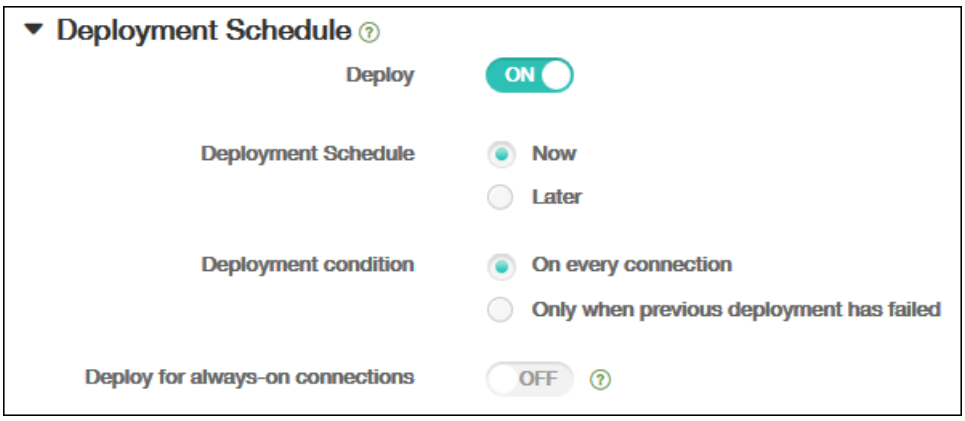
8. Klicken Sie auf Next. Der Seite für die nächste Plattform bzw. die Seite Assignment wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



11. Klicken Sie auf Save, um die Richtlinie zu speichern.

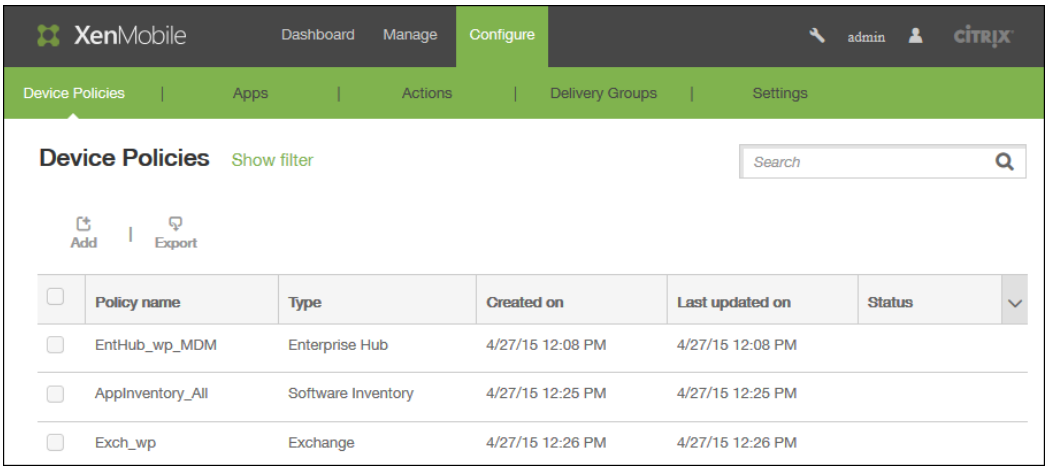
So fügen Sie eine App-Tunnelrichtlinie für Android-Geräte hinzu

Nov 12, 2015

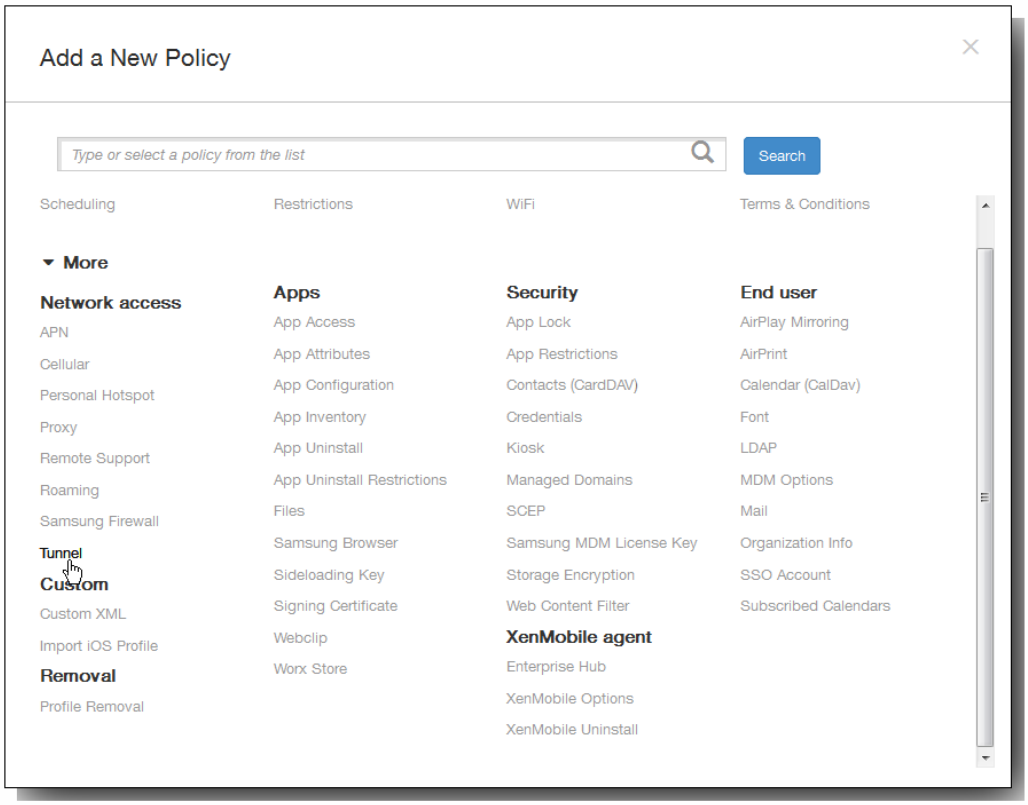
App-Tunnel verbessern die Dienstkontinuität und die Zuverlässigkeit bei der Datenübertragung für mobile Apps. Mit App-Tunneln werden Proxyparameter zwischen der Clientkomponente beliebiger Mobilgeräte-Apps und der App-Serverkomponente definiert. Sie können App-Tunnel auch für den Remotesupport auf Geräten nutzen.

Hinweis: Jeglicher App-Datenverkehr, der über einen in dieser Richtlinie definierten Tunnel gesendet wird, durchläuft zunächst XenMobile, bevor er an den Server mit der App umgeleitet wird.

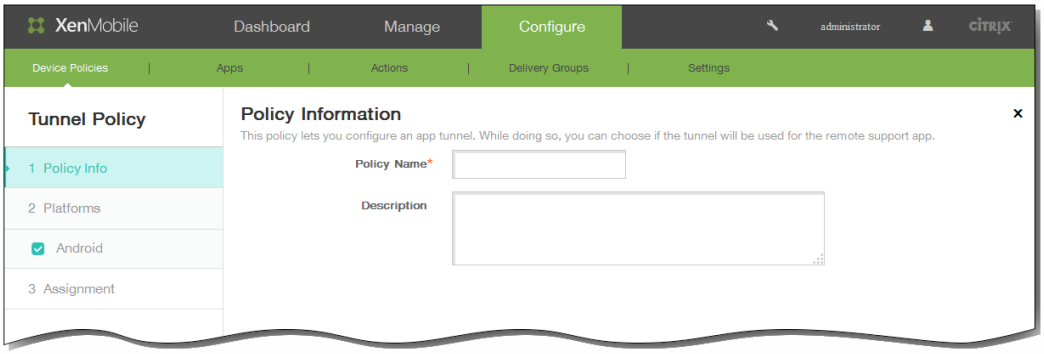
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



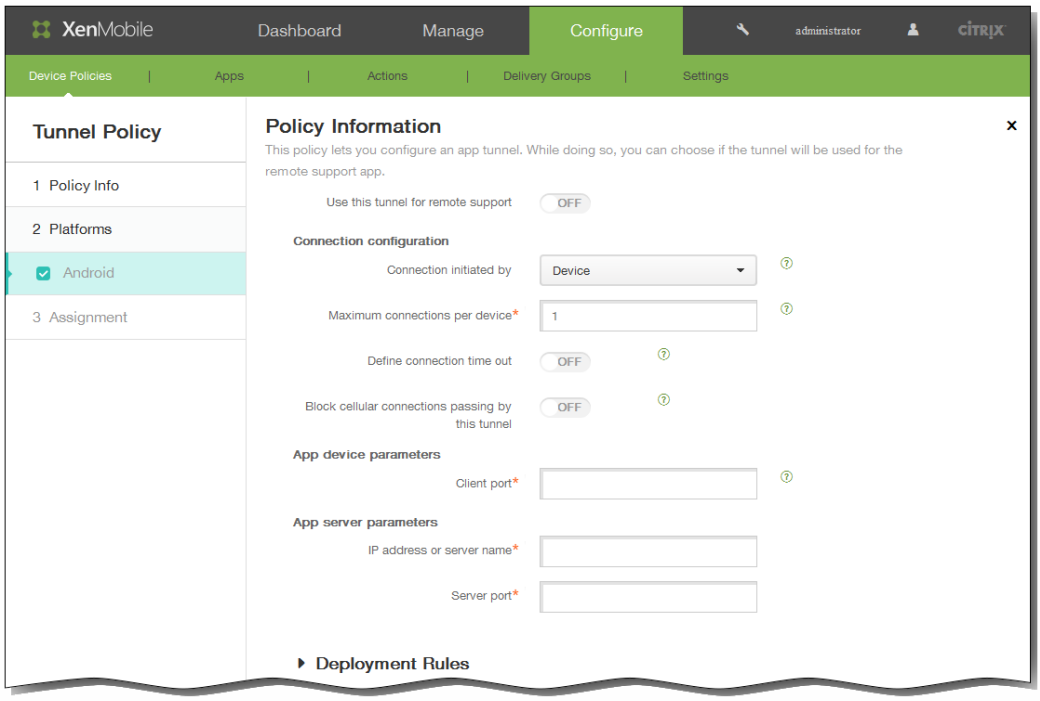
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter Network access auf Tunnel. Die Seite Tunnel Policy wird angezeigt.



4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Android Policy wird angezeigt.

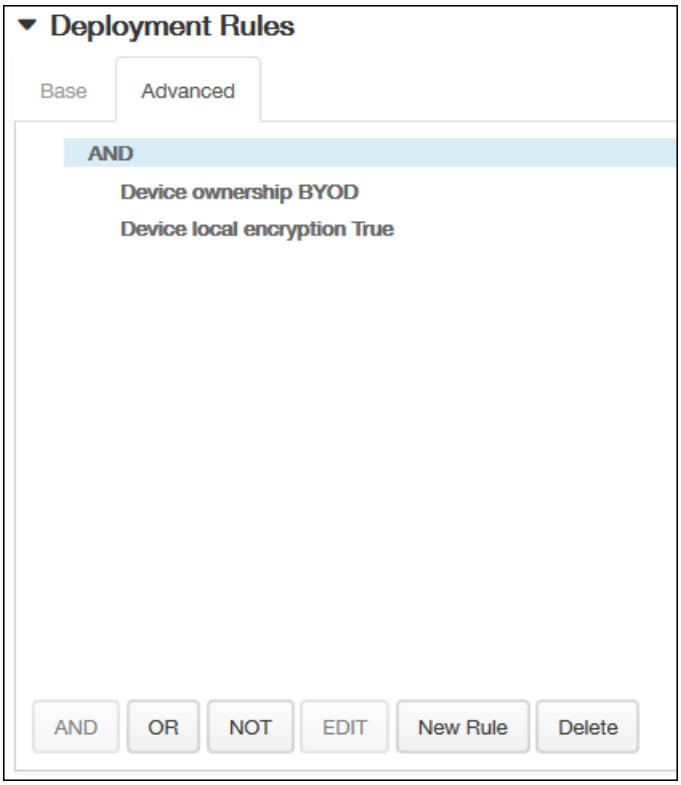


6. Geben Sie in Use this tunnel for remote support an, ob der Tunnel für Remotesupport verwendet werden soll.
   Hinweis: Die Konfigurationsschritte unterscheiden sich je nachdem, ob Sie hier Remotesupport auswählen.
   Wenn Sie Remotesupport **nicht auswählen**, führen Sie folgende Schritte aus:
   1. Connection initiated by: Klicken Sie auf Device oder Server, um die Quelle für die Aufnahme der Verbindung anzugeben.
   2. Maximum connections per device: Geben Sie die Zahl der gleichzeitig zulässigen TCP-Verbindungen für die App ein. Dieses Feld gilt nur für geräteseitig initiierte Verbindungen.
   3. Define connection time out: Wählen Sie aus, ob festgelegt werden soll, wie lange eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
   4. Connection time out: Wenn Sie für Define connection time out die Option On festgelegt haben, geben Sie hier die Zeitdauer in Sekunden ein, die eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
   5. Block cellular connections passing by this tunnel: Wählen Sie aus, ob der Tunnel beim Roaming blockiert werden soll. Hinweis: WiFi- und USB-Verbindungen werden nicht blockiert.
   6. Client port: Geben Sie die Nummer des Clientports ein. In den meisten Fällen entspricht diese der Nummer des Serverports.
   7. IP address or server name: Geben Sie die IP-Adresse oder den Namen des App-Servers ein. Dieses Feld gilt nur für geräteseitig initiierte Verbindungen.
   8. Server port: Geben Sie die Nummer des Serverports ein.

   Wenn Sie Remotesupport **auswählen**, führen Sie folgende Schritte aus:
   1. Use this tunnel for remote support: Legen Sie On fest.
   2. Define connection time out: Wählen Sie aus, ob festgelegt werden soll, wie lange eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
   3. Connection time out: Wenn Sie für Define connection time out die Option On festgelegt haben, geben Sie hier die Zeitdauer in Sekunden ein, die eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
   4. Use SSL connection: Wählen Sie aus, ob für den Tunnel eine SSL-Verbindung verwendet werden soll.
   5. Block cellular connections passing by this tunnel: Wählen Sie aus, ob der Tunnel beim Roaming blockiert werden soll. Hinweis: WiFi- und USB-Verbindungen werden nicht blockiert.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird

standardmäßig angezeigt.

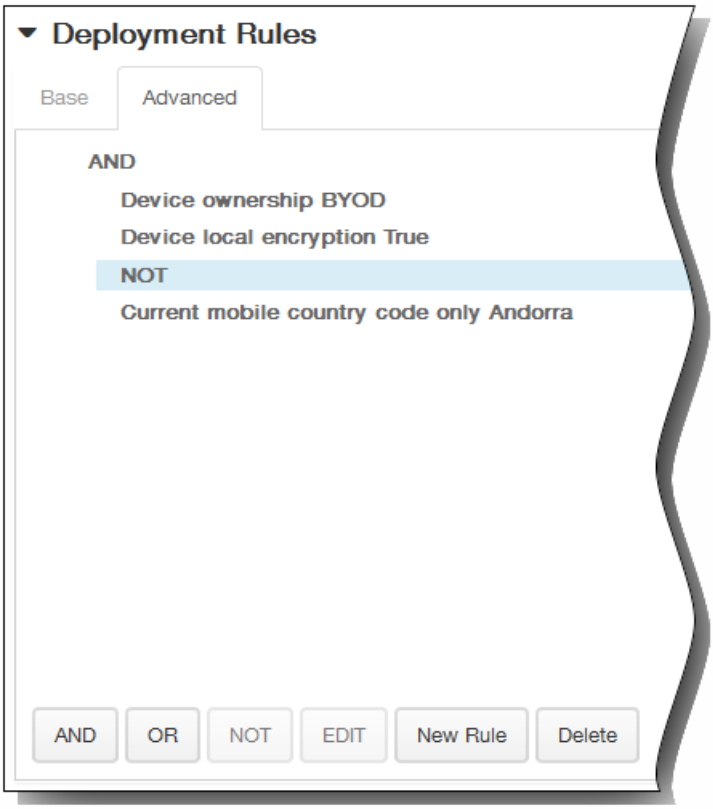
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
   3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
   4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



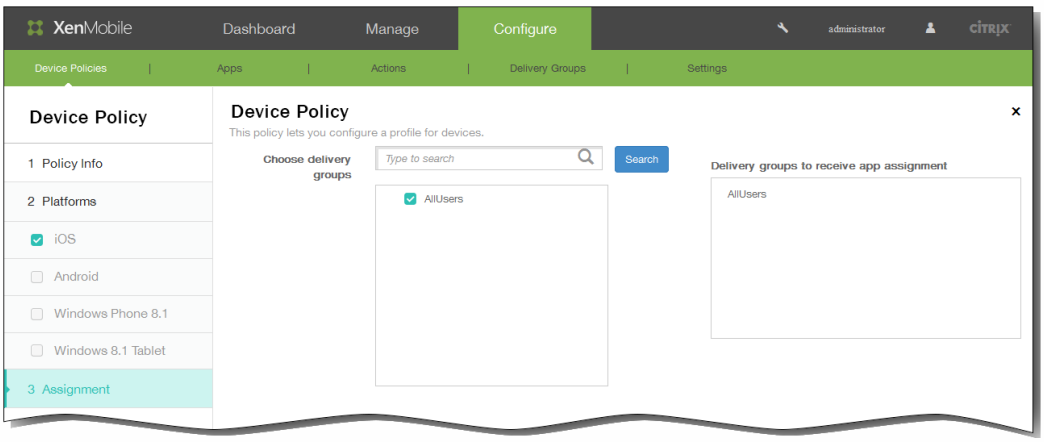
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete,

um die Bedingung zu löschen.

3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
   In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



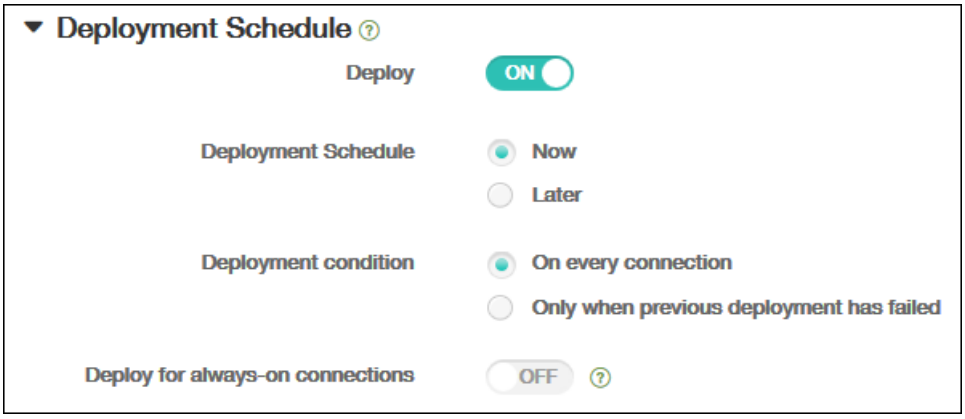
8. Klicken Sie auf Next. Die Seite Tunnel Policy zum Zuweisen der Tunnelrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:

1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



11. Klicken Sie auf Save, um die Richtlinie zu speichern.

Benutzerdefinierte XML-Richtlinien für Geräte

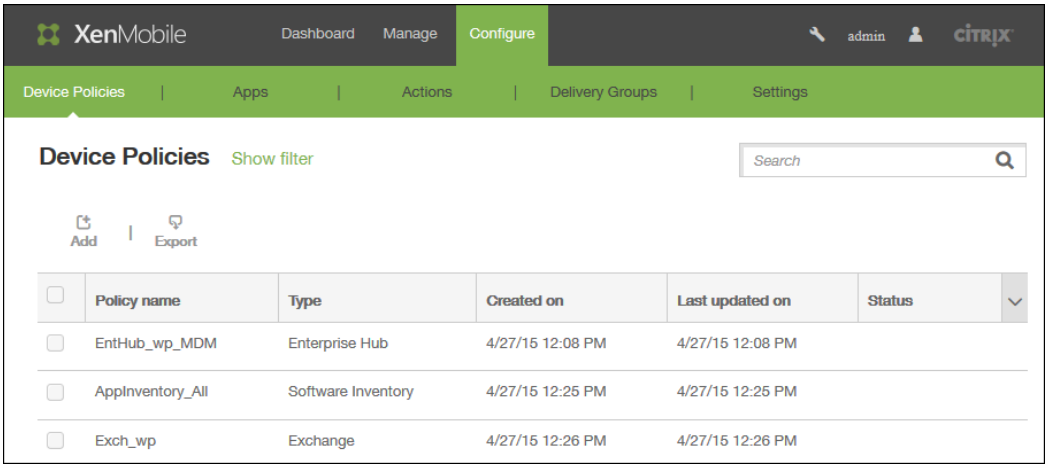
Nov 12, 2015

Sie können benutzerdefinierte XML-Richtlinien in XenMobile erstellen, wenn Sie die folgenden Features auf Windows Phone 8.1-, Windows 8.1 Tablet- und Symbian-Geräten anpassen möchten:

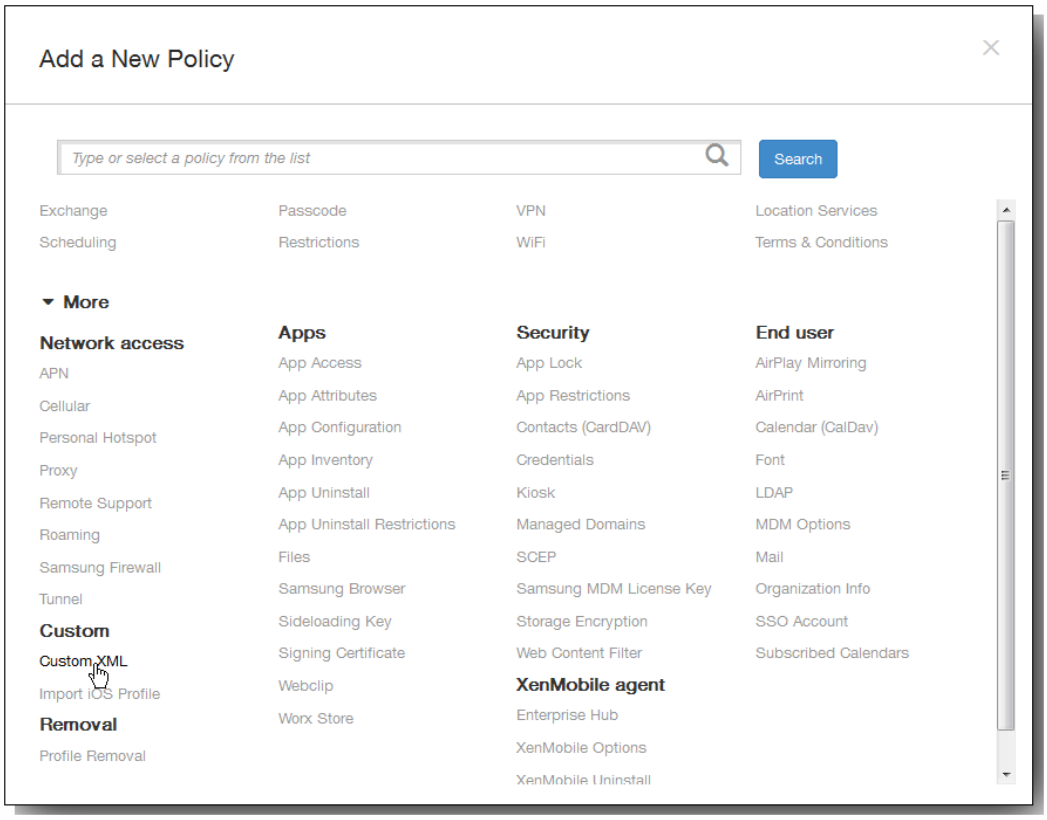
- Provisioning, d. h. Konfiguration des Geräts und Aktivieren bzw. Deaktivieren von Features
- Gerätekonfiguration, einschließlich des Zulassens der Änderung von Einstellungen und Geräteparametern durch die Benutzer
- Softwareupgrades, d. h. Bereitstellung neuer Software oder von Fehlerbehebungen für Geräte, einschließlich Apps und Systemsoftware
- Fehlerverwaltung, d. h. Empfang von Fehler- und von Statusberichten von den Geräten

Zum Erstellen einer eigenen XML-Konfiguration wird die Open Mobile Alliance Device Management-API (OMA DM) in Windows 8.1 verwendet. Das Erstellen benutzerdefinierter XML-Konfigurationen mit der OMA DM-API geht über den Rahmen dieses Abschnitts hinaus. Weitere Informationen zur Verwendung der OMA DM-API finden Sie auf Microsoft Developer Network unter OMA Device Management.

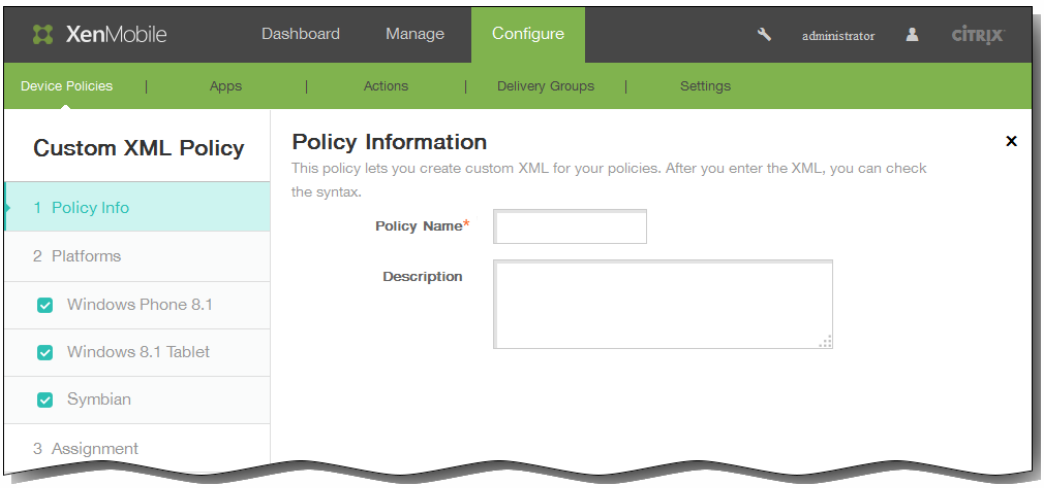
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



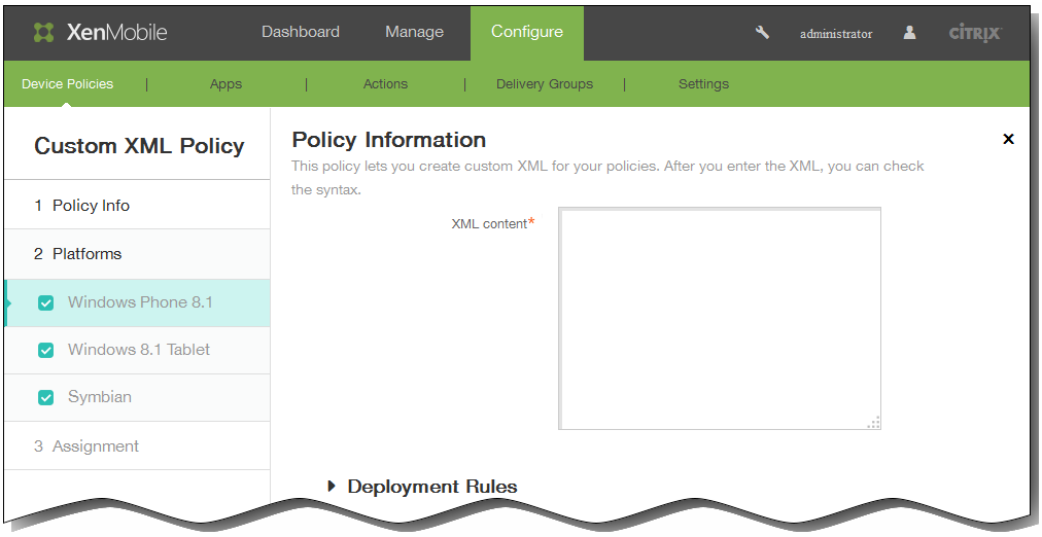
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter Custom auf Custom XML. Die Seite Custom XML Policy wird angezeigt.

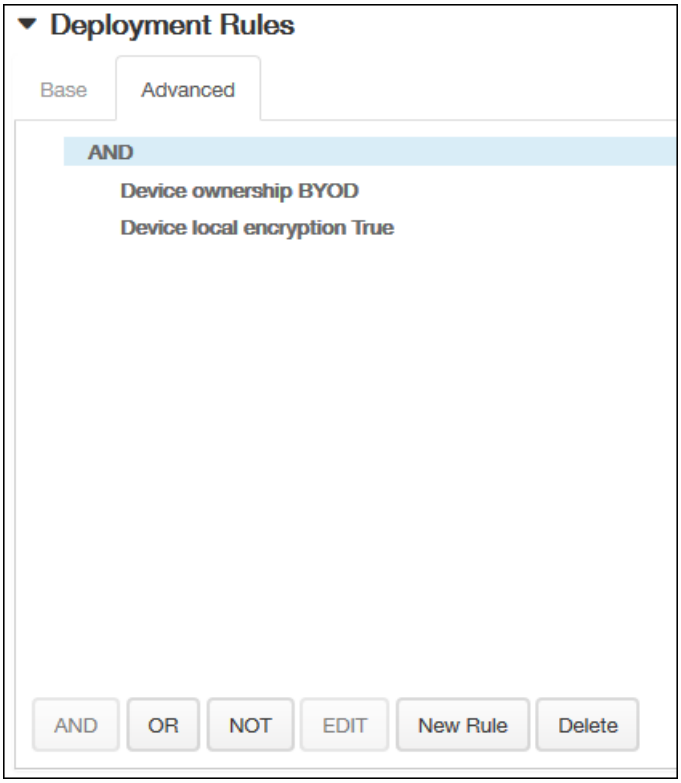


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Policy Platforms wird angezeigt.
   Hinweis: Auf der Seite Policy Platforms sind alle Plattformen ausgewählt, der Konfigurationsbereich für die Windows Phone 8.1-Plattform wird als erstes angezeigt.



6. Stellen Sie unter Platforms sicher, dass nur die gewünschten Plattformen ausgewählt sind.
7. Geben Sie in XML content den benutzerdefinierten XML-Code ein, den Sie der Richtlinie hinzufügen möchten. Einen umfangreichen Code können Sie aus der Quelldatei ausschneiden und hier einfügen.
8. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

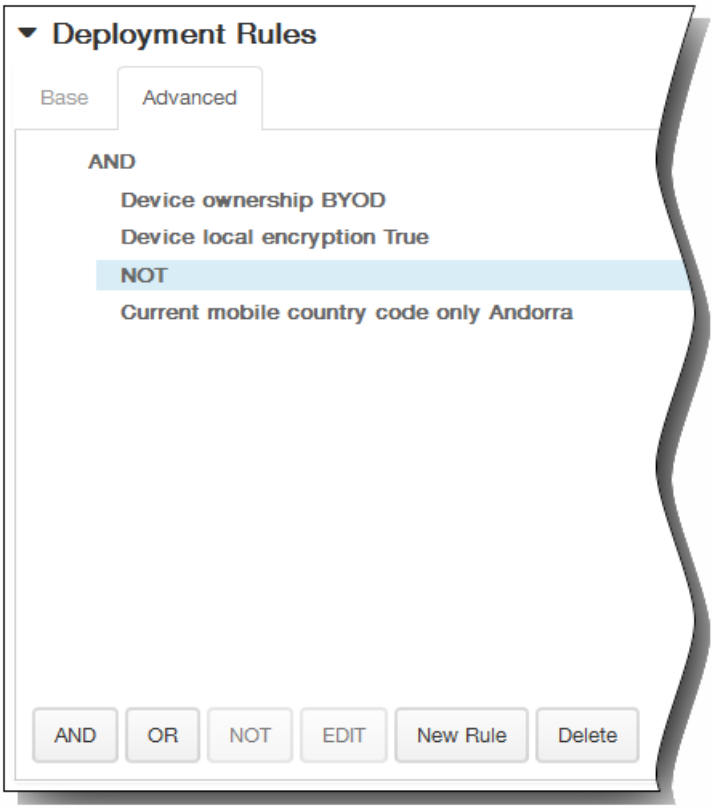
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
   3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
   4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

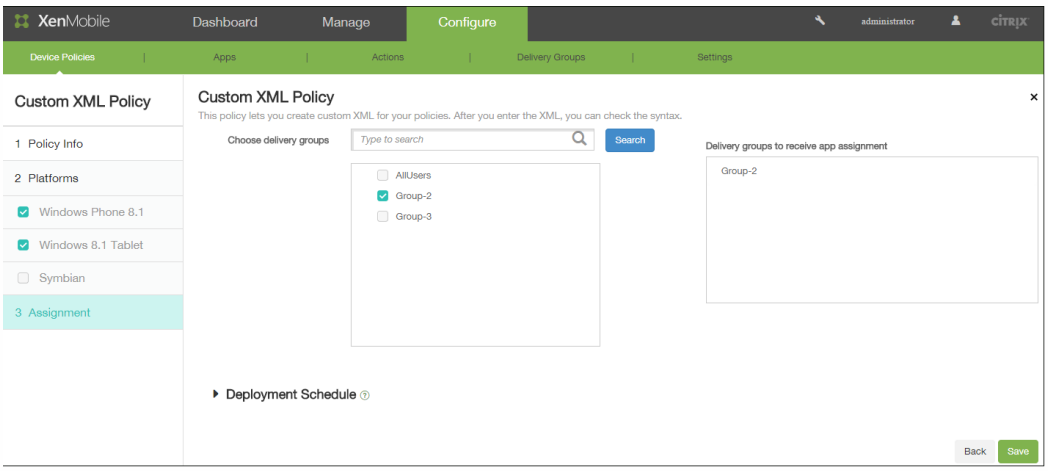
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



9. Klicken Sie auf Next. XenMobile überprüft die Syntax des XML-Inhalts. Syntaxfehler werden unterhalb des Inhaltsfelds angezeigt. Sie müssen alle Fehler korrigieren, bevor Sie fortfahren können.
   Werden keine Syntaxfehler gefunden, wird die Seite Assignment für die benutzerdefinierte XML-Richtlinie angezeigt.

10. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.

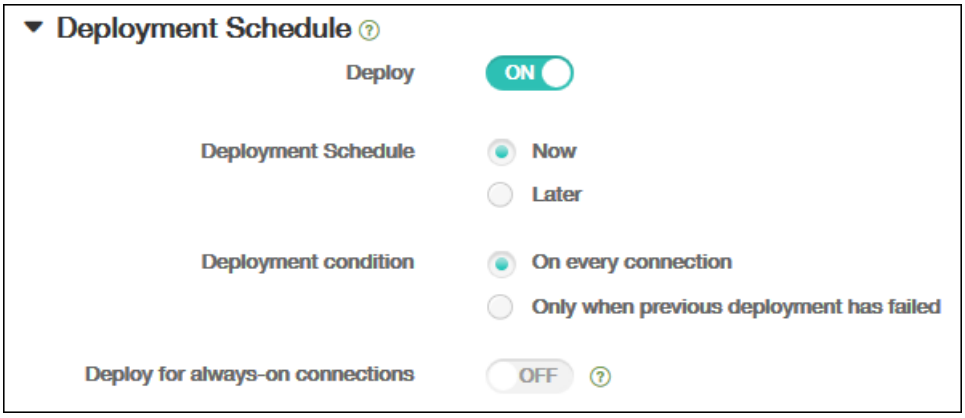


11. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die

Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen gemachten Änderungen werden auf alle Plattformen angewendet.



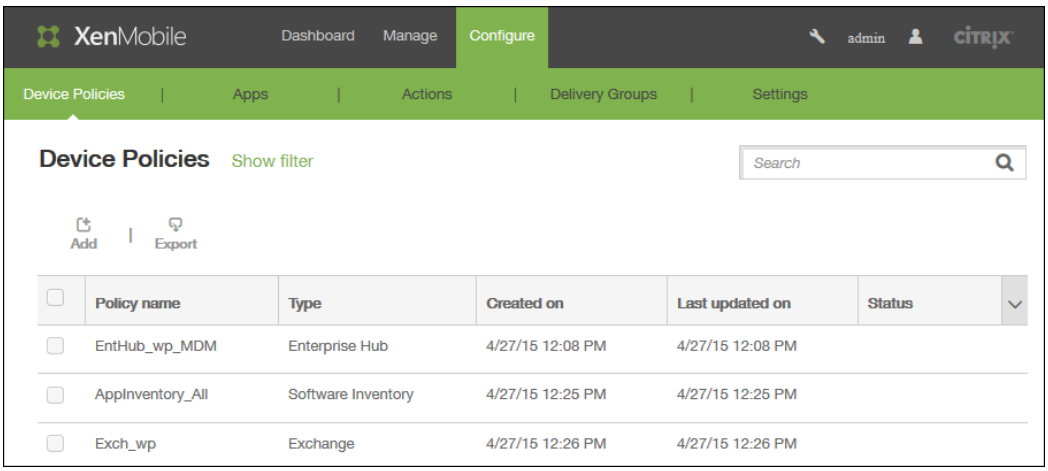
12. Klicken Sie auf Save, um die Richtlinie zu speichern.

App-Deinstallationsrichtlinien für Geräte

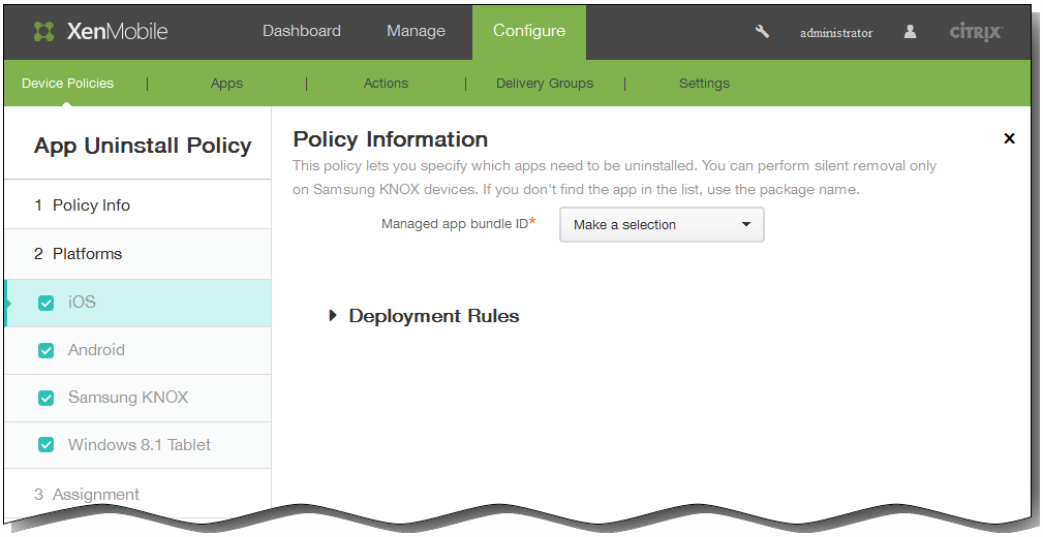
Nov 12, 2015

Sie können App-Deinstallationsrichtlinien für die folgenden Plattformen erstellen: iOS, Android, Samsung KNOX, Android for Work und Windows 8.1-Tablets. Mit einer App-Deinstallationsrichtlinie können Sie Apps von Benutzergeräten entfernen. Grund für die Notwendigkeit des Entfernens von Apps kann sein, dass Sie für diese keinen Support mehr leisten möchten, dass das Unternehmen sie durch ähnliche Apps eines anderen Herstellers ersetzen möchte usw. Die Apps werden entfernt, wenn diese Richtlinie auf den Geräten der Benutzer bereitgestellt wird. Bei allen Geräten mit Ausnahme von Samsung KNOX-Geräten werden Benutzer dazu aufgefordert, die entsprechende App zu deinstallieren.

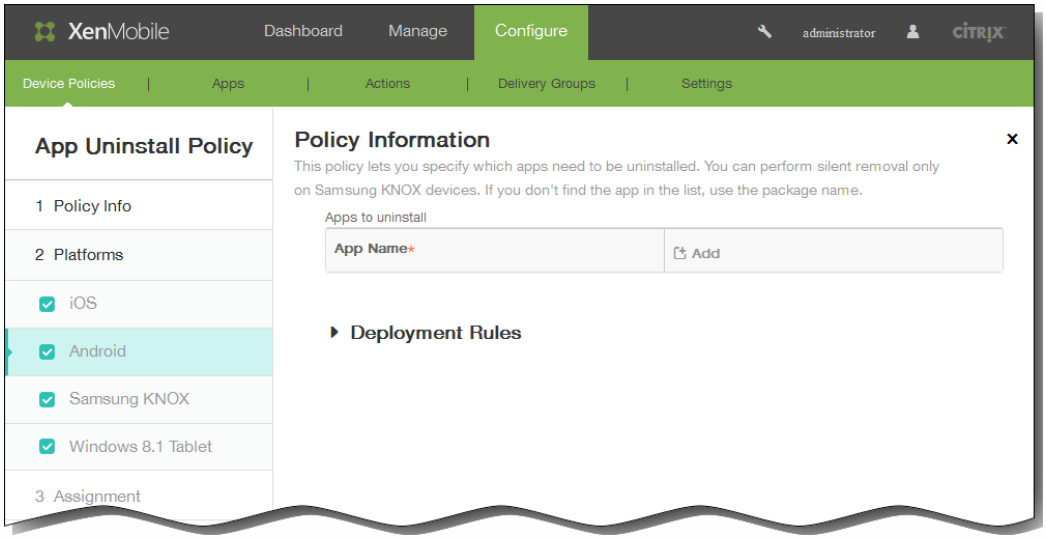
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt. Klicken Sie auf der Seite Device Policies auf Add.



2. Klicken Sie im Dialogfeld Add a New Policy auf More und dann unter Apps auf App Uninstall.
3. Geben Sie im Bereich App Uninstall Policy die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
   3. Klicken Sie auf Next.
4. Auf der Seite Policy Platforms sind alle Plattformen ausgewählt, der Konfigurationsbereich für die iOS-Plattform wird als erstes angezeigt. Wählen Sie unter Platforms die gewünschten Plattformen aus und deaktivieren Sie die nicht gewünschten.



5. Konfigurieren Sie je nach ausgewählter Plattform die folgenden Einstellungen:
   1. Bei Auswahl von iOS klicken Sie in der Liste Managed app bundle ID auf eine vorhandene App oder auf Add new.
      Hinweis: Wenn keine Apps für diese Plattform konfiguriert sind, ist die Liste leer und Sie müssen eine neue App hinzufügen.
      Wenn Sie auf Add klicken, wird ein Feld eingeblendet, in dem Sie einen Namen für die App eingeben können.
   2. Bei Auswahl von Android, Samsung KNOX, Android for Work oder Windows 8.1 Tablet:



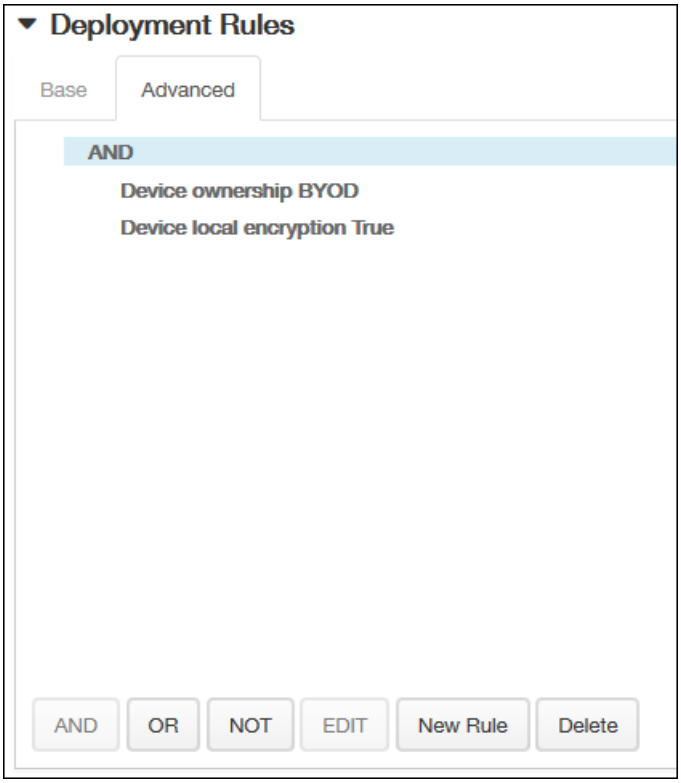
   Klicken Sie unter Apps to uninstall auf Add und führen Sie die folgenden Schritte aus:

   1. App name: Klicken Sie in der Liste auf eine vorhandene App oder klicken Sie auf Add, um einen neuen App-Namen einzugeben.
      Hinweis: Wenn keine Apps für diese Plattform konfiguriert sind, ist die Liste leer und Sie müssen neue Apps hinzufügen.
   2. Klicken Sie auf Add, um die App hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.

3. Wiederholen Sie die Schritte i und ii für jede App, die Sie der Deinstallationsrichtlinie hinzufügen möchten.
   Hinweis: Zum Löschen einer vorhandenen App aus der Deinstallationsrichtlinie zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf Delete zum Löschen des Eintrags oder auf Edit, um ihn beizubehalten.
   Zum Bearbeiten einer App zeigen Sie auf deren Zeile und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf Save, um die Änderungen zu speichern oder auf Cancel, um den Vorgang abzubrechen.

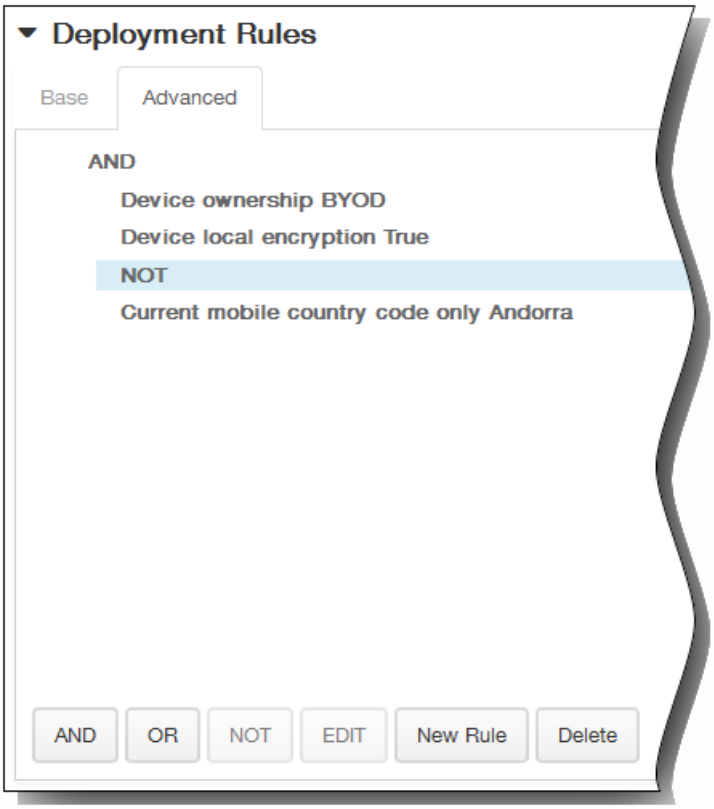
6. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
   3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
   4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.

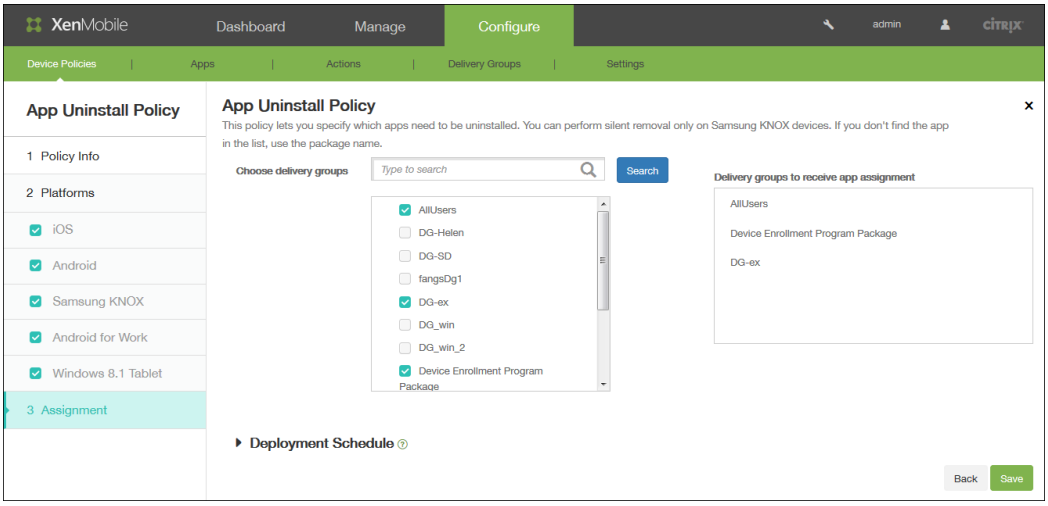


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.
   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



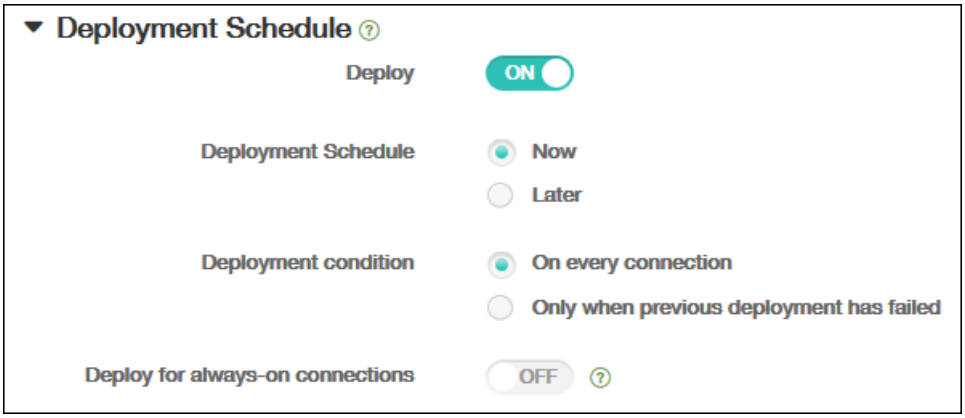
7. Klicken Sie auf Next. Die Seite Assignment für die Deinstallationsrichtlinie wird angezeigt.
8. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



9. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
   1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.

2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



10. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Dateirichtlinie für Android-Geräte hinzu

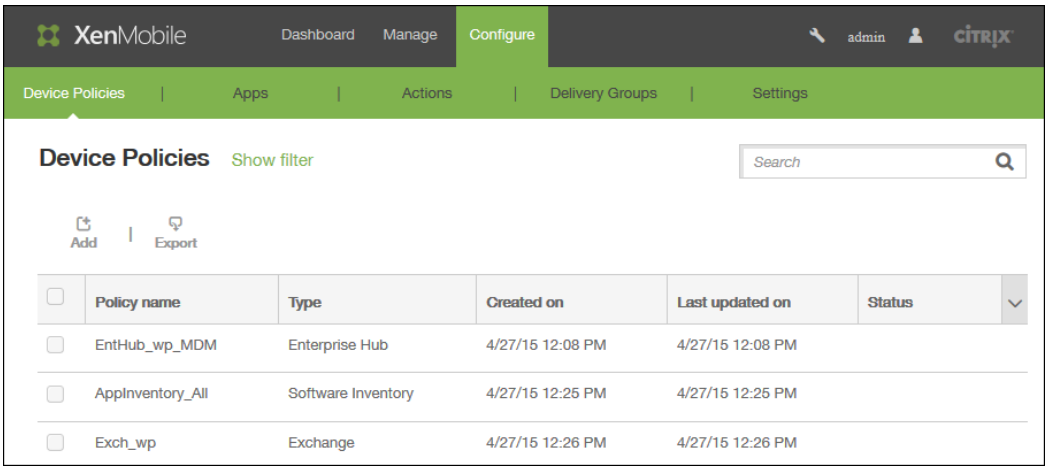
Jul 27, 2016

Sie können XenMobile Skriptdateien zum Durchführen bestimmter Funktionen für Benutzer hinzufügen und Sie können Dokumentdateien hinzufügen, die Benutzern von Android-Geräten auf deren Geräten zugänglich sein sollen. Beim Hinzufügen einer Datei können Sie festlegen, in welchem Verzeichnis diese auf dem Gerät gespeichert werden soll. Wenn Sie beispielsweise Android-Benutzern ein Unternehmensdokument oder eine PDF-Datei zukommen lassen möchten, können Sie die Datei auf den Geräten bereitstellen und die Benutzer dann darüber informieren, wo sie ist.

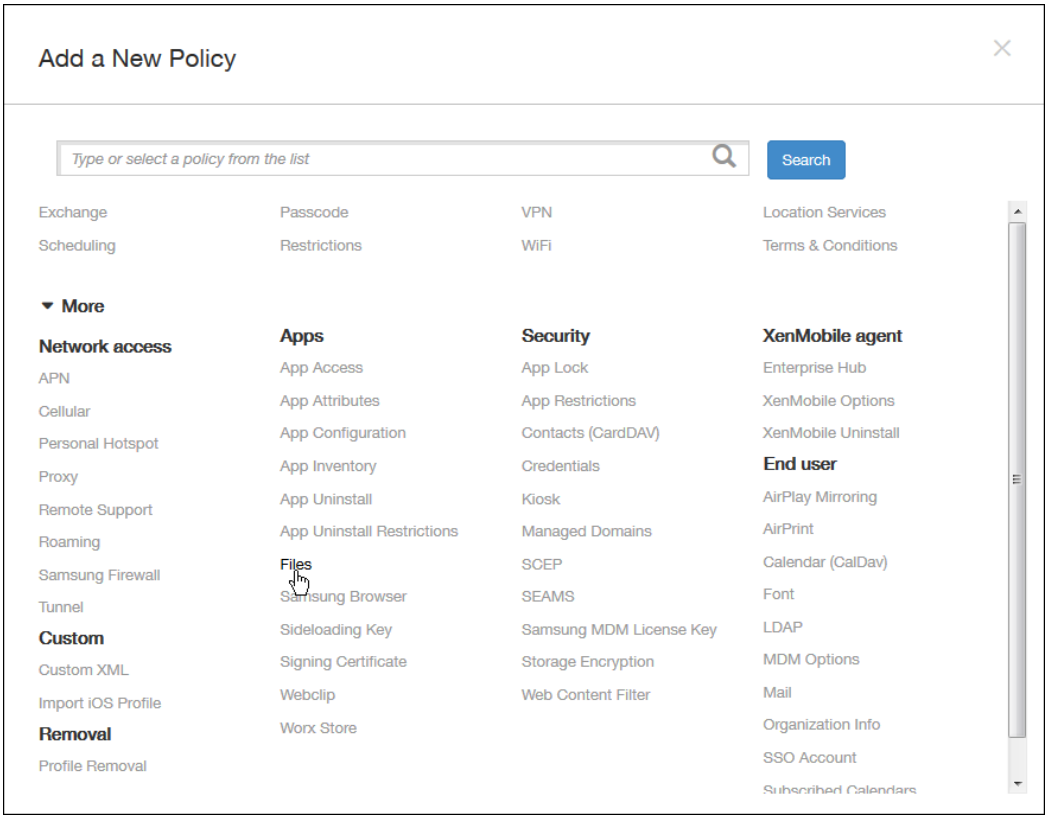
Sie können mit dieser Richtlinie die folgenden Dateitypen hinzufügen:

- Textbasierte Dateien (.xml, .html, .py, usw.)
- Andere Dateien (z. B. Dokumente, Präsentationen Bilder, Kalkulationstabellen)
- Nur für Windows Mobile und Windows CE: mit MortScript erstellte Skriptdateien

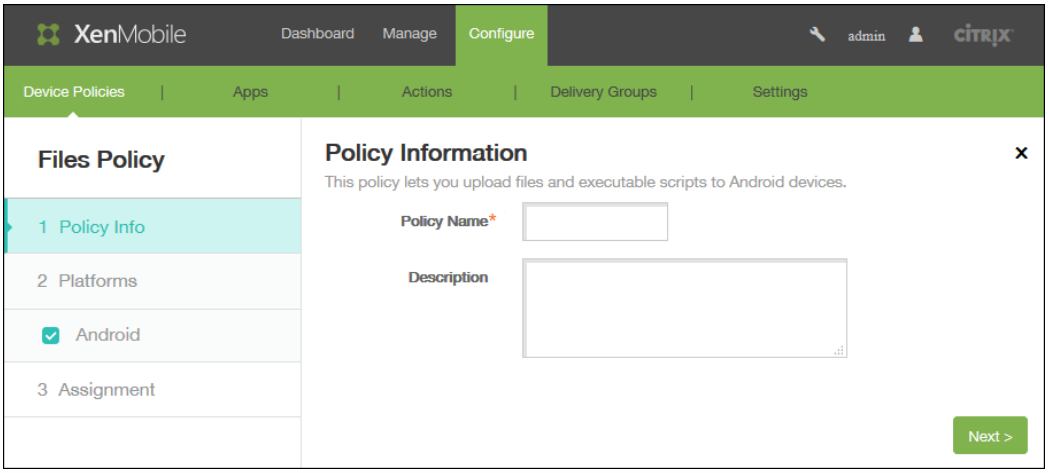
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



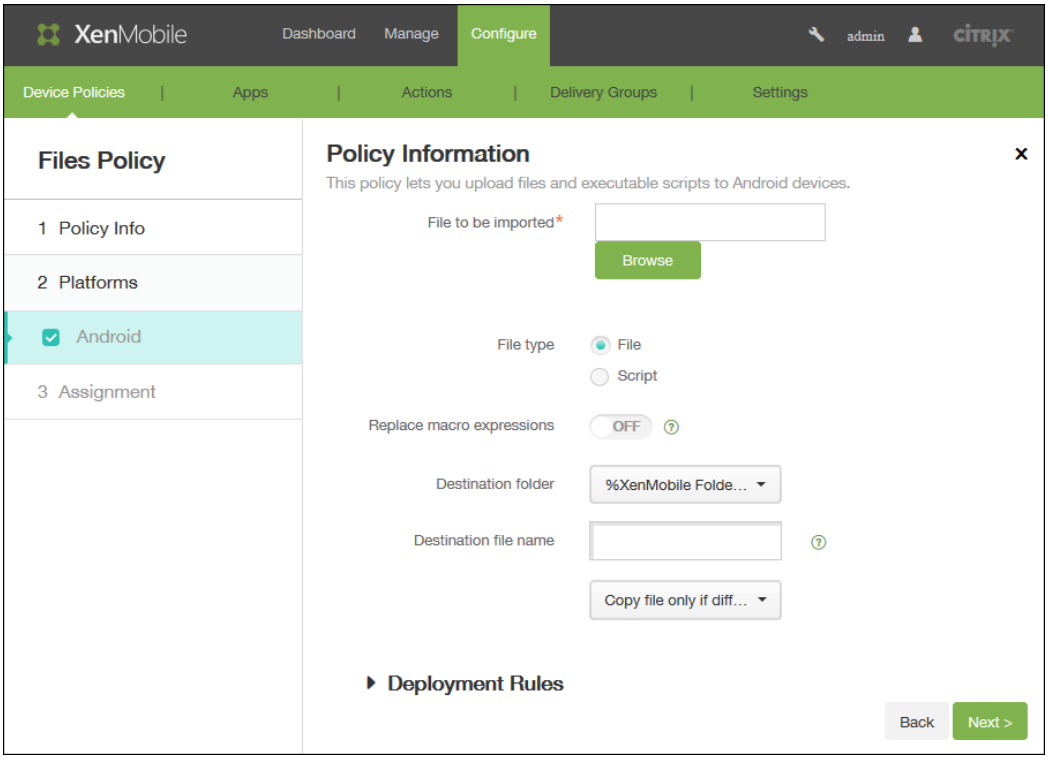
2. Klicken Sie auf Add. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter Apps auf Files. Die Informationsseite Files Policy wird angezeigt.



4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Informationsseite Android Platform wird angezeigt.

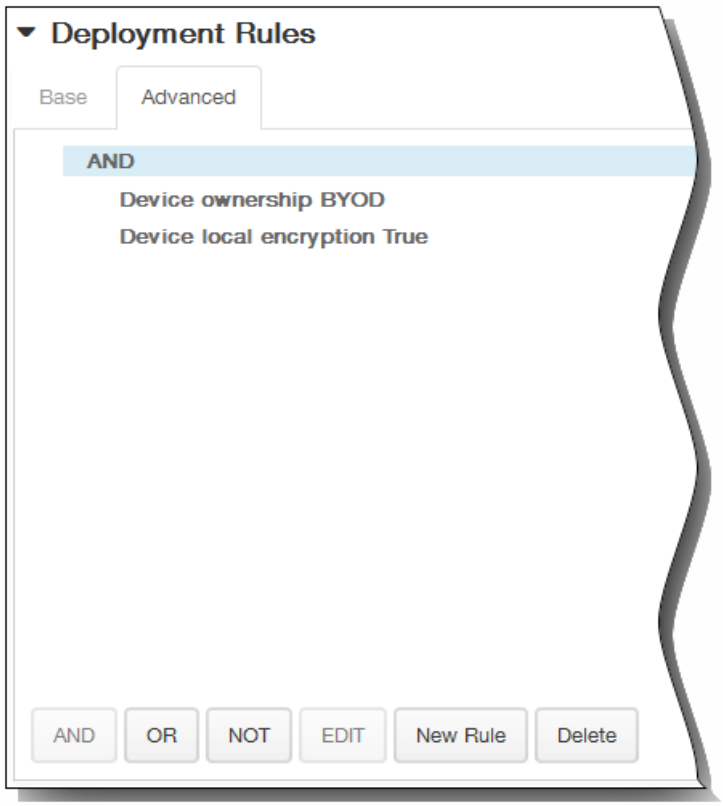


6. Geben Sie auf der Seite Android Platform die folgenden Informationen ein:
   1. File to be imported: Klicken Sie zur Auswahl der zu importierenden Datei auf Browse und navigieren Sie zum Speicherort der Datei.
   2. File type: Wählen Sie File oder Script. Wenn Sie Script auswählen, wird Execute immediately angezeigt. Legen Sie fest, ob das Skript ausgeführt werden soll, sobald die Datei hochgeladen wurde. Der Standardwert ist OFF.
   3. Replace macro expressions: Wählen Sie, ob die Namen von Makrotoken in einem Skript durch eine Geräte- oder Benutzereigenschaft ersetzt werden.
   4. Destination folder: Wählen Sie in der Liste den Speicherort für die hochgeladene Datei aus.
   5. Destination file name: Optional können Sie einen anderen Namen für die Datei eingeben, wenn er vor der Bereitstellung auf einem Gerät geändert werden muss.
   6. Copy file only if different: Wählen Sie in der Liste aus, ob die Datei kopiert werden soll, wenn sie nicht mit der vorhandenen Datei übereinstimmt, oder ob die vorhandene Datei überschrieben werden soll.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

   1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.

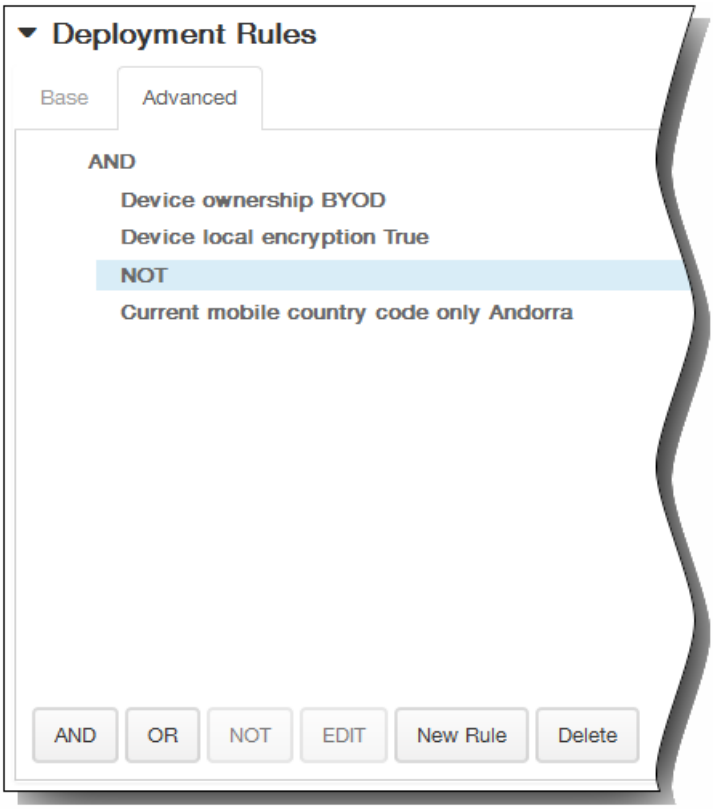
1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.

2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.

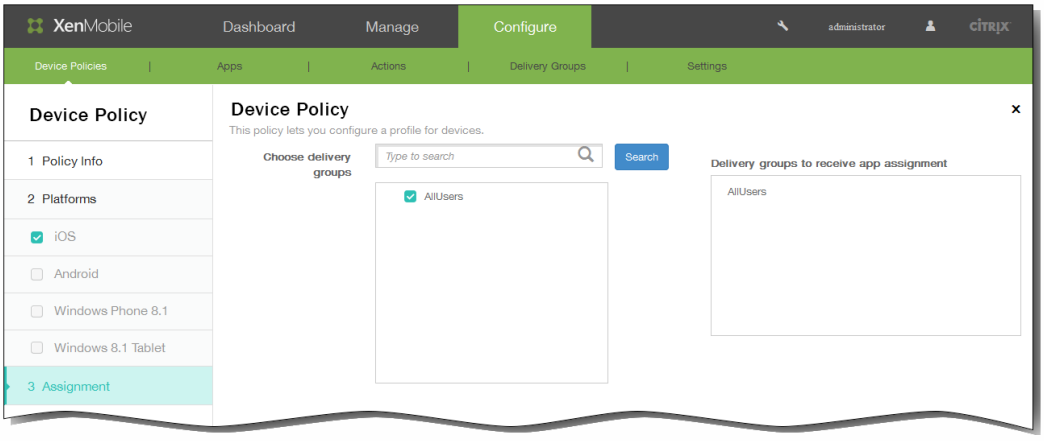


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.
   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



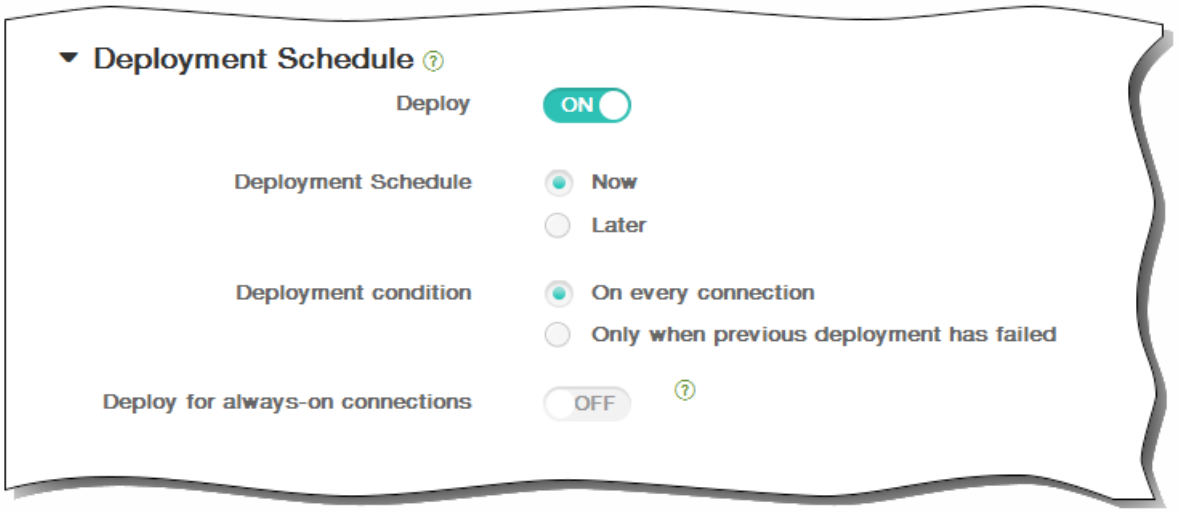
8. Klicken Sie auf Next. Die Zuweisungsseite für Files Policy wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



11. Klicken Sie auf Save, um die Richtlinie zu speichern.

APN-Geräterichtlinien

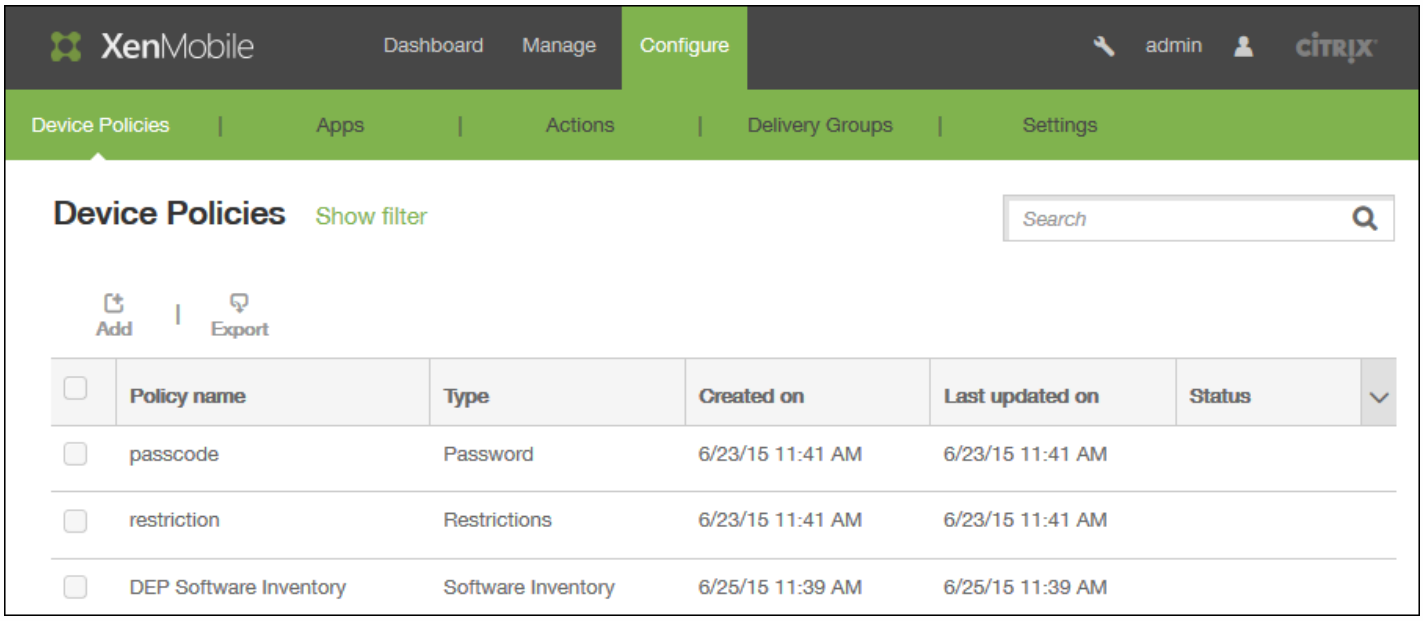
Nov 12, 2015

Sie können eine benutzerdefinierte Geräterichtlinie für Zugriffspunktnamen (APN) für iOS- und Android-Geräte hinzufügen. Sie verwenden diese Richtlinie, wenn Ihr Unternehmen keinen Consumer-APN verwendet, über den mit mobilen Geräten eine Verbindung zum Internet hergestellt werden kann. Eine APN-Richtlinie definiert die Einstellungen für die Verbindung zwischen den Geräten und dem General Packet Radio Service (GPRS) eines Netzbetreibers. Diese Einstellung ist bei den meisten neueren Telefonen bereits definiert.

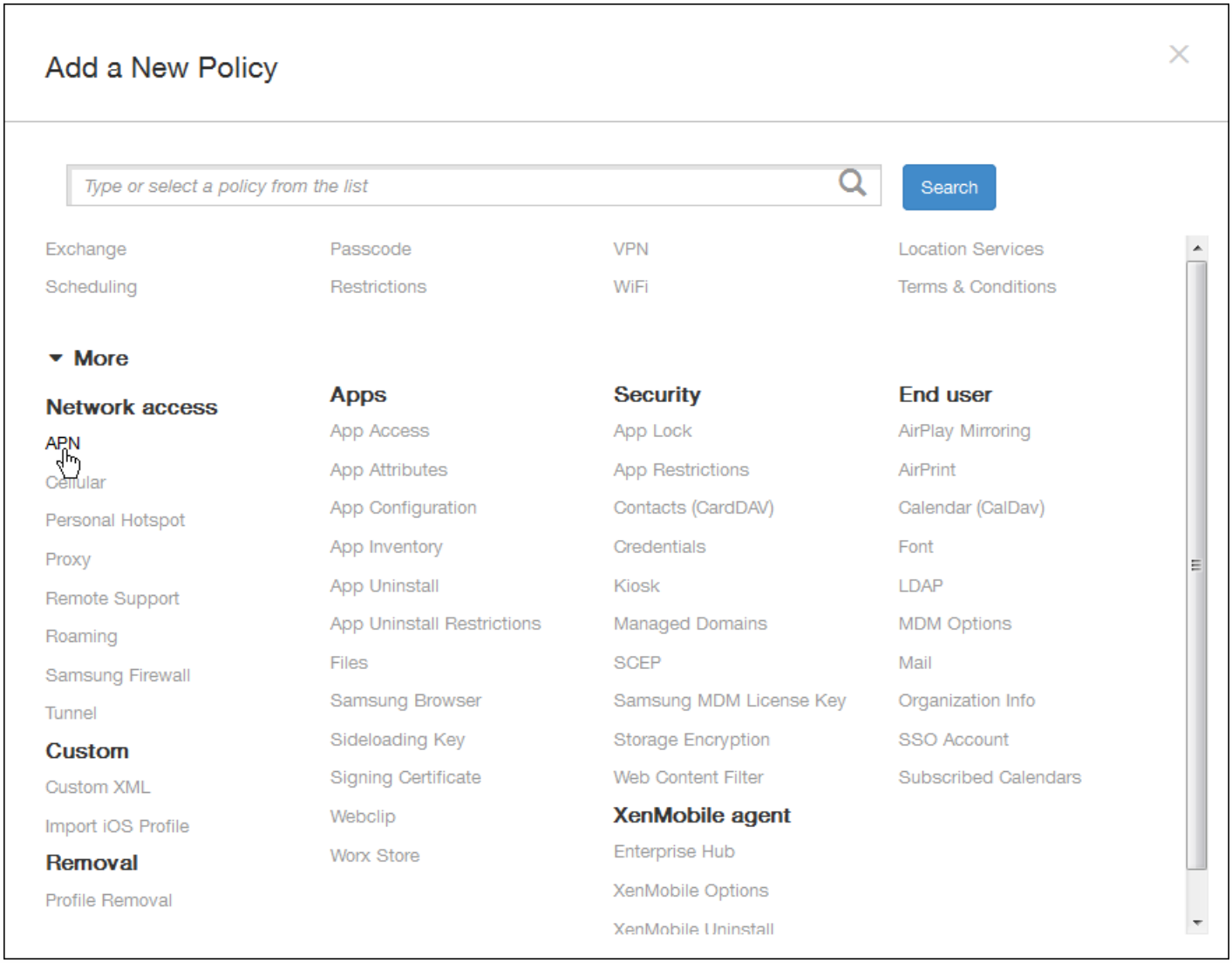
iOS-Einstellungen

Android-Einstellungen

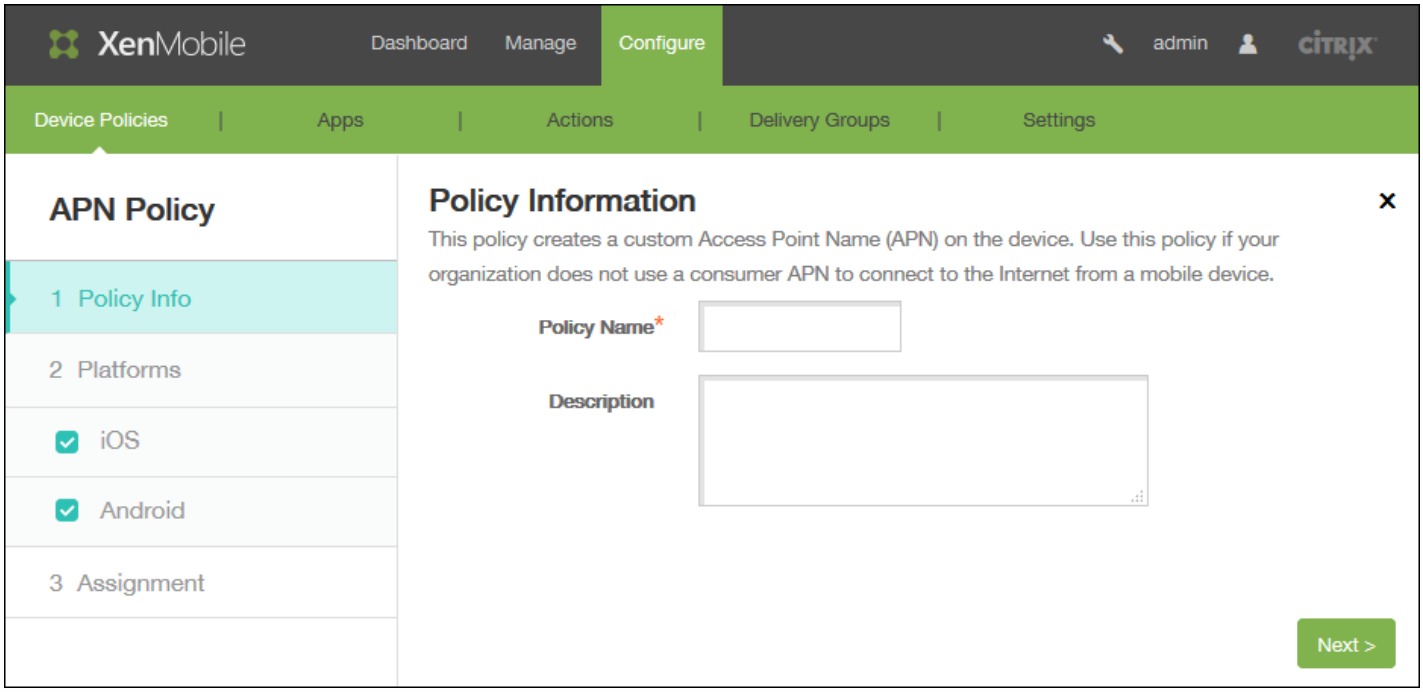
1. Klicken Sie in der XenMobile-Konsole auf **Configure > Device Policies**. Die Seite **Device Policies** wird angezeigt.



2. Klicken Sie auf **Add**, um eine neue Richtlinie hinzuzufügen. Die Seite **Add a new Policy** wird angezeigt.



3. Klicken Sie auf der Seite **Add a New Policy** auf **More** und dann unter **Network access** auf **APN**. Die Seite **APN Policy** wird angezeigt.



4. Geben Sie im Bereich **Policy Information** die folgenden Informationen ein:

- **Policy Name**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Description**: Geben Sie optional eine Beschreibung der Richtlinie ein.

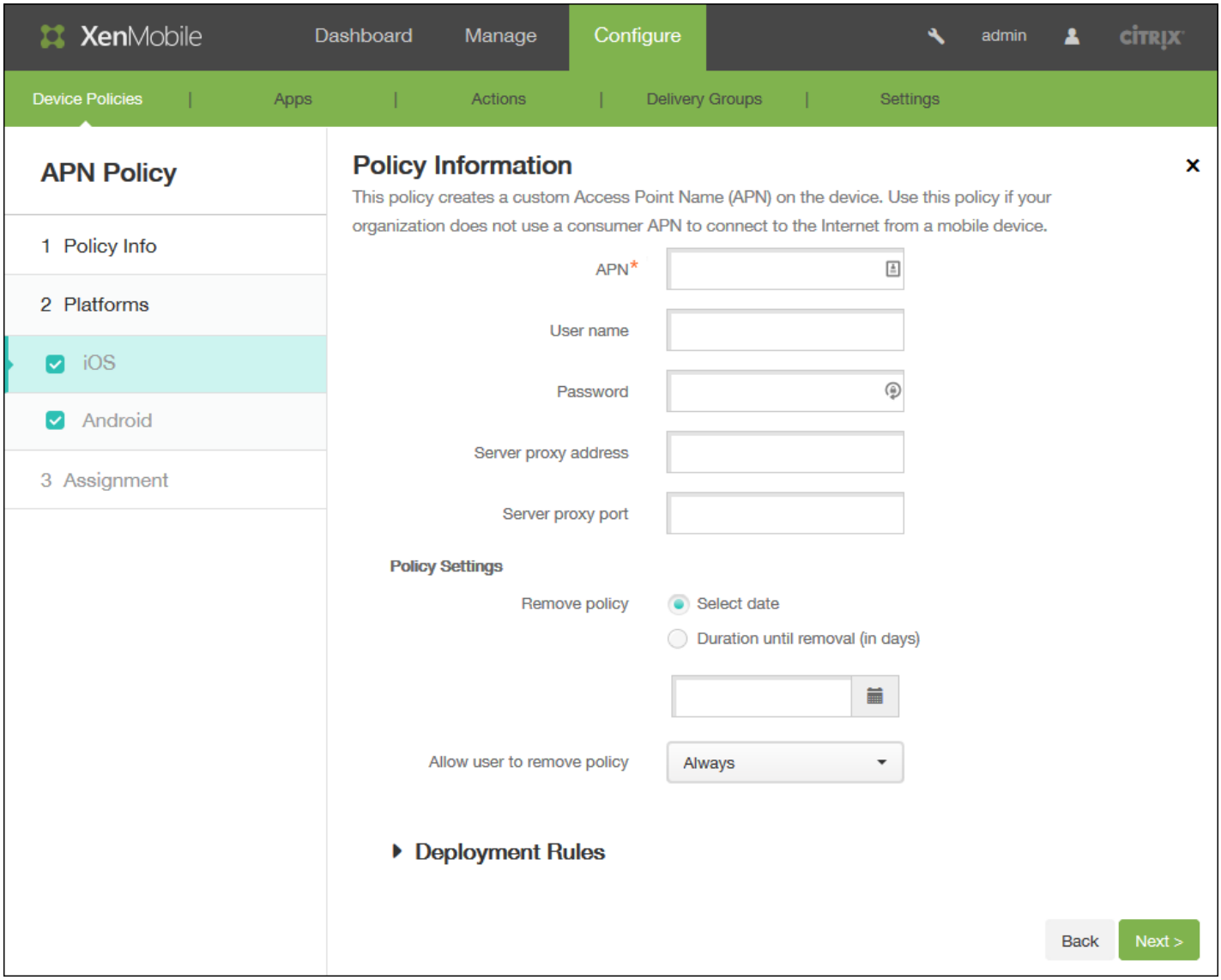
5. Klicken Sie auf **Next**. Die Seite **Policy Platforms** wird angezeigt.

Hinweis: Auf der Seite **Policy Platforms** sind alle Plattformen ausgewählt und die iOS-Plattform wird als erste angezeigt.

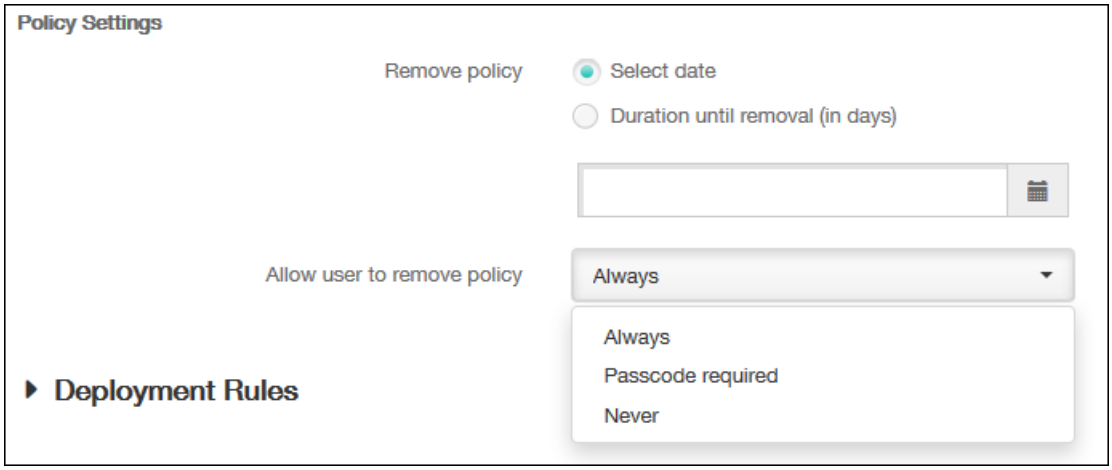
6. Wählen Sie unter **Platforms** die gewünschten Plattformen aus.

Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der Bereitstellungsregeln für diese Plattform unter Schritt 7.

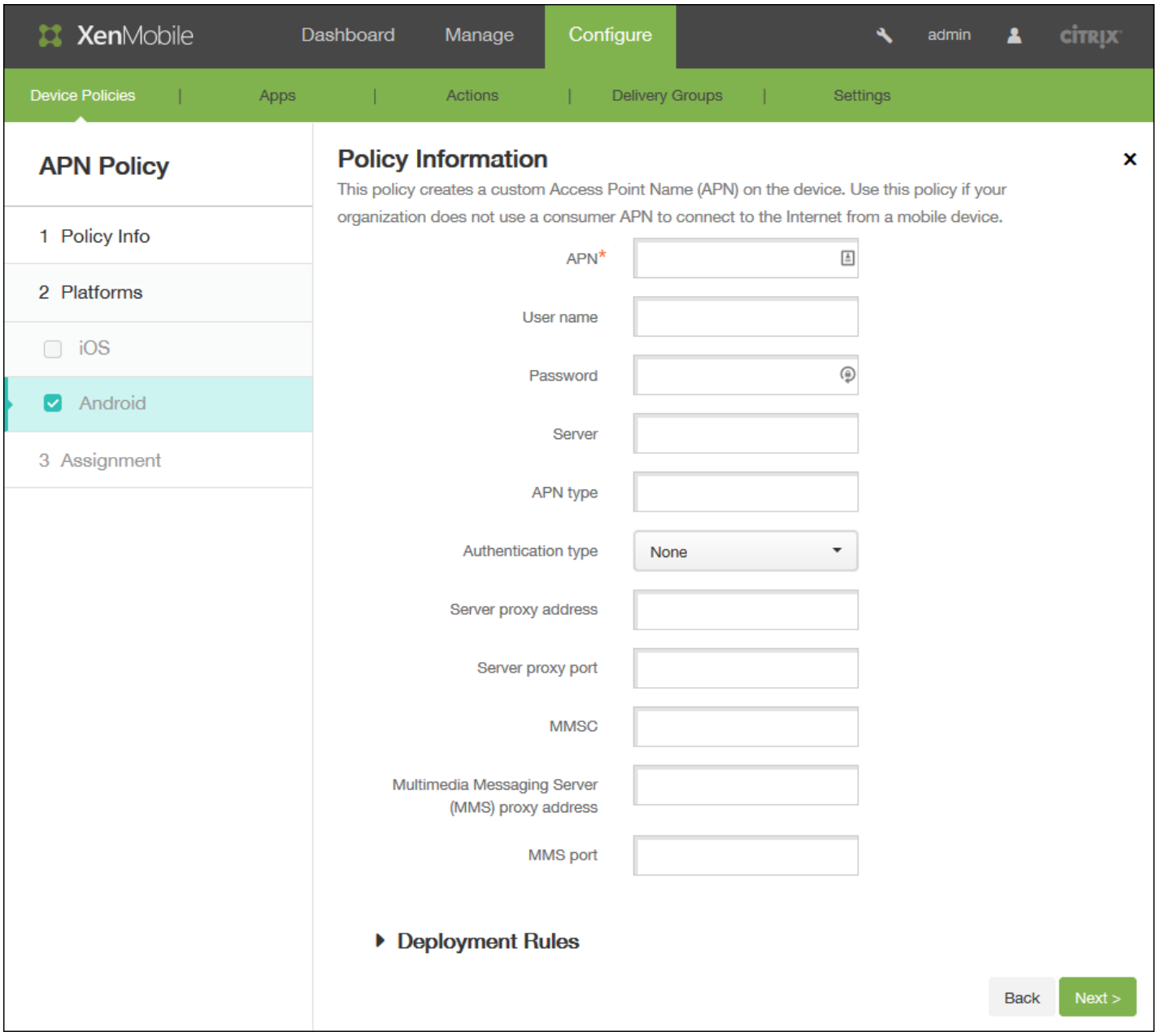
iOS-Einstellungen



- **APN**: Geben Sie den Namen des Zugriffspunkts ein. Der Name muss mit einem akzeptierten iOS-Zugriffspunkt übereinstimmen, sonst schlägt die Richtlinie fehl.
- **User name**: Diese Zeichenfolge repräsentiert den Benutzernamen für diesen APN. Fehlt der Benutzername , wird die Zeichenfolge während der Profilinstallation angefordert.
- **Password**: Das Kennwort für den Benutzer für den APN. Für höhere Sicherheit ist das Kennwort codiert. Fehlt es, fordert das Gerät die Zeichenfolge während der Profilinstallation an.
- **Server proxy address**: IP-Adresse oder URL des APN-Proxy
- **Server proxy port**: Portnummer des APN-Proxys. Sie ist erforderlich, wenn Sie eine Serverproxyadresse eingegeben haben.
- Klicken Sie unter **Policy Settings** für **Remove policy** auf **Select date** oder **Duration until removal (in days)**.
  - Bei Auswahl von **Select date** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Allow user to remove policy** auf **Always**, **Password required** oder **Never**.
  - Bei Auswahl von **Password required** geben Sie für **Removal password** das Kennwort ein.



Android-Einstellungen

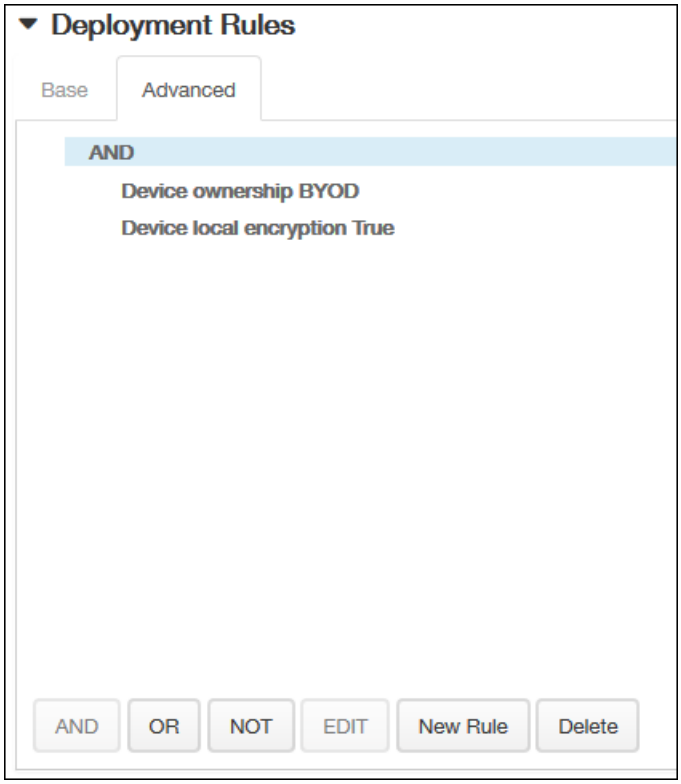


- **APN**: Geben Sie den Namen des Zugriffspunkts ein. Der Name muss mit einem akzeptierten Android-Zugriffspunkt übereinstimmen, sonst schlägt die Richtlinie fehl.
- **User name**: Diese Zeichenfolge repräsentiert den Benutzernamen für diesen APN. Fehlt der Benutzername, wird die Zeichenfolge während der Profilinstallation angefordert.
- **Password**: Das Kennwort für den Benutzer für den APN. Für höhere Sicherheit ist das Kennwort codiert. Fehlt es, fordert das Gerät die Zeichenfolge während der Profilinstallation an.
- **Server**: Diese Einstellung stammt aus der Zeit vor Smartphones und ist in der Regel leer. Sie verweist auf einen WAP-Gateway-Server (Wireless Application-Protokoll) für Telefone, bei denen der Zugriff auf oder das Rendern von Standardwebsites nicht möglich war.
- **APN type**: Diese Einstellung muss der vom Netzbetreiber beabsichtigten Nutzung des Zugriffspunkts entsprechen. Es handelt sich um eine durch Trennzeichen getrennte Zeichenfolge mit APN-Dienstspezifizierern, die den vom Netzbetreiber veröffentlichten Definitionen entsprechen müssen. Beispiele:
  - *. Der gesamte Datenverkehr läuft über diesen Zugriffspunkt.
  - mms. Multimediadatenverkehr läuft über diesen Zugriffspunkt.
  - default: Der gesamte Datenverkehr, einschließlich Multimedia, läuft über diesen Zugriffspunkt.
  - supl. Secure User Plane Location wird im Zusammenhang mit Assisted Global Positioning System verwendet.
  - dun: DFÜ-Netzwerk ist veraltet und dürfte nur noch selten verwendet werden.
  - hipri. Netzwerk mit hoher Priorität.
  - fota. Firmware Over-the-Air wird zur Übertragung von Firmwareupdates verwendet.
- **Authentication type**: Klicken Sie in der Liste auf den gewünschten Authentifizierungstyp. Standardwert ist "None".
- **Server proxy address**: IP-Adresse oder URL des APN-HTTP-Proxys des Netzbetreibers.
- **Server proxy port**: Portnummer des APN-Proxys. Sie ist erforderlich, wenn Sie eine Serverproxyadresse eingegeben haben.
- **MMSC**: Die vom Netzbetreiber angegebene Adresse des MMS Gateway Servers.
- Multimedia Messaging Server (MMS) proxy address: Dies ist der Multimedia-Messaging-Dienstserver für MMS. MMS ist der Nachfolger von SMS und eignet sich für das Senden größerer Nachrichten mit Multimediainhalten z. B. Bilder oder Videos. Diese Server erfordern bestimmte Protokolle (z. B. MM1,... MM11).
- **MMS port**: Der Port des MMS-Proxyservers.

7. Erweitern Sie **Deployment Rules** und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte **Base** wird standardmäßig angezeigt.

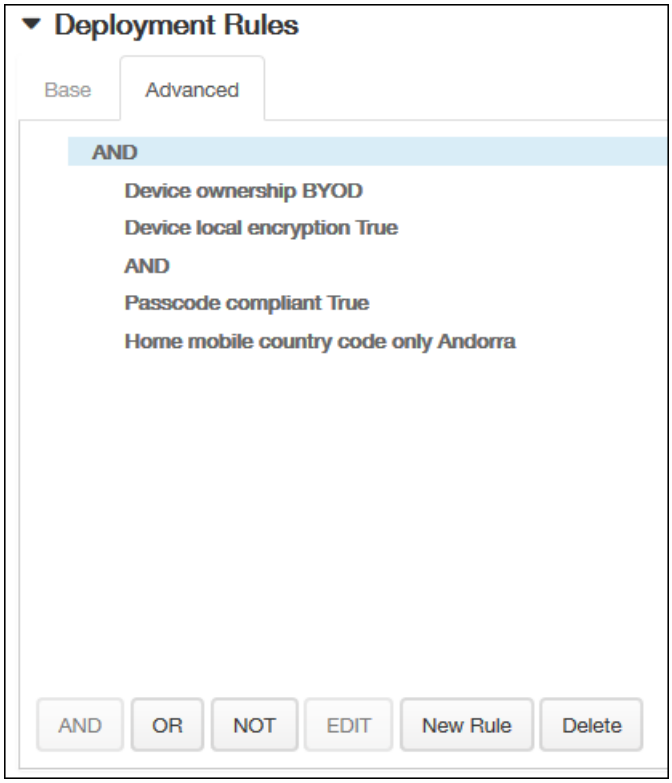
- Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
  - Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist **All**.
  - Klicken Sie auf **New Rule**, um Bedingungen zu definieren.
  - Klicken Sie in der Liste auf Bedingungen wie **Device ownership** oder **BYOD** (siehe Abbildung oben).
  - Klicken Sie erneut auf **New Rule**, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.

- Klicken Sie auf die Registerkarte **Advanced**, um die Regeln mit booleschen Optionen zu kombinieren. Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.



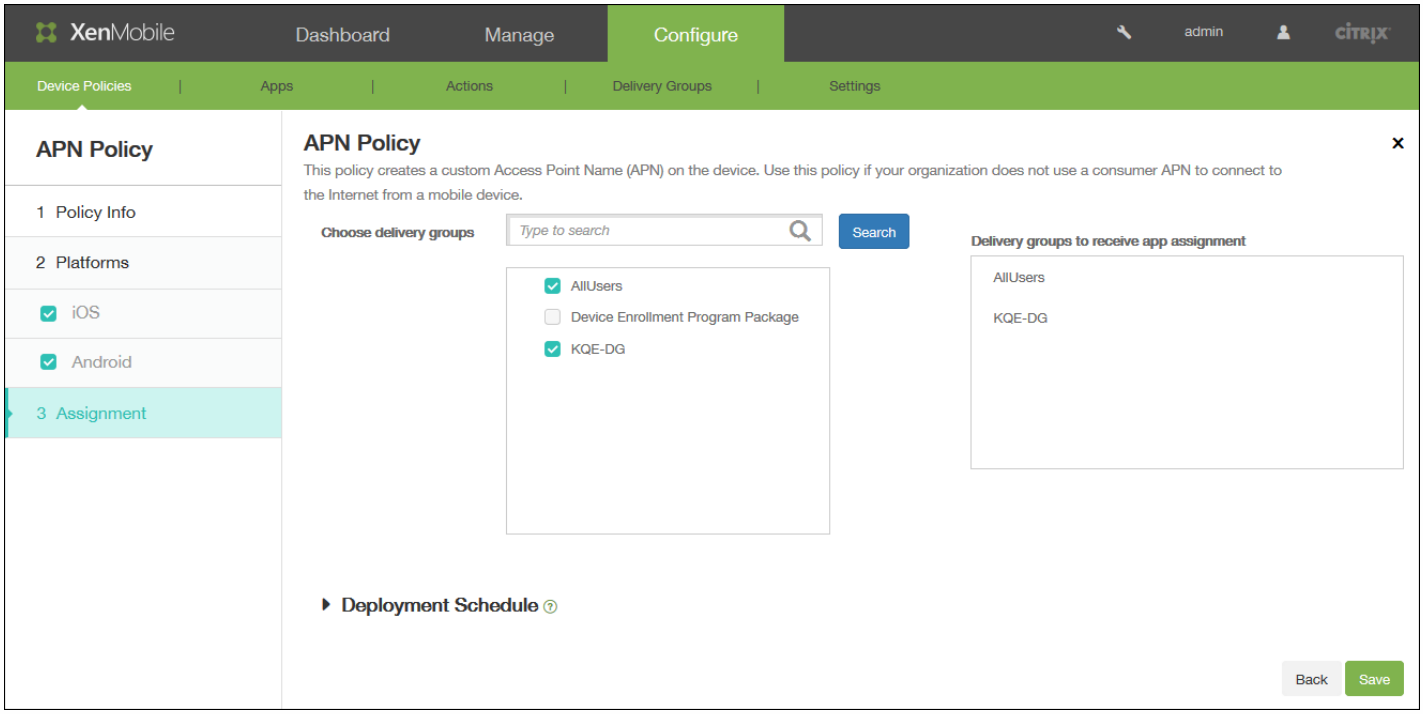
- Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
  - Klicken Sie auf **AND**, **OR** oder **NOT**.
  - Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
    Sie können jederzeit auf eine Bedingung und dann auf **EDIT** klicken, um die Bedingung zu ändern, oder auf **Delete**, um die Bedingung zu löschen.
  - Klicken Sie erneut auf **New Rule**, wenn Sie weitere Bedingungen hinzufügen möchten.

    In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



8. Klicken Sie auf **Next**. Die Seite **Assignment** für die APN-Richtlinie wird angezeigt.

9. Machen Sie neben **Choose delivery groups** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Delivery groups to receive app assignment** angezeigt.



10. Erweitern Sie **Deployment Schedule** und konfigurieren Sie folgende Einstellungen:

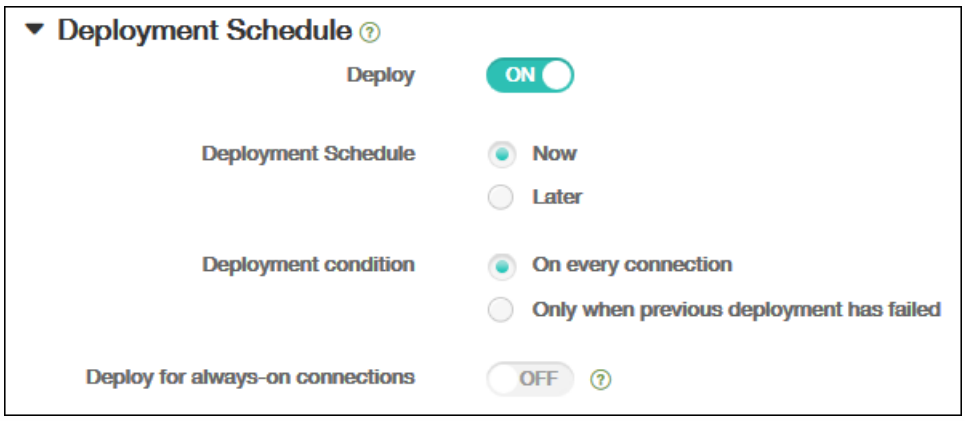
- Klicken Sie neben **Deploy** auf **ON**, um die Bereitstellung zu planen, oder auf **OFF**, um die Bereitstellung zu verhindern. Die Standardeinstellung ist **ON**. Wenn Sie **OFF** auswählen, müssen keine anderen Optionen konfiguriert werden.

- Klicken Sie neben **Deployment schedule** auf **Now** oder **Later**. Die Standardeinstellung ist **Now**.
- Wenn Sie auf **Later** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Deployment condition** auf **On every connection** oder auf **Only when previous deployment has failed**. Die Standardeinstellung ist **On every connection**.
- Klicken Sie neben **Deploy for always-on connection** auf **ON** oder **OFF**. Die Standardeinstellung ist **OFF**.

Hinweis:

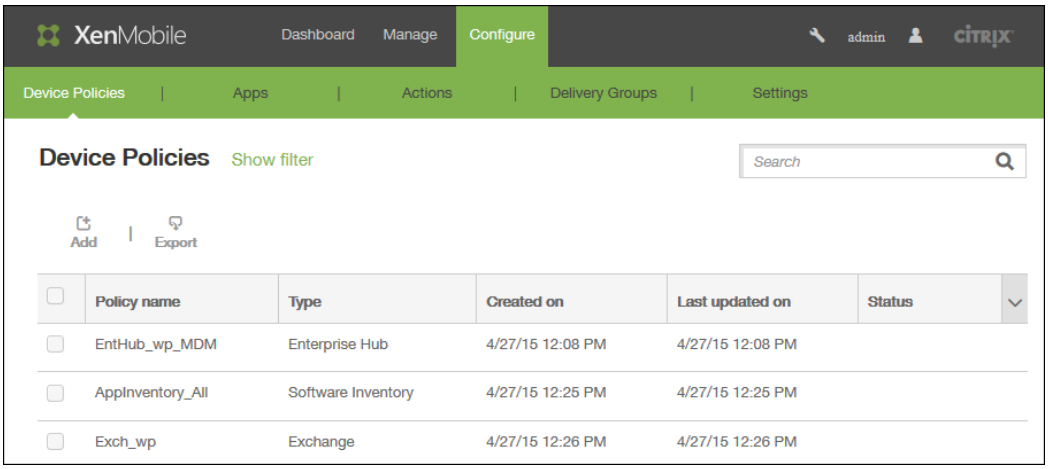
Diese Option gilt, wenn Sie unter **Settings > Server Properties** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

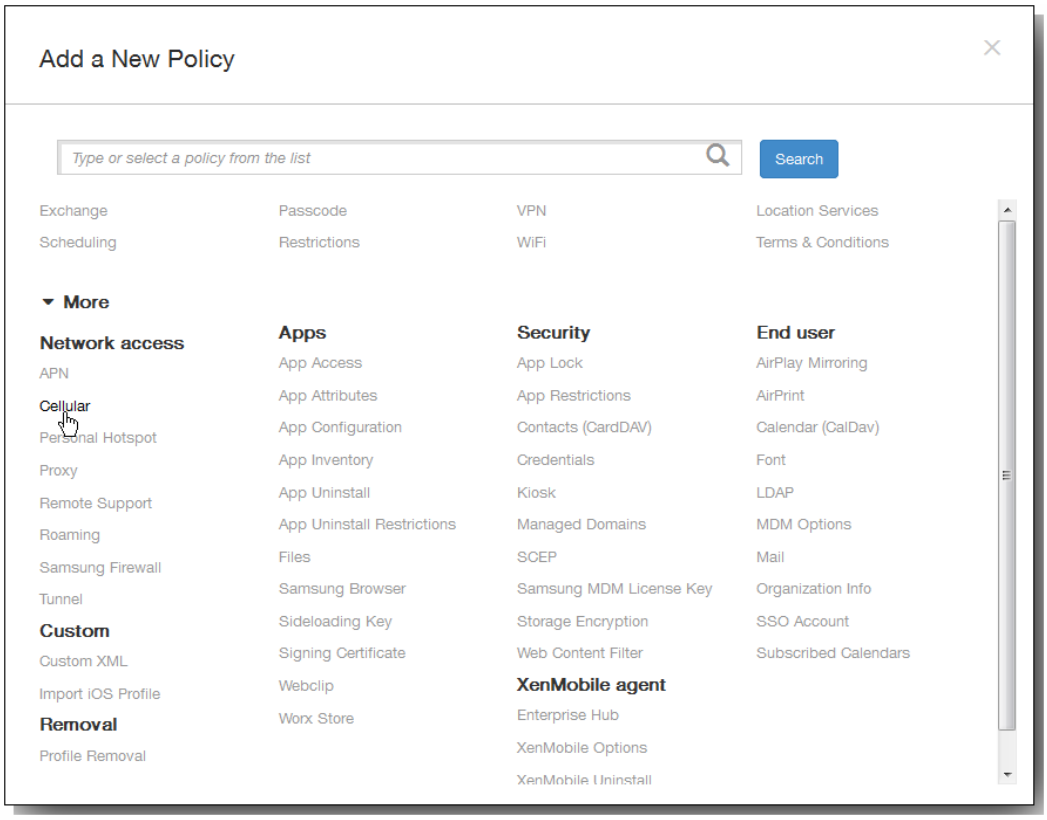
Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Deploy for always on connection**, denn diese Option gilt nicht für iOS.

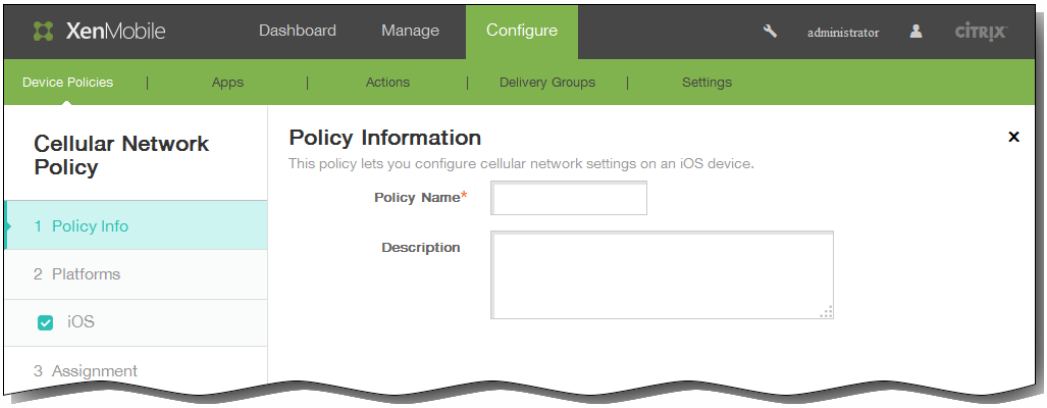


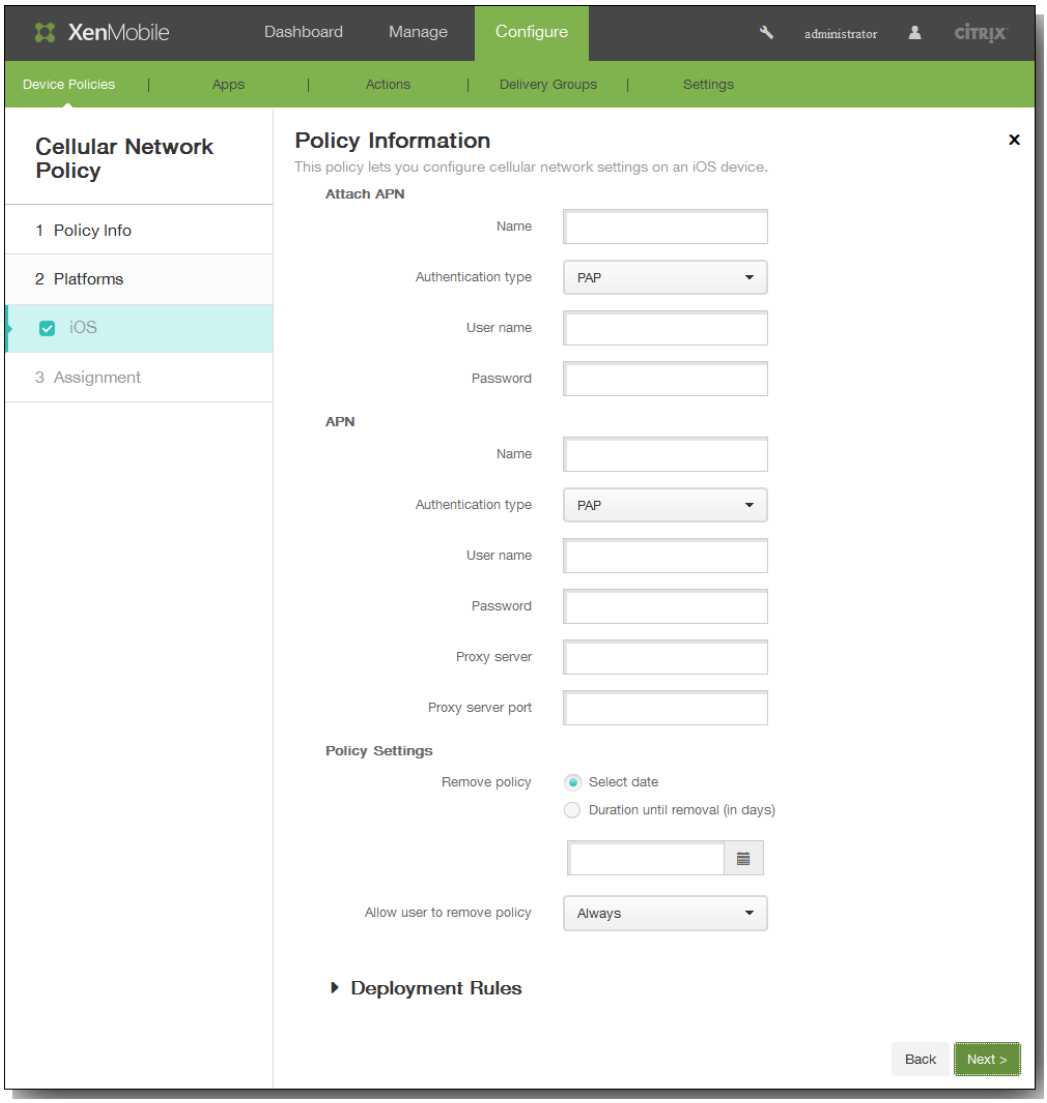
11. Klicken Sie auf **Save**, um die Richtlinie zu speichern.

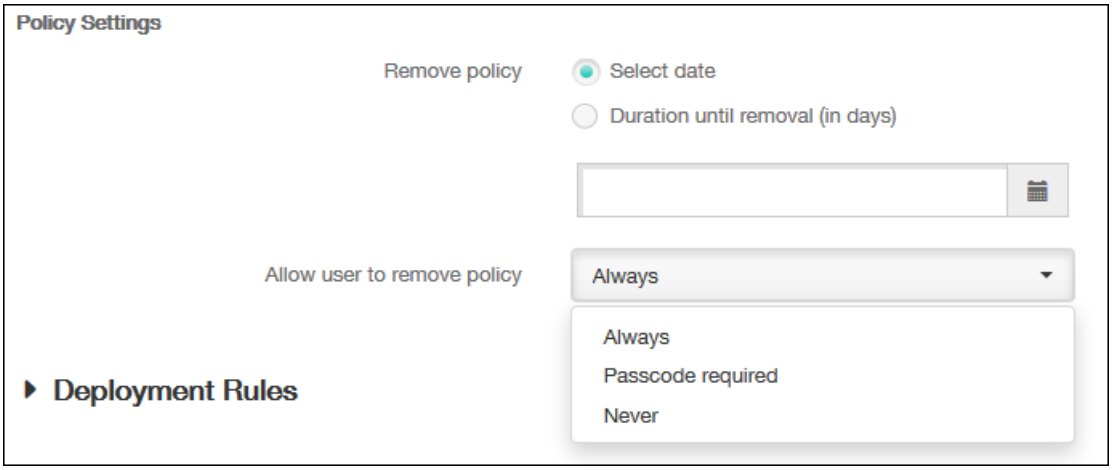
So fügen Sie eine Mobilfunkrichtlinie für iOS-Geräte hinzu

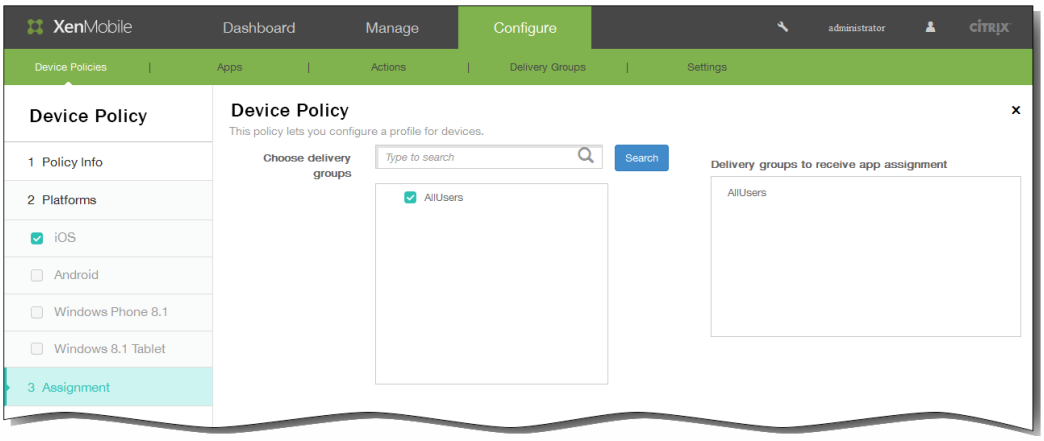


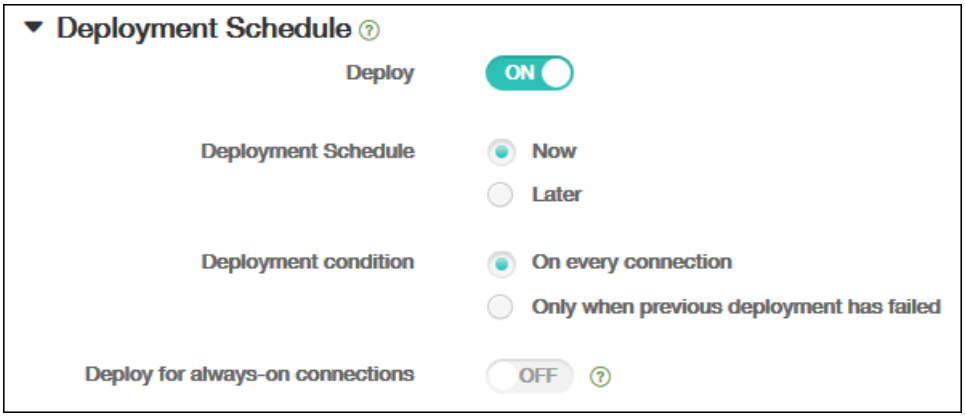






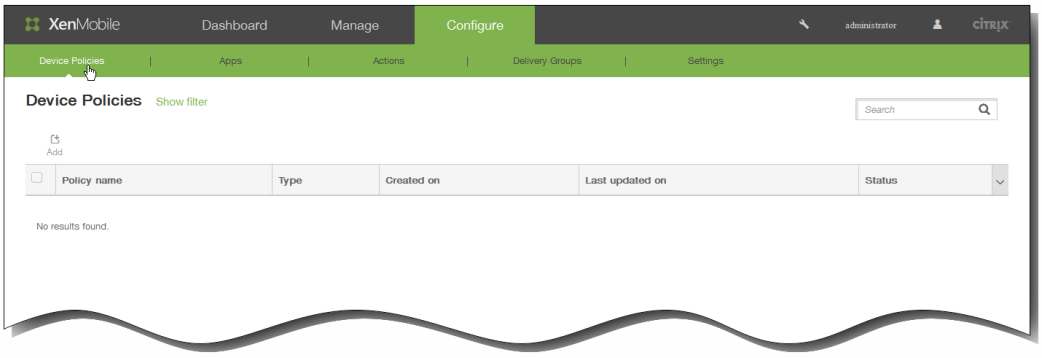


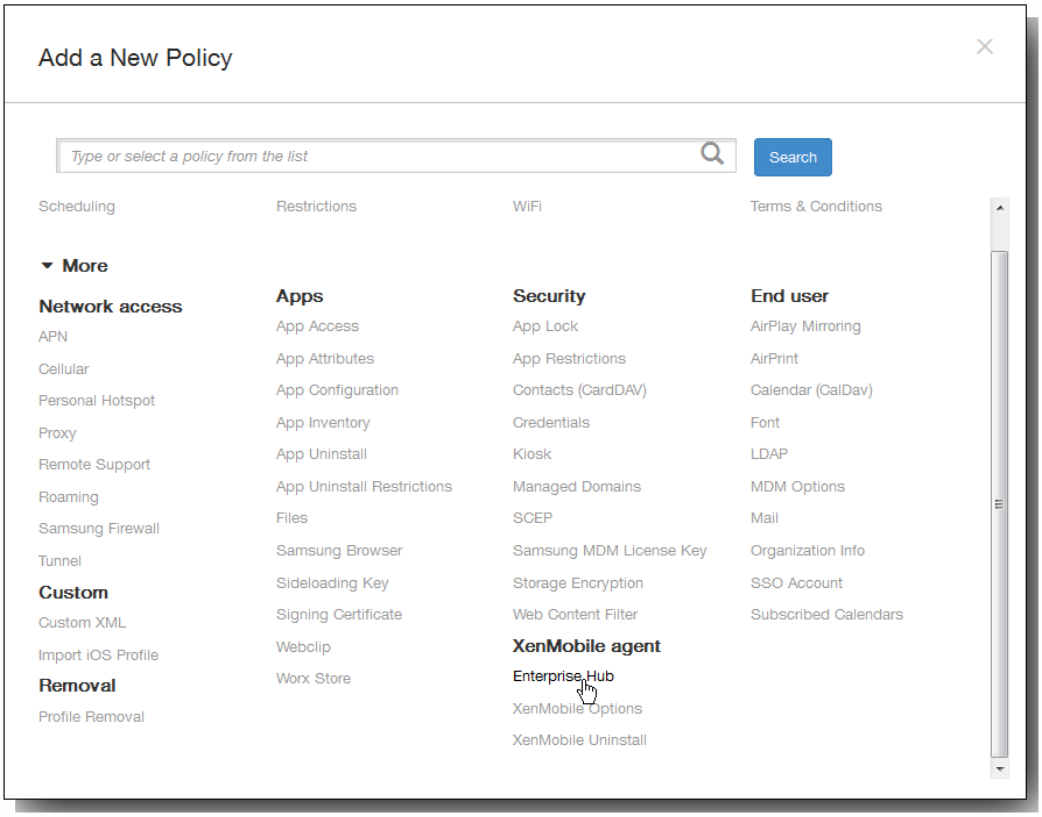


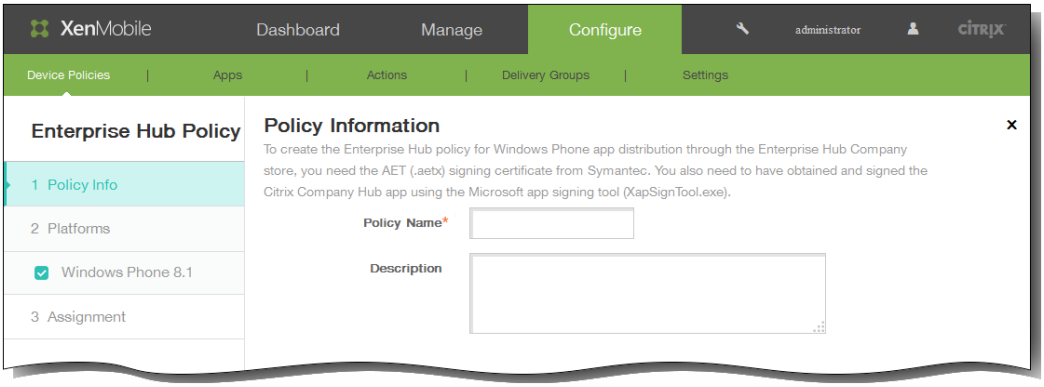


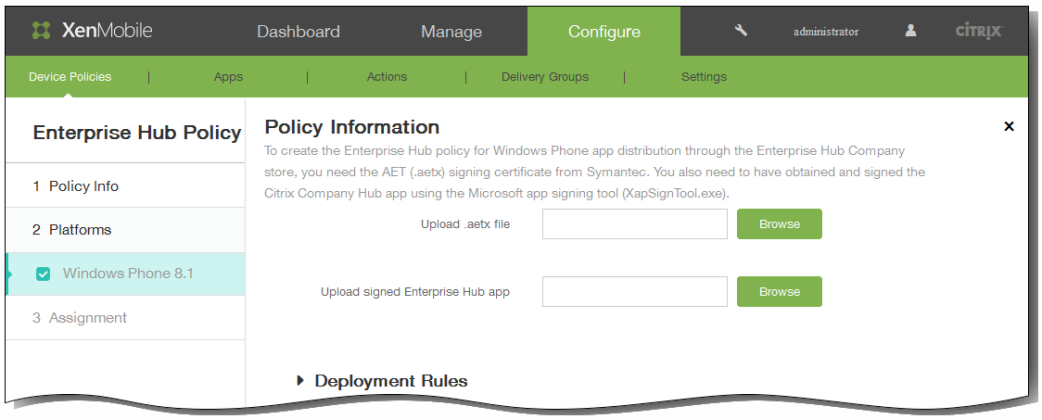
So fügen Sie eine Enterprise Hub-Richtlinie für Windows Phone 8.1-Geräte hinzu

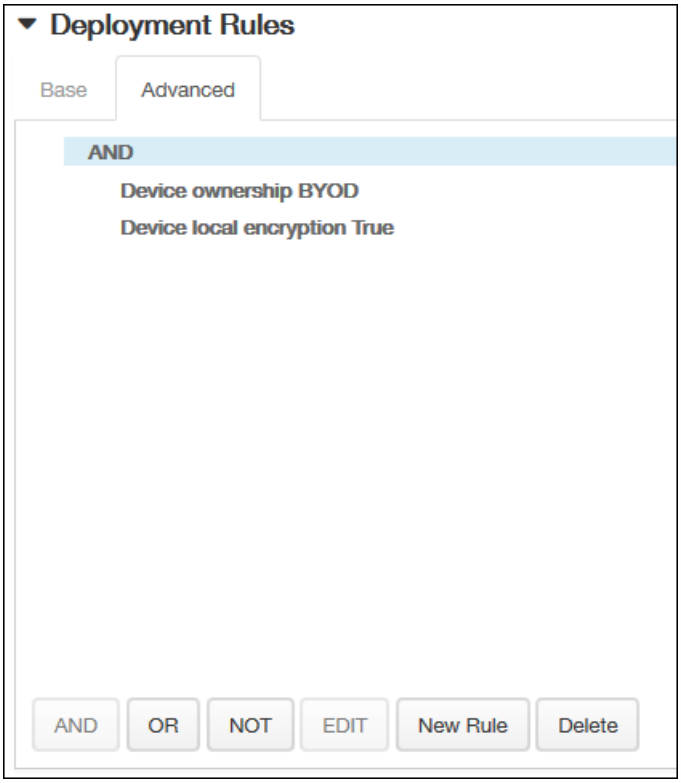
-
-

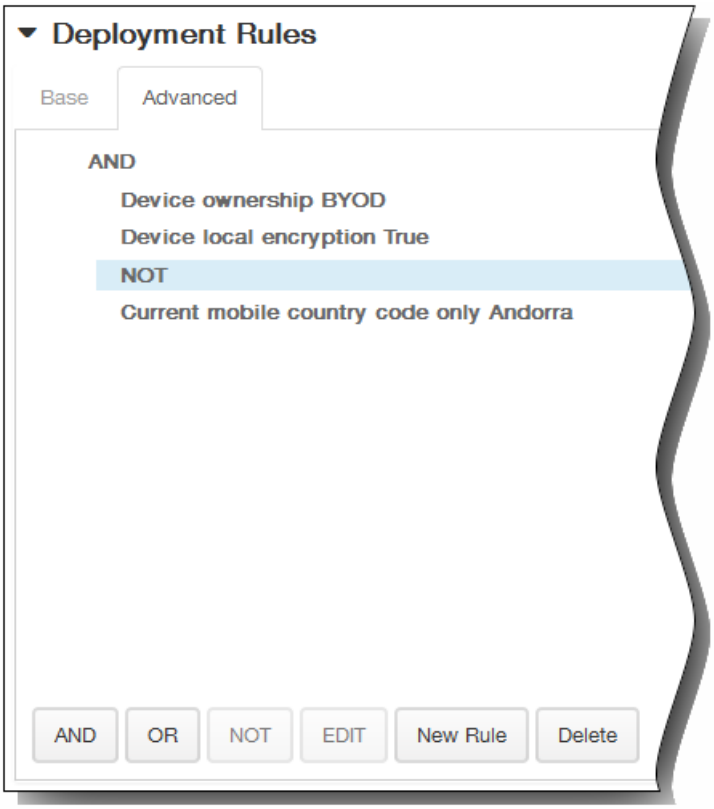


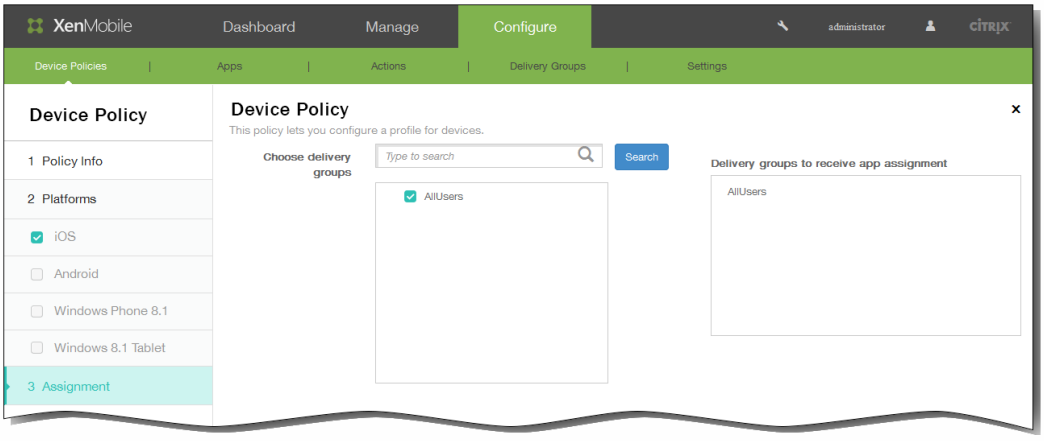


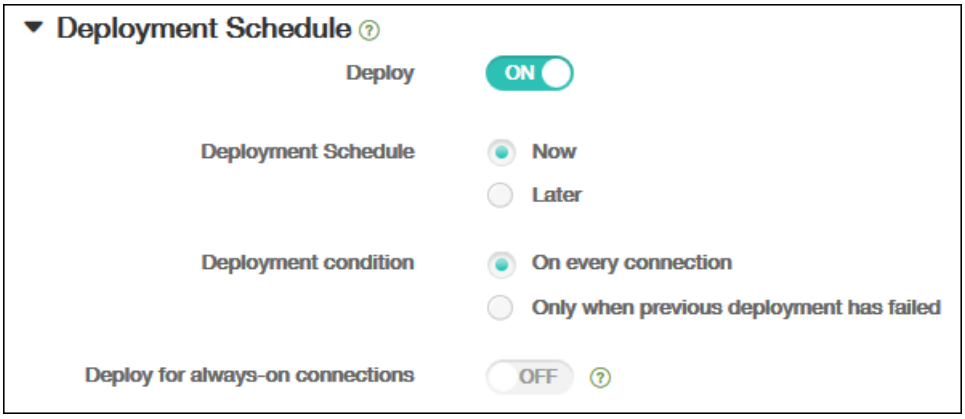




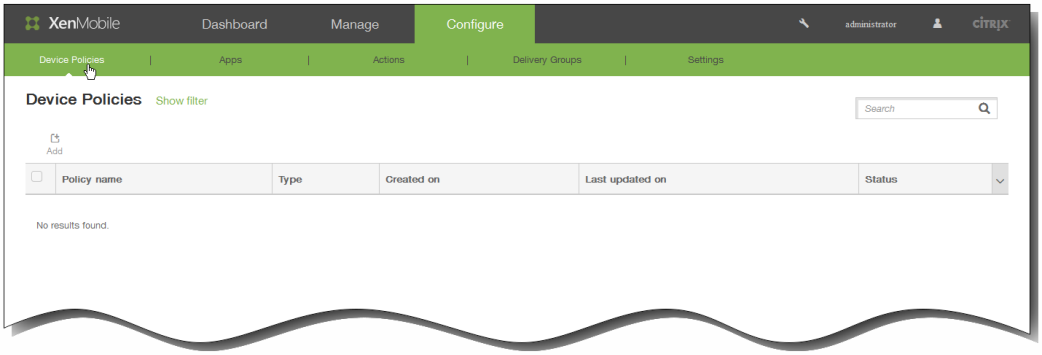


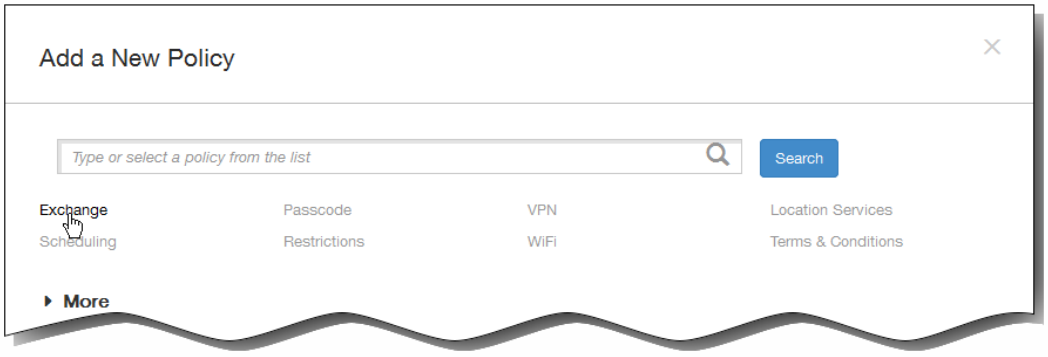


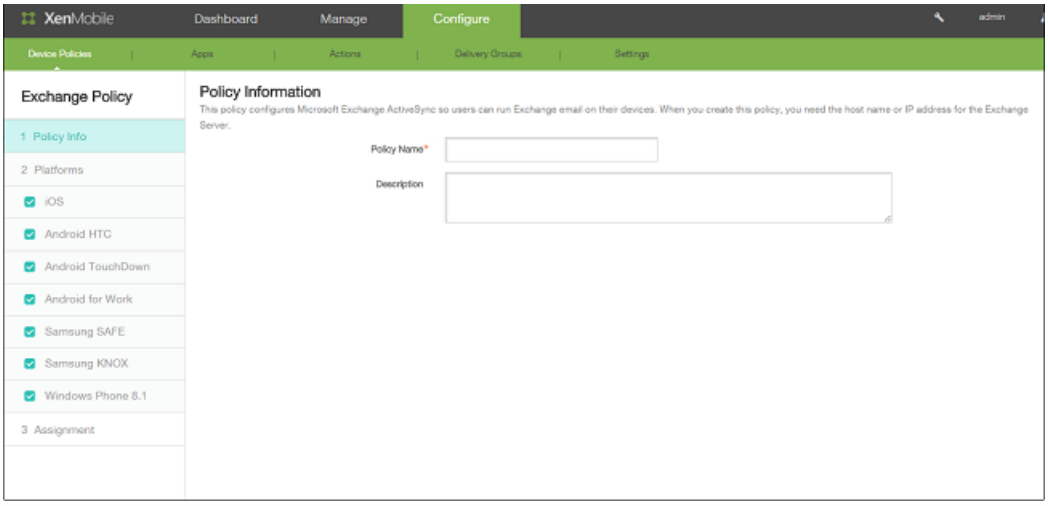




Microsoft Exchange ActiveSync-Geräterichtlinien



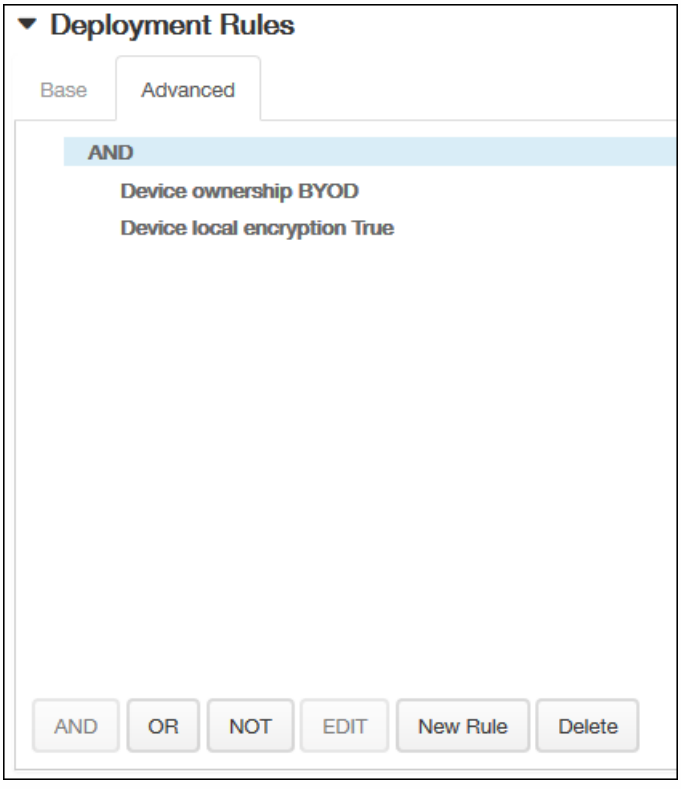


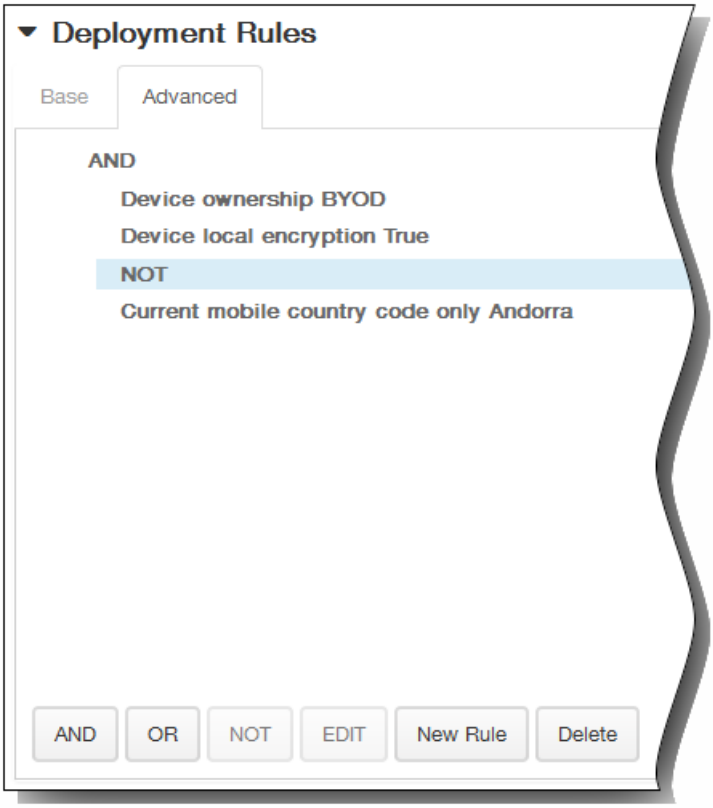


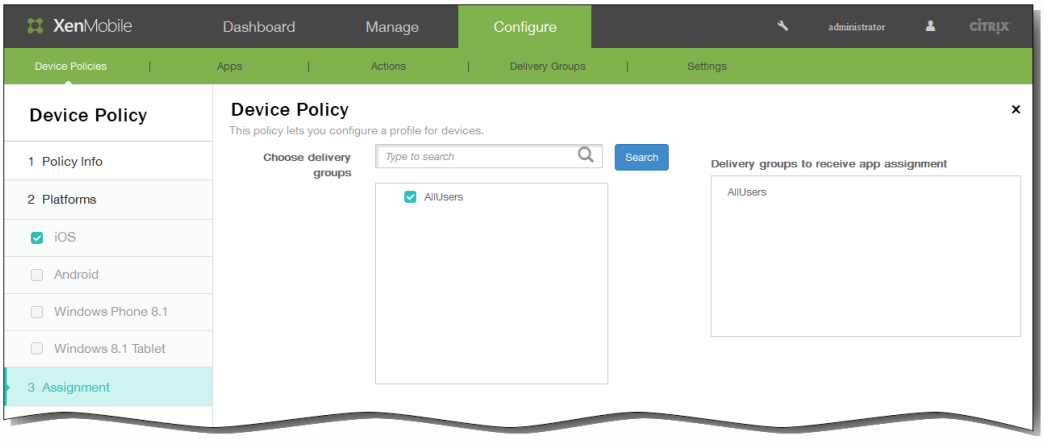
-
-

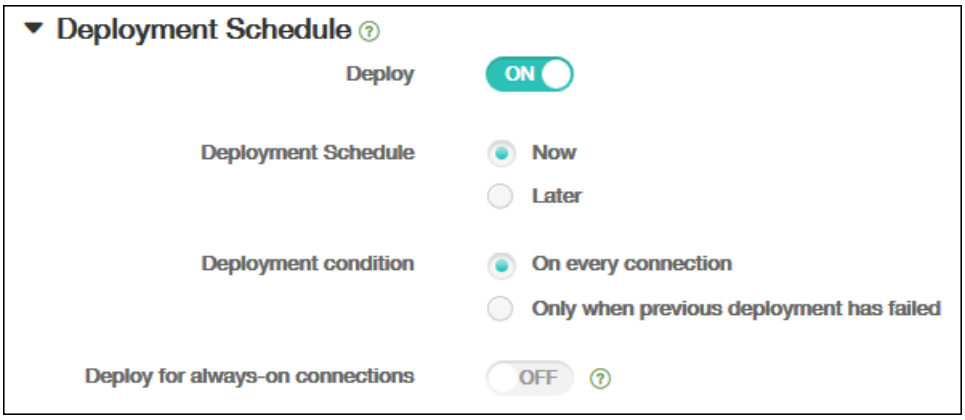
-
-

-

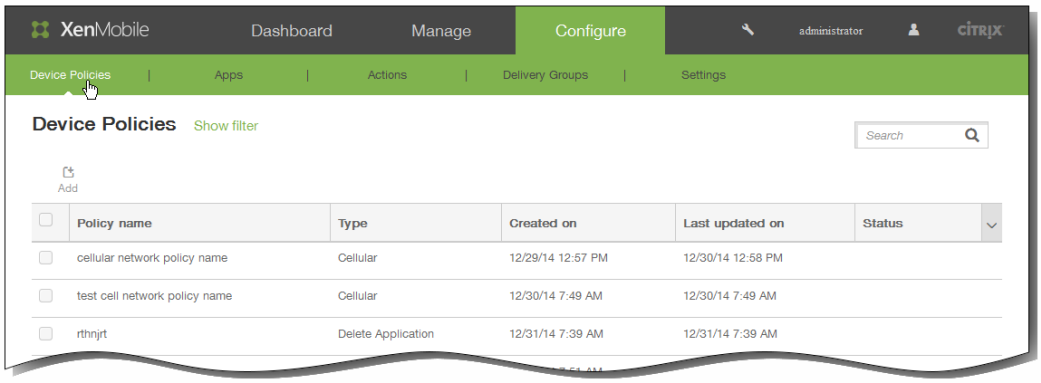


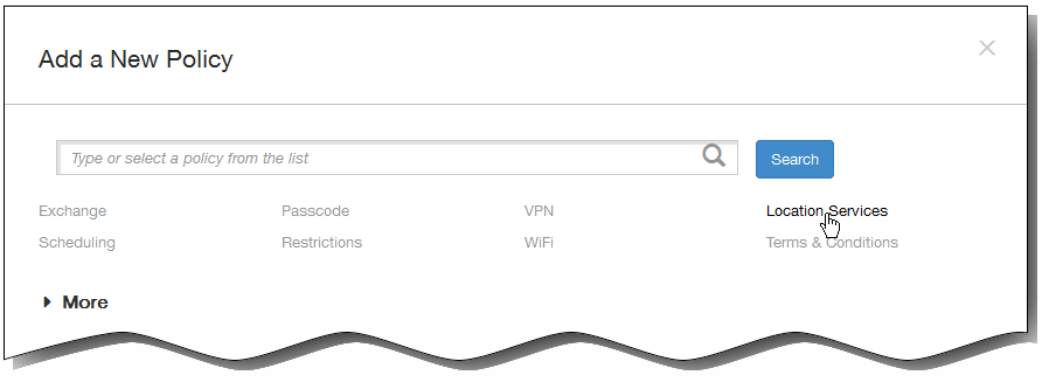


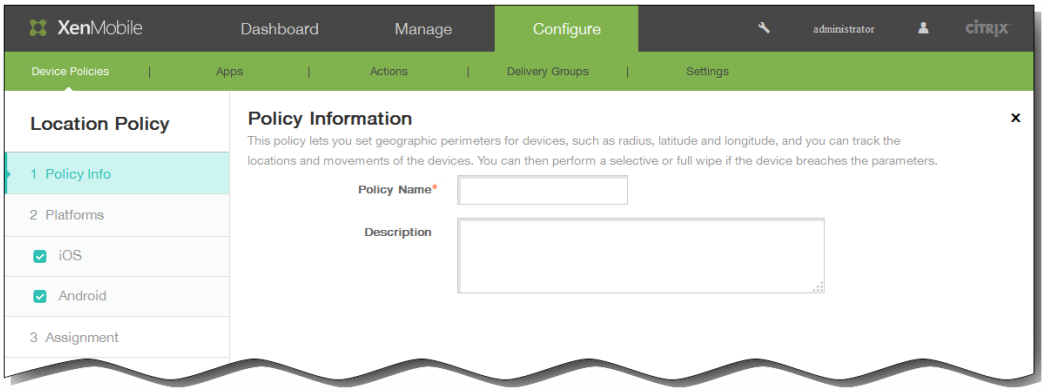


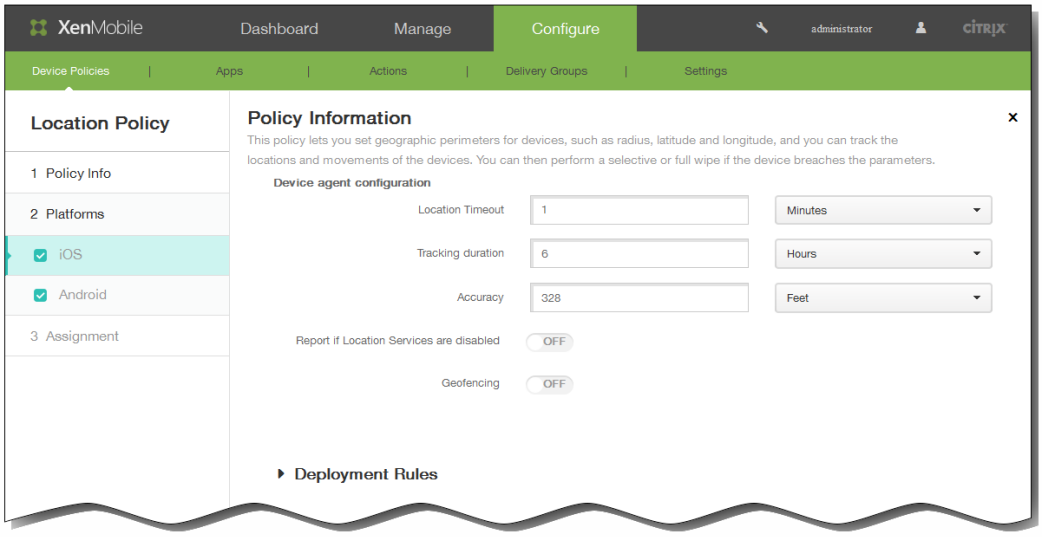


Standortrichtlinien für Geräte

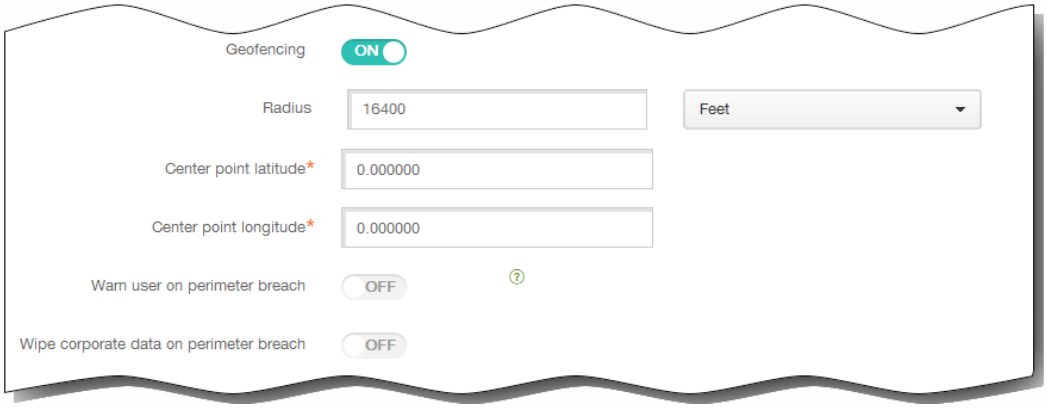


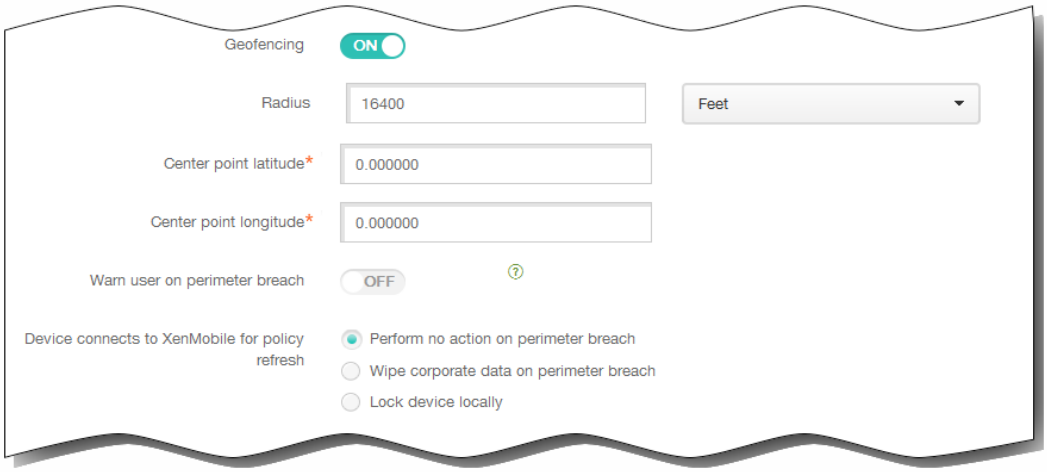






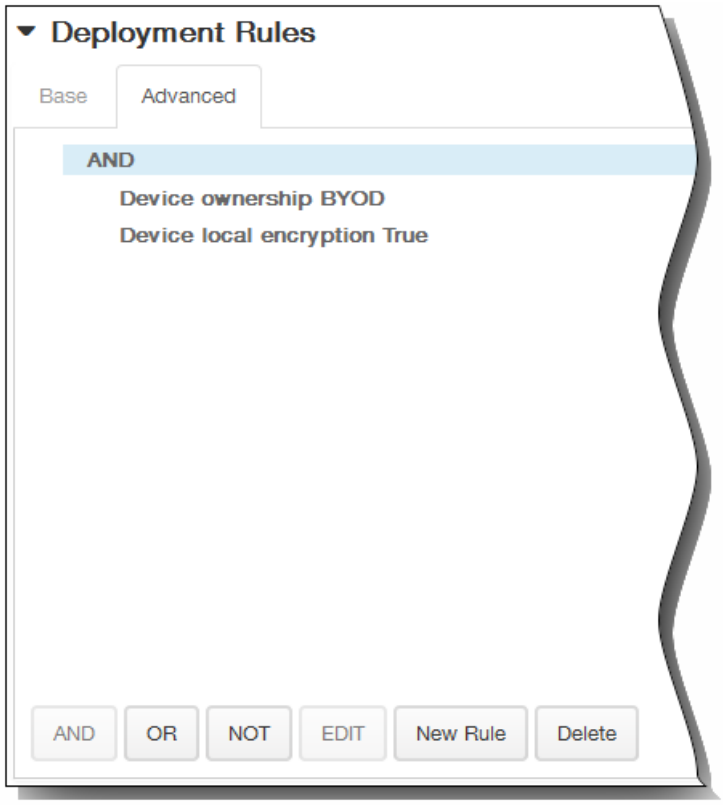
•

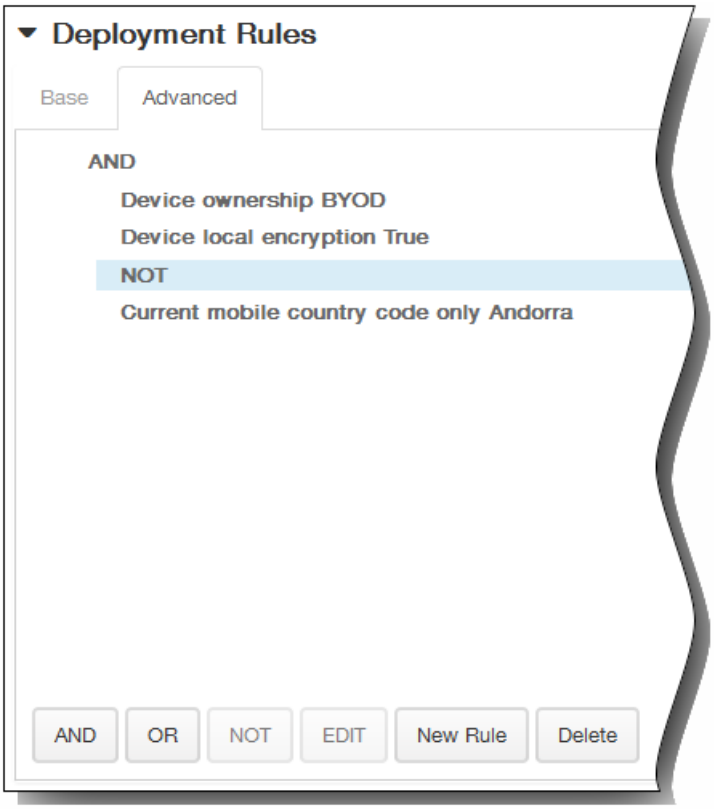


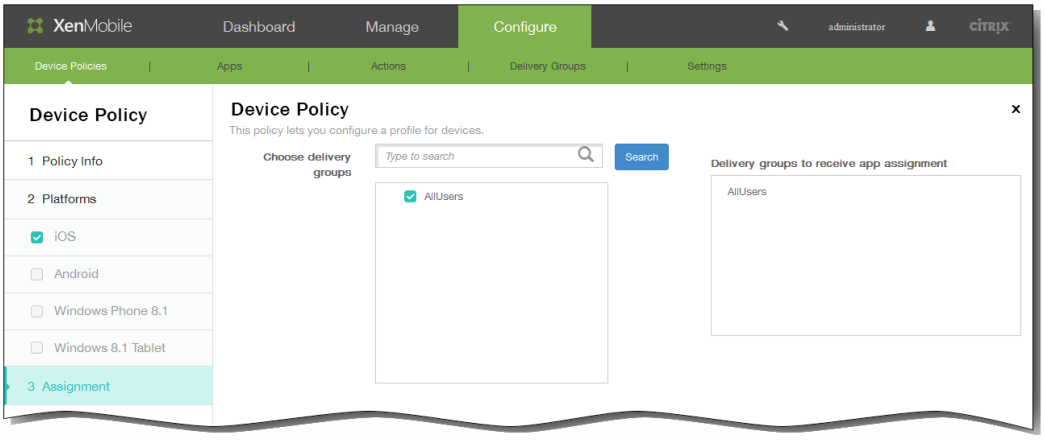


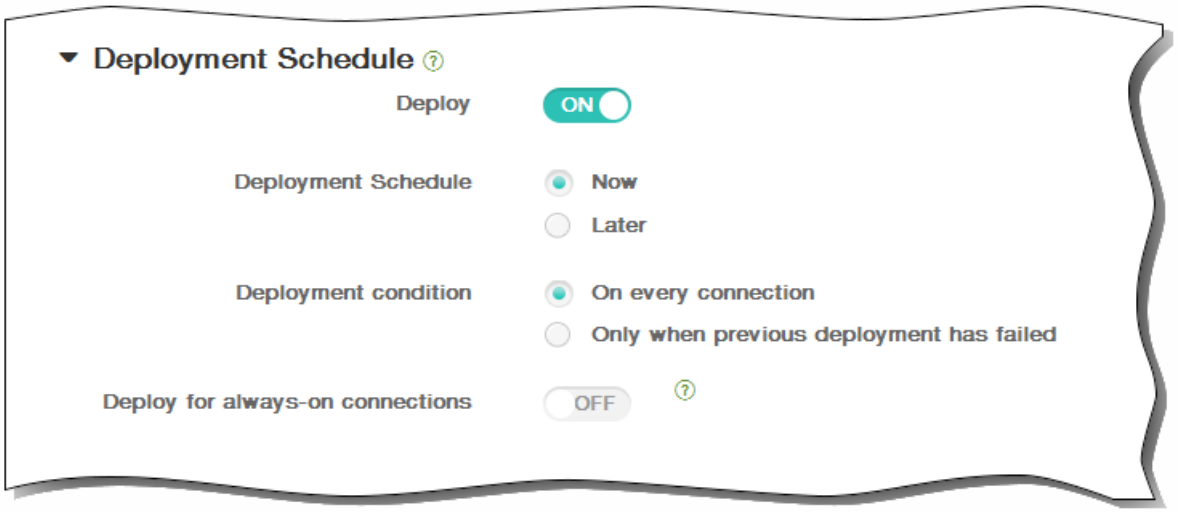
-
  -
  -
  -
  -
  -
-
-
-
-
  -
  -

-

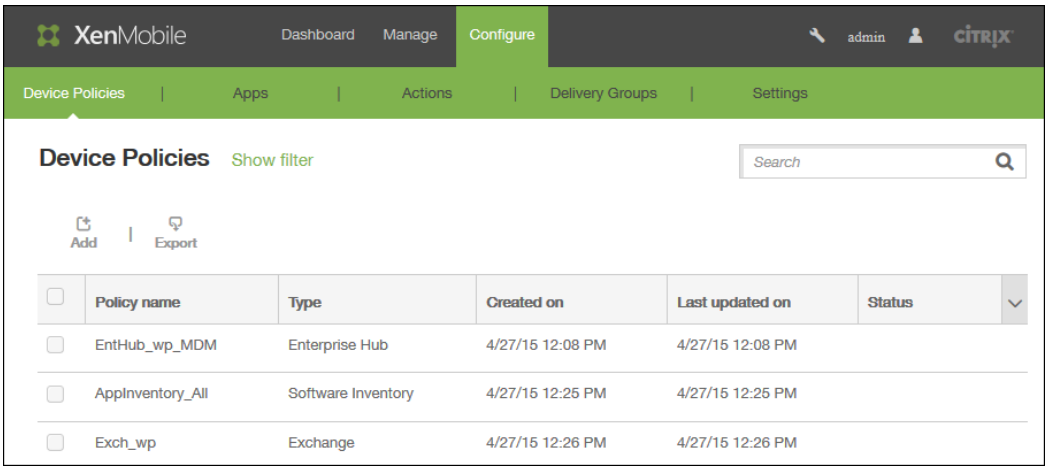




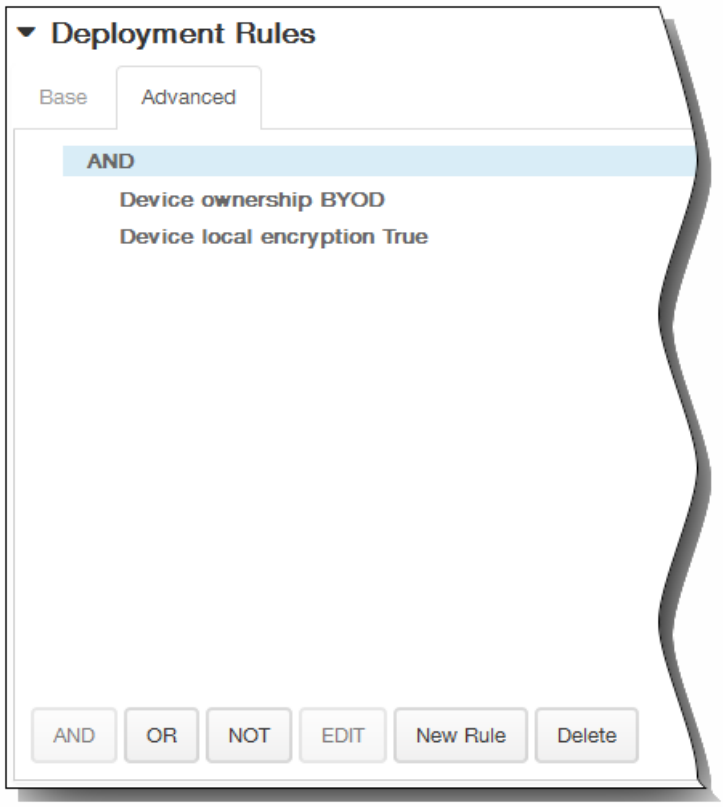


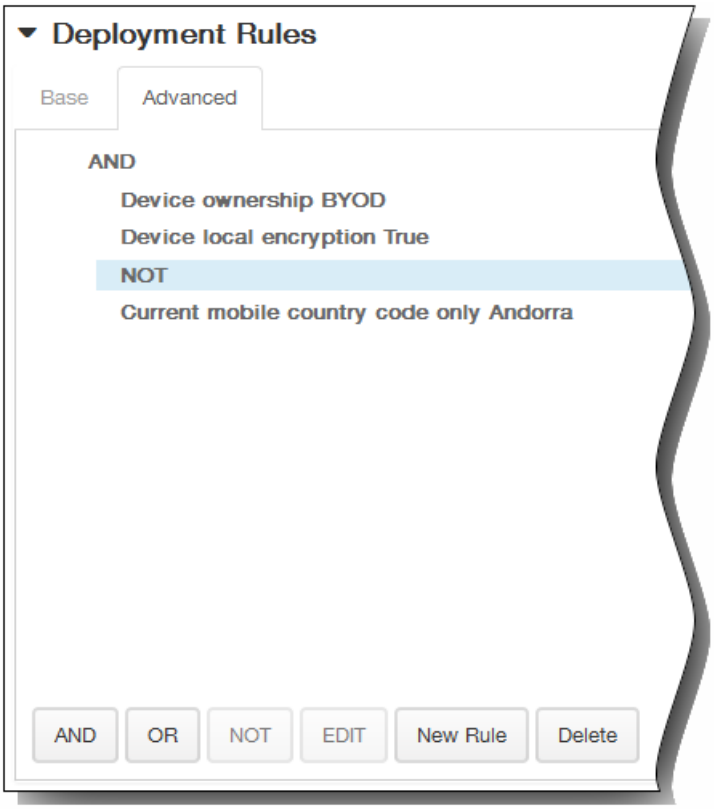


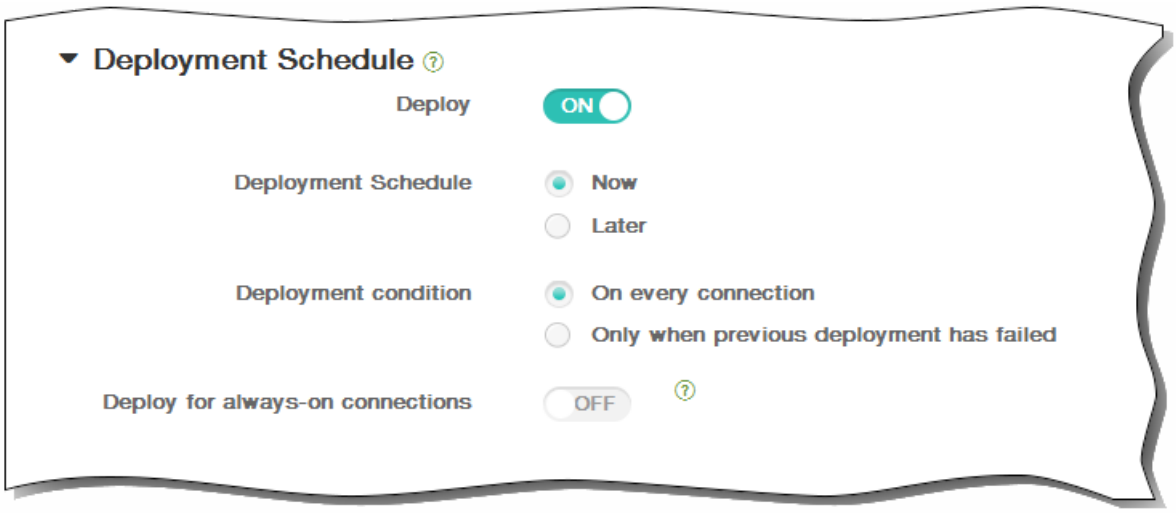
Verbindungszeitplanrichtlinien für Geräte



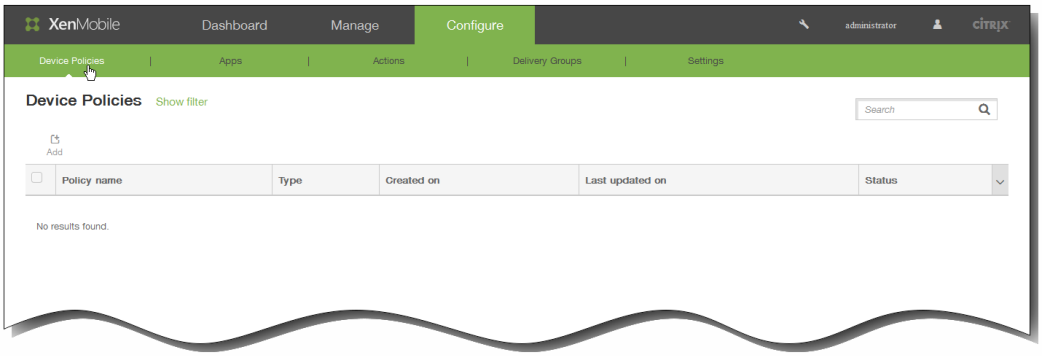
-
-
-
-

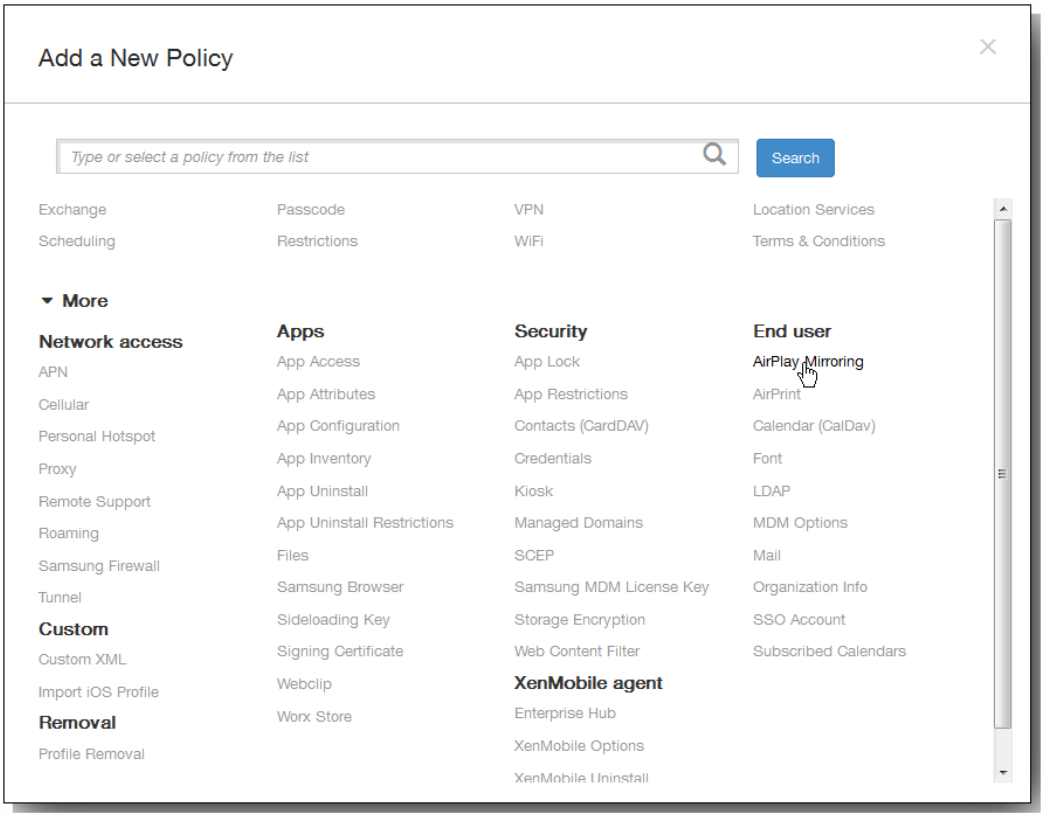


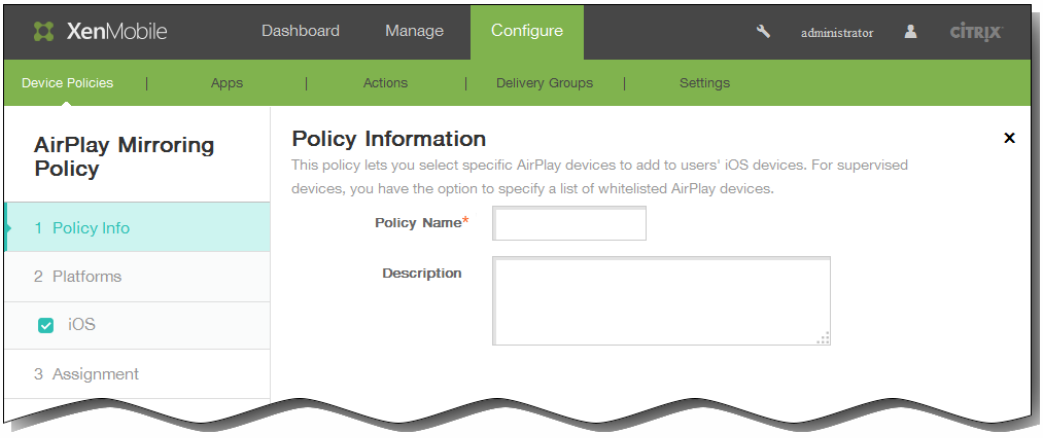




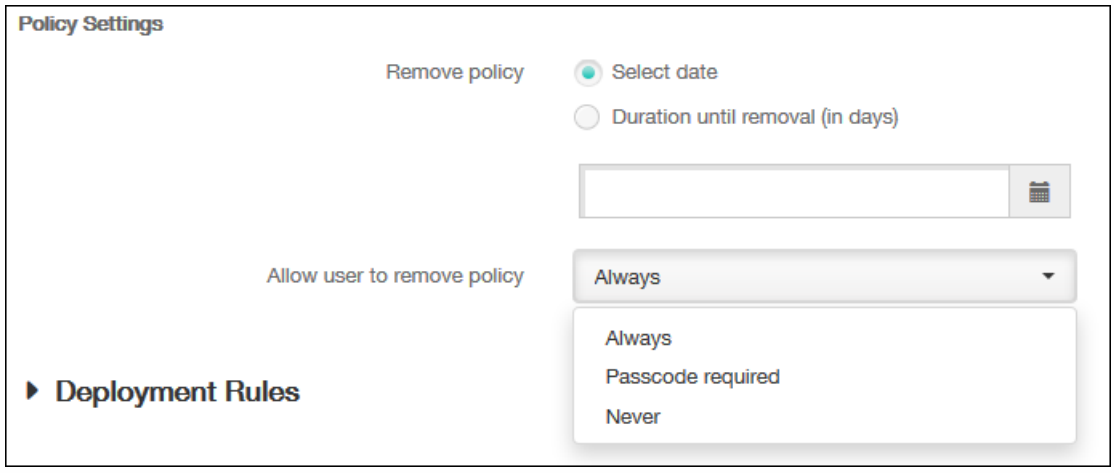
So fügen Sie eine AirPlay-Spiegelungsrichtlinie für iOS-Geräte hinzu

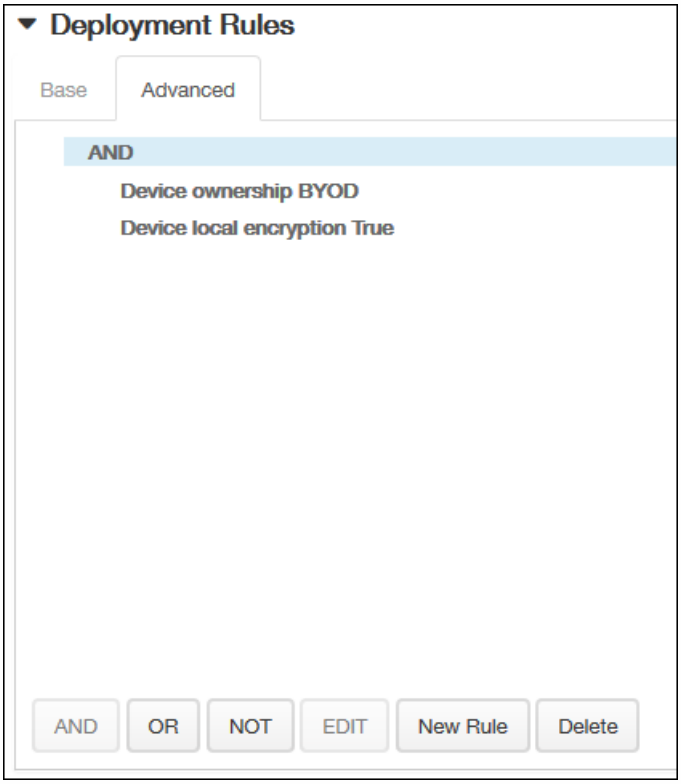


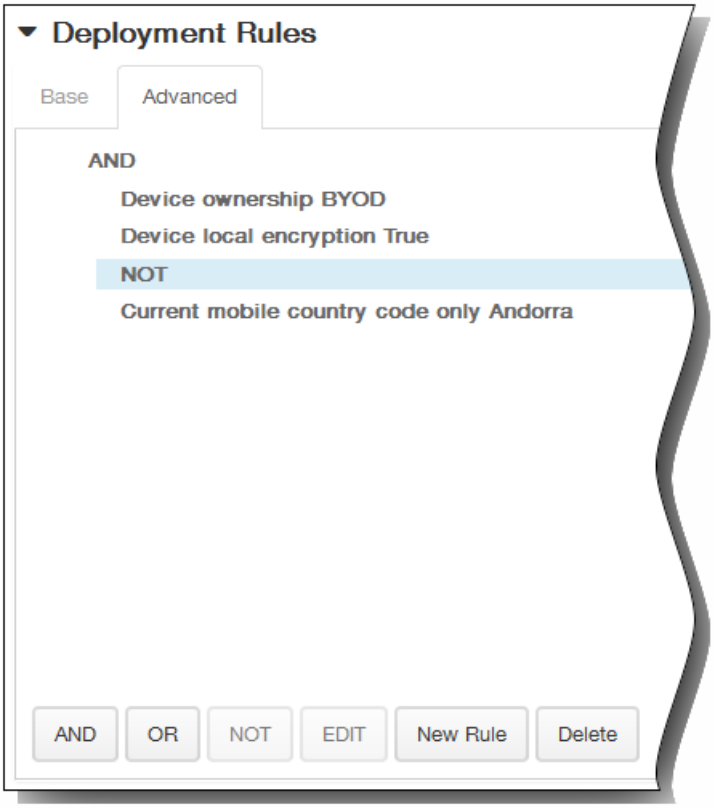


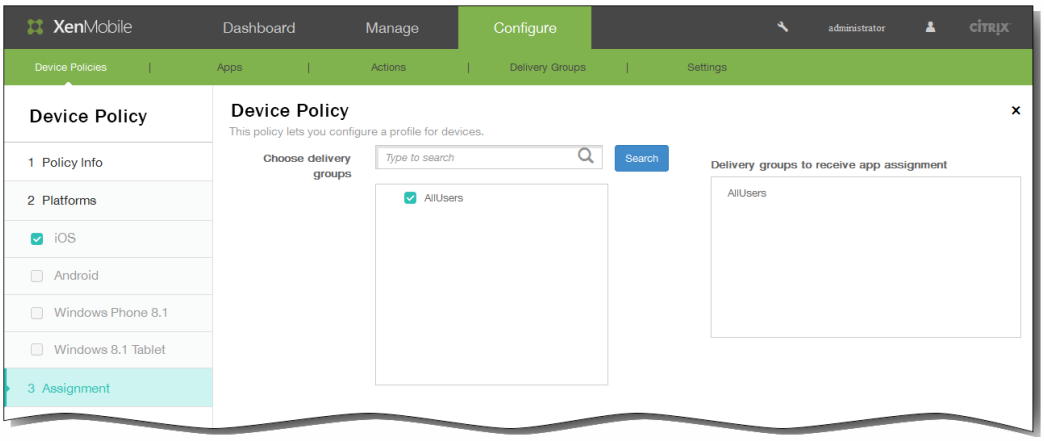


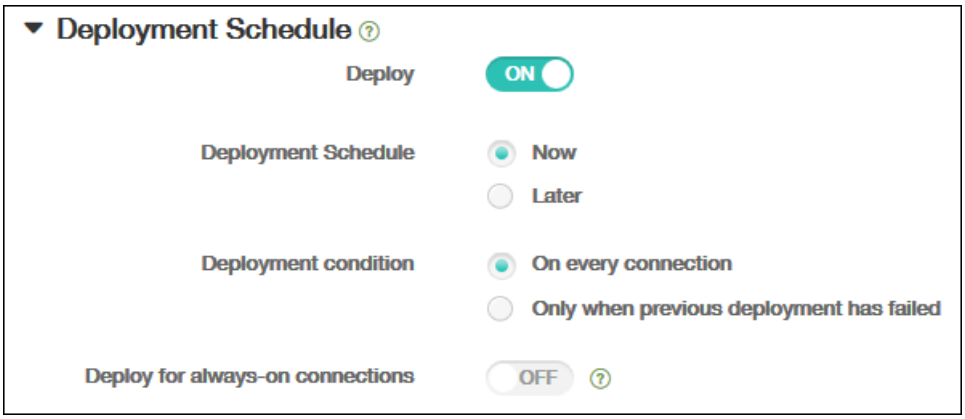
xx:xx:xx:xx:xx:xx





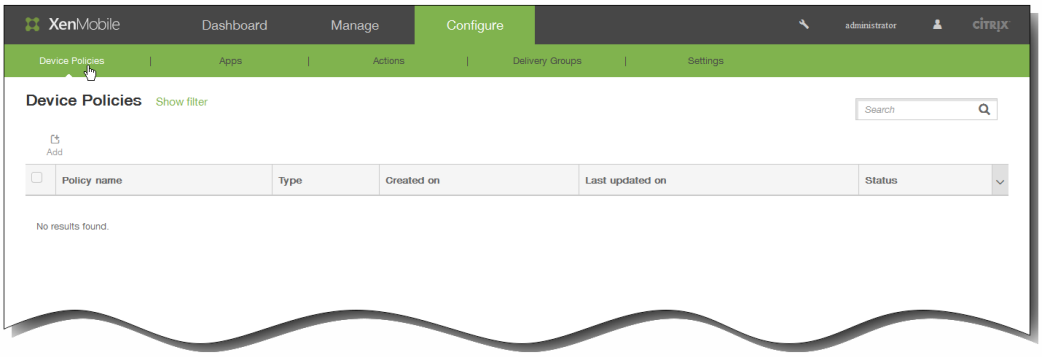


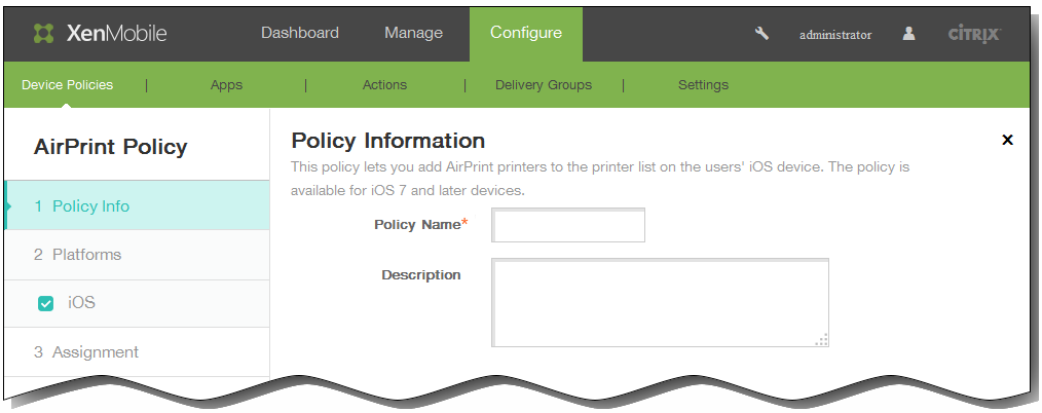


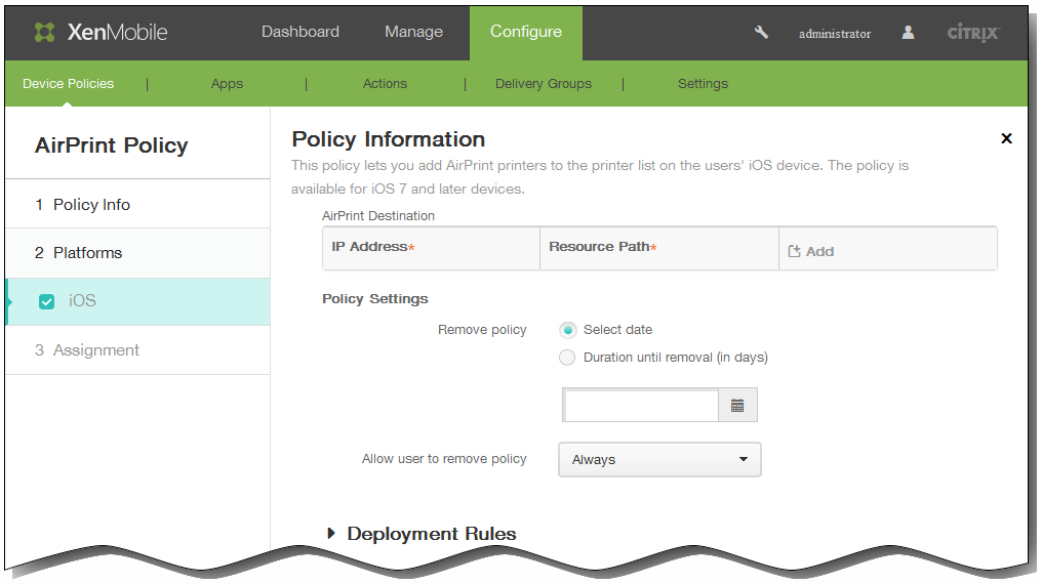


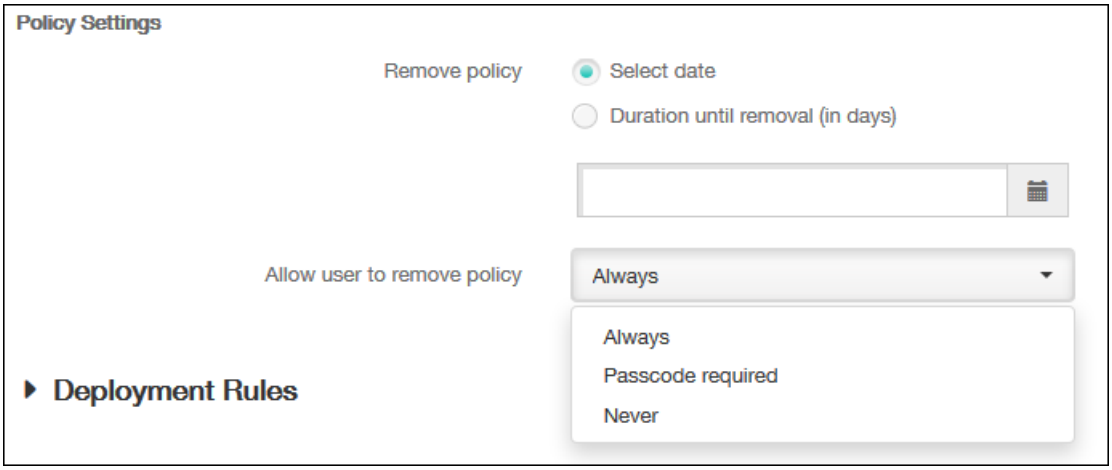
So fügen Sie eine AirPrint-Geräterichtlinie für iOS hinzu

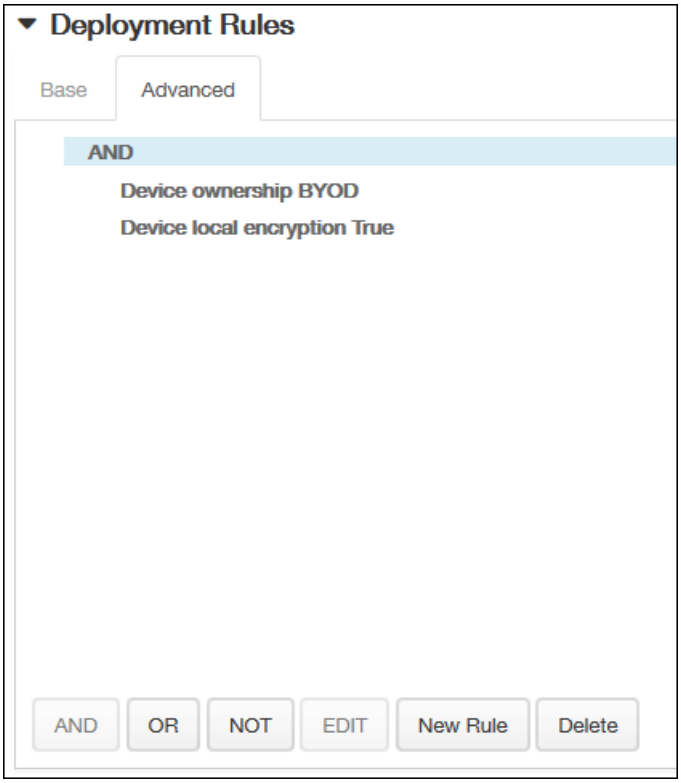
-
-

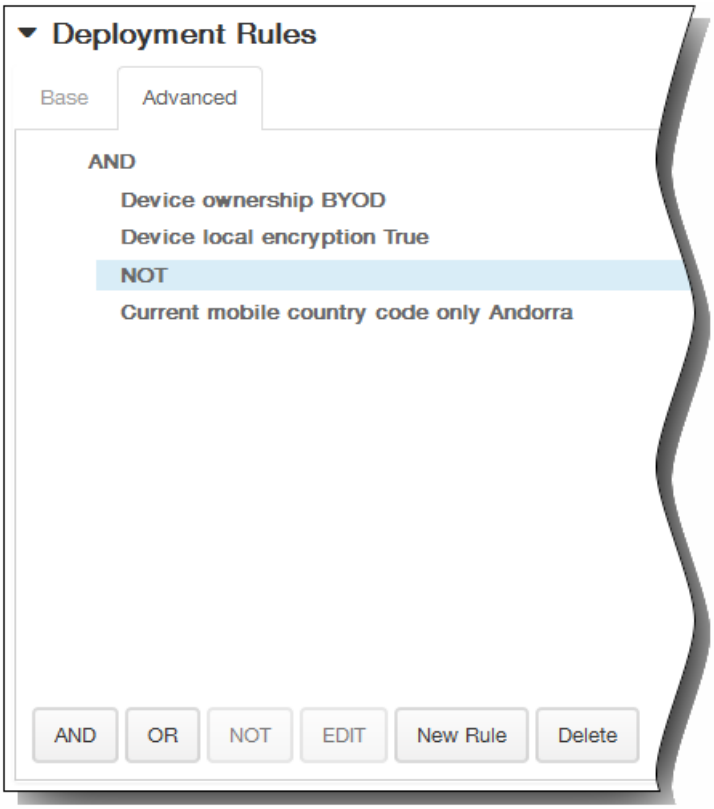


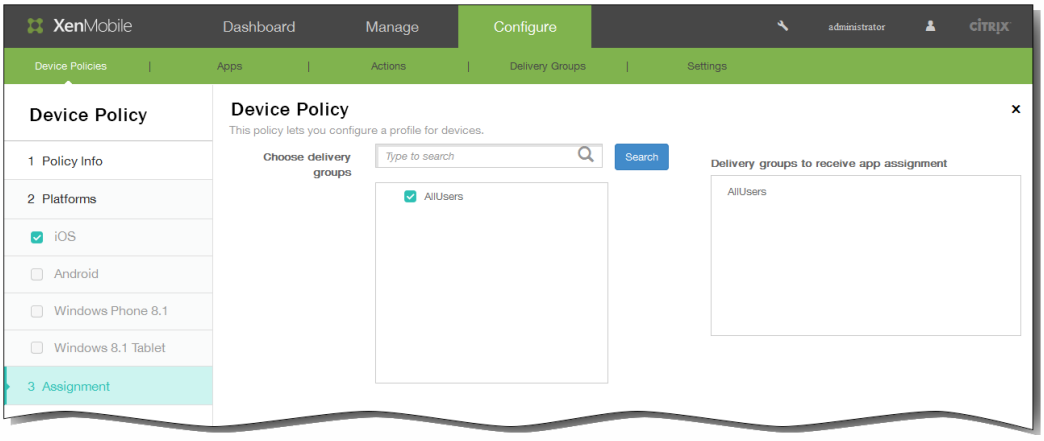


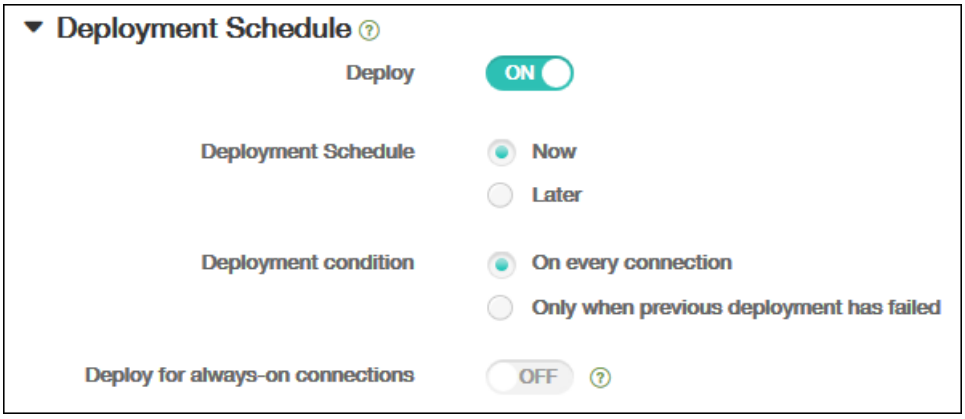




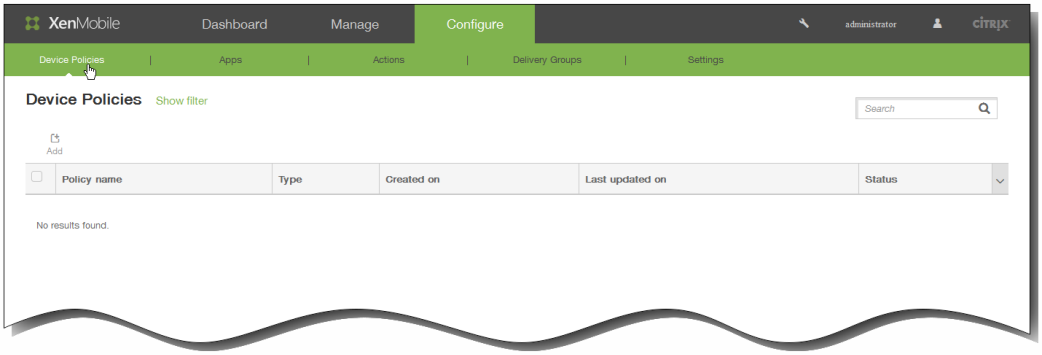


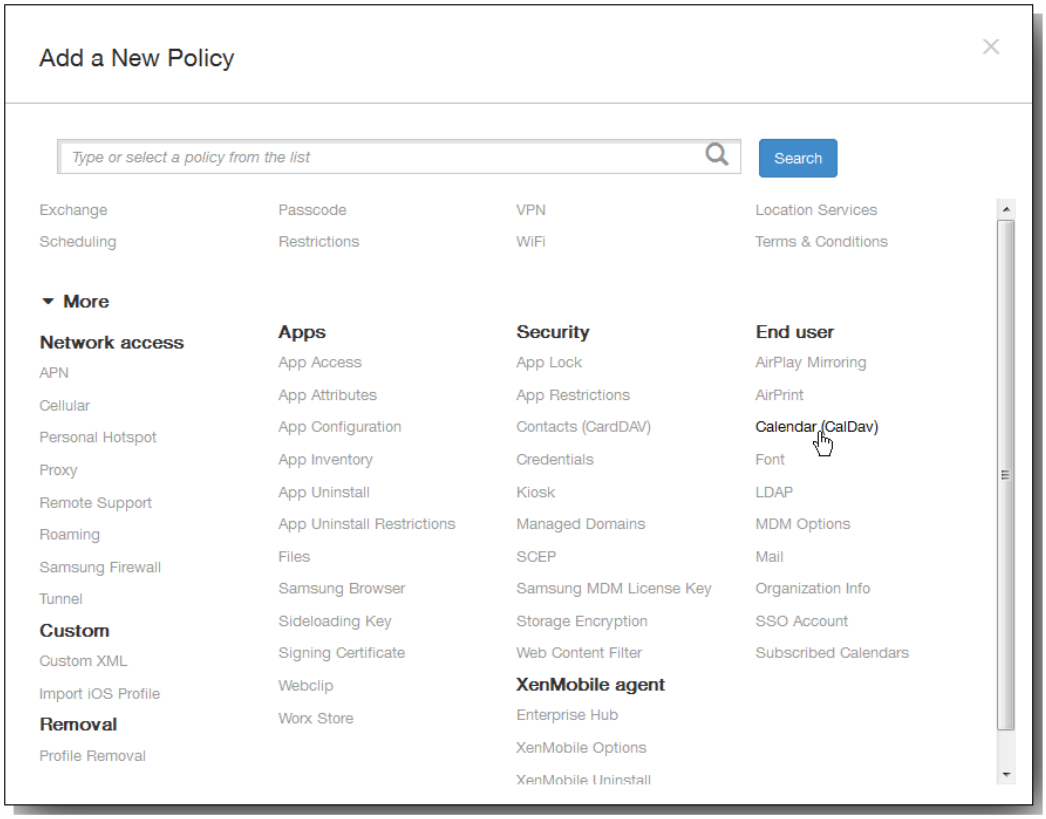


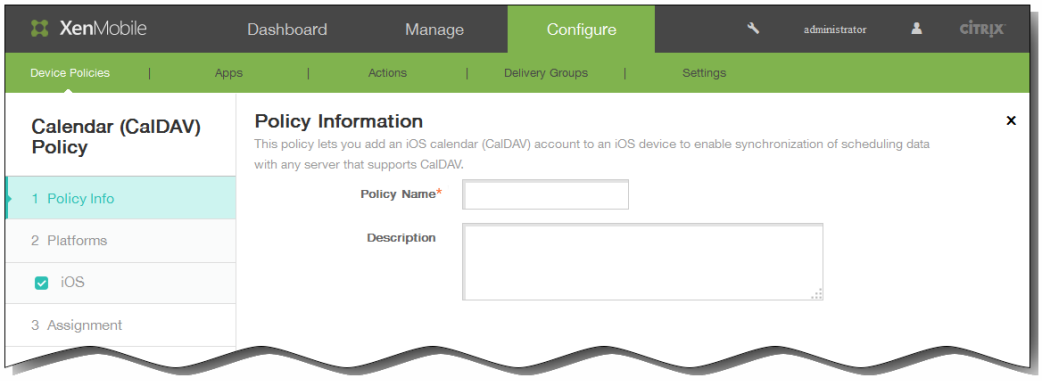


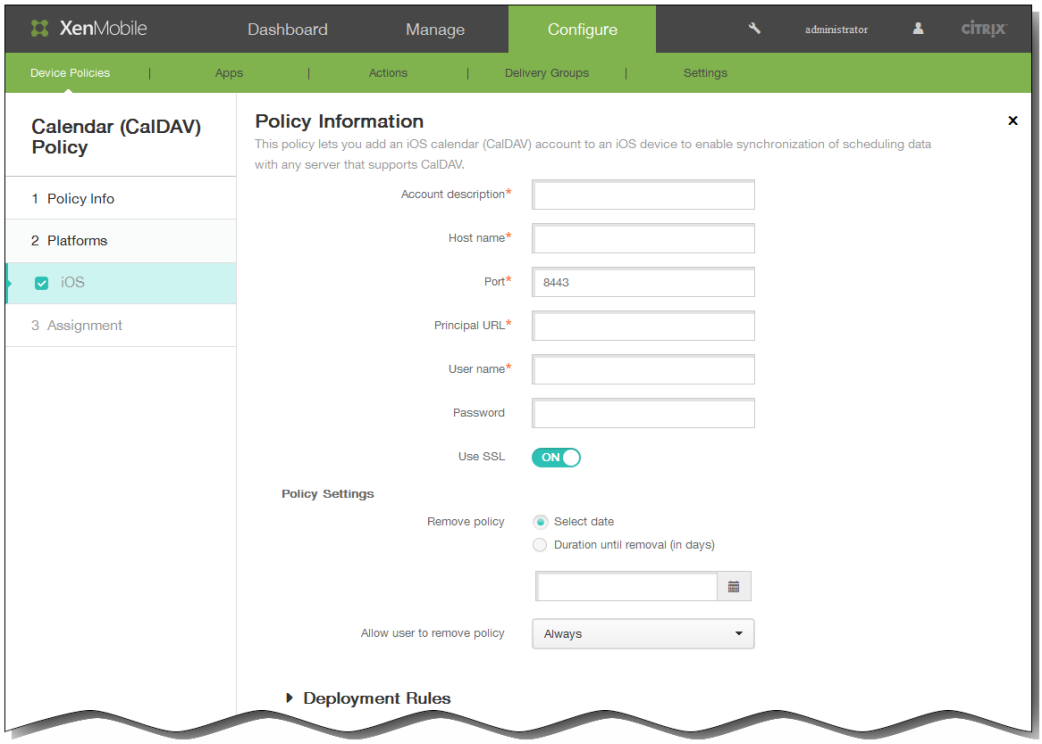


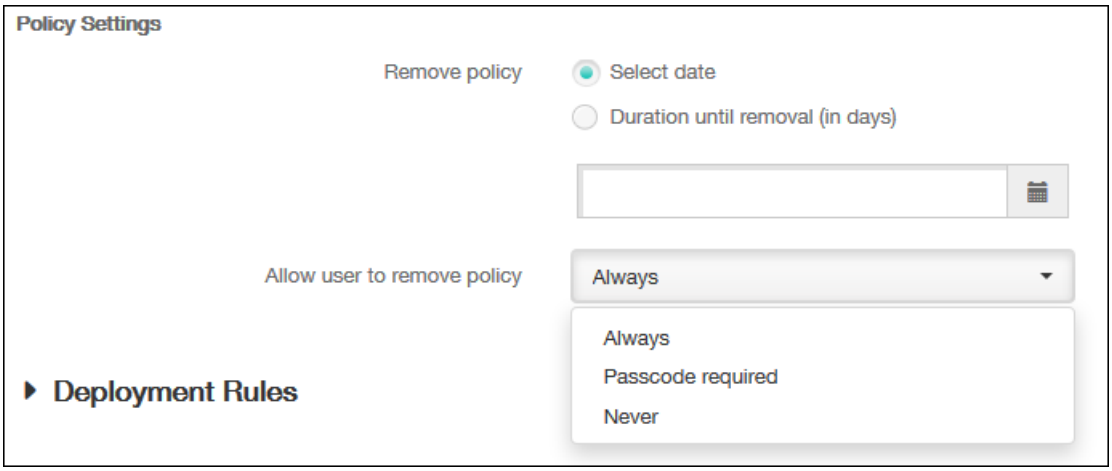
So fügen Sie eine Kalenderrichtlinie (CalDAV) für iOS-Geräte hinzu

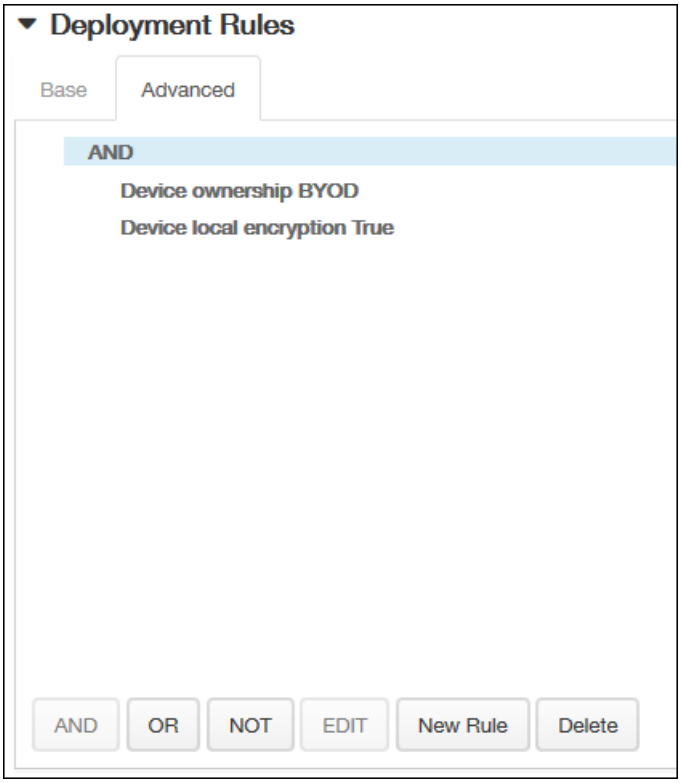


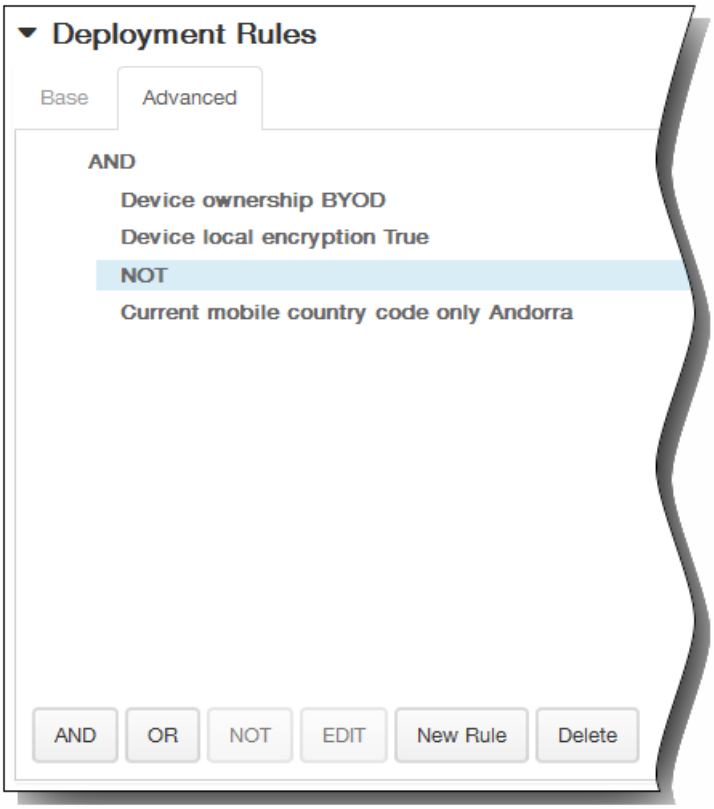


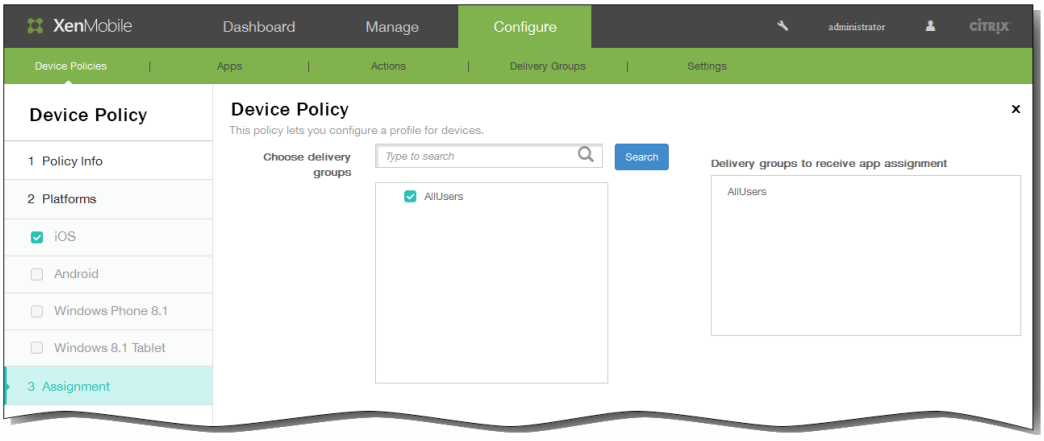


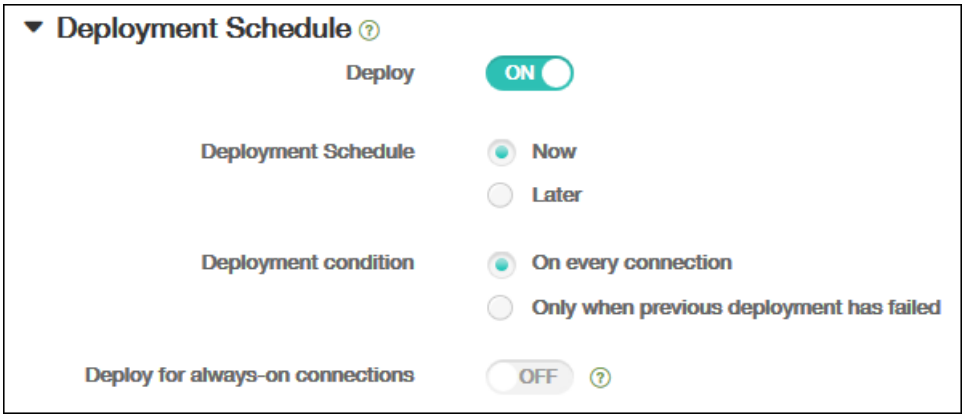




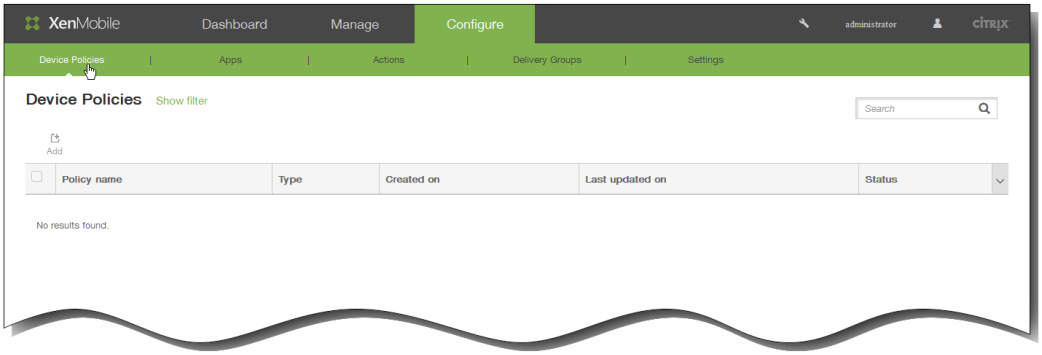


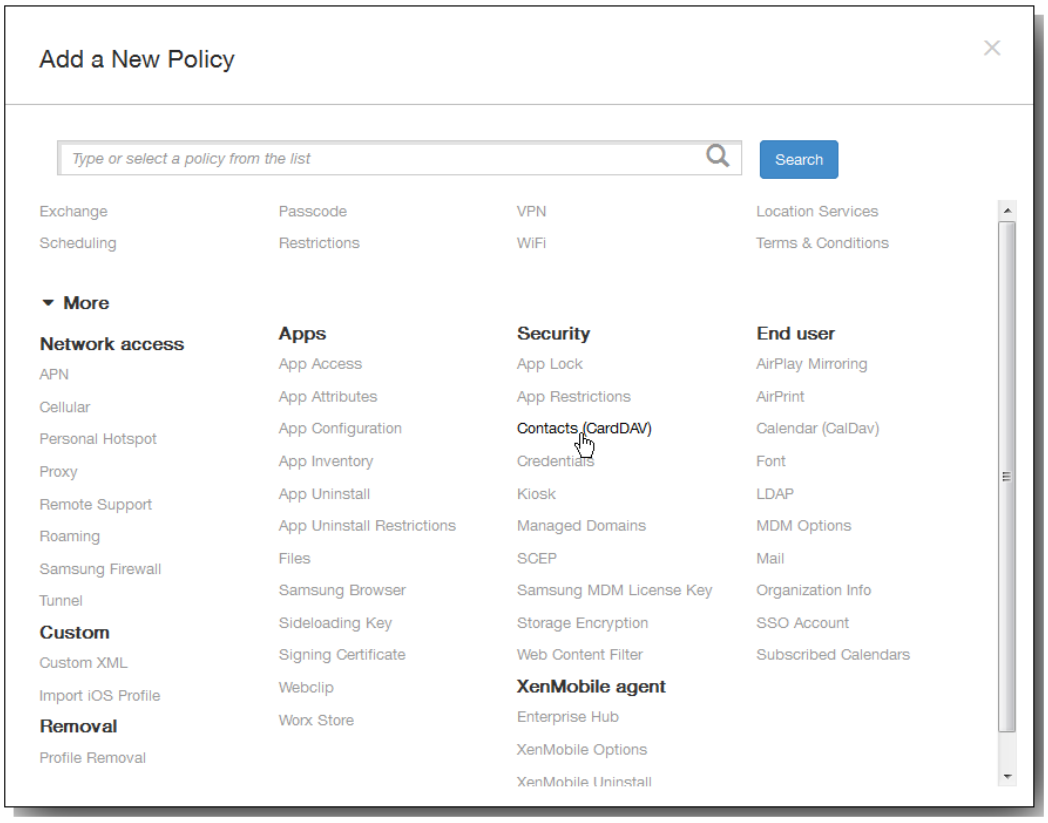


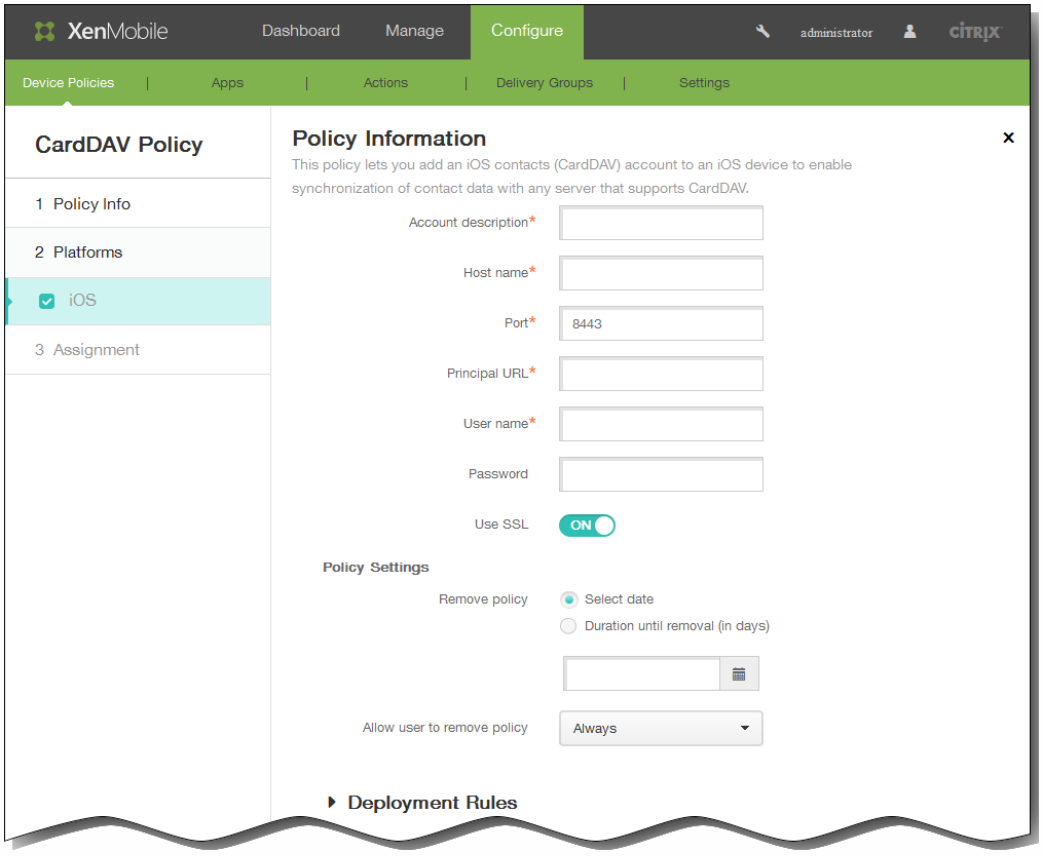


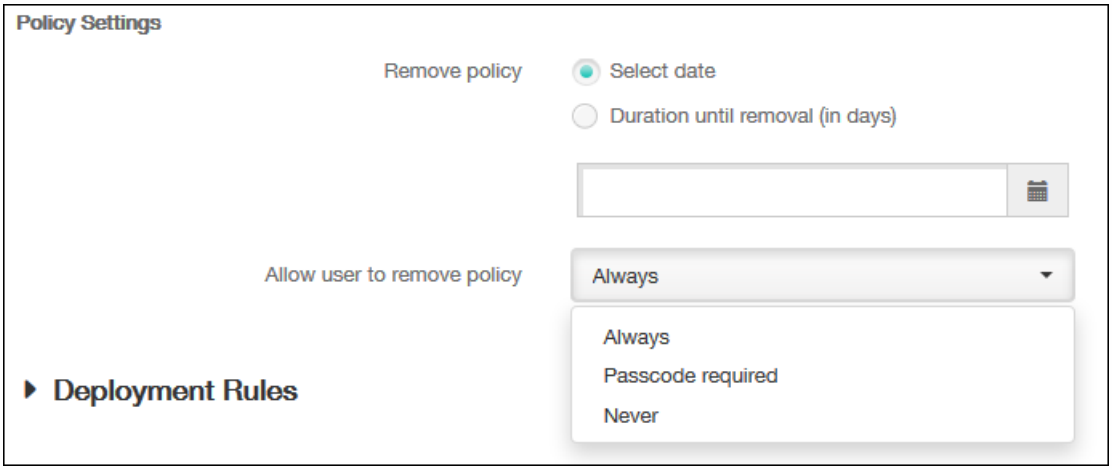


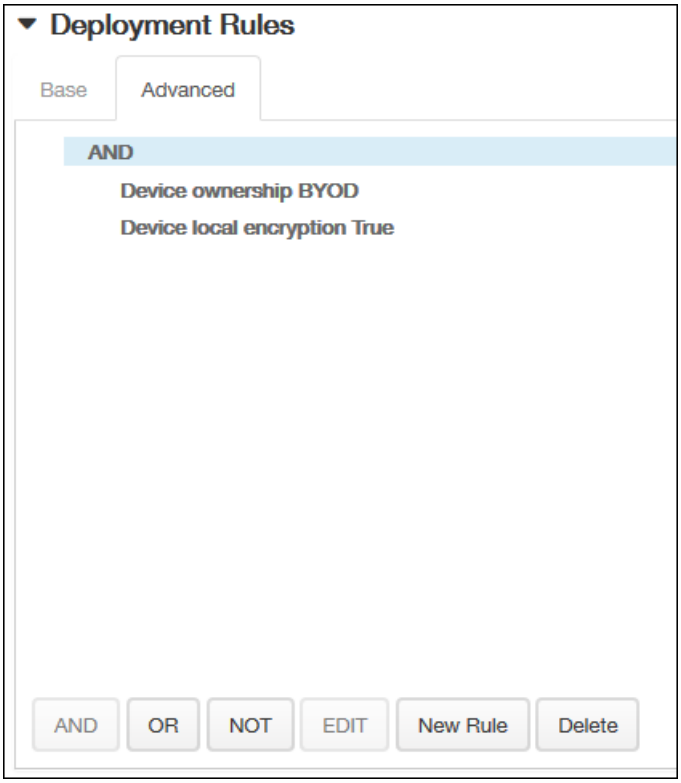
So fügen Sie eine Kontakterichtlinie (CardDAV) für iOS-Geräte hinzu

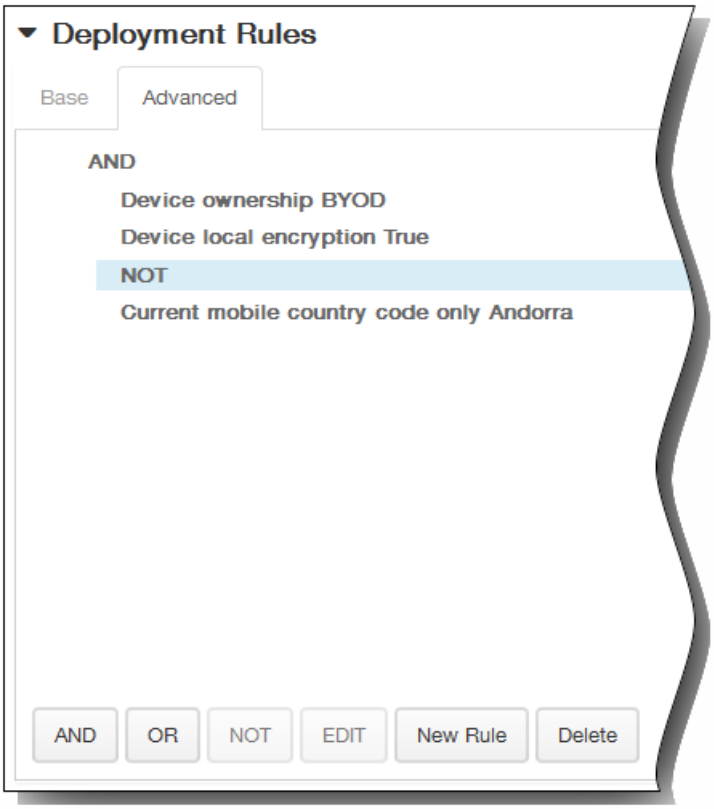


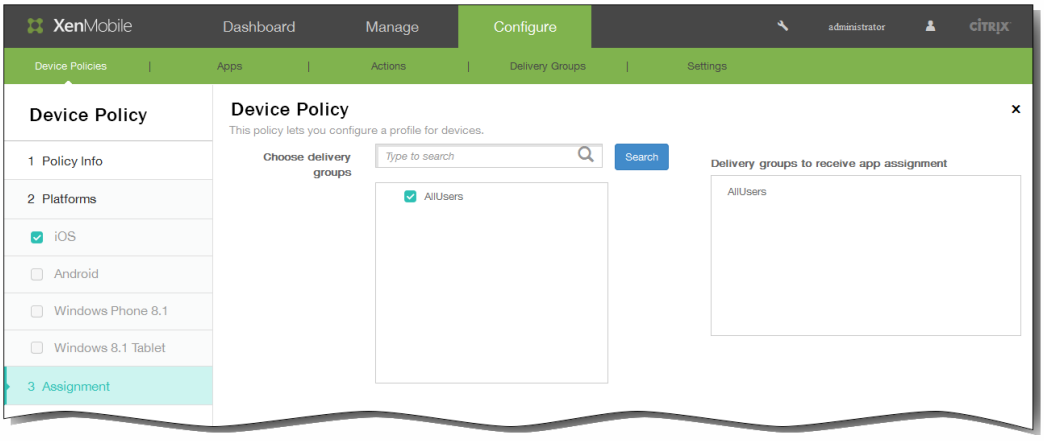


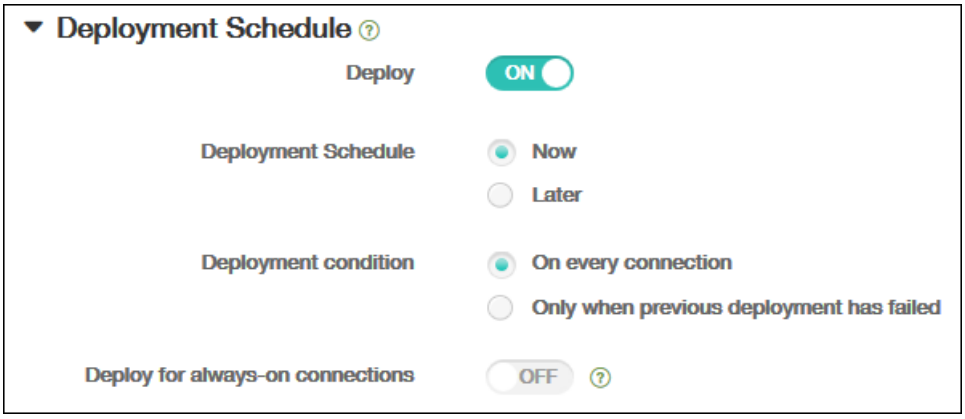




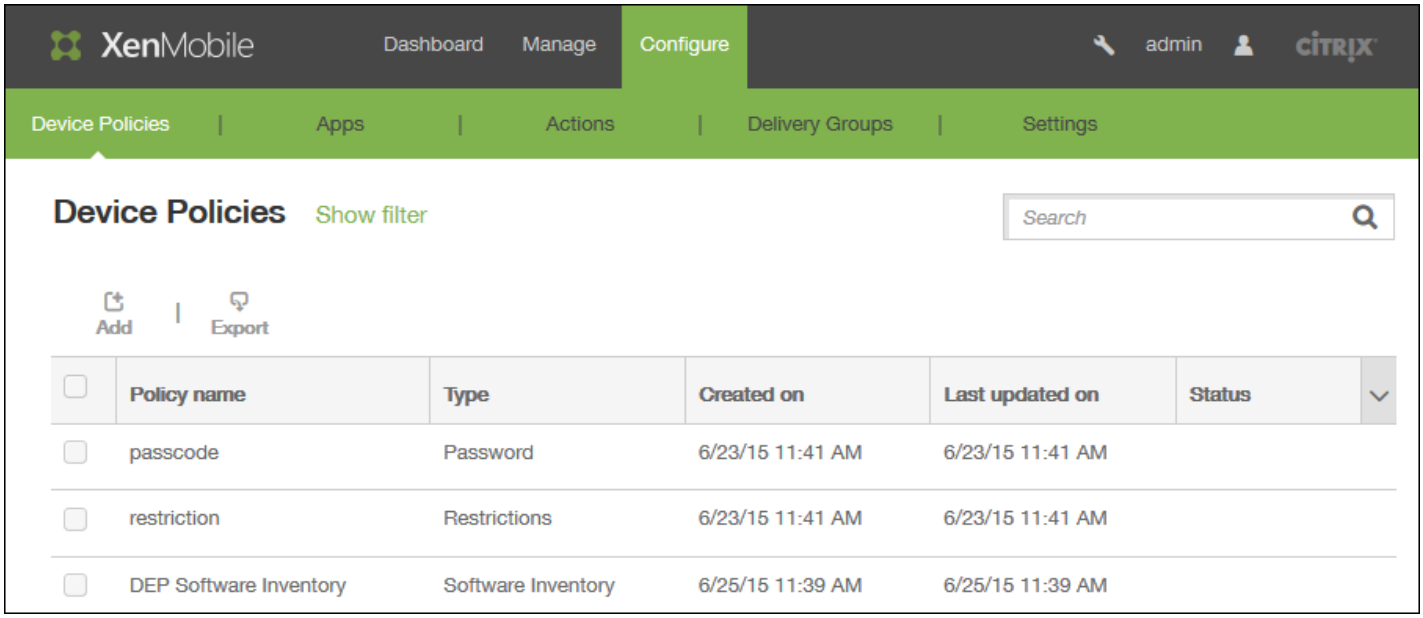


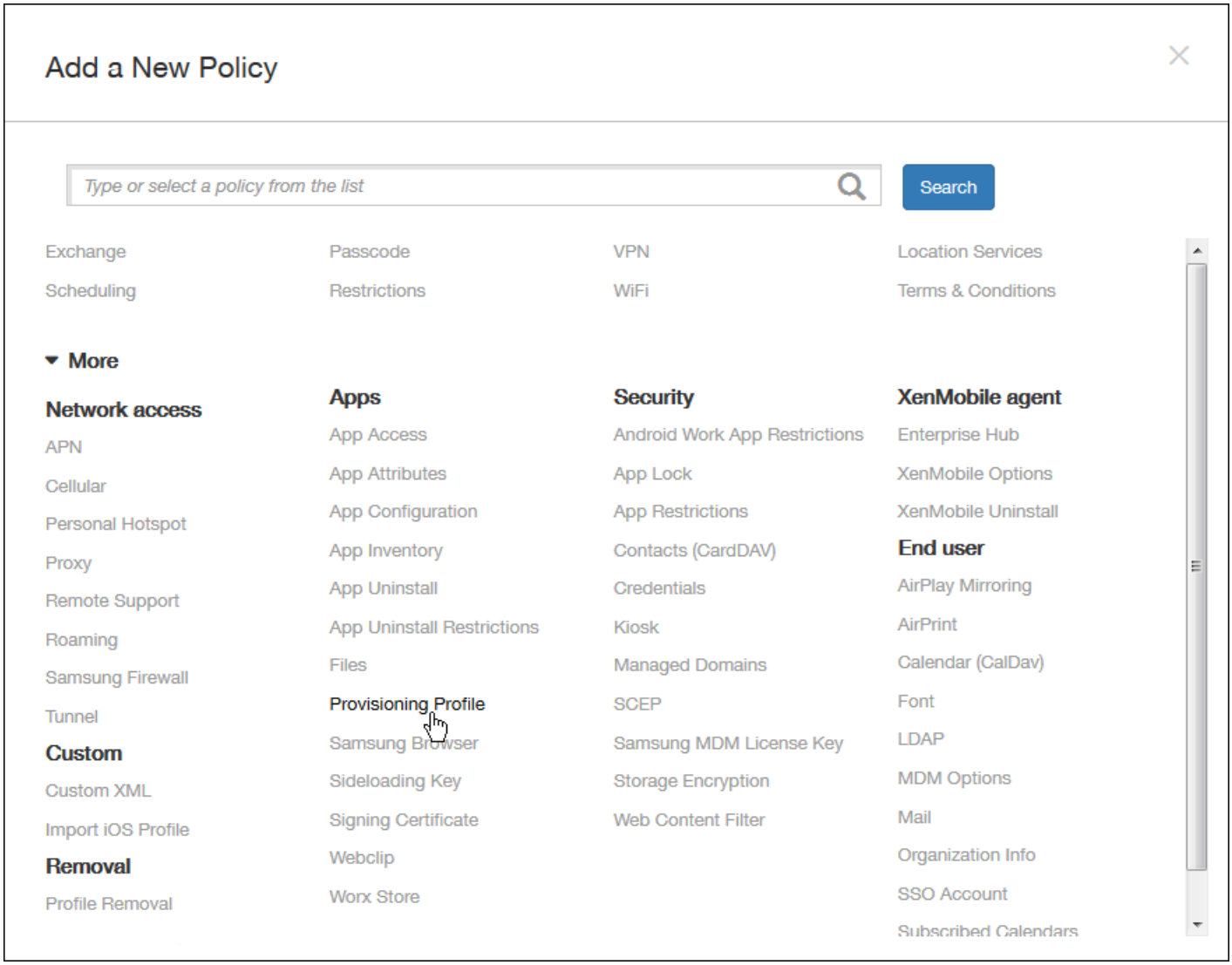


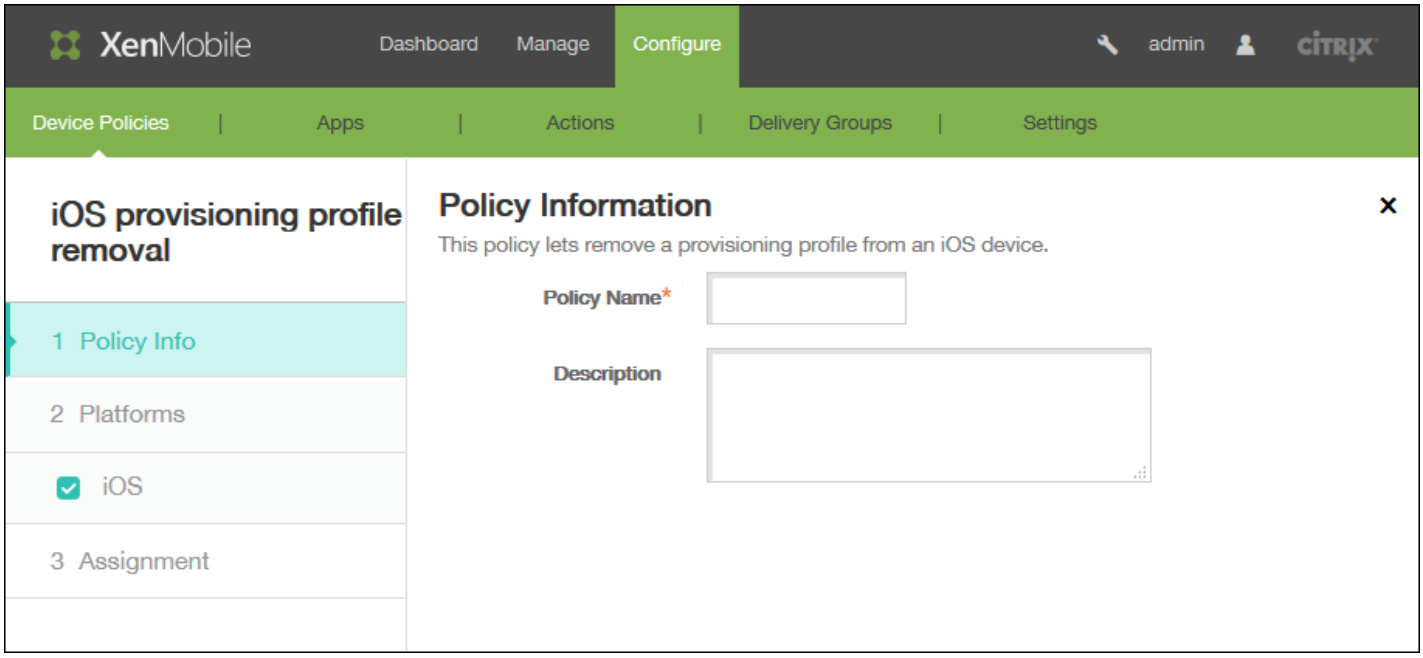




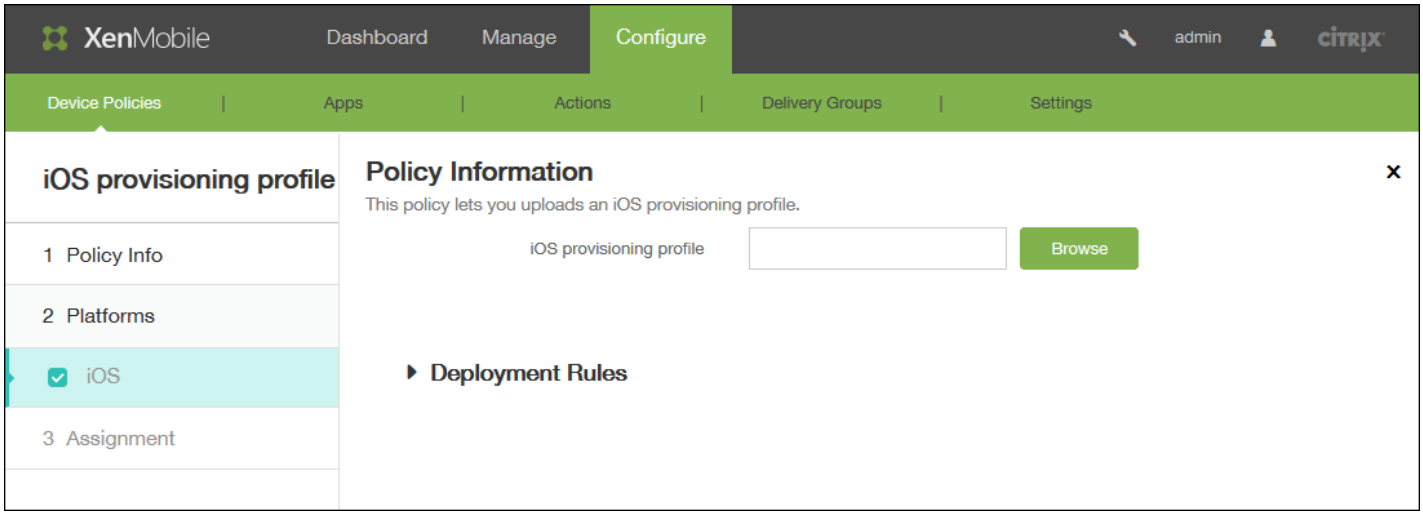
So fügen Sie eine Provisioningprofilrichtlinie für iOS-Geräte hinzu



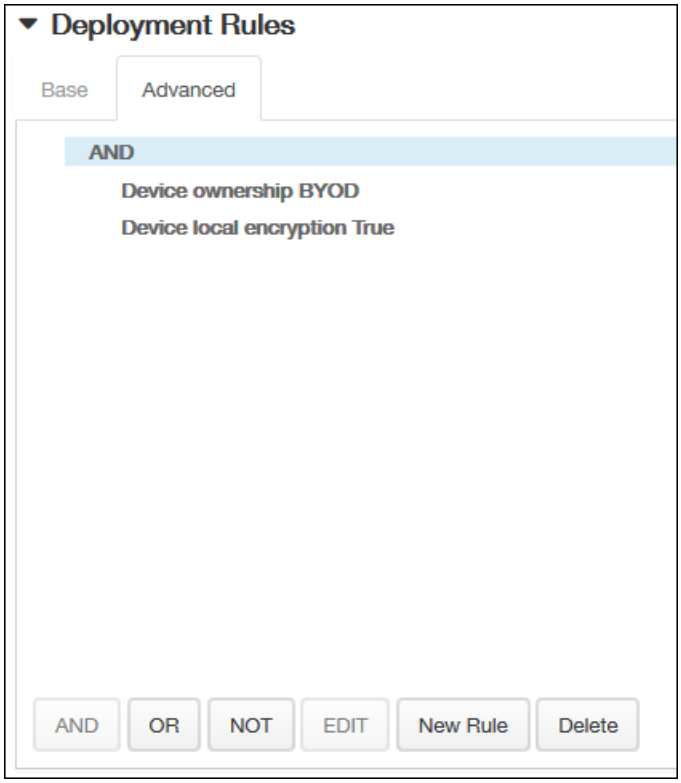




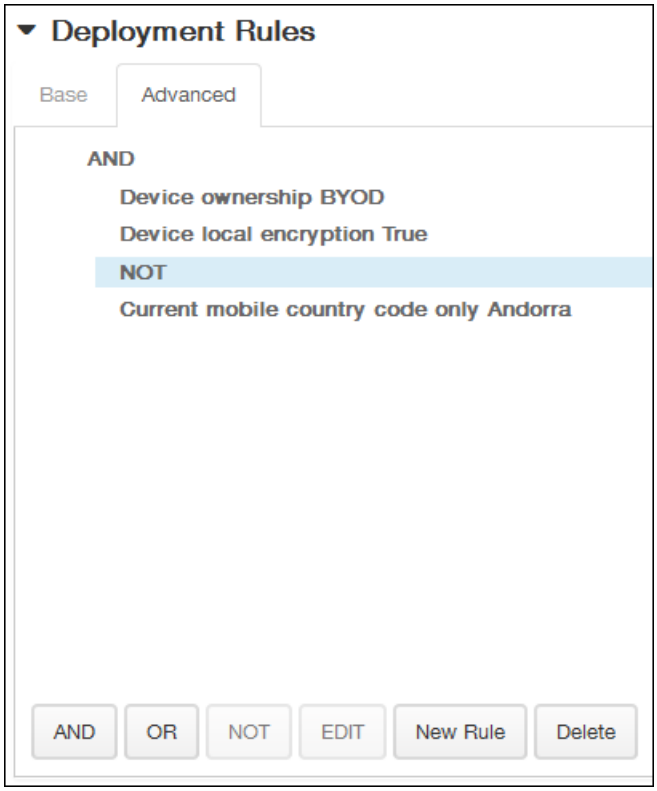
-
-

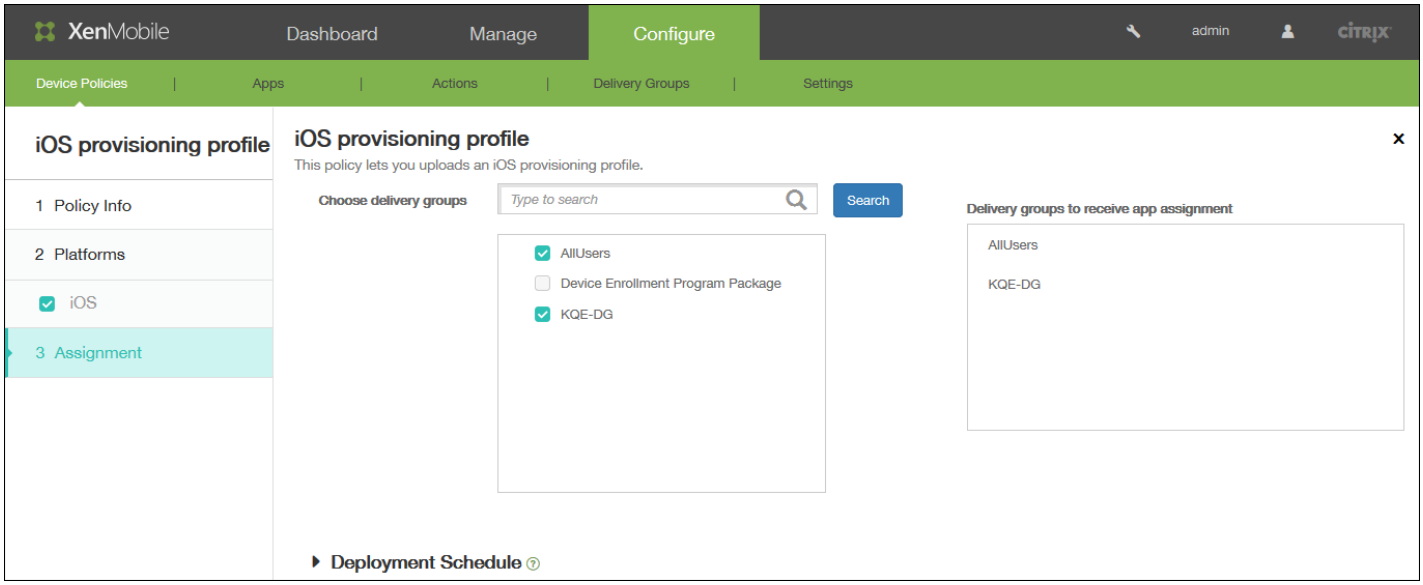


-
-
-
-



-
-
-
-

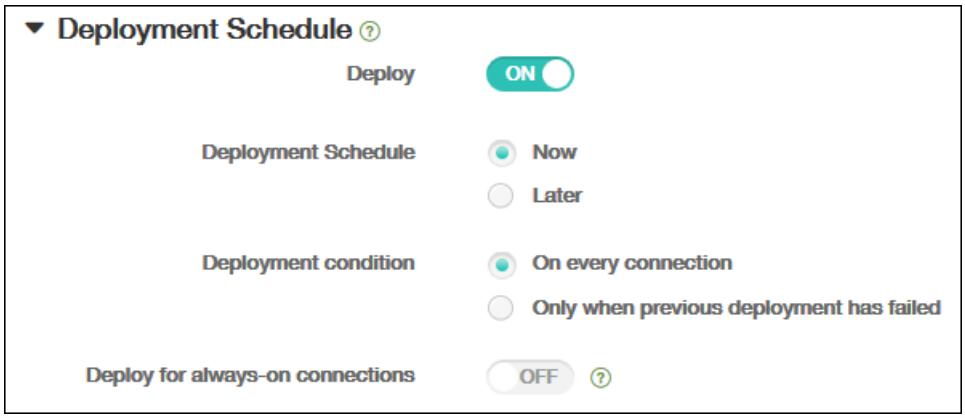




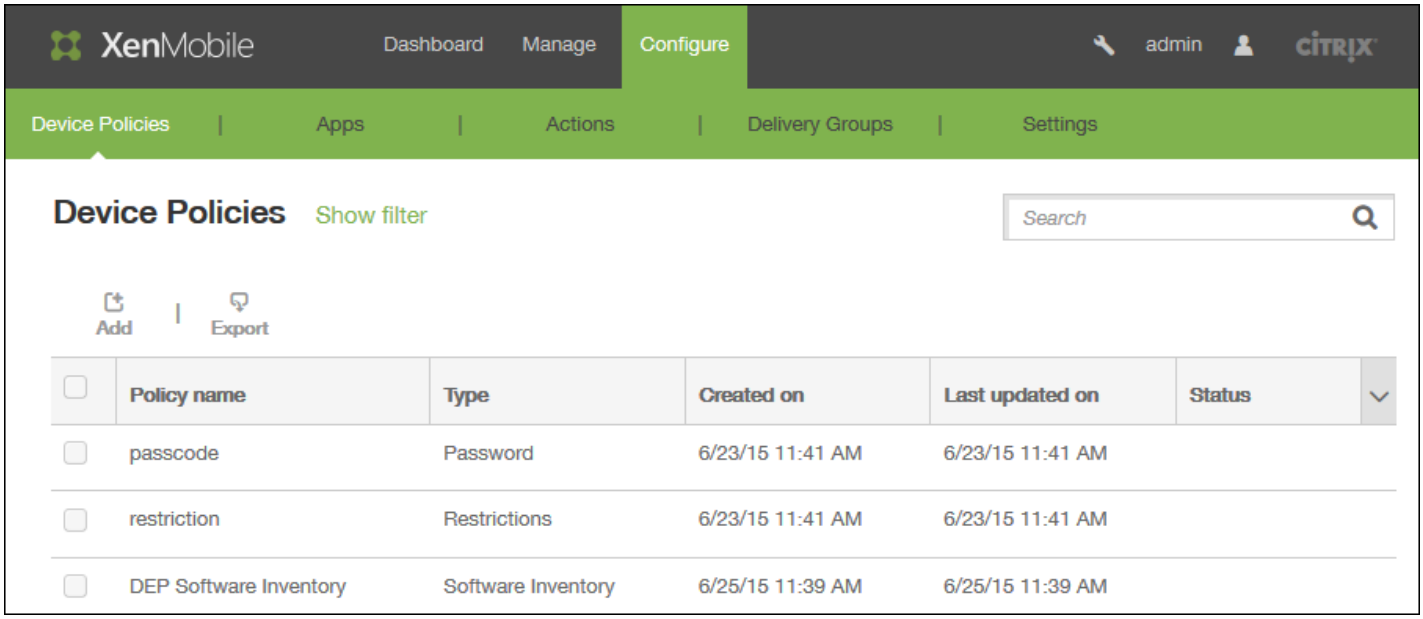
•

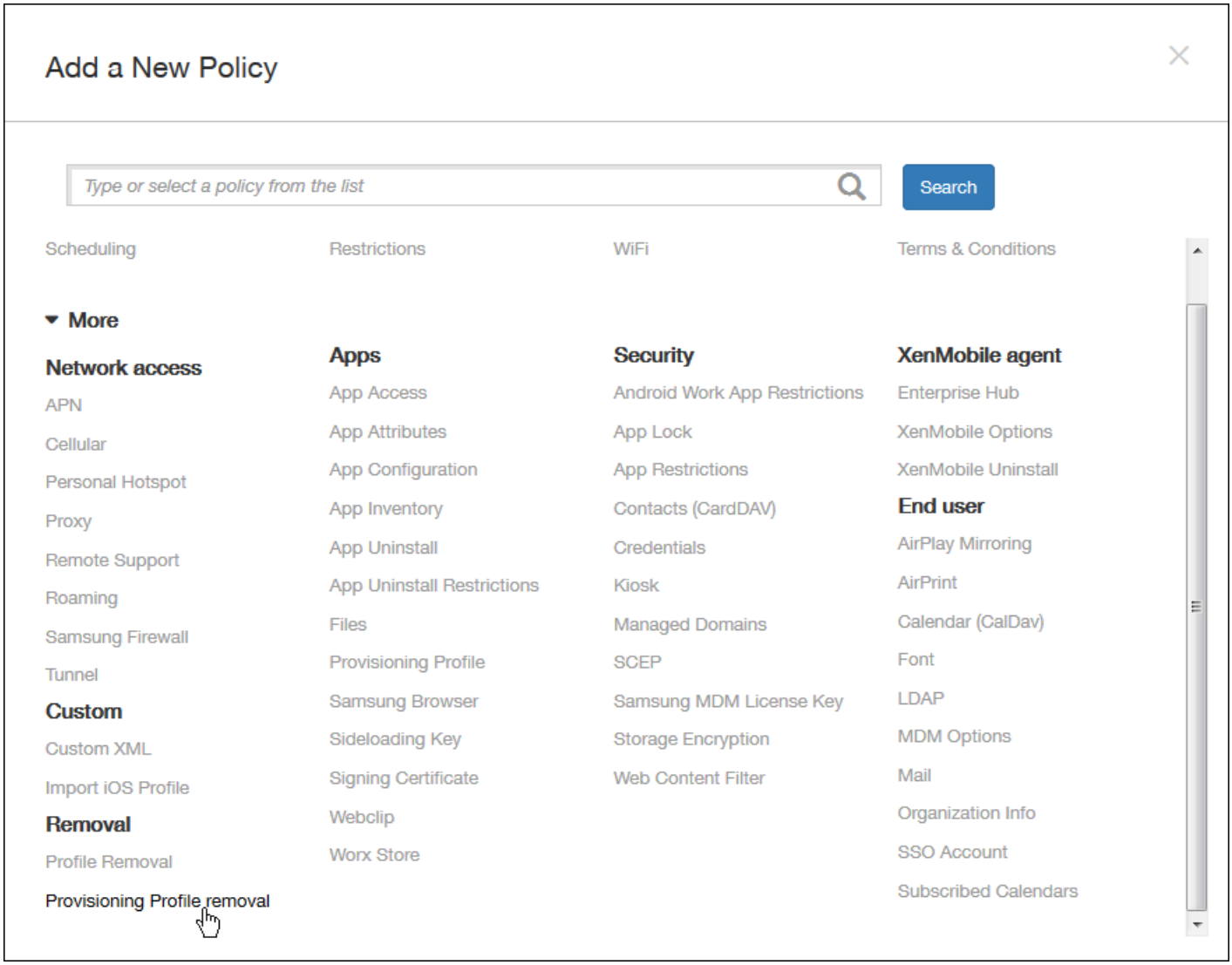
-
-
-
-

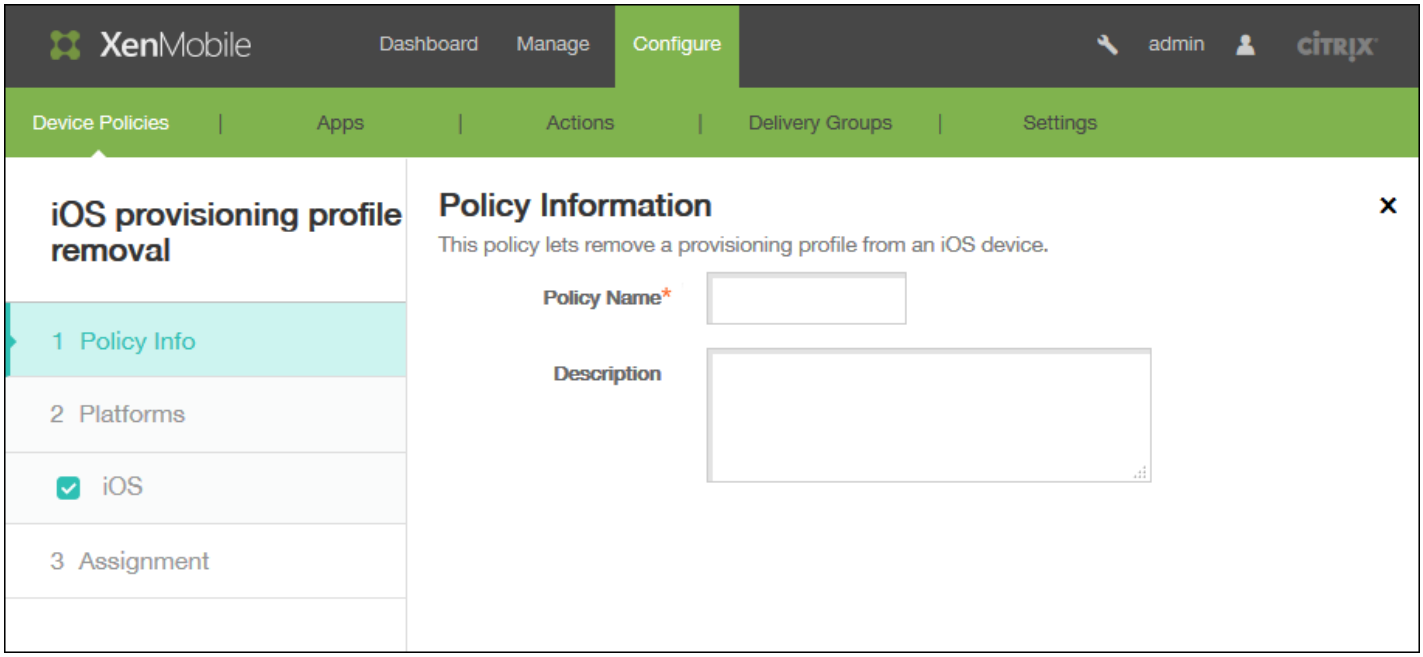
> Hinweis



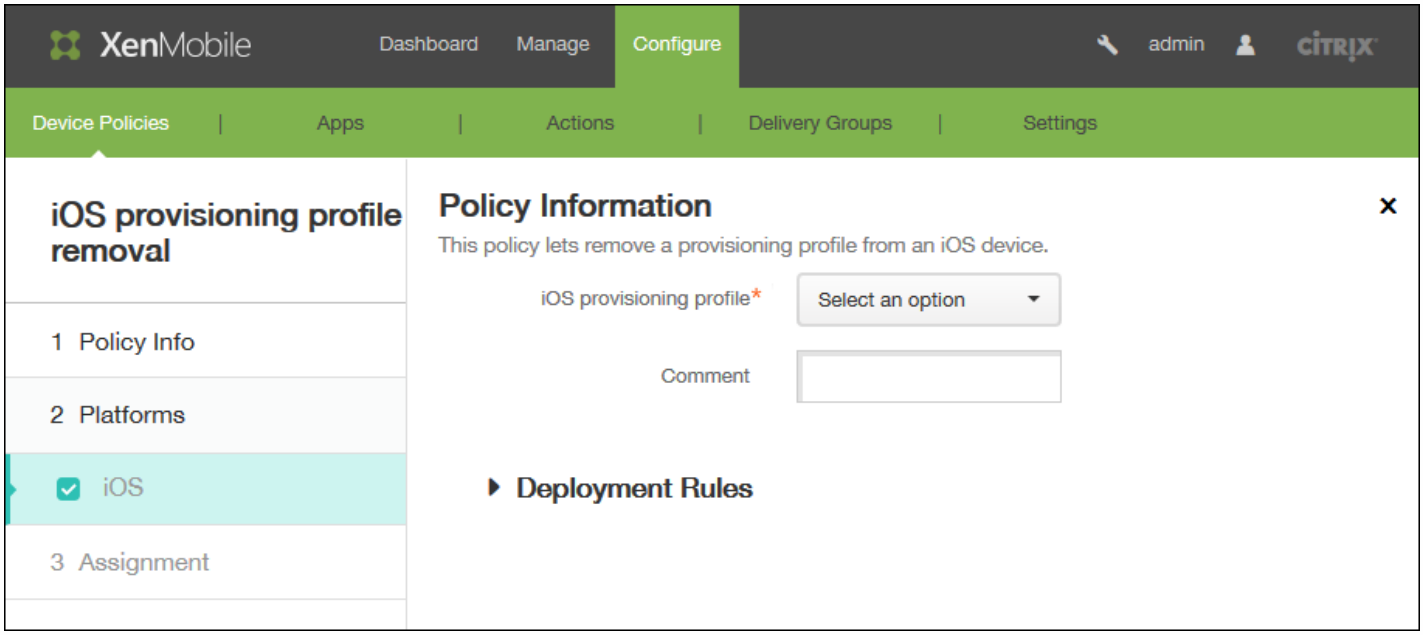
So fügen Sie eine Richtlinie zum Entfernen von Provisioningprofilen für iOS-Geräte hinzu





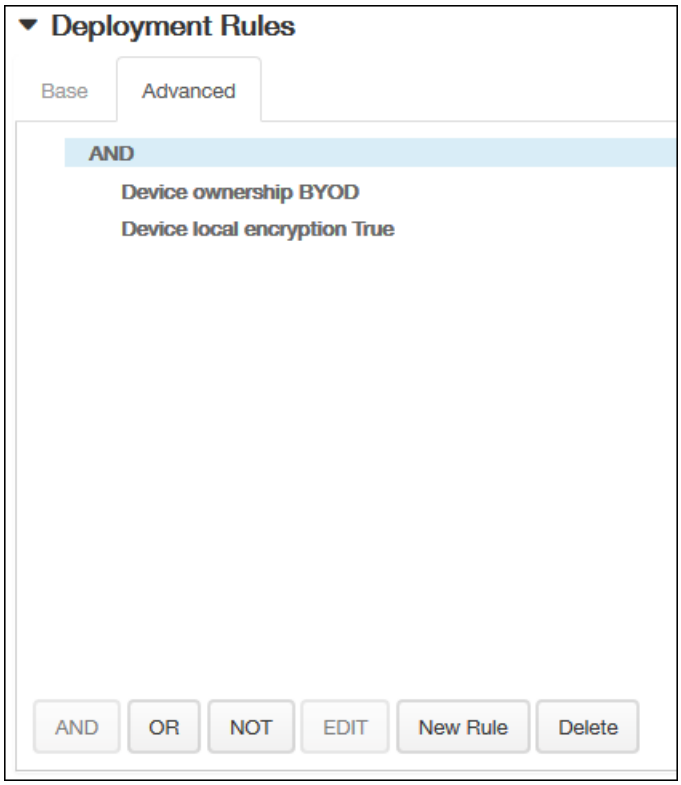


-
-

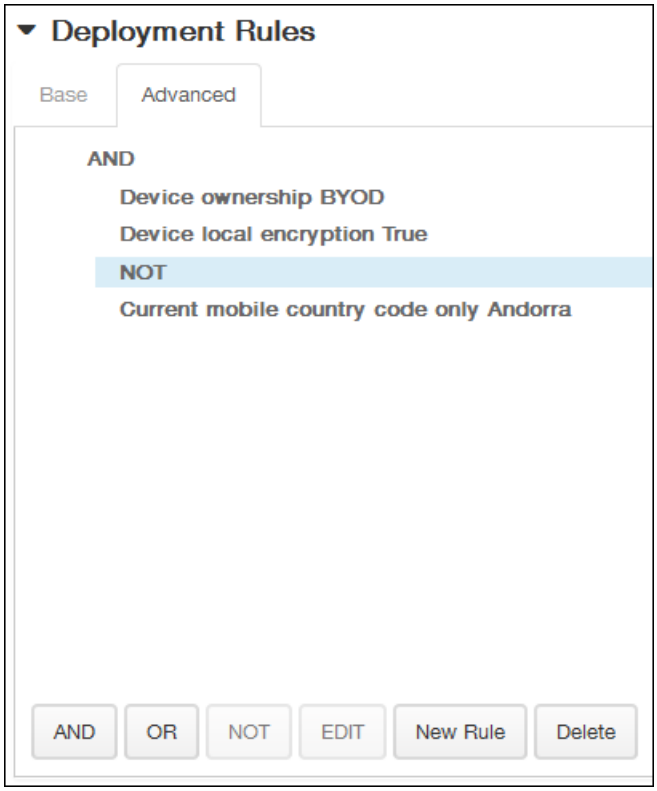


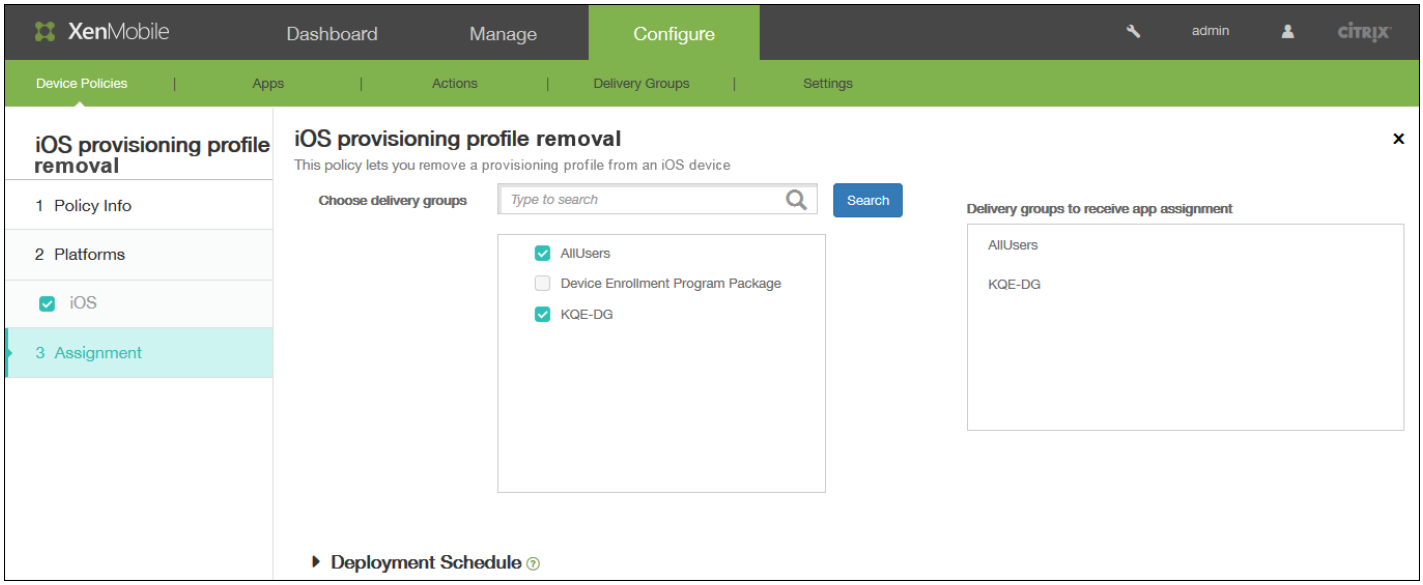
-
-

-
-
-
-



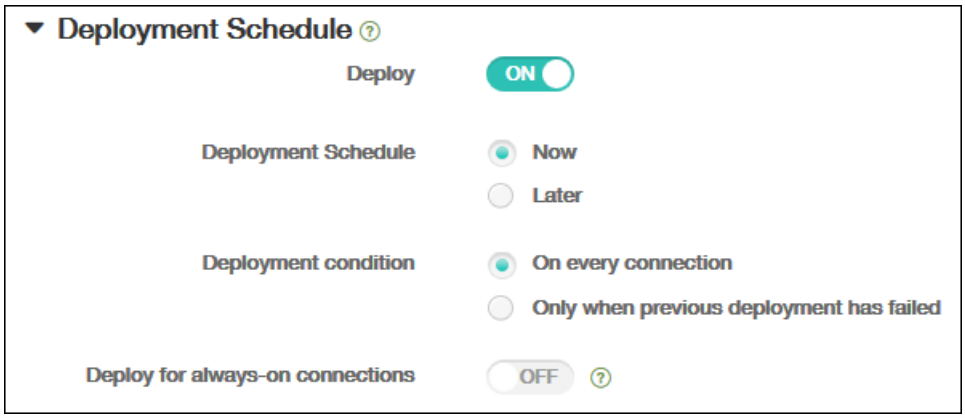
-
-
-
-



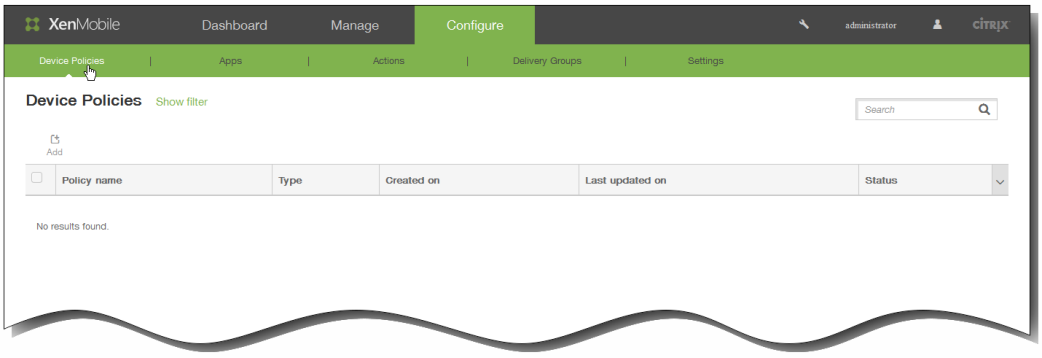


-
-
-
-

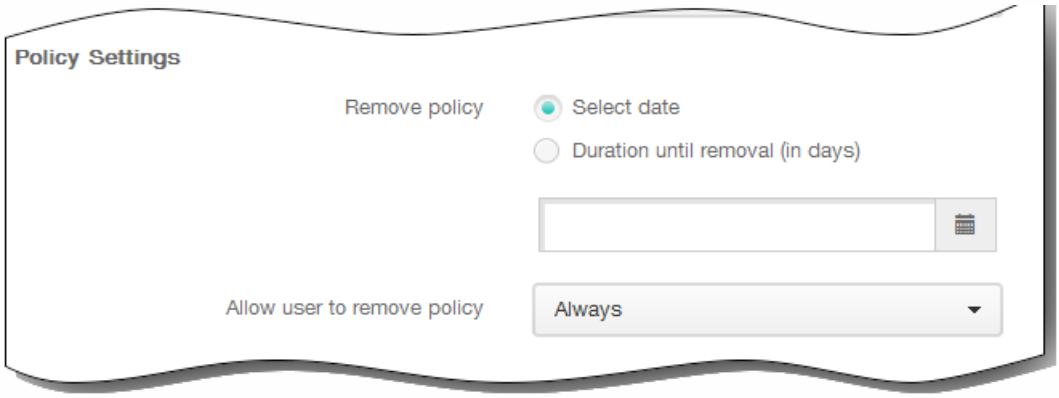
> Hinweis



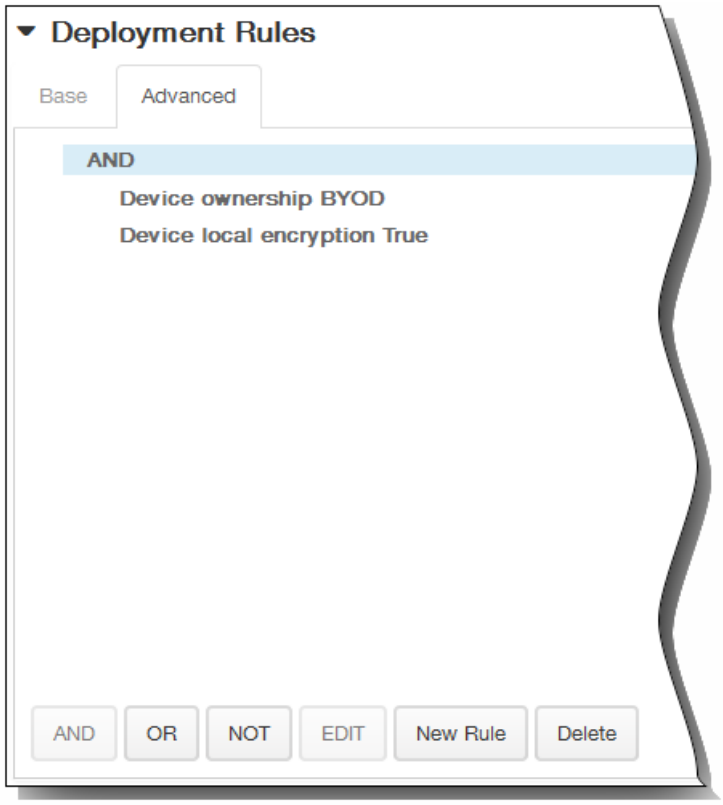
Anmeldeinformationsrichtlinien für Geräte

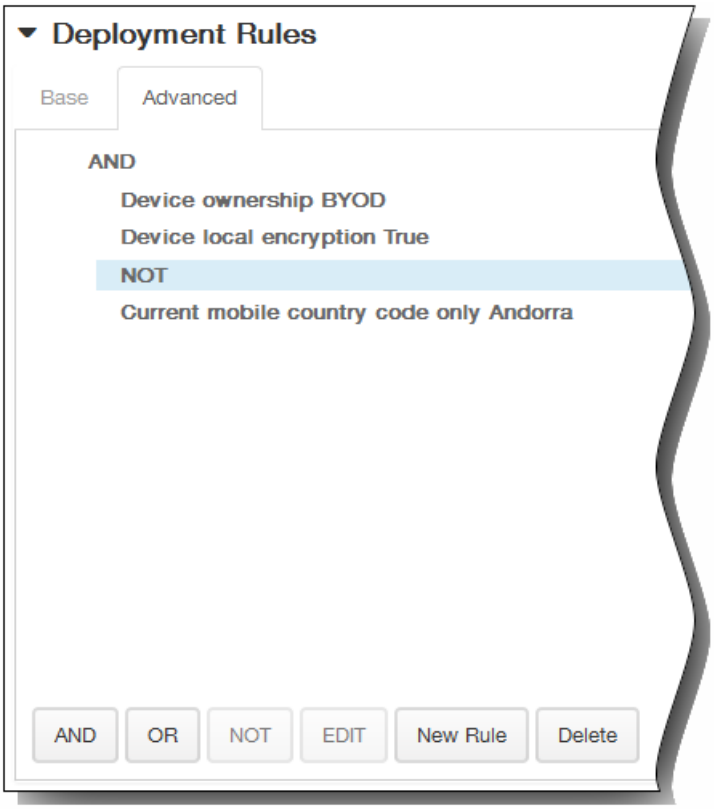
- 

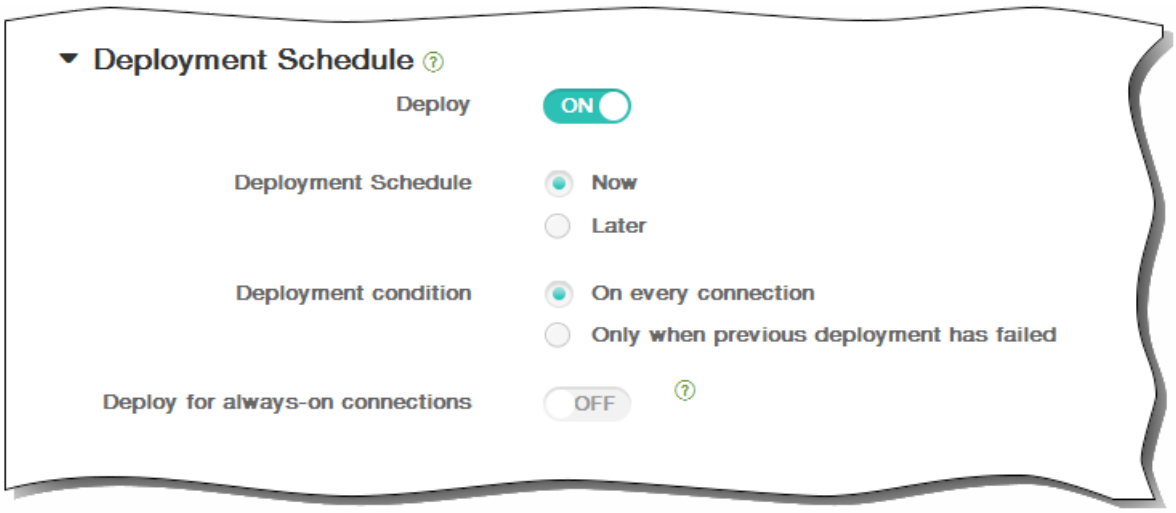
-
  -
    -
    -
  -
    -



-

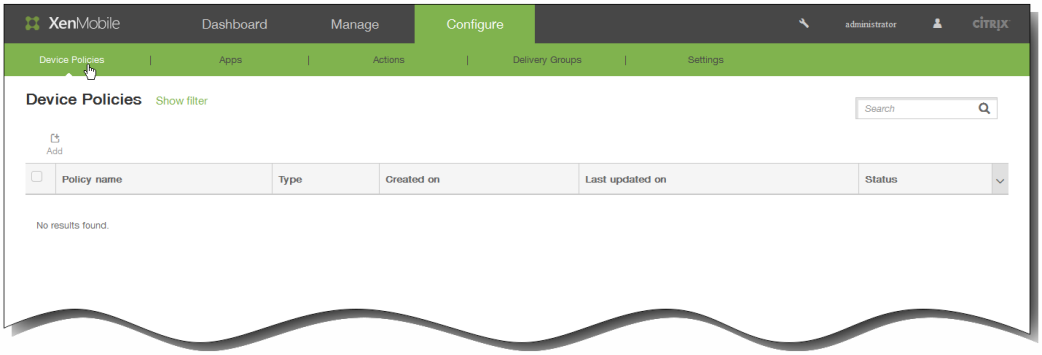


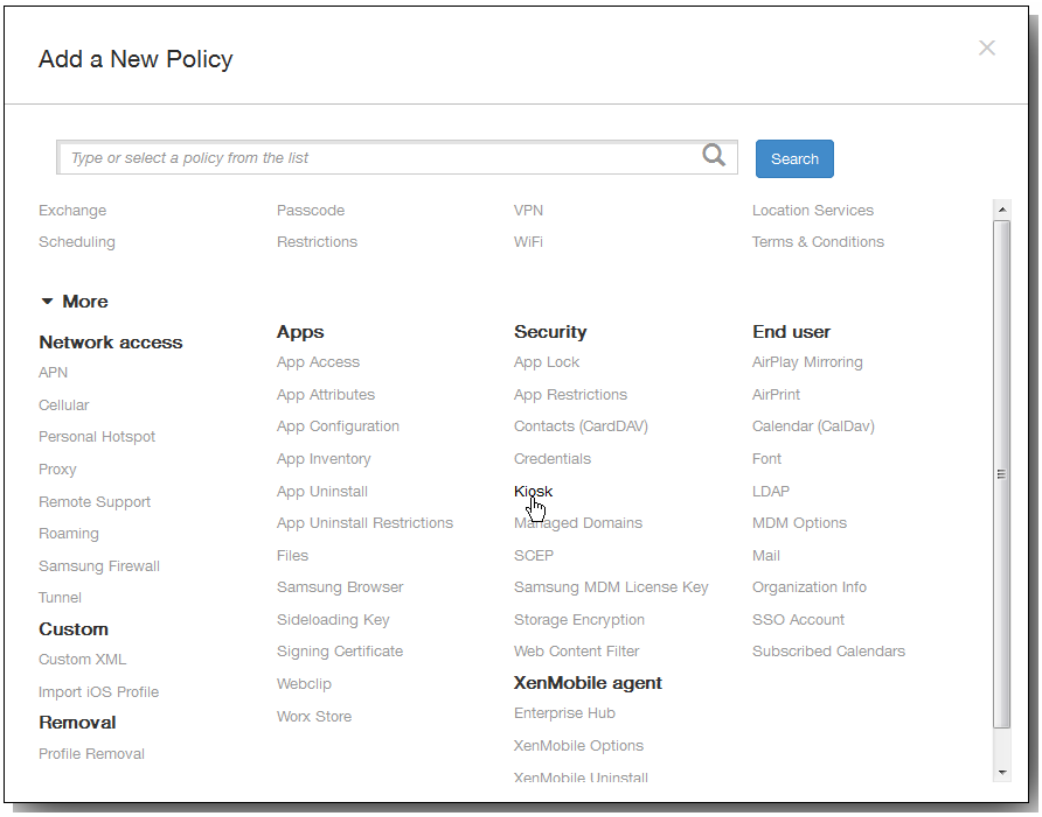


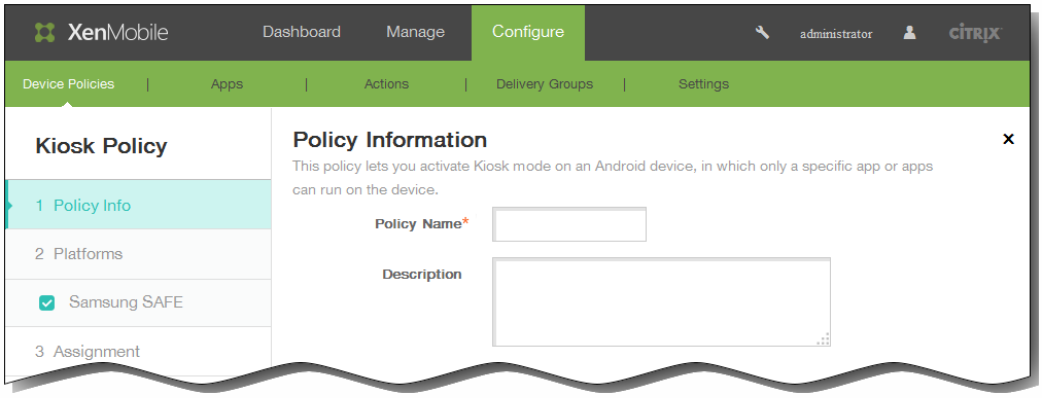


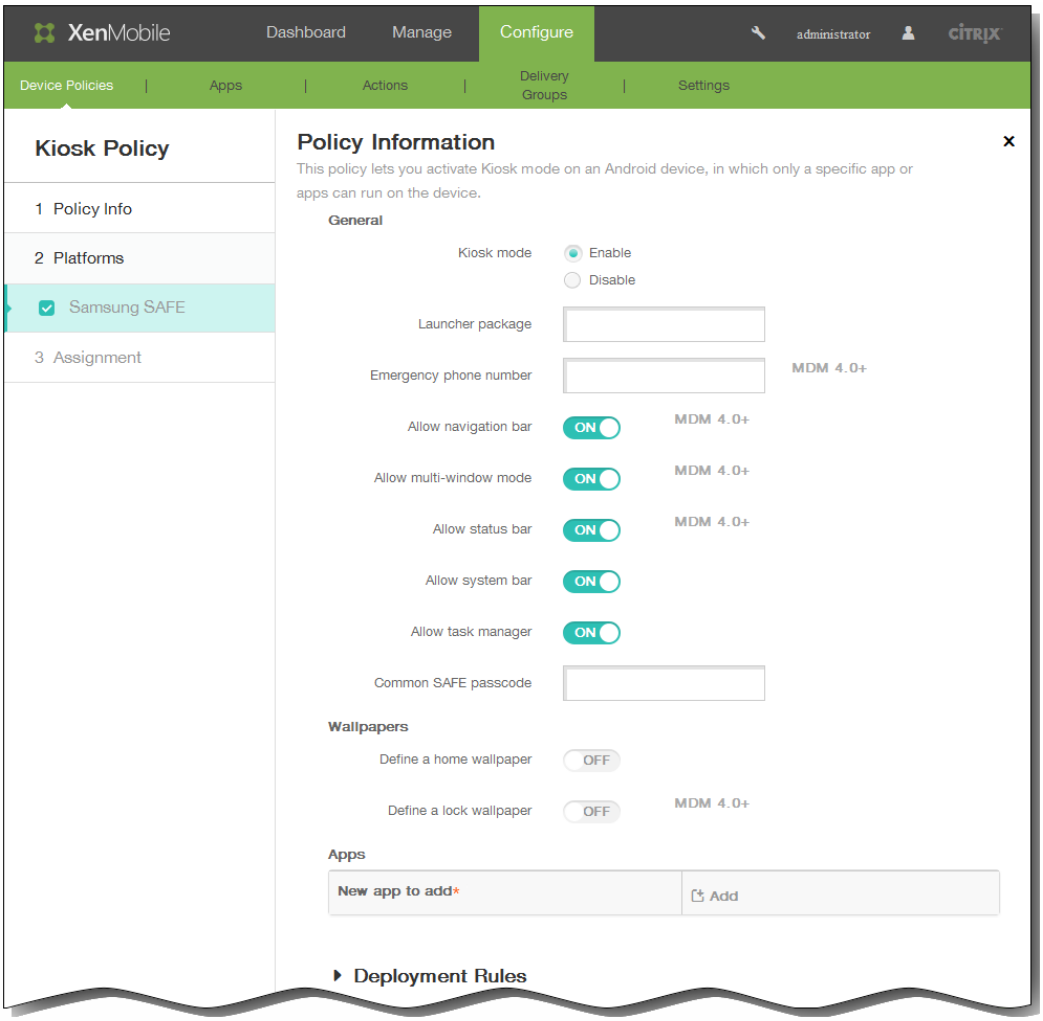
So fügen Sie eine Kioskrichtlinie für Samsung SAFE-Geräte hinzu

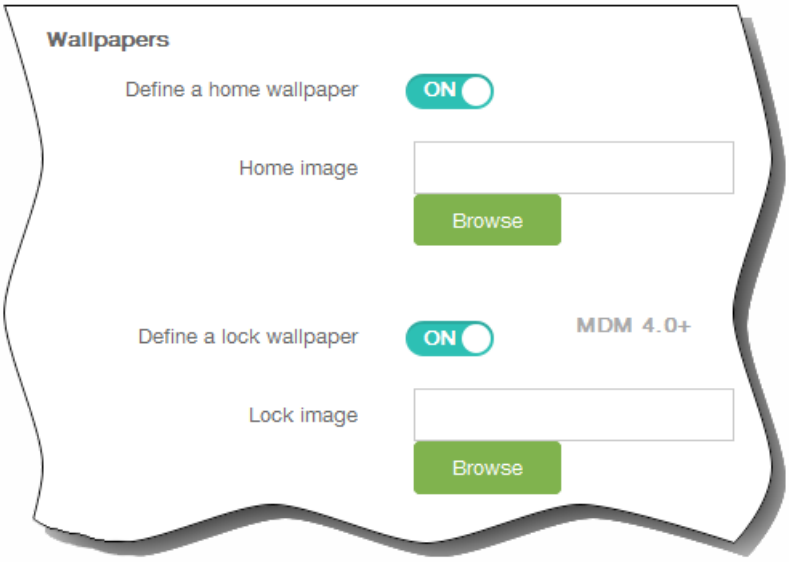
-
-

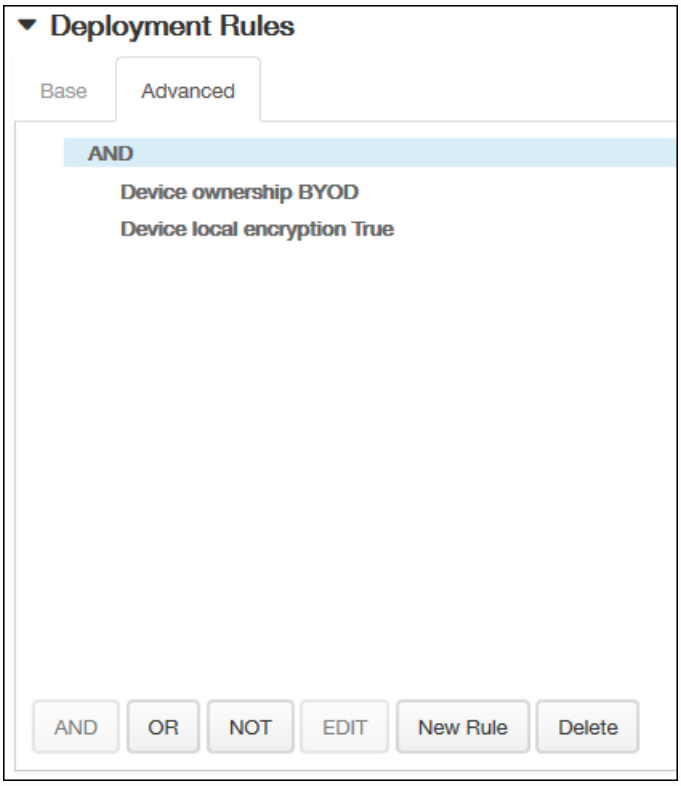


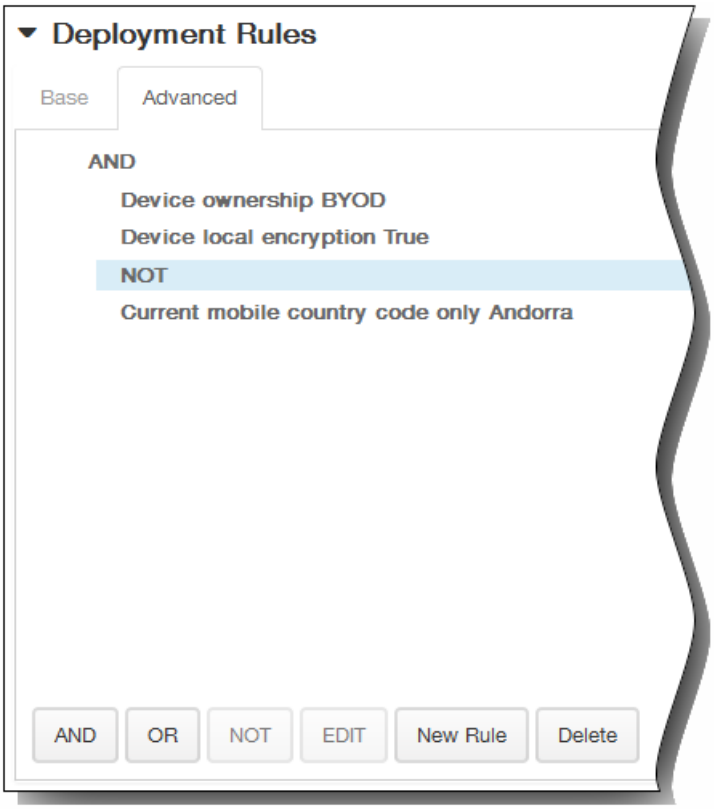


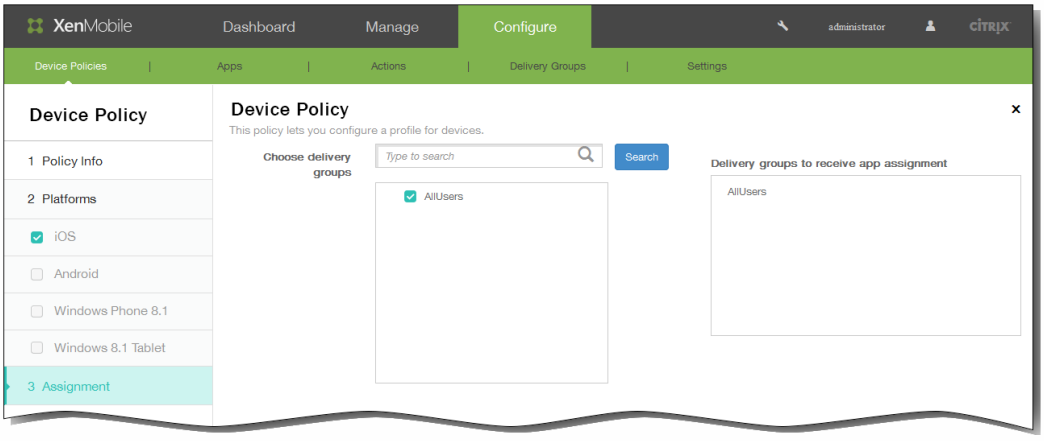


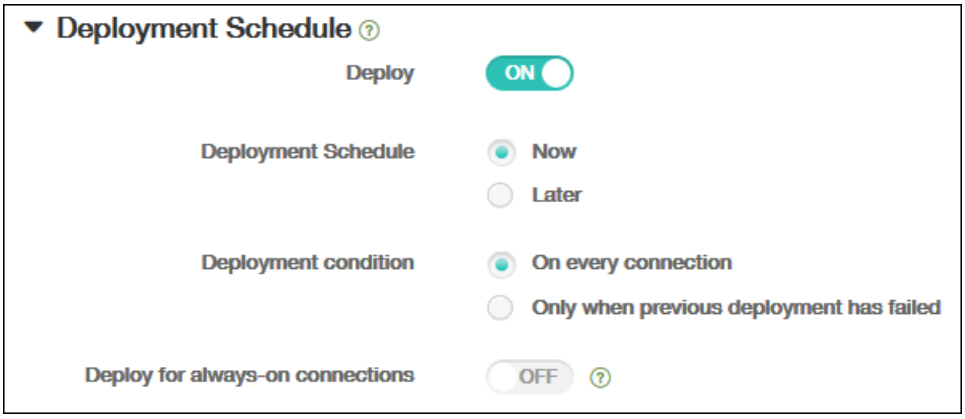




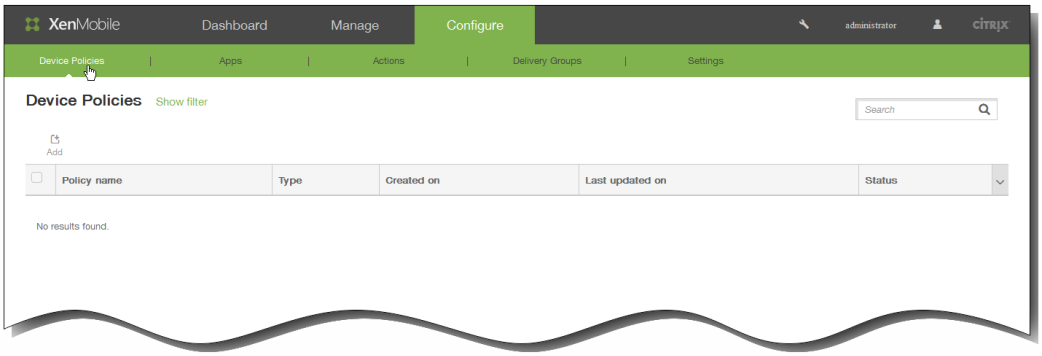


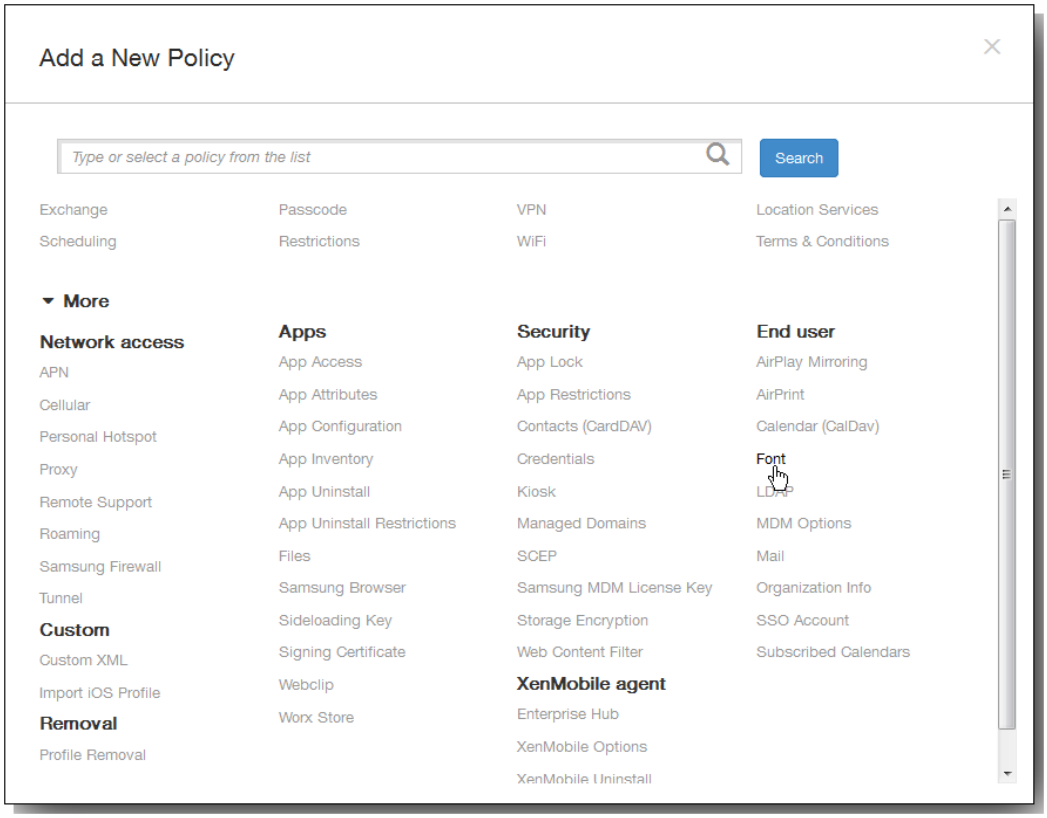


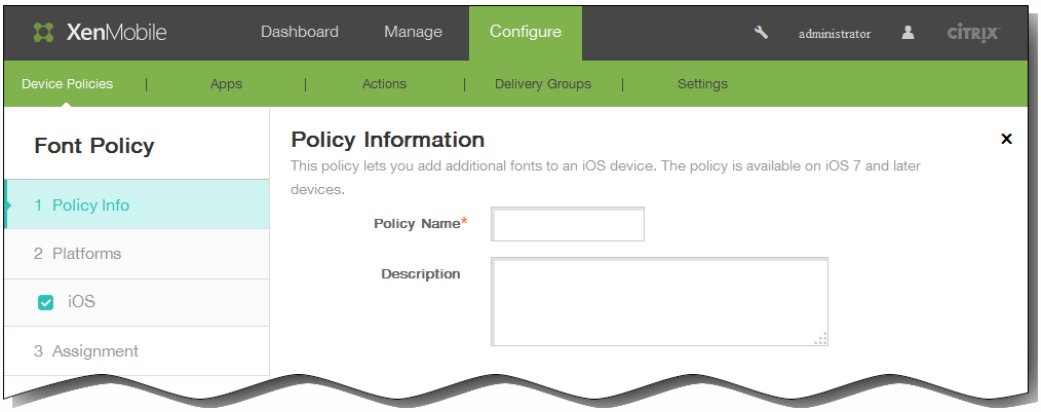


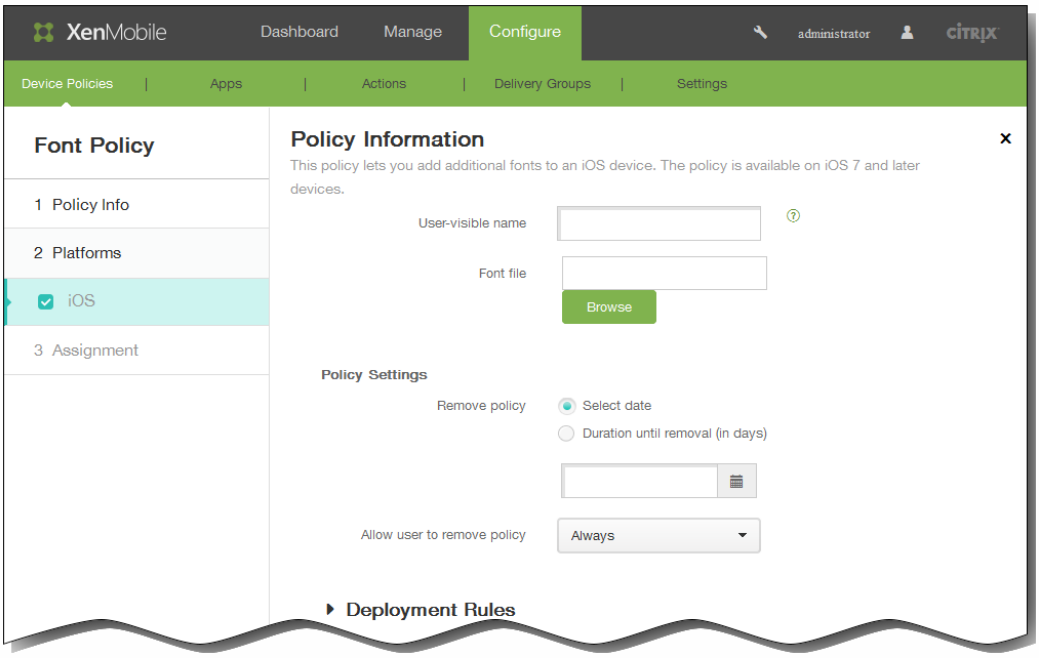


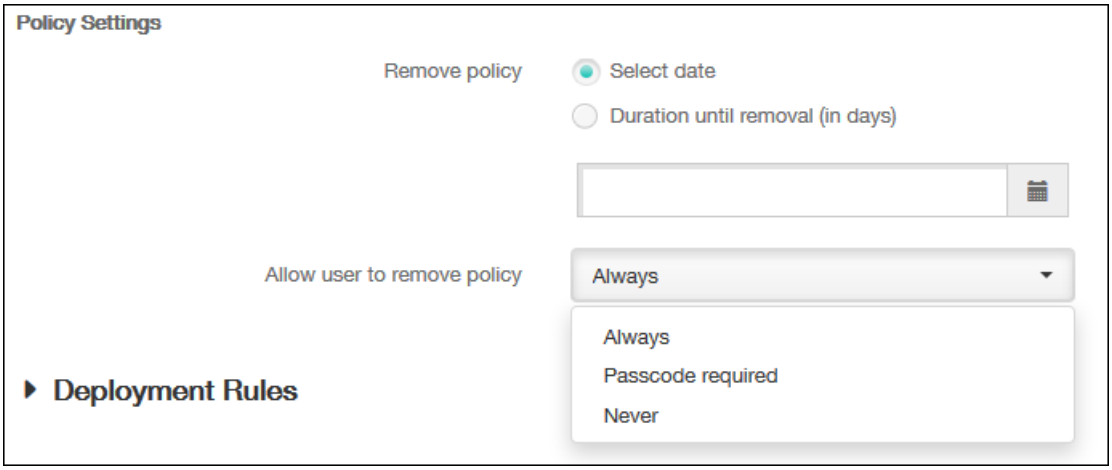
So fügen Sie eine Schriftartrichtlinie für iOS-Geräte hinzu

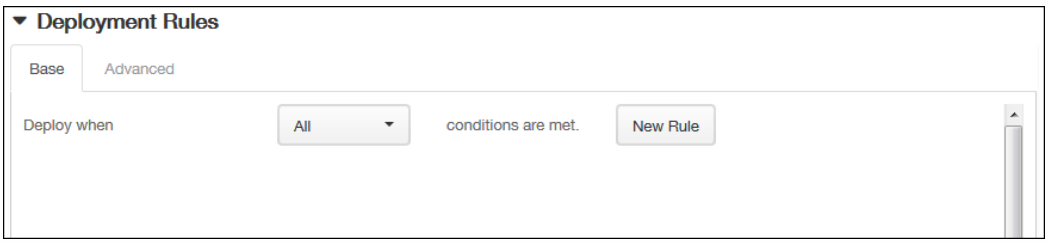


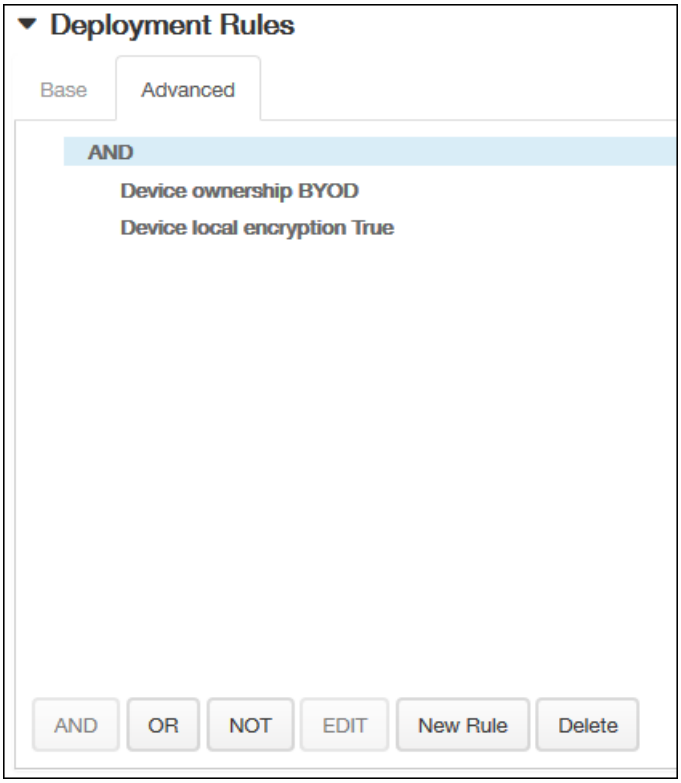


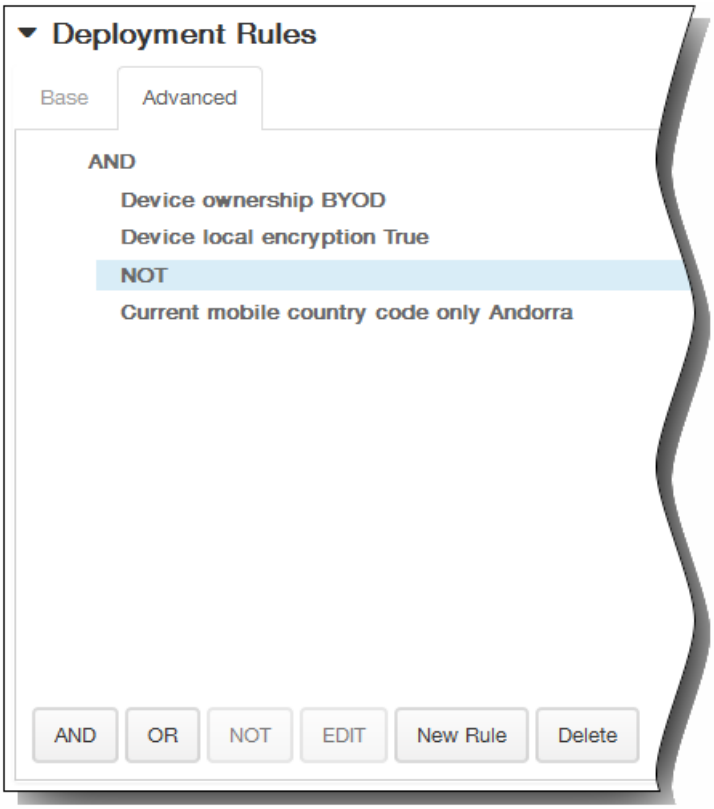


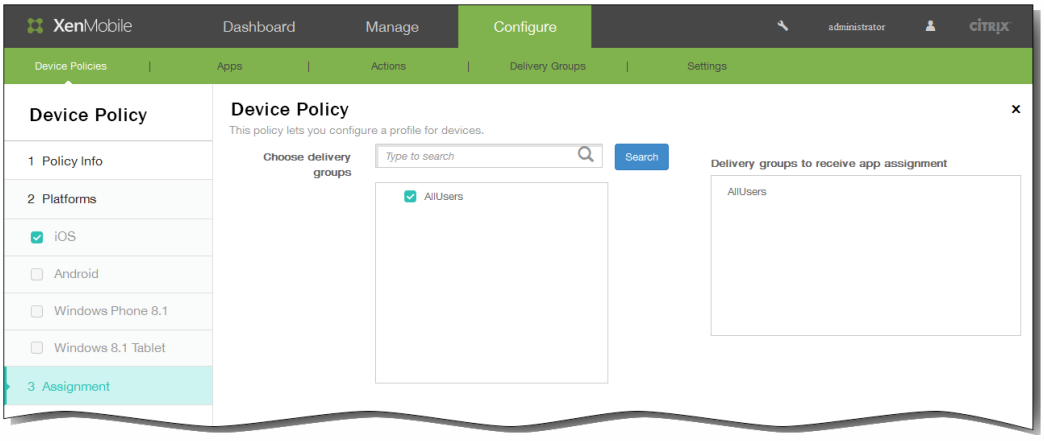


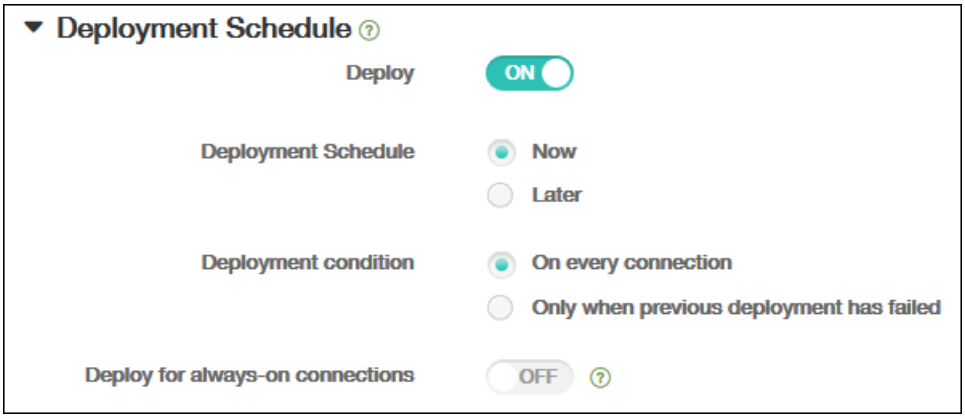




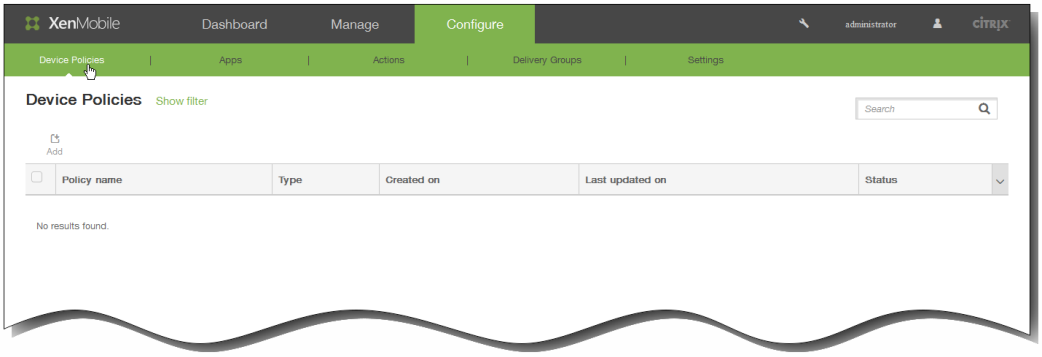


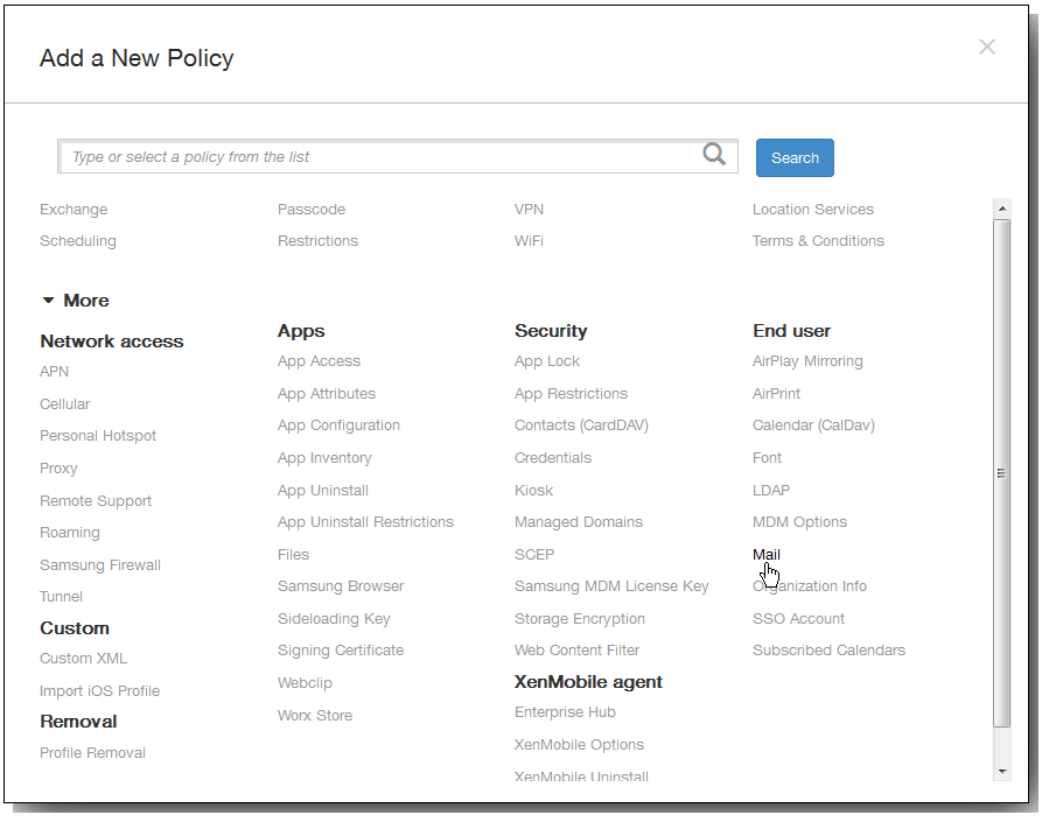


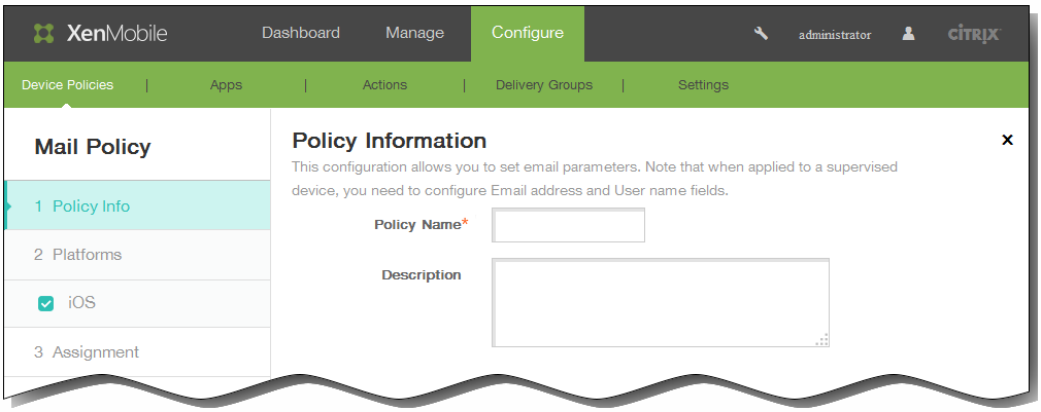


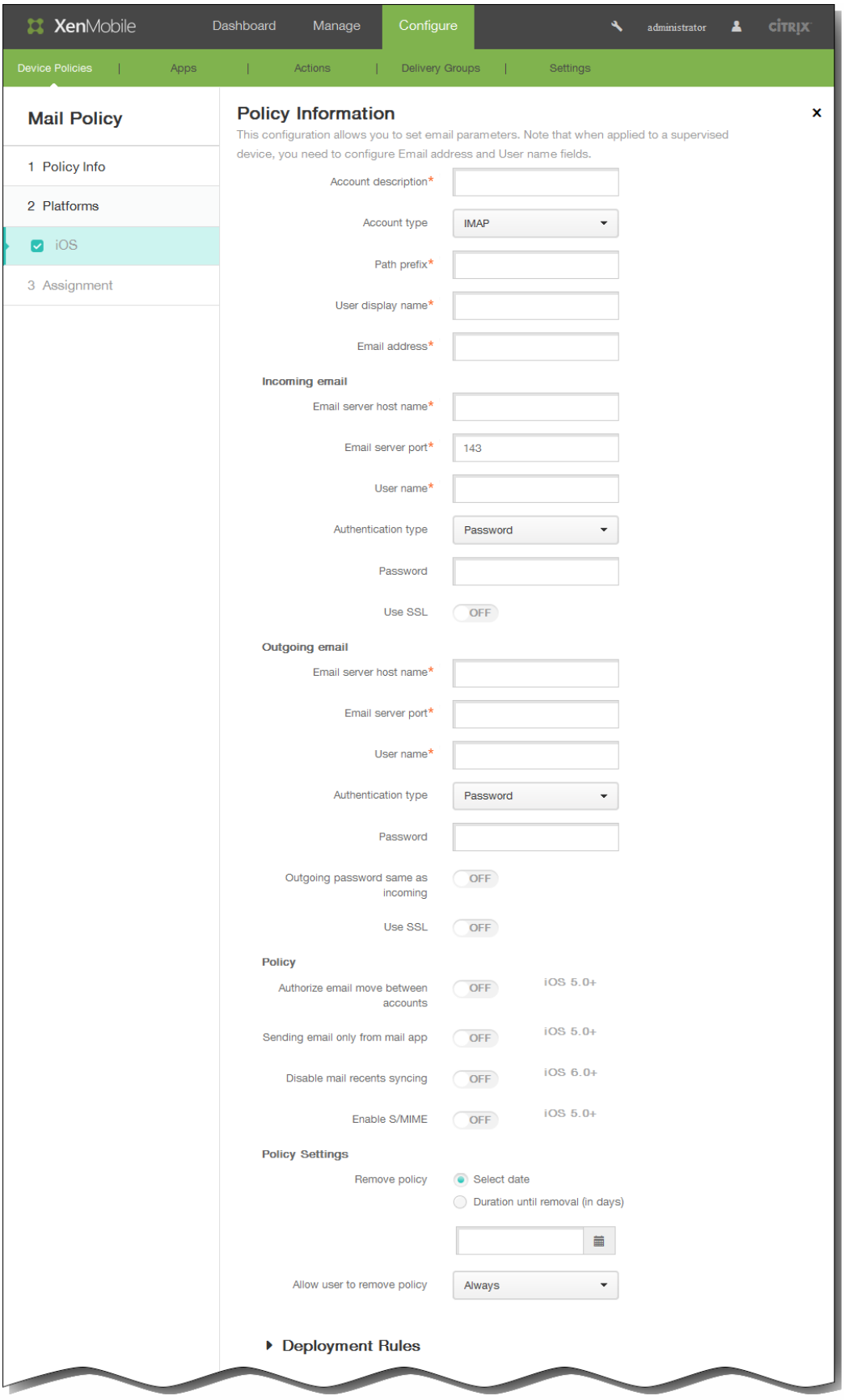


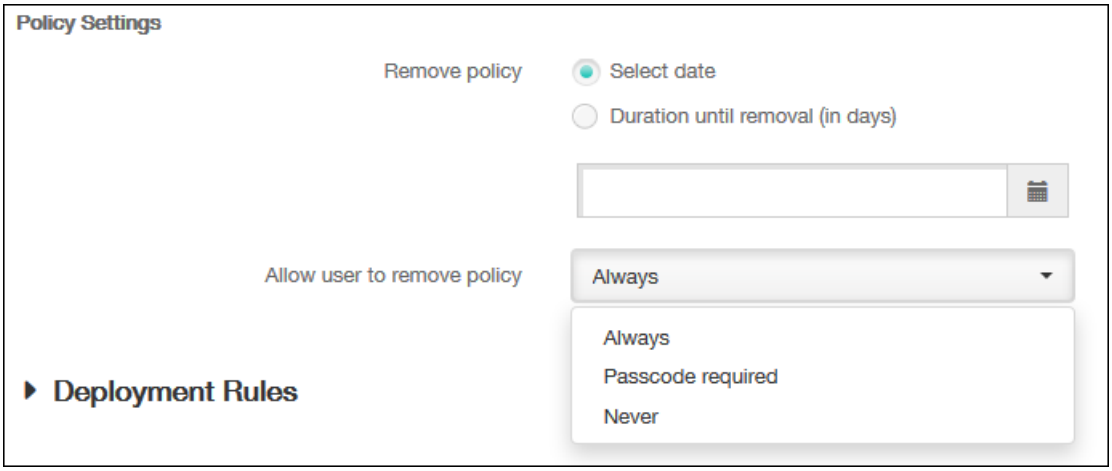
So fügen Sie eine E-Mail-Richtlinie für iOS-Geräte hinzu

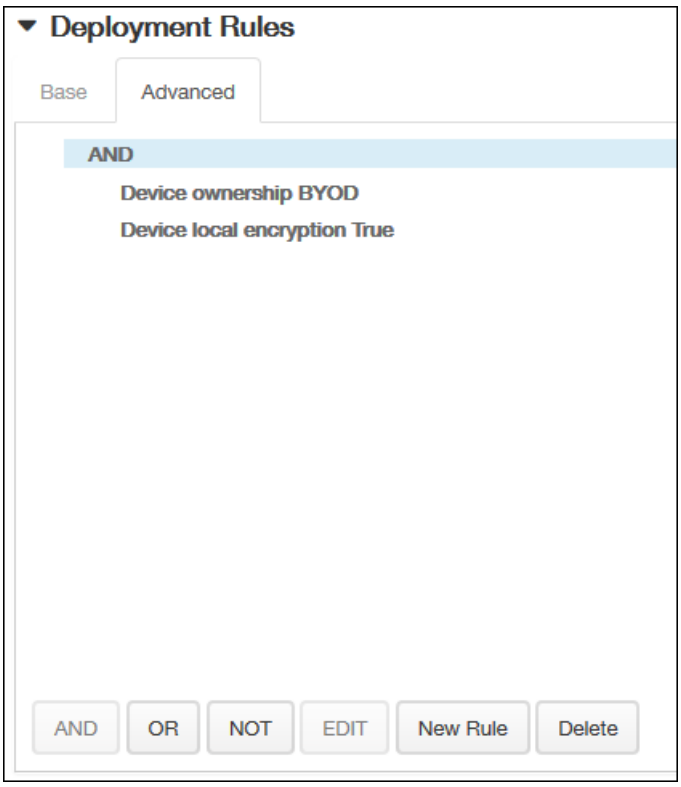


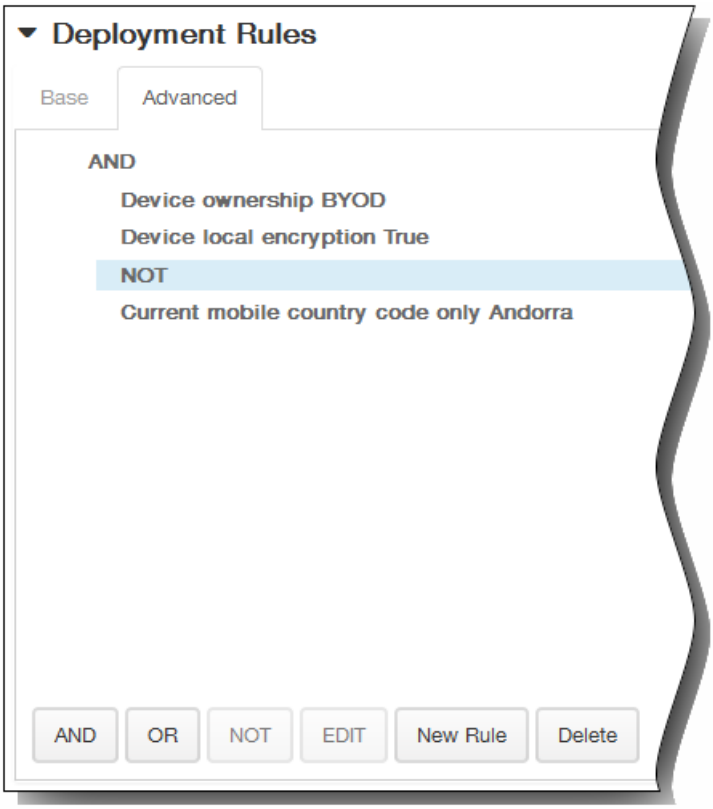


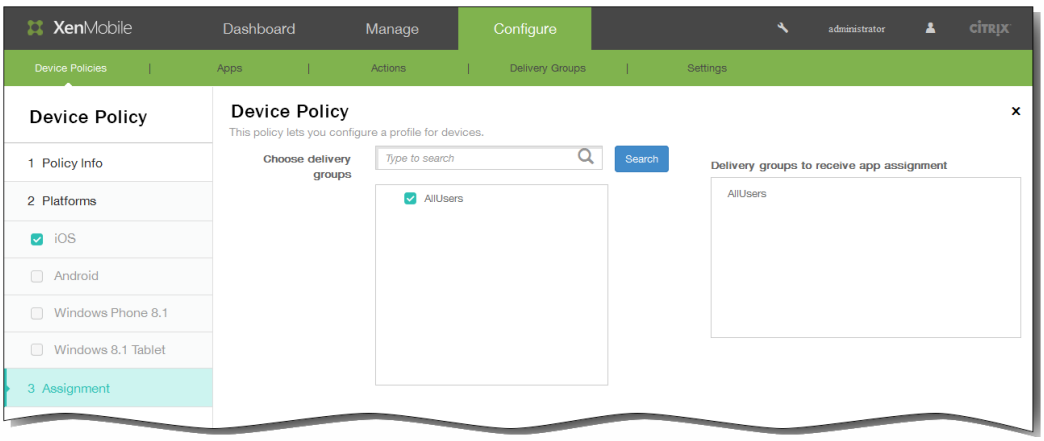


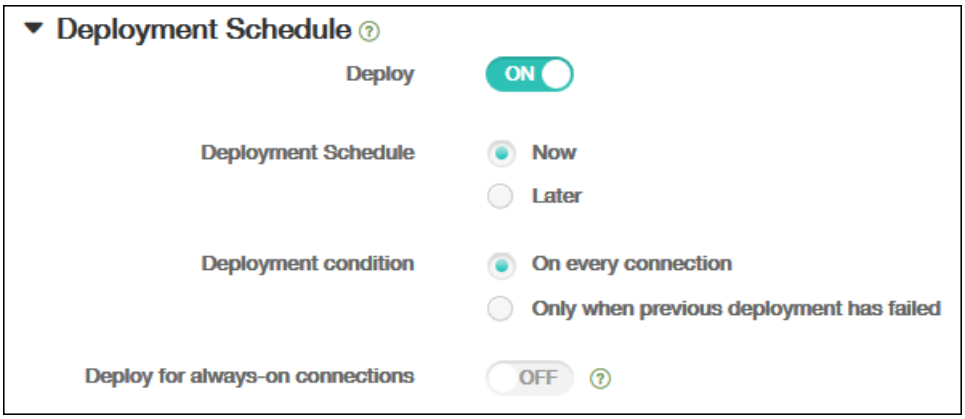




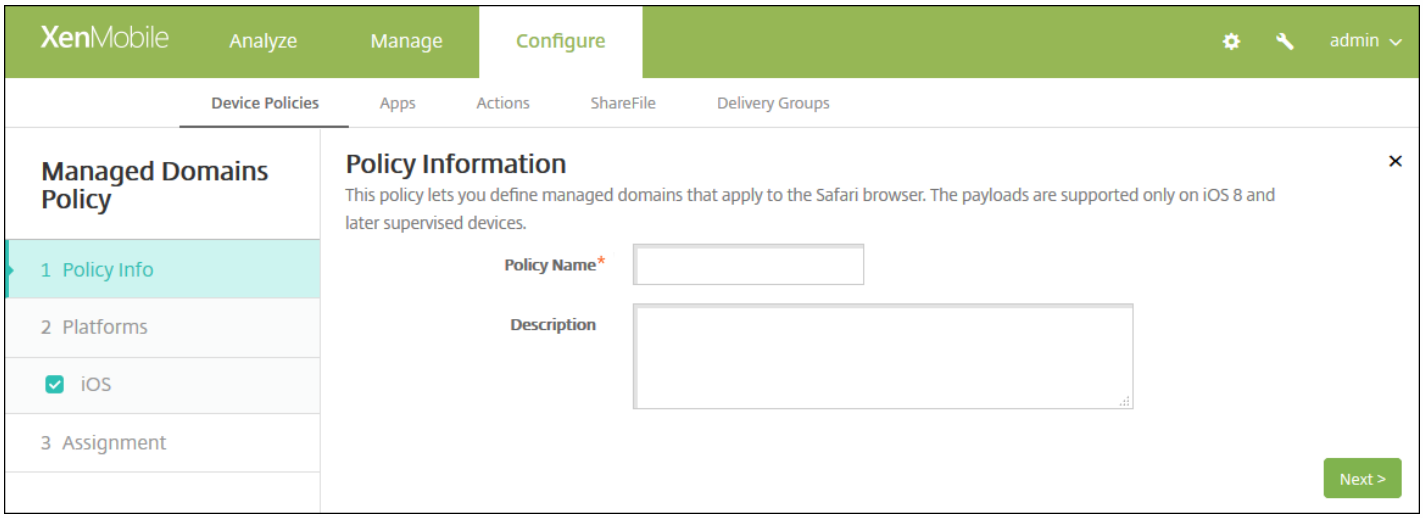




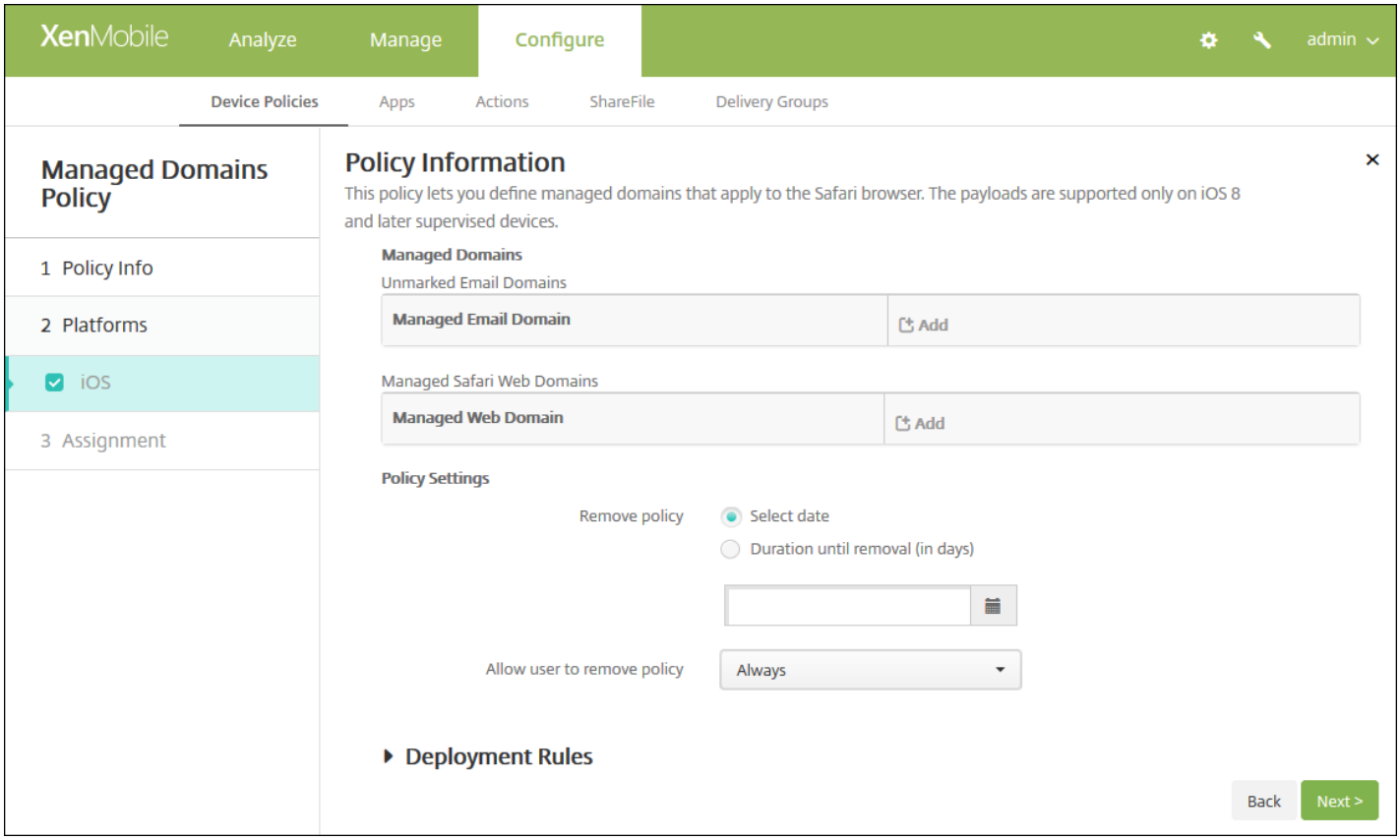


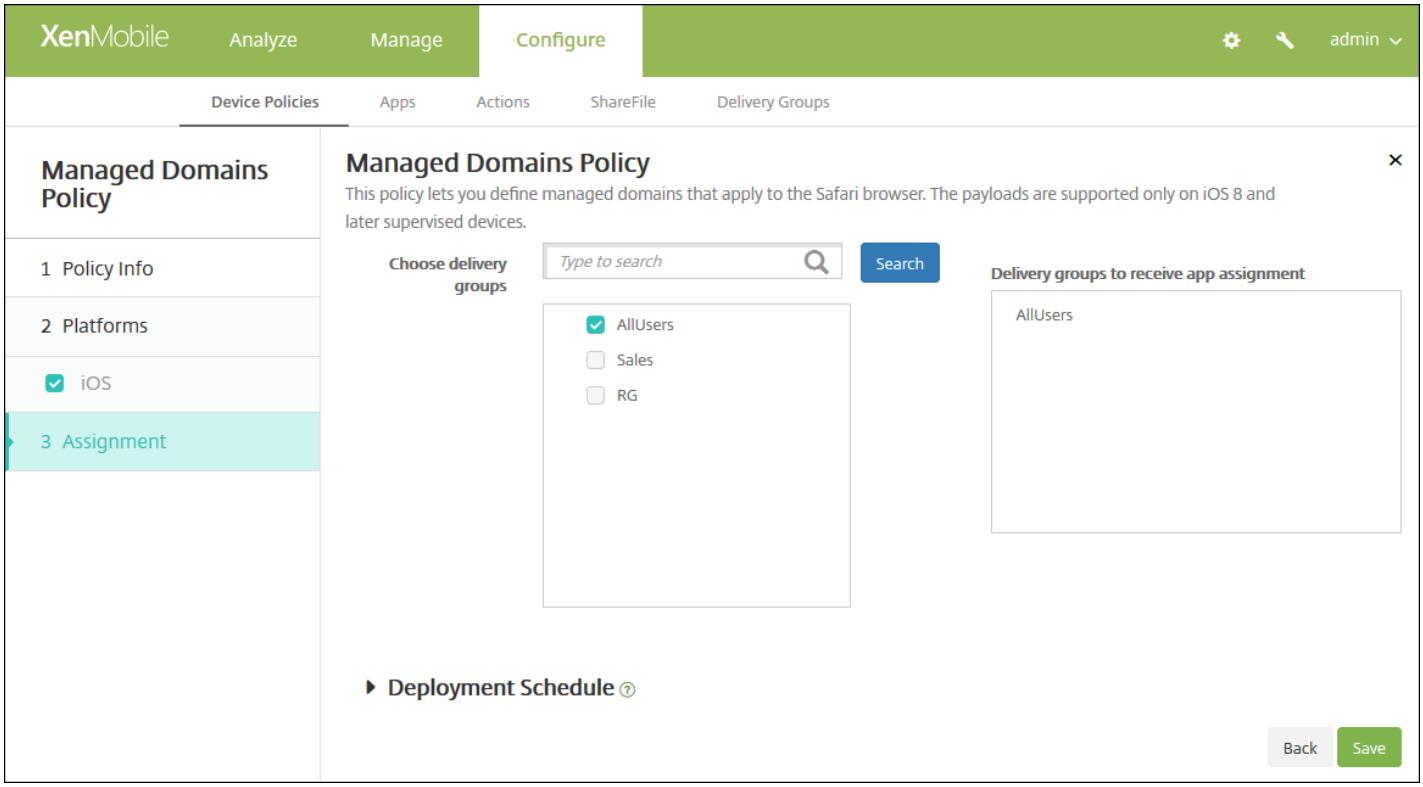


Geräterichtlinie für verwaltete Domänen

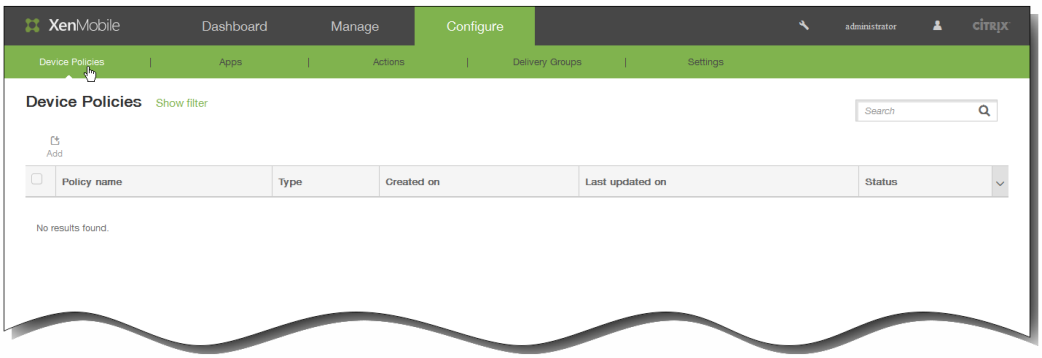


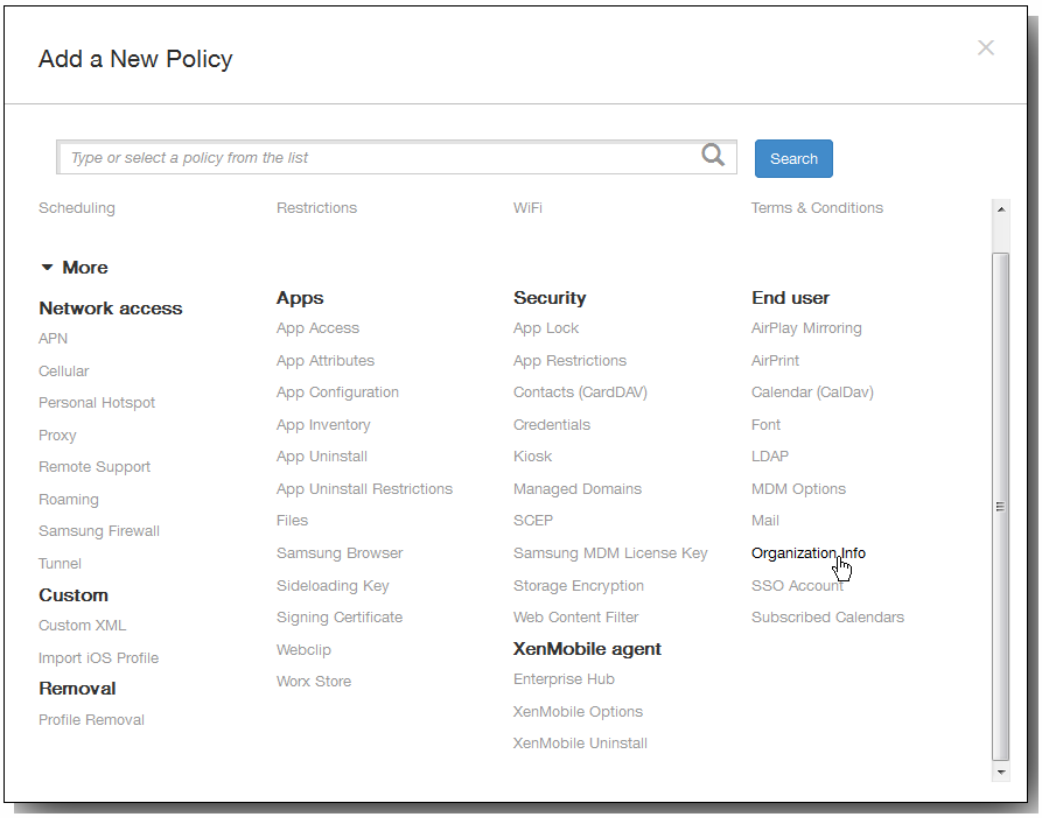
-
-

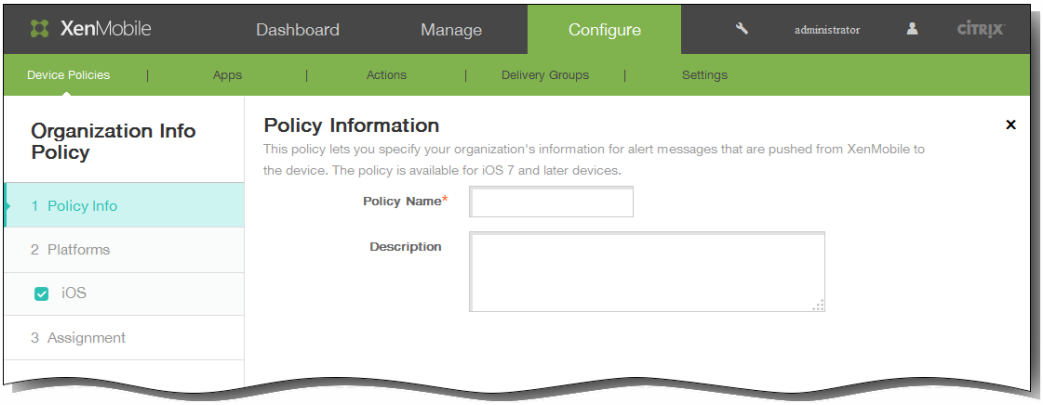


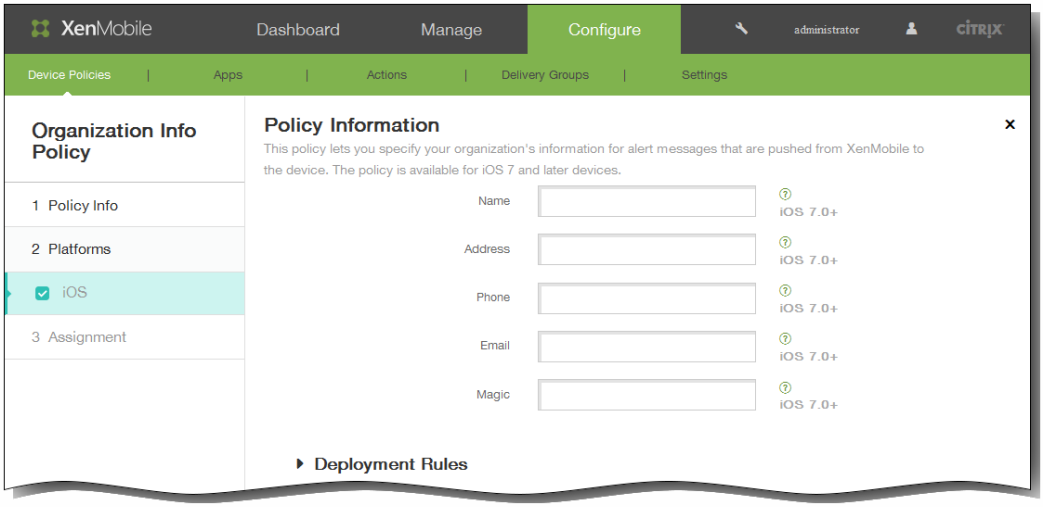


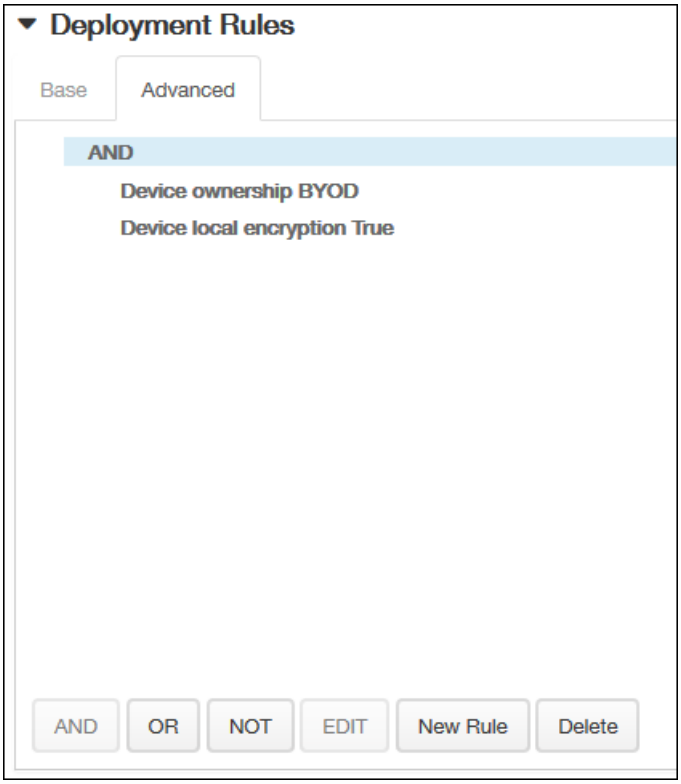
So fügen Sie eine Richtlinie für Unternehmensinformationen für iOS-Geräte hinzu

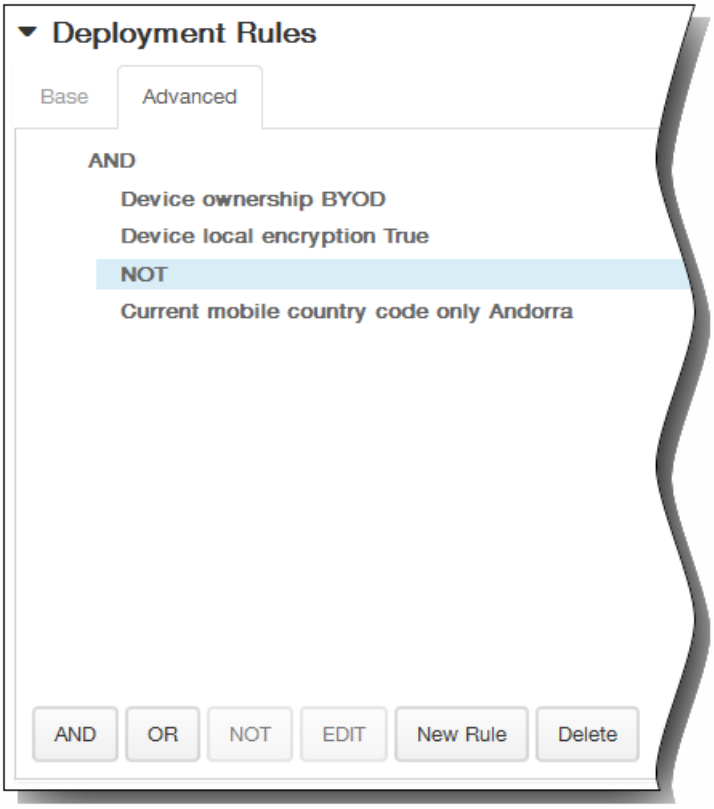


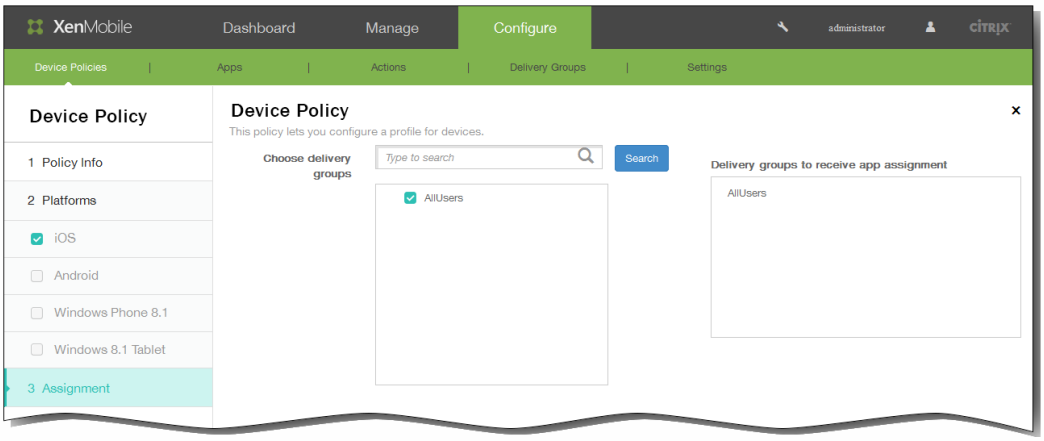


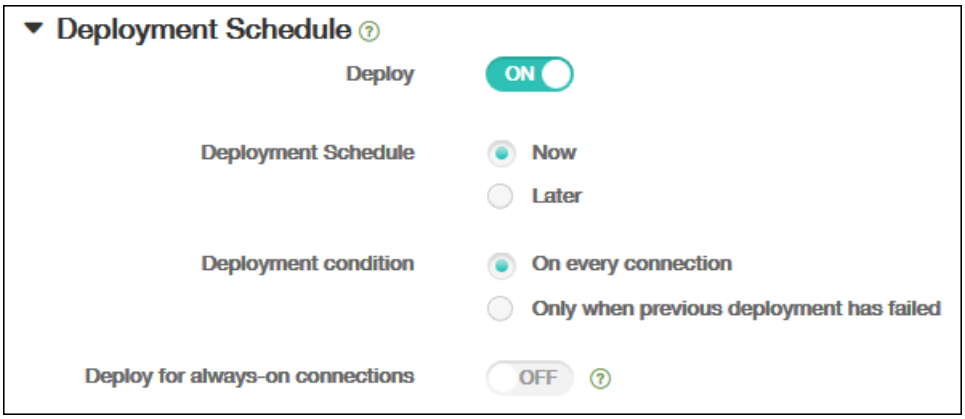




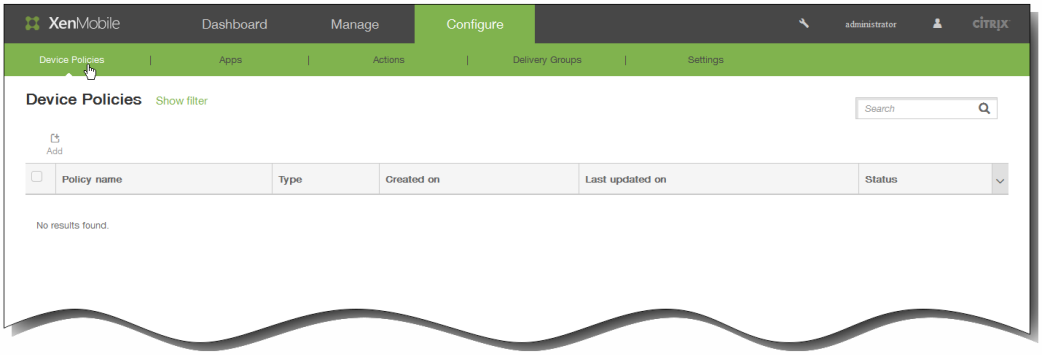


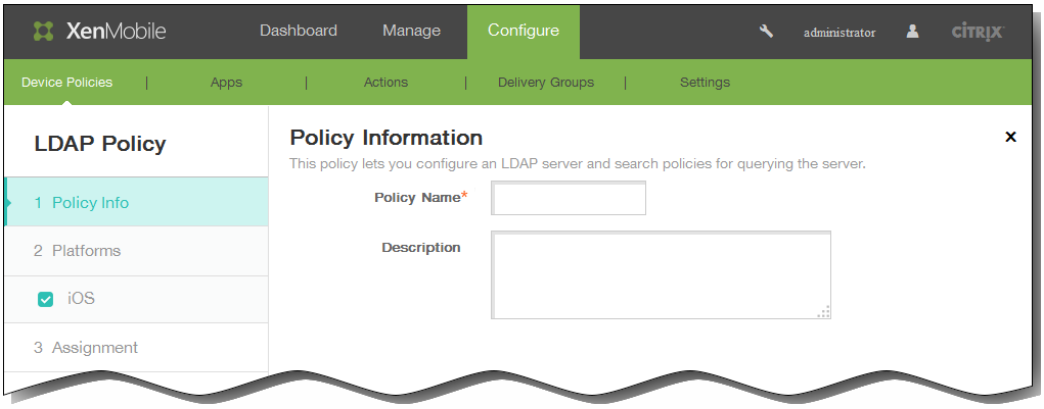






So fügen Sie eine LDAP-Richtlinie für iOS-Geräte hinzu

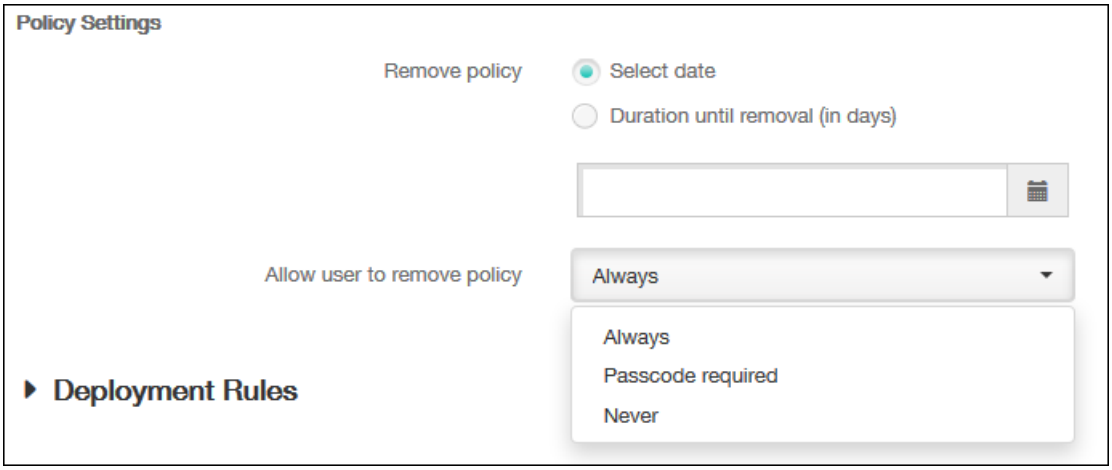


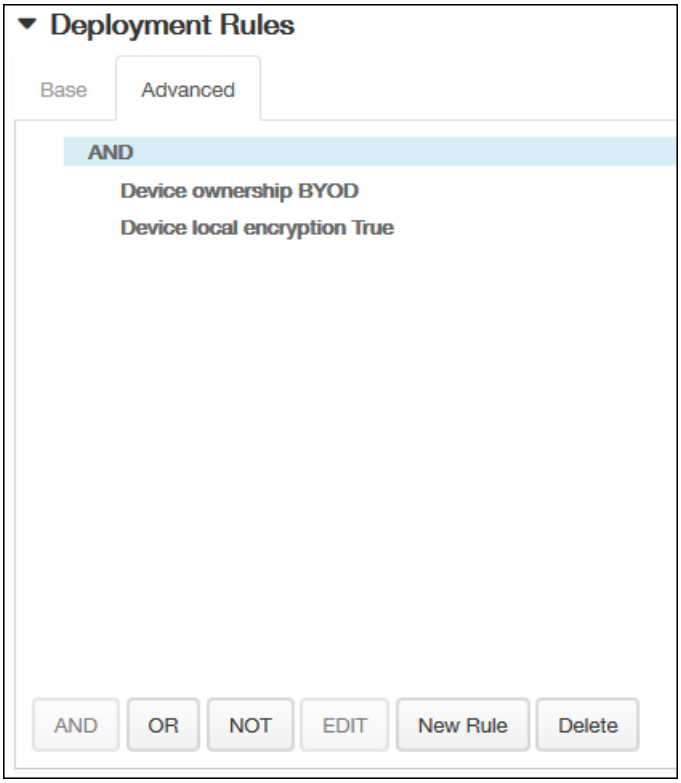


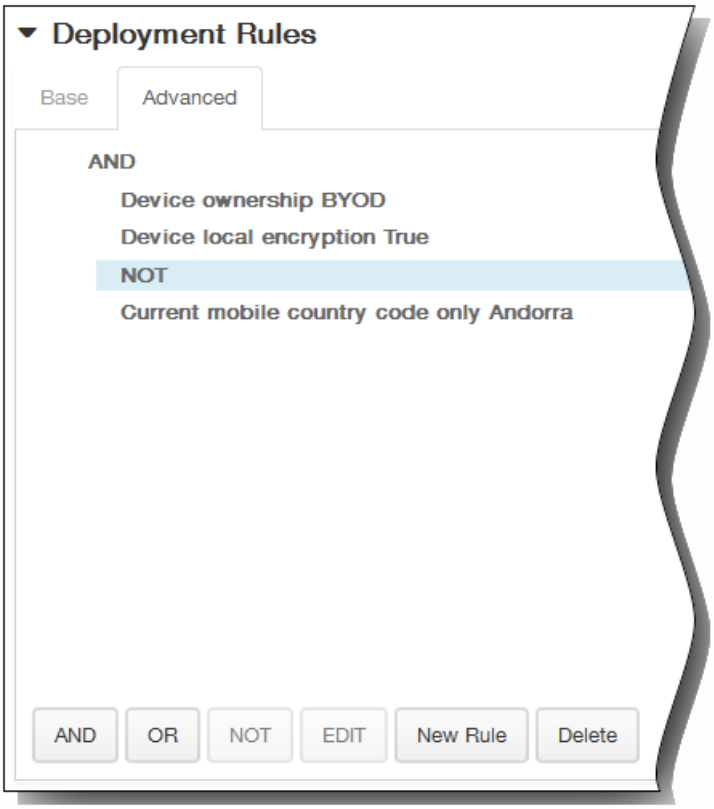
-
-
-

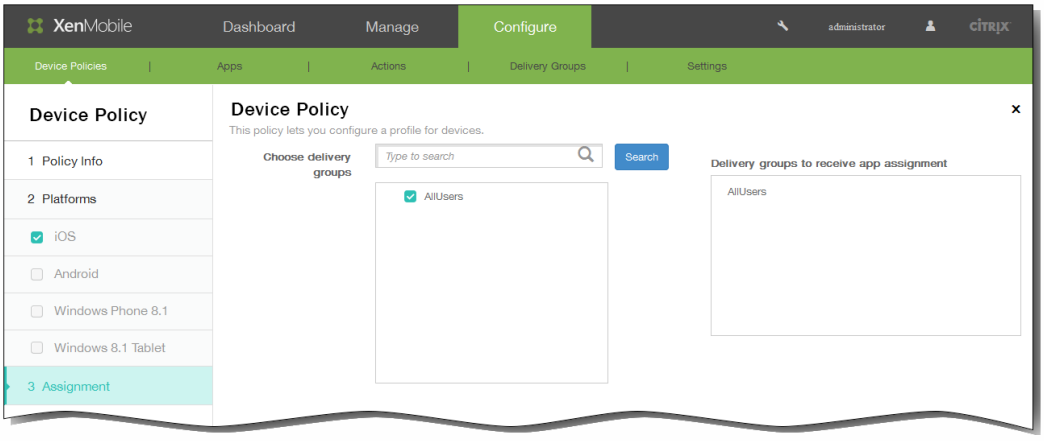
ou=people

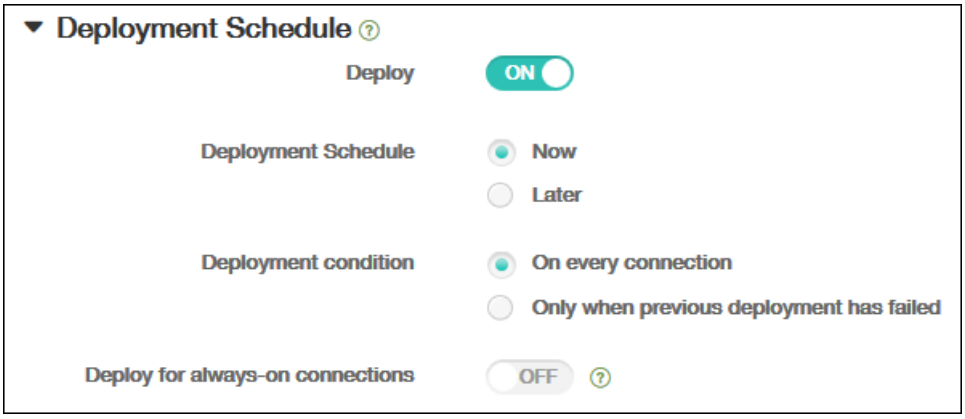
0=example corp



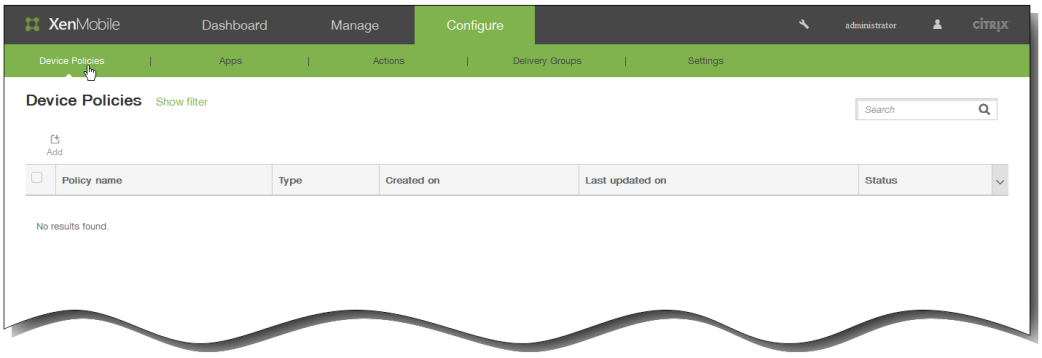


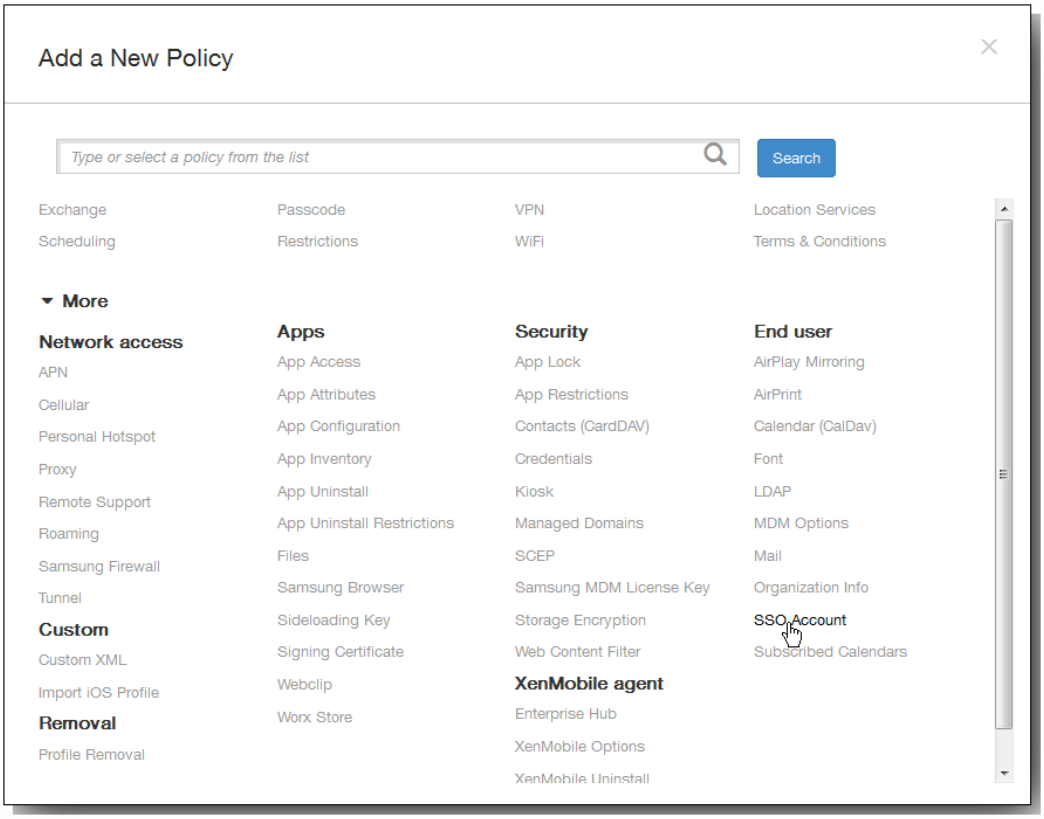


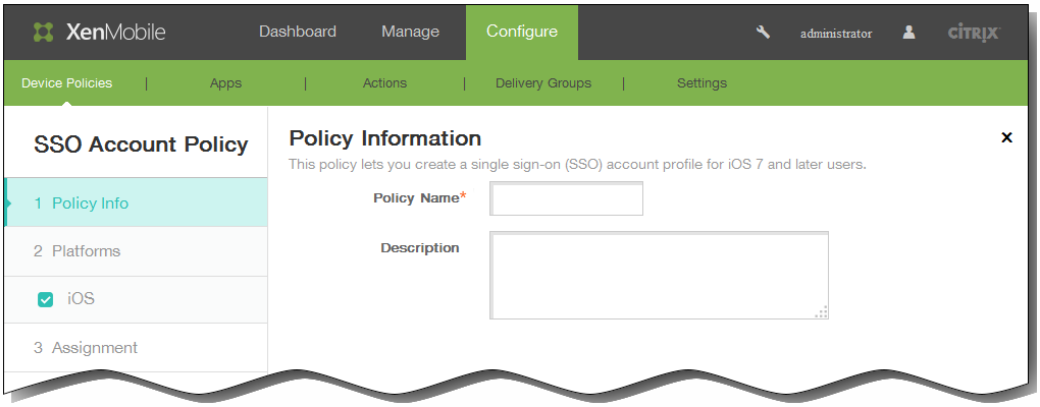


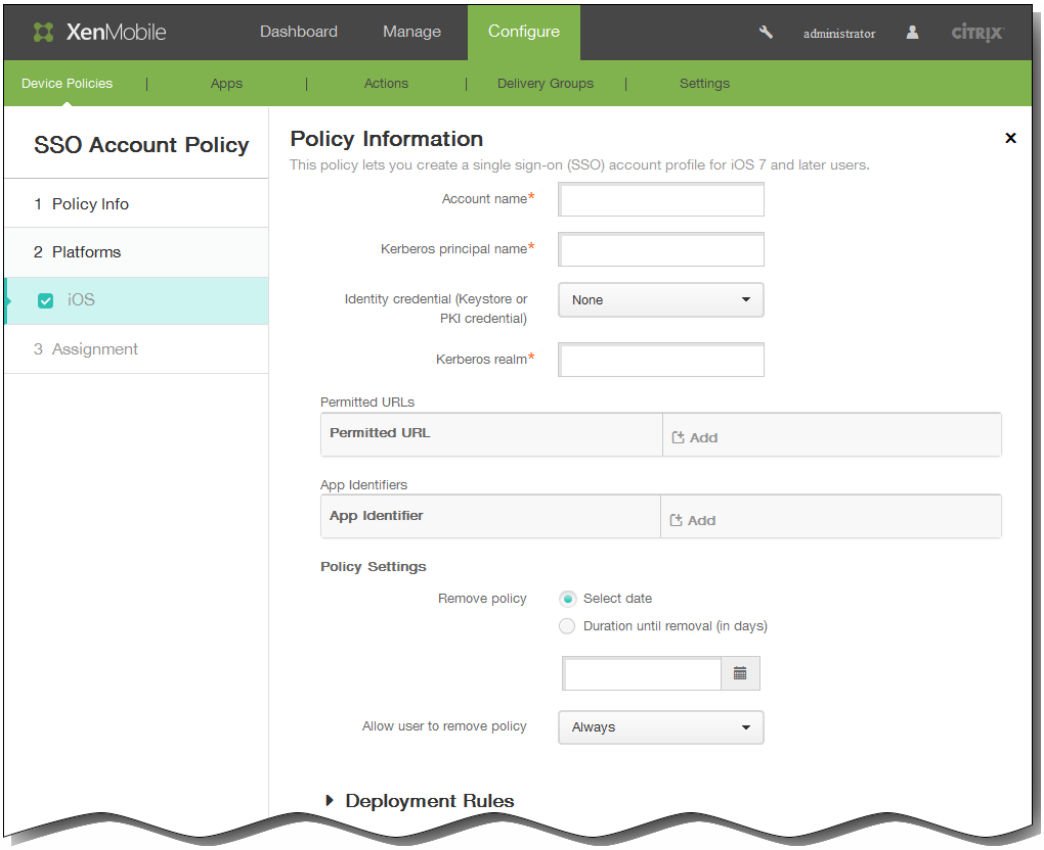


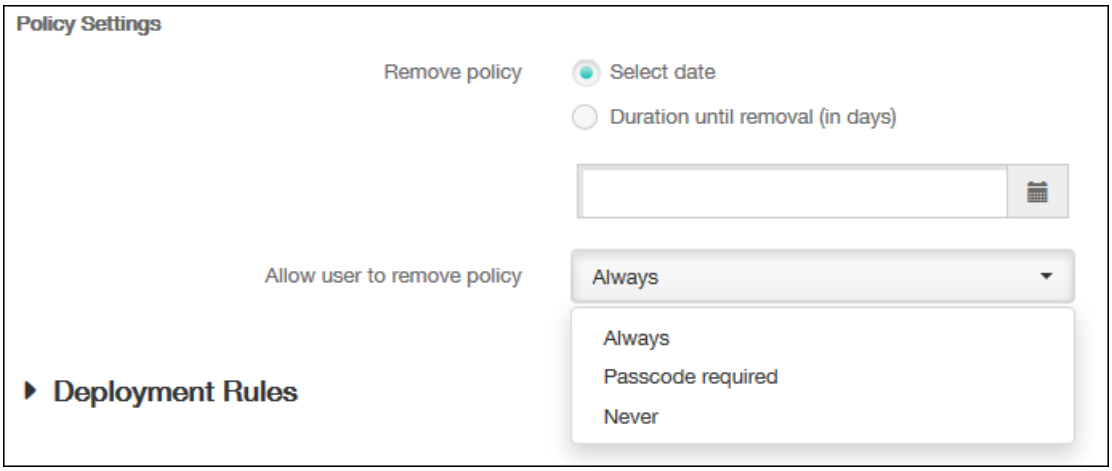
So fügen Sie eine Single Sign-On-Kontorichtlinie für iOS-Geräte hinzu

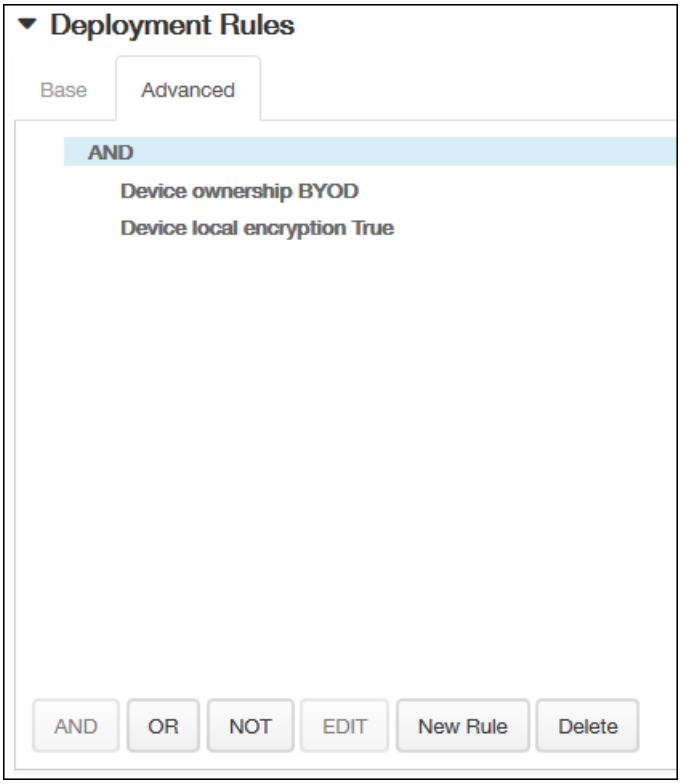


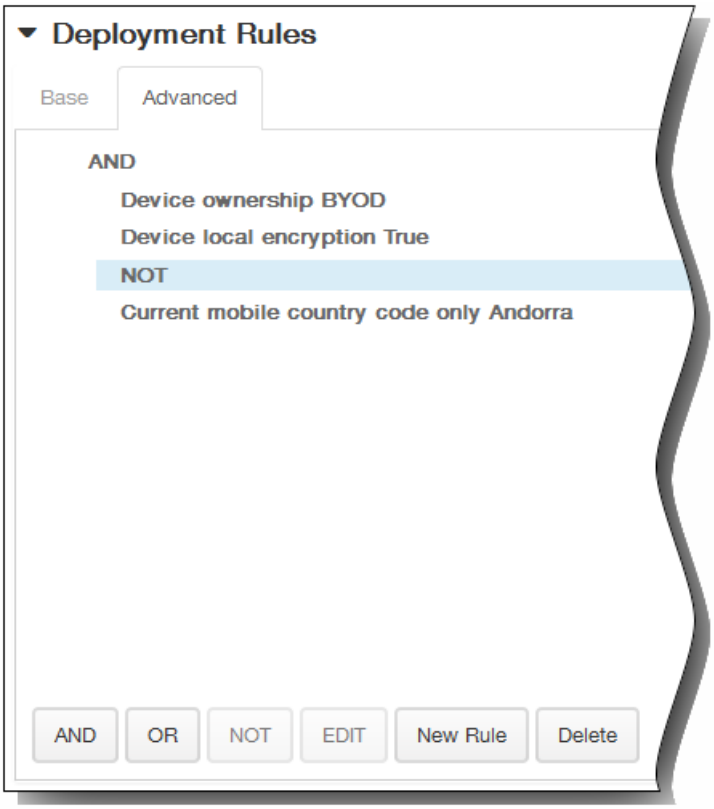


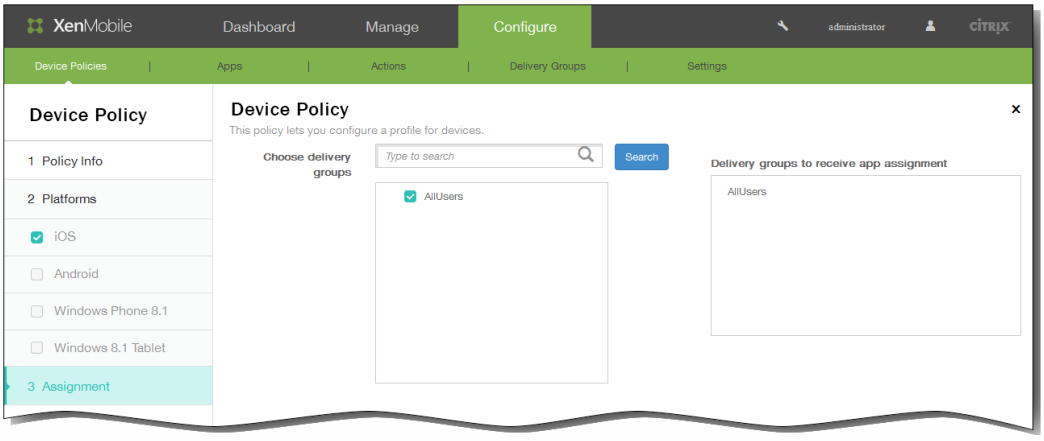


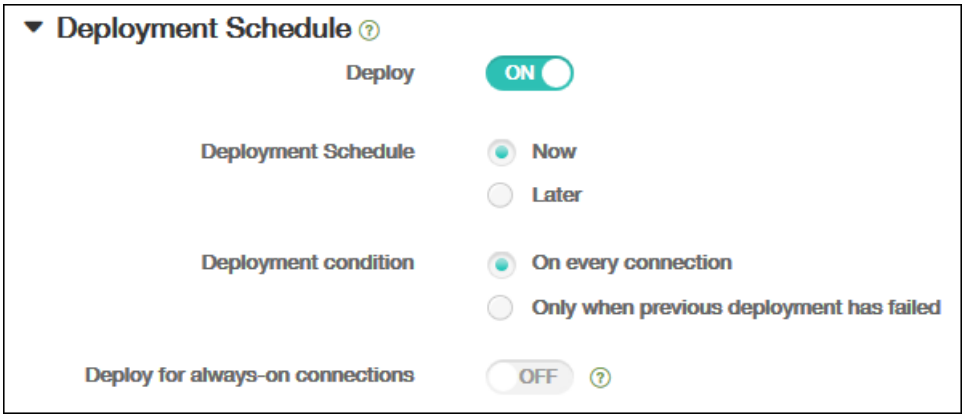




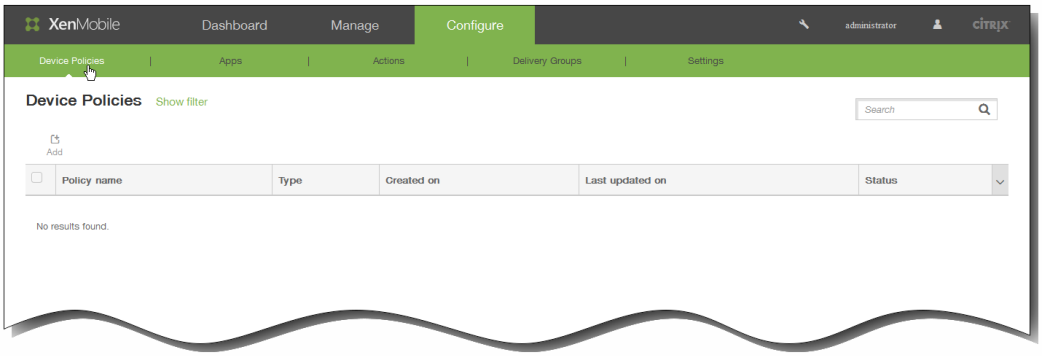


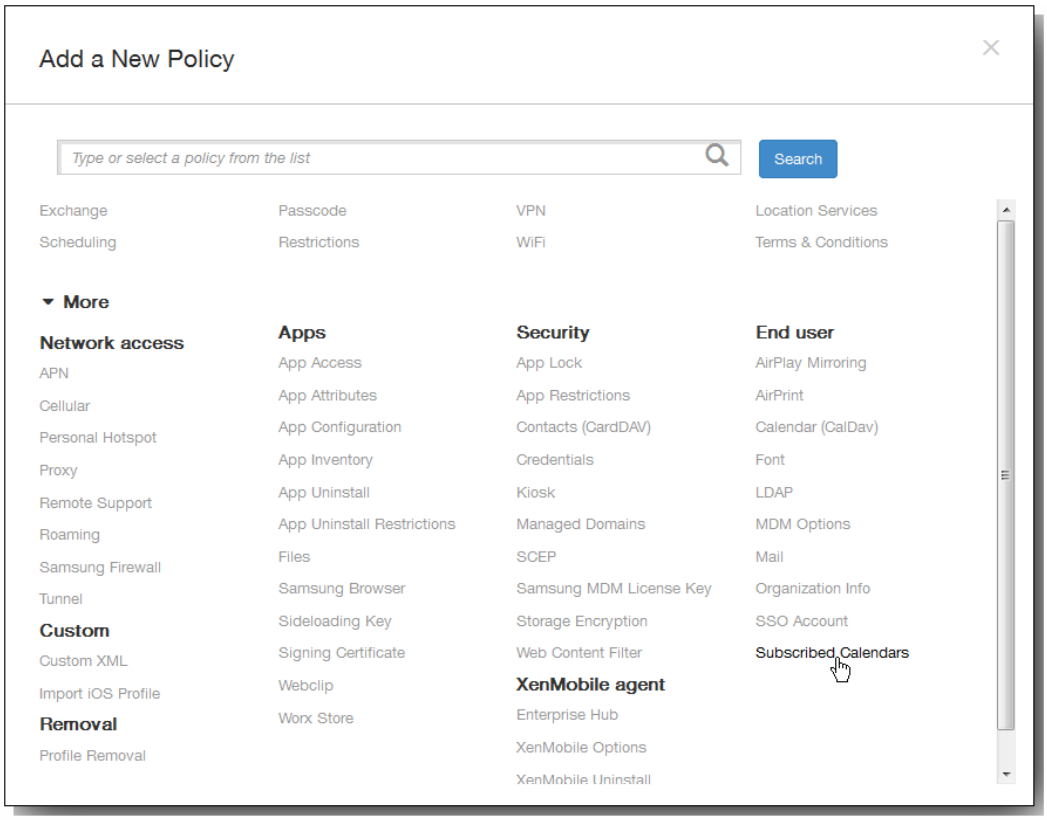


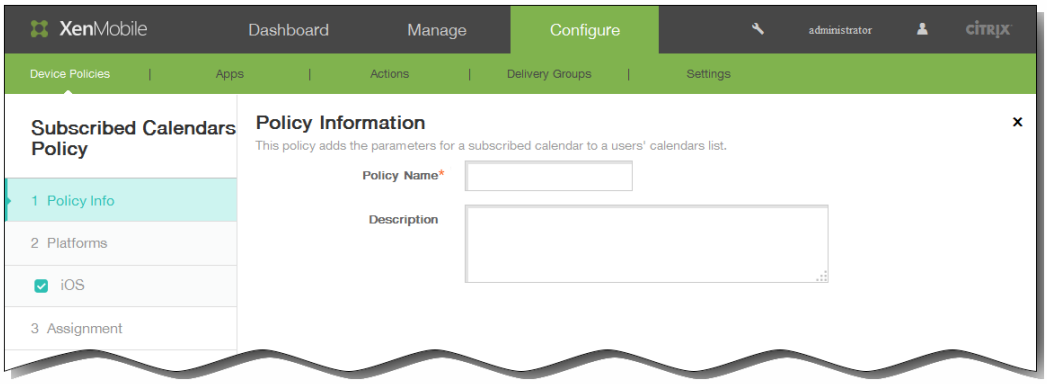


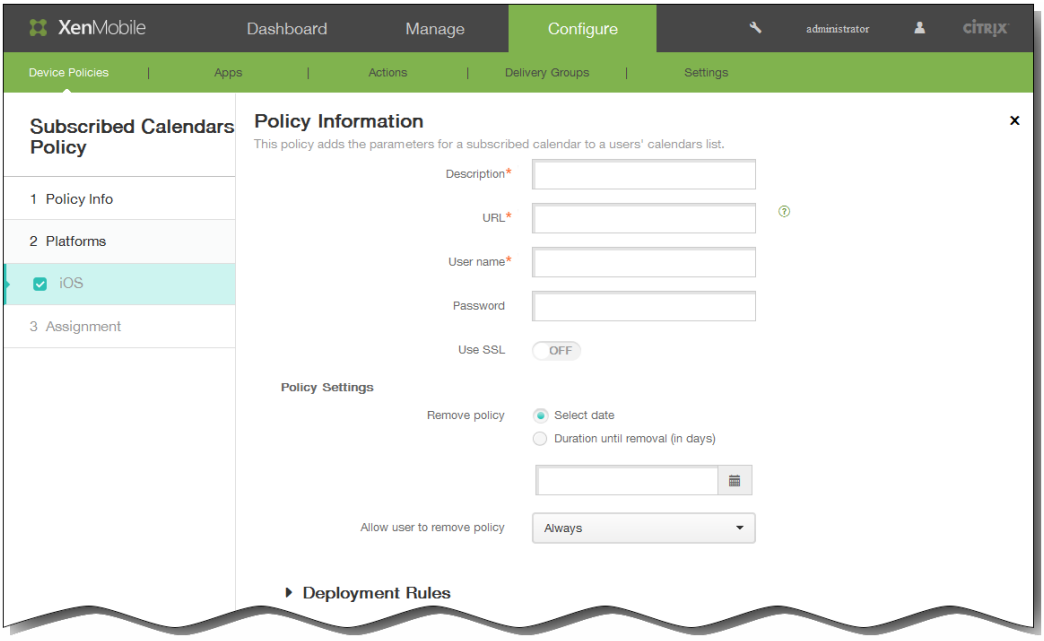


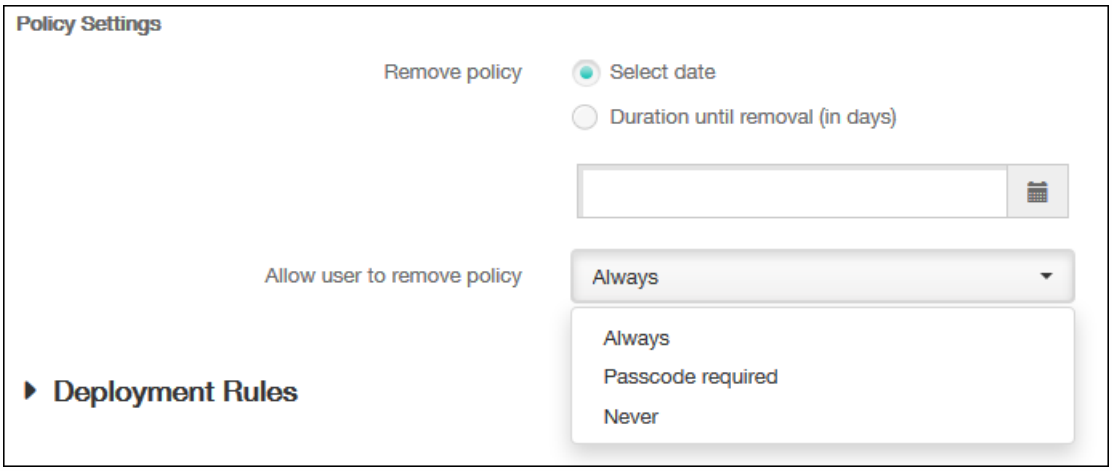
So fügen Sie eine Richtlinie für abonnierte Kalender für iOS-Geräte hinzu

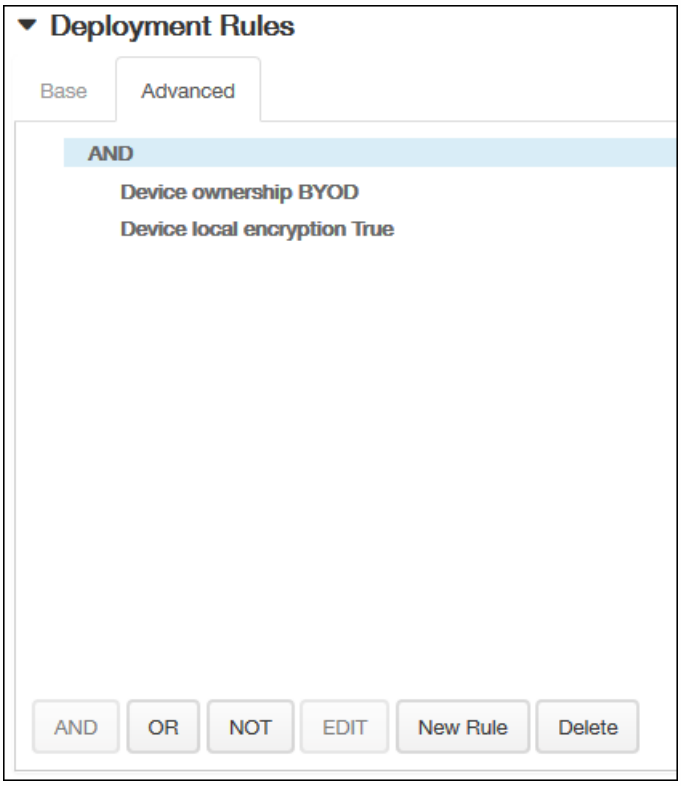


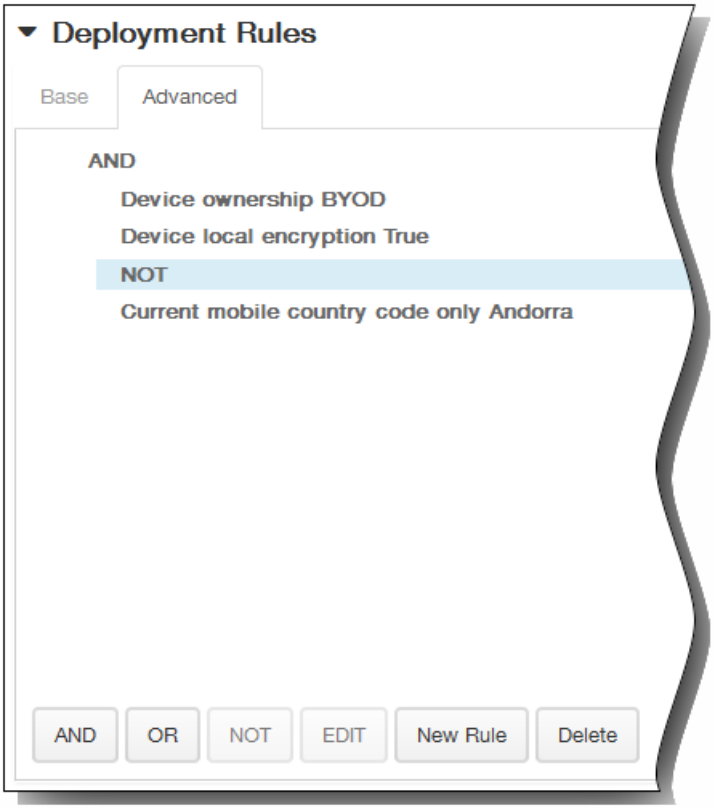


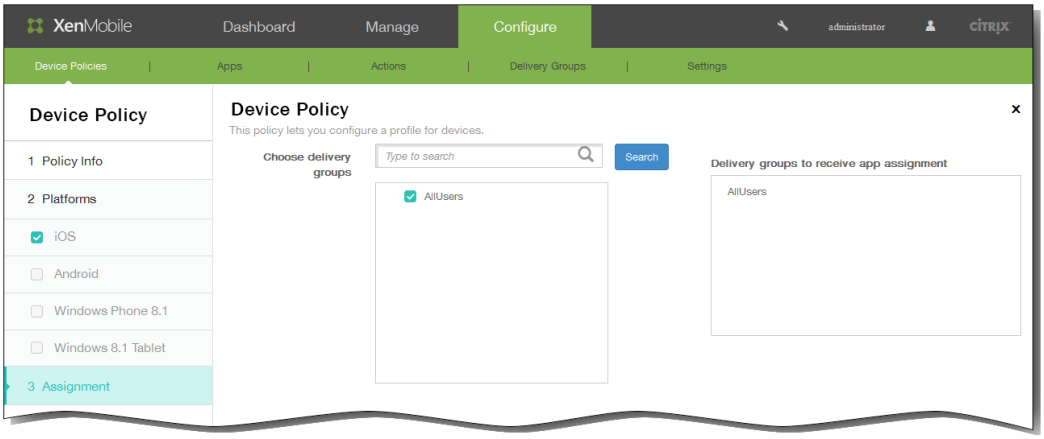


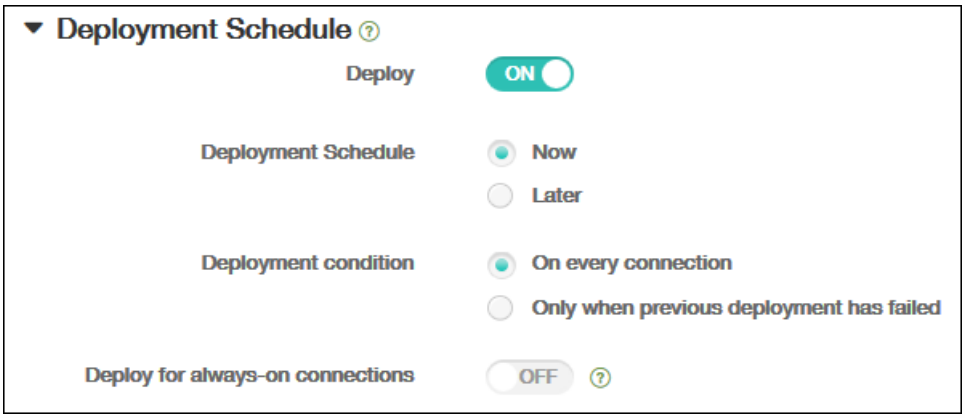










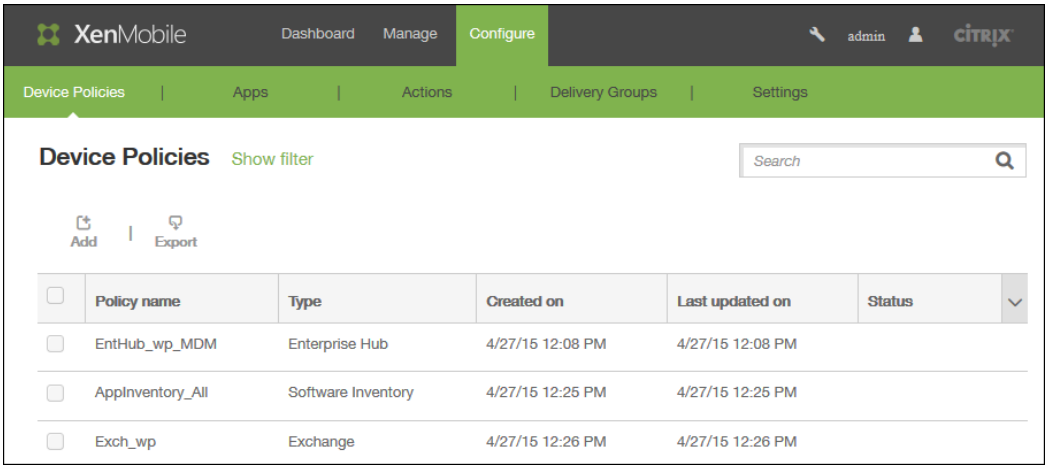


Passcoderichtlinien für Geräte

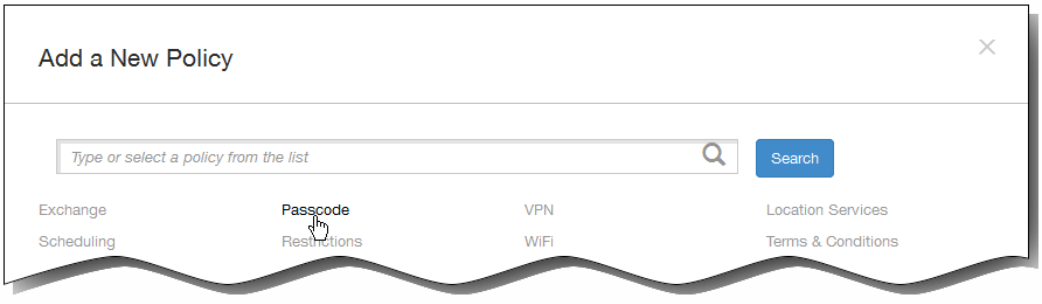
Jul 27, 2016

Sie erstellen Passcoderichtlinien in XenMobile gemäß den Standards Ihres Unternehmens. Sie können festlegen, dass Passcodes auf den Geräten der Benutzer eingegeben werden müssen, und verschiedene Formate und Passcoderegeln vorgeben. Solche Richtlinien können für iOS-, Android-, Android for Work-, Samsung KNOX-, Windows Phone 8.1-Geräte und Windows 8.1-Tablets erstellt werden. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Abschnitt beschrieben.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Geräterichtlinien wird angezeigt. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen.



2. Klicken Sie auf der Seite Add New Policy auf Passcode.



3. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Richtlinienname: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Beschreibung: Geben Sie optional eine Beschreibung der Richtlinie ein.
   3. Klicken Sie auf Next.
4. Wählen Sie unter Platforms die Plattformen aus, für die Sie diese Richtlinie konfigurieren möchten.
   Hinweis: Auf der Seite Policy Platforms sind alle Plattformen ausgewählt, der Konfigurationsbereich für die iOS-Plattform

wird als erstes angezeigt.

- Bei Auswahl von iOS konfigurieren Sie die folgenden Einstellungen:

  Passcode erforderlich: Wählen Sie diese Option aus, damit ein Passcode erforderlich ist, und um die Konfigurationsoptionen für die iOS-Passcoderichtlinie anzuzeigen. Die Seite wird erweitert, damit Sie die Einstellungen für Passcodeanforderungen, Passcodesicherheit und Richtlinieneinstellungen konfigurieren können.

  Passcodeanforderungen

  Mindestlänge: Klicken Sie in der Liste auf die Mindestlänge für den Passcode. Der Standardwert ist 6.

  Einfache Passcodes zulassen: Wählen Sie aus, ob einfache Passcodes zugelassen werden sollen. Einfache Passcodes sind Zeichenfolgen mit wiederholten oder sequenziellen Zeichen. Der Standardwert ist EIN.

  Erforderliche Zeichen: Wählen Sie aus, ob Passcodes mindestens einen Buchstaben enthalten sollen. Der Standardwert ist AUS.

  Mindestanzahl von Symbolen: Klicken Sie in der Liste auf die Anzahl Symbole, die ein Passcode enthalten muss.

  Passcodesicherheit

  Kulanzzeitraum für Gerätesperre (Minuten Inaktivität): Klicken Sie in der Liste auf die Zeitdauer, innerhalb derer die Benutzer einen Passcode zum Entsperren eines gesperrten Geräts eingeben müssen. Der Standardwert ist Ohne.

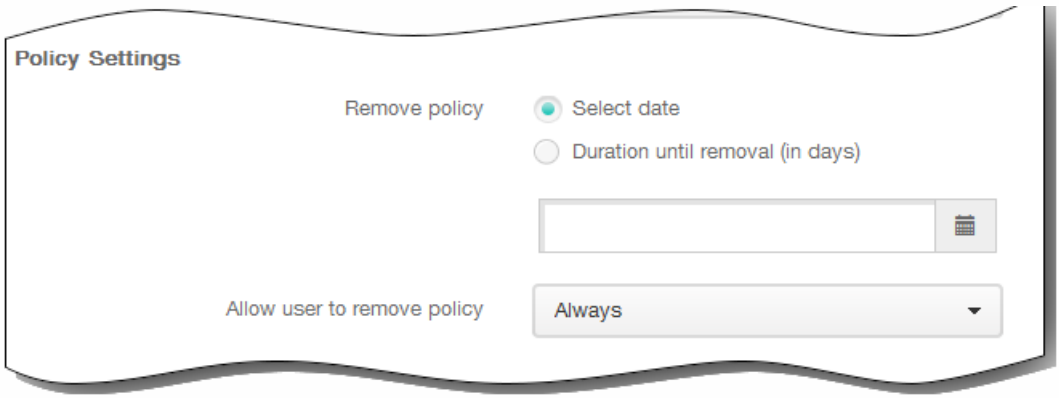
  Gerät sperren nach (Minuten Inaktivität): Klicken Sie in der Liste auf den Zeitraum, den ein Gerät inaktiv sein darf, bevor es gesperrt wird. Der Standardwert ist Ohne.

  Passcode expiration in days (1-730): Geben Sie die Anzahl der Tage ein, nach denen der Passcode abläuft. Gültige Werte sind 1-730. Der Standardwert ist 0, was bedeutet, dass der Passcode nie abläuft.

  Previous passwords saved (0-50): Geben Sie an, wie viele verwendete Kennwörter gespeichert werden sollen. Die Benutzer können kein gespeichertes Kennwort wiederverwenden. Gültige Werte sind 0-50. Der Standardwert ist 0, was bedeutet, dass Benutzer Kennwörter wiederverwenden können.

  Maximale Anzahl der Anmeldeversuchsfehler: Klicken Sie in der Liste auf die Anzahl fehlgeschlagener Anmeldeversuche, nach denen die Daten auf dem betroffenen Gerät vollständig gelöscht werden. Die Standardeinstellung ist Nicht definiert.

  Richtlinieneinstellungen



1. Klicken Sie unter Richtlinieneinstellungen für Richtlinie entfernen auf Datum auswählen oder Zeit bis zum Entfernen (in Tagen).
2. Bei Auswahl von Datum auswählen klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
3. Klicken Sie in der Liste Benutzer darf Richtlinie entfernen auf Immer, Passcode erforderlich oder Nie.
4. Bei Auswahl von Passcorde erforderlich geben Sie für Passcode zum Entfernen den Passcode ein.

- Bei Auswahl von Android konfigurieren Sie die folgenden Einstellungen:

  Hinweis: Die Standardeinstellung für Android ist OFF. Die Seite wird erweitert, damit Sie die Einstellungen für Passcodeanforderungen, Passcodesicherheit, Passcodeverschlüsselung und Samsung SAFE konfigurieren können.
  Passcodeanforderungen

  Mindestlänge: Klicken Sie in der Liste auf die Mindestlänge für den Passcode. Der Standardwert ist 6.

  Biometrische Erkennung: Wählen Sie aus, ob die Biometrieerkennung aktiviert werden soll. Wenn Sie diese Option aktivieren, wird das Feld Required characters ausgeblendet. Der Standardwert ist AUS.

  Required characters: Klicken Sie in der Liste auf No Restriction, Both numbers and letters, Numbers only oder Letters only, um die Zusammensetzung des Passcodes vorzugeben. Der Standardwert ist No restriction.

  Erweiterte Regeln: Wählen Sie aus, ob erweiterte Passcoderegeln angewendet werden sollen. Diese Option ist für Android 3.0 und höher verfügbar. Der Standardwert ist AUS.

  Wenn Sie Advanced rules auf ON festlegen, wählen Sie aus den folgenden Listen die Mindestzahl der Zeichen des jeweiligen Typs aus, die der Passcode enthalten muss:
  - Symbole: Mindestanzahl der Symbole.
  - Buchstaben: Mindestanzahl der Buchstaben.
  - Kleinbuchstaben: Mindestanzahl der Kleinbuchstaben.
  - Großbuchstaben: Mindestanzahl der Großbuchstaben.
  - Ziffern oder Symbole: Mindestanzahl der Ziffern oder Symbole.
  - Ziffern: Mindestanzahl der Ziffern.

  Passcodesicherheit

  Gerät sperren nach (Minuten Inaktivität): Klicken Sie in der Liste auf den Zeitraum, den ein Gerät inaktiv sein darf, bevor es gesperrt wird. Der Standardwert ist Ohne.

  Passcode expiration in days (1-730): Geben Sie die Anzahl der Tage ein, nach denen der Passcode abläuft. Gültige Werte sind 1-730. Der Standardwert ist 0, was bedeutet, dass der Passcode nie abläuft.

  Previous passwords saved (0-50): Geben Sie an, wie viele verwendete Kennwörter gespeichert werden sollen. Die Benutzer können kein gespeichertes Kennwort wiederverwenden. Gültige Werte sind 0-50. Der Standardwert ist 0, was bedeutet, dass Benutzer Kennwörter wiederverwenden können.

  Maximale Anzahl der Anmeldeversuchsfehler: Klicken Sie in der Liste auf die Anzahl fehlgeschlagener Anmeldeversuche, nach denen die Daten auf dem betroffenen Gerät vollständig gelöscht werden. Die Standardeinstellung ist Nicht definiert.

Verschlüsselung

Verschlüsselung aktivieren: Wählen Sie aus, ob die Verschlüsselung aktiviert werden soll. Diese Option ist für Android 3.0 und höher verfügbar. Diese Option ist unabhängig von der Einstellung für Passcode erforderlich verfügbar.

Use same passcode across all users: Wählen Sie aus, ob der gleiche Passcode für alle Benutzer verwendet werden soll. Diese Option gilt nur für Samsung SAFE-Geräte und ist unabhängig von der Einstellung für Passcode required verfügbar. Der Standardwert ist AUS.

Geben Sie den gewünschten Passcode in das Feld ein, das angezeigt wird, wenn Sie diese Option aktivieren.

- Bei Auswahl von Samsung KNOX konfigurieren Sie die folgenden Einstellungen:

  Passcodeanforderungen

  Mindestlänge: Klicken Sie in der Liste auf die Mindestlänge für den Passcode.

  Allow users to make password visible: Wählen Sie aus, ob Benutzern das Anzeigen des Kennworts ermöglicht werden soll.

- Verbotene Zeichenfolgen: Durch das Konfigurieren verbotener Zeichenfolgen verhindern Sie, dass Benutzer unsichere, einfach zu erratende Zeichenfolgen ("Kennwort", "Willkommen", "123456", "111111" usw.) verwenden können. Führen Sie einen der folgenden Schritte aus:
  - **So fügen Sie eine verbotene Zeichenfolge hinzu**
    1. Klicken Sie auf Add.
    2. Geben Sie die verbotene Zeichenfolge ein.
    3. Klicken Sie auf Save, um die Zeichenfolge hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
    4. Wiederholen Sie die Schritte i bis iii für jede verbotene Zeichenfolge, die Sie hinzufügen möchten.
  - **So bearbeiten Sie eine verbotene Zeichenfolge**
    1. Previous passwords saved (0-50): Geben Sie an, wie viele verwendete Kennwörter gespeichert werden sollen. Die Benutzer können kein gespeichertes Kennwort wiederverwenden. Gültige Werte sind 0-50. Der Standardwert ist 0, was bedeutet, dass Benutzer Kennwörter wiederverwenden können.
    1. Zeigen Sie auf die Zeichenfolge, die Sie bearbeiten möchten.
    2. Klicken Sie auf das Stiftsymbol rechts neben dem Eintrag.
    3. Nehmen Sie die Änderungen an der Zeichenfolge vor.
    4. Klicken Sie auf Save, um die Zeichenfolge zu speichern, oder auf Cancel, um den Vorgang abzubrechen.

  Mindestanzahl

  Changed characters: Geben Sie die Anzahl der Zeichen ein, die Benutzer an ihrem vorherigen Passcode ändern müssen. Der Standardwert ist 0.

  Symbols: Geben Sie die erforderliche Mindestzahl der Symbole in einem Passcode vor. Der Standardwert ist 0.

  Maximale Anzahl

  Number of times a character can occur: Geben Sie an, wie oft ein Zeichen in einem Passcode höchstens vorkommen darf. Der Standardwert ist 0.

  Alphabetic sequence length: Geben Sie die maximal zulässige Länge einer Reihe alphabetisch geordneter Zeichen in einem Passcode an. Der Standardwert ist 0.

Numeric sequence length: Geben Sie die maximal zulässige Länge einer Reihe numerisch geordneter Zeichen in einem Passcode an. Der Standardwert ist 0.

Passcodesicherheit

Gerät sperren nach (Minuten Inaktivität): Klicken Sie in der Liste auf den Zeitraum, den ein Gerät inaktiv sein darf, bevor es gesperrt wird. Der Standardwert ist Ohne.
Hinweis: Obwohl in der Feldbezeichnung "minutes of inactivity" steht, wird in XenMobile die Sperre nach dem festgelegten Wert in *Sekunden* aktiviert.
Passcode expiration in days (1-730): Geben Sie die Anzahl der Tage ein, nach denen der Passcode abläuft. Gültige Werte sind 1-730. Der Standardwert ist 0, was bedeutet, dass der Passcode nie abläuft.

Previous passwords saved (0-50): Geben Sie an, wie viele verwendete Kennwörter gespeichert werden sollen. Die Benutzer können kein gespeichertes Kennwort wiederverwenden. Gültige Werte sind 0-50. Der Standardwert ist 0, was bedeutet, dass Benutzer Kennwörter wiederverwenden können.

Maximale Anzahl der Anmeldeversuchsfehler: Klicken Sie in der Liste auf die Anzahl fehlgeschlagener Anmeldeversuche, nach der ein Gerät gesperrt wird. Die Standardeinstellung ist Nicht definiert.

- Bei Auswahl von Windows Phone 8.1 konfigurieren Sie die folgenden Einstellungen:

  Passcode required: Wählen Sie diese Option, wenn für Windows Phone 8.1-Geräte kein Passcode erforderlich sein soll. Die Standardeinstellung ist EIN, ein Passcode ist also erforderlich. Die Seite wird verkleinert und die nachfolgenden Optionen werden ausgeblendet. Wenn Sie das Passcodeerfordernis nicht deaktiviert haben, fahren Sie mit der Konfiguration der folgenden Einstellungen fort.

  Einfache Passcodes zulassen: Wählen Sie aus, ob einfache Passcodes zugelassen werden sollen. Einfache Passcodes sind Zeichenfolgen mit wiederholten oder sequenziellen Zeichen. Der Standardwert ist AUS.

  Passcodeanforderungen

  Mindestlänge: Klicken Sie in der Liste auf die Mindestlänge für den Passcode. Der Standardwert ist 6.

  Erforderliche Zeichen: Klicken Sie in der Liste auf Numerisch oder alphanumerisch, Nur Buchstaben oder Nur Ziffern, um die zulässige Zusammensetzung der Passcodes festzulegen. Der Standardwert ist Nur Buchstaben.

  Mindestanzahl von Symbolen: Klicken Sie in der Liste auf die Anzahl Symbole, die ein Passcode enthalten muss. Der Standardwert ist 1.

  Passcodesicherheit

  Gerät sperren nach (Minuten Inaktivität): Klicken Sie in der Liste auf den Zeitraum, den ein Gerät inaktiv sein darf, bevor es gesperrt wird. Der Standardwert ist 0.

  Passcode expiration in 0-730 days: Geben Sie die Anzahl der Tage ein, nach denen der Passcode abläuft. Gültige Werte sind 1-730. Der Standardwert ist 0, was bedeutet, dass der Passcode nie abläuft.

  Previous passwords saved (0-50): Geben Sie an, wie viele verwendete Kennwörter gespeichert werden sollen. Die Benutzer können kein gespeichertes Kennwort wiederverwenden. Gültige Werte sind 0-50. Der Standardwert ist 0, was bedeutet, dass Benutzer Kennwörter wiederverwenden können.

  Maximum failed sign-on attempts before wipe (0-999): Klicken Sie in der Liste auf die Anzahl fehlgeschlagener

Anmeldeversuche, nach der Unternehmensdaten vom Gerät gelöscht werden. Der Standardwert ist 0.

- Bei Auswahl von Windows 8.1 Tablet konfigurieren Sie die folgenden Einstellungen:

  Komfortanmeldung nicht zulassen: Wählen Sie aus, ob Benutzern der Zugriff auf ihre Geräte über Bildkennwörter oder Biometrieanmeldungen gestattet werden soll. Der Standardwert ist AUS.

  Minimum passcode length: Klicken Sie in der Liste auf die Mindestlänge für den Passcode. Der Standardwert ist 6.

  Maximum passcode attempts before wipe: Klicken Sie in der Liste auf die Anzahl fehlgeschlagener Anmeldeversuche, nach der ein Gerät gesperrt wird. Der Standardwert ist 4.

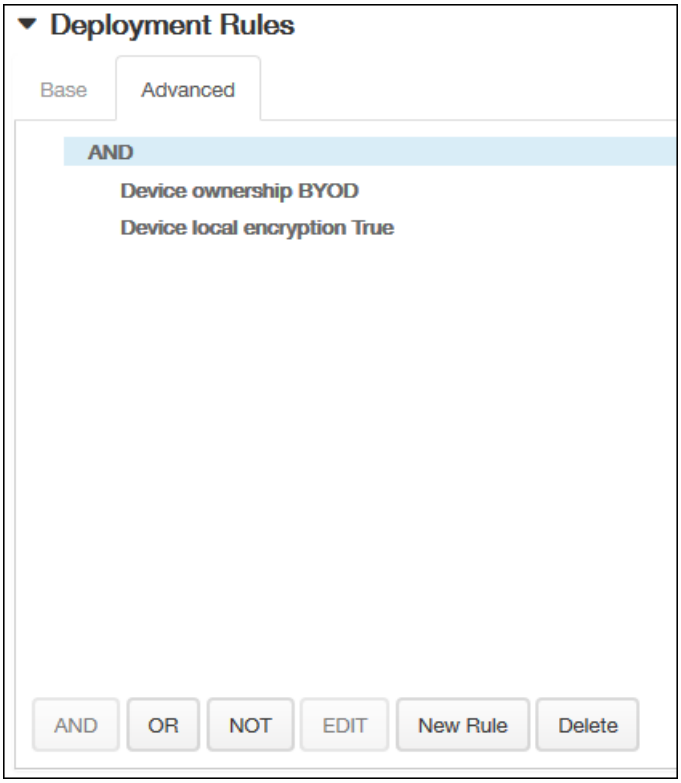
  Passcode expiration in days (0-999): Geben Sie die Anzahl der Tage ein, nach denen der Passcode abläuft. Gültige Werte sind 1-999. Der Standardwert ist 0, was bedeutet, dass der Passcode nie abläuft.

  Passcode history: (1-24): Geben Sie an, wie viele verwendete Passcodes gespeichert werden sollen. Die Benutzer können keinen gespeicherten Passcode wiederverwenden. Gültige Werte sind 1-24. Sie müssen eine Zahl zwischen 1 und 24 in diesem Feld eingeben.

  Maximum inactivity before device lock in minutes (1-1200): Geben Sie den Zeitraum in Minuten an, während dessen ein Gerät inaktiv sein darf, bevor es gesperrt wird. Gültige Werte sind 1-1200. Sie müssen eine Zahl zwischen 1 und 1200 in diesem Feld eingeben.

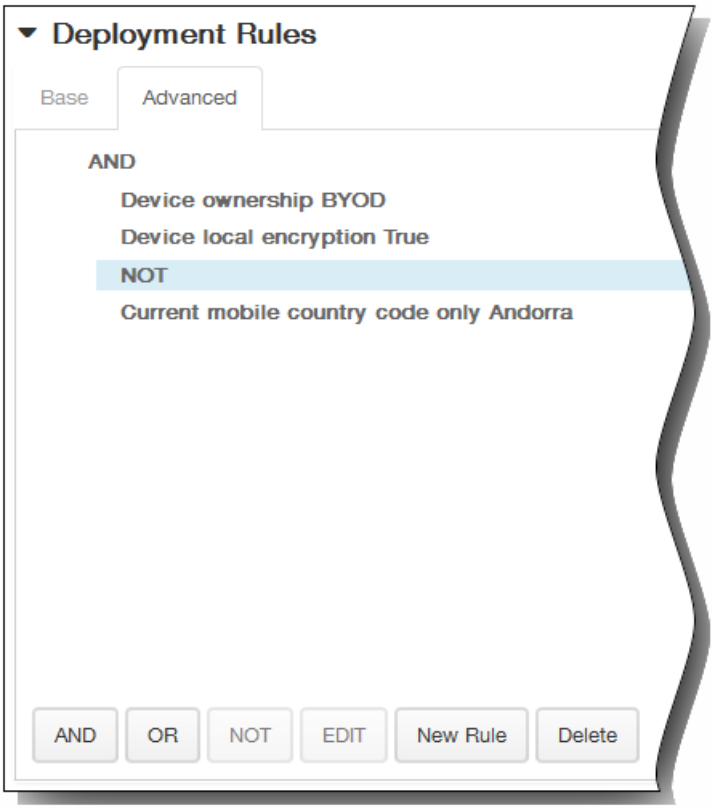
5. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist Alle.
   2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
   3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
   4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.

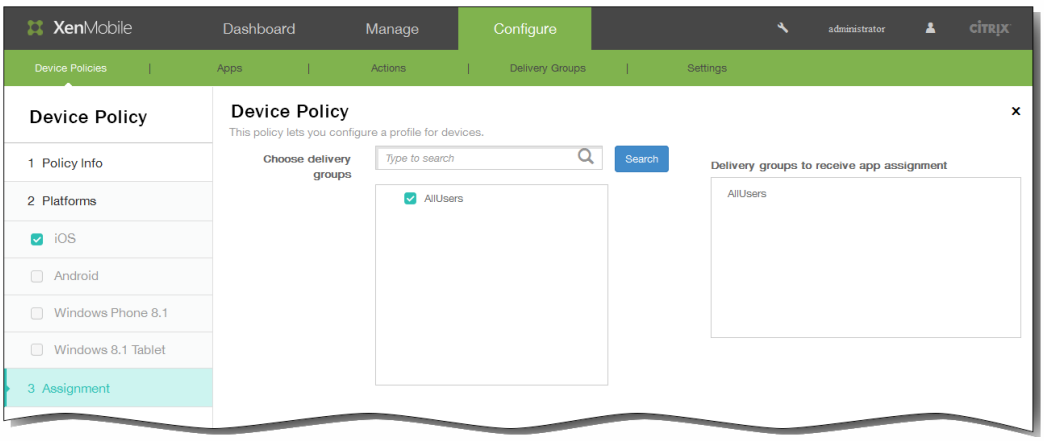


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.
   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Gerätebesitz" "BYOD", für "Lokale Verschlüsselung des Geräts" und "Passcode richtlinientreu" "Wahr" eingestellt und "Aktueller Ländercode für mobiles Gerät" auf Andorra eingeschränkt.



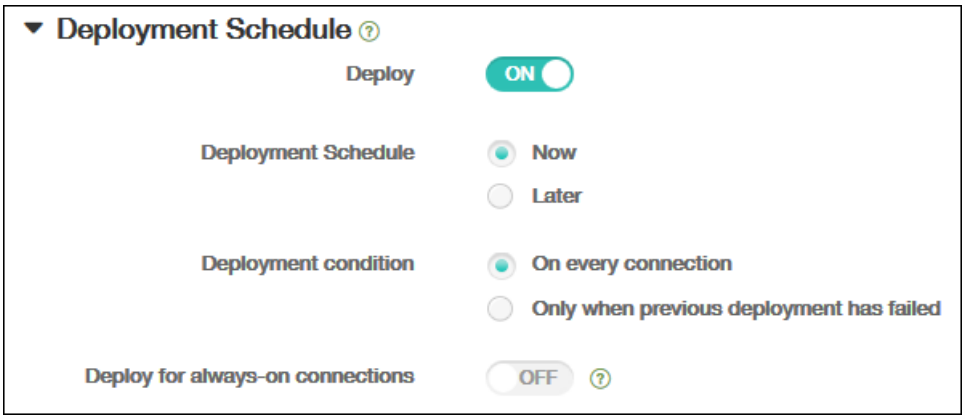
6. Klicken Sie auf Next. Die Seite Assignment für die Passcoderichtlinie wird angezeigt.
7. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



8. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
   1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
   2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.

3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



9. Klicken Sie auf Save.

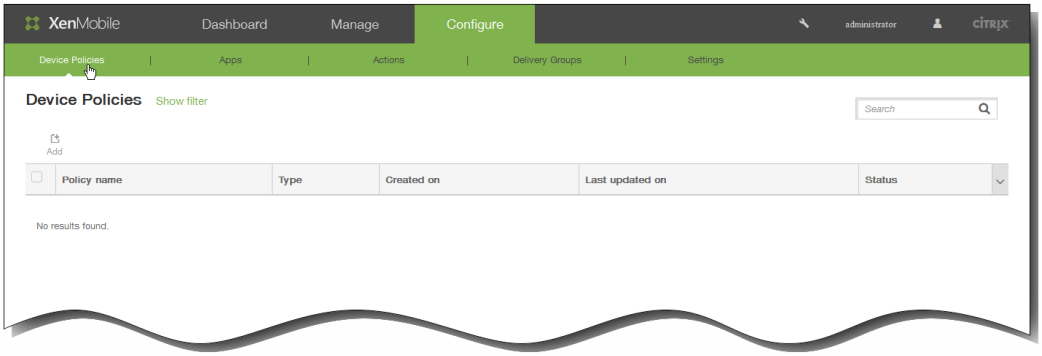
So fügen Sie eine Proxyrichtlinie für iOS-Geräte hinzu

Nov 12, 2015

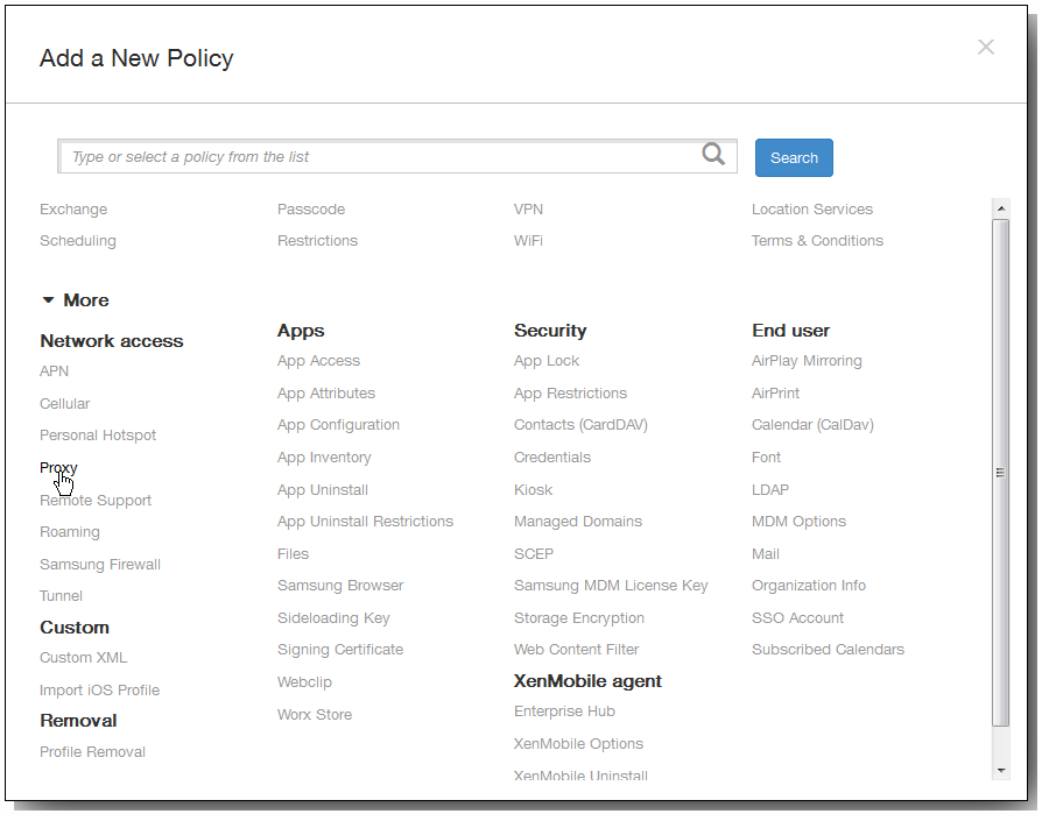
Sie können in XenMobile eine Richtlinie zum Festlegen globaler HTTP-Proxy-Einstellungen für Geräte mit iOS 6.0 oder höher hinzufügen. Sie können nur eine globale HTTP-Proxyrichtlinie pro Gerät bereitstellen.

Hinweis: Versetzen Sie vor dem Bereitstellen dieser Richtlinie alle iOS-Geräte, für die Sie eine globale HTTP-Proxyrichtlinie festlegen möchten, in den betreuten Modus. Details finden Sie unter So versetzen Sie ein iOS-Gerät mit dem Apple Configurator in den betreuten Modus.

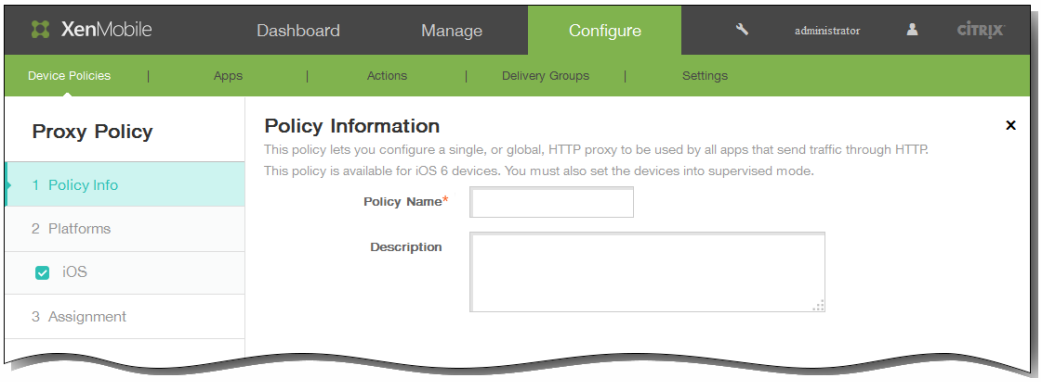
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



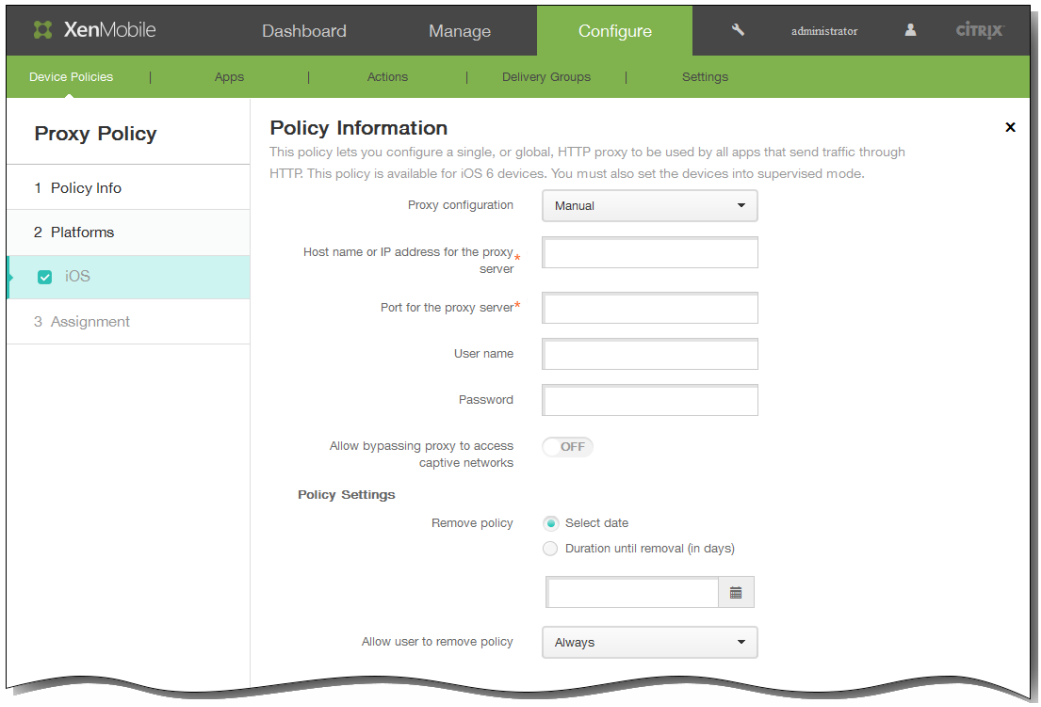
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter Network access auf Proxy. Die Seite Proxy Policy wird angezeigt.



4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite iOS Platform Information wird angezeigt.



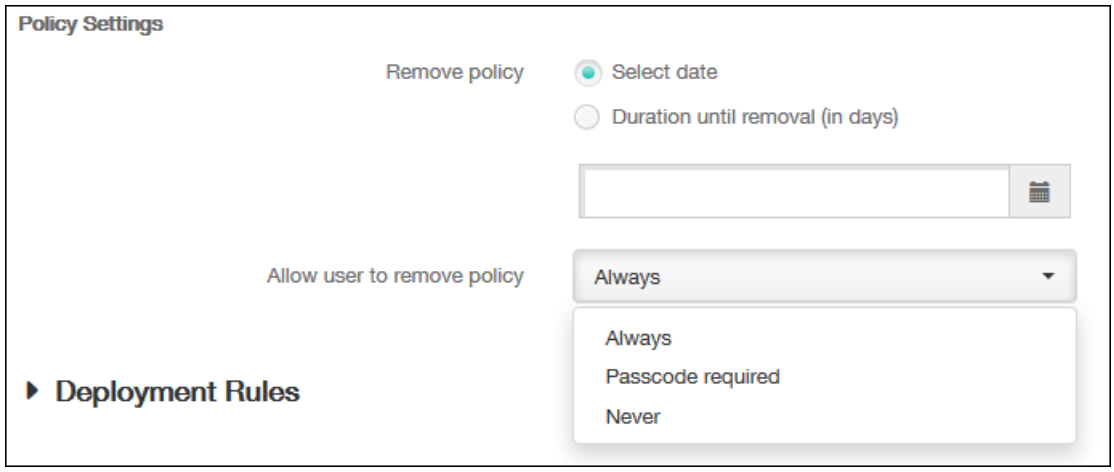
6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:
   1. Proxy configuration: Klicken Sie auf Manual oder Automatic, um festzulegen, wie der Proxy auf den Geräten der Benutzer konfiguriert wird. In der folgenden Tabelle werden die Optionen für jede Proxykonfiguration aufgeführt. In jeder Zelle wird angegeben, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Manuell	Automatisch
Host name or IP address for the proxy server	Erforderlich	–

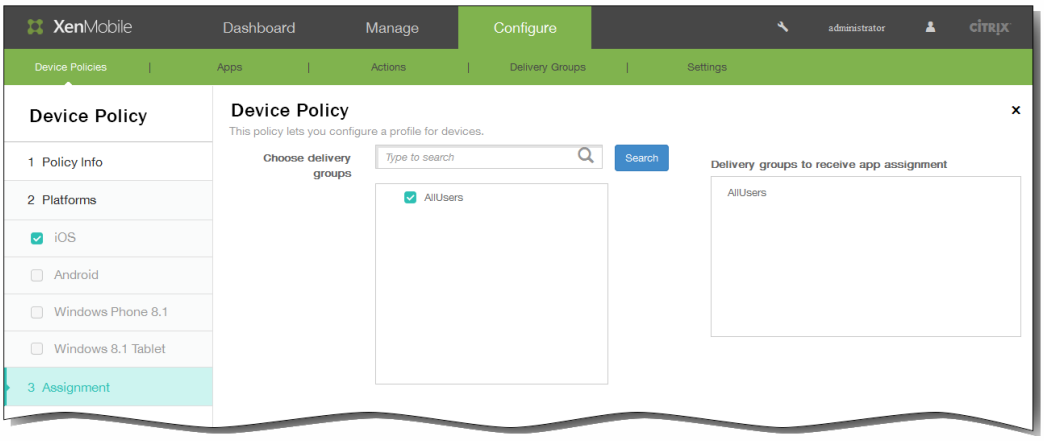
	Erforderlich	–
Port for the proxy server	Manuell	Automatisch
User name	Optional	–
Password	Optional	–
Proxy PAC URL	–	Optional
Allow direct connection if PAC is unreachable	–	OFF

2. Allow bypassing proxy to access captive networks: Wählen Sie aus, ob die Proxyumgehung für den Zugriff auf Captive-Netzwerke zulässig sein soll.

7. Klicken Sie unter Policy Settings für Remove policy auf Select date oder Duration until removal (in days).
8. Bei Auswahl von Select date klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
9. Klicken Sie in der Liste Allow user to remove policy auf Always, Password required oder Never.
10. Bei Auswahl von Password required geben Sie für Removal password das Kennwort ein.

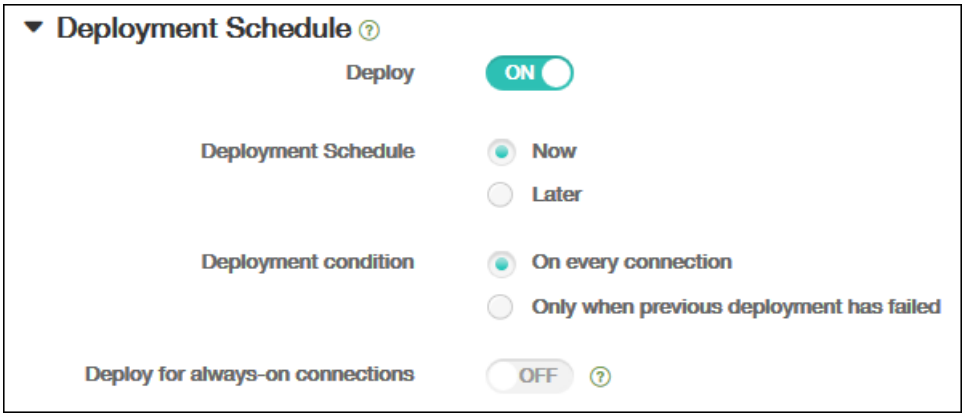


11. Klicken Sie auf Next. Die Seite Assignment für die Proxyrichtlinie wird angezeigt.
12. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



13. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
    4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
    5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
       Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

    Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



14. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Remotesupportrichtlinie für Samsung KNOX-Geräte hinzu

Nov 12, 2015

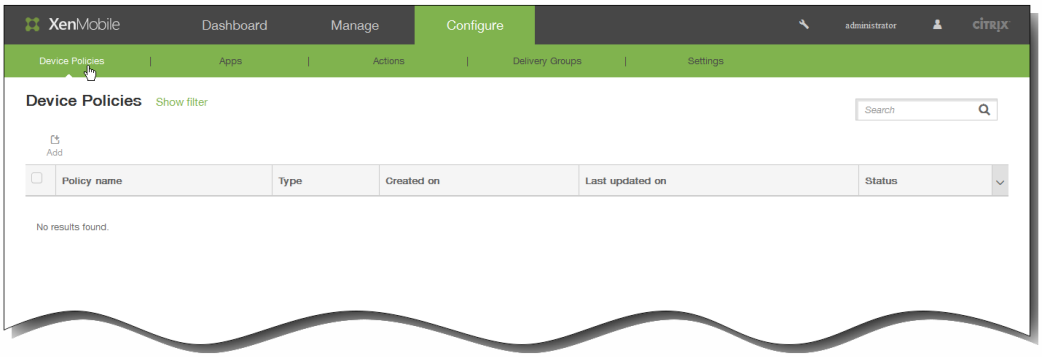
Sie erstellen eine Remotesupportrichtlinie in XenMobile, um Remotezugriff auf Samsung KNOX-Geräte zu erhalten. Sie können Support zweierlei Art konfigurieren:

- **Basic**: Der einfache Support ermöglicht das Anzeigen von Diagnoseinformationen zum Gerät, z. B. Systeminformationen, ausgeführte Prozesse, Task-Manager (Arbeitsspeicher und CPU-Nutzung), Inhalt des Ordners für installierte Software usw.
- **Premium**: Beim erweiterten Support können Sie den Gerätebildschirm remote steuern, einschließlich Steuerung der Farben (im Hauptfenster oder in einem separaten unverankerten Fenster), Einrichtung einer VoIP-Sitzung zwischen Helpdesk und Benutzer, Konfiguration von Einstellungen und Einrichten einer Chatsitzung zwischen Helpdesk und Benutzer.

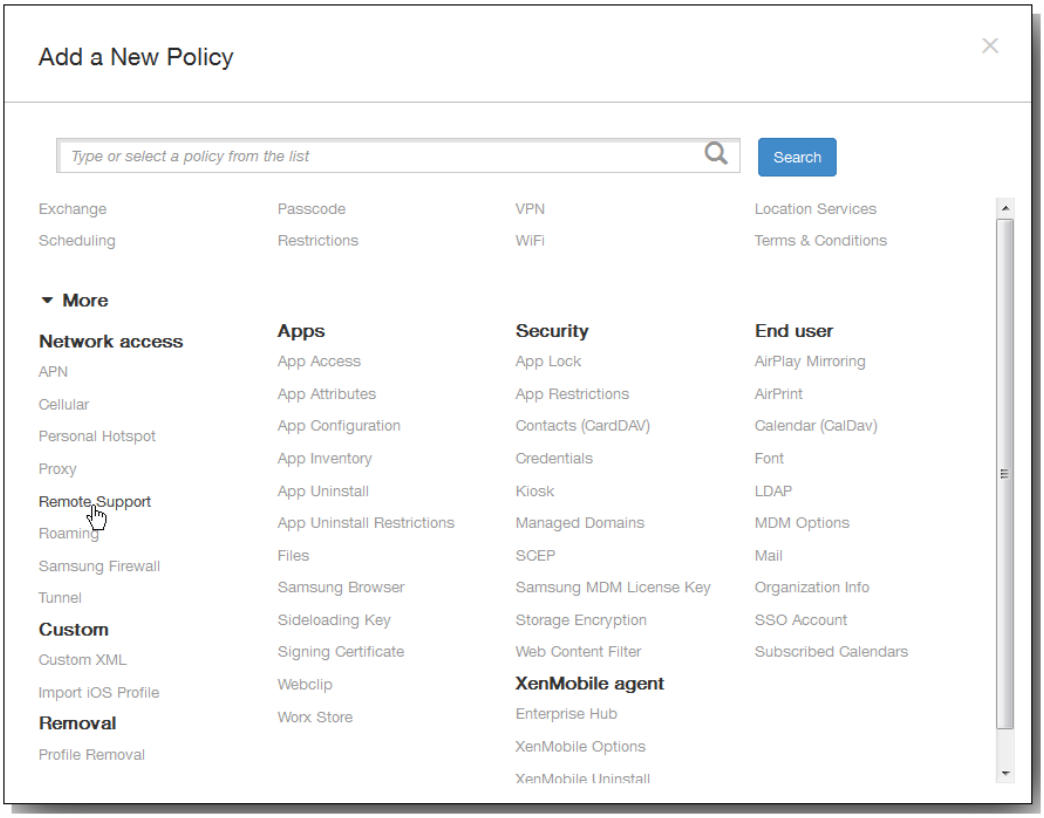
Hinweis: Zum Implementieren der Richtlinie müssen Sie die folgenden Schritte ausführen:

- Installieren der XenMobile Remote Support-App in der Umgebung
- Konfigurieren eines App-Tunnels für Remote Support; Einzelheiten finden Sie unter So fügen Sie eine App-Tunnelrichtlinie für Android-Geräte hinzu.
- Konfigurieren einer Samsung KNOX-Remotesupportrichtlinie gemäß der Anweisungen in diesem Abschnitt
- Bereitstellen des App-Tunnels und der Samsung KNOX-Remotesupportrichtlinie auf den Geräten der Benutzer

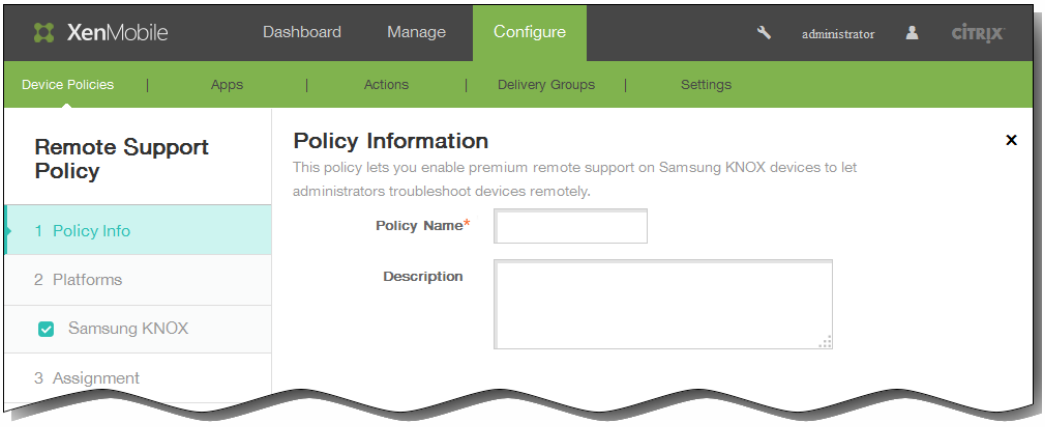
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



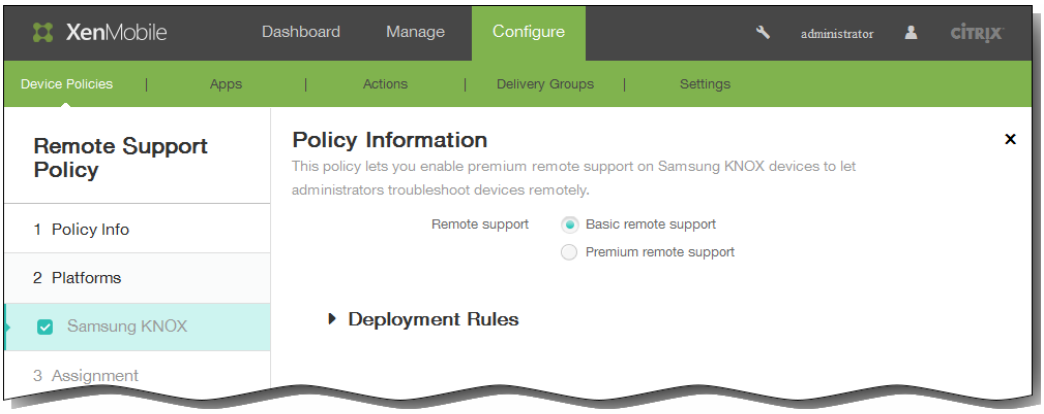
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



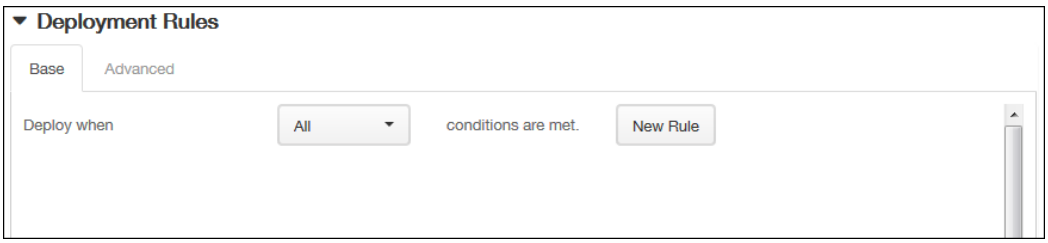
3. Klicken Sie auf More und dann unter Network access auf Remote Support. Die Seite Remote Support Policy wird angezeigt.



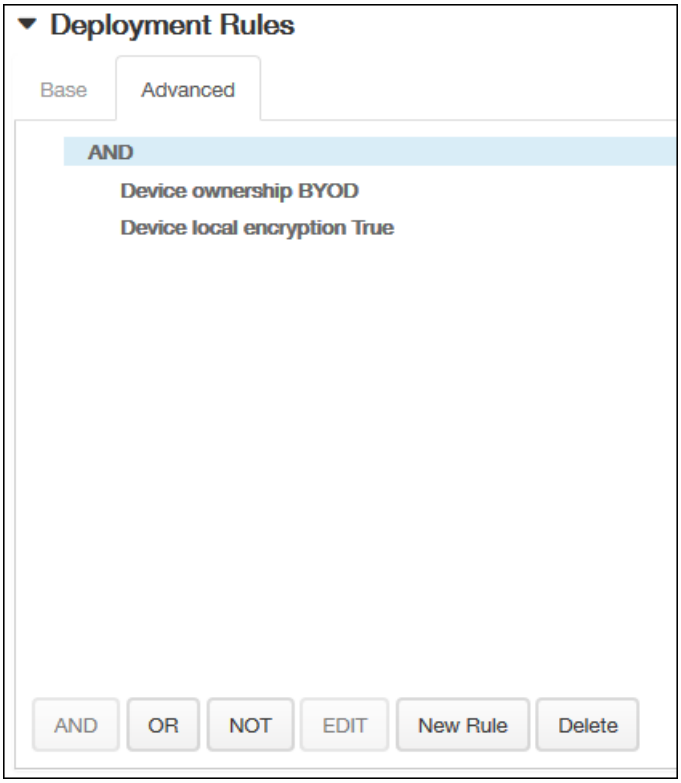
4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite mit Plattforminformationen für Samsung KNOX wird angezeigt.



6. Geben Sie auf der Seite Samsung KNOX die folgenden Informationen ein:
   1. Remote support: Wählen Sie Basic remote support oder Premium remote support aus. Die Standardeinstellung ist Basic remote support.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.



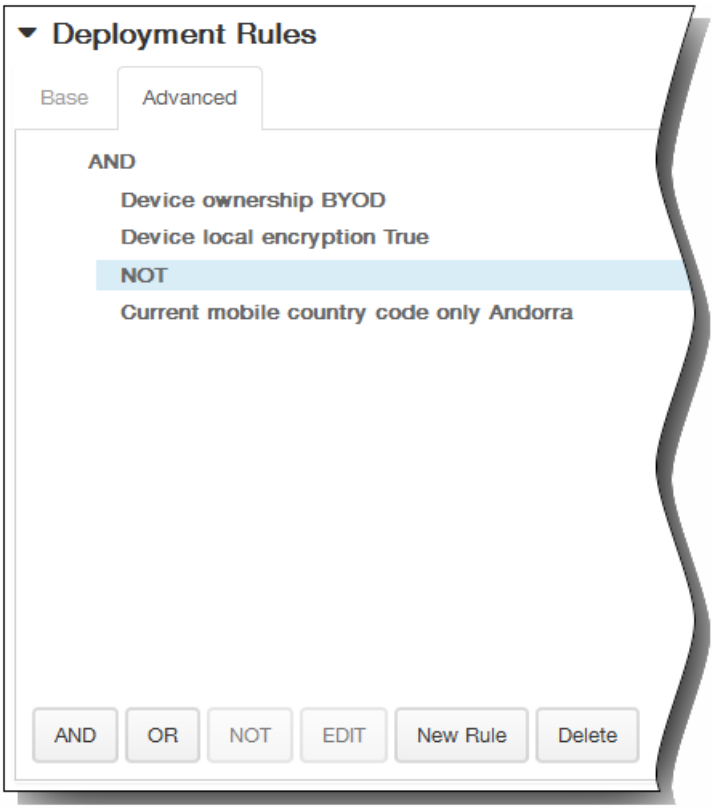
   1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
      1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
      2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
      3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
      4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
   2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



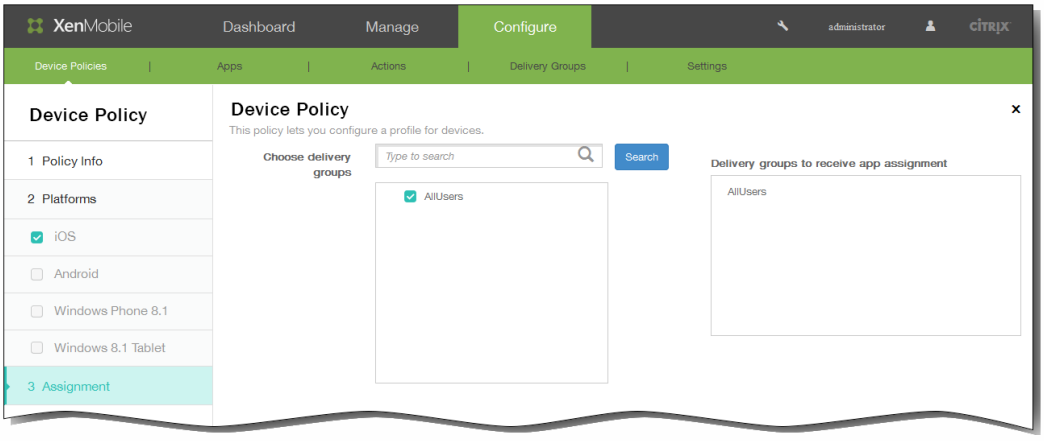
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



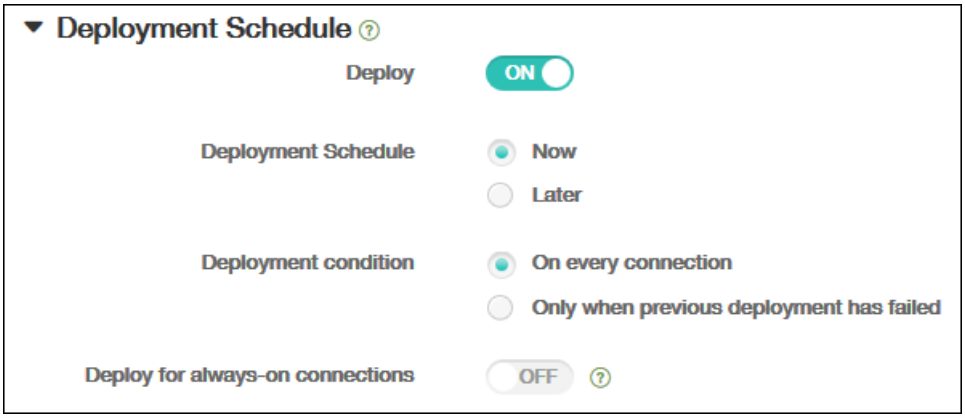
8. Klicken Sie auf Next. Die Seite Assignment für die Remotesupportrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



11. Klicken Sie auf Save, um die Richtlinie zu speichern.

Einschränkungsrichtlinien für Geräte

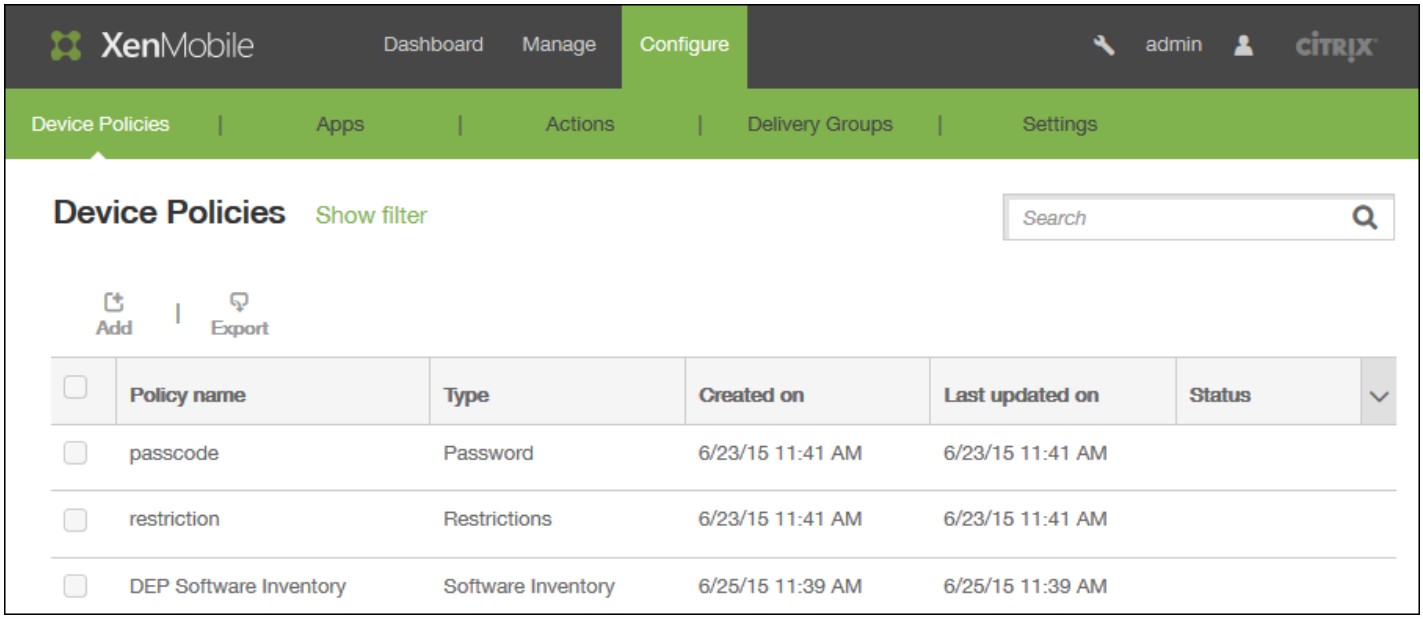
Jul 27, 2016

Sie können eine Geräterichtlinie in XenMobile hinzufügen, um Features und Funktionalität auf den Geräten der Benutzer einzuschränken. Einschränkungsrichtlinien können für folgende Plattformen konfiguriert werden: iOS, Samsung SAFE, Samsung KNOX, Windows 8.1-Tablet, Windows Phone 8.1 und Amazon. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Abschnitt beschrieben.

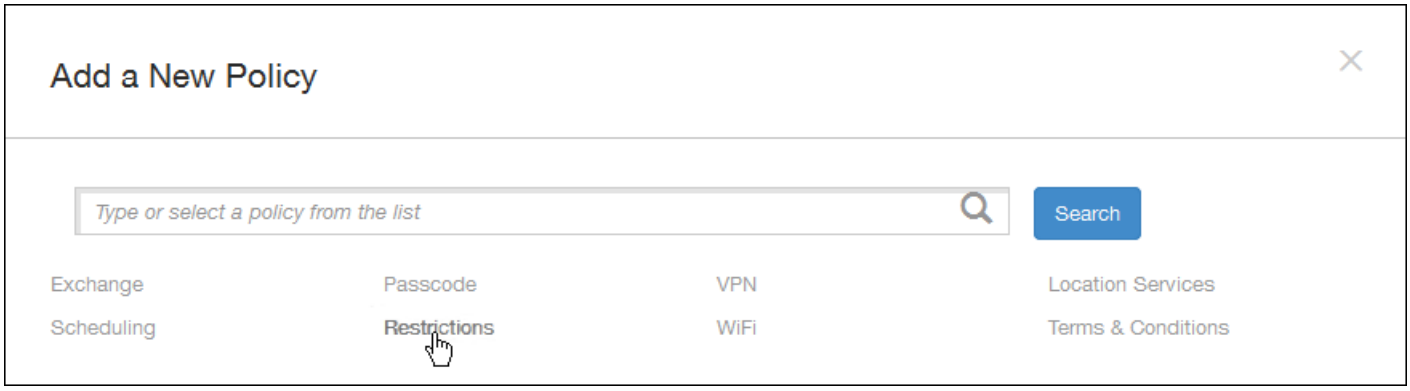
Diese Geräterichtlinie ermöglicht oder verhindert, dass Benutzer auf bestimmte Features auf Geräten, z. B. die Kamera, zugreifen. Sie können außerdem Einschränkungen für Sicherheit und Medieninhalte festlegen und vorgeben, welche App-Typen Benutzer installieren können. Die meisten Einschränkungen sind standardmäßig auf **ON** bzw. *zugelassen* festgelegt. Die wichtigsten Ausnahmen bilden das Feature "iOS- Security - Force" sowie alle Windows 8.1-Tablet-Features, die standardmäßig auf **OFF** bzw. *beschränkt* festgelegt sind.
Tipp: Alle Optionen, die Sie auf **ON** festlegen, bewirken, dass die Benutzer den entsprechenden Vorgang ausführen oder das Feature verwenden
— können
. Beispiel:

- **Camera**: Bei Auswahl von **ON** können Benutzer die Kamera auf Geräten verwenden. Bei Auswahl von **OFF** können Benutzer die Kamera auf Samsung SAFE-Geräten nicht verwenden.
- **Screen shots**: Bei Auswahl von **ON** können Benutzer Screenshots auf den Geräten erstellen. Bei Auswahl von **OFF** können Benutzer keine Screenshots auf den Geräten erstellen.

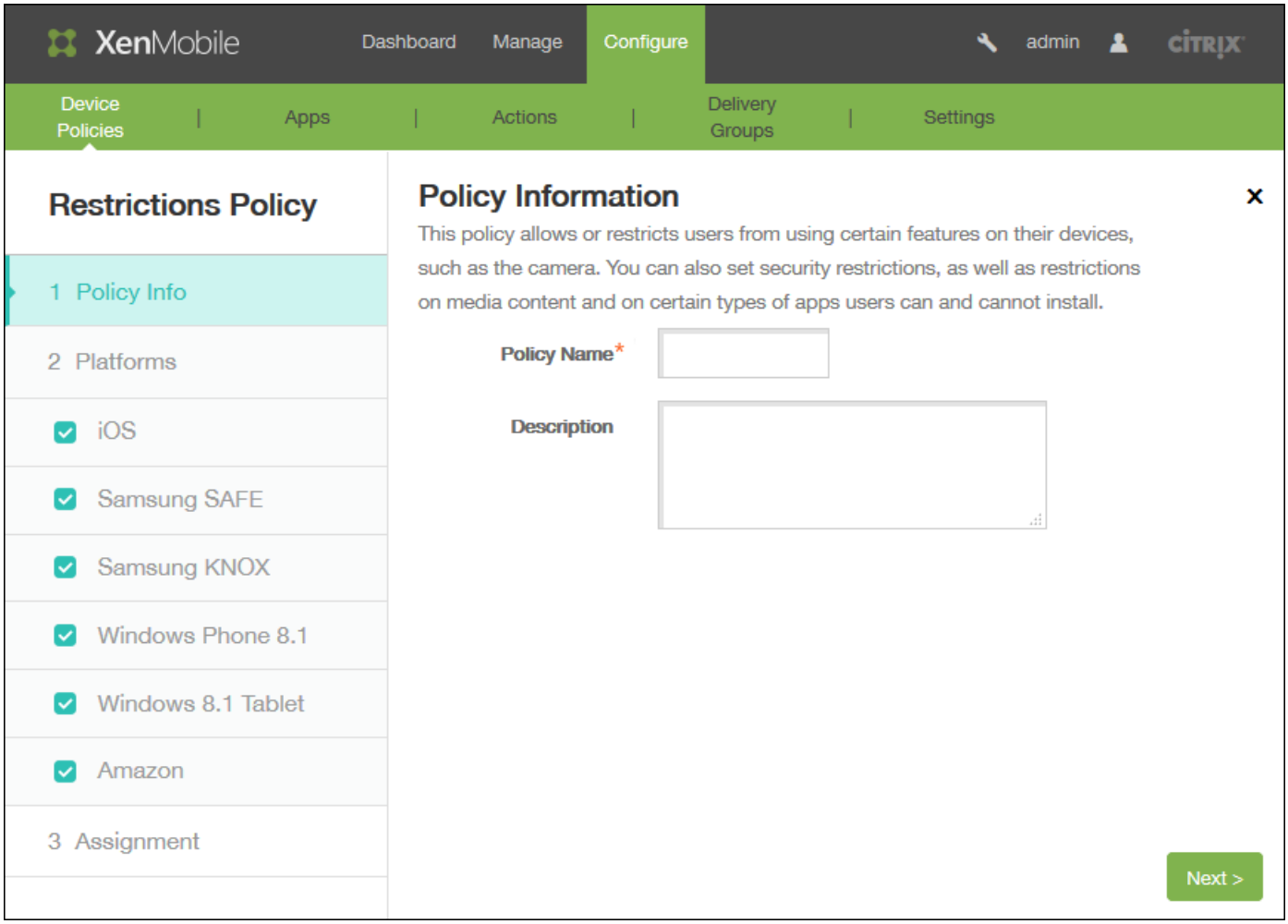
1. Klicken Sie in der XenMobile-Konsole auf **Configure > Device Policies**. Die Seite **Device Policies** wird angezeigt.



2. Klicken Sie auf **Add**. Die Seite **Add a New Policy** wird angezeigt.



3. Klicken Sie auf **Restrictions**. Die Seite **Restrictions Policy** wird angezeigt.



4. Geben Sie im Bereich **Policy Information** die folgenden Informationen ein:

- **Policy Name**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Description**: Geben Sie optional eine Beschreibung der Richtlinie ein.

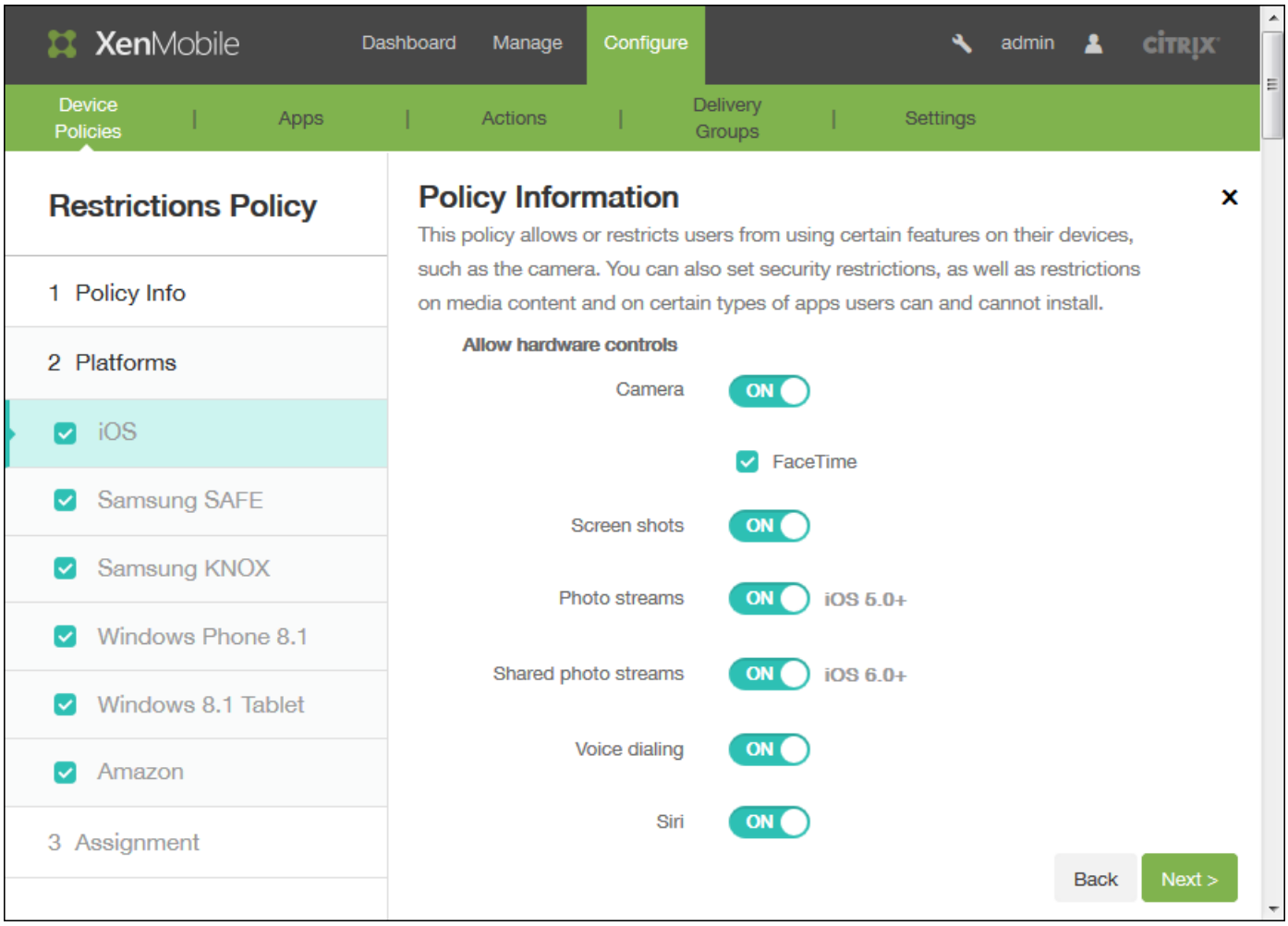
5. Wählen Sie unter **Platforms** die gewünschten Plattformen aus. Sie können anschließend die Richtlinieninformationen für jede ausgewählte Plattform ändern. Klicken Sie zum Einschränken auf die gewünschten Features (siehe nachfolgende Abschnitte), wodurch deren Einstellung in **OFF** geändert wird. Wenn nicht anders angegeben, sind Features in der Standardeinstellung aktiviert.

Konfigurieren von iOS

Konfigurieren von Samsung SAFE
Konfigurieren von Samsung KNOX
Konfigurieren von Windows Phone 8.1
Konfigurieren von Windows 8.1 Tablet
Konfigurieren von Amazon

Wenn Sie die Einschränkungen für eine Plattform fertig eingestellt haben, fahren Sie mit Schritt 6 zum Festlegen der Bereitstellungsregeln für diese Plattform fort.

Bei Auswahl von iOS konfigurieren Sie die folgenden Einstellungen:



Hinweis

Einige iOS-Einschränkungen gelten nur für bestimmte iOS-Versionen (die Seite in der XenMobile-Konsole enthält dann einen entsprechenden Hinweis). Die Option "AirDrop" gilt beispielsweise nur für Geräte mit iOS 7 oder Nachfolgeversionen, während "Photo streams" auf Geräten mit iOS 5 und Nachfolgeversionen unterstützt wird. Einige Optionen werden außerdem nur angewendet, wenn das Gerät im betreuten Modus ist. Anweisungen zum Versetzen von iOS-Geräten in den betreuten Modus finden Sie unter So versetzen Sie ein iOS-Gerät mit dem Apple Configurator in den betreuten Modus.

- Allow hardware controls
  - Camera: Verwendung der Kamera von Geräten zulassen.
    - FaceTime: Verwendung von FaceTime auf Geräten zulassen.
    - Screen shots: Erstellen von Screenshots auf Geräten zulassen.
    - Photo streams: Verwendung von MyPhotoStream zum Teilen von Fotos über iCloud für alle eigenen iOS-Geräte zulassen (verfügbar in iOS 5.0 und höher).
    - Shared photo streams: Verwendung von iCloud Photo Sharing zum Teilen von Fotos mit Kollegen, Freunden und Familie zulassen (verfügbar in iOS 6.0 und höher).
    - VoIP dialing: Sprachwahl auf Geräten zulassen.
    - Siri
      - Allow while device is locked: Verwendung von Siri bei gesperrtem Gerät zulassen.
      - Siri profanity filter: Schimpfwortfilter von Siri aktivieren. Standardmäßig ist dieses Feature eingeschränkt, d. h. es wird kein Schimpfwortfilter verwendet.
  - Installing apps: App-Installation durch Benutzer zulassen.
- Allow apps
  - YouTube: Zugriff auf Inhalte auf YouTube zulassen.
  - iTunes Store: Zugriff auf iTunes Store zulassen.
  - In-app purchases: In-App-Käufe zulassen.
    - Require iTunes password for purchases: Kennwort für In-App-Käufe anfordern. Standardmäßig ist dieses Feature eingeschränkt, d. h. für In-App-Käufe ist kein Kennwort erforderlich (verfügbar in iOS 5.0 und höher).
  - Safari:
    - Autofill: Einrichtung des automatischen Ausfüllens für Benutzernamen und Kennwörter in Safari zulassen.
    - Force fraud warning: Wenn diese Option aktiviert ist, wird der Benutzer von Safari beim Besuch einer unter Phishing-Verdacht stehenden Website gewarnt. Standardmäßig ist dieses Feature eingeschränkt, d. h. es werden keine Warnungen ausgegeben.
    - Enable JavaScript: Ausführung von JavaScript in Safari zulassen.
    - Block pop-ups: Popups beim Besuch von Websites blockieren. Standardmäßig ist dieses Feature eingeschränkt, d. h. es werden keine Popups blockiert.
  - Accept cookies: Legen Sie fest, in welchem Maß Cookies akzeptiert werden sollen. Klicken Sie in der Liste auf eine Option zum Zulassen oder Einschränken von Cookies. In der Standardeinstellung "Always" können Cookies von allen Websites in Safari gespeichert werden. Die anderen Optionen sind "Never" und "From visited sites only".
- Network - Allow iCloud actions
  - Documents and data sync: Synchronisierung von Dokumenten und Daten mit iCloud zulassen (verfügbar in iOS 5.0 und höher).
  - Device backup: Sicherung von Geräten in iCloud zulassen (verfügbar in iOS 5.0 und höher).
  - Automatic sync while roaming: automatische Synchronisierung von E-Mail-Konten mit iCloud im Roamingbetrieb zulassen.
  - iCloud keychain: Speichern von Benutzernamen, Kennwörtern, WiFi-Netzwerkinformationen und Kreditkartendaten in der iCloud-Schlüsselsammlung zulassen (verfügbar in iOS 7.0 und höher).
- Security - Force
  Standardmäßig sind folgende Features eingeschränkt, d. h. keines der Sicherheitsfeatures ist aktiviert.
  - Encrypted backups: Verschlüsseln von Sicherungen in iCloud erzwingen.
  - Limited ad tracking: gezieltes Ad-Tracking sperren (verfügbar in iOS 7.0 und höher).
  - Passcode on first Airplay pairing: Prüfung AirPlay-aktivierter Geräte über einen einmaligen auf dem Bildschirm angezeigten Code vor der Verwendung von AirPlay erzwingen (verfügbar in iOS 7.0 und höher).
- Security - Allow

- **Accepting untrusted SSL certificates**: Akzeptieren nicht vertrauenswürdiger SSL-Zertifikate von Websites zulassen (verfügbar in iOS 5.0 und höher).
- **Automatic update to certificate trust settings**: automatisches Update vertrauenswürdiger Zertifikate zulassen (verfügbar in iOS 7.0 und höher)
- **Documents from managed apps in unmanaged apps**: Übertragen von Daten von verwalteten Apps (Unternehmens-Apps) in nicht verwaltete (private) Apps zulassen.
- **Documents from unmanaged apps in managed apps**: Übertragen von Daten von nicht verwalteten (privaten) Apps in verwaltete Apps (Unternehmens-Apps) zulassen.
- **Diagnostic submission to Apple**: Senden anonymer Diagnosedaten über Benutzergeräte an Apple zulassen.
- **Touch ID to unlock device**: Entsperren von Geräten per Fingerabdruck zulassen (verfügbar in iOS 7.0 und höher).
- **Passbook notifications when locked**: Anzeige von Passbook-Benachrichtigungen auf dem Sperrbildschirm zulassen (verfügbar in iOS 6.0 und höher).
- **Handoff**: Übertragung von Aktivitäten von einem iOS-Gerät zu einem nächstgelegenen iOS-Gerät zulassen (verfügbar in iOS 8.0 und höher).
- **iCloud sync for managed apps**: Synchronisierung verwalteter Apps mit iCloud zulassen (verfügbar in iOS 8.0 und höher).
- **Backup for enterprise books**: Sicherung von Enterprise-Büchern in iCloud zulassen (verfügbar in iOS 8.0 und höher).
- **Notes and highlights sync for enterprise books**: Synchronisierung der von Benutzern in Enterprise-Büchern erstellten Anmerkungen und Markierungen mit iCloud zulassen (verfügbar in iOS 8.0 und höher).

- **Supervised only settings - Allow**
  Diese Einstellungen gelten nur für überwachte Geräte. Anweisungen zum Versetzen von iOS-Geräten in den betreuten Modus finden Sie unter So versetzen Sie ein iOS-Gerät mit dem Apple Configurator in den betreuten Modus.

  - **Internet results in Spotlight**: Anzeige von Suchergebnissen aus dem Internet neben solchen vom Gerät in Spotlight zulassen (verfügbar in iOS 8.0 und höher).
  - **Erase all content and settings**: Löschen aller Inhalte und Einstellungen von den Geräten zulassen (verfügbar in iOS 8.0 und höher).
  - **Configuring restrictions**: Konfigurieren von Jugendschutzeinstellungen auf den Geräten zulassen (verfügbar in iOS 8.0 und höher).
  - **Podcasts**: Download und Synchronisierung von Podcasts zulassen (verfügbar in iOS 8.0 und höher).
  - **Installing configuration profiles**: Installation eines anderen Konfigurationsprofils als des von Ihnen bereitgestellten zulassen (verfügbar in iOS 6.0 und höher).
  - **AirDrop**: Teilen von Fotos, Videos, Websites, Orten usw. mit nahegelegenen iOS-Geräten zulassen (in iOS 7.0 und höher).
  - **iMessage**: Verwenden von iMessage für den Versand von SMS über WiFi zulassen (verfügbar in iOS 6.0 und höher).
  - **Siri user-generated content**: Abfrage benutzergenerierter Inhalte vom Internet durch Siri zulassen. Benutzergenerierte Inhalte werden von Verbrauchern anstelle von Journalisten erstellt, Beispiele sind Inhalte auf Twitter oder Facebook. (verfügbar in iOS 7.0 und höher).
  - **iBooks**: Verwendung der iBooks-App zulassen (verfügbar in iOS 6.0 und höher).
  - **Removing apps**: Entfernen von Apps von den Geräten zulassen (verfügbar in iOS 7.0 und höher).
  - **Game Center**: Spielen von Onlinespielen über Game Center auf den Geräten zulassen (verfügbar in iOS 6.0 und höher).
    - **Add friends**: Senden von Aufforderungen an Freunde zum Spielen zulassen.
    - **Multiplayer gaming**: Starten eines Spiels mit mehreren Spielern auf Geräten zulassen.
  - **Modifying account settings**: Ändern der Gerätekontoeinstellungen zulassen (verfügbar in iOS 7.0 und höher).
  - **Modifying app cellular data settings**: Ändern der Verwendung mobiler Daten durch Apps zulassen (verfügbar in iOS 7.0 und höher).
  - **Modifying Find My Friends settings**: Ändern der Einstellungen für Find My Friends zulassen (verfügbar in iOS 7.0

und höher).

- **Pairing with non-Configurator hosts**: Festlegen des Zielgerätetyps für die Kopplung durch Administrator zulassen. Wenn Sie diese Einstellung deaktivieren, ist keine Kopplung möglich, es sei denn, auf dem überwachenden Host wird Apple Configurator ausgeführt. Ist kein Zertifikat für den überwachenden Host konfiguriert, ist die Kopplung gänzlich deaktiviert (verfügbar in iOS 7.0 und höher).
- **Predictive keyboards**: Verwendung der Tastatur mit Texterkennung zur Anzeige von Wortvorschlägen bei der Texteingabe zulassen (verfügbar in iOS 8.1.3 und höher). Deaktivieren Sie diese Option, wenn Sie nicht möchten, dass Benutzer Zugriff auf vorgeschlagene Wörter haben, etwa bei der Verarbeitung standardisierter Texte.
- **Keyboard auto-corrections**: Verwendung der automatischen Korrektur bei der Texteingabe zulassen (verfügbar in iOS 8.1.3 und höher). Deaktivieren Sie diese Option, wenn Sie nicht möchten, dass Benutzer Zugriff auf korrigierte Wörter haben, etwa bei der Verarbeitung standardisierter Texte.
- **Keyboard spell-check**: Verwendung der Rechtschreibprüfung bei der Texteingabe zulassen (verfügbar in iOS 8.1.3 und höher). Deaktivieren Sie diese Option, wenn Sie nicht möchten, dass Benutzer Zugriff auf die Rechtschreibprüfung haben, etwa bei der Verarbeitung standardisierter Texte.
- **Definition lookup**: Verwendung der Funktion zum Nachschlagen von Definitionen bei der Texteingabe zulassen (verfügbar in iOS 8.1.3 und höher). Deaktivieren Sie diese Option, wenn Sie nicht möchten, dass Benutzer Zugriff auf Definitionen haben, etwa bei der Verarbeitung standardisierter Texte.
- **Single App bundle ID**: Erstellen einer Liste von Apps, die die Kontrolle über das Gerät haben und eine Interaktion mit anderen Apps oder Funktionen verhindern.
  Zum Hinzufügen von Apps klicken Sie auf "Add" und führen Sie folgende Schritte aus:

  a. **App name**: Geben Sie einen App-Namen ein.

  b. Klicken Sie auf **Save** oder **Cancel**.

  c. Wiederholen Sie die Schritte a und b für jede App, die Sie hinzufügen möchten.

  Tipp: Zum Löschen einer vorhandenen App zeigen Sie auf deren Namen und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf "Delete", um die Einladung zu löschen oder auf Cancel zum Beibehalten des Eintrag.
  Zum Bearbeiten einer App zeigen Sie auf deren Namen und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf "Save", um die Änderungen zu speichern oder auf "Cancel", um den Vorgang abzubrechen.

- Security - Show in lock screen
  - **Control Center**: Zugriff auf Control Center auf dem Sperrbildschirm zulassen, damit Benutzer Einstellungen für Flugmodus, WiFi, Bluetooth, den Nicht stören-Modus und die Ausrichtungssperre einfach ändern können (verfügbar in iOS 7.0 und höher).
  - **Notification**: Anzeige von Benachrichtigungen auf dem Sperrbildschirm zulassen (verfügbar in iOS 7.0 und höher).
  - **Today view**: Anzeige von "Ansicht heute" mit Informationen wie Wetter und aktuelle Kalendereinträge auf dem Sperrbildschirm zulassen.
- Media content - Allow
  - **Explicit music, podcasts, and iTunes U material**: anstößige Inhalte auf den Geräten zulassen.
  - **Explicit sexual content in iBooks**: Download anstößiger Inhalte aus iBooks zulassen (verfügbar in iOS 6.0 und höher).
  - **Ratings region**: Region, aus der die Wertungen für den Jugendschutz abgerufen werden sollen. Klicken Sie in der Liste auf gewünschte Land. Der Standard ist United States.
  - **Movies**: Legen Sie fest, ob Filme auf den Geräten zugelassen werden sollen. Wenn Sie Filme zulassen, legen Sie

optional die Wertungen für Filme fest. Klicken Sie in der Liste auf eine Option zum Zulassen oder Einschränken von Filmen. Der Standardwert ist "Allow all movies".

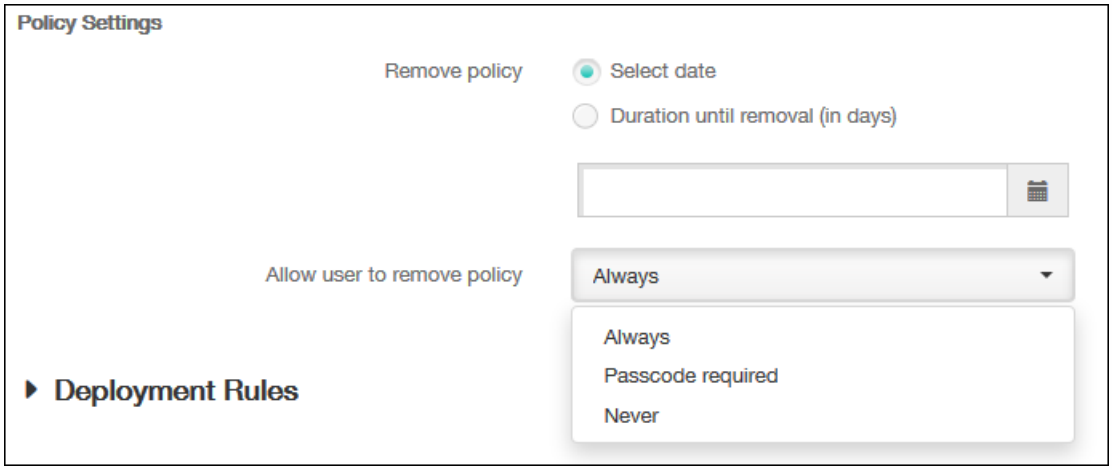
- **TV Shows**: Legen Sie fest, ob Fernsehsendungen auf den Geräten zugelassen werden sollen. Wenn Sie Fernsehsendungen zulassen, legen Sie optional die Wertungen für Fernsehsendungen fest. Klicken Sie in der Liste auf eine Option zum Zulassen oder Einschränken von Fernsehsendungen. Der Standardwert ist "Allow all TV Shows".
- **Apps**: Legen Sie fest, ob Apps auf den Geräten zugelassen werden sollen. Wenn Sie Apps zulassen, legen Sie optional die Wertungen für Apps fest. Klicken Sie in der Liste auf eine Option zum Zulassen oder Einschränken von Apps. Der Standardwert ist "Allow all apps".

- **Richtlinieneinstellungen**
  Klicken Sie neben **Remove policy** auf **Select date** oder **Duration until removal (in days)**.

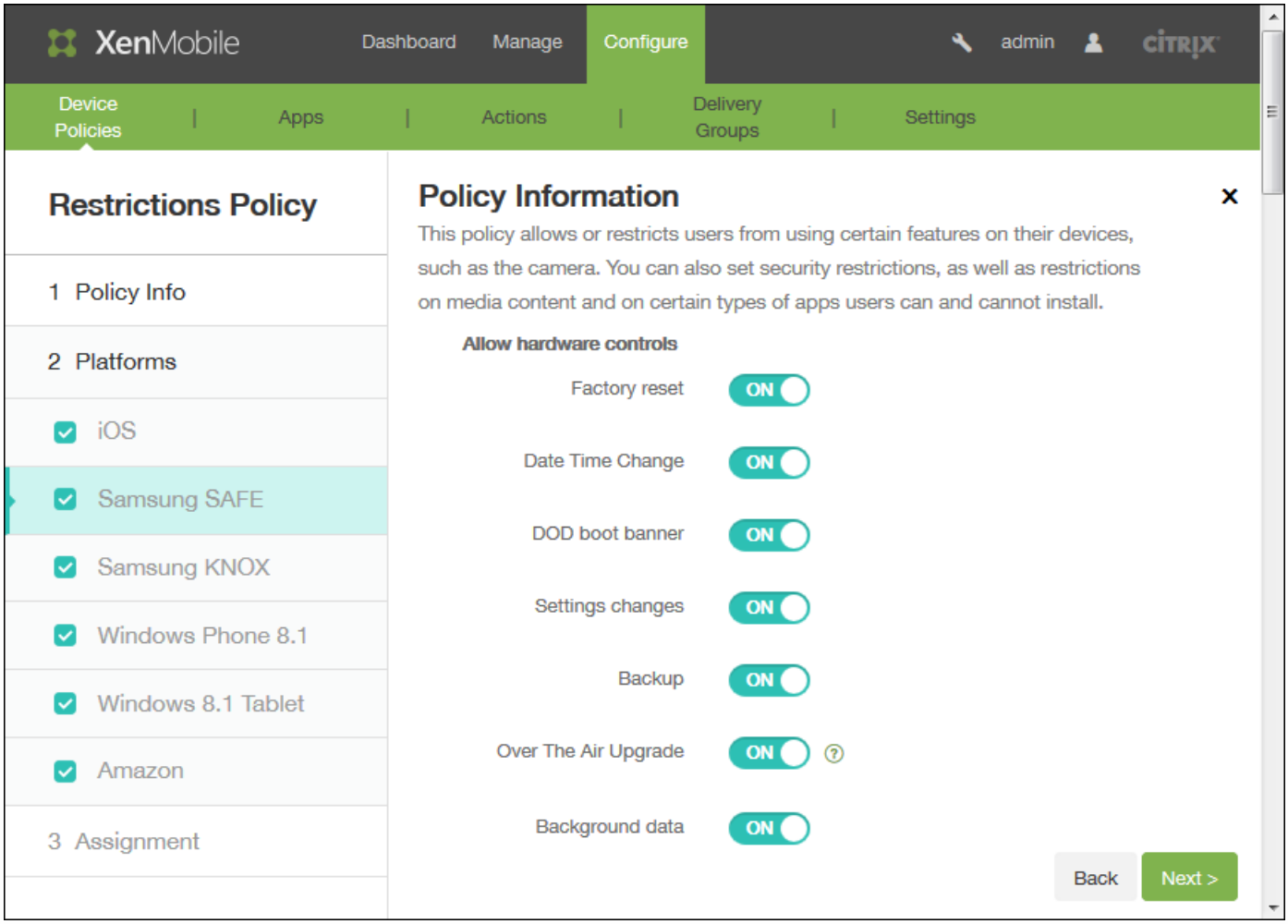
  Bei Auswahl von **Select date** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.

  Klicken Sie in der Liste **Allow user to remove policy** auf **Always**, **Password required** oder **Never**.

  Bei Auswahl von **Password required** geben Sie für **Removal password** das Kennwort ein.



Bei Auswahl von "Samsung SAFE" konfigurieren Sie die folgenden Einstellungen:



Hinweis

Einige Optionen stehen nur in bestimmten APIs zur Samsung-Mobilgeräteverwaltung (MDM) zur Verfügung. Für diese ist die entsprechende Versionsangabe aufgeführt.

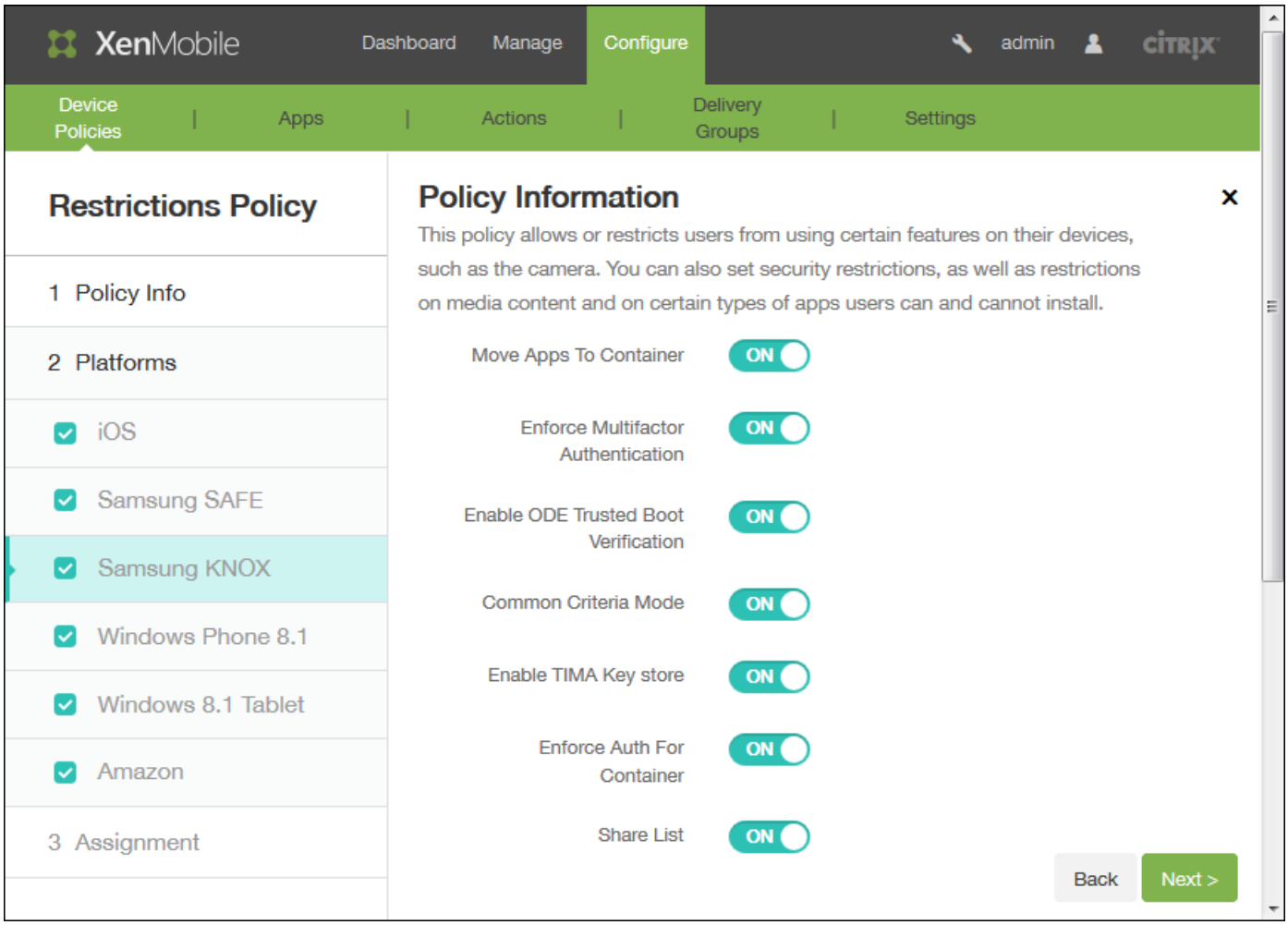
- Allow hardware controls
  - **Factory Reset**: Zurücksetzen der Geräte zulassen.
  - **Date Time Change**: Änderung von Datum und Uhrzeit auf den Geräten zulassen.
  - **DOD reboot banner**: Beim Geräteneustart eine Benachrichtigung oder ein Banner über die vom Department of Defense genehmigte Systemnutzung anzeigen.
  - **Settings changes**: Ändern von Einstellungen auf Geräten zulassen.
  - **Backup**: Sicherung von Anwendungs- und Systemdaten auf Geräten zulassen.
  - **Over The Air Upgrade**: Erhalt von Softwareupdates über eine drahtlose Schnittstelle zulassen (MDM 3.0 und höher).
  - **Background data**: Synchronisierung von Daten durch Apps im Hintergrund zulassen.
  - **Camera**: Verwendung der Kamera von Geräten zulassen.
  - **Clipboard**: Kopieren von Daten in die Zwischenablage von Geräten zulassen.
    - **Clipboard share**: Teilen von Inhalten in der Zwischenablage zwischen Geräten und Computern zulassen (MDM 4.0 und höher).
  - **Home key**: Verwendung der Home-Taste auf den Geräten zulassen.
  - **Microphone**: Verwendung des Gerätemikrofons zulassen.

- **Mock location**: Vortäuschung eines GPS-Standorts zulassen.
- **NFC (Near Field Communication)**: Verwendung von NFC zulassen (MDM 3.0 und höher).
- **Power off**: Ausschalten des Geräts zulassen (MDM 3.0 und höher).
- **Screenshot**: Erstellen von Screenshots auf Geräten zulassen.
- **SD card**: Verwendung einer SD-Karte (sofern verfügbar) zulassen.
- **Voice Dialer**: Verwendung der Sprachwahl auf den Geräten zulassen (MDM 4.0 und höher).
- **SBeam**: Teilen von Inhalten über NFC und Wi-Fi Direct zulassen (MDM 4.0 und höher).
- **SVoice**: Verwendung des intelligenten persönlichen Assistenten und Wissensnavigators auf Geräten zulassen (MDM 4.0 und höher).

- Allow apps
  - **Browser**: Verwendung des Webbrowsers zulassen.
  - **YouTube**: Zugriff auf YouTube zulassen.
  - **Google Play/Marketplace**: Zugriff auf Google Play und Google Apps Marketplace zulassen.
  - **Allow Non-Google Play apps**: Download von Apps aus anderen Websites als Google Play und Google Apps Marketplace zulassen.
  - **Stop system app**: Deaktivieren vorinstallierter System-Apps zulassen (MDM 4.0 und höher).
- Network
  - **Incoming Mms**: Empfang von MMS-Nachrichten zulassen.
  - **Incoming Sms**: Empfang von SMS-Nachrichten zulassen.
  - **Outgoing Mms**: Senden von MMS-Nachrichten zulassen.
  - **Outgoing Sms**: Senden von SMS-Nachrichten zulassen.
  - **Bluetooth**: Verwendung von Bluetooth zulassen.
    - **Tethering**: gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über die Bluetooth-Verbindung des Geräts zulassen.
  - **WiFi** Verbindung mit WiFi-Netzwerk zulassen.
    - **Tethering**: gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über die WiFi-Verbindung des Geräts zulassen.
    - **Direct**: direkte Verbindung mit einem anderen Gerät über die WiFi-Verbindung zulassen (MDM 4.0 und höher).
    - **State Change**: Änderung des WiFi-Verbindungszustands durch Apps zulassen.
  - **Tethering**: gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät zulassen.
  - **Cellular data**: Verwendung der Mobilfunkverbindung für Daten zulassen.
  - **Allow roaming**: Verwendung mobiler Daten beim Roaming zulassen. Der Standardwert ist "OFF", d. h. Roaming ist auf den Geräten deaktiviert.
  - **Only secure connections**: nur die Verwendung sicherer Verbindungen zulassen (MDM 4.0 oder höher).
  - **Android beam**: Senden von Webseiten, Fotos, Videos oder anderer Inhalte an andere Geräte über NFC zulassen (MDM 4.0 und höher).
  - **Audio record**: Audioaufzeichnungen auf den Geräten zulassen (MDM 4.0 und höher).
  - **Video record**: Videoaufzeichnungen auf den Geräten zulassen (MDM 4.0 und höher).
  - **Location services**: Einschalten von GPS auf den Geräten zulassen.
  - **Limit by day (MB)**: Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Tag übertragen dürfen. Der Standardwert ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).
  - **Limit by week (MB)**: Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Woche übertragen dürfen. Der Standardwert ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).
  - **Limit by month (MB)**: Geben Sie die Menge der mobilen Daten in MB ein, die Benutzer pro Monat übertragen dürfen. Der Standardwert ist 0, d. h. dieses Feature ist deaktiviert (MDM 4.0 und höher).
- **Allow USB actions**: USB- Verbindung zwischen Geräten und Computern zulassen.

- **Debugging**: Debuggen über USB zulassen.
- **Host storage**: Verwendung der Geräte als USB-Host bei Verbindung eines USB-Geräts mit den Geräten zulassen. Die Geräte müssen hierbei USB-Geräte mit Strom versorgen.
- **Mass storage**: Übertragung großer Datendateien zwischen Geräten und Computern über eine USB-Verbindung zulassen.
- **Kies media player**: Verwendung von Samsung Kies zum Synchronisieren von Dateien zwischen Gerät und Computer zulassen.
- **Tethering**: gemeinsame Verwendung einer mobilen Datenverbindung mit einem anderen Gerät über eine USB-Verbindung zulassen.

Bei Auswahl von "Samsung KNOX" konfigurieren Sie die folgenden Einstellungen:



Hinweis

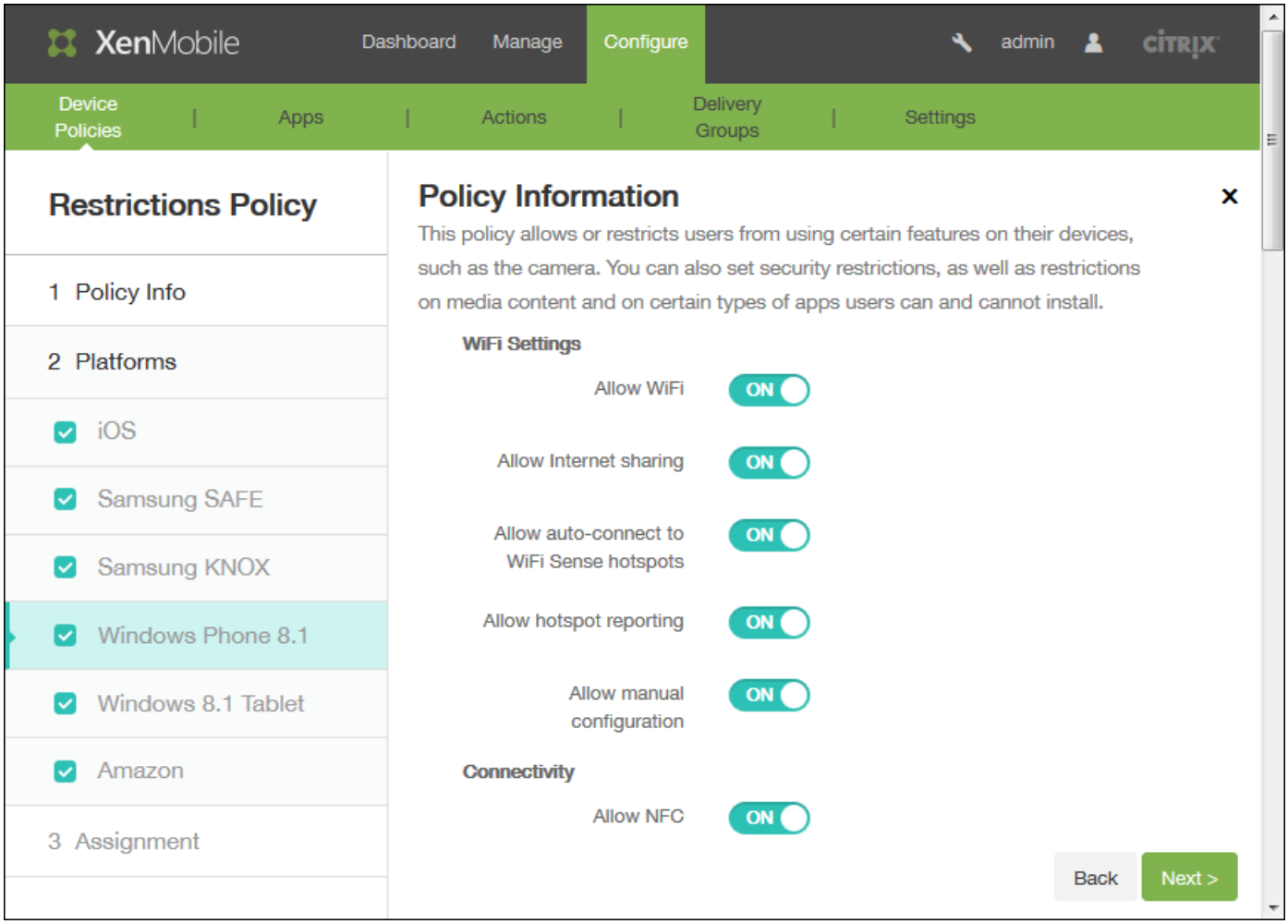
Diese Optionen stehen nur unter Samsung KNOX Premium (KNOX 2.0) zur Verfügung.

- **Move Apps To Container**: Verschieben von Apps zwischen dem KNOX-Container und dem privaten Bereich auf

Geräten zulassen.

- **Enforce Multifactor Authentication**: Benutzer müssen einen Fingerabdruck und eine weitere Authentifizierungsmethode, z. B. Kennwort oder PIN zum Öffnen ihrer Geräte verwenden.
- **Enable ODE Trusted Boot Verification**: Verwenden der ODE-Prüfung auf vertrauenswürdigen Start zur Erstellung einer Vertrauenskette zwischen Bootloader und Systemimage.
- **Common Criteria Mode**: Schalten von Geräten in den Common Criteria-Modus. Die Common Criteria-Konfiguration erzwingt strenge Sicherheitsvorgänge.
- **Enable TIMA Key store**: Aktivieren von TIMA KeyStore. TIMA KeyStore bietet TrustZone-basierte sichere Schlüsselspeicherung für symmetrische Schlüssel. RSA-Schlüsselpaare und -Zertifikate werden zur Speicherung an den Standard-Schlüsselspeicheranbieter geleitet.
- **Enforce Auth For Container**: Verwendung einer separaten Authentifizierung zum Öffnen des KNOX-Containers, die sich von der für das Entsperren des Geräts unterscheidet.
- **Share List**: Teilen von Inhalten zwischen Apps in der Liste "Share Via" zulassen.
- **Enable Audit Log**: Erstellen von Ereignisüberwachungsprotokollen für die forensische Analyse von Geräten aktivieren.
- **Use Secure Keypad**: Benutzer zur Verwendung einer sicheren Tastatur im KNOX-Container zwingen.
- **Enable Google Apps**: Download von Apps aus Google Mobile Services in den KNOX-Container zulassen.
- **Authentication Smart Card Browser**:

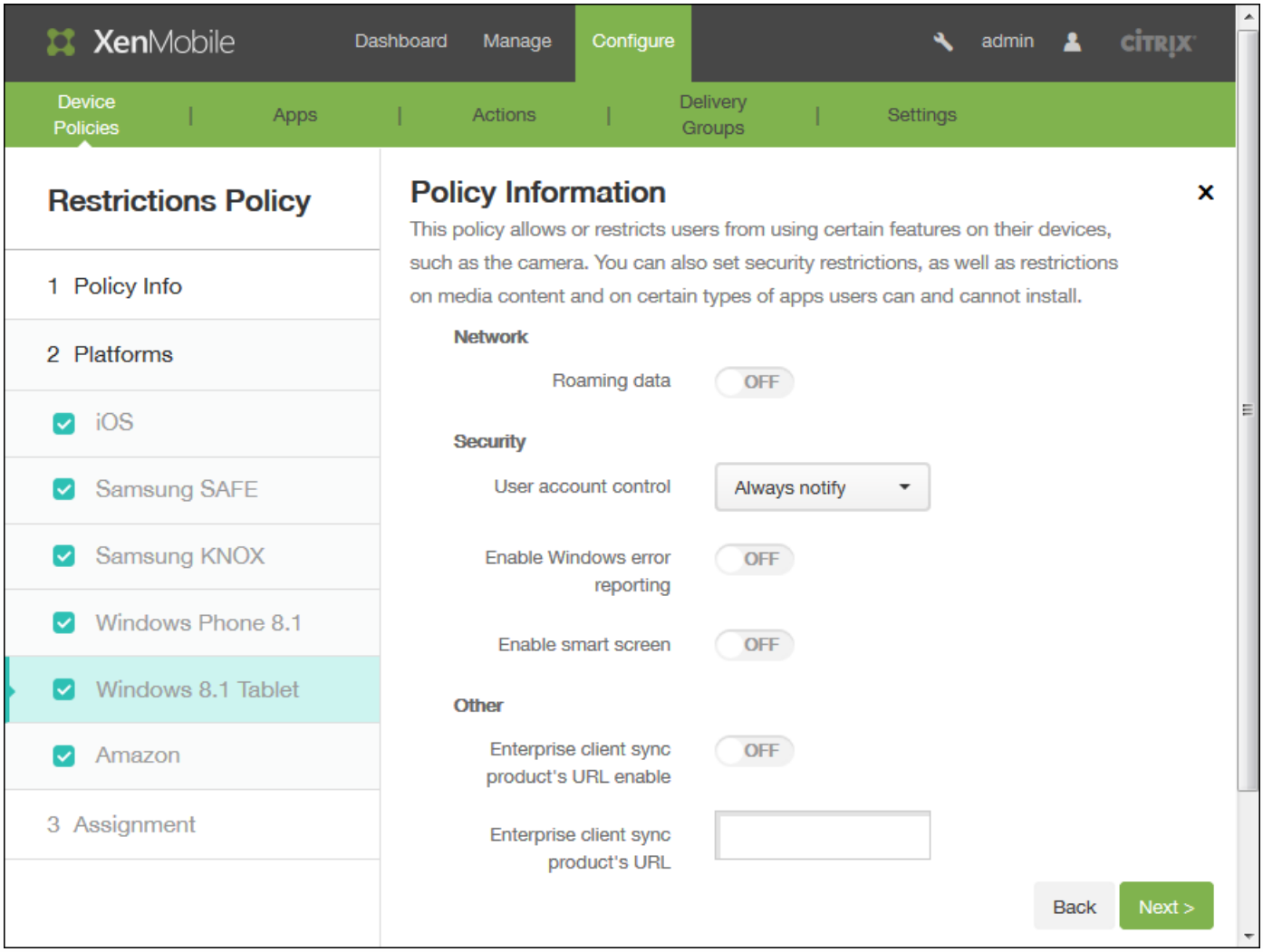
Bei Auswahl von "Windows Phone 8.1" konfigurieren Sie die folgenden Einstellungen:



- WiFi Settings
  - **Allow WiFi**: Verbindung von Geräten mit einem WiFi-Netzwerk zulassen.
  - **Allow Internet sharing**: gemeinsame Verwendung der Internetverbindung eines Geräts mit anderen Geräten durch Nutzung des Geräts als WiFi-Hotspot zulassen.
  - **Allow auto-connect to WiFi Sense hotspots**: automatische Verbindung von Geräten mit WiFi Sense-Hotspots zulassen. Für diese Option müssen Positionsdienste aktiviert sein. Weitere Informationen zu WiFi Sense für Windows Phone finden Sie in den FAQ zu WiFi Sense.
  - **Allow hotspot reporting**: Melden der Hotspots, durch Geräte zulassen, mit denen diese eine Verbindung herstellen.
  - **Allow manual configuration**: manuelle Konfiguration von WiFi-Verbindungen durch die Benutzer zulassen.
- Connectivity
  - **Allow NFC (Near Field Communication)**: Kommunikation zwischen Geräten und NFC-Tags oder NFC-Sendern zulassen.
  - **Allow bluetooth**: Verbindungen von Geräten über Bluetooth zulassen.
  - **Allow VPN over cellular**: Verbindungen zwischen Geräten über ein VPN mit einem mobilen Netzwerk zulassen.
  - **Allow VPN over cellular while roaming**: Verbindungen von Geräten über ein VPN im Roamingbetrieb zulassen.
  - **Allow USB connection**: Verbindungen zwischen Desktop und Gerätespeicher über USB zulassen.
  - **Allow cellular data roaming**: Verwendung mobiler Daten beim Roaming zulassen.
- Accounts
  - **Allow Microsoft account connection**: Verwendung eines Microsoft-Kontos durch Geräte für Verbindungsauthentifizierung und Dienste ohne E-Mail-Bezug zulassen.
  - **Allow non-Microsoft email**: Hinzufügen Microsoft-externer E-Mail-Konten durch die Benutzer zulassen.

- Search
  - **Allow search to use location**: Verwendung des Gerätepositionsdiensts durch die Suche zulassen.
  - **Filter adult content**: nicht jugendfreien Inhalt zulassen. Der Standardwert ist "OFF", d. h. nicht jugendfreier Inhalt wird nicht gefiltert.
  - **Allow Bing Vision to store images**: Speichern von bei Bing Vision-Suchen erfassten Bildern zulassen.
- System
  - **Allow storage card**: Verwendung einer Speicherkarte durch Geräte zulassen.
  - **Allow location services**: Positionsdienste zulassen.
  - **Allow use of camera**: Verwendung der Gerätekamera zulassen.
  - **Telemetry**: Klicken Sie in der Liste auf eine Option zum Zulassen oder Einschränken des Versands von Telemetrieinformationen durch Geräte. Der Standardwert ist "Allowed". Andere Optionen sind "Not allowed" und "Allowed, except for secondary data request".
- Security
  - **Allow manual root certificate installation**: manuelle Installation eines Stammzertifikats durch Benutzer zulassen.
  - **Require device encryption**: Geräteverschlüsselung erzwingen. Wenn die Verschlüsselung auf einem Gerät aktiviert wurde, kann sie nicht wieder deaktiviert werden. Der Standardwert ist "OFF".
  - **Allow copy and paste**: Kopieren und Einfügen Daten auf Geräten zulassen.
  - **Allow screen capture**: Erstellen von Screenshots auf Geräten zulassen.
  - **Allow voice recording**: Sprachaufzeichnung auf Geräten zulassen.
  - **Allow Save As of Office files**: Speichern von Office-Dateien mit der Option "Speichern unter" zulassen.
  - **Allow action center notifications**: Anzeige von Action Center-Benachrichtigungen auf dem Sperrbildschirm zulassen.
  - **Allow Cortana**: Verwendung des intelligenten persönlichen Assistenten und Wissensnavigators Cortana auf Geräten zulassen.
  - **Allow sync of device settings**: Synchronisierung von Einstellungen zwischen Windows Phone 8.1-Geräten im Roamingbetrieb zulassen.
- Apps
  - **Allow store access**: Zugriff auf Microsoft Store zulassen.
  - **Allow developer unlock**: Registrierung von Geräten bei Microsoft und Entwicklung oder Installation von Apps, die nicht im App-Store für Windows Phone sind, zulassen.
  - **Allow web browser access**: Internet Explorer auf Geräten zulassen.

Bei Auswahl von "Windows 8.1 tablet" konfigurieren Sie die folgenden Einstellungen:



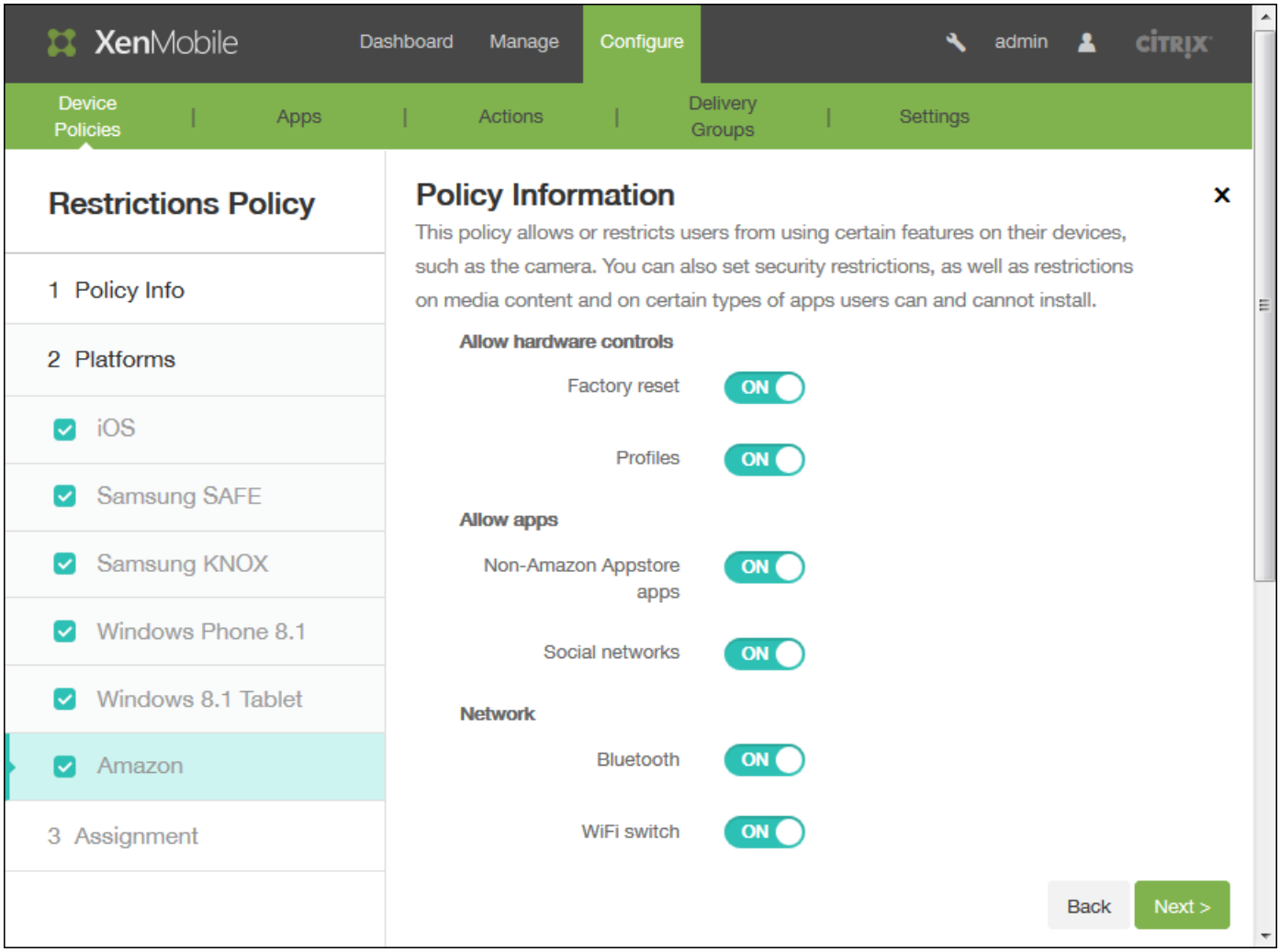
Hinweis

Der Standardwert für die folgenden Einstellungen ist "OFF".

- Network
  - **Roaming data**: Verwendung mobiler Daten beim Roaming zulassen.
- Security
  - **User account control**: Maß der Benachrichtigung festlegen, die Benutzer erhalten, wenn Apps Änderungen an den Geräten versuchen. Wählen Sie in der Liste eine Option für die Benachrichtigung aus. Der Standardwert ist **Always notify**, d. h. dass bei allen Änderungen der Bildschirm des Geräts abgedunkelt und eine Meldung angezeigt wird, die der Benutzer beantworten muss, bevor er fortfahren kann. Weitere Optionen sind **Notify app changes**, **Notify app changes (no dim)** und **Never notify**.
  - **Enable Windows error reporting**: Meldung von Problemen mit Geräten durch die Windows-Fehlerberichterstattung an Microsoft zulassen.
  - **Enable smart screen**: Windows SmartScreen zum Prüfen heruntergeladener Dateien und Internet-Inhalte in Apps auf schädliche Software und potenziell nicht sicheren Inhalt aktivieren.
- Sonstiges
  - **Enterprise client sync product's URL enable**: Enterprise Client Sync auf Geräten aktivieren.

- **Enterprise client sync product's URL**: Wenn Sie "Enterprise client sync product's URL" auf "ON" festlegen, geben Sie eine gültige URL ein.

Bei Auswahl von "Amazon" konfigurieren Sie die folgenden Einstellungen:



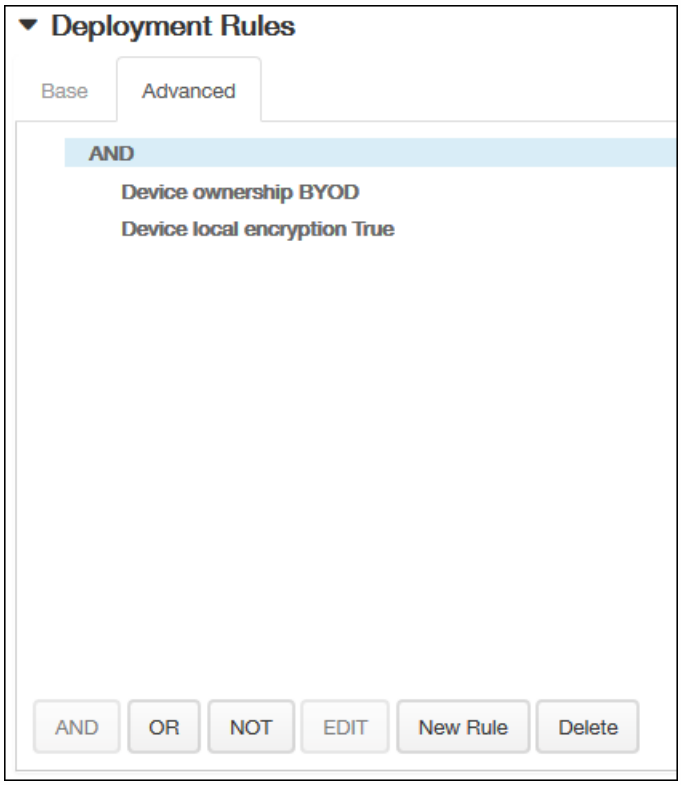
- Allow hardware controls
  - **Factory reset**: Zurücksetzen der Geräte auf die werkseitige Voreinstellung zulassen.
  - **Profiles**: Ändern des Hardwareprofils auf Geräten zulassen.
- Allow apps
  - **Non-Amazon Appstore apps**: Installation von Apps, die nicht aus dem Amazon App-Shop stammen, auf Geräten zulassen.
  - **Social networks**: Zugriff auf soziale Netzwerke von den Geräten aus zulassen.
- Network
  - **Bluetooth**: Verwendung von Bluetooth zulassen.
  - **WiFi switch**: Wechseln des WiFi-Verbindungszustands durch Apps zulassen.
  - **WiFi settings**: Ändern der WiFi-Einstellungen zulassen.
  - **Cellular data**: Verwendung der Mobilfunkverbindung für Daten zulassen.

- **Roaming data**: Verwendung mobiler Daten beim Roaming zulassen.
- **Location services**: GPS-Verwendung zulassen.

- **USB actions**:
  - **Debugging**: USB-Verbindungen mit einem Computer für das Debugging zulassen.

6. Erweitern Sie **Deployment Rules** und konfigurieren Sie folgende Einstellungen: Standardmäßig wird die Registerkarte **Base** angezeigt.

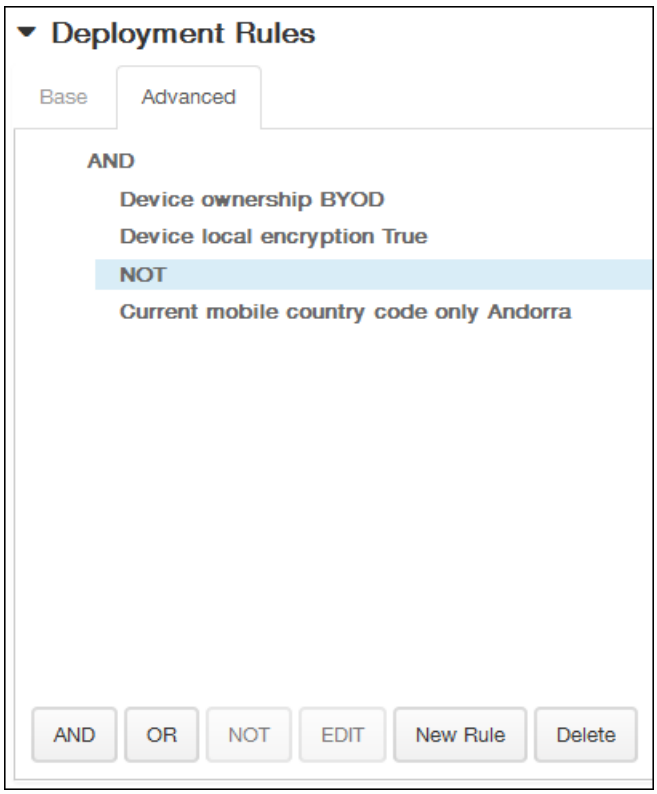
- Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
  - Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist **All**.
  - Klicken Sie auf **New Rule**, um Bedingungen zu definieren.
  - Klicken Sie in der Liste auf Bedingungen wie **Device ownership** oder **BYOD** (siehe Abbildung oben).
  - Klicken Sie erneut auf **New Rule**, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
  - Klicken Sie auf die Registerkarte **Advanced**, um die Regeln mit booleschen Optionen zu kombinieren. Die Bedingungen, die Sie auf der Registerkarte **Base** ausgewählt haben, werden angezeigt.



- Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
  - Klicken Sie auf **AND**, **OR** oder **NOT**.

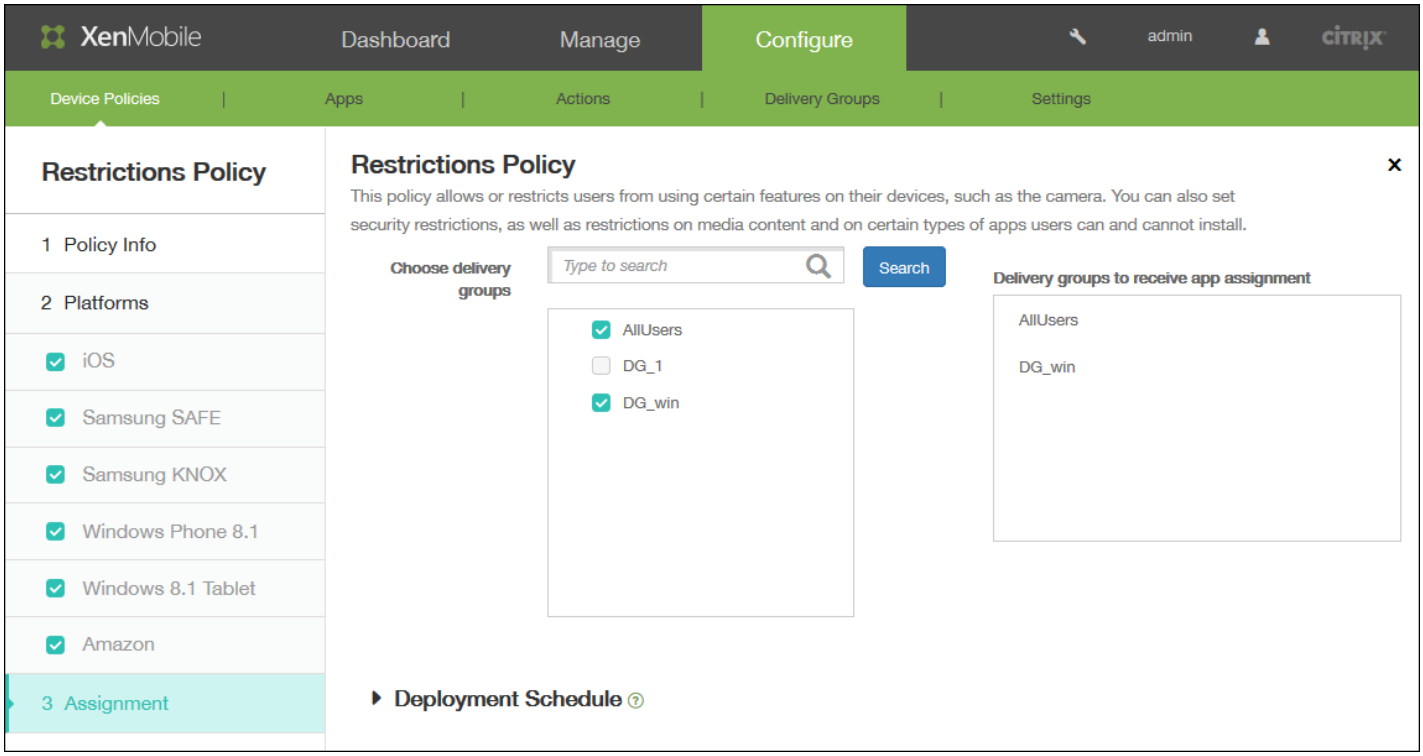
- Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
  Sie können jederzeit auf eine Bedingung und dann auf **EDIT** klicken, um die Bedingung zu ändern, oder auf **Delete**, um die Bedingung zu löschen.
- Klicken Sie erneut auf **New Rule**, wenn Sie weitere Bedingungen hinzufügen möchten.

In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



7. Nach Abschluss der Konfiguration der Einstellungen für eine oder mehrere Plattformen klicken Sie auf **Next**. Es wird dann die Seite **Assignment** für die Einschränkungsrichtlinie angezeigt.

8. Machen Sie neben **Choose delivery groups** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Delivery groups to receive app assignment** angezeigt.



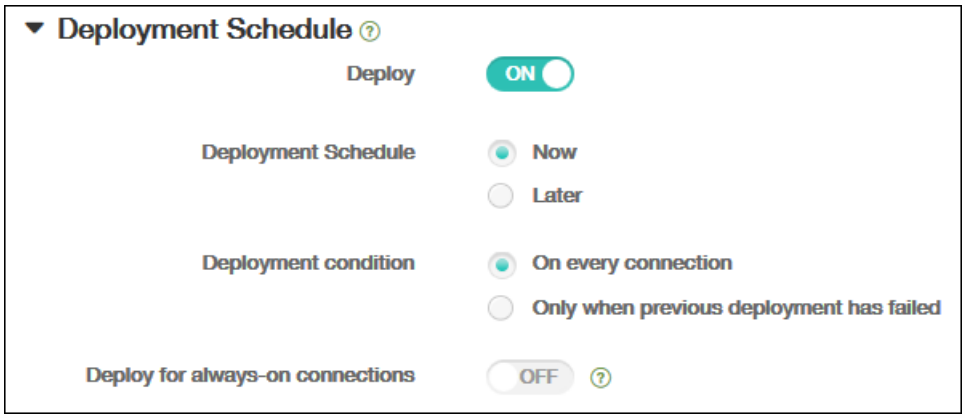
9. Erweitern Sie **Deployment Schedule** und konfigurieren Sie folgende Einstellungen:

- Klicken Sie neben **Deploy** auf **ON**, um die Bereitstellung zu planen, oder auf **OFF**, um die Bereitstellung zu verhindern. Die Standardeinstellung ist **ON**. Wenn Sie **OFF** auswählen, müssen keine anderen Optionen konfiguriert werden.
- Klicken Sie neben **Deployment schedule** auf **Now** oder **Later**. Die Standardeinstellung ist **Now**.
- Wenn Sie auf **Later** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Deployment condition** auf **On every connection** oder auf **Only when previous deployment has failed**. Die Standardeinstellung ist **On every connection**.
- Klicken Sie neben **Deploy for always-on connection** auf **ON** oder **OFF**. Die Standardeinstellung ist **OFF**.

Hinweis:

Diese Option gilt, wenn Sie unter **Settings > Server Properties** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Deploy for always on connection**, denn diese Option gilt nicht für iOS.



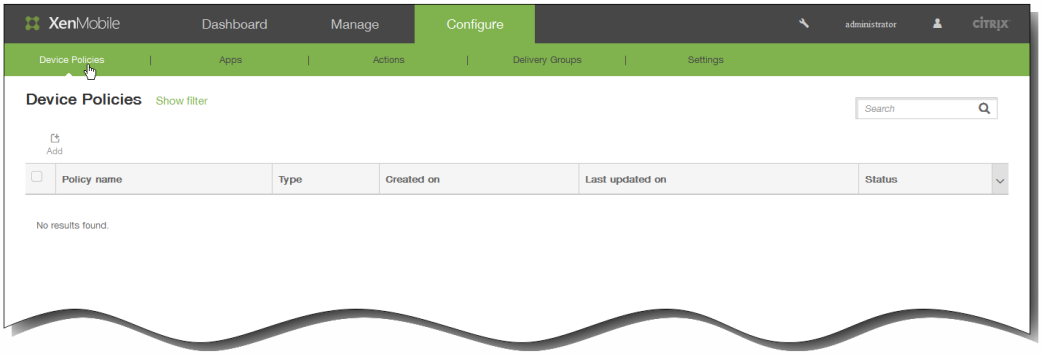
Klicken Sie auf **Save**, um die Richtlinie zu speichern.

So fügen Sie eine Roamingrichtlinie für iOS-Geräte hinzu

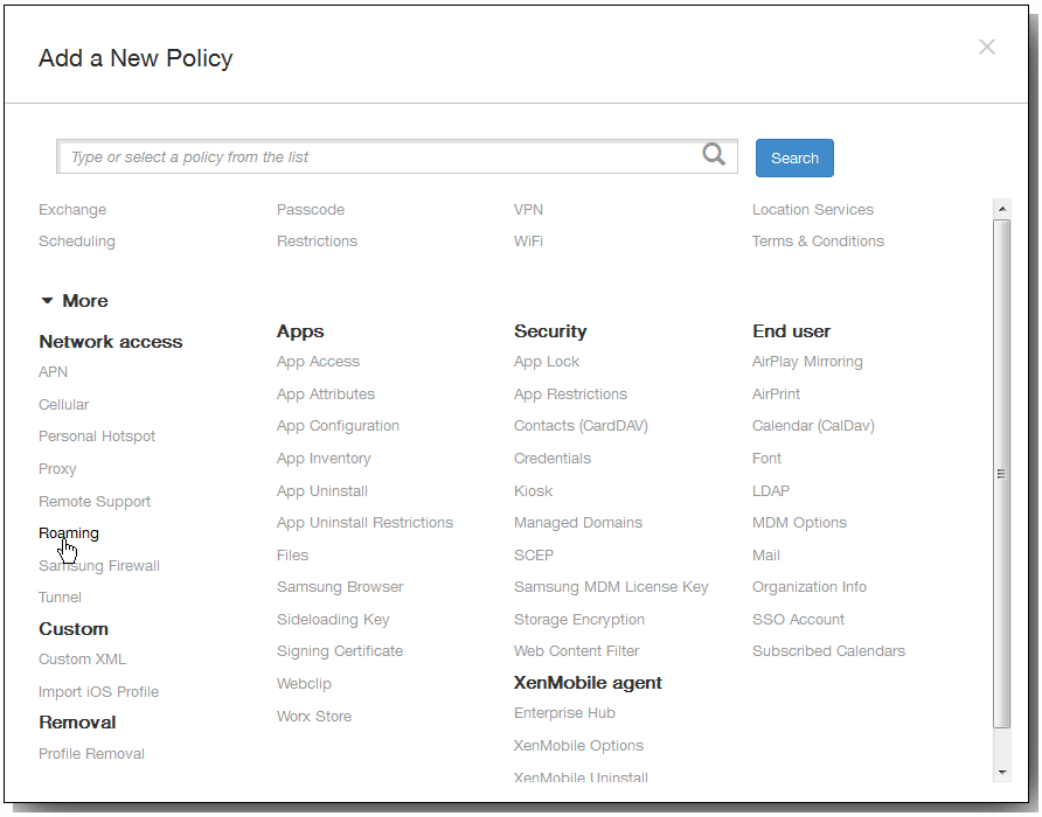
Nov 12, 2015

Sie können in XenMobile eine Geräterichtlinie einrichten, um vorzugeben, ob auf iOS-Geräten Sprach- und Datenroaming zugelassen wird. Wird Sprachroaming deaktiviert, dann wird Datenroaming automatisch auch deaktiviert. Diese Richtlinie gilt nur für iOS 5.0 und höher.

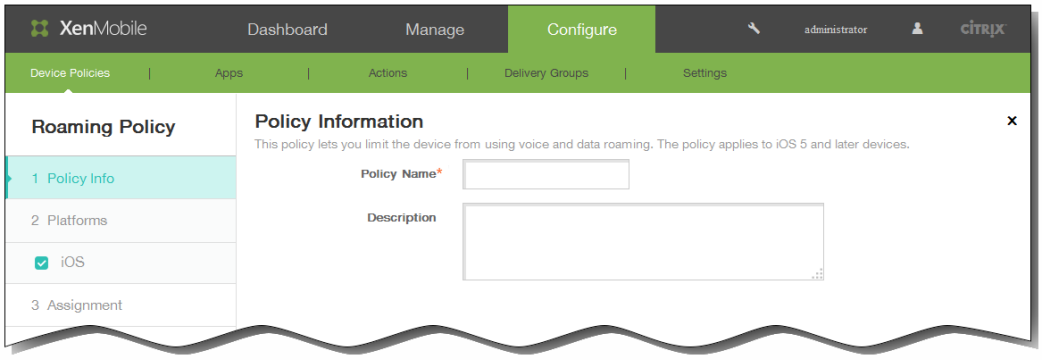
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



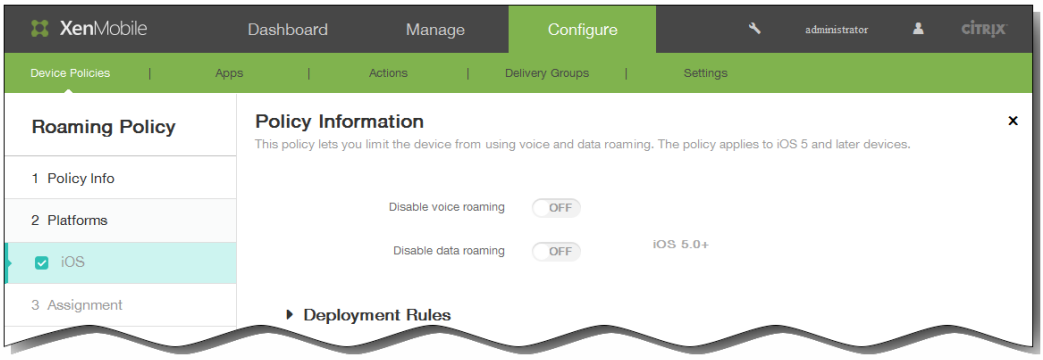
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter Network access auf Roaming. Die Seite Roaming Info Policy wird angezeigt.

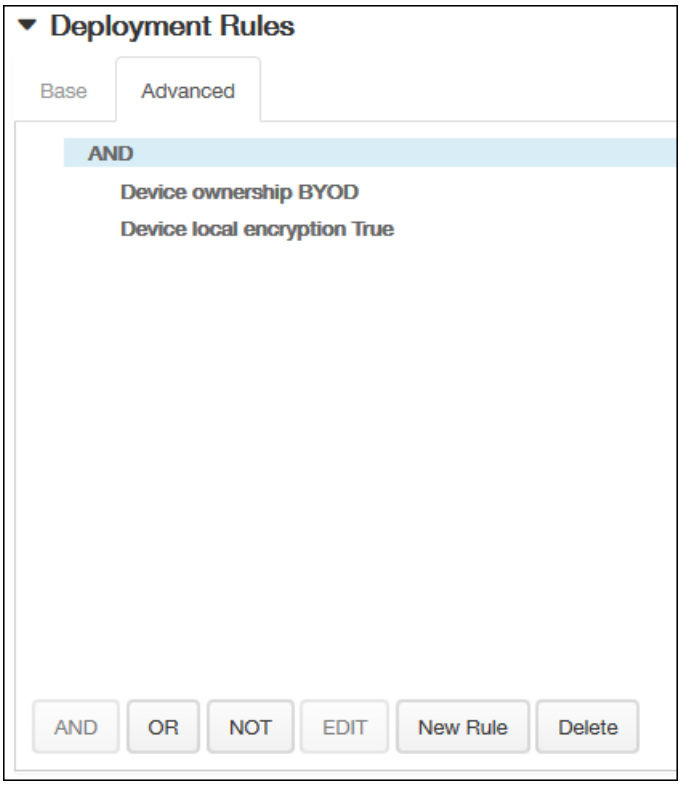


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite iOS Platform Information wird angezeigt.



6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:
   1. Disable voice roaming: Wählen Sie aus, ob das Sprachroaming deaktiviert werden soll. Wird diese Option deaktiviert, dann wird Datenroaming automatisch auch deaktiviert. Die Standardeinstellung ist OFF, Sprachroaming ist also zugelassen.
   2. Disable data roaming: Wählen Sie aus, ob das Datenroaming deaktiviert werden soll. Diese Option ist nur verfügbar, wenn Sprachroaming aktiviert ist. Die Standardeinstellung ist OFF, Datenroaming ist also zugelassen.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

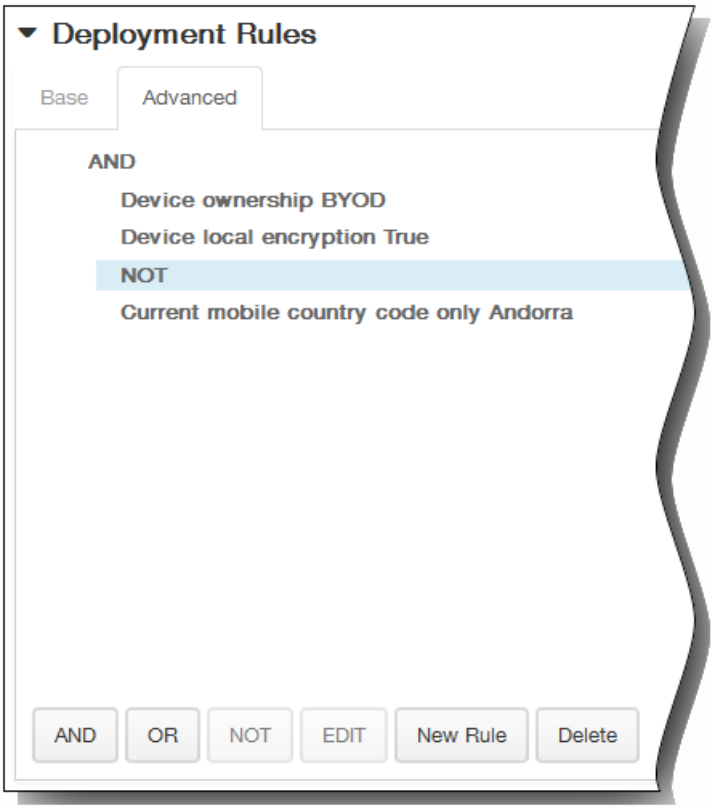
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



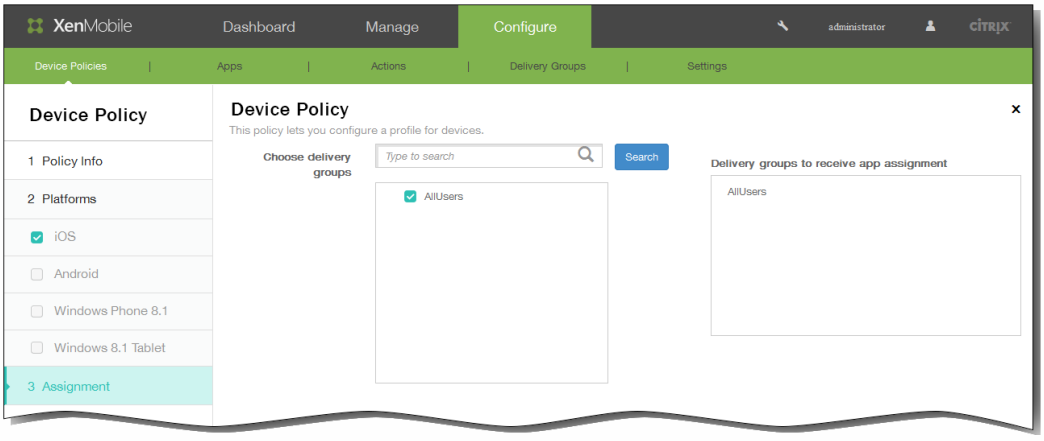
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
    1. Klicken Sie auf AND, OR oder NOT.
    2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
    Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

    3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
    In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



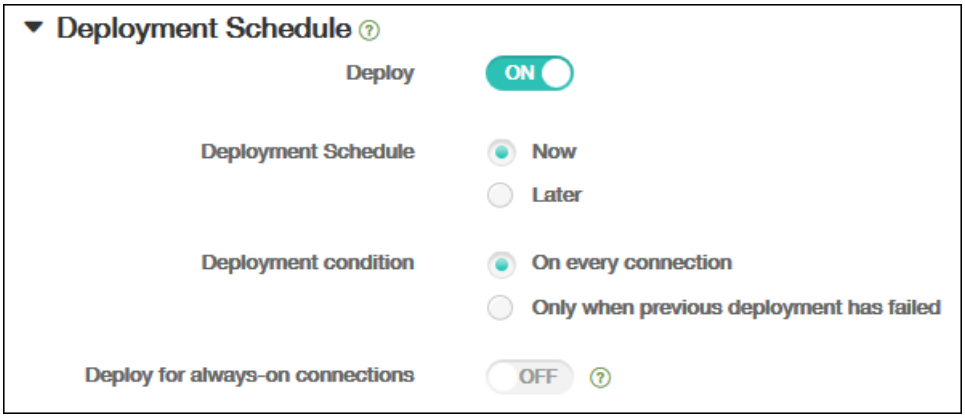
8. Klicken Sie auf Next. Die Seite Assignment für die Roamingrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



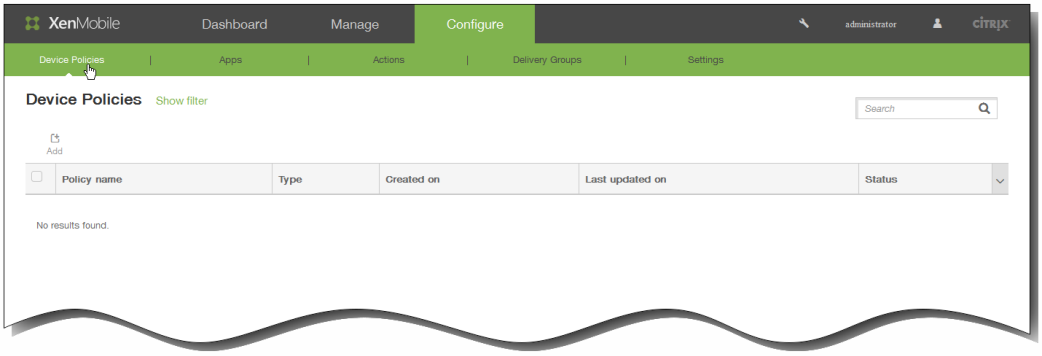
11. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine SCEP-Richtlinie für iOS-Geräte hinzu

Nov 12, 2015

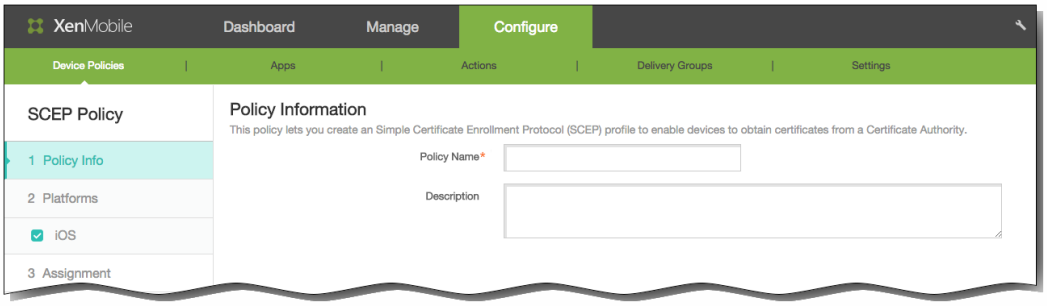
Mit dieser Richtlinie können Sie iOS-Geräte für den Empfang eines Zertifikats über Simple Certificate Enrollment Protocol (SCEP) von einem externen SCEP-Server konfigurieren. Wenn Sie Zertifikate mit SCEP von einer mit XenMobile verbundenen PKI auf Geräten bereitstellen möchten, erstellen Sie eine PKI-Entität und einen PKI-Anbieter im verteilten Modus. Weitere Informationen finden Sie unter PKI-Entitäten.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies.
   Die Seite Device Policies wird angezeigt.



2. Klicken Sie auf Add.
   Die Seite Add a New Policy wird angezeigt.

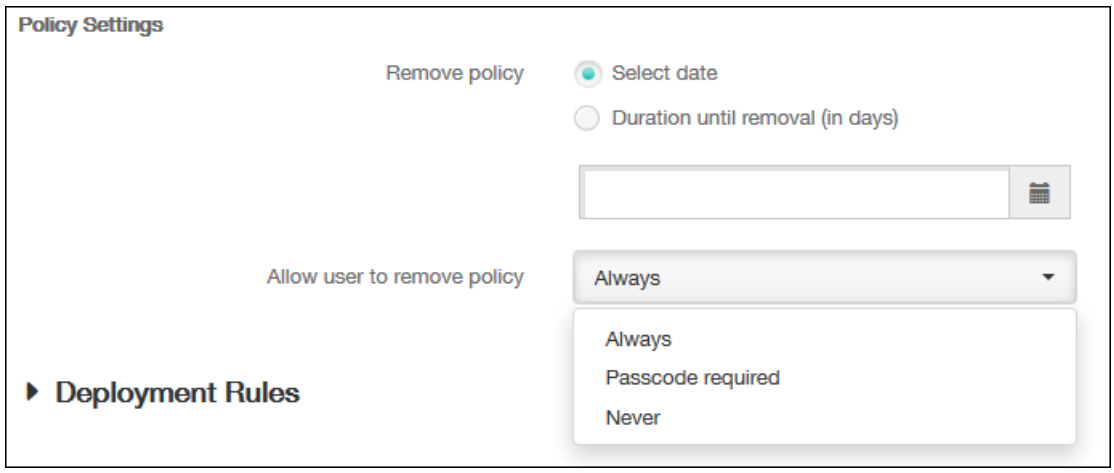
3. Klicken Sie auf der Seite Add a New Policy auf More und dann unter Security auf SCEP.
   Die Seite SCEP Policy wird angezeigt.



4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung für die Richtlinie ein.
5. Klicken Sie auf Next.
   Die Seite iOS Platform Information wird angezeigt.

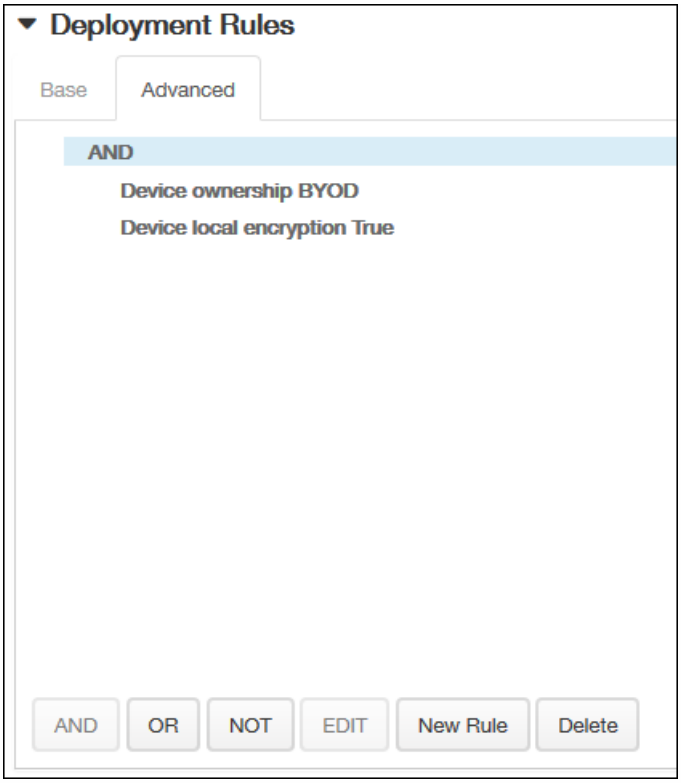
6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:
   1. URL base: Geben Sie die Adresse des SCEP-Servers ein, an den SCEP-Anforderungen über HTTP oder HTTPS gesendet werden. Der private Schlüssel wird nicht mit der Zertifikatsignieranforderung gesendet, daher kann die Anforderung ggf. unverschlüsselt gesendet werden. Wenn das Einmalkennwort jedoch wiederverwendet werden darf, sollten Sie HTTPS zum Schutz des Kennworts verwenden. Dieser Schritt ist erforderlich.
   2. Instance name: Geben Sie eine beliebige Zeichenfolge ein, die der SCEP-Server erkennt. Dies kann beispielsweise ein Domänenname wie "example.org" sein. Wenn eine Zertifizierungsstelle mehrere Zertifizierungsstellenzertifikate hat, können Sie dieses Feld zur Unterscheidung der Domäne verwenden. Dieser Schritt ist erforderlich.
   3. Subject X.500 name (RFC 2253): Geben Sie die Darstellung eines X.500-Namens als Anordnung von Objektbezeichner (OID) und Wert ein. Beispielsweise /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, was folgendermaßen übersetzt würde: [[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]. OIDs können als Zahlen mit Punkten und Abkürzungen für Land (C), Ort (L), Staat (ST), Organisation (O), Organisationseinheit (OU) und Common Name (CN) dargestellt werden.
   4. Klicken Sie in der Liste Subject alternative names type auf einen alternativen Namenstyp. In der SCEP-Richtlinie kann optional ein alternativer Namenstyp definiert sein, der die von der Zertifizierungsstelle für die Ausstellung eines Zertifikats angeforderten Werte bereitstellt. Zur Auswahl stehen None, RFC 822 name, DNS name und URI.
   5. Maximum retries: Geben Sie die zulässige Anzahl Wiederholungen bei Eingabe eines falschen Kennworts an. Der Standardwert ist 3.
   6. Retry delay: Geben Sie ein Intervall an, nach dem bei Überschreiten der maximal zulässigen Anzahl Wiederholungen eine Sperrung erfolgt. Der Standardwert ist 10.
   7. Challenge password: Geben Sie einen gemeinsamen geheimen Schlüssel ein. Dieser Schritt ist erforderlich.
   8. Key size (bits): Klicken Sie in der Liste auf die Schlüsselgröße in Bit (1024 oder 2048). Der Standardwert ist 1024.
   9. Use as digital signature: Geben Sie an, ob das Zertifikat als digitale Signatur verwendet werden soll. Wenn jemand das Zertifikat verwendet, um eine digitale Signatur zu prüfen (z. B., um zu prüfen, ob ein Zertifikat von einer Zertifizierungsstelle ausgestellt wurde), prüft der SCEP-Server, ob das Zertifikat auf diese Weise verwendet werden kann, bevor er den Hashwert mit dem öffentlichen Schlüssel entschlüsselt.
   10. Use for key encipherment: Geben Sie an, ob das Zertifikat für die Schlüsselchiffrierung verwendet werden soll. Bevor ein Server mit dem öffentlichen Schlüssel in einem von einem Client stammenden Zertifikat prüft, ob bestimmte Daten mit dem privaten Schlüssel verschlüsselt wurden, prüft er, ob das Zertifikat zur Schlüsselchiffrierung verwendet werden kann. Sonst kann die Spiegelung nicht durchgeführt werden.
   11. SHA1/MD5 fingerprint (hexadecimal string): Wenn Ihre Zertifizierungsstelle HTTP verwendet, geben Sie hier den Fingerabdruck des CA-Zertifikats an, anhand derer Geräte die Echtheit der Antwort von der Zertifizierungsstelle prüfen. Sie können einen SHA1- oder MD5-Fingerabdruck eingeben oder ein Zertifikat für den Import von dessen Signatur auswählen.
7. Klicken Sie unter Policy Settings für Remove policy auf Select date oder Duration until removal (in days).
8. Bei Auswahl von Select date klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.

9. Klicken Sie in der Liste Allow user to remove policy auf Always, Password required oder Never.
10. Bei Auswahl von Password required geben Sie für Removal password das Kennwort ein.



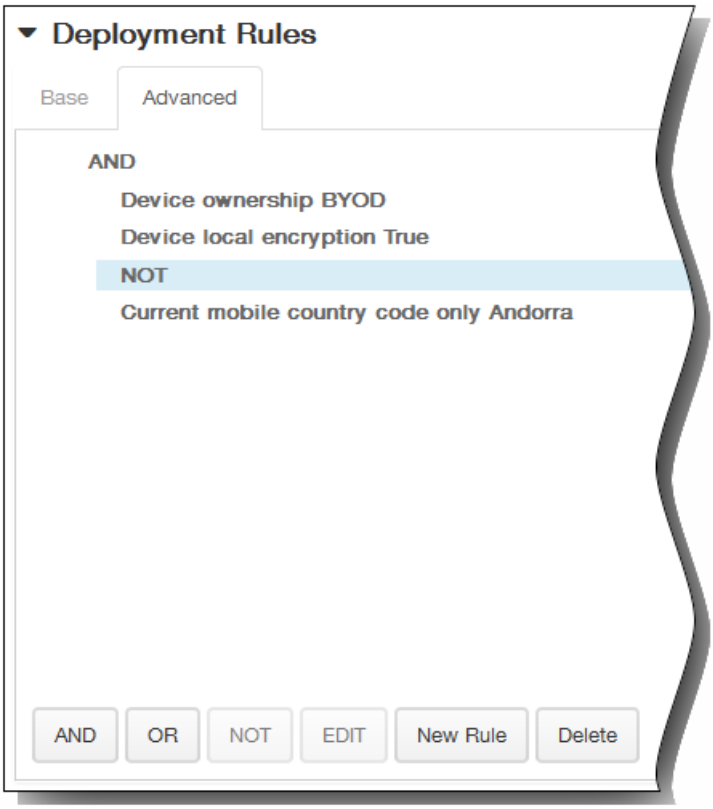
11. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.

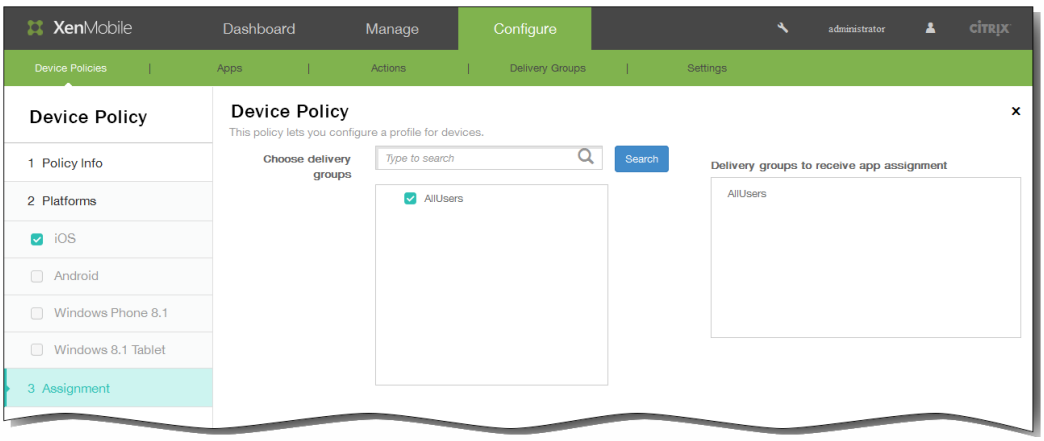


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.
   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



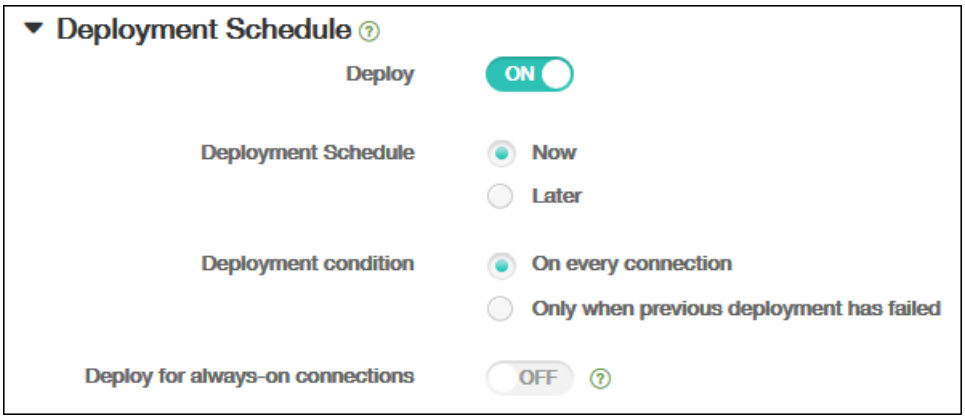
12. Klicken Sie auf Next. Die Seite Assignment für die SCEP-Richtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



14. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.

3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



15. Klicken Sie auf Save, um die Richtlinie zu speichern.

Samsung MDM-Richtlinien für Geräte

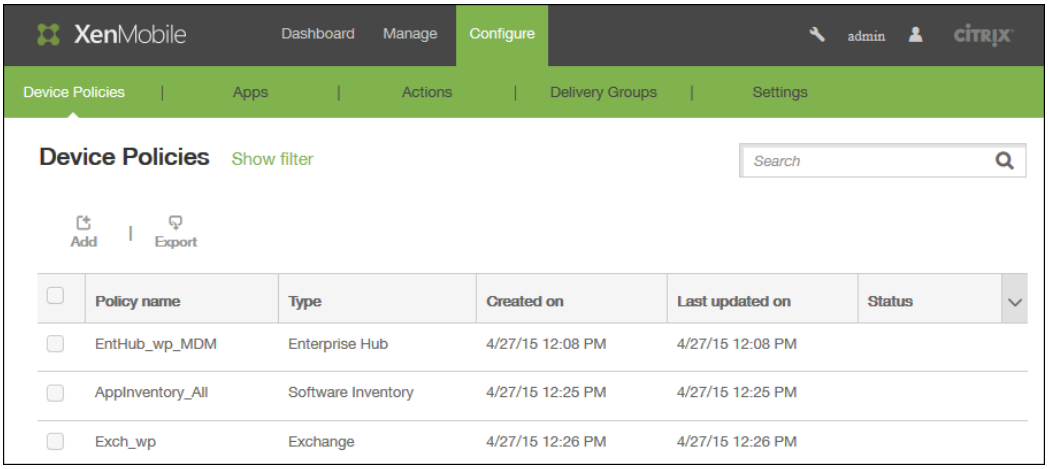
Nov 12, 2015

XenMobile unterstützt und erweitert Samsung for Enterprise- (SAFE) und Samsung KNOX-Richtlinien. SAFE ist eine Serie von Lösungen, die durch die Integration in Lösungen für die Mobilgeräteverwaltung Sicherheit und Featureerweiterungen für Unternehmen bietet. Samsung KNOX ist eine Lösung des SAFE-Programms, die Unternehmen eine sicherere Android-Plattform bietet.

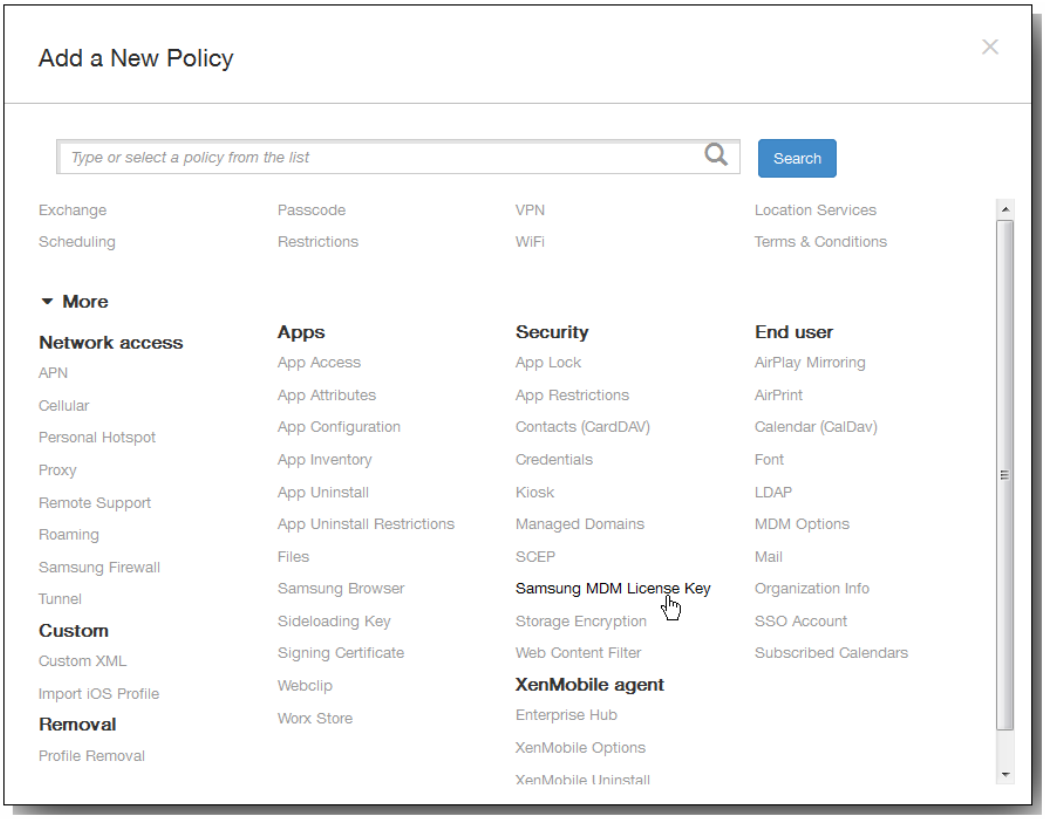
Bevor Sie SAFE-Richtlinien und -Einschränkungen bereitstellen können, müssen Sie die SAFE-APIs durch Bereitstellen des integrierten Samsung Enterprise License Management-Schlüssels (ELM) auf Geräten aktivieren. Zum Aktivieren der Samsung KNOX-API müssen Sie zusätzlich zur Bereitstellung des ELM-Schlüssels über Samsung KNOX License Management System (KLMS) eine Samsung KNOX-Lizenz erwerben. Samsung KLMS liefert gültige Lizenzen für Lösungen zur Mobilgeräteverwaltung, damit über diese die Samsung KNOX-APIs auf Mobilgeräten aktiviert werden können. Diese Lizenzen sind nicht bei Citrix erhältlich, sie müssen bei Samsung erworben werden.

Zum Aktivieren der SAFE- und KNOX-APIs müssen Sie neben dem Samsung ELM-Schlüssel Worx Home bereitstellen. In den Geräteeigenschaften können Sie prüfen, ob die SAFE-APIs aktiviert sind. Ist der Samsung ELM-Schlüssel bereitgestellt, lautet der Wert von "Samsung MDM API available" True.

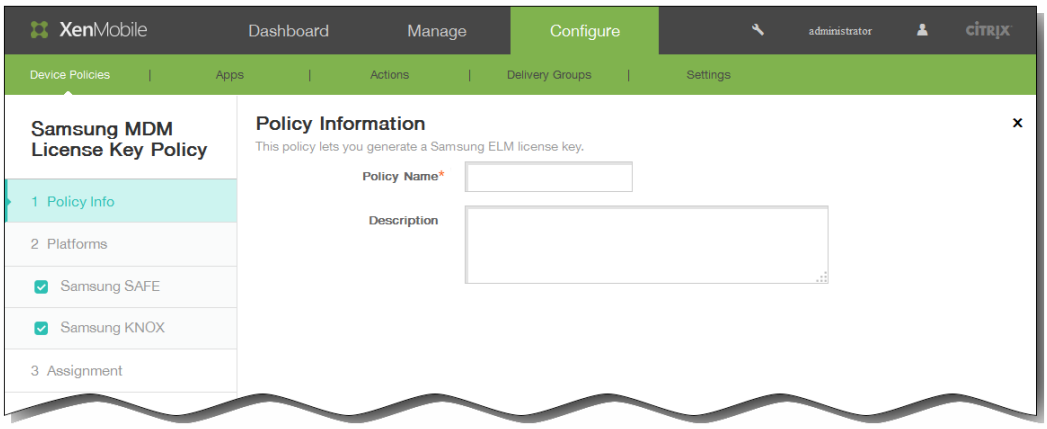
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



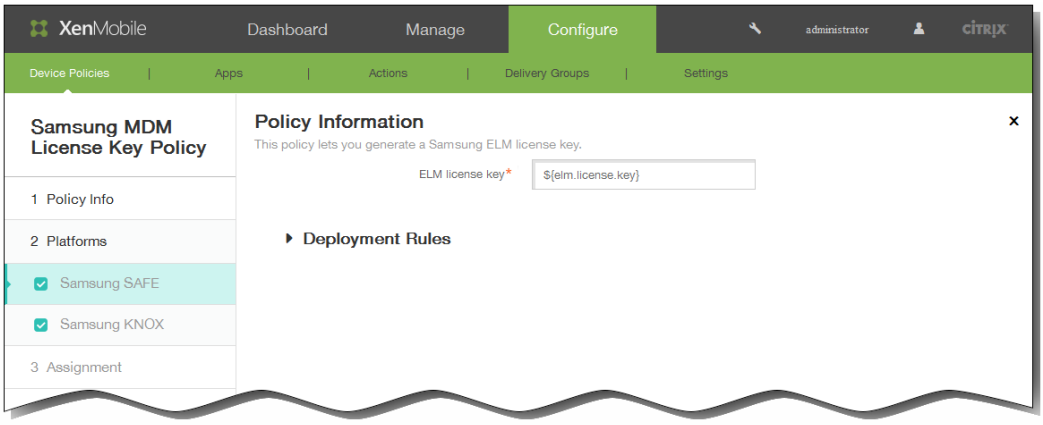
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter Security auf Samsung MDM Licence Key. Die Seite Samsung MDM License Key Policy wird angezeigt.

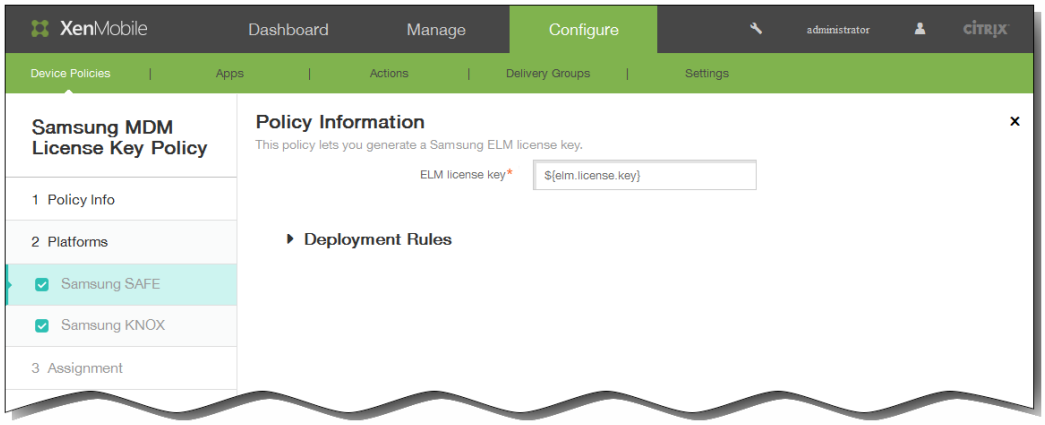


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Policy Platforms wird angezeigt.
   Hinweis: Auf der Seite Policy Platforms sind beide Plattformen ausgewählt, der Konfigurationsbereich für die Samsung SAFE-Plattform wird als erstes angezeigt.

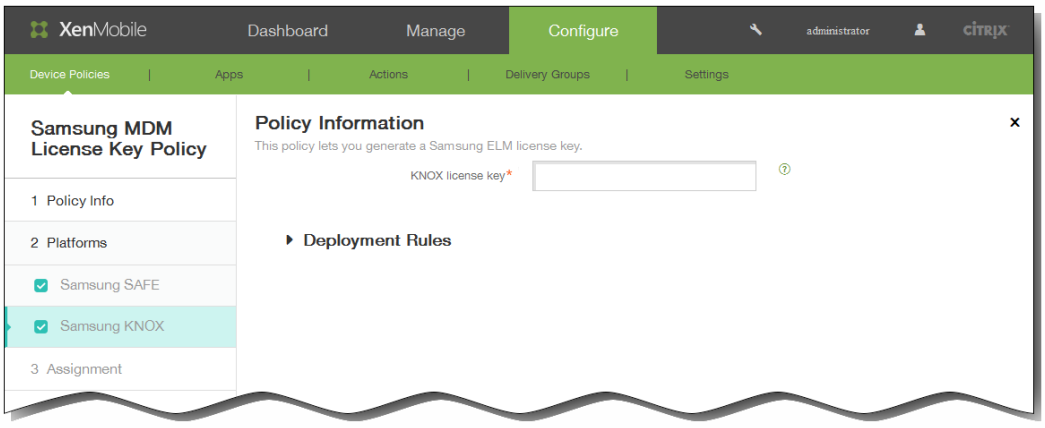


6. Wählen Sie unter Platforms die Samsung-Plattformen aus, für die Sie diese Richtlinie erstellen möchten. Deaktivieren Sie alle Plattformen, die Sie nicht in die Richtlinie einschließen möchten.

   - Bei Auswahl von Samsung SAFE geben Sie für ELM license key das Makro ${elm.license.key} ein, um den ELM-Lizenzschlüssel zu generieren. Das Feld sollte das Makro bereits enthalten:

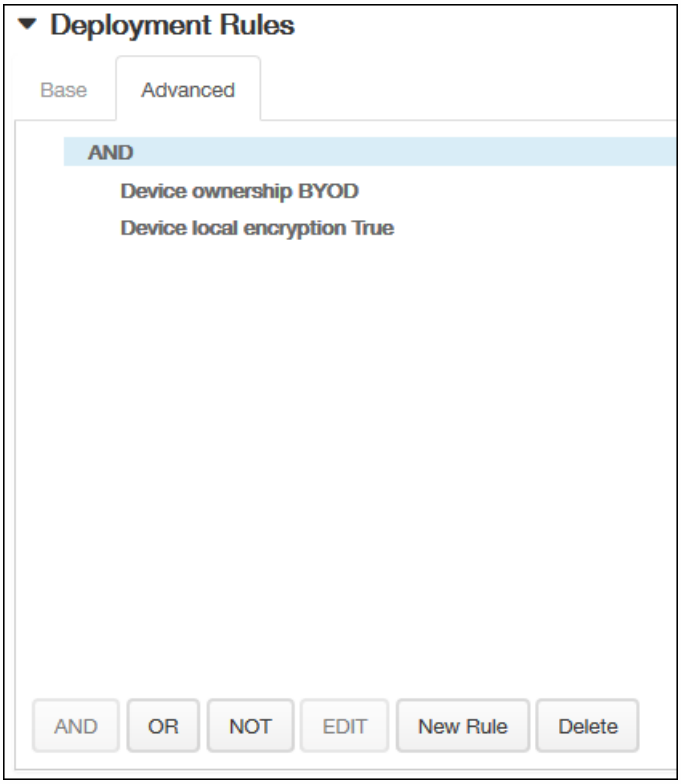


   - Bei Auswahl von Samsung KNOX geben Sie für KNOX license key den 25-stelligen KNOX-Lizenzschlüssel ein:



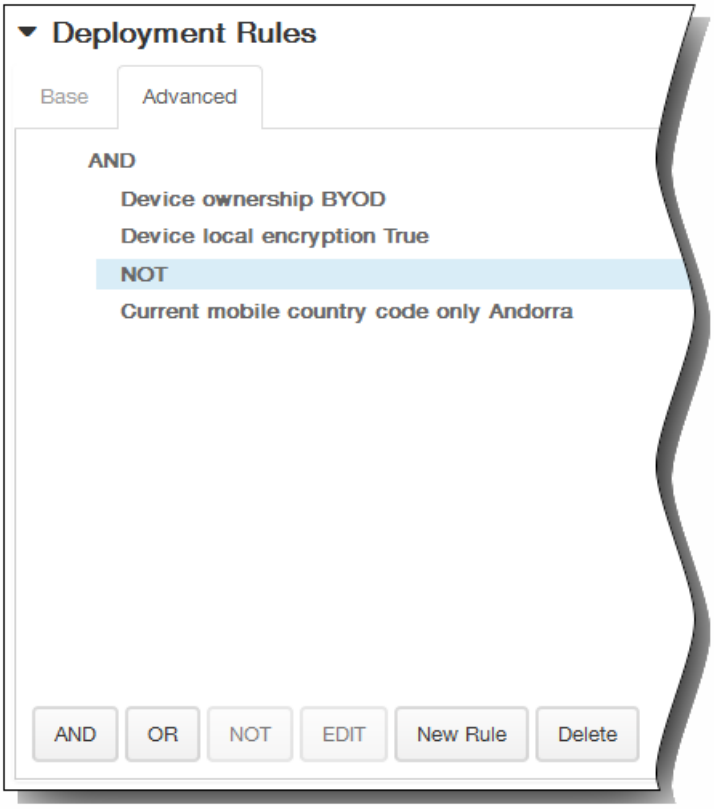
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
   3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
   4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.

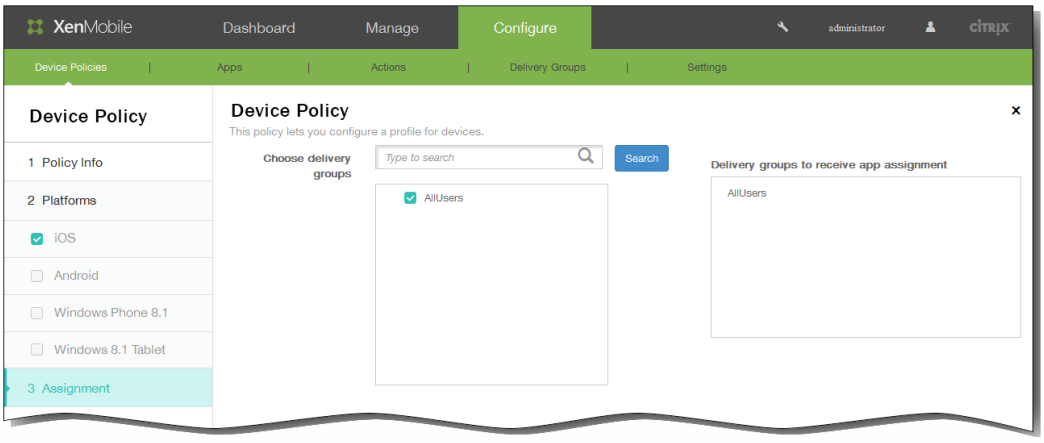


   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.
   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.

In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



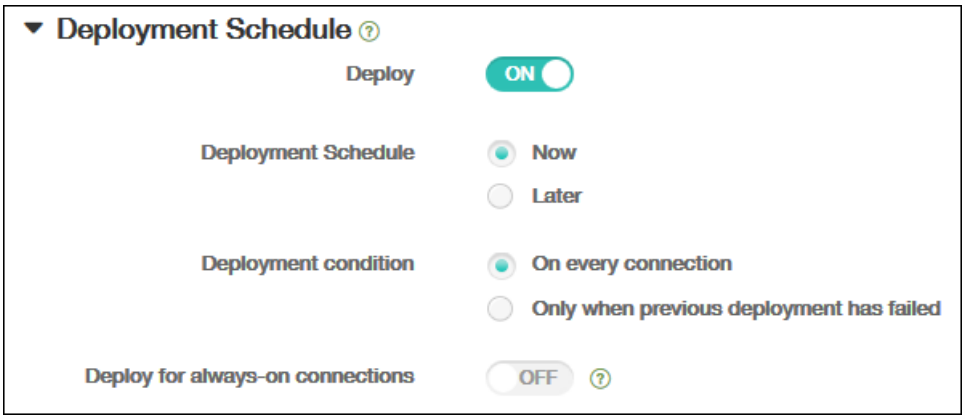
8. Klicken Sie auf Next. Die Seite Samsung MDM License Key Policy wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.

3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



11. Klicken Sie auf Save, um die Richtlinie zu speichern.

Speicherverschlüsselungsrichtlinie für Geräte

Nov 12, 2015

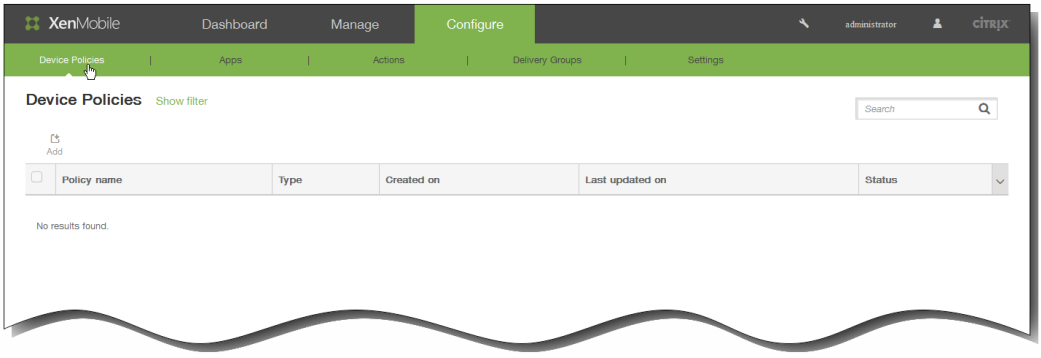
Sie erstellen Speicherverschlüsselungsrichtlinien in XenMobile, um den internen und externen Speicher zu verschlüsseln und – je nach Gerät –, um zu verhindern, dass Benutzer die Gerätespeicherkarte verwenden.

Solche Richtlinien können Sie für Samsung SAFE-, Windows 8.1- und Android-Sony-Geräte erstellen. Jede Plattform erfordert andere Werte. Diese werden in den folgenden Schritten detailliert beschrieben:

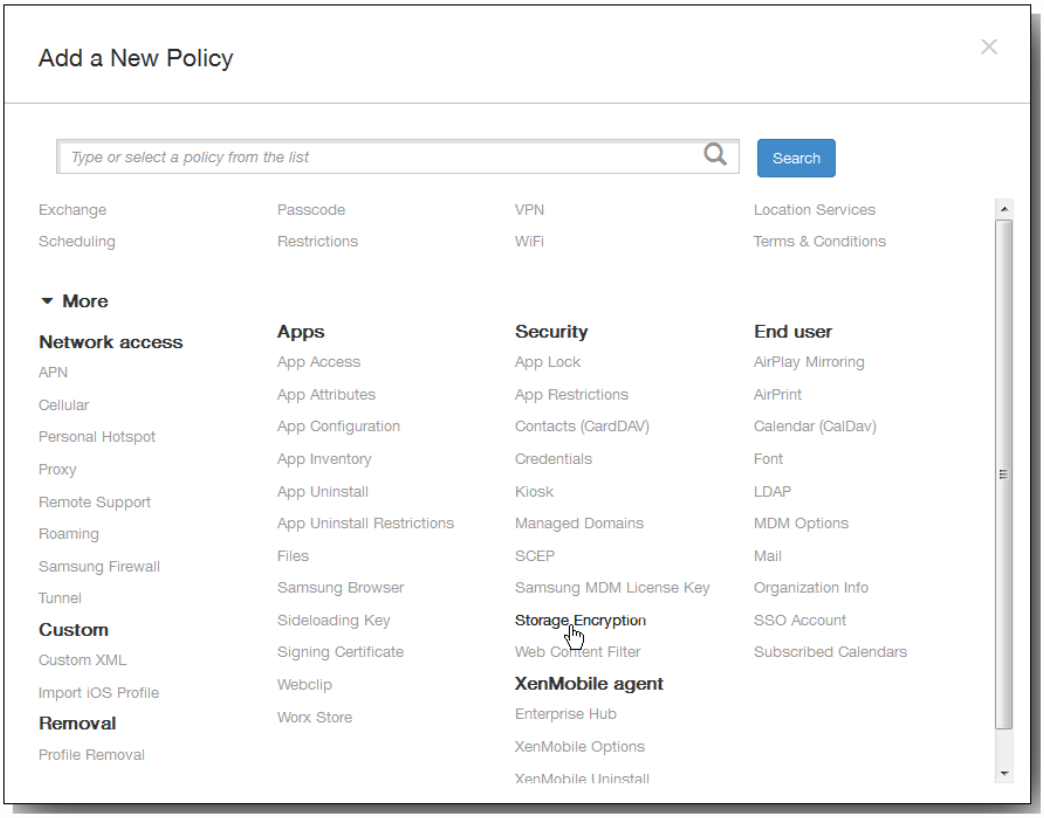
Hinweis: Vergewissern Sie sich vor der Konfiguration dieser Richtlinie, dass bei Samsung SAFE-Geräten die folgenden Anforderungen erfüllt sind:

- Die Bildschirmsperre ist auf den Geräten der Benutzer aktiviert.
- Die Geräte müssen am Netz angeschlossen und zu 80 Prozent aufgeladen sein.
- Für das Gerät muss ein Kennwort mit Zahlen und Buchstaben oder Symbolen erforderlich sein.

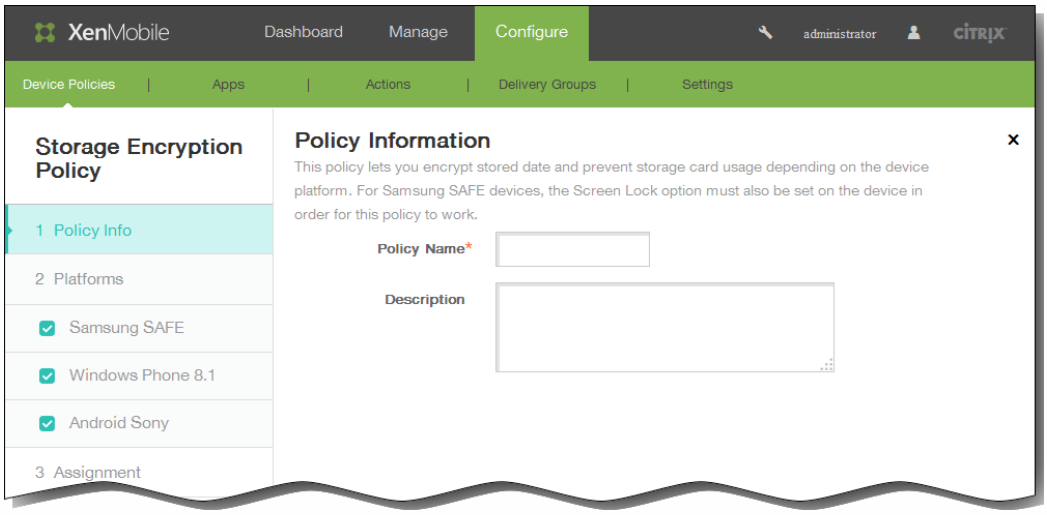
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add New Policy wird angezeigt.

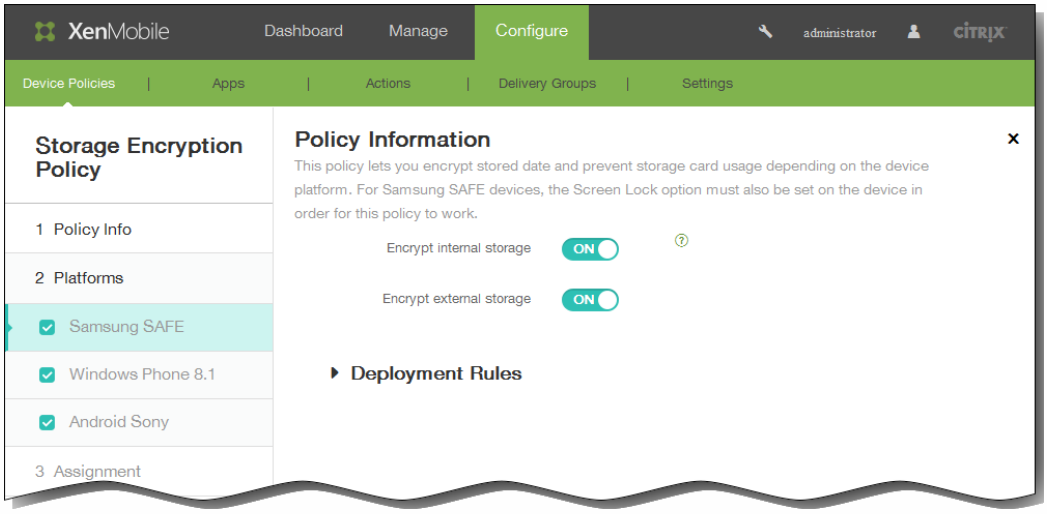


3. Klicken Sie auf More und dann unter Security auf Storage Encryption. Die Seite Storage Encryption Policy wird angezeigt.

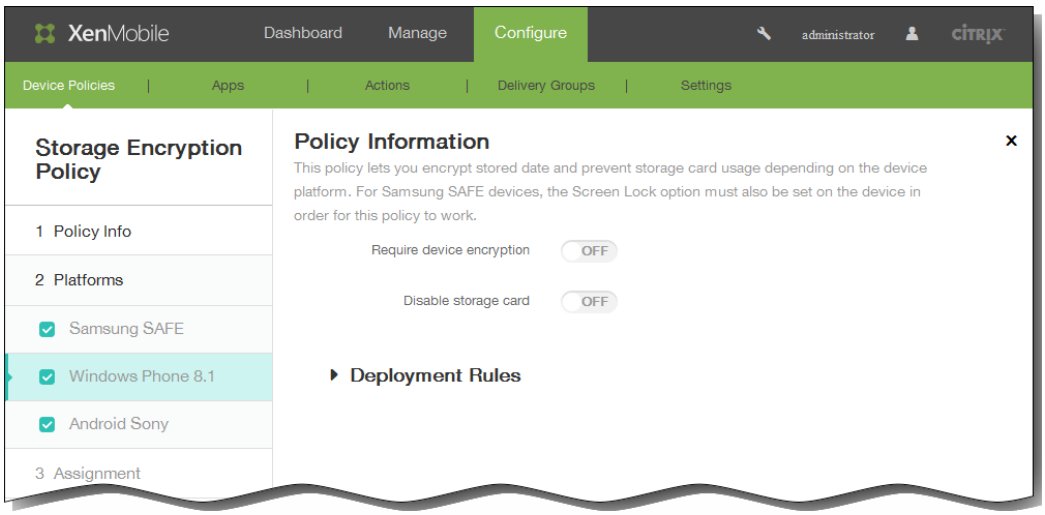


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Policy Platforms wird angezeigt.
   Hinweis: Auf der Seite Policy Platforms sind alle Plattformen ausgewählt, der Konfigurationsbereich für die Samsung SAFE-Plattform wird als erstes angezeigt.

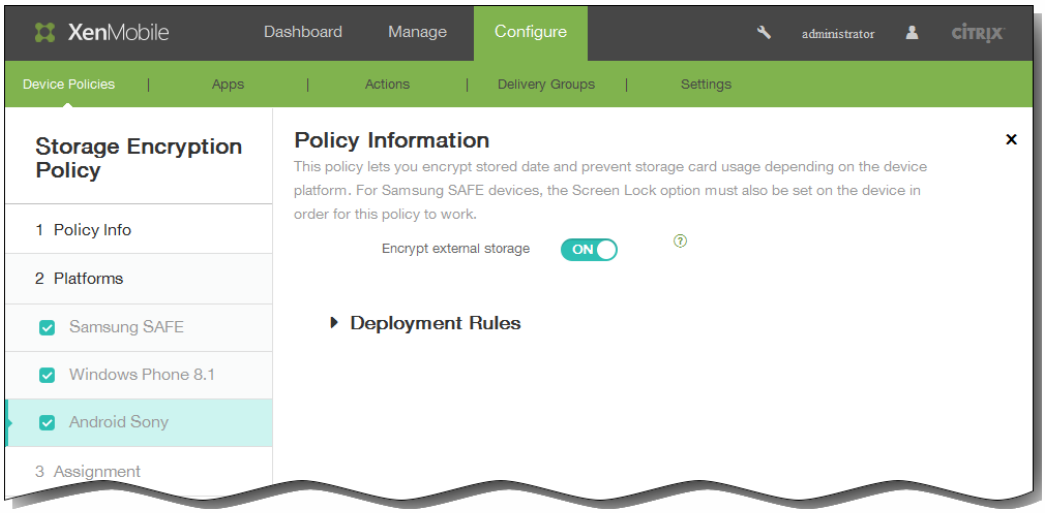
6. Wählen Sie unter Platforms die Plattformen aus, für die Sie diese Richtlinie konfigurieren möchten. Deaktivieren Sie alle anderen ggf. ausgewählten Plattformen.
   - Bei Auswahl von Samsung SAFE:
     - Encrypt internal storage: Wählen Sie aus, ob der interne Speicher auf Geräten verschlüsselt werden soll. Zum internen Speicher gehört auch der Gerätespeicher. Die Standardeinstellung ist ON.
     - Encrypt external storage: Wählen Sie aus, ob der externe Speicher auf Geräten verschlüsselt werden soll. Die Standardeinstellung ist ON.



   - Bei Auswahl von Windows Phone 8.1:
     - Require device encryption: Wählen Sie aus, ob die Geräte der Benutzer verschlüsselt werden sollen. Der Standardwert ist OFF.
     - Disable storage card: Wählen Sie aus, ob die Verwendung der Speicherkarte der Geräte unterbunden werden soll. Der Standardwert ist OFF.

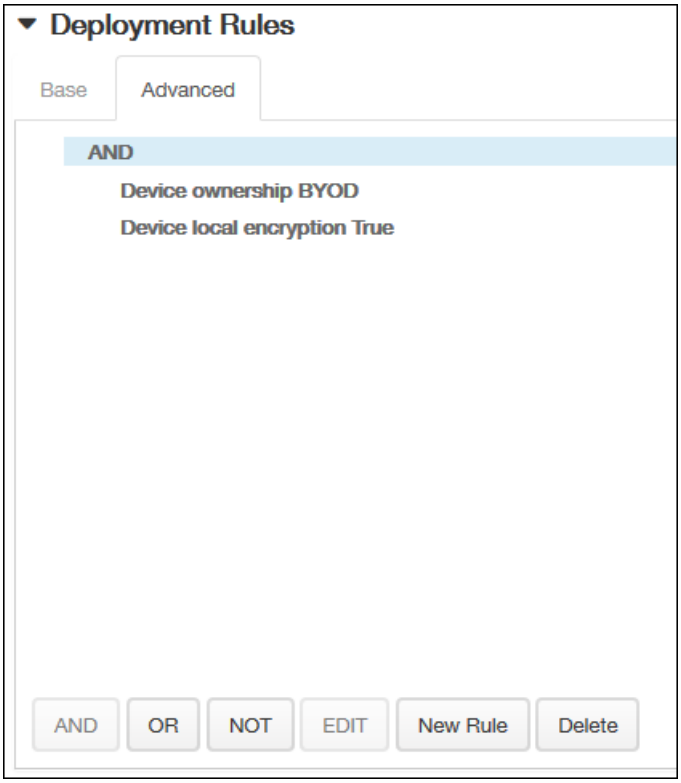


   - Wenn Sie Android Sony ausgewählt haben, wählen Sie für Encrypt external storage aus, ob der externe Speicher auf Geräten verschlüsselt werden soll. Für das Gerät muss ein Kennwort mit Zahlen und Buchstaben oder Symbolen erforderlich sein. Die Standardeinstellung ist ON.



7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

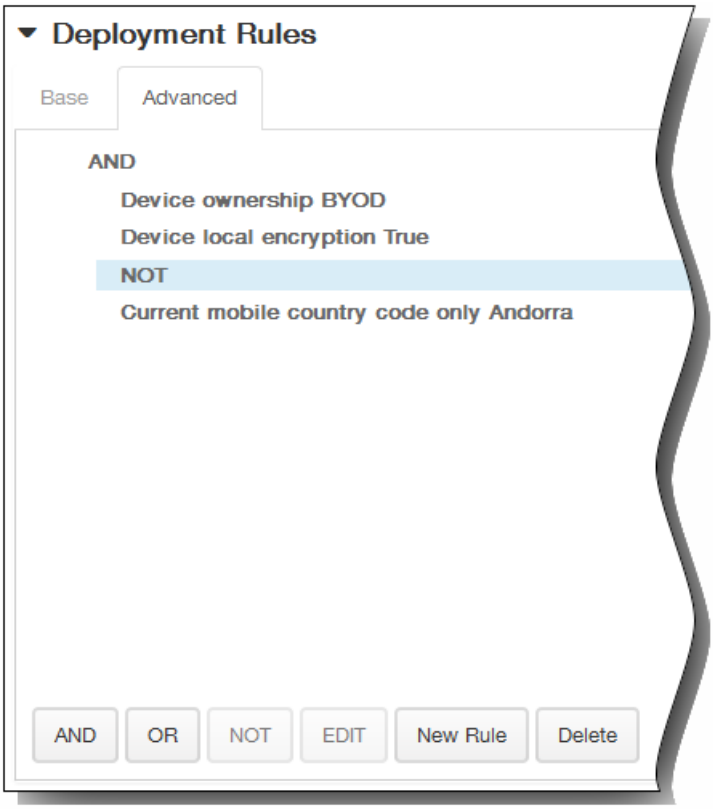
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



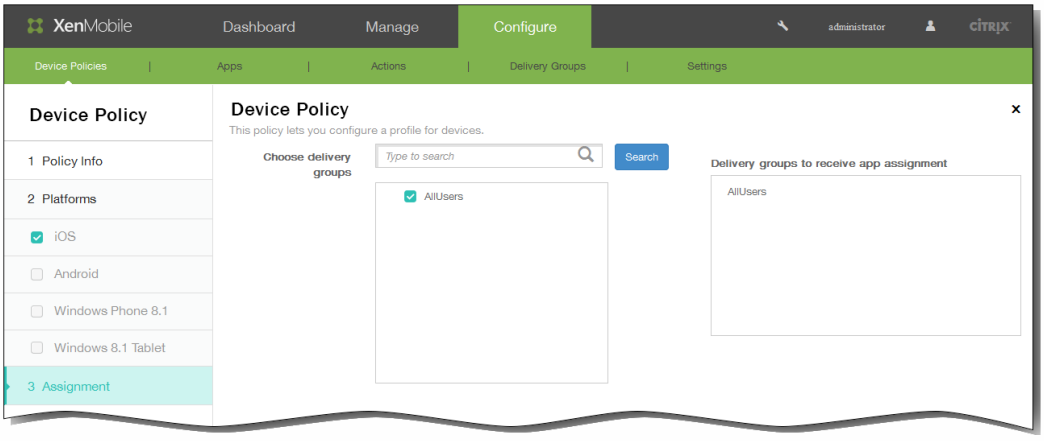
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



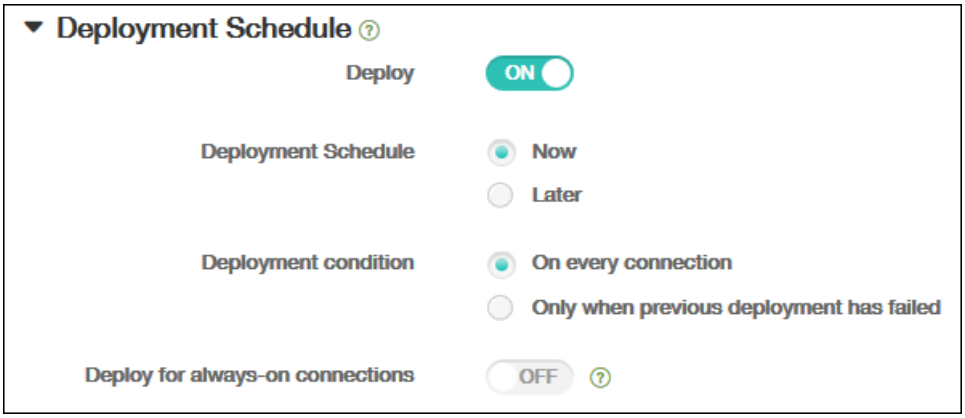
8. Klicken Sie auf Next. Die Seite Assignment für die Speicherverschlüsselungsrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



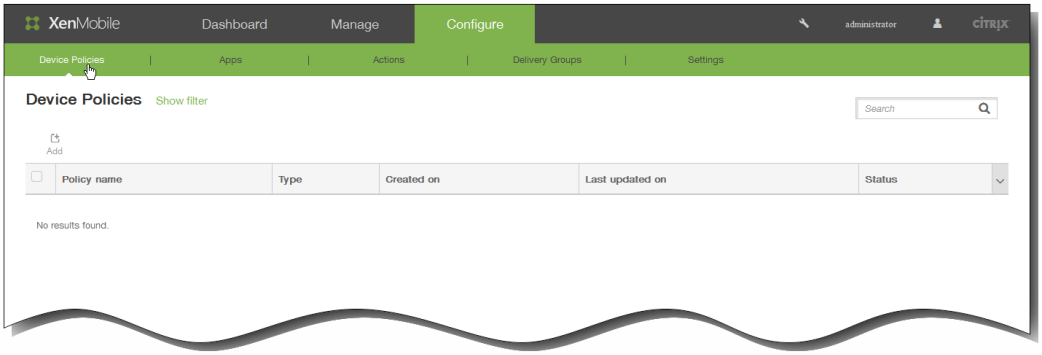
11. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Webinhaltsrichtlinie für iOS-Geräte hinzu

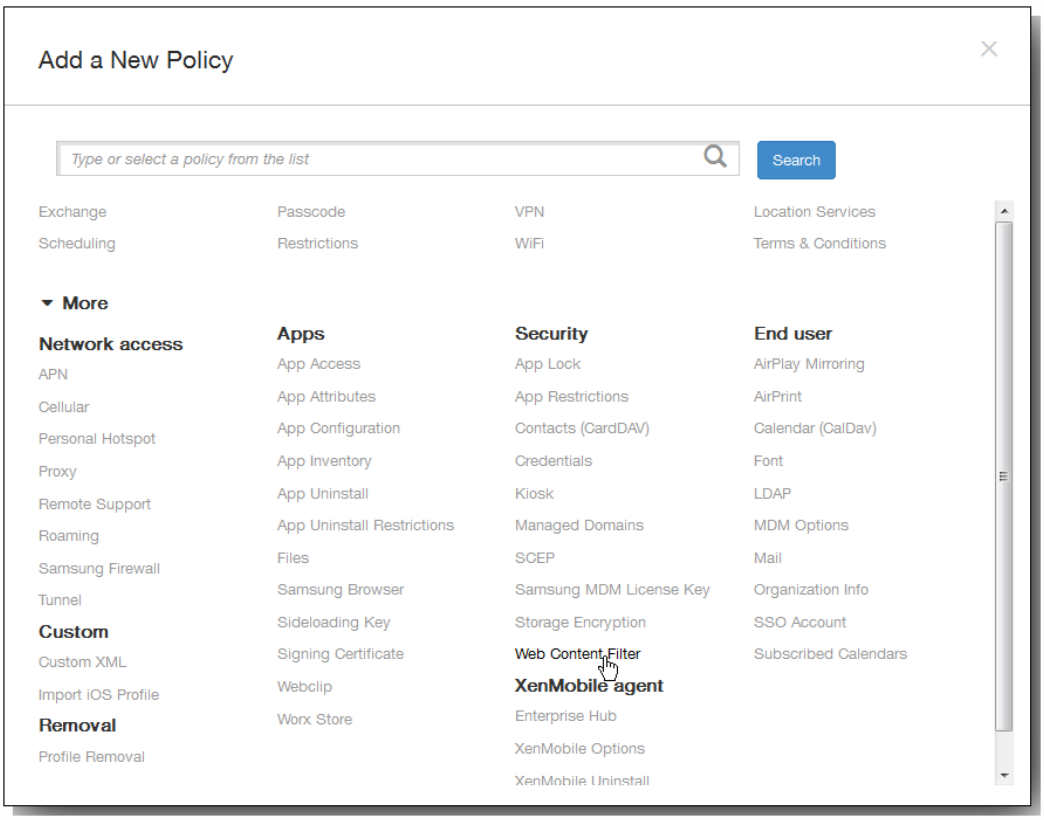
Nov 12, 2015

Sie können in XenMobile eine Geräterichtlinie zum Filtern von Webinhalt auf iOS-Geräten mit der automatischen Filterfunktion von Apple in Verbindung mit Ihren Website-Positivlisten und -Sperrlisten hinzufügen. Diese Richtlinie gilt nur für iOS 7.0 und höher im betreuten Modus. Informationen, wie Sie Geräte in den betreuten Modus versetzen finden Sie unter So versetzen Sie ein iOS-Gerät mit dem Apple Configurator in den betreuten Modus.

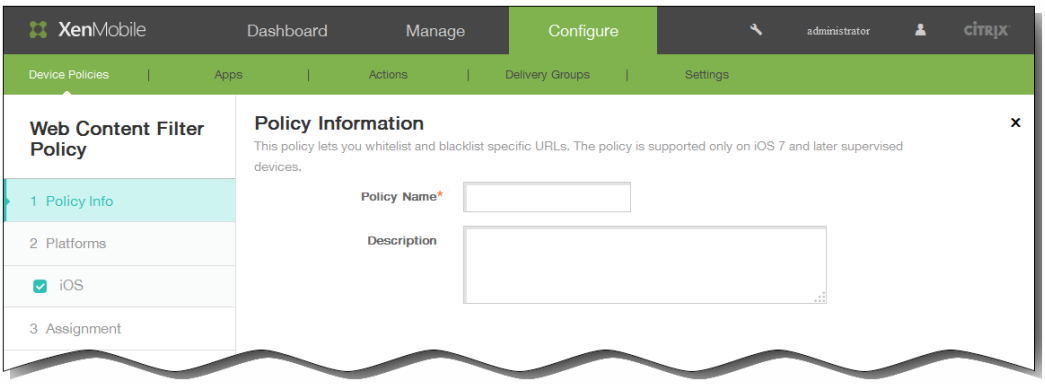
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



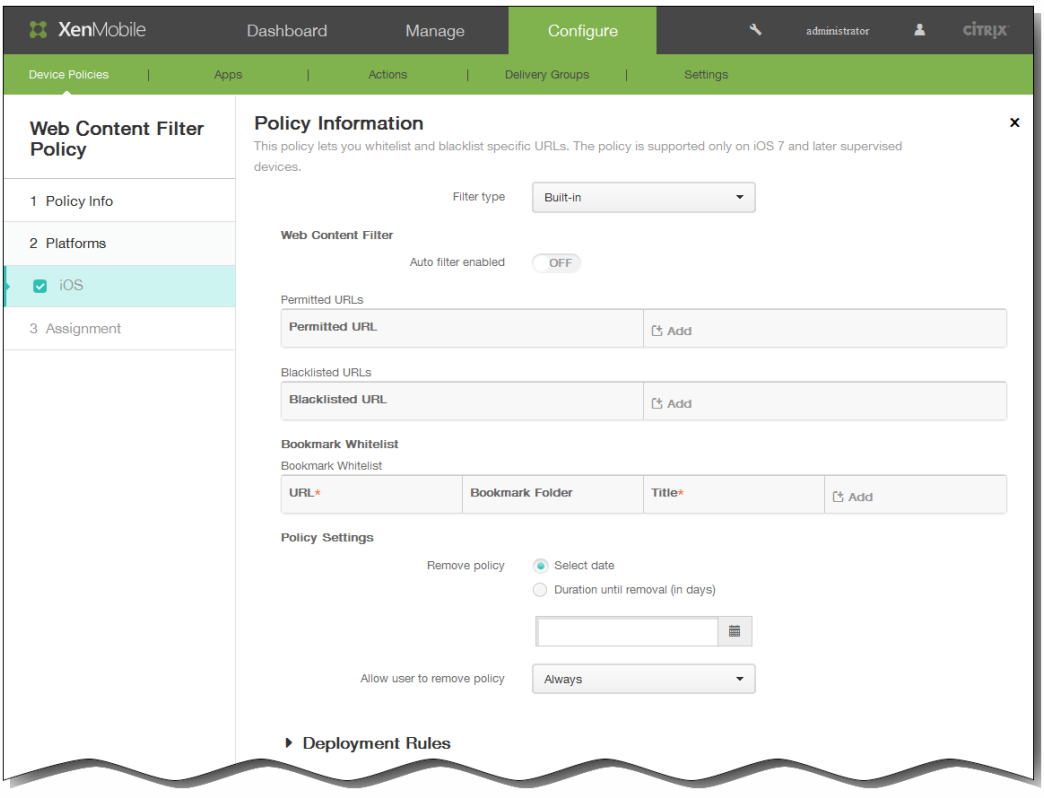
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter Security auf Web Content Filter. Die Seite Web Content Filter Policy wird angezeigt.



4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite iOS Platform wird angezeigt.



6. Treffen Sie auf der Seite iOS Platform Information in der Liste Filter type eine Auswahl wie folgt und folgen Sie dann den jeweils relevanten Anweisungen weiter unten:
   - Behalten Sie den Standardfiltertyp Built-in bei.

- Klicken Sie auf Plug-in, um den Plug-In-Filter zu bearbeiten.

So konfigurieren Sie den integrierten Filter

1. Auto filter enabled: Wählen Sie aus, ob der automatische Filter von Apple zum Analysieren von Websites auf nicht geeigneten Inhalt verwendet werden soll. Der Standardwert ist OFF.
2. Permitted URLs: Diese Liste wird ignoriert, wenn Auto filter enabled auf OFF festgelegt ist. Wenn Auto filter enabled auf ON festgelegt ist, besteht immer Zugriff auf die Elemente in dieser Liste, unabhängig davon, ob der automatische Filter einen Zugriff zulässt.
   Klicken Sie auf Add und führen Sie folgende Schritte aus, um Websites zu der Positivliste hinzuzufügen:

   1. Geben Sie die URL der zulässigen Website ein. Die URL muss mit "http://" bzw. "https://" beginnen.
   2. Klicken Sie auf Save, um die Website der Positivliste hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
   3. Wiederholen Sie die Schritte i und ii für jede Website, die Sie der Positivliste hinzufügen möchten.
3. Blacklisted URLs: Elemente in dieser Liste werden immer blockiert.
   Klicken Sie auf Add und führen Sie folgende Schritte aus, um Websites zu der Sperrliste hinzuzufügen:

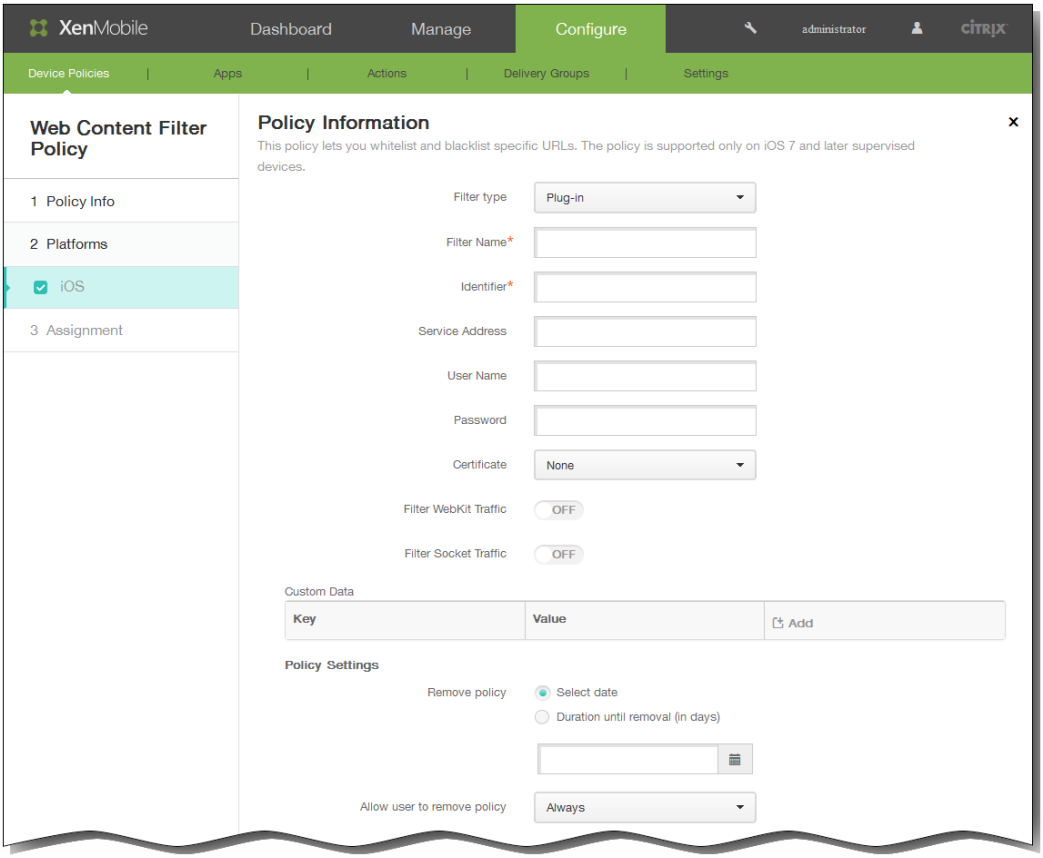
   1. Geben Sie die URL der Website ein, die gesperrt werden soll. Die URL muss mit "http://" bzw. "https://" beginnen.
   2. Klicken Sie auf Save, um die Website der Sperrliste hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
   3. Wiederholen Sie die Schritte i und ii für jede Website, die Sie der Sperrliste hinzufügen möchten.
4. Bookmark whitelist: Die Elemente in dieser Liste sind die einzigen Websites, auf die Benutzer zugreifen können.
   Klicken Sie auf Add und führen Sie folgende Schritte aus, um Lesezeichen für Websites hinzuzufügen:

   1. URL: Geben Sie die URL der Website ein, für die ein Lesezeichen hinzugefügt werden soll. Die URL muss mit "http://" bzw. "https://" beginnen. Diese Angabe ist erforderlich.
   2. Bookmark folder: Geben Sie optional den Namen eines Lesezeichenordners ein. Wenn dieses Feld leer bleibt, wird das Lesezeichen in den Standardlesezeichenordner eingefügt.
   3. Title: Geben Sie einen aussagekräftigen Titel für die Website ein. Beispiel "Google" für die URL "http://google.com".
   4. Klicken Sie auf Save, um die Website der Sperrliste hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
   5. Wiederholen Sie die Schritte i bis iv für jede Website, für die Sie ein Lesezeichen hinzufügen möchten.

   Hinweis: Zum Löschen einer vorhandenen Website zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf Delete zum Löschen des Eintrags oder auf Edit, um ihn beizubehalten.
   Zum Bearbeiten einer Website zeigen Sie auf deren Zeile und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf Save, um die Änderungen zu speichern oder auf Cancel, um den Vorgang abzubrechen.

5. Zum Abschließen der Konfiguration des integrierten Filters siehe Schritt 7.

So konfigurieren Sie den Plug-In-Filter



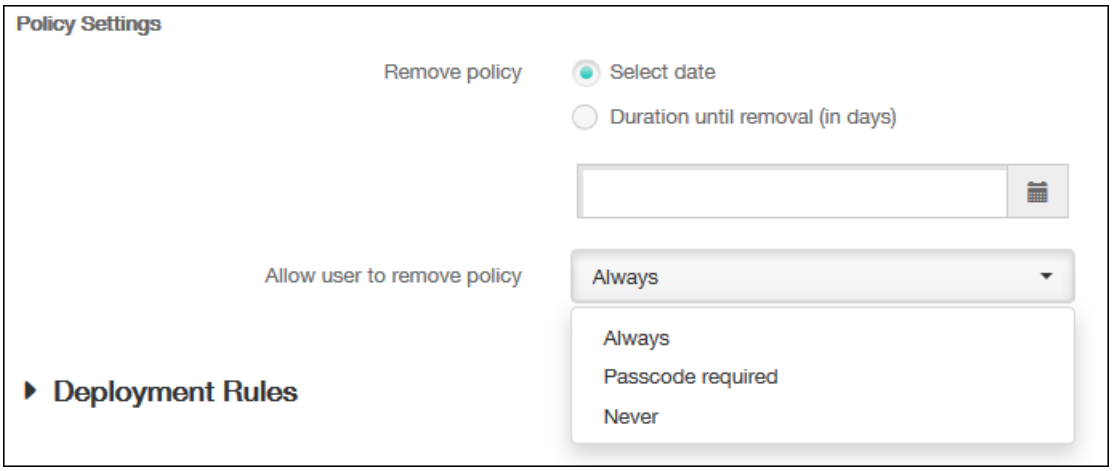
1. Filter name: Geben Sie einen eindeutigen Namen für den Filter ein.
2. Identifier: Geben Sie die Paket-ID des Filterdienst-Plug-Ins ein.
3. Service address: Geben Sie optional eine Serveradresse ein. Gültige Formate sind IP-Adressen, Hostnamen oder URLs.
4. User name: Geben Sie optional einen Benutzernamen für den Dienst ein.
5. Password: Geben Sie optional ein Kennwort für den Dienst ein.
6. Certificate: Wählen Sie in der Liste optional ein Identitätszertifikat aus, das für die Authentifizierung des Benutzers bei dem Dienst verwendet werden soll. Der Standardwert ist None.
7. Filter WebKit traffic: Wählen Sie aus, ob WebKit-Datenverkehr gefiltert werden soll.
8. Filter Socket traffic: Wählen Sie aus, ob Socket-Datenverkehr gefiltert werden soll.
9. Custom Data: Klicken Sie auf Add und führen Sie die folgenden Schritte aus, um dem Webinhaltsfilter benutzerdefinierte Daten hinzuzufügen:
   1. Key: Geben Sie den benutzerdefinierten Schlüssel ein.
   2. Value: Geben Sie einen Wert für den benutzerdefinierten Schlüssel ein.
   3. Klicken Sie auf Save, um den benutzerdefinierten Schlüssel zu speichern, oder auf Cancel, um den Vorgang abzubrechen.
   4. Wiederholen Sie die Schritte i bis iii für jeden benutzerdefinierten Schlüssel, den Sie hinzufügen möchten.

   Hinweis: Zum Löschen eines vorhandenen Schlüssels zeigen Sie auf dessen Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf Delete zum Löschen des Eintrags oder auf Edit, um ihn beizubehalten.

   Zum Bearbeiten eines Schlüssels zeigen Sie auf dessen Zeile und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf Save, um die Änderungen zu speichern oder auf Cancel, um den Vorgang abzubrechen.

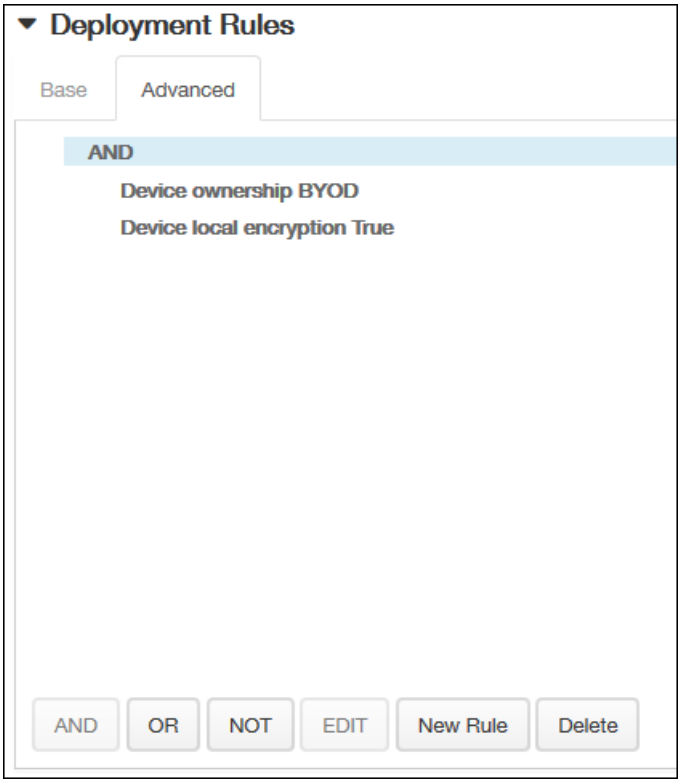
7. Klicken Sie unter Policy Settings für Remove policy auf Select date oder Duration until removal (in days).

8. Bei Auswahl von Select date klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
9. Klicken Sie in der Liste Allow user to remove policy auf Always, Password required oder Never.
10. Bei Auswahl von Password required geben Sie für Removal password das Kennwort ein.



11. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

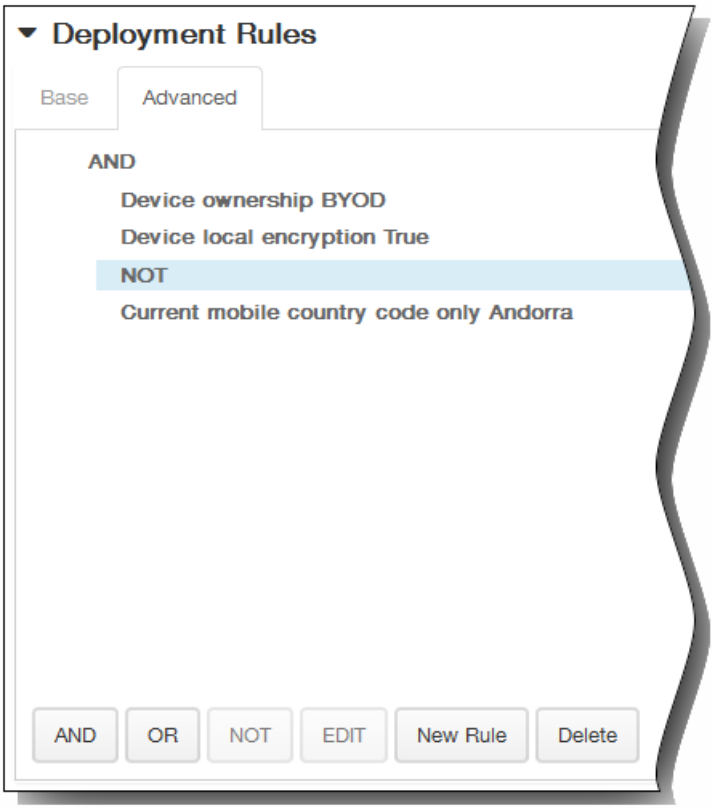
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



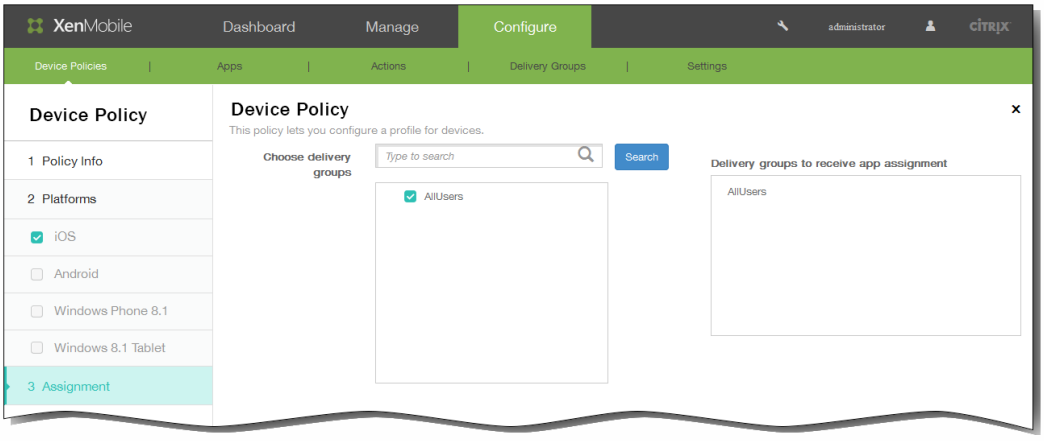
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



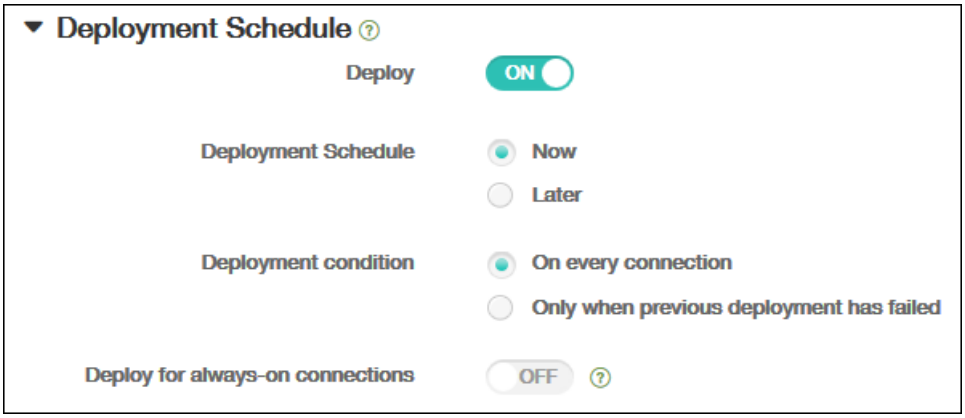
12. Klicken Sie auf Next. Die Seite Assignment für die Webinhaltsfilterrichtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



14. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



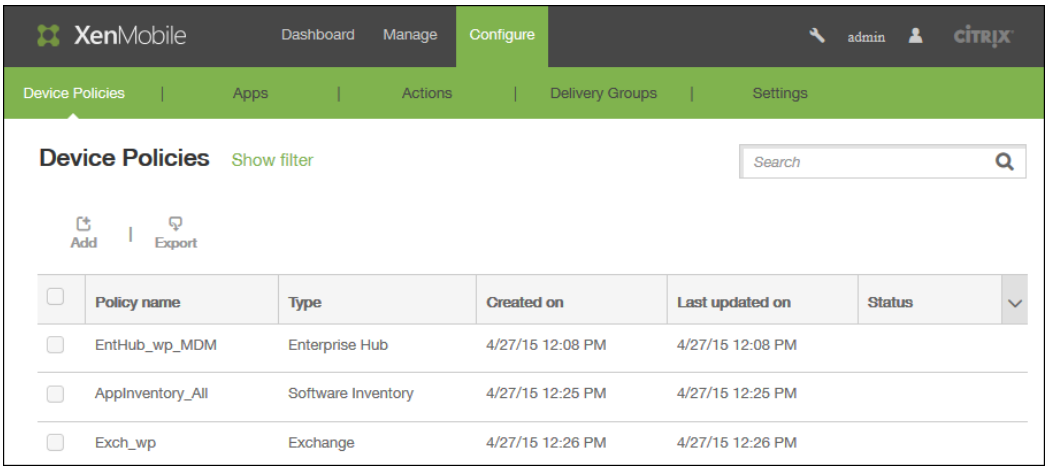
15. Klicken Sie auf Save, um die Richtlinie zu speichern.

Browserrichtlinien für Geräte

Nov 12, 2015

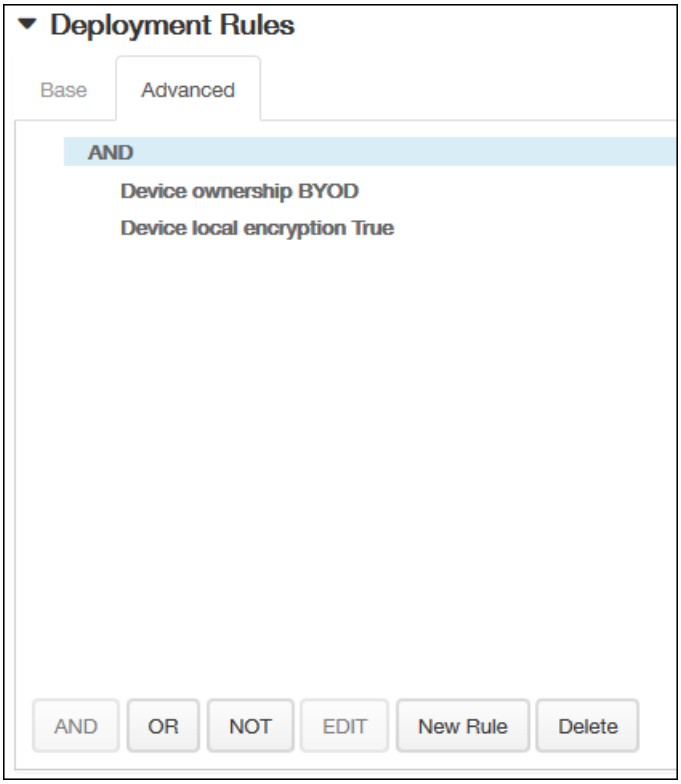
Sie können Browserrichtlinien für Samsung SAFE- und Samsung KNOX-Geräte erstellen, um festzulegen, ob die Benutzer den Browser verwenden können, oder um die Browserfunktionen einzuschränken, die auf den Geräten verwendet werden können. Sie können den Browser vollständig deaktivieren oder Popupfenster, JavaScript, Cookies, automatisches Ausfüllen und Betrugswarnungen aktivieren oder deaktivieren.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



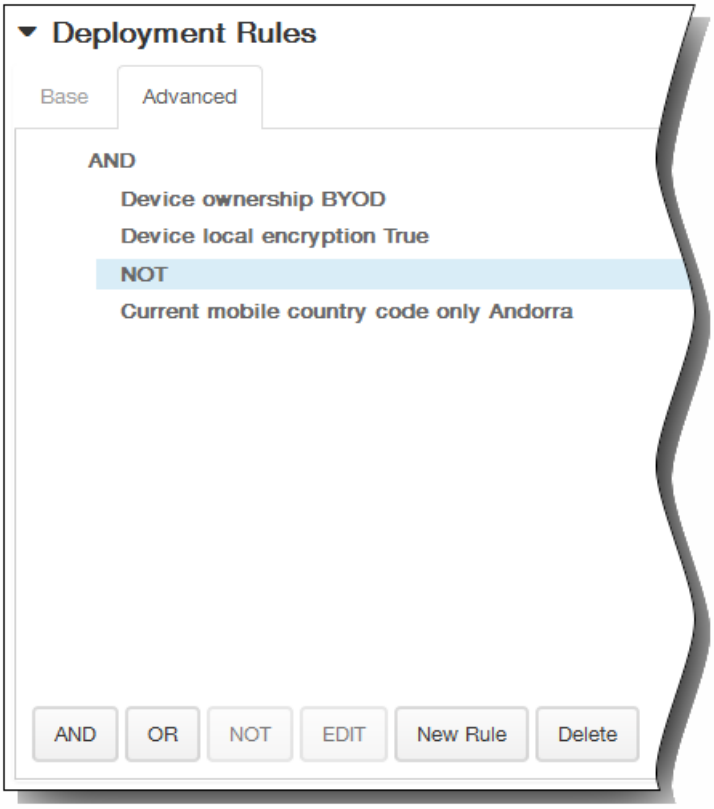
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add New Policy wird angezeigt.
3. Klicken Sie auf More und dann unter Apps auf Samsung Browser. Die Seite Samsung Browser Policy wird angezeigt.
4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Policy Platforms wird angezeigt.
   Hinweis: Auf der Seite Policy Platforms sind beide Plattformen ausgewählt, der Konfigurationsbereich für die Samsung SAFE-Plattform wird als erstes angezeigt.
6. Wählen Sie unter Platforms die gewünschten Samsung-Plattformen aus. Wenn Sie nur eine Plattform konfigurieren möchten, deaktivieren Sie die andere und legen Sie die folgenden Einstellungen fest:
   1. Disable browser: Wählen Sie aus, ob der Samsung-Browser auf den Geräten komplett deaktiviert werden soll. Der Standardwert ist OFF, d. h. die Benutzer können den Browser verwenden. Wenn Sie den Browser deaktivieren, werden die nachfolgend aufgeführten Optionen ausgeblendet.
   2. Disable pop-up: Wählen Sie aus, ob Popupfenster im Browser zugelassen werden sollen.
   3. Disable JavaScript: Wählen Sie aus, ob die Ausführung von JavaScript im Browser zugelassen werden soll.
   4. Disable cookies: Wählen Sie aus, ob Cookies zugelassen werden sollen.
   5. Disable autofill: Wählen Sie aus, ob die Funktion zum automatischen Ausfüllen im Browser aktiviert werden soll.
   6. Force fraud warning: Wählen Sie aus, ob eine Warnung angezeigt werden soll, wenn Benutzer eine betrügerische oder manipulierte Website besuchen.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
   3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
   4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



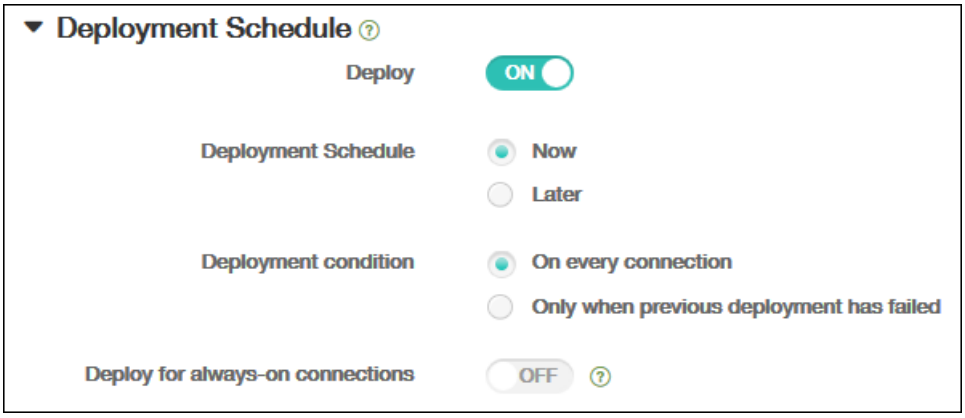
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.
   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.

In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



8. Klicken Sie auf Next. Die Seite Samsung Browser Device Policy wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.
10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
    4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
    5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
    Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

    Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



11. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Sideloadingrichtlinie für Windows 8.1-Tablets hinzu

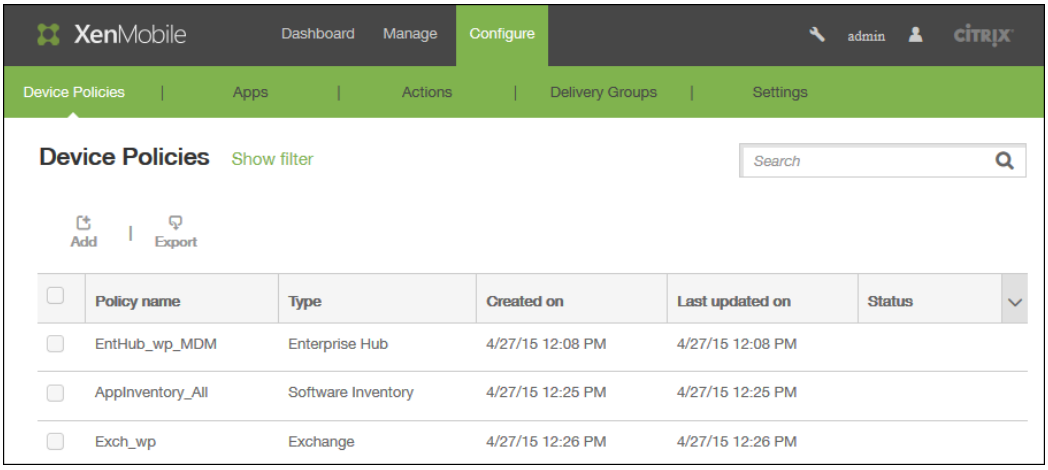
Nov 12, 2015

Durch Sideloading können Sie in XenMobile Apps auf Windows 8.1-Geräten bereitstellen, die nicht beim Windows Store erworben wurden. Häufig werden Apps per Sideloading bereitgestellt, die für die Verwendung im Unternehmen entwickelt wurden und nicht im Windows Store veröffentlicht werden sollen. Für das Sideloading konfigurieren Sie den Sideloadingschlüssel und die Schlüsselaktivierungen und stellen die Apps dann auf den Geräten der Benutzer bereit.

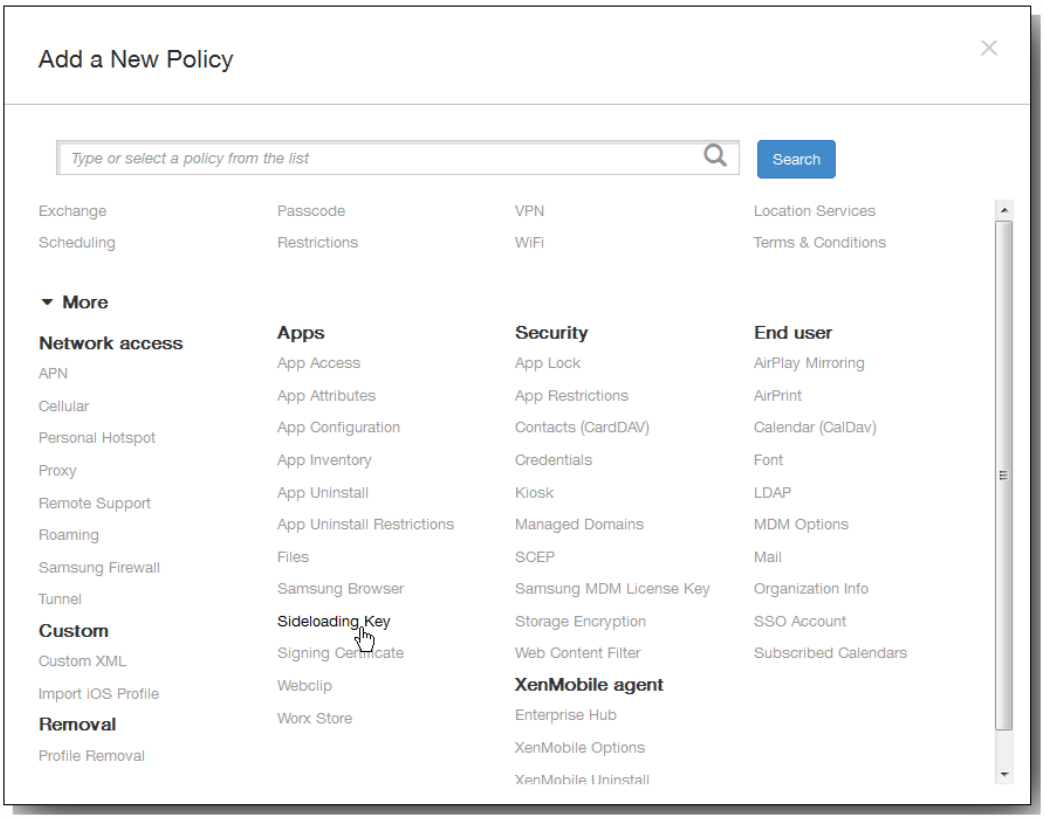
Sie benötigen zum Erstellen der Richtlinie die folgenden Informationen:

- Sideloading-Produktschlüssel, den Sie durch Anmeldung beim Microsoft Volume Licensing Service Center erhalten
- Schlüsselaktivierung, die Sie nach Erhalt des Sideloading-Produktschlüssels über die Befehlszeile erstellen

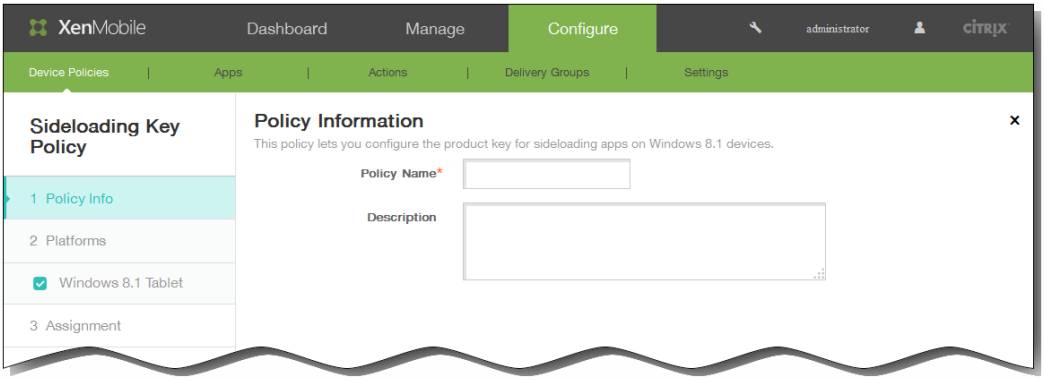
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



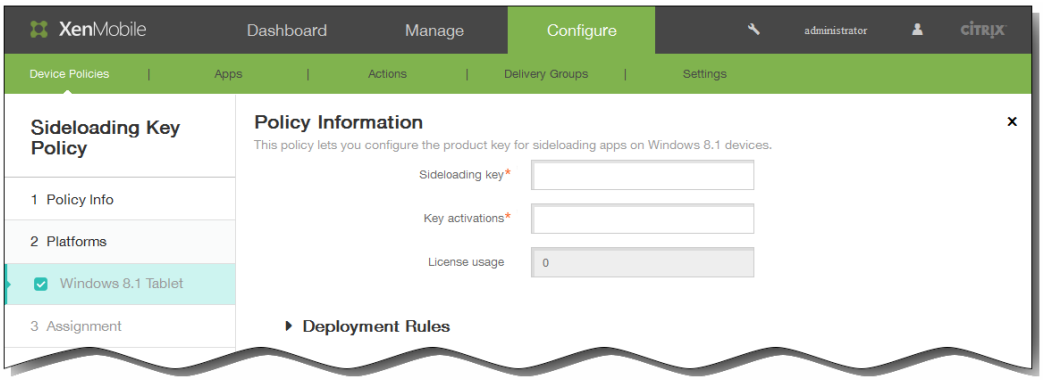
2. Klicken Sie auf Add. Das Dialogfeld Add New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter Apps auf Sideloading Key. Die Seite Sideloading Key Policy wird angezeigt.

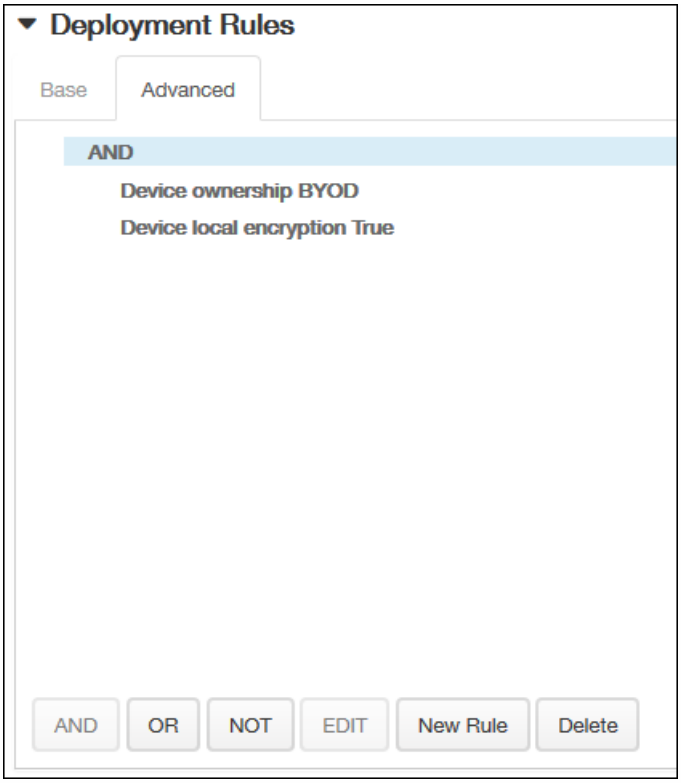


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next.
   Die Seite Windows 8.1 Tablet Platform wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:
   1. Sideloading key: Geben Sie den Sideloadingschlüssel ein, den Sie vom Microsoft Volume Licensing Service Center erhalten haben.
   2. Key activations: Geben Sie die Schlüsselaktivierung ein, die Sie für den Sideloadingschlüssel erstellt haben.
   3. License usage: XenMobile berechnet diesen Wert abhängig von der Zahl angemeldeter Tablets. Sie können dieses Feld nicht ändern.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

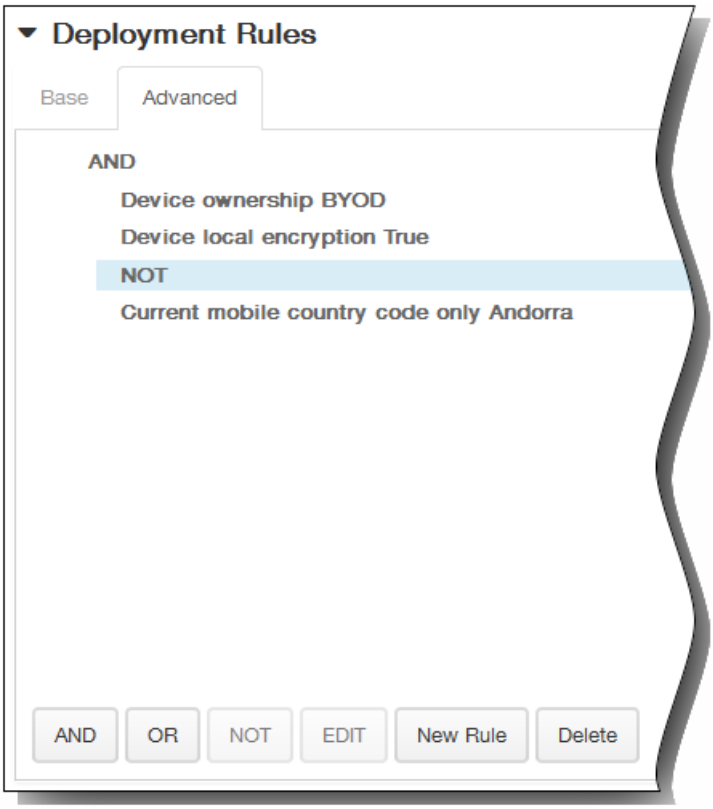
   1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
      1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
      2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
      3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
      4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
   2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



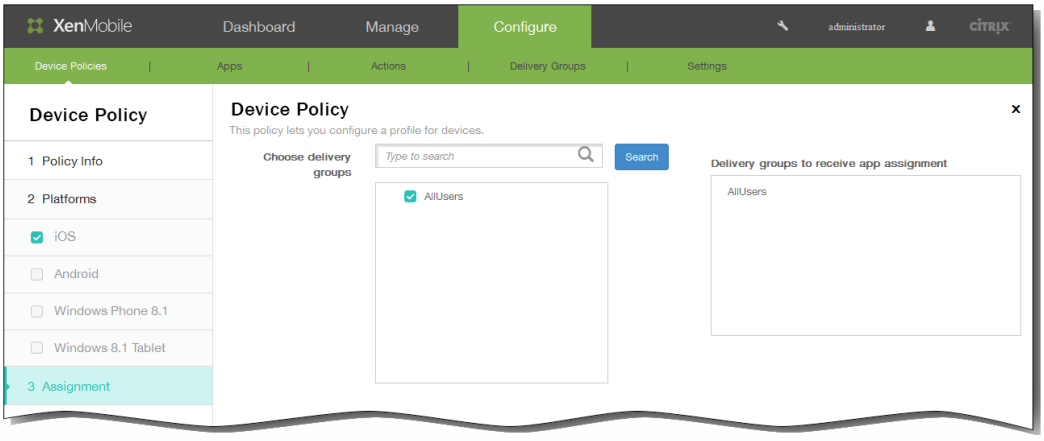
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



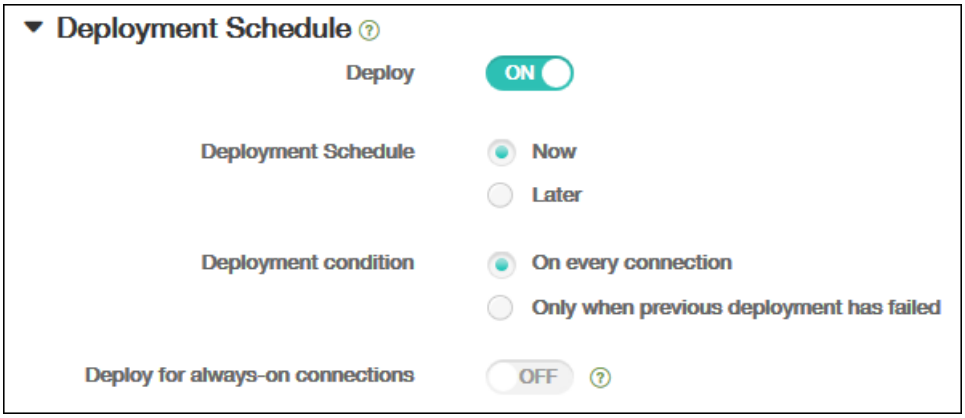
8. Klicken Sie auf Next. Die Seite Assignment für die Sideloadingrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.

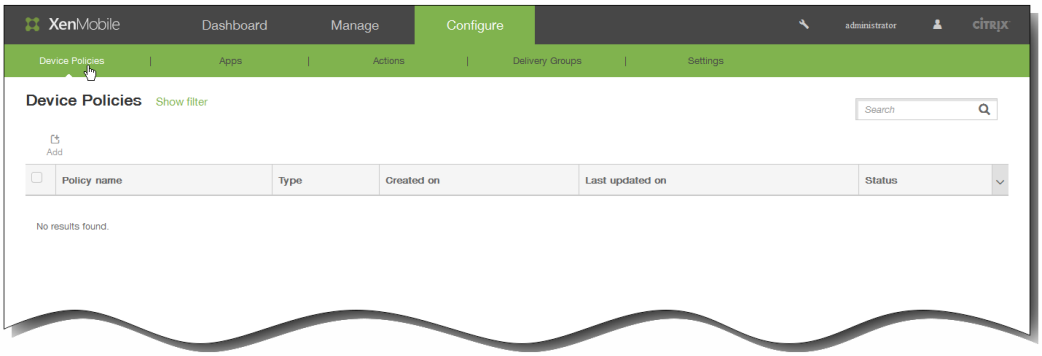


So fügen Sie eine Signaturzertifikat-Richtlinie für Windows 8.1-Tablets hinzu

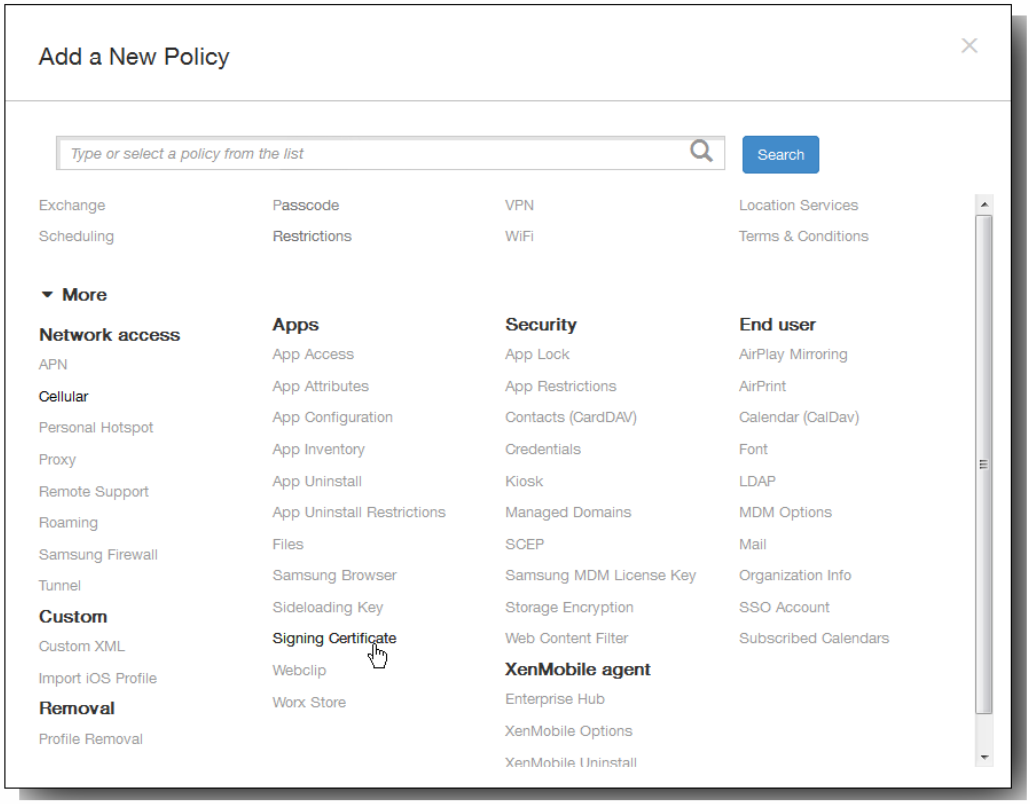
Nov 12, 2015

Sie können in XenMobile eine Geräterichtlinie zum Konfigurieren der Zertifikate hinzufügen, mit denen APPX-Dateien signiert werden. Sie benötigen Signaturzertifikate, wenn Sie APPX-Dateien an die Benutzer verteilen möchten, damit diese Apps auf Windows 8.1-Tablets installieren können.

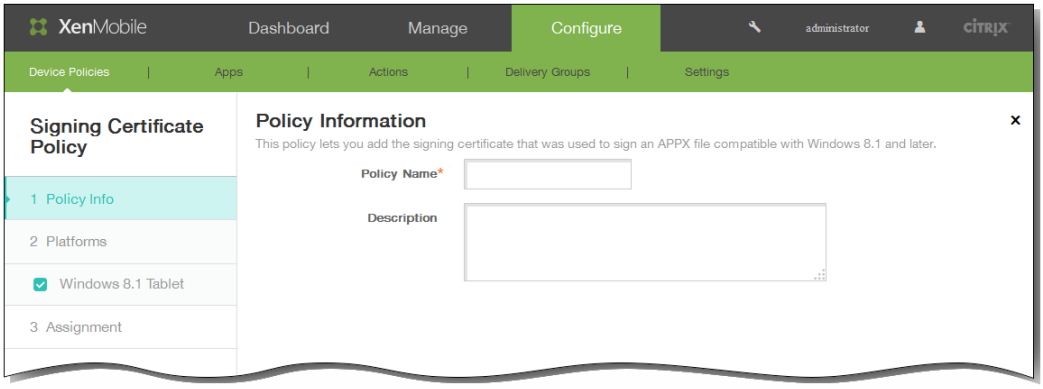
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



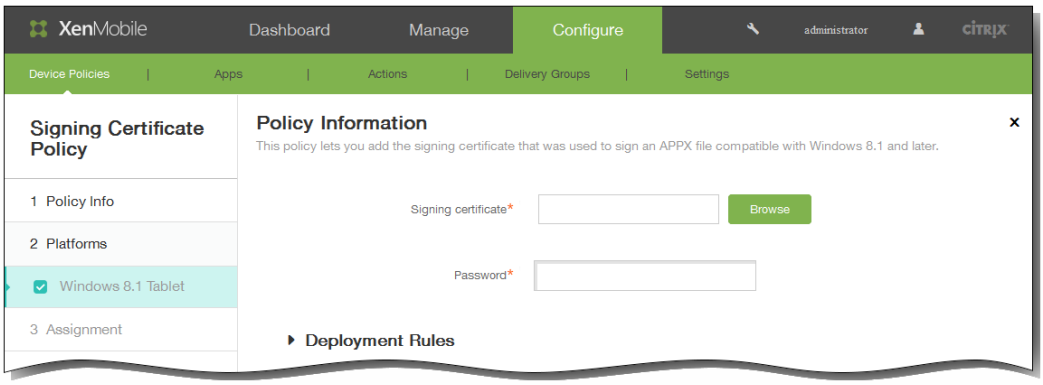
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Wenn Sie auf Add klicken, wird das Dialogfeld Add a New Policy angezeigt.



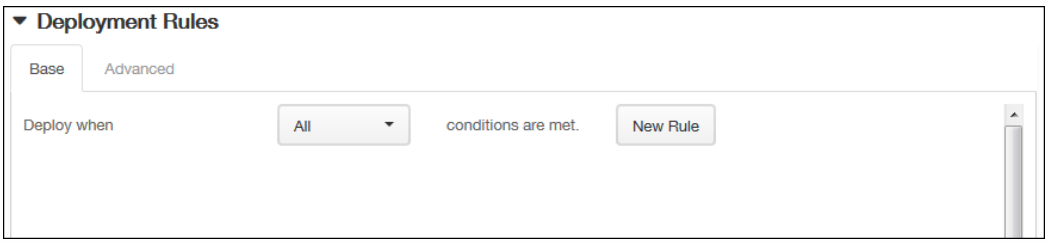
3. Klicken Sie auf More und dann unter Apps auf Signing Certificate. Die Seite Signing Certificate Policy wird angezeigt.



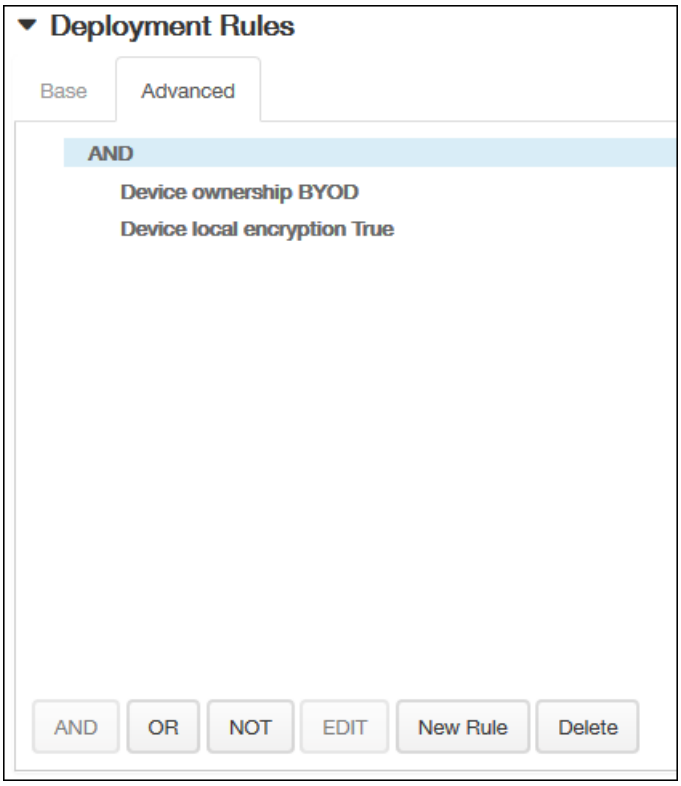
4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung für die Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Platform Information wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:
   1. Signing Certificate: Navigieren Sie zum Speicherort des Zertifikats, das zum Signieren der APPX-Datei verwendet wurde, und wählen Sie dieses aus.
   2. Password: Geben Sie das Kennwort für den Zugriff auf das Signaturzertifikat ein.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.



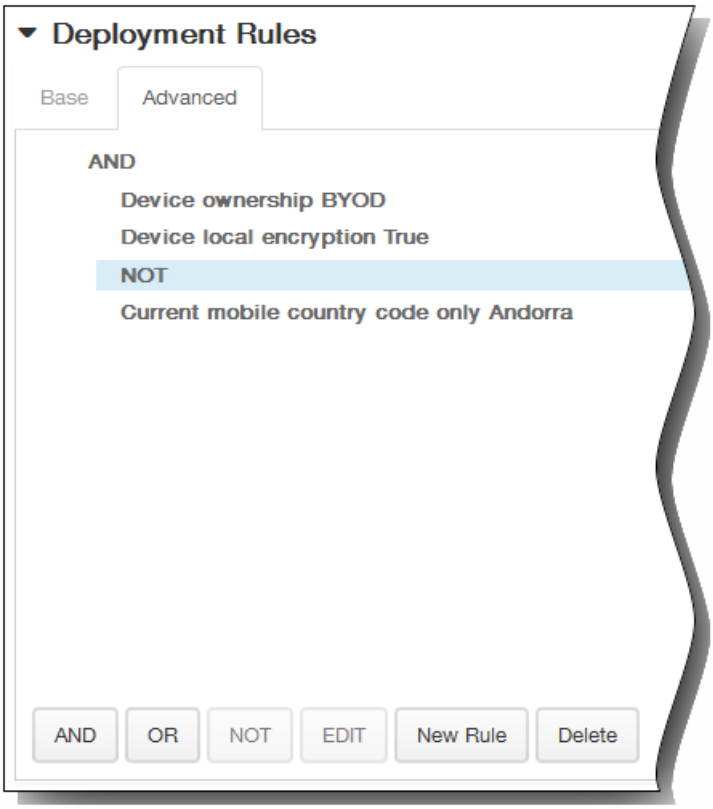
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



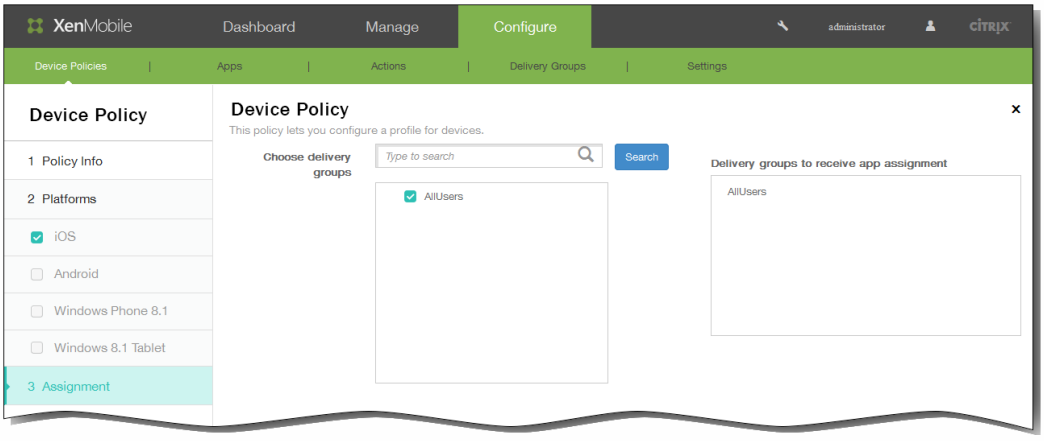
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
    1. Klicken Sie auf AND, OR oder NOT.
    2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
    Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

    3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
    In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



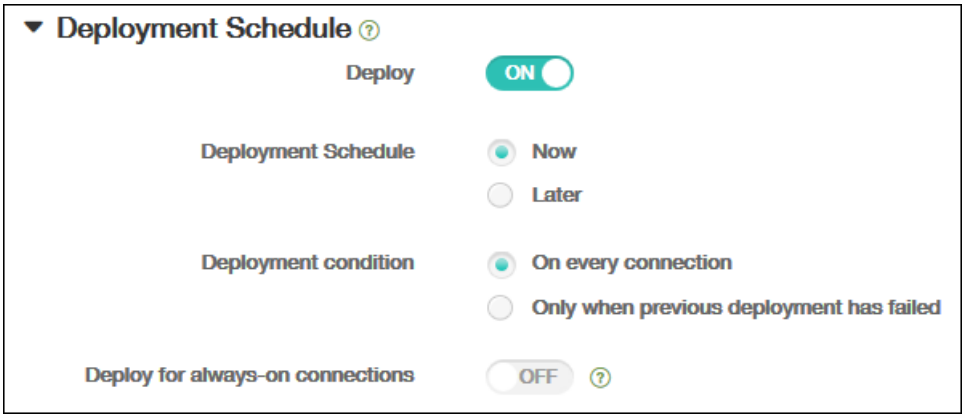
8. Klicken Sie auf Next. Die Seite Assignment wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



11. Klicken Sie auf Save, um die Richtlinie zu speichern.

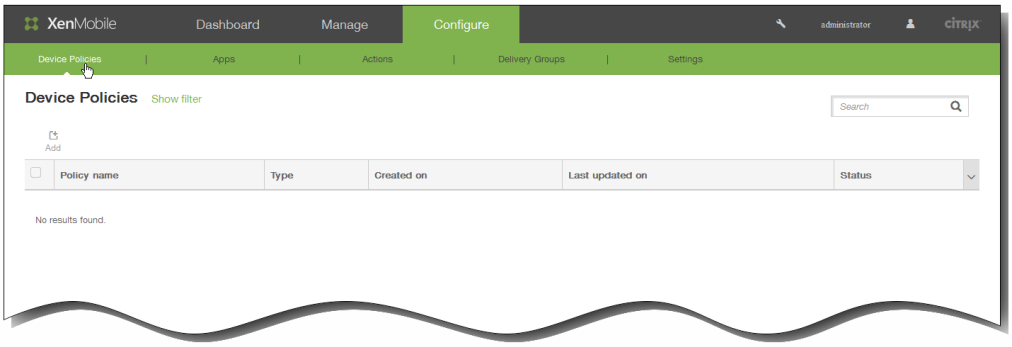
VPN-Geräterichtlinien

Nov 12, 2015

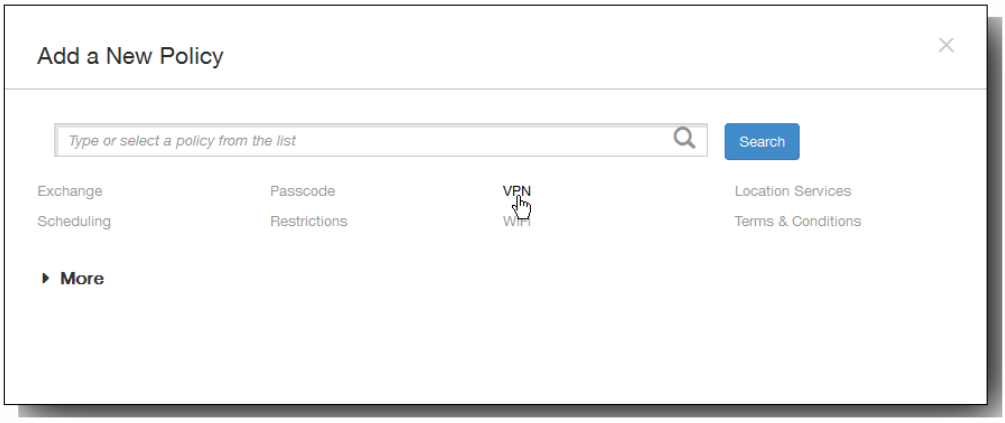
Sie können in XenMobile eine Geräterichtlinie hinzufügen, um die Einstellungen für ein VPN (virtuelles privates Netzwerk) für eine sichere Verbindung zwischen Geräten und Unternehmensressourcen zu konfigurieren. VPN-Richtlinien können für folgende Plattformen konfiguriert werden: iOS, Samsung SAFE, Samsung KNOX, Windows 8.1-Tablets und Amazon. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Artikel detailliert beschrieben.

So fügen Sie eine VPN-Richtlinie für Geräte hinzu

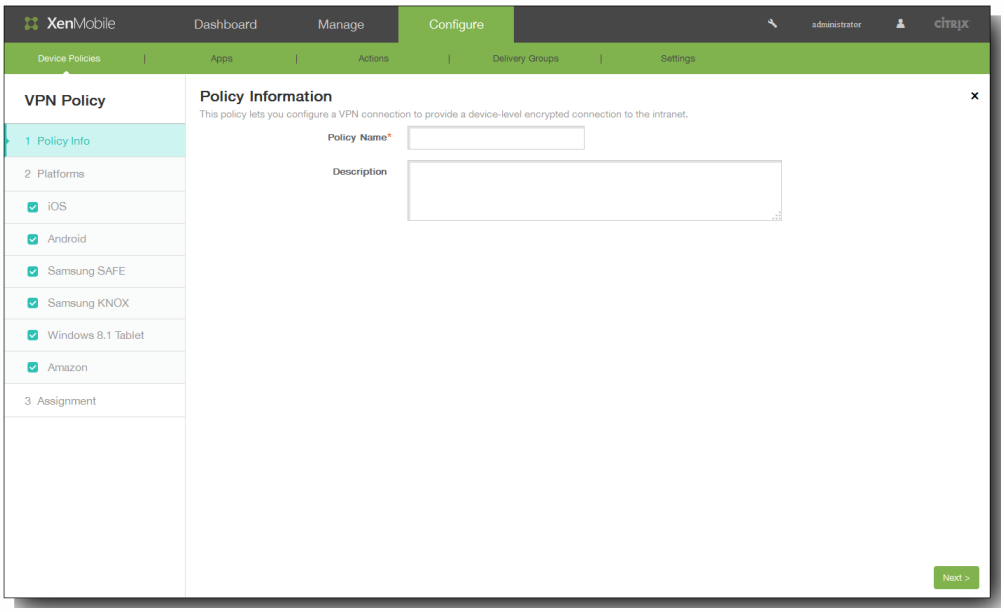
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



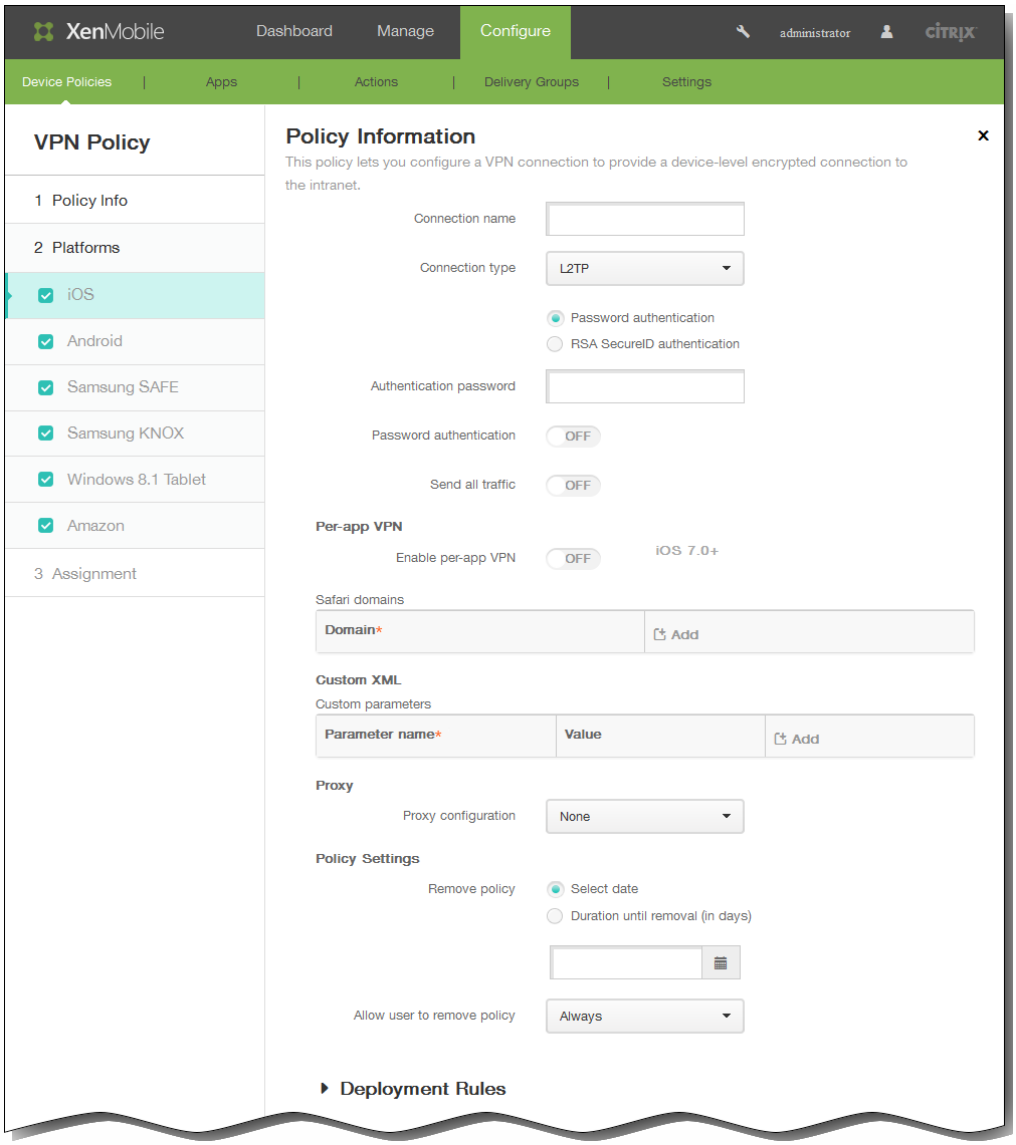
2. Klicken Sie auf Add. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf VPN. Die Seite VPN Policy wird angezeigt.



4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
   3. Klicken Sie auf Next.
5. Wählen Sie unter Platforms die gewünschten Plattformen aus.
   Bei Auswahl von iOS konfigurieren Sie die folgenden Einstellungen:



1. Connection name: Geben Sie einen Namen für die Verbindung ein.
2. Connection type: Wählen Sie in der Liste das Protokoll aus, das für die Verbindung verwendet werden soll.
   - L2TP: Layer-2-Tunnelingprotokoll mit Authentifizierung mit vorinstalliertem Schlüssel. Dies ist die Standardeinstellung.
   - PPTP: Point-to-Point Tunneling
   - IPSec: Ihre Unternehmens-VPN-Verbindung
   - Cisco AnyConnect: Cisco AnyConnect VPN-Client
   - Juniper SSL: Juniper Networks SSL VPN-Client
   - F5 SSL: F5 Networks SSL VPN-Client
   - SonicWALL Mobile Connect: Dell VPN-Client für iOS
   - Ariba VIA: Ariba Networks Virtual Internet Access-Client
   - IKEv2 (iOS only): Internet Key Exchange Version 2 für iOS
   - Custom SSL: benutzerdefiniertes Secure Socket Layer

   In den folgenden Abschnitten werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt.

Konfigurieren Sie für L2TP die folgenden Optionen

1. Wählen Sie Password authentication oder RSA SecureID authentication aus.

2. Authentication password: Geben Sie ein optionales Authentifizierungskennwort ein.
3. Password authentication: Aktivieren oder deaktivieren Sie die Kennwortauthentifizierung.
4. Send all traffic: Wählen Sie aus, ob der gesamte Datenverkehr über das VPN geleitet werden soll.

Konfigurieren Sie für PPTP die folgenden Optionen

1. Wählen Sie Password authentication oder RSA SecureID authentication aus.
2. Authentication password: Geben Sie ein optionales Authentifizierungskennwort ein.
3. Password authentication: Aktivieren oder deaktivieren Sie die Kennwortauthentifizierung.
4. Encryption level: Wählen Sie den gewünschten Verschlüsselungsgrad aus.
5. Send all traffic: Wählen Sie aus, ob der gesamte Datenverkehr über das VPN geleitet werden soll.

Konfigurieren Sie für IPsec die folgenden Optionen

1. Authentication password: Geben Sie ein optionales Authentifizierungskennwort ein.
2. Authentication type for the connection: Wählen Sie den Authentifizierungstyp für die Verbindung aus.

In der folgenden Tabelle werden die Optionen für jeden Verbindungstyp aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern eine Option existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Password	Zertifikat	Shared Secret
Group name	–	–	Optional
Password authentication	OFF	OFF	OFF
Identity credential	–	Keine	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Erforderlich, wenn Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Eingabeaufforderung für Kennwort	–	–	OFF
Auth password	Optional	–	–

Konfigurieren Sie für Cisco AnyConnect die folgenden Optionen

1. Authentication password: Geben Sie ein optionales Authentifizierungskennwort ein.
2. Group: Geben Sie optional einen Gruppennamen ein.
3. Authentication type for the connection: Wählen Sie den Authentifizierungstyp für die Verbindung aus.

In der folgenden Tabelle werden die Optionen für jeden Verbindungstyp aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern eine Option existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Password	Zertifikat	Shared Secret

Group name	–	–	Optional
Password authentication	OFF	OFF	OFF
Identity credential	–	Keine	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Erforderlich, wenn Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Eingabeaufforderung für Kennwort	–	–	OFF
Auth password	Optional	–	–

Konfigurieren Sie für Juniper SSL die folgenden Optionen

1. Authentication password: Geben Sie ein optionales Authentifizierungskennwort ein.
2. Realm: Geben Sie optional einen Bereichsnamen ein.
3. Role: Geben Sie optional einen Rollennamen ein.
4. Authentication type for the connection: Wählen Sie den Authentifizierungstyp für die Verbindung aus.

In der folgenden Tabelle werden die Optionen für jeden Verbindungstyp aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern eine Option existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Password	Zertifikat	Shared Secret
Group name	–	–	Optional
Password authentication	OFF	OFF	OFF
Identity credential	–	Keine	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Erforderlich, wenn Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Eingabeaufforderung für Kennwort	–	–	OFF
Auth password	Optional	–	–

	Password	Zertifikat	Shared Secret

Konfigurieren Sie für F5 SSL die folgenden Optionen

1. Authentication password: Geben Sie ein optionales Authentifizierungskennwort ein.
2. Authentication type for the connection: Wählen Sie den Authentifizierungstyp für die Verbindung aus.

In der folgenden Tabelle werden die Optionen für jeden Verbindungstyp aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern eine Option existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Password	Zertifikat	Shared Secret
Group name	–	–	Optional
Password authentication	OFF	OFF	OFF
Identity credential	–	Keine	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Erforderlich, wenn Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Eingabeaufforderung für Kennwort	–	–	OFF
Auth password	Optional	–	–

Konfigurieren Sie für SonicWALL Mobile Connect folgenden Optionen

1. Authentication password: Geben Sie ein optionales Authentifizierungskennwort ein.
2. Logon group or domain: Geben Sie optional eine Anmeldegruppe oder -domäne ein.
3. Authentication type for the connection: Wählen Sie den Authentifizierungstyp für die Verbindung aus.

In der folgenden Tabelle werden die Optionen für jeden Verbindungstyp aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern eine Option existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Password	Zertifikat	Shared Secret
Group name	–	–	Optional
Password authentication	OFF	OFF	OFF
Identity credential	–	Keine	–
Prompt for PIN when connecting	–	OFF	–

Enable VPN on demand On Demand Domain	– Password –	OFF Zertifikat Erforderlich, wenn Enable VPN on demand = ON	– Shared Secret –
Use hybrid authentication	–	–	OFF
Eingabeaufforderung für Kennwort	–	–	OFF
Auth password	Optional	–	–

Konfigurieren Sie für Ariba VIA die folgenden Optionen

1. Authentication password: Geben Sie ein optionales Authentifizierungskennwort ein.
2. Authentication type for the connection: Wählen Sie den Authentifizierungstyp für die Verbindung aus.

In der folgenden Tabelle werden die Optionen für jeden Verbindungstyp aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern eine Option existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Password	Zertifikat	Shared Secret
Group name	–	–	Optional
Password authentication	OFF	OFF	OFF
Identity credential	–	Keine	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Erforderlich, wenn Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF
Eingabeaufforderung für Kennwort	–	–	OFF
Auth password	Optional	–	–

Konfigurieren Sie für IKEv2 (nur iOS) die folgenden Optionen

1. Authentication password: Geben Sie ein optionales Authentifizierungskennwort ein.
2. Password authentication: Aktivieren oder deaktivieren Sie die Kennwortauthentifizierung.
3. Always-on VPN: Wählen Sie aus, ob die VPN-Verbindung immer aktiv sein soll.
   Die nachfolgenden Optionen sind nur relevant, wenn für Always-on VPN die Einstellung "ON" gewählt wird.
4. Server name or IP address: Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
5. User Account: Geben Sie optional ein Benutzerkonto ein.
6. Authentication type for the connection: Wählen Sie den Authentifizierungstyp für die Verbindung aus.

In der folgenden Tabelle werden die Optionen für jeden Verbindungstyp aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern eine Option existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Password	Zertifikat	Shared Secret
Group name	–	–	Optional
Shared secret	–	–	Optional
Use hybrid authentication	–	–	OFF
Eingabeaufforderung für Kennwort	–	–	OFF
Allow user to disable automatic connection	OFF	OFF	OFF
Local identifier	Erforderlich	Erforderlich	Erforderlich
Remote identifier	Erforderlich	Erforderlich	Erforderlich
Extended Authentication Enabled	OFF	OFF	OFF
Dead Peer Detection Interval	Keine	Keine	Keine
Encryption Algorithm	2DES	2DES	2DES
Integrity Algorithm	SHA1-96	SHA1-96	SHA1-96
Diffie Hellman Group	2	2	2
LifeTime in Minutes	1440	1440	1440
Voice Mail	Allow traffic via tunnel	Allow traffic via tunnel	Allow traffic via tunnel
Allow traffic from captive web sheet outside the VPN	OFF	OFF	OFF
Allow traffic from all captive networking apps outside the VPN tunnel	OFF	OFF	OFF
AirPrint	Allow traffic via tunnel	Allow traffic via tunnel	Allow traffic via tunnel
Captive networking app bundle identifiers	Optional	Optional	Optional

Konfigurieren Sie für Custom SSL die folgenden Optionen

1. Custom SSL identifier (reverse DNS format): Geben Sie den SSL-Bezeichner im Reverse DNS-Format ein.
2. Authentication password: Geben Sie ein optionales Authentifizierungskennwort ein.
3. Password authentication: Aktivieren oder deaktivieren Sie die Kennwortauthentifizierung.
4. Authentication type for the connection: Wählen Sie den Authentifizierungstyp für die Verbindung aus.

In der folgenden Tabelle werden die Optionen für jeden Verbindungstyp aufgeführt. In jeder Zelle wird der Standardwert

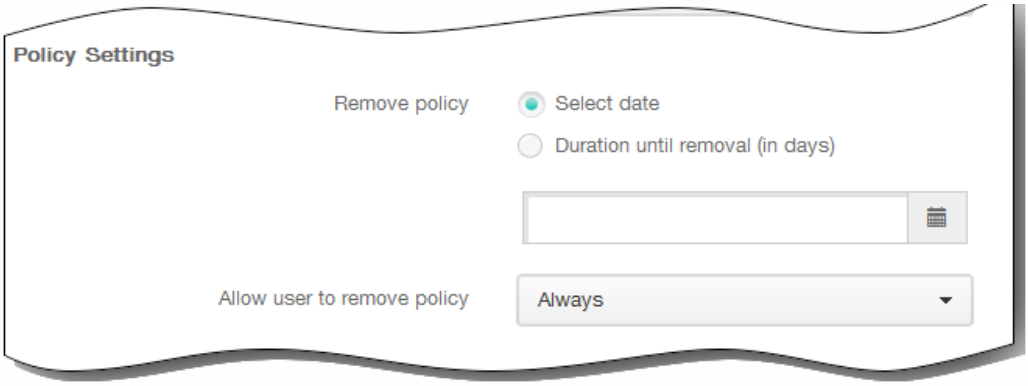
für die jeweilige Option angegeben, sofern eine Option existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Password	Zertifikat	Shared Secret
Group name	–	–	Optional
Eingabeaufforderung für Kennwort	–	–	OFF
Auth password	Optional	–	OFF
Identity credential	–	Keine	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–
On Demand Domain	–	Erforderlich, wenn Enable VPN on demand = ON	–
Use hybrid authentication	–	–	OFF

3. Enable per-app VPN: Aktivieren oder deaktivieren Sie nach Wahl das VPN auf App-Basis (verfügbar ab iOS 7). Wenn Sie die Option aktivieren, aktivieren oder deaktivieren Sie On-demand match enabled.
4. Safari domains: Klicken Sie auf Add, um eine Safari-Domäne hinzuzufügen, mit deren Hilfe die App eine sichere VPN-Verbindung über Safari auf App-Basis erstellen kann.
5. Custom XML: Klicken Sie auf Add um in Parameter name und Value Parameter-/Wertepaare zum Anpassen der Verbindung einzugeben.
6. Proxy Configuration: Wählen Sie in der Liste nach Bedarf das Routing der VPN-Verbindung über einen Proxyserver aus und konfigurieren Sie ggf. zusätzliche Optionen.
   In der folgenden Tabelle werden die für Manual und Automatic verfügbaren Optionen aufgeführt. Für None sind keine weiteren Angaben erforderlich. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern eine Option existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

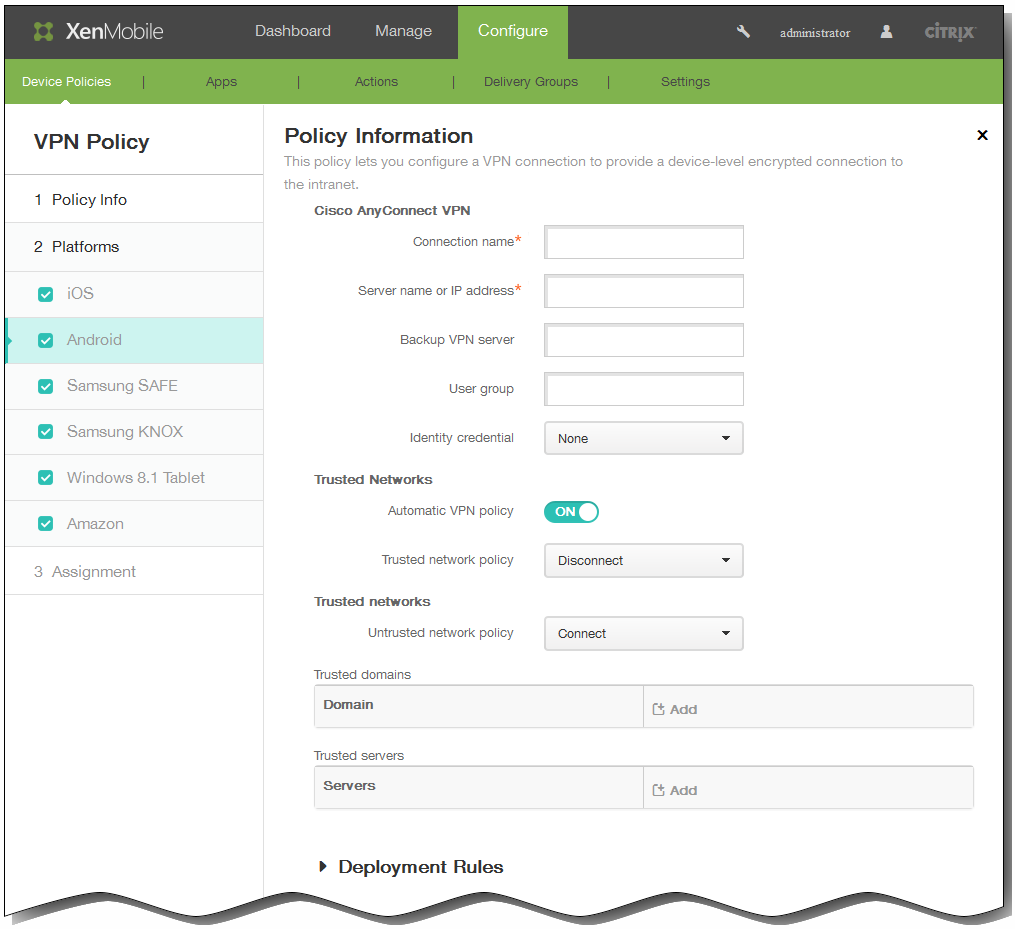
	Manuell	Automatisch
Host name or IP address for the proxy server	Erforderlich	–
Port for the proxy server	Erforderlich	–
User name	Optional	–
Password	Optional	–
Proxy server URL	–	Erforderlich

Richtlinieneinstellungen



1. Klicken Sie unter Policy Settings für Remove policy auf Select date oder Duration until removal (in days).
2. Bei Auswahl von Select date klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
3. Klicken Sie in der Liste Allow user to remove policy auf Always, Password required oder Never.
4. Bei Auswahl von Password required geben Sie für Removal password das Kennwort ein.

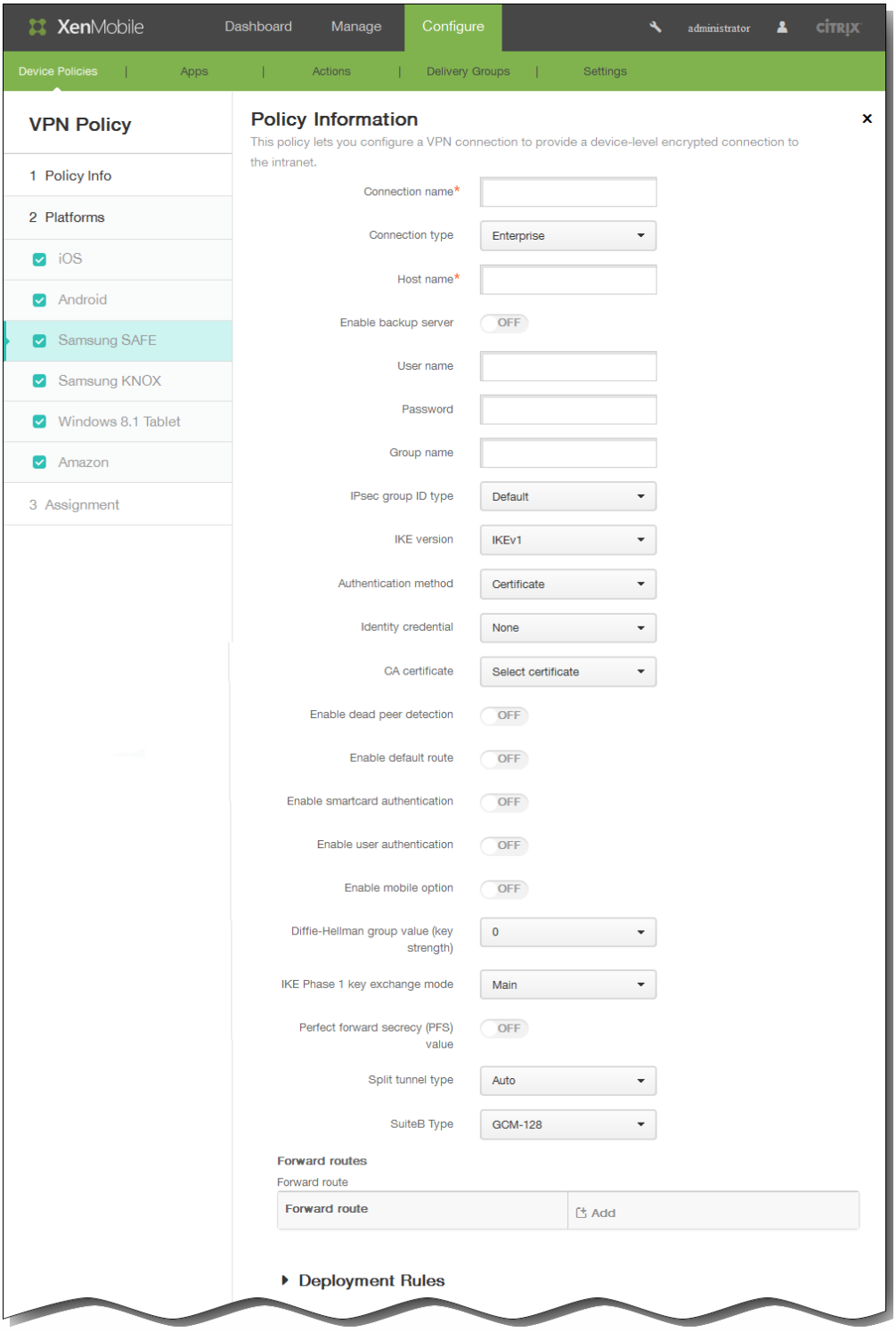
Bei Auswahl von Android konfigurieren Sie die folgenden Einstellungen:



1. Connection name: Geben Sie einen Namen für die Cisco AnyConnect VPN-Verbindung ein.

2. Server name or IP address: Geben Sie den Namen oder die IP-Adresse des VPN-Servers ein.
3. Backup VPN server: Geben Sie die Informationen des sekundären VPN-Servers ein.
4. User group: Geben Sie die Informationen zur Benutzergruppe ein.
5. Identity credential: Wählen Sie in der Liste Anmeldeinformationen aus.
6. Automatic VPN policy: Aktivieren oder deaktivieren Sie diese Option, um festzulegen, wie das VPN auf vertrauenswürdige und nicht vertrauenswürdige Netzwerke reagiert. Wenn Sie diese Option aktivieren, geben Sie die folgenden Informationen ein:
   - Trusted network policy: Klicken Sie in der Liste auf die gewünschte Richtlinie.
   - Untrusted network policy: Klicken Sie in der Liste auf die gewünschte Richtlinie.

Bei Auswahl von Samsung SAFE konfigurieren Sie die folgenden Einstellungen:



1. Connection name: Geben Sie einen Namen für die Verbindung ein.
2. Connection type: Wählen Sie in der Liste das Protokoll aus, das für die Verbindung verwendet werden soll:
   - L2TP with pre-shared key: Layer-2-Tunnelingprotokoll mit Authentifizierung mit vorinstalliertem Schlüssel. Dies ist die Standardeinstellung.
   - L2TP with certificate: Layer-2-Tunnelingprotokoll mit Zertifikat
   - PPTP: Point-to-Point Tunneling
   - Enterprise: Ihre Unternehmens-VPN-Verbindung

   In der folgenden Tabelle werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt. In jeder

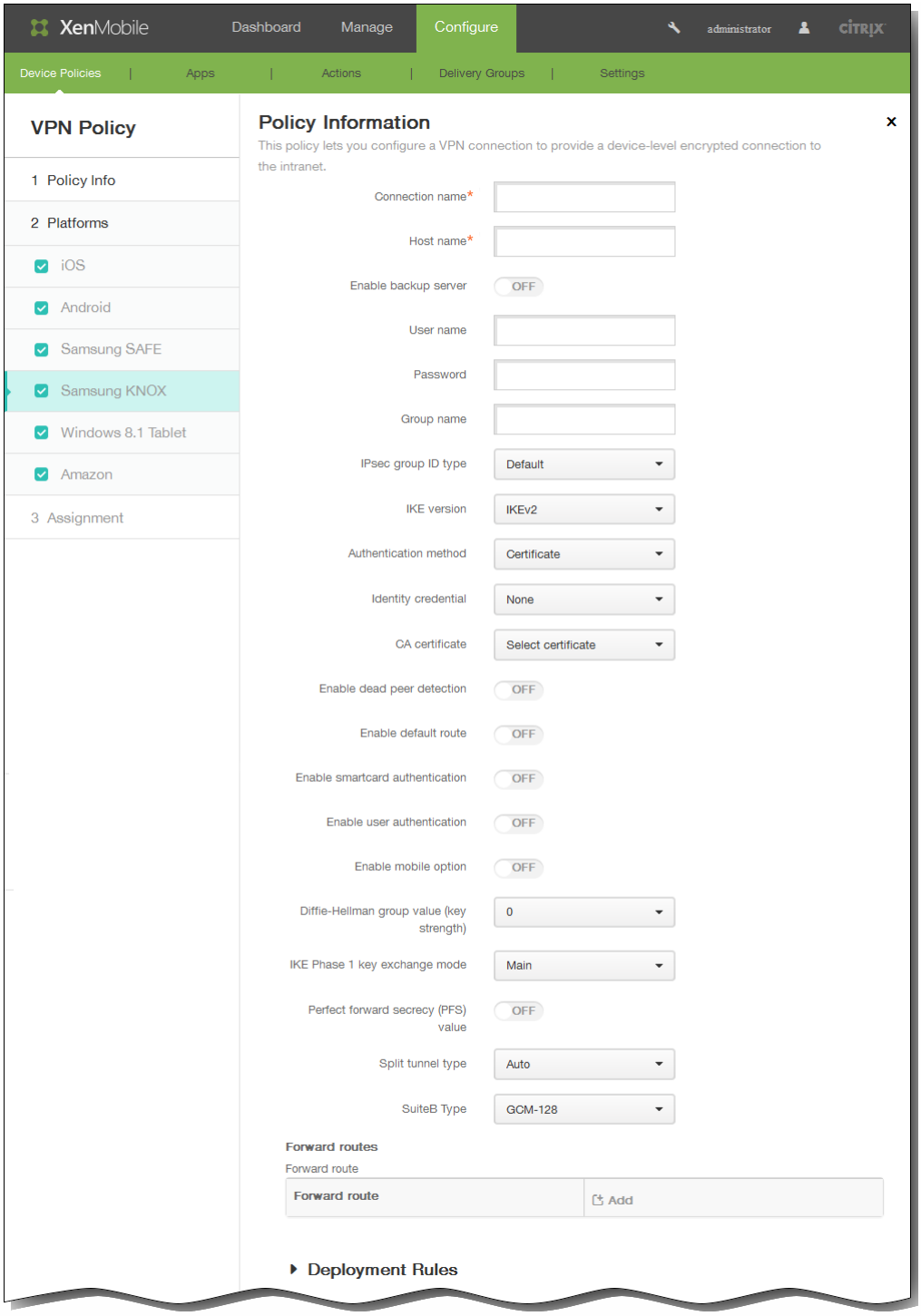
Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	L2TP with pre-shared key	L2TP with certificate	PPTP	Enterprise				
Hostname	Erforderlich	Erforderlich	Erforderlich	Erforderlich				
Enable backup server	–	–	–	Off				
Backup VPN server	–	–	–	Erforderlich, wenn Enable backup server = On				
User name	Optional	Optional	Optional	Optional				
Password	Optional	Optional	Optional	Optional				
Group name	–	–	–	Optional				
IPsec group ID type	–	–	–	Standard				
IKE version	–	–	–	IKEv1				
Authentication method	–	–	–	Certificate (Standard)	Pre-shared key	Hybrid RSA	EAP MD5	EAP MSCHAPv2
Identity credential	–	Erforderlich	–	Keine	Keine	–	–	–
CA certificate	–	–	–	Zertifikat auswählen				
Enable dead peer detection	–	–	–	Off				
Enable default route	–	–	–	Off				
Enable smartcard authentication	–	–		Off				
Enable user authentification	–	–	–	Off				
Enable mobile option	–	–	–	Off				

Diffie-Hellman group value (key strength) IKE Phase 1 key exchange mode	L2TP with pre-shared key –	– L2TP with certificate –	– PPTP –	Enterprise –	0 Main			
Perfect forwared secrecy (PFS) value	–	–	–	Off				
Split tunnel type	–			Auto				
SuiteB Type	–	–	–	GCM-128				
Pre-shared key	Erforderlich	–	–	–	Optional	–	–	–
Enable encryption	–	–	Off	–	–	–	–	–

3. Forward routes: Fügen Sie optional beliebige Weiterleitungsrouten hinzu, wenn Ihr VPN-Server mehrere Routentabellen unterstützt.

Bei Auswahl von Samsung KNOX konfigurieren Sie die folgenden Einstellungen:



1. Connection name: Geben Sie einen Namen für die Verbindung ein.
2. Host name: Geben Sie den Hostnamen ein.
3. Enable backup server: Wählen Sie aus, ob ein sekundärer VPN-Server aktiviert werden soll. Ein weiteres Feld wird angezeigt, wenn Sie diese Option auswählen. Geben Sie die Informationen für den sekundären Server ein.
4. User name: Geben Sie einen optionalen Benutzernamen ein.
5. Password: Geben Sie ein optionales Kennwort ein.
6. Group name: Geben Sie einen optionalen Benutzernamen ein.
7. IPsec group ID type: Klicken Sie in der Liste auf den IPsec-Gruppen-ID-Typ.
8. IKE version: Klicken Sie in der Liste auf die IKE-Version.

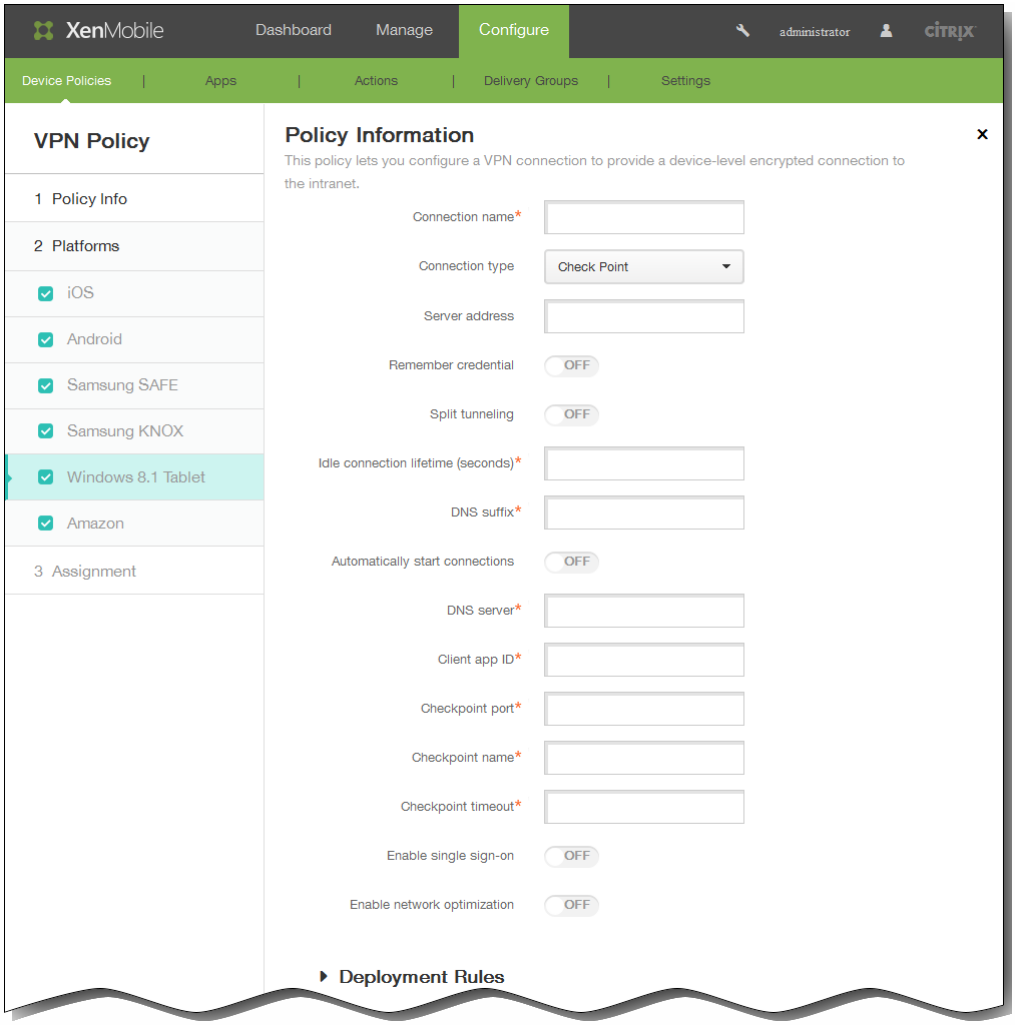
9. Authentication method: Klicken Sie in der Liste auf die Authentifizierungsmethode.
   - Certificate: zertifikatbasierte Authentifizierung
   - Pre-shared key: Authentifizierung mit einem vorinstallierten Schlüssel
   - Hybrid RSA: Hybridauthentifizierung mit RSA-Zertifikaten
   - EAP MD5: Extensible Authentication Protocol mit MD5-Hashfunktion
   - EAP MSCHAPv2: Extensible Authentication Protocol mit Microsoft Challenge Handshake Authentication Protocol Version 2

   In der folgenden Tabelle werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Zertifikat	Pre-shared key	Hybrid RSA	EAP MD5	EAP MSCHAPv2
Pre-shared key	–	Erforderlich	–	–	–
Identity credential	Keine	Keine	–	–	–
CA certificate	Erforderlich	Erforderlich	Erforderlich	Erforderlich	Erforderlich
Enable dead peer detection	OFF	OFF	OFF	OFF	OFF
Enable default route	OFF	OFF	OFF	OFF	OFF
Enable smartcard authentication	OFF	OFF	OFF	OFF	OFF
Enable user authentication	OFF	OFF	OFF	OFF	OFF
Enable mobile option	OFF	OFF	OFF	OFF	OFF
DIfffie-Hellman group value (key strength)	0	0	0	0	0
IKE Phase 1 key exchange mode	Main	Main	Main	Main	Main
Perfect forward secrecy (PFS) value	OFF	OFF	OFF	OFF	OFF
Split tunnel type	Auto	Auto	Auto	Auto	Auto
SuiteB Type	GCM-128	GCM-128	GCM-128	GCM-128	GCM-128

10. Forward route: Fügen Sie optional beliebige Weiterleitungsrouten hinzu, wenn Ihr VPN-Server mehrere Routentabellen unterstützt.

Bei Auswahl von Windows 8.1 tablet konfigurieren Sie die folgenden Einstellungen:



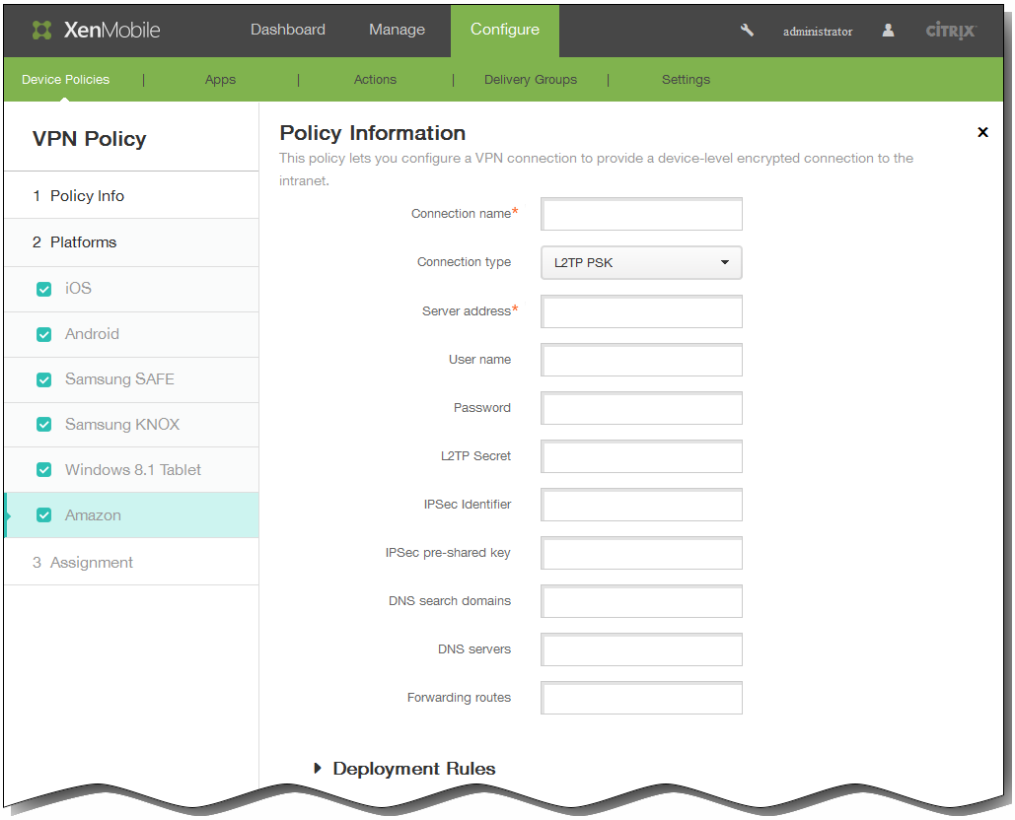
1. Connection name: Geben Sie einen Namen für die Verbindung ein.
2. Connection type: Klicken Sie in der Liste auf den Verbindungstyp.
   - SonicWALL: Dell VPN-Client für iOS
   - Check Point: Check Point Software Technologies SSL VPN-Client
   - Juniper: Juniper Networks SSL VPN-Client
   - Microsoft: Microsoft VPN-Client
   - F5: F5 Networks SSL VPN-Client

   In der folgenden Tabelle werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	SonicWALL	Check Point	Juniper	Microsoft Word	F5
Server address	Optional	Optional	Optional	Optional	Optional
Remember credential	OFF	OFF	OFF	OFF	OFF
Split-Tunneling	OFF	OFF	OFF	OFF	OFF
Idle connection lifetime (seconds)	Erforderlich	Erforderlich	Erforderlich	Erforderlich	Erforderlich

	SonicWALL	Check Point	Juniper	Microsoft Word	F5
DNS suffix	Erforderlich	Erforderlich	Erforderlich	Erforderlich	Erforderlich
Automatically start connections	OFF	OFF	OFF	–	OFF
DNS server	Erforderlich	Erforderlich	Erforderlich	–	Erforderlich
Client app ID	Erforderlich	Erforderlich	Erforderlich	–	Erforderlich
Checkpoint port	–	Erforderlich	–	–	–
Checkpoint name	–	Erforderlich	–	–	–
Checkpoint timeout	–	Erforderlich	–	–	–
Enable single sign-on	–	OFF	–	–	–
Enable network optimization	–	OFF	–	–	–
Enable compression	OFF	–	–	–	–
Require smart card certificate	OFF	–	–	–	–
Automatically select client certificate	OFF	–	–	–	–
Enable client logging	OFF	–	–	–	–
Enable packet capture	OFF	–	–	–	–
Use single sign-on credentials	–	–	OFF	–	–
Make connection available to all users	–	–	–	OFF	–
Tunneling protocol	–	–	–	Erforderlich	–
Authentication method	–	–	–	Erforderlich	–
VPN server name	–	–	–	Erforderlich	–
VPN friendly name	–	–	–	Erforderlich	–
Automatically detect settings	–	–	–	OFF	–
Bypass porxy server for local addresses	–	–	–	OFF	–
Automatically use Windows credentials	–	–	–	OFF	–
Client certificate issuer	–	–	–	–	Erforderlich

Bei Auswahl von Amazon konfigurieren Sie die folgenden Einstellungen:



1. Connection name: Geben Sie einen Namen für die Verbindung ein.
2. Connection type: Klicken Sie auf den Verbindungstyp.
   - L2TP PSK: Layer-2-Tunnelingprotokoll mit Authentifizierung mit vorinstalliertem Schlüssel
   - L2TP RSA : Layer-2-Tunnelingprotokoll mit RSA-Authentifizierung
   - IPSEC XAUTH PSK: Internet Protocol Security mit vorinstalliertem Schlüssel und erweiterter Authentifizierung
   - IPSEC XAUTH RSA: Internet Protocol Security mit RSA- und erweiterter Authentifizierung
   - IPSEC HYBRID RSA: Internet Protocol Security mit Hybrid-RSA-Authentifizierung
   - PPTP: Point-to-Point Tunneling

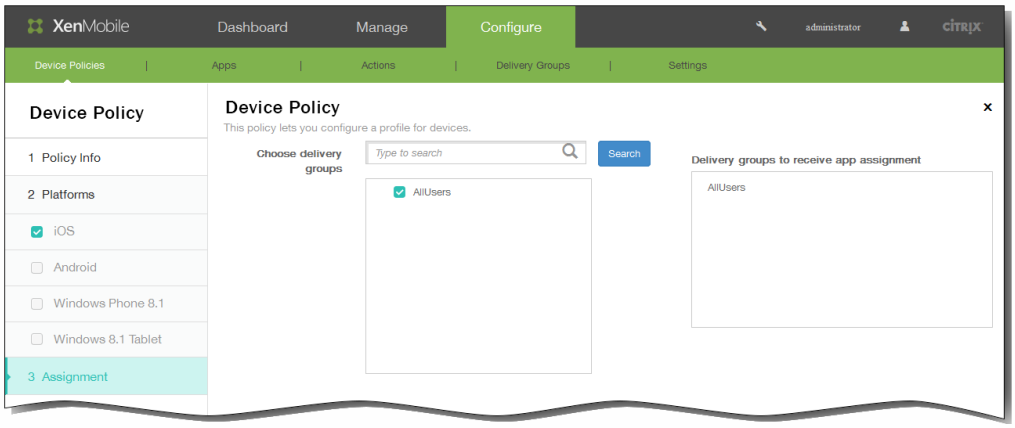
   In der folgenden Tabelle werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	L2TP PSK	L2TP RSA	IPSEC XAUTH PSK	IPSEC XAUTH RSA	IPSEC HYBRID RSA	PPTP
Server address	Erforderlich	Erforderlich	Erforderlich	Erforderlich	Erforderlich	Erforderlich
User name	Optional	Optional	Optional	Optional	Optional	Optional
Password	Optional	Optional	Optional	Optional	Optional	Optional
L2TP Secret	Optional	Optional	–	–	–	–
IPSec identifier	Optional	–	Optional	–	–	–

IPSec pre-shared key	Optional	–	Optional	–	–	–
	L2TP PSK	L2TP RSA	IPSEC XAUTH PSK	IPSEC XAUTH RSA	IPSEC HYBRID RSA	PPTP
DNS search domains	Optional	Optional	Optional	Optional	Optional	Optional
DNS servers	Optional	Optional	Optional	Optional	Optional	Optional
Forwarding routes	Optional	Optional	Optional	Optional	Optional	Optional
Serverzertifikat	–	Auswählen	–	Auswählen	Auswählen	–
CA certificate	–	Auswählen	–	Auswählen	Auswählen	–
Identity credential	–	Erforderlich	–	Erforderlich	–	–
PPP encryption MMPE)	–	–	–	–	–	OFF

3. Forwarding route: Fügen Sie optional beliebige Weiterleitungsrouten hinzu, wenn Ihr VPN-Server mehrere Routentabellen unterstützt.

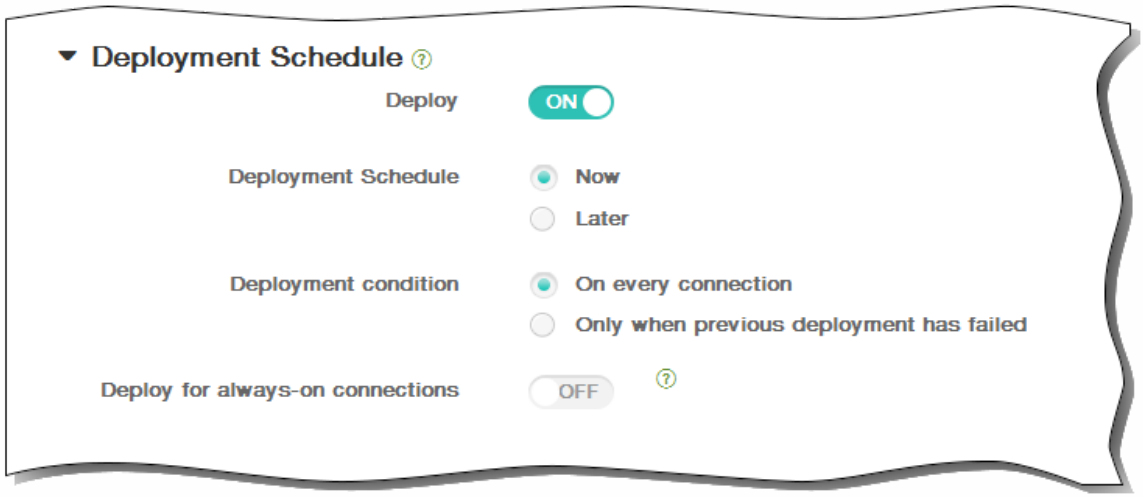
6. Nach Abschluss der Konfiguration der Einstellungen für eine oder mehrere Plattformen klicken Sie auf Next. Es wird dann die Seite Assigment für die VPN-Richtlinie angezeigt.
7. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



8. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
   1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
   2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
   3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
   4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
   5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.

Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



9. Klicken Sie auf Save, um die Richtlinie zu speichern.

WiFi-Richtlinien für Geräte

Nov 12, 2015

WiFi-Geräterichtlinien werden in XenMobile über die Seite Device Policies der XenMobile-Konsole erstellt und bearbeitet. Mit WiFi-Richtlinien legen Sie fest, wie Benutzer mit ihrem Gerät eine Verbindung mit WiFi-Netzwerken aufbauen, indem Sie Netzwerknamen und -typen sowie Authentifizierungs- und Sicherheitsrichtlinien definieren, festlegen, ob Proxyserver verwendet werden sollen, und weitere WiFi-bezogene Informationen für alle Benutzer der von Ihnen ausgewählten Geräteplattform vorgeben.

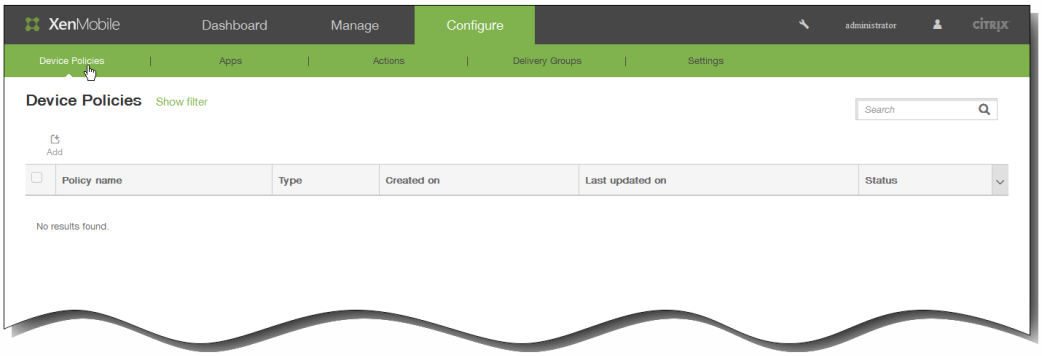
WiFi-Einstellungen können für folgende Plattformen konfiguriert werden: iOS, Android, Windows Phone 8.1 und Windows 8.1-Tablets. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Artikel detailliert beschrieben.

Wichtig: Führen Sie vor dem Erstellen einer neuen Richtlinie die folgenden Schritte aus:

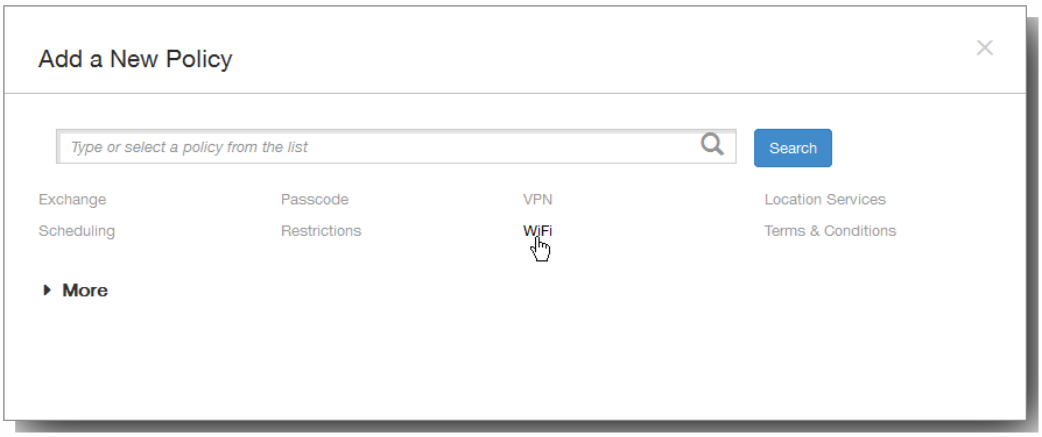
- Erstellen Sie alle Bereitstellungsgruppen, die Sie verwenden möchten.
- Halten Sie Namen und Typ des Netzwerks bereit.
- Planen Sie die zu verwendenden Authentifizierungs-/Sicherheitstypen.
- Halten alle ggf. erforderlichen Proxyserverinformationen bereit.
- Installieren Sie alle erforderlichen Zertifizierungsstellenzertifikate.
- Halten Sie alle erforderlichen gemeinsamen Schlüssel bereit.

So erstellen Sie eine neue WiFi-Geräterichtlinie

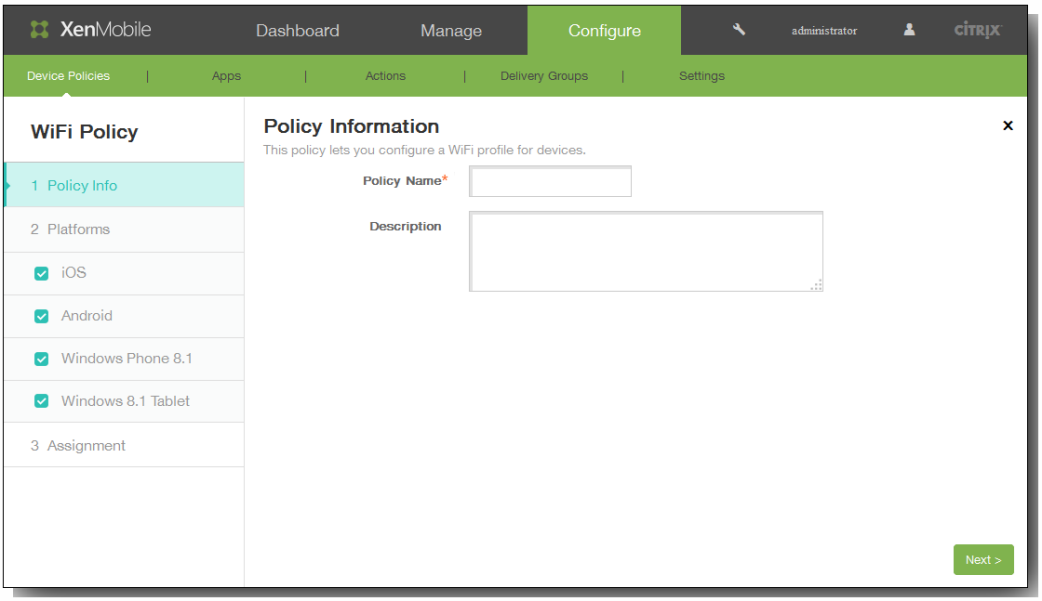
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt. Klicken Sie auf WiFi.



Die Seite WiFi Policy wird angezeigt.



3. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
   3. Klicken Sie auf Next.
4. Wählen Sie unter Platforms die gewünschten Plattformen aus. Deaktivieren Sie die Plattformen, für die Sie die Richtlinie nicht konfigurieren möchten.
   Bei Auswahl von iOS konfigurieren Sie die folgenden Einstellungen:

1. Wählen Sie in der Liste Network type auf den Netzwerktyp, den Sie verwenden möchten.
2. Wenn Sie Standard oder Legacy Hotspot auswählen, geben Sie die folgenden Informationen ein:

1. Network Name: Geben Sie die SSID ein, die in der Liste der verfügbaren Netzwerke angezeigt wird.
2. Hidden network (enable if network is open or off): Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.
3. Auto Join: Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.

3. Wenn Sie Hotspot 2.0 ausgewählt haben, geben Sie die nach Security type aufgelisteten Informationen ein:
   Hinweis: Diese Optionen gelten nur für iOS 7.0 und höher.
   1. Displayed operator name: Geben Sie den Betreibernamen ein, der angezeigt werden soll.
   2. Domain name: Geben Sie den Domänennamen ein.
   3. Allow connecting to roaming partner networks: Wählen Sie aus, ob Geräte eine Verbindung mit den Netzen von Roamingpartnern herstellen dürfen.
   4. Roaming Consortium Organization Identifiers (OI): Geben Sie optional Roaming Consortium-OIs ein.
   5. Network Access Identifier (NAI) realm names: Geben Sie optional NAI-Bereichsnamen ein.
   6. Mobile Country Codes (MCCs) and Mobile Network Configurations (MNCs): Geben Sie optional MCCs und MNCs ein.
4. Security type: Klicken Sie in der Liste auf den Typ der Sicherheit, der für die WiFi-Verbindung verwendet werden soll.
   - Keine
   - WEP
   - WPA/WPA2 Personal
   - Any (Personal)
   - WEP Enterprise
   - WPA/WPA2 Enterprise
   - Any (Enterprise)

   In der folgenden Tabelle werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Keine	WEP	WPA/WPA2 Personal	Any (Personal)	WEP Enterprise	WPA/WPA2 Enterprise	Any (Enterprise)
Password	–	Optional	Optional	Optional	–	–	–
TLS	–	–	–	–	OFF	OFF	OFF
TTLS	–	–	–	–	OFF	OFF	OFF
LEAP	–	–	–	–	OFF	OFF	OFF
PEAP	–	–	–	–	OFF	OFF	OFF
EAP-FAST	–	–	–	–	OFF	OFF	OFF
EAP-SIM	–	–	–	–	OFF	OFF	OFF
Inner authentication (TTLS)	–	–	–	–	MSCHAPv2 (wenn TTLS = On)	**MSCHAPv2 (wenn TTLS = On)**	MSCHAPv2 (wenn TTLS = On)
Outer identity	–	–	–	–	Optional (wenn PEAP, TTLS	Optional (wenn PEAP, TTLS oder	Optional (wenn PEAP, TTLS oder

	Keine	WEP	WPA/WPA2 Personal	Any (Personal)	WEP Enterprise	WPA/WPA2 Enterprise	Any (Enterprise)
Verwenden von PAC	–	–	–	–	OFF	OFF	OFF
Provisioning PAC	–	–	–	–	OFF (wenn Use PAC = On)	OFF (wenn Use PAC = On)	OFF (wenn Use PAC = On)
Provisioning PAC anonymously	–	–	–	–	OFF (wenn Provisioning PAC = On)	OFF (wenn Provisioning PAC = On)	OFF (wenn Provisioning PAC = ON)
User name	–	–	–	–	Optional	Optional	Optional
Per-connection password	–	–	–	–	OFF	OFF	OFF
Password	–	–	–	–	Optional	Optional	Optional
Identity credential (Keystore or PKI credential)	–	–	–	–	Keine	Keine	Keine
Requires a TLS certificate	–	–	–	–	OFF	OFF	OFF
Trusted certificates	–	–	–	–	Optional	Optional	Optional
Trusted server certificate names	–	–	–	–	Optional	Optional	Optional
Allow trust exceptions	–	–	–	–	ON	ON	ON

oder EAP-FAST = On)

EAP-FAST = On)

EAP-FAST = On)

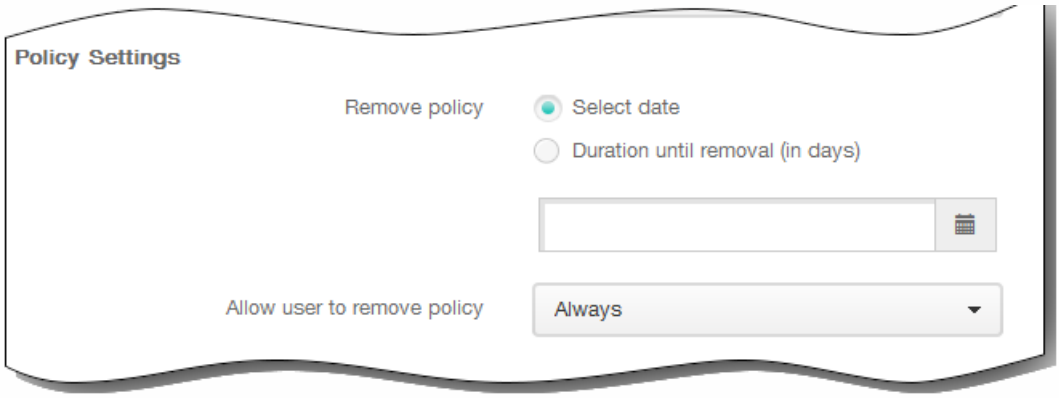
5. Proxy Configuration: Wählen Sie in der Liste nach Bedarf das Routing der VPN-Verbindung über einen Proxyserver aus und konfigurieren Sie ggf. zusätzliche Optionen.
   In der folgenden Tabelle werden die für Manual und Automatic verfügbaren Optionen aufgeführt. Für None sind keine weiteren Angaben erforderlich. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern eine Option existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Manuell	Automatisch

Host name or IP address for the proxy server	Erforderlich	–
Port for the proxy server	Erforderlich	–
User name	Optional	–
Password	Optional	–
Proxy server URL	–	Erforderlich
Allow direct connection if PAC is unreachable	–	On (iOS 7.0 und höher)

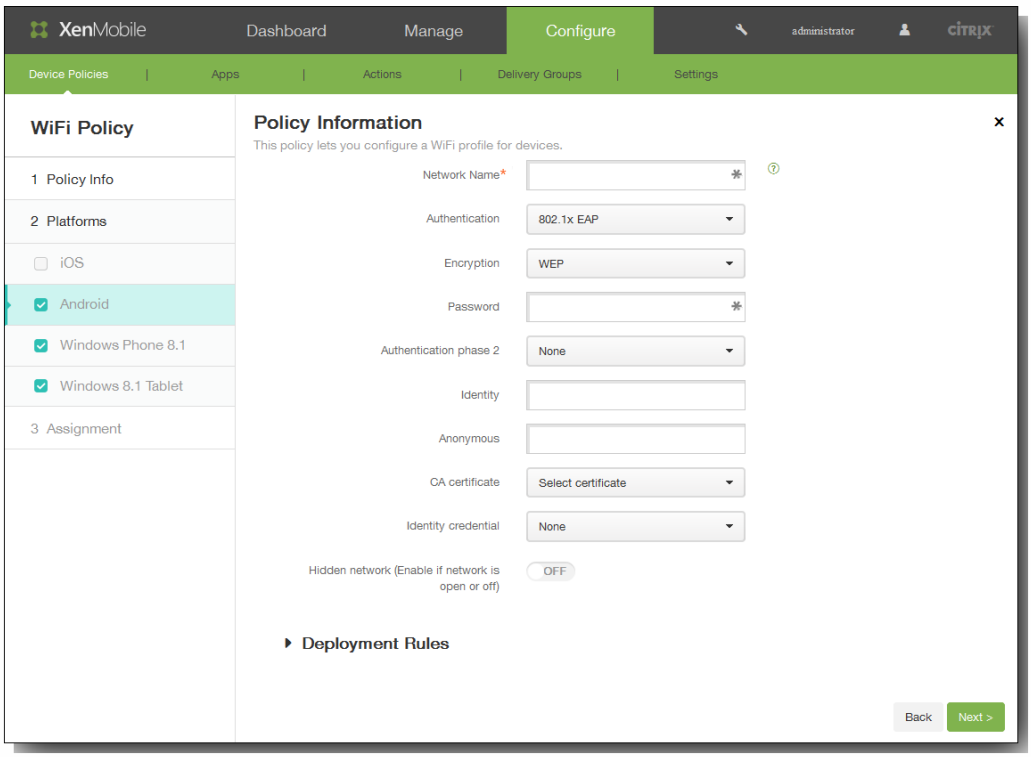
Manuell **Automatisch**

Richtlinieneinstellungen



1. Klicken Sie unter Policy Settings für Remove policy auf Select date oder Duration until removal (in days).
2. Bei Auswahl von Select date klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
3. Klicken Sie in der Liste Allow user to remove policy auf Always, Password required oder Never.
4. Bei Auswahl von Password required geben Sie für Removal password das Kennwort ein.

Bei Auswahl von Android konfigurieren Sie die folgenden Einstellungen:



1. Network name: Geben Sie die SSID ein, die in der Liste der verfügbaren Netzwerke auf den Geräten der Benutzer angezeigt wird.
2. Authentication: Klicken Sie in der Liste auf den Typ der Authentifizierung, der für die WiFi-Verbindung verwendet werden soll.
   - Open
   - Shared
   - WPA
   - WPA-PSK
   - WPA2
   - WPA2-PSK
   - 802.1x EAP

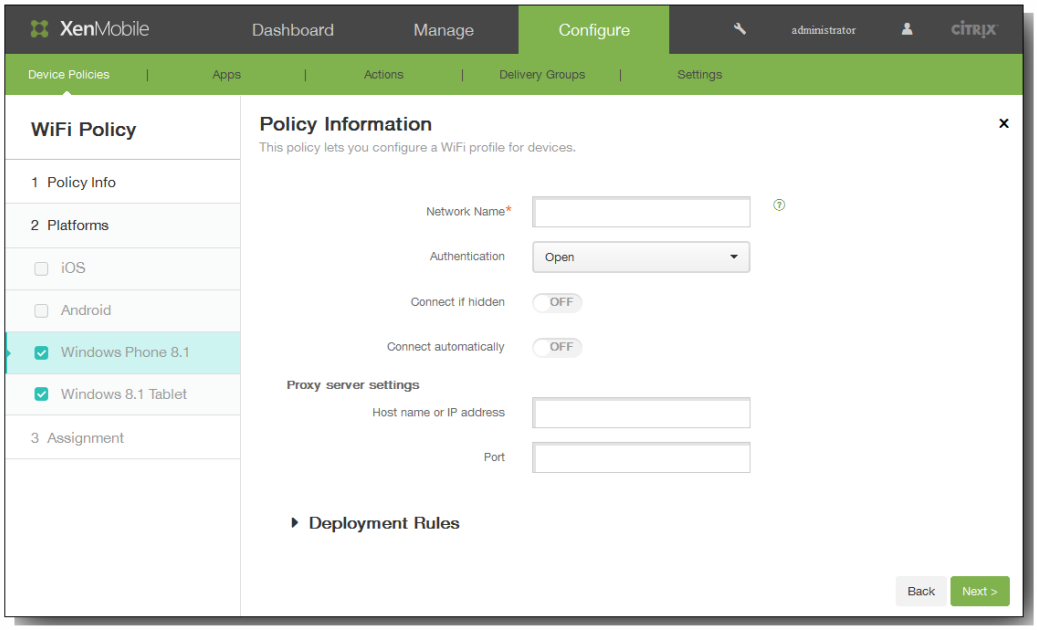
   In der folgenden Tabelle werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Open	Shared	WPA	WPA-PSK	WPA2	WPA2-PSK	802.1 EAP
Verschlüsselung	WEP	WEP	TKIP	TKIP	TKIP	TKIP	–
Password	Optional	Optional	–	–	–	–	Optional
EAP type	–	–	–	–	–	–	PEAP
Authentication phase 2	–	–	–	–	–	–	Keine
Identity	–	–	–	–	–	–	Optional

Anonymous	Open	Shared	WPA	WPA-PSK	WPA2	WPA2-PSK	Optional 802.1 EAP
CA certificate	–	–	–	–	–	–	Auswählen
Identity credential	–	–	–	–	–	–	Keine

3. Hidden network (Enable if network is open or off): Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.

Bei Auswahl von Windows Phone 8.1 konfigurieren Sie die folgenden Einstellungen:



1. Network name: Geben Sie die SSID ein, die in der Liste der verfügbaren Netzwerke auf den Geräten der Benutzer angezeigt wird.
2. Authentication: Klicken Sie in der Liste auf den Typ der Authentifizierung, der für die WiFi-Verbindung verwendet werden soll.
   - Open
   - WPA Personal
   - WPA-2 Personal
   - WPA-2 Enterprise

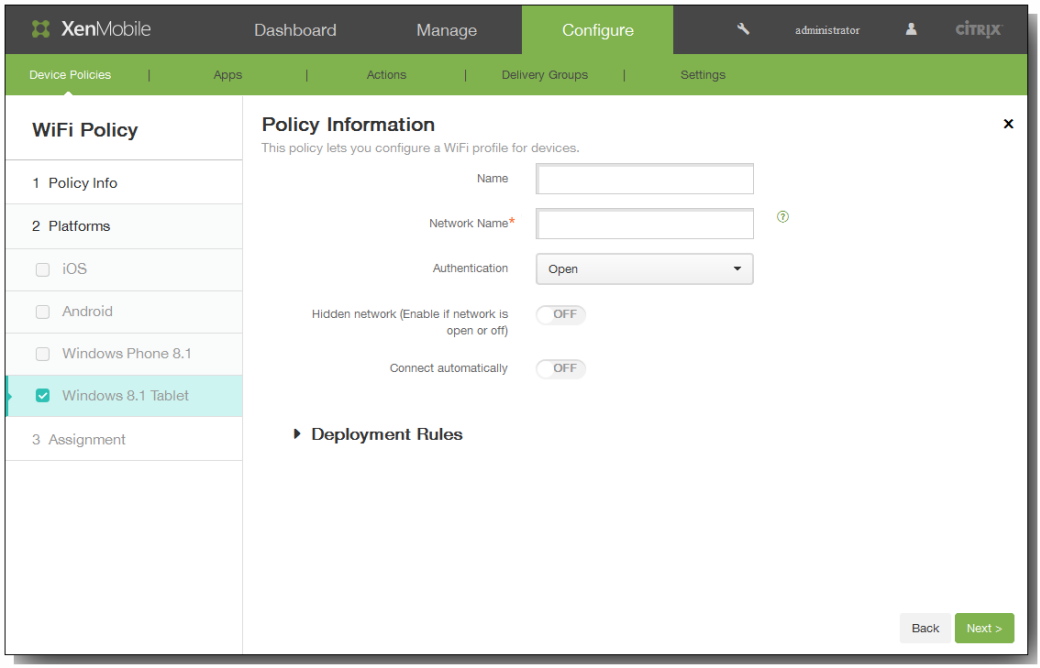
   In der folgenden Tabelle werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Open	WPA Personal	WPA-2 Personal	WPA-2 Enterprise
Verschlüsselung	–	AES	AES	AES
Shared key	–	Optional	Optional	–

3. Connect if hidden: Wählen Sie aus, ob eine Verbindung hergestellt werden soll, wenn das Netzwerk ausgeblendet ist.
4. Connect automatically: Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.

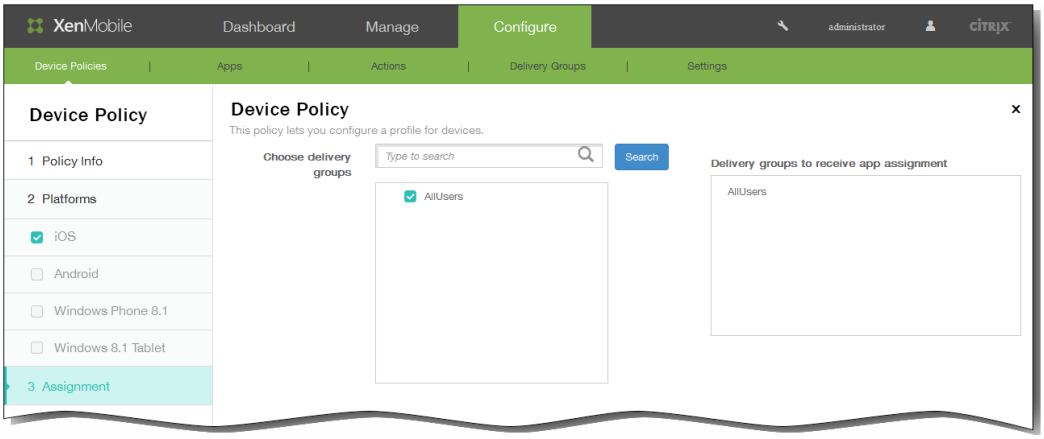
5. Host name or IP address: Geben Sie den Namen oder die IP-Adresse eines Proxyservers ein.
6. Port: Geben Sie die Portnummer des Proxyservers ein.

Bei Auswahl von Windows 8.1 tablet konfigurieren Sie die folgenden Einstellungen:



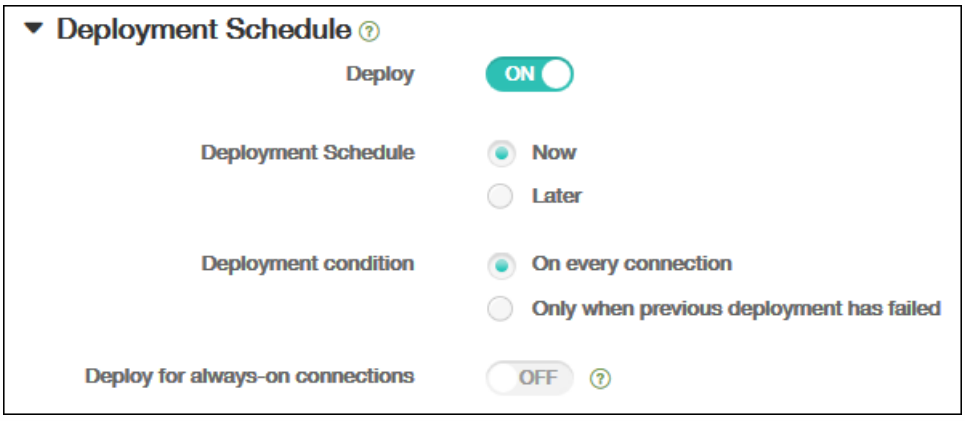
1. Name: Geben Sie einen Namen für das Netzwerk ein.
2. Network name: Geben Sie die SSID ein, die in der Liste der verfügbaren Netzwerke auf den Geräten der Benutzer angezeigt wird.
3. Authentication: Klicken Sie in der Liste auf den Typ der Authentifizierung, der für die WiFi-Verbindung verwendet werden soll.
   - Open
   - WPA Personal
   - WPA-2 Personal
   - WPA Enterprise
   - WPA-2 Enterprise
4. Hidden network (Enable if network is open or off): Wählen Sie aus, ob das Netzwerk ausgeblendet werden soll.
5. Connect automatically: Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.

5. Nach Abschluss der Konfiguration der Einstellungen für eine oder mehrere Plattformen klicken Sie auf Next. Es wird dann die Seite Assigment angezeigt.
6. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



7. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
   1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
   2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
   3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
   4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
   5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
      Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

   Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



8. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Nutzungsbestimmungen-Richtlinie für alle Plattformen hinzu

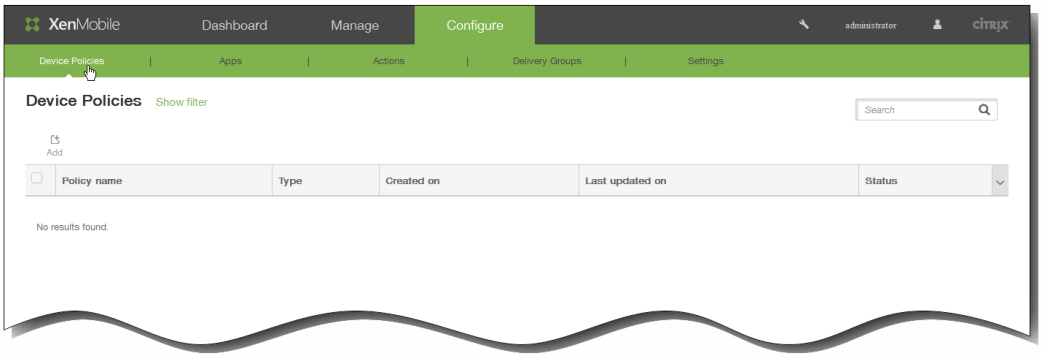
Nov 12, 2015

Sie erstellen Geräterichtlinien für Nutzungsbestimmungen in XenMobile, wenn Sie möchten, dass die Benutzer die unternehmensspezifischen Richtlinien für Verbindungen mit dem Unternehmensnetzwerk akzeptieren. Wenn Benutzer ihr Gerät bei XenMobile registrieren, werden ihnen die Nutzungsbestimmungen angezeigt. Sie müssen diese akzeptieren, damit sie ihr Gerät registrieren können. Lehnen sie die Nutzungsbedingungen ab, wird die Registrierung abgebrochen.

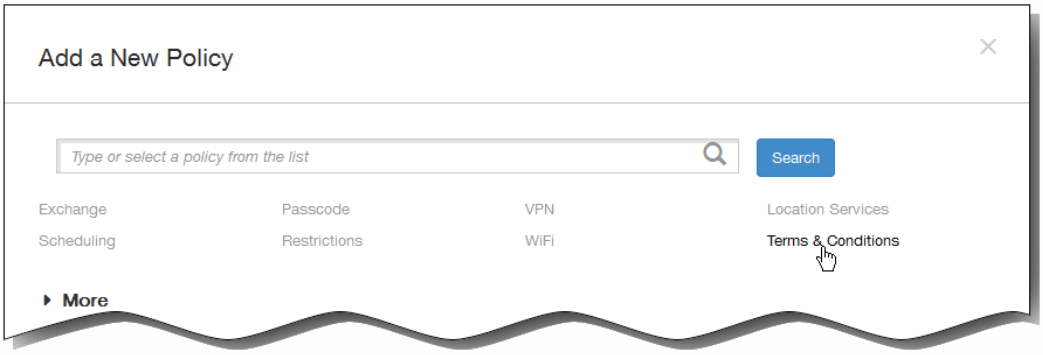
Sie können mehrere Richtlinien für Nutzungsbestimmungen in unterschiedlichen Sprachen erstellen, wenn Ihr Unternehmen internationale Benutzer hat und Sie möchten, dass diese die Nutzungsbestimmungen in ihrer Muttersprache annehmen.

Hinweis: Nutzungsbestimmungen müssen als PDF-Dateien vorliegen.

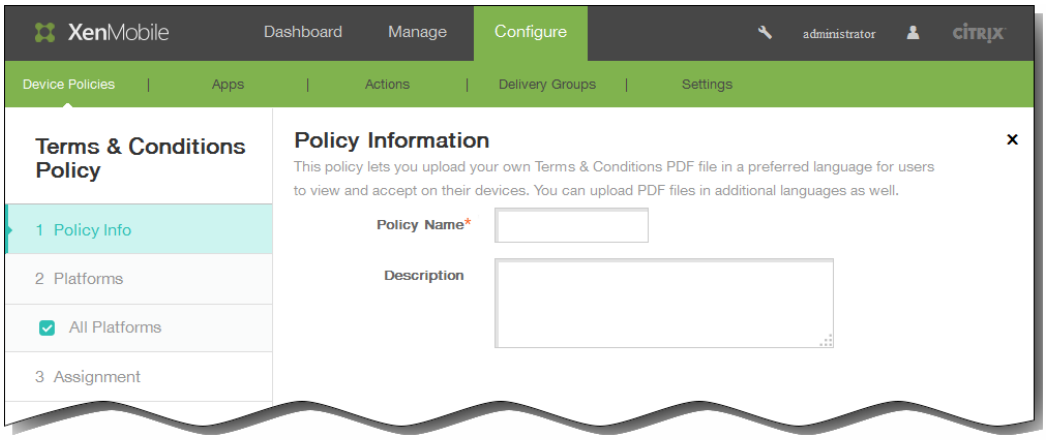
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



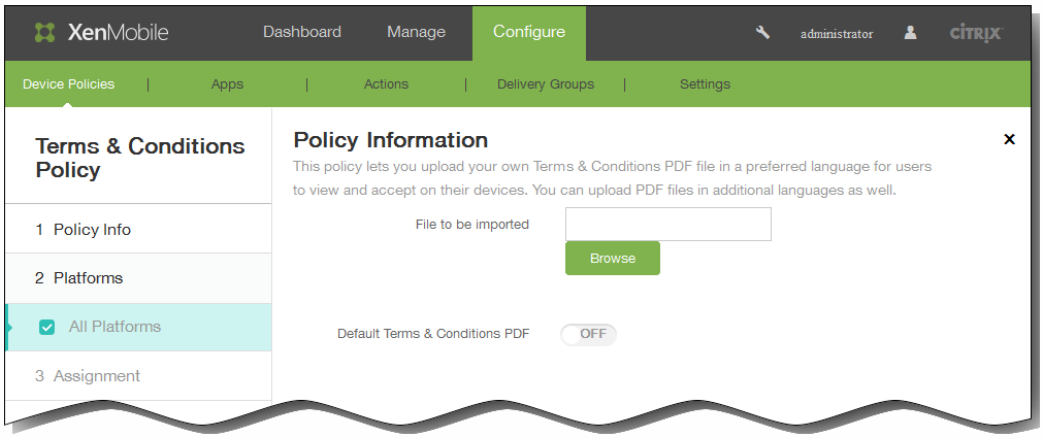
2. Klicken Sie auf Add. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf Terms & Conditions. Die Seite Terms & Conditions Policy wird angezeigt.

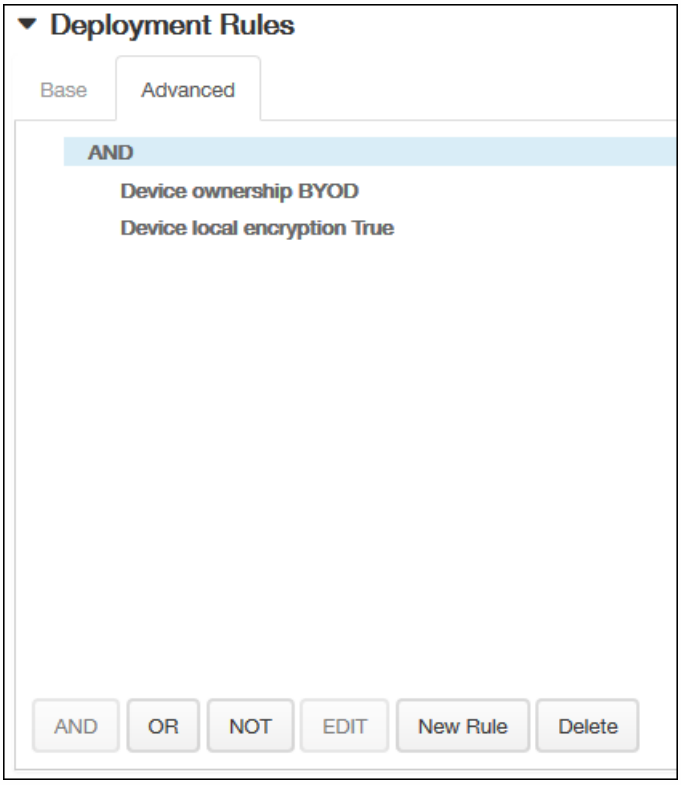


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Informationsseite All Platforms wird angezeigt.



6. Geben Sie auf der Seite All Platforms die folgenden Informationen ein:
   1. File to be imported: Klicken Sie zur Auswahl der zu importierenden Datei mit den Nutzungsbestimmungen auf Browse und navigieren Sie zum Speicherort der Datei.
   2. Default Terms & Conditions PDF: Wählen Sie aus, ob die importierte Datei als Standarddokument für Benutzer verwendet werden soll, die Mitglied mehrerer Gruppen mit unterschiedlichen Nutzungsbestimmungen sind. Der Standardwert ist OFF.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

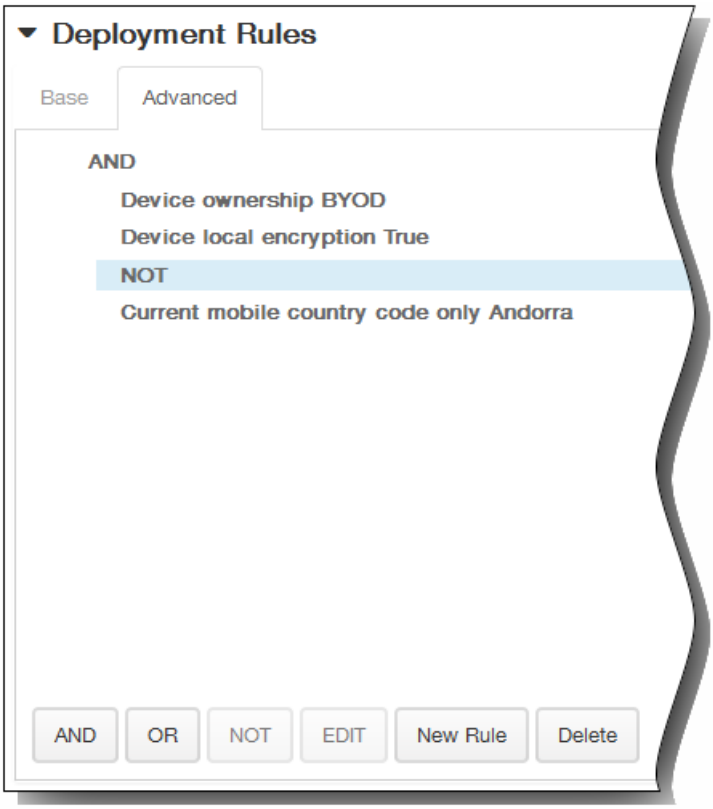
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



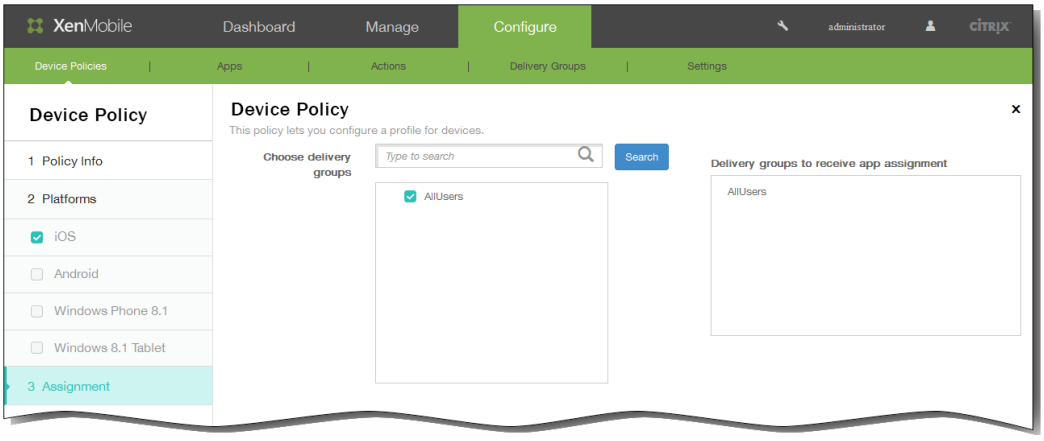
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
    1. Klicken Sie auf AND, OR oder NOT.
    2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
    Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

    3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
    In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



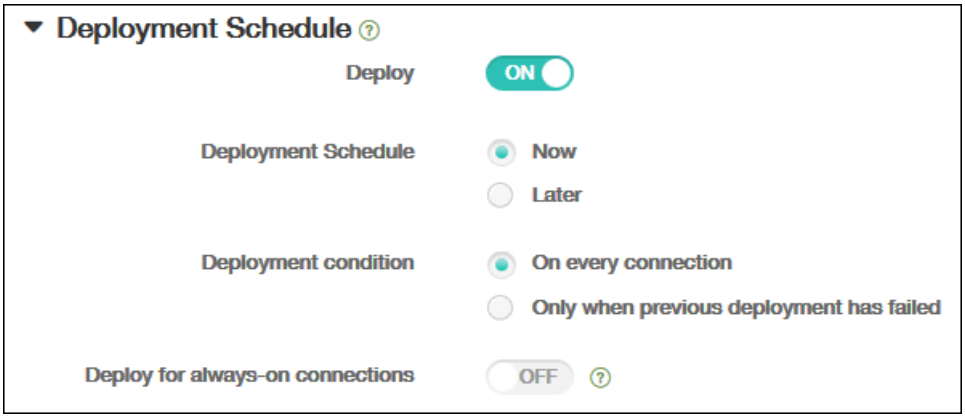
8. Klicken Sie auf Next. Die Seite Assignment für die Nutzungsbestimmungen-Richtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



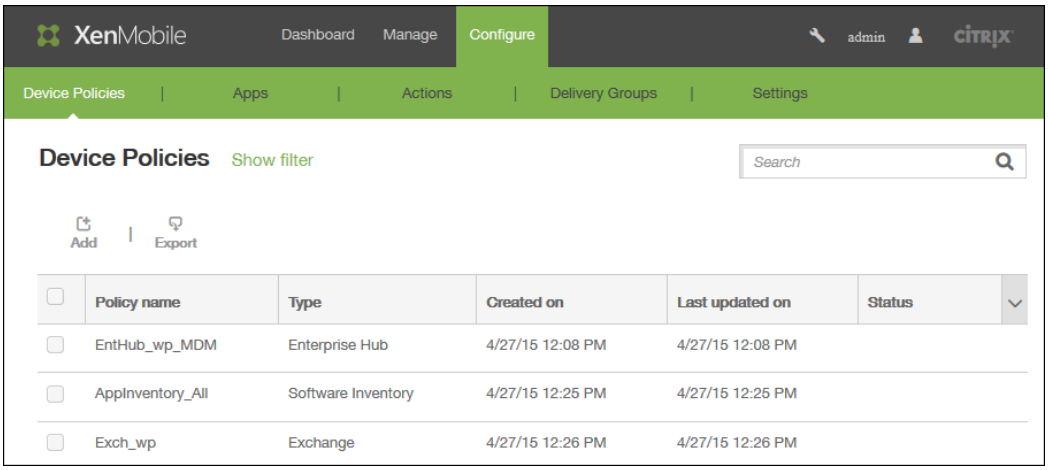
11. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Worx Store-Richtlinie für Geräte hinzu

Nov 12, 2015

Über diese Richtlinie wird festgelegt, wann ein Worx Store-Webclip auf Geräten angezeigt werden soll. Die Richtlinie kann für folgende Plattformen eingerichtet werden: iOS, Android und Windows 8.1-Tablets.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.

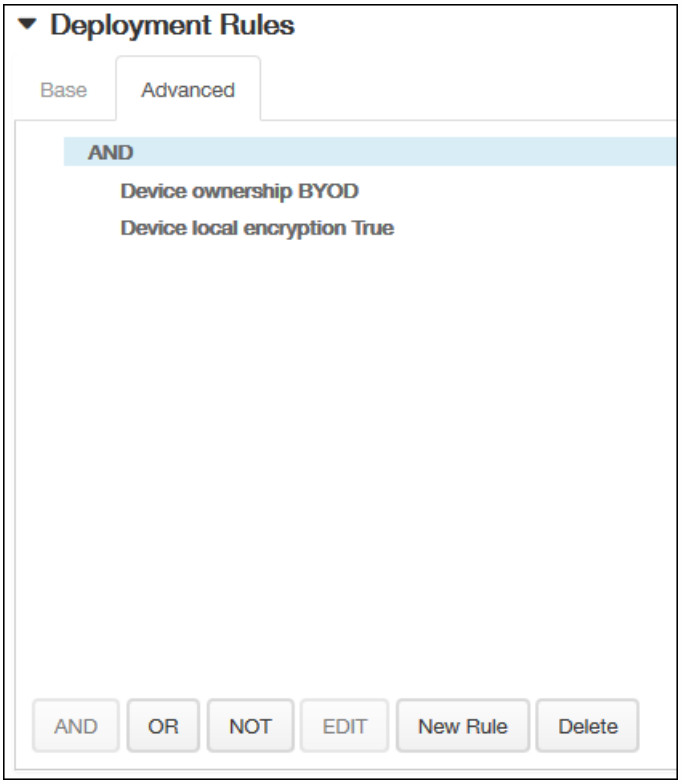


2. Klicken Sie auf der Seite Add a New Policy auf More > Worx Store.
3. Geben Sie auf der Seite Worx Store Policy im Bereich Policy Information folgende Informationen ein und klicken Sie auf Next.
    1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
    2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
4. Wählen Sie unter Platforms die gewünschten Plattformen aus.
5. Behalten Sie für jede ausgewählte Plattform den Standardwert ON bei oder klicken Sie auf OFF, wenn auf den Geräten kein Worx Store-Webclip angezeigt werden soll.
6. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.

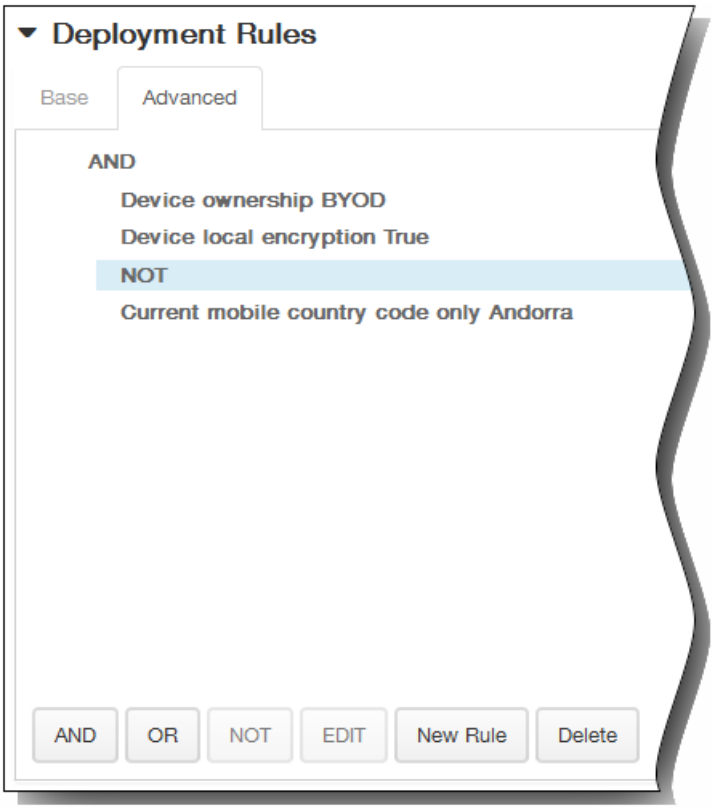
2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.

2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.

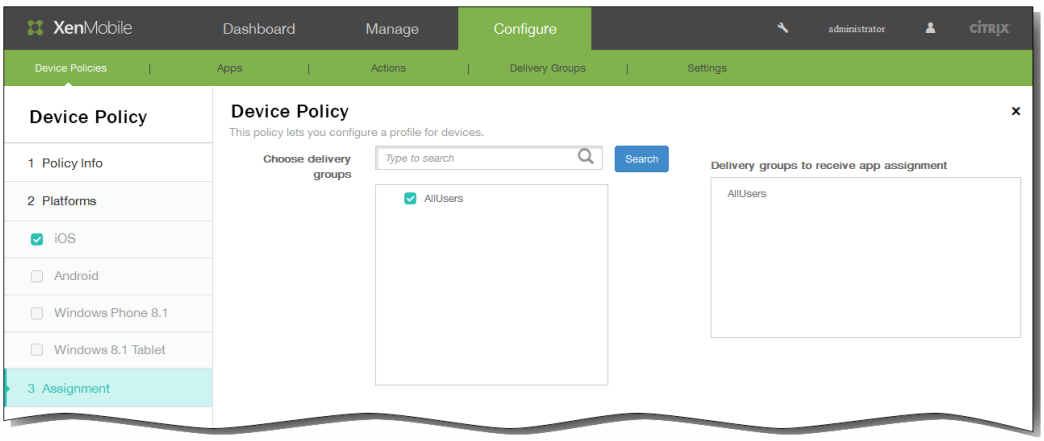


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.
   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



7. Nach Abschluss der Konfiguration der Einstellungen für die ausgewählten Plattformen klicken Sie auf Next. Es wird dann die Seite Assigment angezeigt.
8. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.

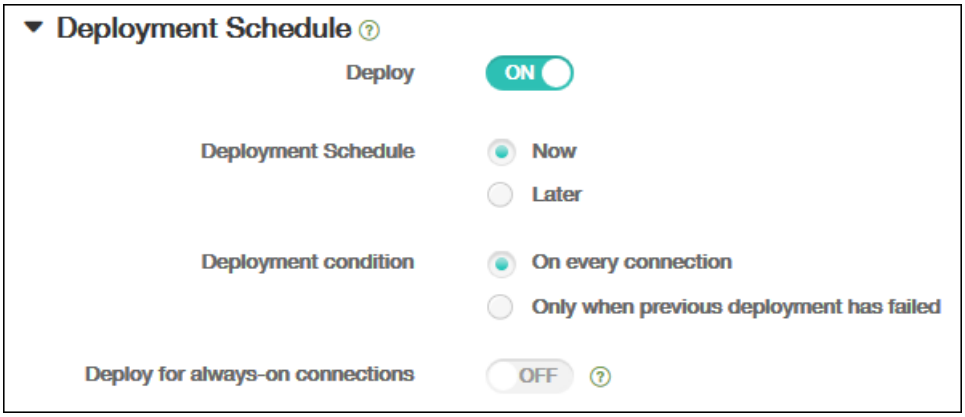


9. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
   1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
   2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
   3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die

Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



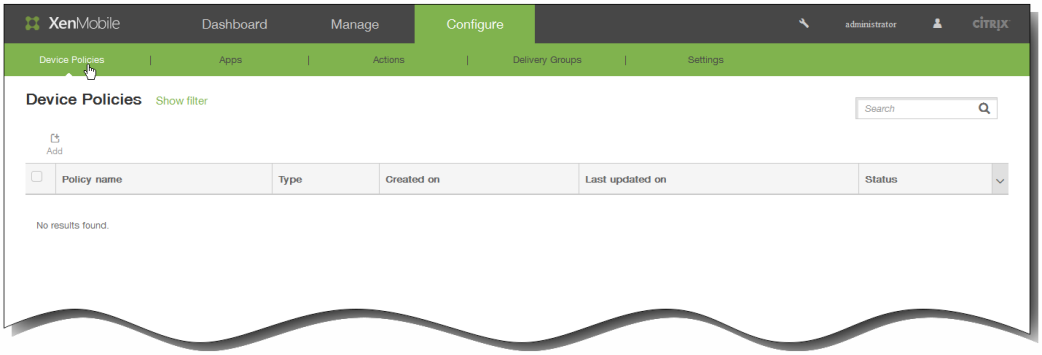
10. Klicken Sie auf Save, um die Richtlinie zu speichern.

XenMobile-Optionsrichtlinien für Geräte

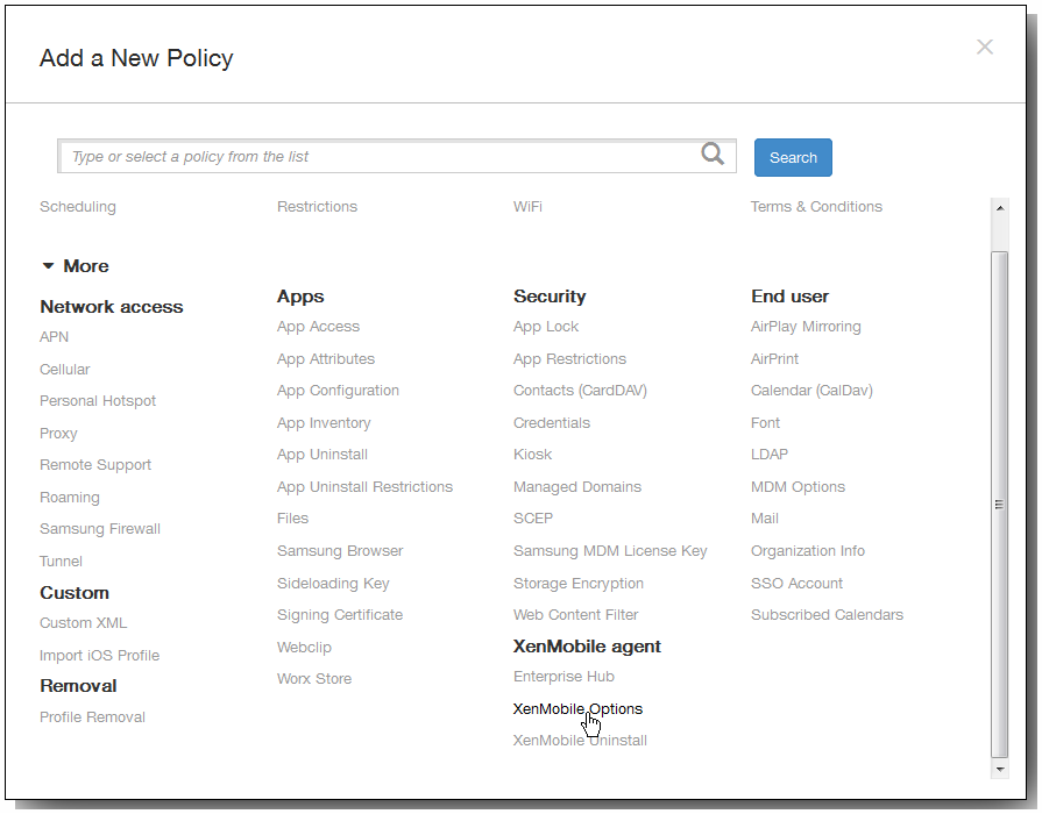
Nov 12, 2015

Sie fügen eine XenMobile-Optionsrichtlinie hinzu, um das Worx Home-Verhalten für Verbindungen zwischen XenMobile und Android- bzw. Symbian-Geräten zu konfigurieren.

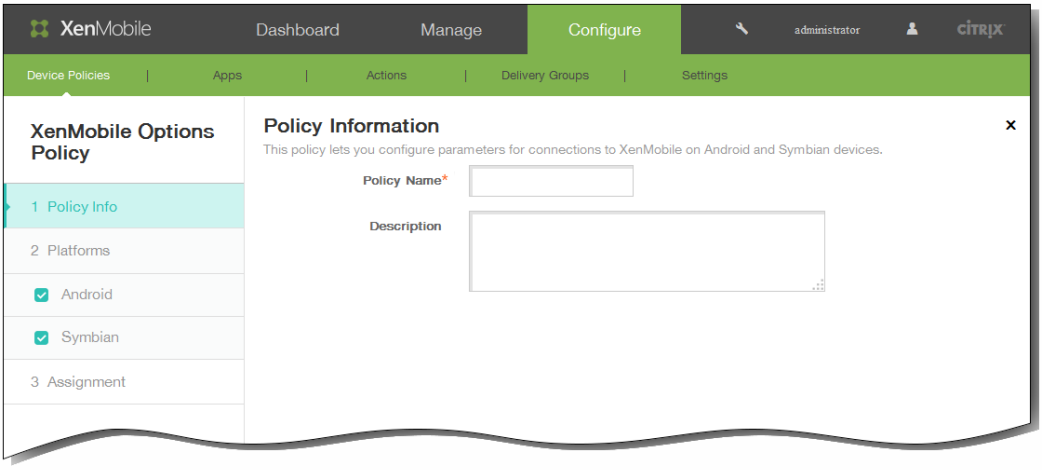
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



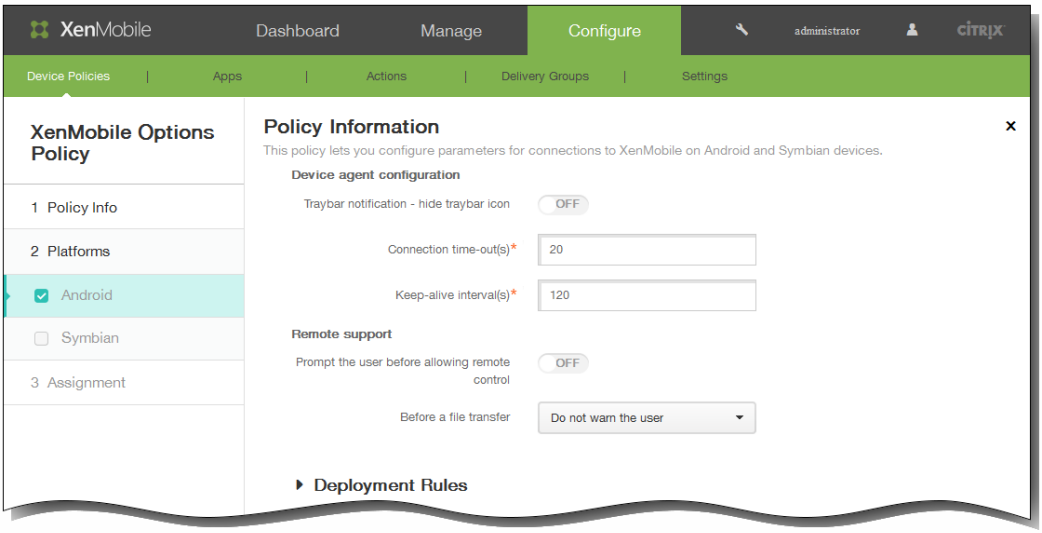
2. Klicken Sie auf Add. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter XenMobile agent auf XenMobile Options. Die Seite XenMobile Options Policy wird angezeigt.



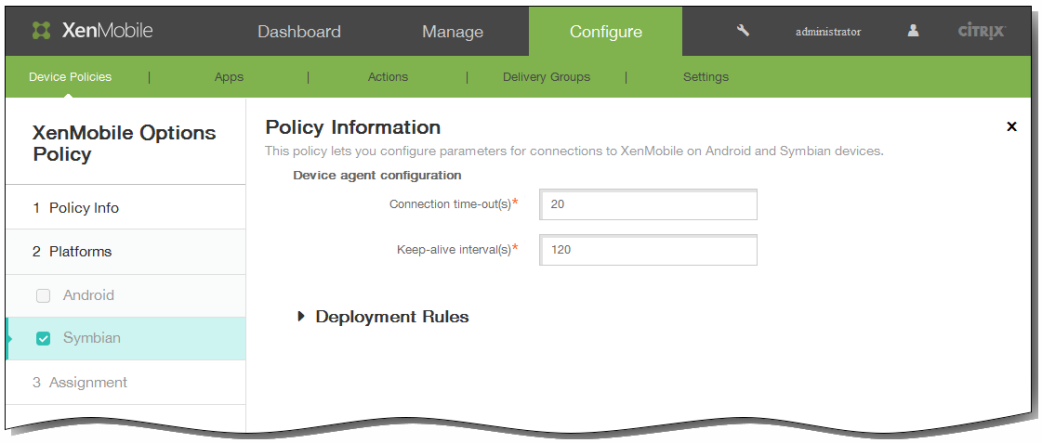
4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
   3. Klicken Sie auf Next.
5. Wählen Sie unter Platforms die gewünschten Plattformen aus.
   Bei Auswahl von Android konfigurieren Sie die folgenden Einstellungen:



1. Traybar notification - hide traybar icon: Wählen Sie aus, ob das Taskleistensymbol angezeigt oder verborgen werden soll.
2. Connection: time-out(s): Geben Sie an, wie lange (in Sekunden) Verbindungen im Leerlauf sein dürfen, bevor eine Zeitüberschreitung eintritt. Der Standardwert ist 20 Sekunden.
3. Keep-alive interval(s): Geben Sie an wie lange (in Sekunden) Verbindungen aufrechterhalten bleiben sollen. Der Standardwert ist 120 Sekunden.
4. Prompt the user before allowing remote control: Wählen Sie aus, ob vor dem Zulassen des Remotesupports eine Aufforderung an den Benutzer erfolgen soll.

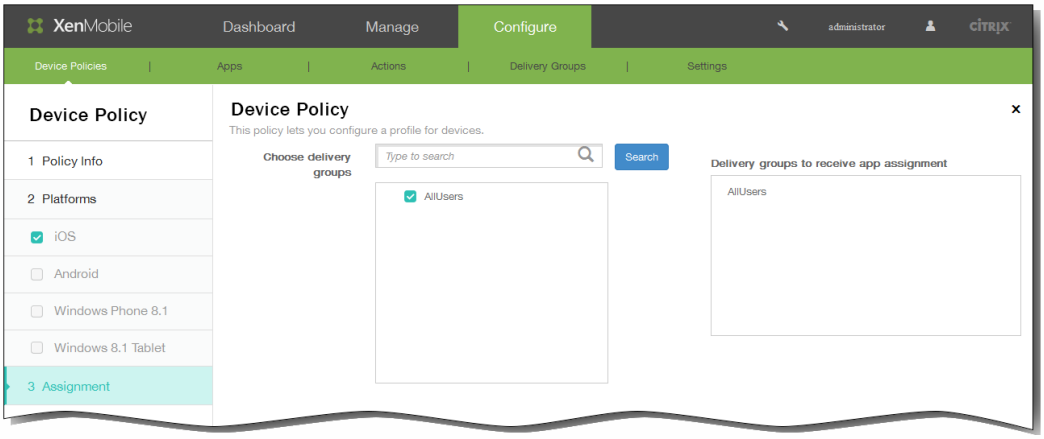
5. Before a file transfer: Wählen Sie in der Liste aus, ob Benutzer bei einer Dateiübertragung gewarnt oder um Erlaubnis gebeten werden sollen.

Bei Auswahl von Symbian konfigurieren Sie die folgenden Einstellungen:



1. Connection: time-outs: Geben Sie an, wie lange (in Sekunden) Verbindungen im Leerlauf sein dürfen, bevor eine Zeitüberschreitung eintritt. Der Standardwert ist 20 Sekunden.
2. Keep-alive interval(s): Geben Sie an wie lange (in Sekunden) Verbindungen aufrechterhalten bleiben sollen. Der Standardwert ist 120 Sekunden.

6. Nach Abschluss der Konfiguration der Einstellungen für eine oder mehrere Plattformen klicken Sie auf Next. Es wird dann die Seite Assigment angezeigt.
7. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.

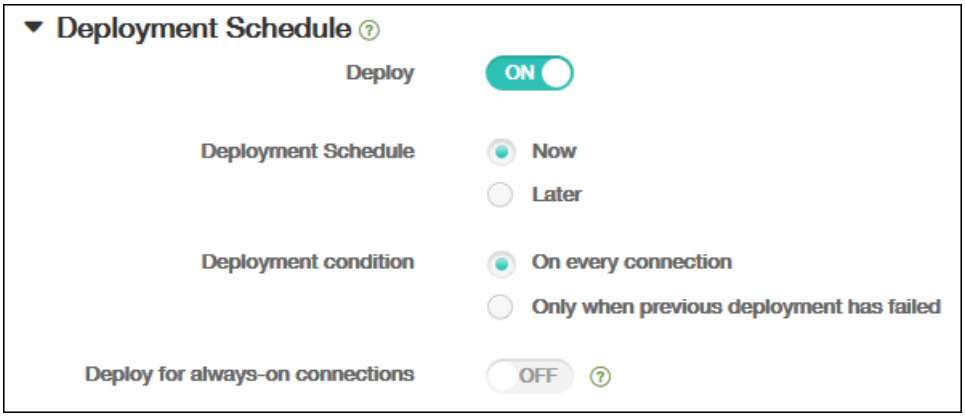


8. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
   1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
   2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
   3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die

Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



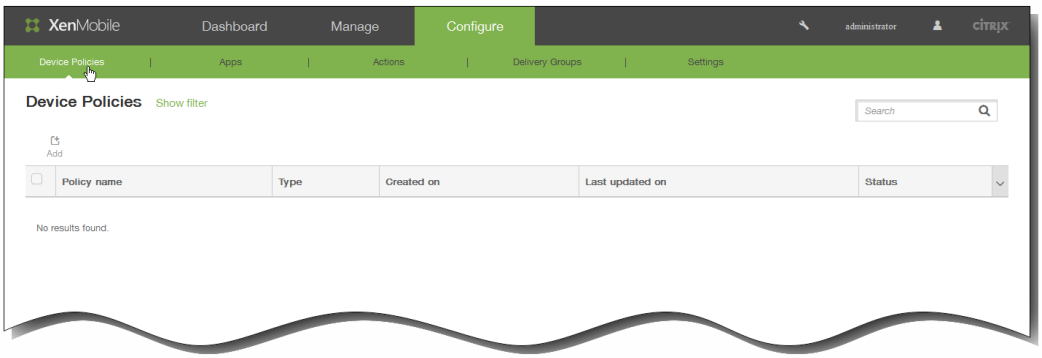
9. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine XenMobile-Deinstallationsrichtlinie für Android-Geräte hinzu

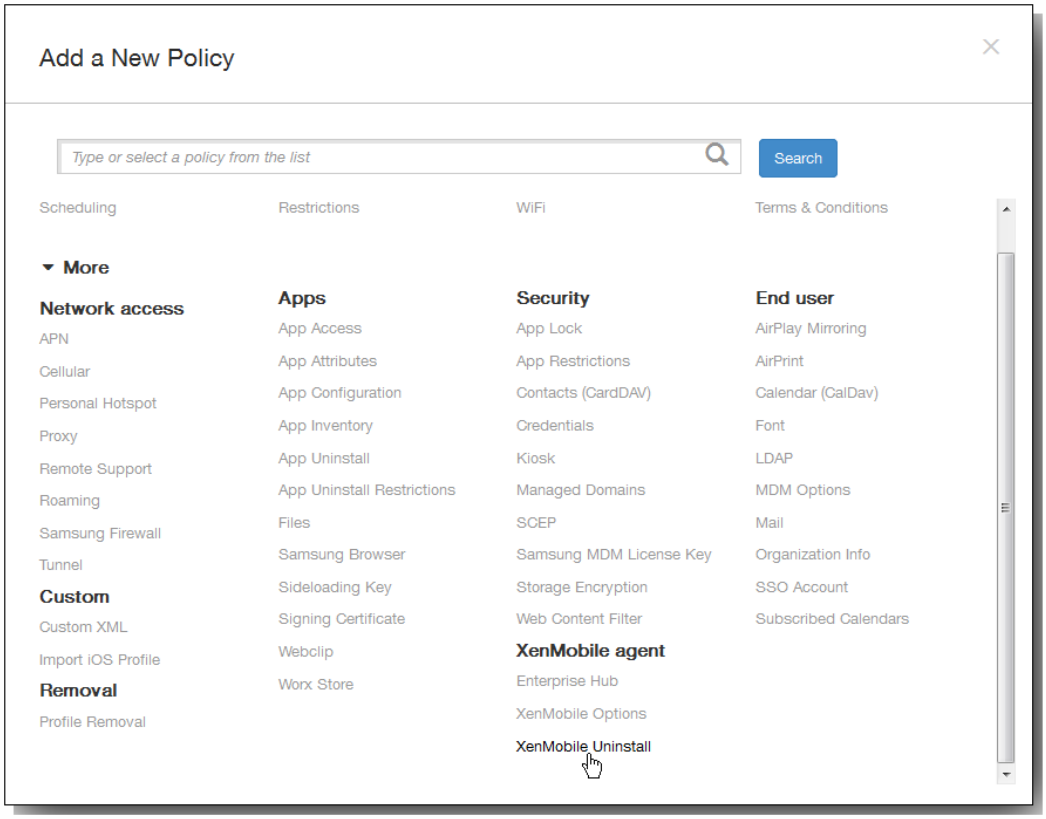
Nov 12, 2015

Sie können in XenMobile eine Geräterichtlinie einrichten, mit der XenMobile von Android-Geräten deinstalliert wird. Wenn diese Richtlinie bereitgestellt wird, entfernt sie XenMobile von allen Android-Geräten in der Bereitstellungsgruppe.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.

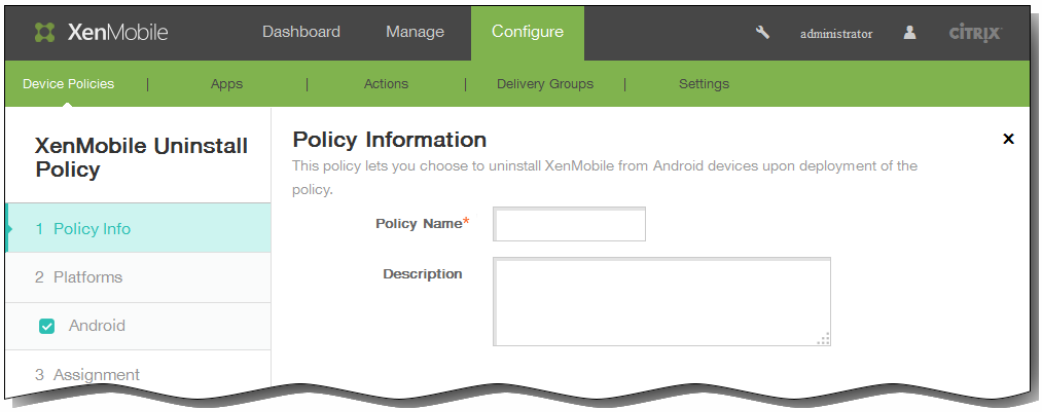


2. Klicken Sie auf Add. Das Dialogfeld Add a New Policy wird angezeigt.

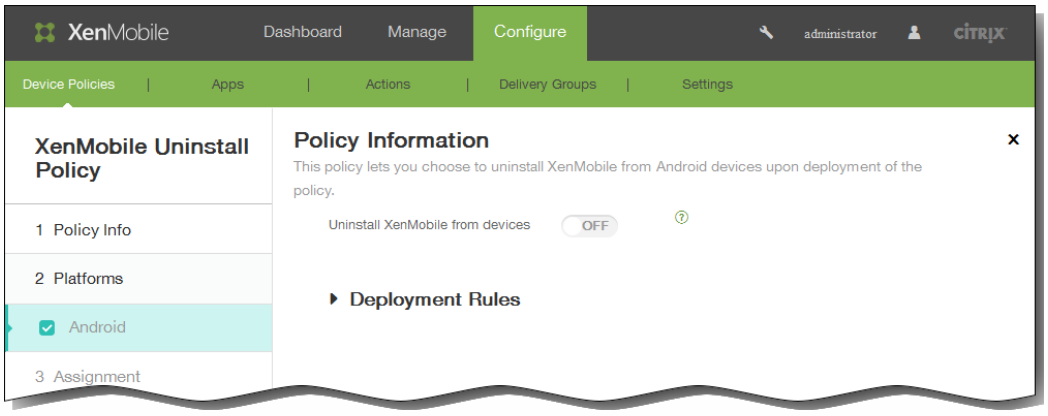


3. Klicken Sie auf More und dann unter XenMobile agent auf XenMobile Uninstall. Die Seite XenMobile Uninstall Policy wird

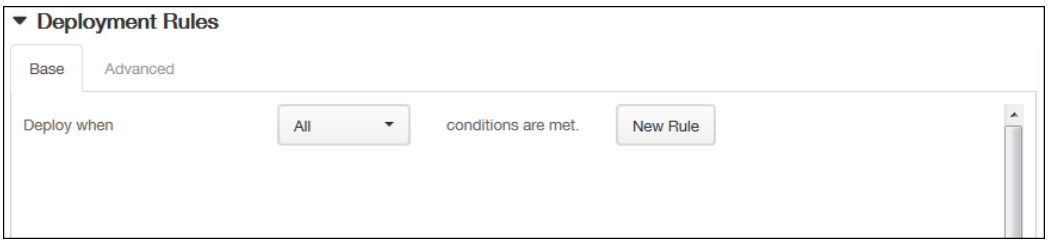
angezeigt.



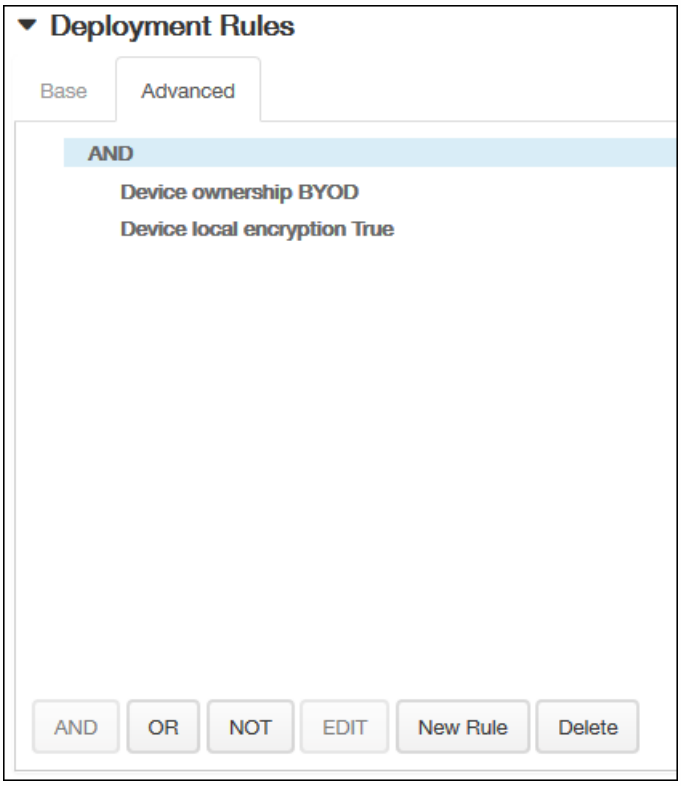
4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Informationsseite Android Platform wird angezeigt.



6. Geben Sie auf der Seite Android Platform die folgenden Informationen ein:
   1. Uninstall XenMobile from devices: Wählen Sie aus, ob XenMobile von Android-Geräten deinstalliert werden soll. Der Standardwert ist OFF.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

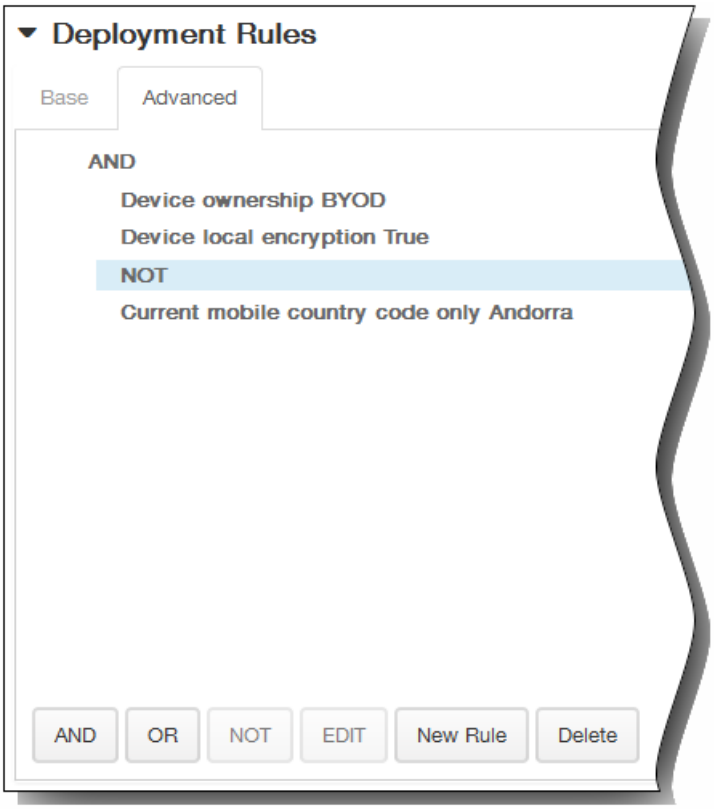


1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
   3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
   4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.

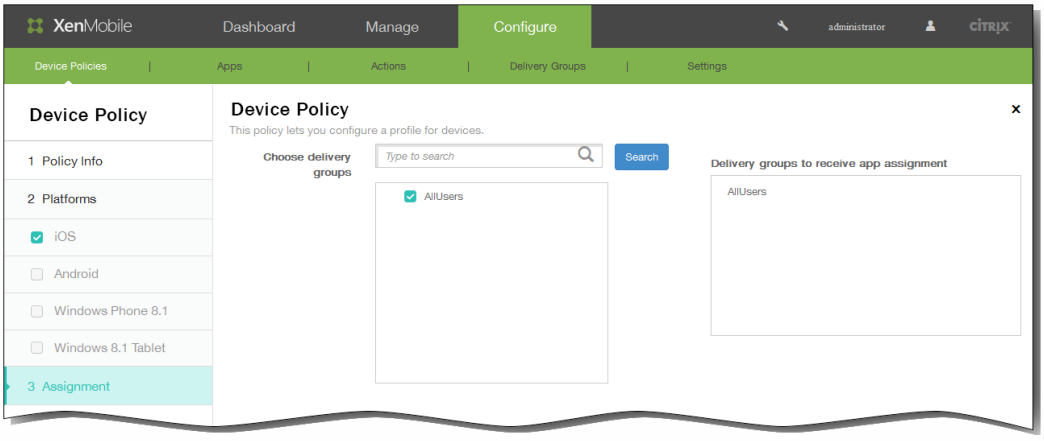


   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



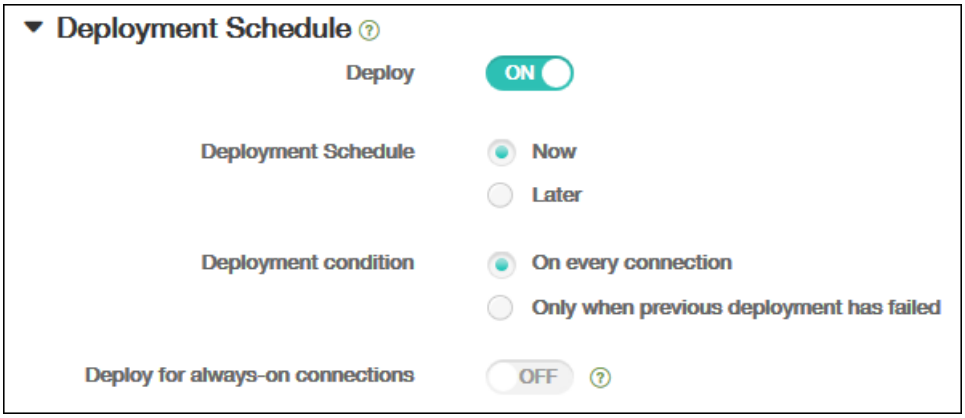
8. Klicken Sie auf Next. Die Seite Assignment für die XenMobile-Deinstallationsrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



10. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



11. Klicken Sie auf Save, um die Richtlinie zu speichern.

So versetzen Sie ein iOS-Gerät mit dem Apple Configurator in den betreuten Modus

Jul 27, 2016

Zur Verwendung des Apple Configurators brauchen Sie einen Apple-Computer mit OS X 10.7.2 oder höher.

> ## Important
>
> Beim Versetzen eines Geräts in den Überwachungsmodus wird die ausgewählte iOS-Version auf dem Gerät installiert und sämtliche zuvor gespeicherten Benutzerdaten und Apps werden von dem Gerät gelöscht.

1. Installieren Sie Apple Configurator aus iTunes.
2. Schließen Sie das iOS-Gerät an den Apple-Computer an.
3. Starten Sie den Apple Configurator. Der Configurator zeigt an, dass ein Gerät zur Vorbereitung für die Überwachung vorhanden ist.
4. So bereiten Sie das Gerät für die Überwachung vor:
    1. Legen Sie für die Betreuung die Option Ein fest. Citrix empfiehlt, diese Einstellung zu aktivieren, wenn Sie ein Gerät kontinuierlich durch regelmäßige Neuanwendung einer Konfiguration steuern möchten.
    2. Geben Sie optional einen Namen für das Gerät ein.
    3. Klicken Sie in iOS auf Latest für die neueste iOS-Version, die Sie installieren möchten.
5. Wenn das Gerät zur Überwachung vorbereitet werden kann, klicken Sie auf Prepare.

Hinzufügen von Apps

Apr 12, 2016

Sie können Apps in XenMobile verwalten. Wenn Sie Apps in der XenMobile-Konsole hinzufügen, können Sie sie in Kategorien einteilen und für Benutzer bereitstellen. Zum Hinzufügen von App-Kategorien folgen Sie den Schritten weiter unten in diesem Abschnitt.

Sie können in XenMobile folgende App-Arten hinzufügen:

- **MDX**: Apps, die mit dem MDX Toolkit umschlossen wurden (und die zugehörigen Richtlinien). Sie stellen MDX-Apps von internen und öffentlichen Stores bereit. Beispiel: WorxMail.
- **Öffentlicher App-Store**: kostenlose oder kostenpflichtige Apps in einem öffentlichen Store, z. B. iTunes oder Google Play. Beispiel: GoToMeeting.
- **Web und SaaS**: Apps, auf die über ein internes Netzwerk (Web-Apps) oder öffentliches Netzwerk (SaaS) zugegriffen wird. Sie können eigene Apps erstellen oder einen der verfügbaren App-Connectors für die Single Sign-On-Authentifizierung bei vorhandenen Web-Apps verwenden. Beispiel: GoogleApps_SAML.
- **Enterprise**: native Apps, die nicht mit dem MDX Toolkit umschlossen wurden und nicht die Richtlinien für MDX-Apps enthalten.
- **Weblinks**: Webadressen (URLs) für eine öffentliche oder private Website oder eine Web-App, die kein Single Sign-On erfordert.

Funktionsweise von mobilen Apps und MDX-Apps

XenMobile unterstützt iOS-, Android- und Windows Phone 8.x-Apps, einschließlich Worx-Apps (z. B. Worx Home, WorxMail und WorxWeb), sowie die Verwendung von MDX-Richtlinien. Mit der XenMobile-Webkonsole können Sie mobile Apps hochladen und dann auf Benutzergeräten bereitstellen. Neben Worx-Apps können Sie die folgenden Arten mobiler Apps hinzufügen:

- Apps, die Sie für Ihre Benutzer entwickeln.
- Apps, in denen Sie Gerätefeatures mit MDX-Richtlinien zulassen oder beschränken möchten.

Mit dem MDX Toolkit von Citrix können mobile Apps für iOS-, Android- und Windows Phone 8.x-Geräte mit Citrix Logik und Richtlinien umschlossen werden. Mit dem Tool können Sie eine Anwendung, die in Ihrer Organisation erstellt wurde, oder eine mobile App, die außerhalb des Unternehmens erstellt wurde, sicher umschließen.

Funktionsweise von Web- und SAAS-Apps

XenMobile enthält eine Reihe von Anwendungsconnectors. Diese Vorlagen können Sie für Single Sign-On (SSO) bei Web- und SaaS-Anwendungen (Software as a Service) und in einigen Fällen auch zum Erstellen und Verwalten von Benutzerkonten konfigurieren. XenMobile umfasst SAML-Connectors (Security Assertion Markup Language). SAML-Connectors werden für Webanwendungen verwendet, die das SAML-Protokoll für SSO und zur Benutzerkontenverwaltung unterstützen. XenMobile unterstützt SAML 1.1 und SAML 2.0.

Sie können auch eigene SAML-Connectors erstellen.

Funktionsweise von Unternehmensapps

In XenMobile können Sie eigene App-Connectors erstellen. Dieser Anwendungstyp befindet sich üblicherweise im internen Netzwerk. Benutzer können eine Verbindung zu den Apps über Worx Home herstellen. Beim Hinzufügen einer Unternehmensapp wird gleichzeitig der App-Connector erstellt.

Funktionsweise des öffentlichen App Store

Sie können Einstellungen zum Abrufen der Namen und Beschreibungen mobiler Apps aus dem Apple App Store, Google Play und dem Windows Store konfigurieren. Bei Abrufen der App-Informationen aus dem Store werden der vorhandene Name und die vorhandene Beschreibung in XenMobile überschrieben.

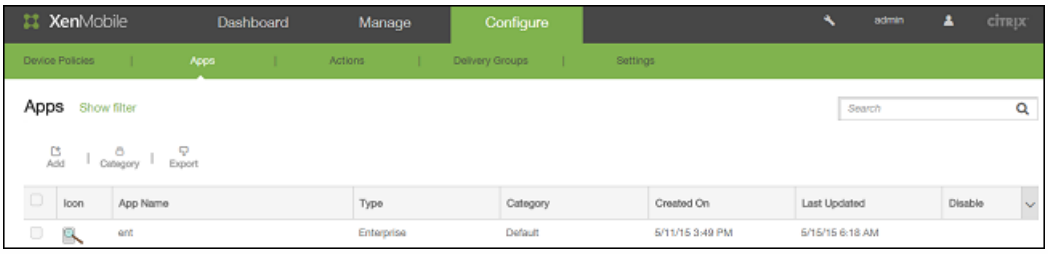
Funktionsweise von Weblinks

Ein Weblink ist die Webadresse einer Internet- oder Intranetsite. Er kann auch auf eine Web-App zeigen, für die kein SSO erforderlich ist. Wenn Sie die Konfiguration eines Weblinks abgeschlossen haben, wird dieser als Symbol im Worx Store angezeigt. Der Link wird mit der Liste der verfügbaren Anwendungen und Desktops angezeigt, wenn Benutzer sich bei Worx Home anmelden.

Das Verfahren zum Hinzufügen einer App mit der Konsole besteht aus vier Schritten:

- Hinzufügen von Informationen über die App
- Auswählen und Konfigurieren der App für jede unterstützte Plattform, z. B. iOS oder Android
- Definieren einer optionalen Genehmigungsmethode
- Festlegen optionaler Bereitstellungsgruppenzuweisungen

1. Klicken Sie in der XenMobile-Konsole auf **Configure > Apps**.
   Die Seite "Apps" wird angezeigt.



   Hinweis: Wenn Sie zum ersten Mal eine Verbindung mit der XenMobile-Konsole herstellen, ist die Apps-Tabelle leer, es werden nur die Optionen **Add** und **Category** angezeigt.
2. Klicken Sie auf Add und folgen Sie je nach App-Typ den Anweisungen in einem der folgenden eDocs-Abschnitte:

- So fügen Sie XenMobile eine MDX-App hinzu
- So fügen Sie XenMobile eine App aus einem öffentlichen App-Store hinzu
- So fügen Sie XenMobile Web- und SaaS-Apps hinzu
- So fügen Sie XenMobile eine Unternehmensapp hinzu
- So fügen Sie XenMobile eine Weblink-App hinzu

Hinweis: Nachdem Sie Apps hinzugefügt haben, werden diese in der Tabelle auf der Seite "Apps" angezeigt, wo Sie sie bearbeiten oder kategorisieren können.

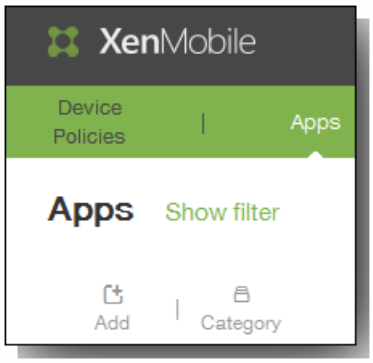
> **Hinweis**
>
> Wenn Sie nach dem Upgrade auf XenMobile 10.1 mobile Worx-Apps in XenMobile 10.1 aktualisieren, die Sie in einem früheren Release konfiguriert haben, werden die App-Einstellungen nicht mehr in der XenMobile-Konsole angezeigt. Sie müssen die Einstellungen für diese Apps erneut bearbeiten und konfigurieren. Die Apps müssen nicht neu installiert werden. Diesen Schritt brauchen Sie nur einmal auszuführen. Die Werte bleiben bei zukünftigen Updates erhalten, wenn Sie die App oder den Server aktualisieren.

So fügen Sie XenMobile eine MDX-App hinzu

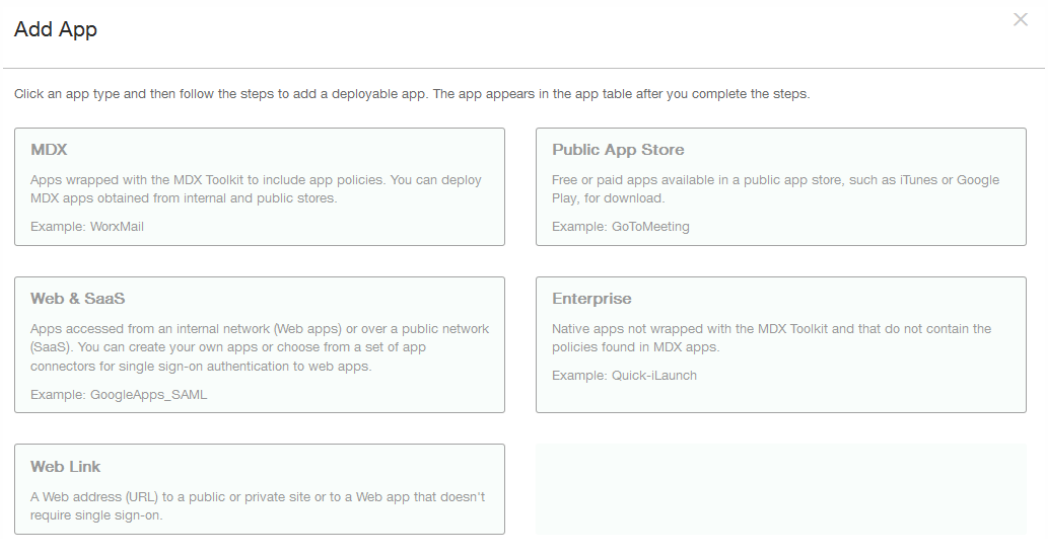
Apr 12, 2016

Wenn Sie eine umschlossene mobile MDX-App für iOS-, Android- oder Windows Phone-Geräte erhalten, können Sie diese in XenMobile hochladen. Nach dem Hochladen der App können Sie die App- und Richtlinieneinstellungen konfigurieren. Weitere Informationen über die verfügbaren App-Richtlinien für jeden Plattformtyp finden Sie unter MDX-Richtlinien für iOS, Android und Windows Phone. In dem Abschnitt finden Sie ebenfalls detaillierte Richtlinieninformationen.

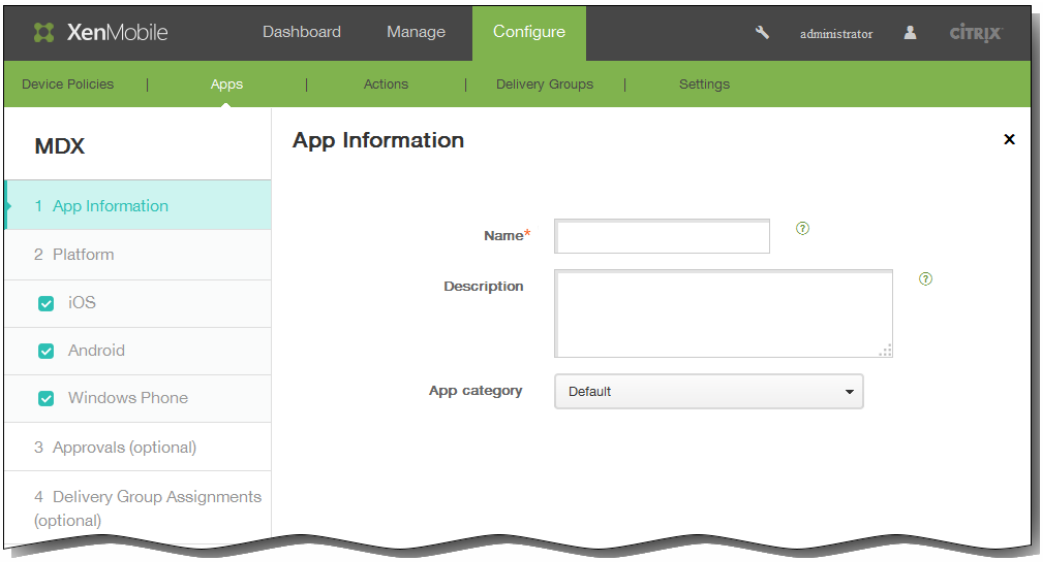
1. Klicken Sie in der XenMobile-Konsole auf Configure > Apps. Die Seite Apps wird angezeigt.
2. Klicken Sie auf Add.



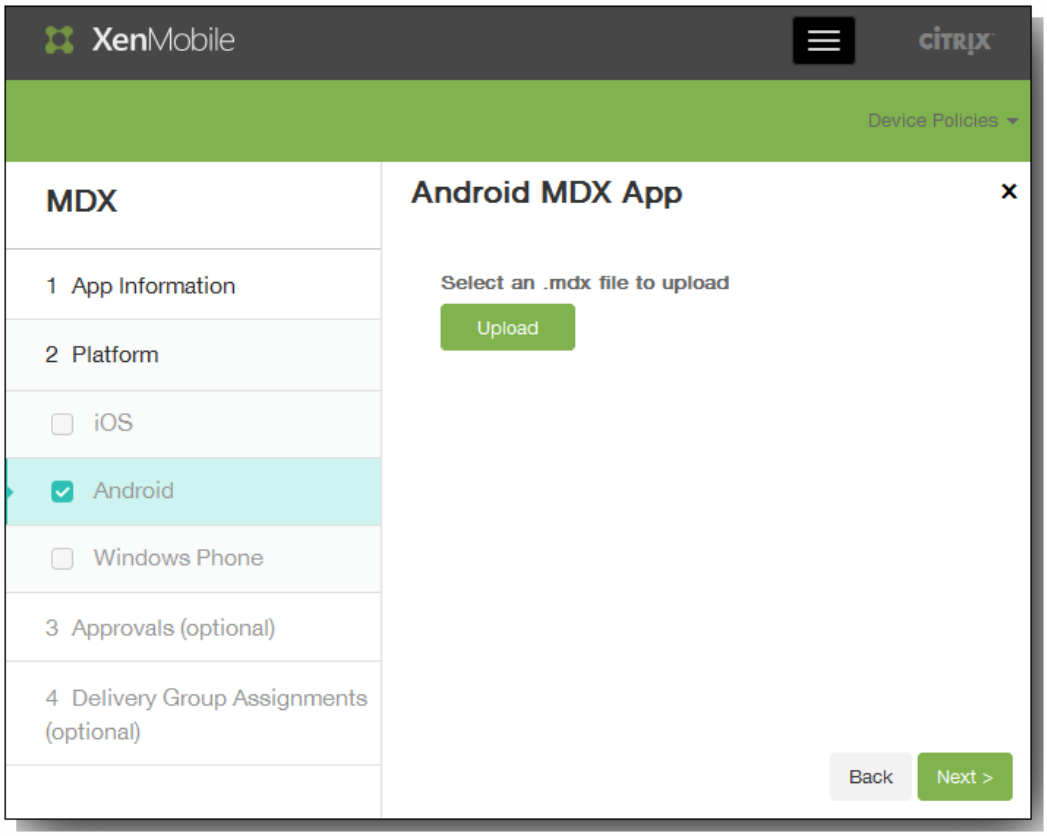
3. Klicken Sie auf der Seite Add App auf MDX.



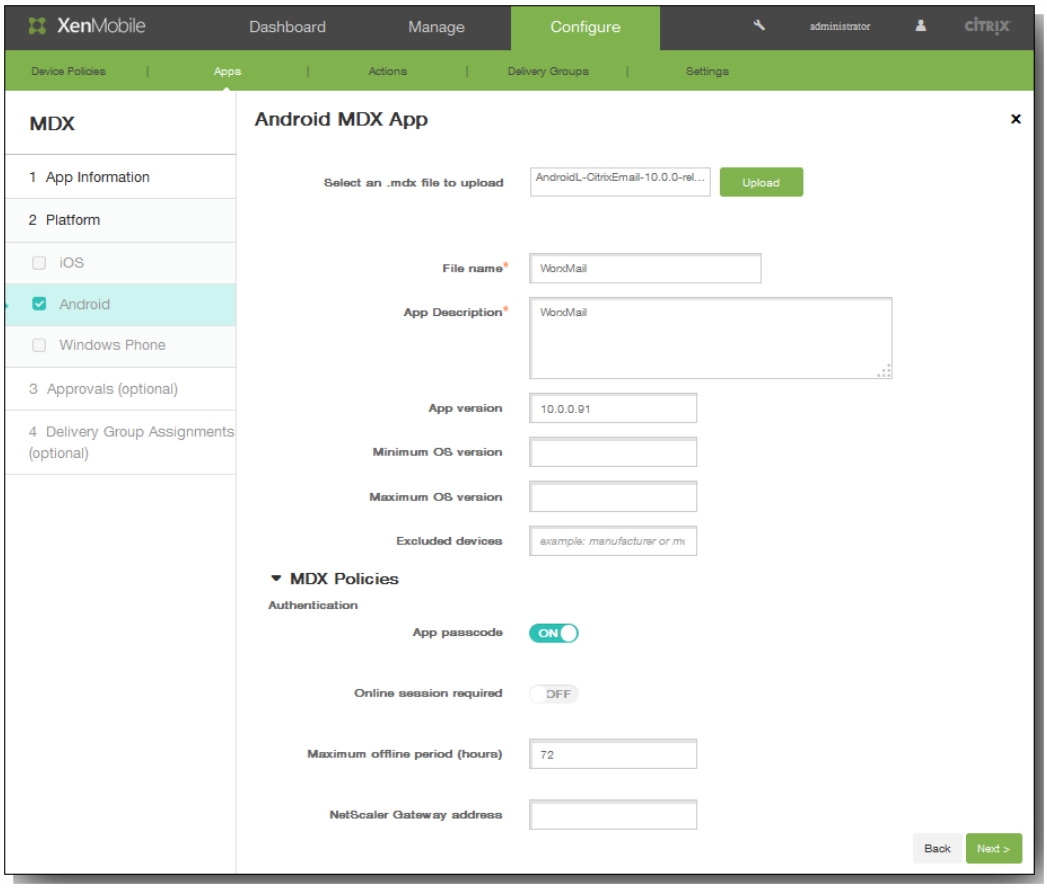
4. Geben Sie auf der Seite App Information unter Name einen Namen und optional unter Description eine Beschreibung für die App ein. Diese Felder werden für interne Zwecke verwendet. Wenn Sie Apps für mehrere Geräte hinzufügen, verwenden Sie die Kontrollkästchen im linken Bereich des Bildschirms, um diese auszuwählen.



5. Klicken Sie in der Liste App category auf die App-Kategorie. Weitere Informationen finden Sie unter Hinzufügen einer Kategorie.
6. Klicken Sie auf Next.
7. Klicken Sie auf Upload, um eine MDX-Datei für den Upload auszuwählen und klicken Sie dann auf Next.

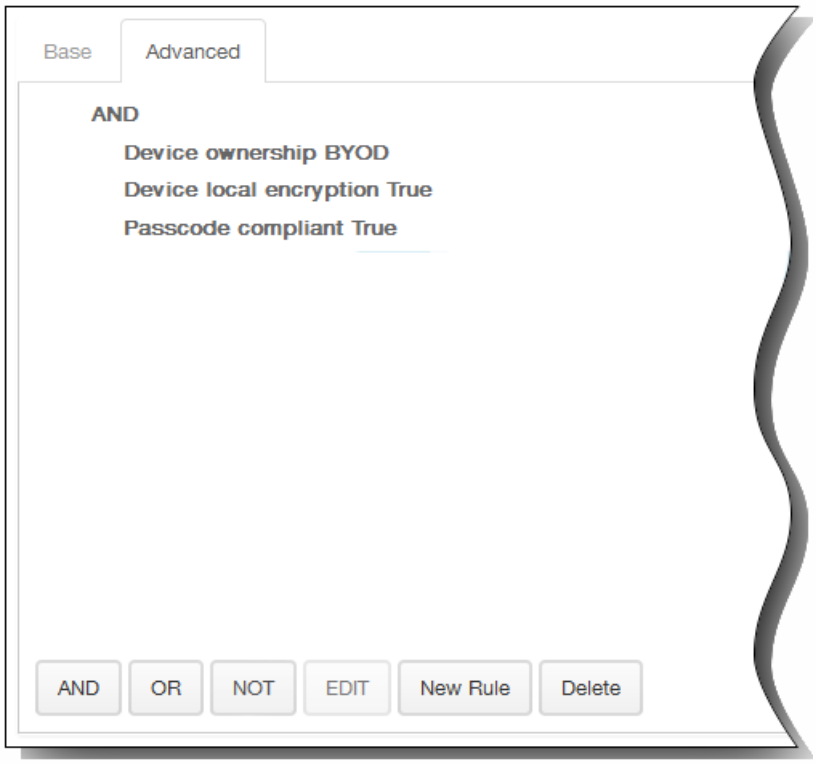


Die Felder für die App-Details und MDX-Richtlinien werden angezeigt.



8. Konfigurieren Sie die folgenden Einstellungen:
   1. File name: Geben Sie den Dateinamen für die App ein.
   2. App Description: Geben Sie eine Beschreibung für die App ein.
   3. Minimum OS version: Geben Sie die älteste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
   4. Maximum OS version: Geben Sie die neueste Betriebssystemversion ein, unter der die App ausgeführt werden kann.
   5. Excluded devices: Geben Sie Hersteller oder Gerätemodelle an, auf denen die App nicht ausgeführt werden kann.
9. Konfigurieren Sie im Bereich MDX Policies Richtlinieneinstellungen für Authentifizierung, Gerätesicherheit, Netzwerkanforderungen und -zugriff, Verschlüsselung, App-Interaktion, App-Einschränkungen usw., die durch den Worx Store durchgesetzt werden sollen.
   Hinweis: In der Konsole können Sie mit dem Mauszeiger auf den Namen einer Richtlinie zeigen und so eine Beschreibung der Richtlinie anzeigen. Weitere Informationen über App-Richtlinien für MDX-Apps, z. B. eine Tabelle mit Informationen dazu, welche Richtlinien für welche Plattformen gelten, finden Sie unter MDX-Richtlinien für iOS, Android und Windows Phone.
10. Erweitern Sie Deployment Rules. Standardmäßig wird die Registerkarte Base angezeigt.

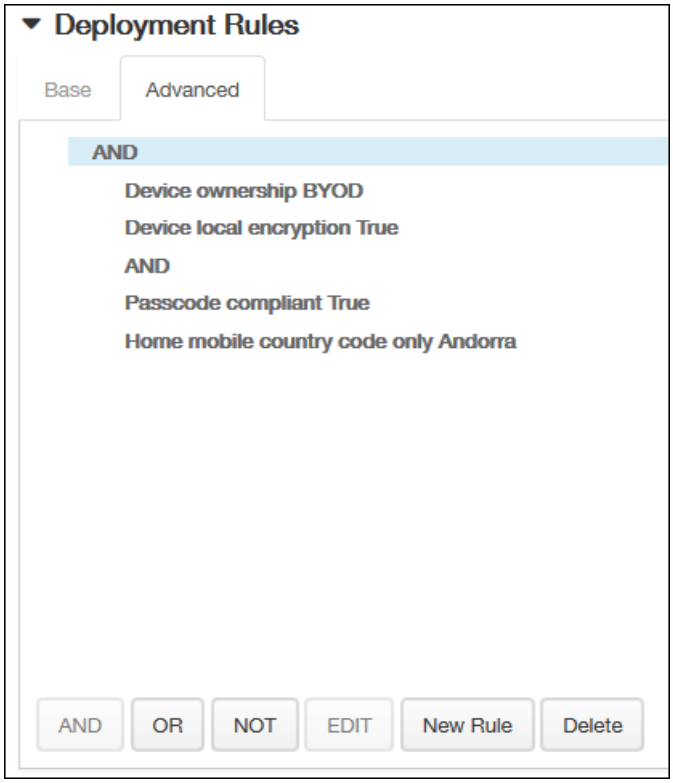
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die App bereitgestellt werden soll.
    1. Sie können die App bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist Alle.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



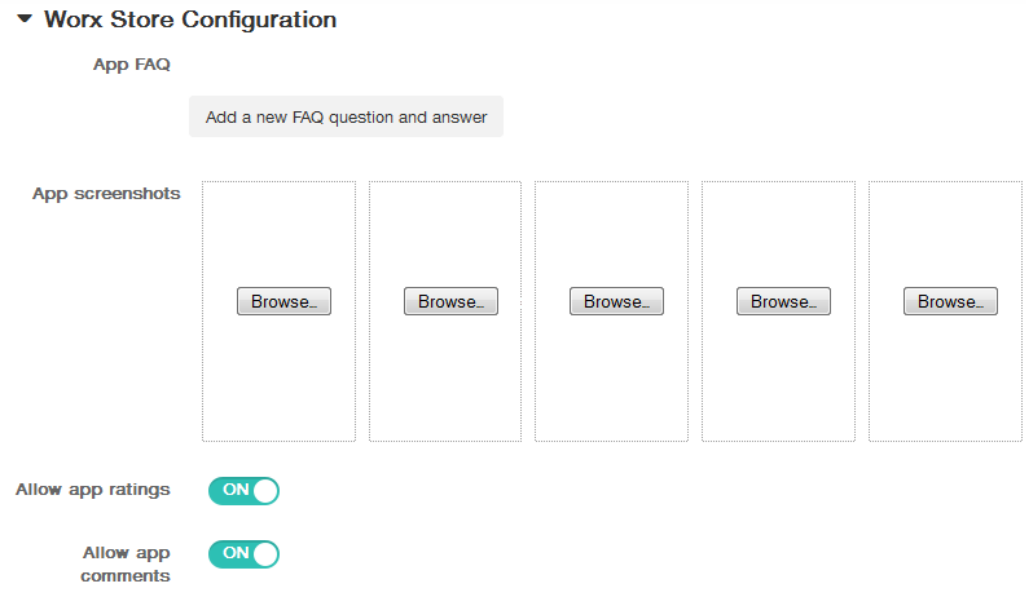
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
    1. Klicken Sie auf AND, OR oder NOT.
    2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
    Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

    3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
    In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.

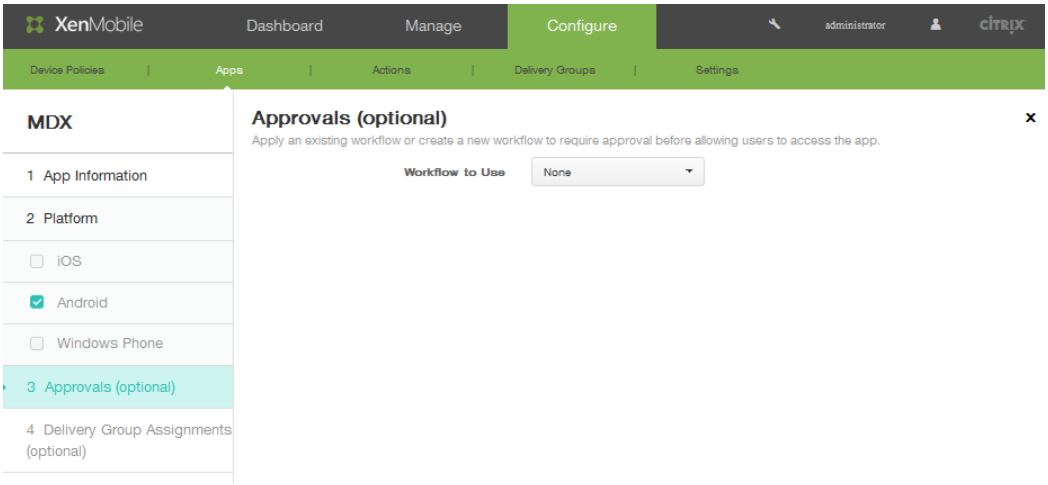


11. Erweitern Sie Worx Store Configuration, um FAQ für die App oder Bildschirmaufnahmen zur Klassifizierung des App im Worx Store hinzuzufügen. Die hochgeladene Grafik muss im PNG-Format sein. Sie können keine GIF- oder JPEG-Bilder hochladen.

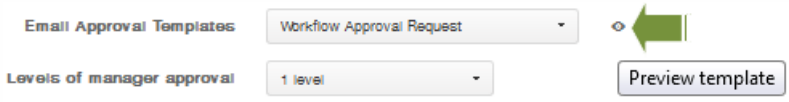


Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.

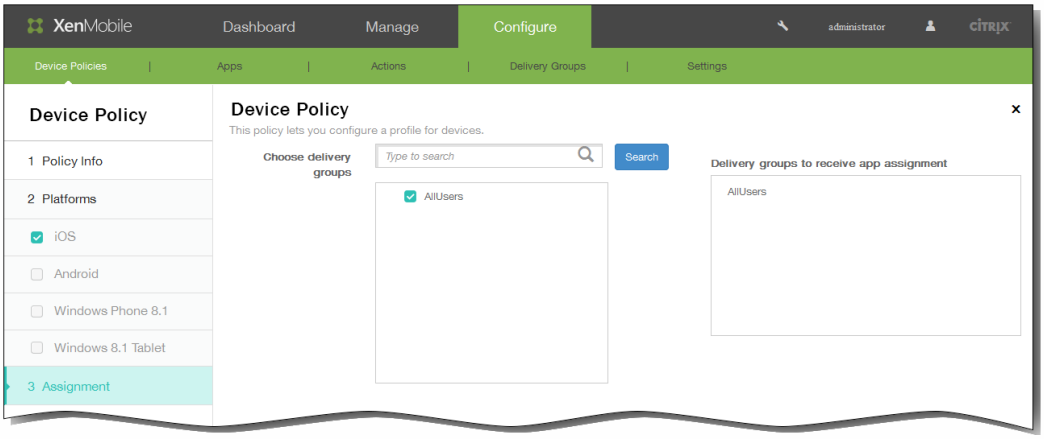
12. Klicken Sie unter Allow app comments auf ON, um eine Kommentierung der App durch die Benutzer zuzulassen.
13. Klicken Sie auf Next. Die Seite Approvals wird angezeigt.



14. Wenn Sie einen neuen Workflow erstellen, werden in der XenMobile-Konsole nun Konfigurationsoptionen für den Freigabeprozess angezeigt. Die betreffenden Felder werden in den nachfolgenden Schritten erläutert. Konfigurieren Sie diese Felder, wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist.
    1. Geben Sie unter **Name** einen Namen für den Workflow ein.
    2. Geben Sie optional unter **Description** eine Beschreibung ein.
    3. Klicken Sie unter **Email Approval Templates** auf eine Benachrichtigungsoption. Klicken Sie auf das **Augensymbol**, um eine Vorschau der ausgewählten Vorlage anzuzeigen.

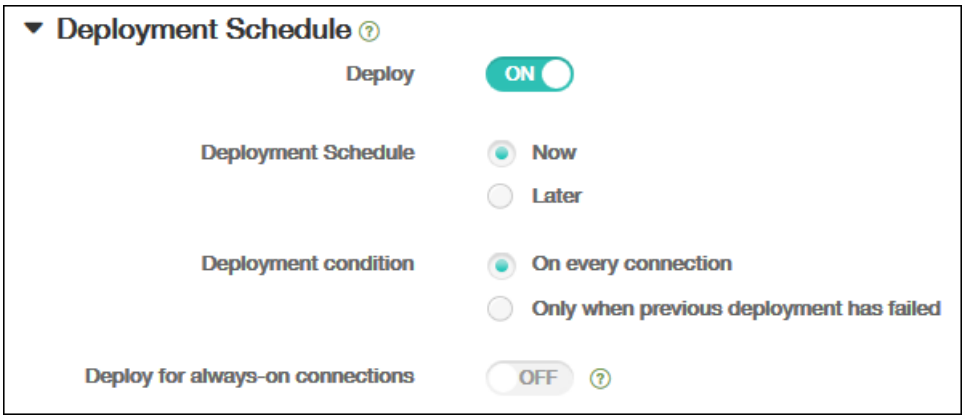


    4. Klicken Sie unter **Levels of manager approval** auf eine Stufe zwischen None und 3. .
    5. Klicken Sie unter **Select Active Directory domain** auf die Domäne.
    6. Geben Sie unter Find additional required approvers optional weitere Freigabeberechtigte ein und klicken Sie auf Search.
15. Klicken Sie auf Next.
16. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



17. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
    4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
    5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
    Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

    Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



18. Klicken Sie auf Save. In der XenMobile-Konsole werden die App-Informationen angewendet.

Erstellen von App-Kategorien in XenMobile

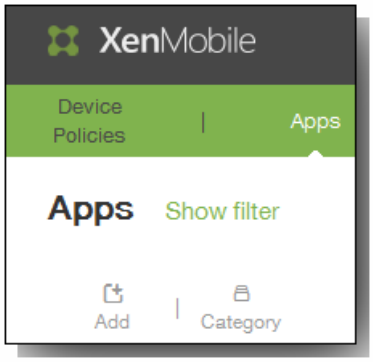
Nov 12, 2015

Wenn Benutzer sich bei Worx Home anmelden, erhalten sie eine Liste der Apps, Weblinks und Stores, die Sie in XenMobile hinzugefügt und konfiguriert haben. Mit App-Kategorien können Sie dafür sorgen, dass Benutzer nur auf die von Ihnen vorgesehenen Apps, Weblinks oder Stores zugreifen können. Sie können beispielsweise eine Kategorie "Finanzen" erstellen und dann nur Apps hinzufügen, die für den Bereich Finanzen relevant sind. Ebenso können Sie eine Kategorie "Vertrieb" konfigurieren, der nur Apps für den Vertrieb zugewiesen werden. Sie können außerdem eine Apple-Kategorie für den App Store konfigurieren.

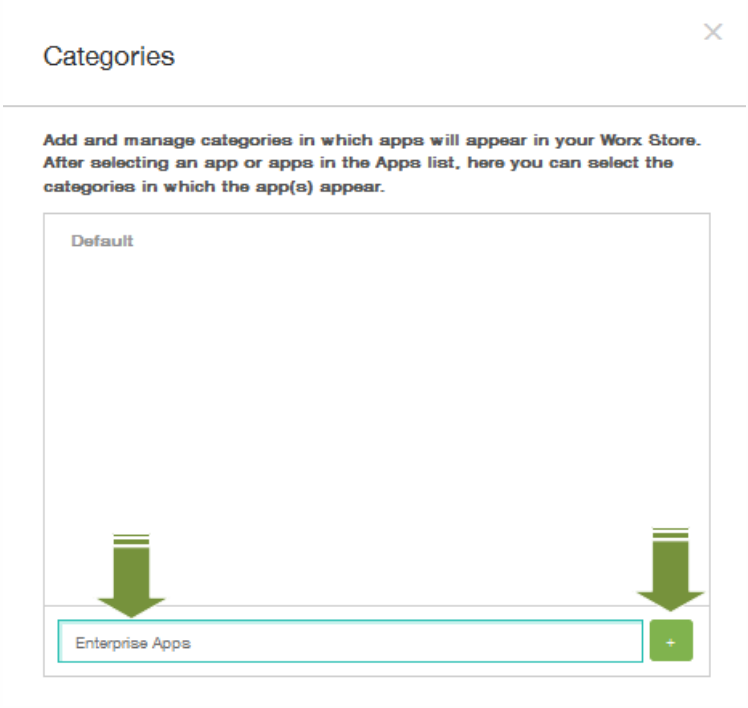
Kategorien werden in XenMobile auf der Seite Apps konfiguriert. Wenn Sie eine App, einen Weblink oder einen Store konfiguriert bzw. bearbeitet haben, können Sie diese(n) einer Kategorie zuweisen.

So fügen Sie eine Kategorie hinzu

1. Klicken Sie in der XenMobile-Konsole auf Configure > Apps. Die Seite Apps wird angezeigt.
2. Klicken Sie auf der Seite Apps auf Category.

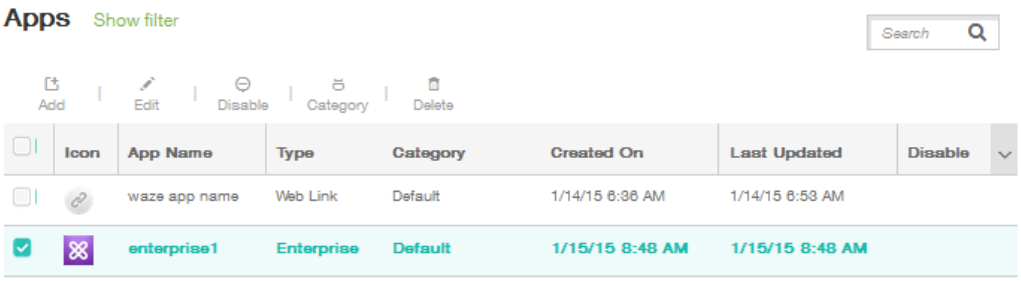


3. Geben Sie im Dialogfeld Categories den Namen der Kategorie ein, die Sie hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) . Geben Sie beispielsweise *Enterprise Apps* ein und klicken Sie auf das Pluszeichen (+).

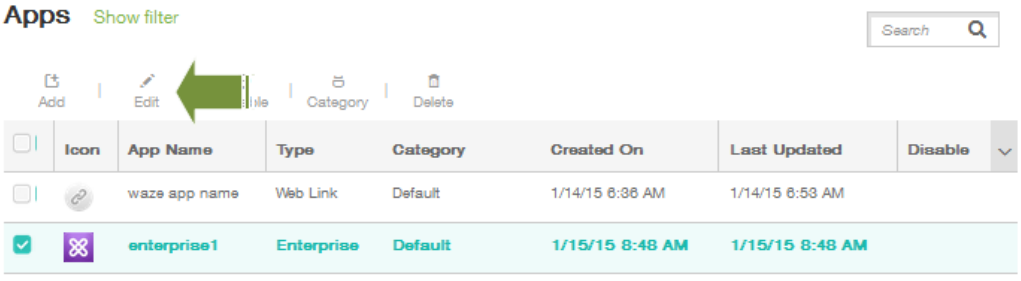


Die neu erstellte Kategorie wird hinzugefügt und wird im gleichen Dialogfeld Categories angezeigt. Wenn keine Kategorien konfiguriert sind, wird nur die Kategorie **Default** angezeigt.

4. Wiederholen Sie Schritt 3 beliebig oft für jede hinzuzufügende Kategorie und schließen Sie dann das Dialogfeld Categories.
5. Auf der Seite Apps können Sie vorhandene Apps einer neuen Kategorie zuweisen. Wählen Sie die App aus, die Sie kategorisieren möchten.

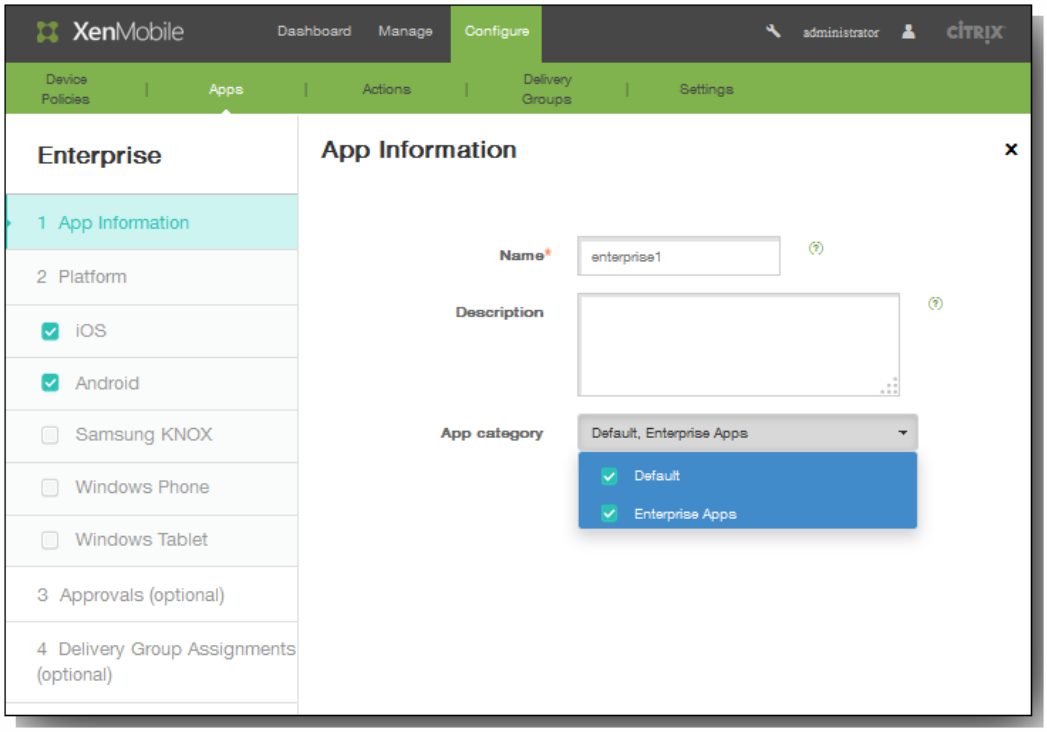


6. Klicken Sie auf Edit, um die App zu kategorisieren.

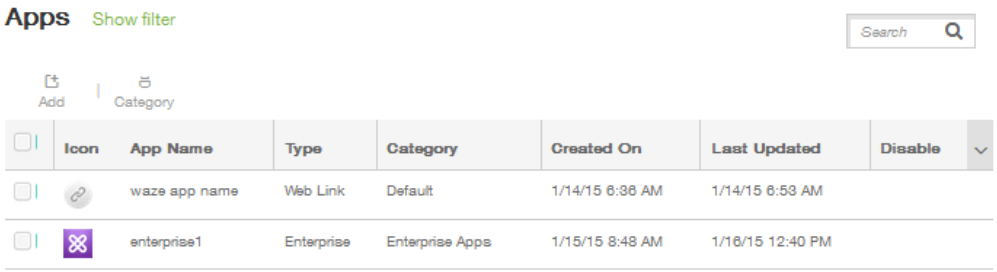


Die Seite App Information wird angezeigt.

7. Wenden Sie die gewünschte Kategorie an, indem Sie das zugehörige Kontrollkästchen in der Liste App category aktivieren.



8. Klicken Sie jeweils auf Next, um die weiteren Seiten der App-Konfiguration auszufüllen.
9. Klicken Sie auf der letzten Seite auf Save, um die Kategorie anzuwenden. Die neu erstellte Kategorie wird auf die App angewendet und in der App-Tabelle angezeigt.

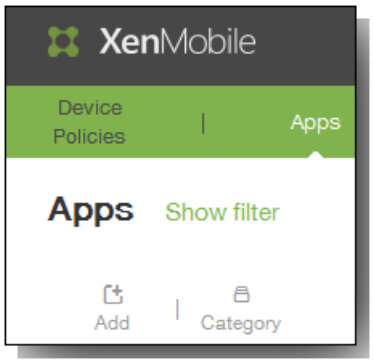


So fügen Sie XenMobile eine App aus einem öffentlichen App-Store hinzu

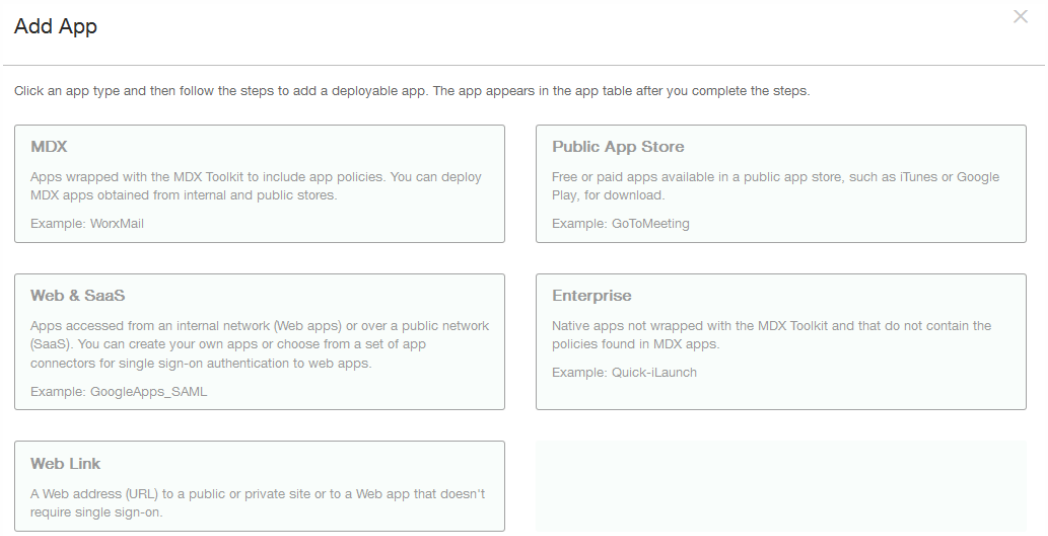
Nov 12, 2015

Sie können XenMobile kostenlose oder kostenpflichtige Apps, die in einem öffentlichen App Store (z. B. iTunes oder Google Play) verfügbar sind, hinzufügen. Beispiel: GoToMeeting.

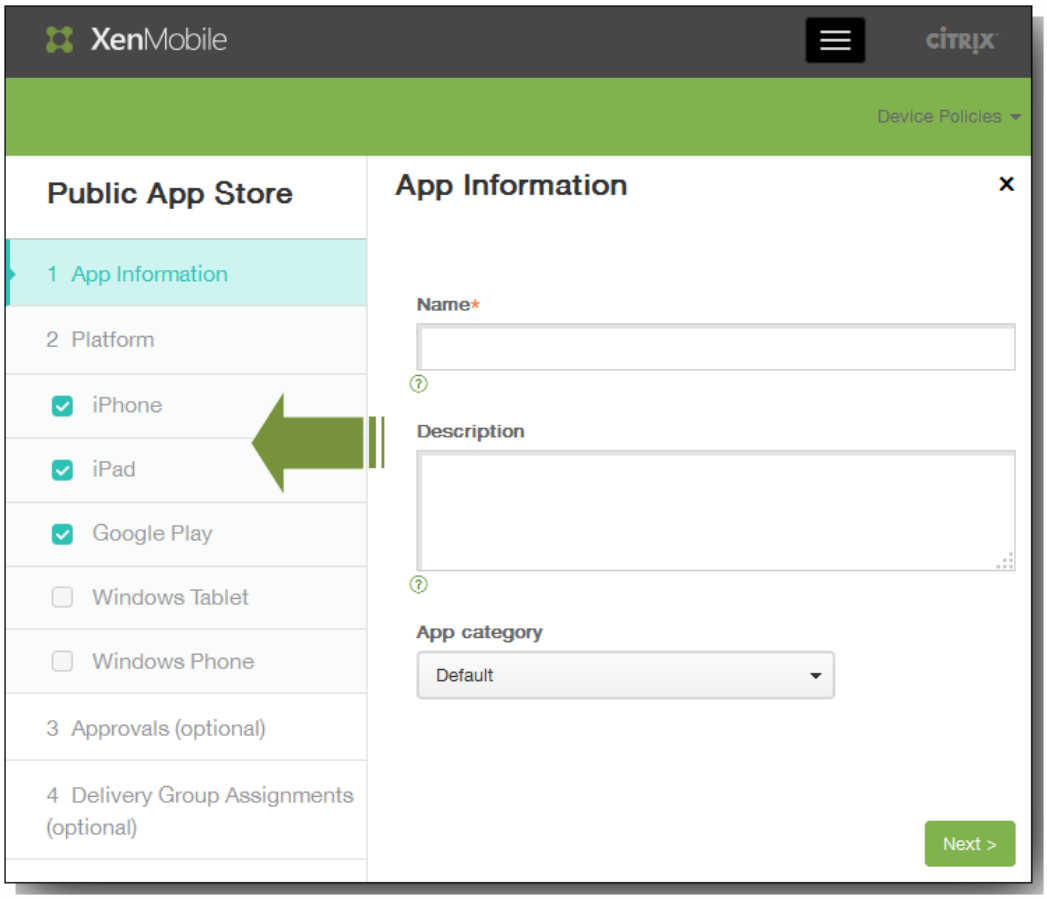
1. Klicken Sie in der XenMobile-Konsole auf Configure > Apps. Die Seite Apps wird angezeigt.



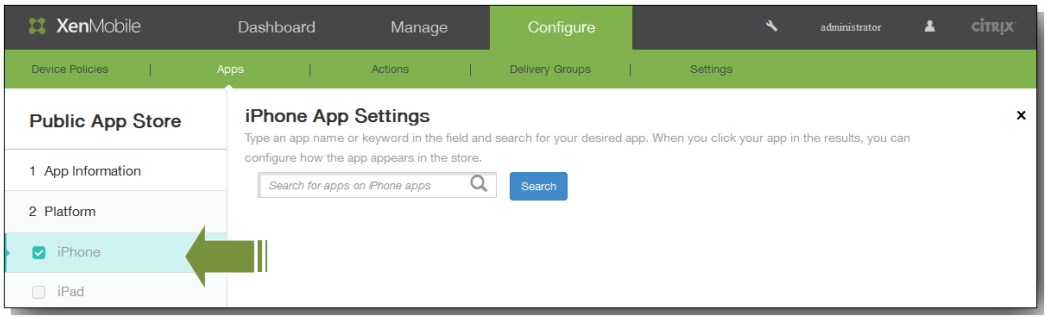
2. Klicken Sie auf Add.
3. Klicken Sie auf der Seite Add App auf Public App Store.



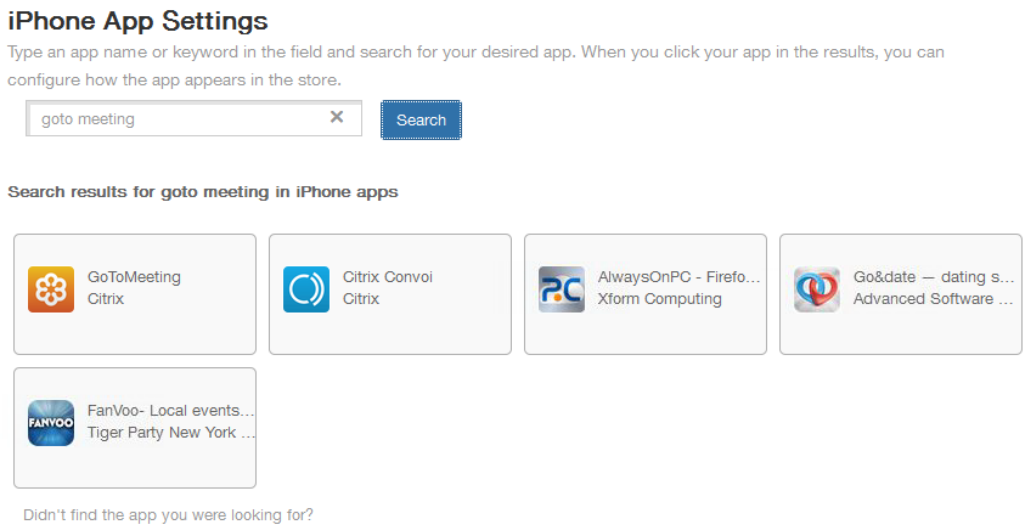
4. Geben Sie auf der Seite App Information unter Name einen Namen und unter Description eine Beschreibung für die App ein. Diese Felder werden für interne Zwecke verwendet. Wenn Sie Apps für mehrere Geräte (z. B. iPhone, iPad und Google Play) hinzufügen, verwenden Sie die Kontrollkästchen im linken Bereich des Bildschirms, um diese auszuwählen.



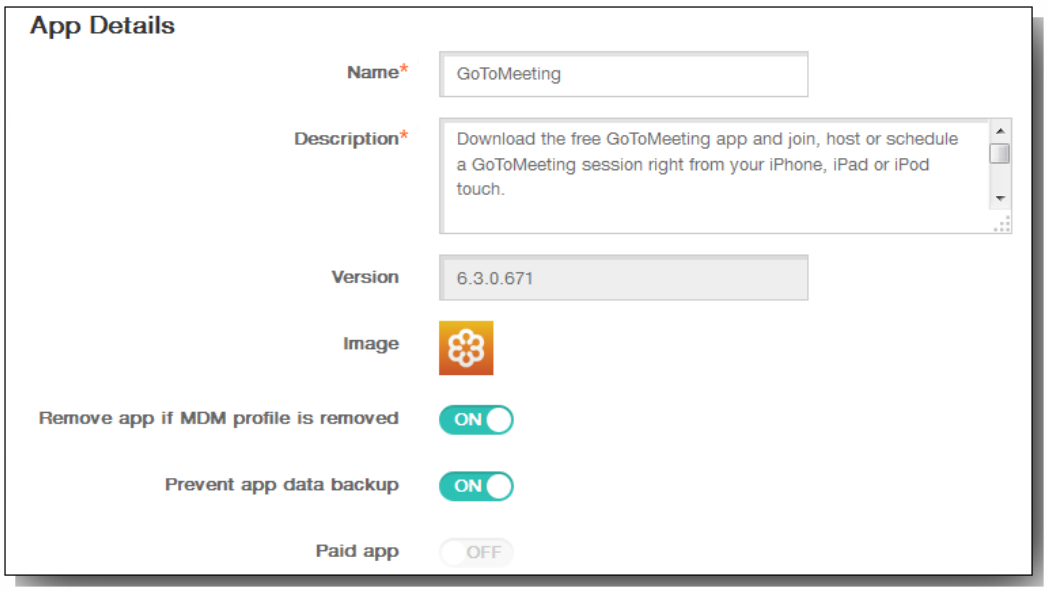
5. Klicken Sie in der Liste App category auf die App-Kategorie.
6. Klicken Sie auf Next.
7. Geben Sie auf der Seite Platform im Suchfeld für den Plattformtyp einen App-Namen oder ein Schlüsselwort ein, um die App zu suchen, die Sie hinzufügen möchten. Wenn Sie beispielsweise eine iPhone-App zum Hinzufügen auswählen, sucht die XenMobile-Konsole Apps für iPhone-Geräte. Wenn Sie Apps für mehrere Plattformen hinzufügen, wird für jede ein eigenes Ergebnis angezeigt.



In der folgenden Abbildung werden Apps angezeigt, die den Suchkriterien entsprechen (z. B. GoToMeeting).



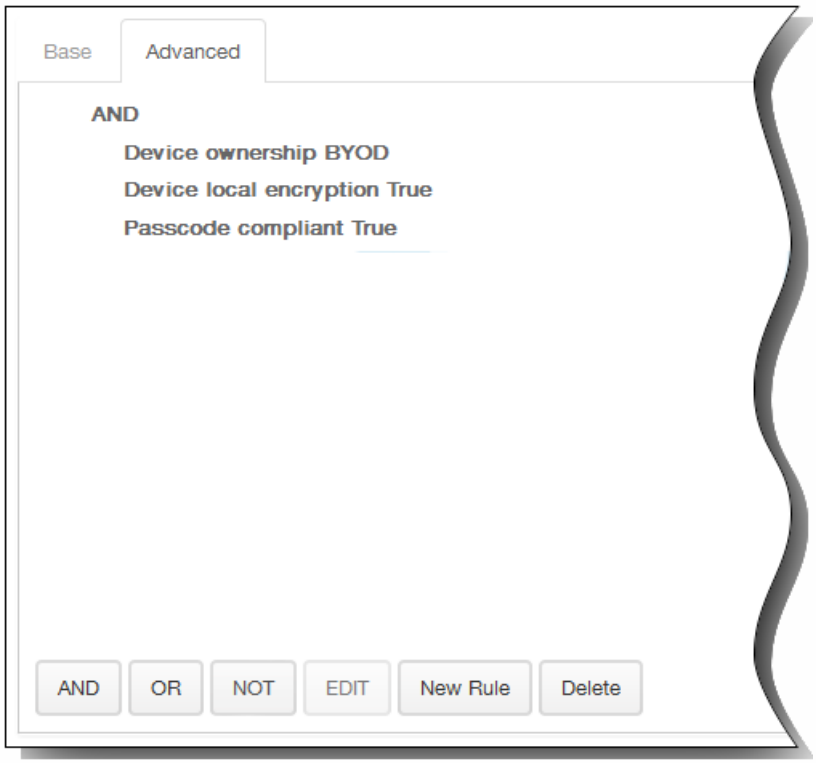
8. Klicken Sie auf eine App im Ergebnis, um vorzugeben, wie diese im Store angezeigt werden soll. Die Felder auf der Seite App Details enthalten bereits Informationen über die gewählte App (einschließlich Namen, Beschreibung, Versionsnummer und zugewiesenes Bild). Falls erforderlich, ändern Sie Namen und Beschreibung der App.



1. Klicken Sie unter Remove app if MDM profile is removed auf ON, wenn die App bei Entfernen des MDM-Profils auch entfernt werden soll. Standardmäßig ist diese Option auf ON festgelegt.
2. Klicken Sie unter "Prevent app data backup" auf ON, wenn Sie verhindern möchten, dass durch die App Daten gesichert werden. Standardmäßig ist diese Option auf ON festgelegt.
3. Das Feld **Paid App** ist vorkonfiguriert und kann nicht geändert werden.

9. Erweitern Sie Deployment Rules. Standardmäßig wird die Registerkarte Base angezeigt.

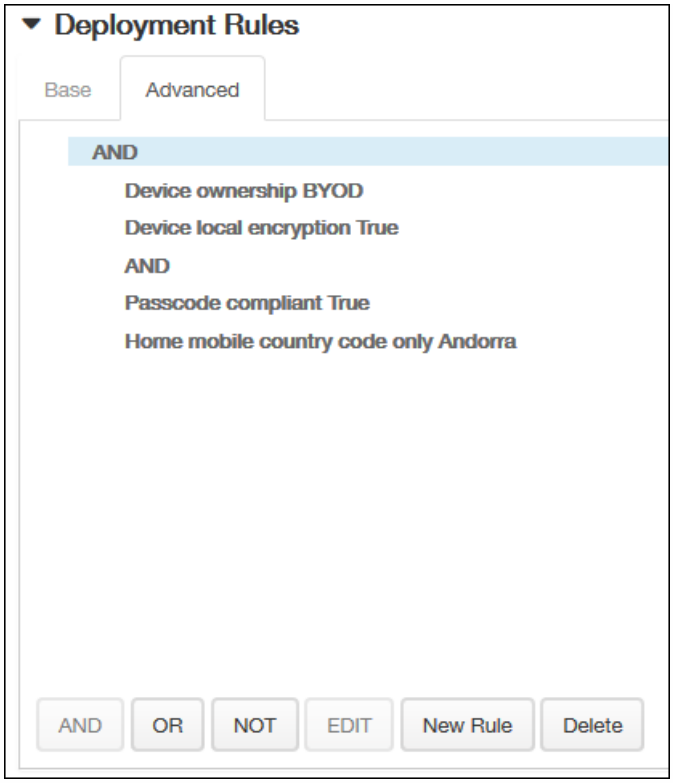
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die App bereitgestellt werden soll.
    1. Sie können die App bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



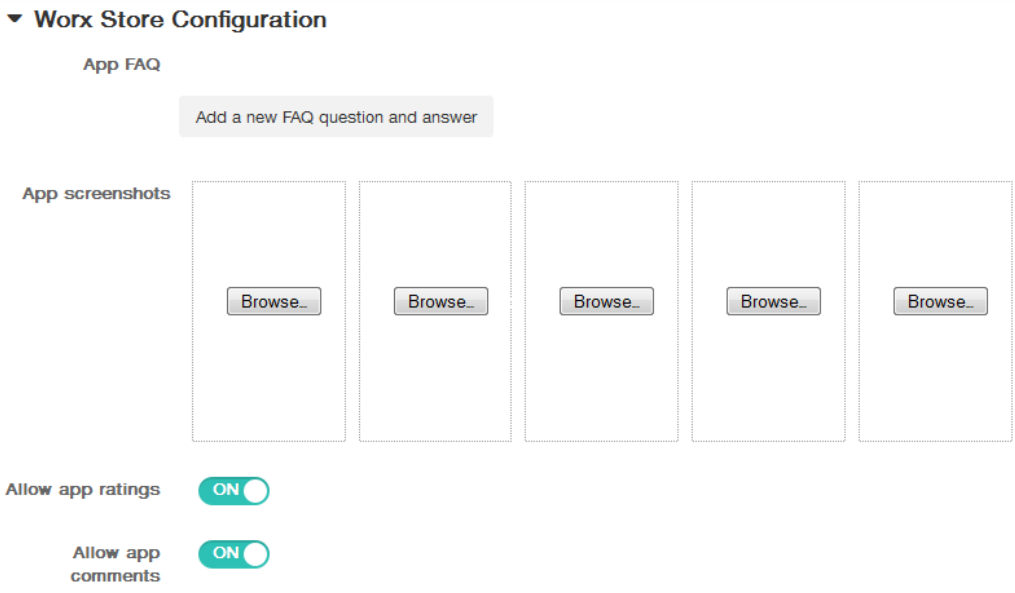
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
    1. Klicken Sie auf AND, OR oder NOT.
    2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
    Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

    3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
    In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.

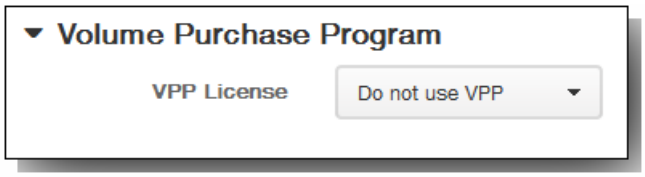


10. Erweitern Sie Worx Store Configuration, um FAQ für die App oder Bildschirmaufnahmen zur Klassifizierung des App im Worx Store hinzuzufügen. Die hochgeladene Grafik muss im PNG-Format sein. Sie können keine GIF- oder JPEG-Bilder hochladen.

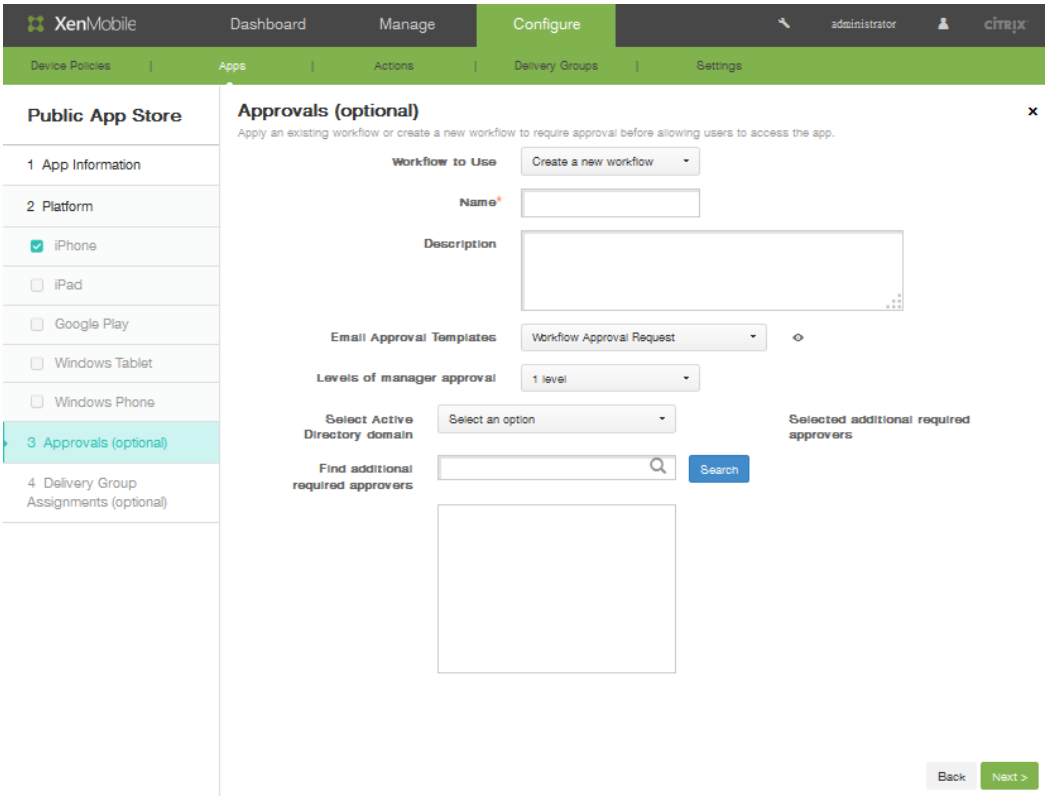


Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.

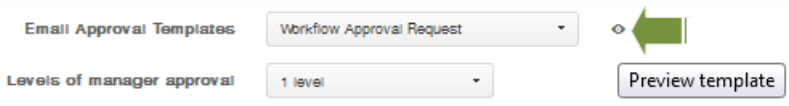
11. Klicken Sie unter Allow app comments auf ON, um eine Kommentierung der App durch die Benutzer zuzulassen.
12. Erweitern Sie Volume Purchase Program und klicken Sie in der Liste VPP license auf Upload a VPP license file, wenn XenMobile der App eine VPP-Lizenz zuweisen können soll.



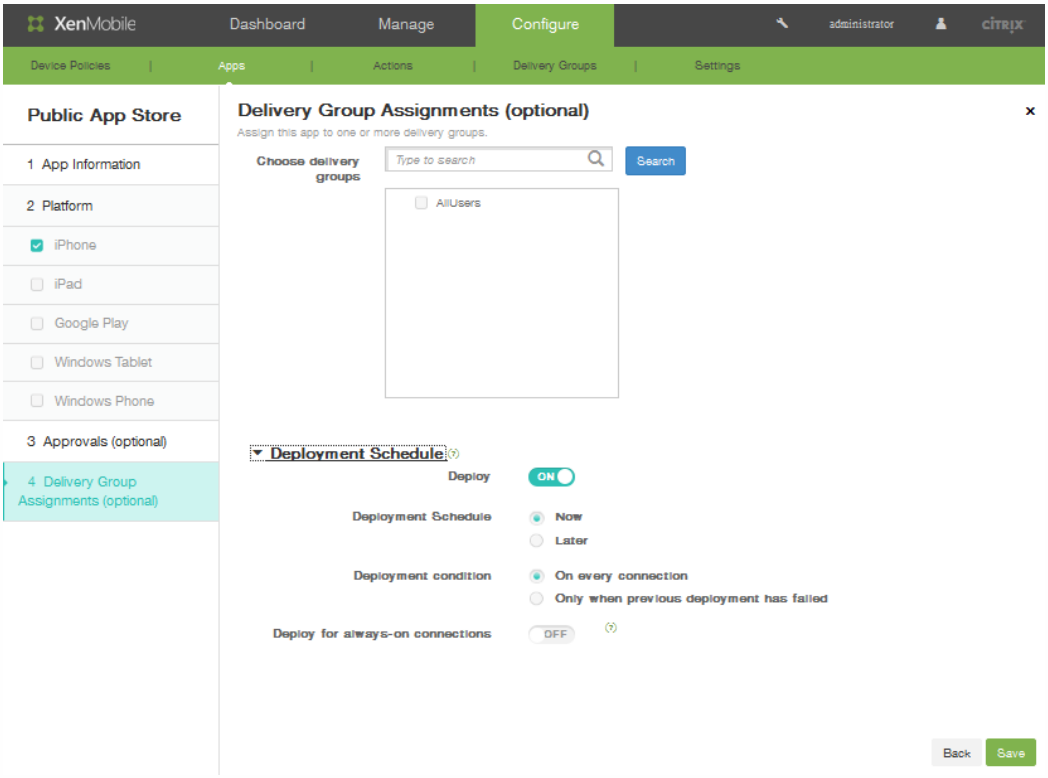
13. Klicken Sie auf Next und wiederholen Sie dann die Schritte 7 bis 16 für jede Plattform, für die Sie öffentliche Apps hinzufügen möchten.
14. Klicken Sie auf der Seite **Approvals** in der Liste **Workflow to use** optional auf einen Workflow oder auf **Create a new workflow**.



15. Wenn Sie einen neuen Workflow erstellen, werden in der XenMobile-Konsole nun Konfigurationsoptionen für den Freigabeprozess angezeigt. Die betreffenden Felder werden in den nachfolgenden Schritten erläutert.
    1. Geben Sie unter **Name** einen Namen für den Workflow ein.
    2. Geben Sie optional unter **Description** eine Beschreibung ein.
    3. Klicken Sie unter **Email Approval Templates** auf eine Benachrichtigungsoption. Klicken Sie auf das **Augensymbol**, um eine Vorschau der ausgewählten Vorlage anzuzeigen.



    4. Klicken Sie unter **Levels of manager approval** auf eine Stufe zwischen None und 3. .
    5. Klicken Sie unter **Select Active Directory domain** auf die Domäne.
    6. Geben Sie unter Find additional required approvers optional weitere Freigabeberechtigte ein und klicken Sie auf Search.
16. Klicken Sie auf **Next**.
17. Weise Sie die App auf der Seite **Delivery Groups Assignment** optional einer oder mehreren Bereitstellungsgruppen zu.



18. Suchen Sie unter Choose delivery groups die Bereitstellungsgruppe(n). Aktivieren Sie das Kontrollkästchen **All Users**, um die App allen XenMobile-Benutzern zuzuweisen.
19. Erweitern Sie Deployment Schedule, um die Bereitstellungsgruppe näher zu definieren.
    1. Deploy: Klicken Sie auf ON, um einen Bereitstellungszeitplan zu aktivieren.
    2. Deployment Schedule: Klicken Sie auf Now oder Later, um den Bereitstellungszeitplan festzulegen.
    3. Deployment condition: Wählen Sie aus, ob die App bei jeder Verbindung oder bei Fehlschlagen der vorherigen Bereitstellung bereitgestellt werden soll.
    4. Klicken Sie unter Deploy for always-on connections auf ON, wenn die Bereitstellung erfolgen soll, wenn die Verbindungsrichtlinie "always-on" festgelegt ist.
       Hinweis: Diese Option wird angewendet, wenn Sie im Bereich "Server Properties" der XenMobile-Konsole unter "Settings" auch Schlüssel für die globale Bereitstellung im Hintergrund konfiguriert haben. Die Richtlinie "always-on" ist für iOS-Geräte nicht verfügbar.
20. Klicken Sie auf Save. In der XenMobile-Konsole werden die App-Informationen angewendet.

So fügen Sie XenMobile Web- und SaaS-Apps hinzu

Nov 12, 2015

Mit der XenMobile-Konsole können Sie Benutzern SSO-Zugriff (Single Sign-On) auf Mobil-, Unternehmens-, Web- und SaaS-Apps gewähren. Zur Aktivierung von Apps für SSO können Sie Vorlagen für Anwendungsconnectors verwenden. Eine Liste der in XenMobile verfügbaren Connectortypen finden Sie unter Liste der Anwendungsconnectortypen.

Sie können auch einen eigenen Connector in XenMobile erstellen.

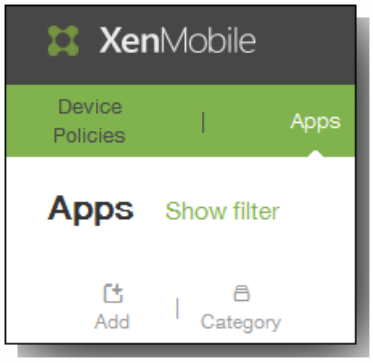
Bei der Konfiguration eines Connectors werden folgende Parameter angegeben:

- Verschiedene Namen (optional). Verwenden Sie einen beliebigen in der Konsole angezeigten App-Connector. Box connector wird nicht mehr unterstützt.
- Eine Beschreibung der App.
- Webadressen mit dem vollqualifizierten Domänennamen (FQDN). Wenn Sie beispielsweise LinkedIn der App-Liste hinzufügen möchten, gehen Sie zu http://www.linkedin.com und klicken Sie auf Sign in. Wenn die Anmeldeseite angezeigt wird, verwenden Sie die Webadresse https://www.linkedin.com zum Konfigurieren der App.
- Der Speicherort der App im Internet oder im internen Netzwerk.
- Anmeldeinformationen für SSO. Benutzer können die App-Anmeldeinformationen verwenden.
- Kategorie der App. Kategorien ermöglichen das Organisieren von Apps in Worx Home.
- App-Richtlinien für jede in XenMobile konfigurierte App.
- Workflow-Genehmigungseinstellungen für alle Apps; hierzu gehört die Angabe der Personen, die das Benutzerkonto genehmigen können.
- Eine Gruppe von Benutzern, denen die App zugewiesen werden soll.

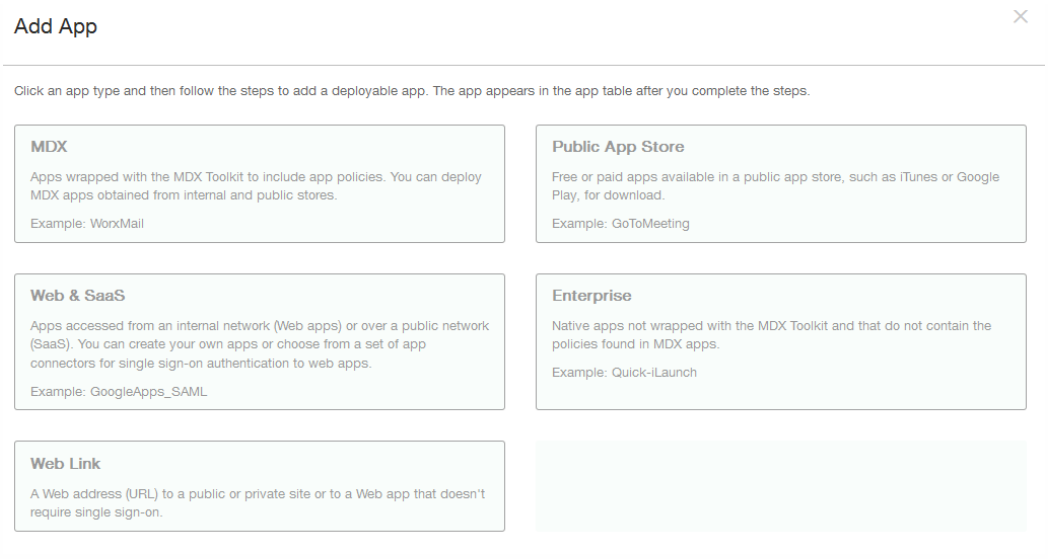
Wenn eine App nur für SSO verfügbar ist, speichern Sie nach der oben beschriebenen Konfiguration die Einstellungen. Die App wird dann auf der Registerkarte Apps in der XenMobile-Konsole angezeigt.

So fügen Sie einen App-Connector in XenMobile hinzu

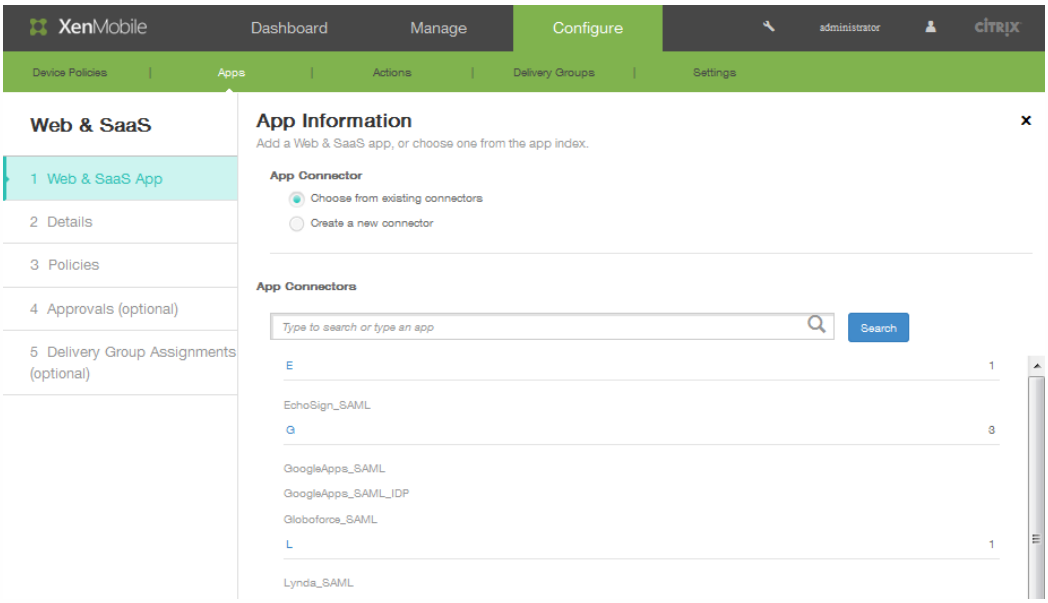
1. Klicken Sie in der XenMobile-Konsole auf Configure > Apps. Die Seite Apps wird geöffnet.
2. Klicken Sie auf der Seite Apps auf **Add**.



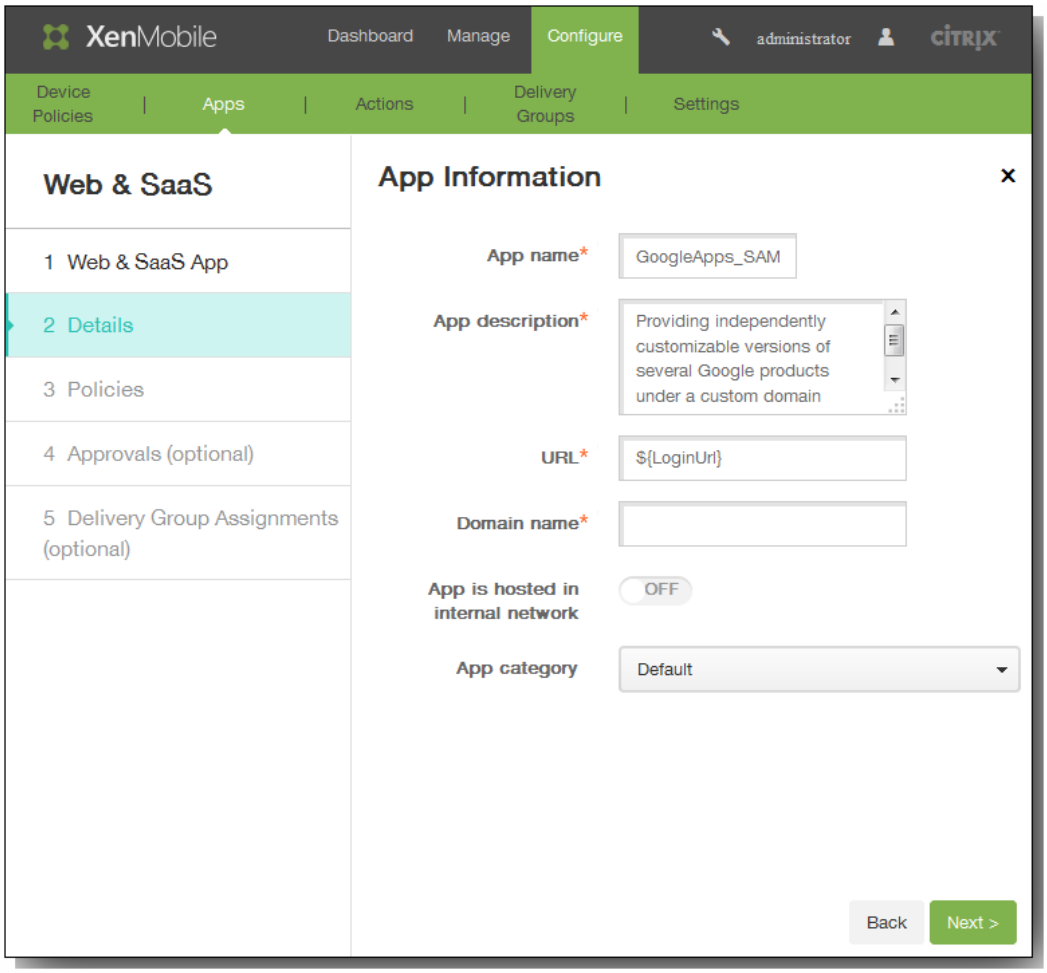
3. Klicken Sie auf der Seite **Add App** auf **Web & SaaS**.



4. Klicken Sie auf der Seite App Information auf Choose from existing connector oder Create a new connector.

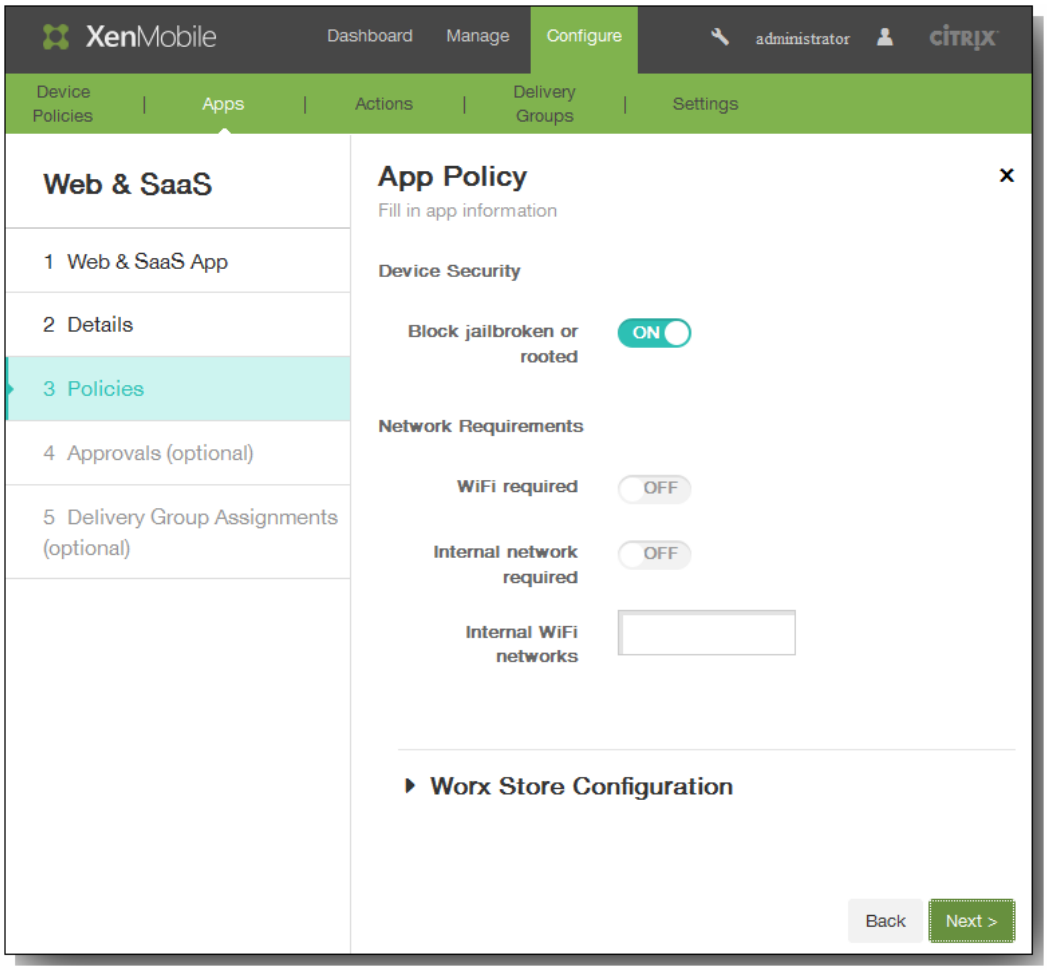


5. Wenn Sie auf eine App in der Liste klicken, wird die Seite Details geöffnet. Die Felder App name, Description und URL sind bereits ausgefüllt.

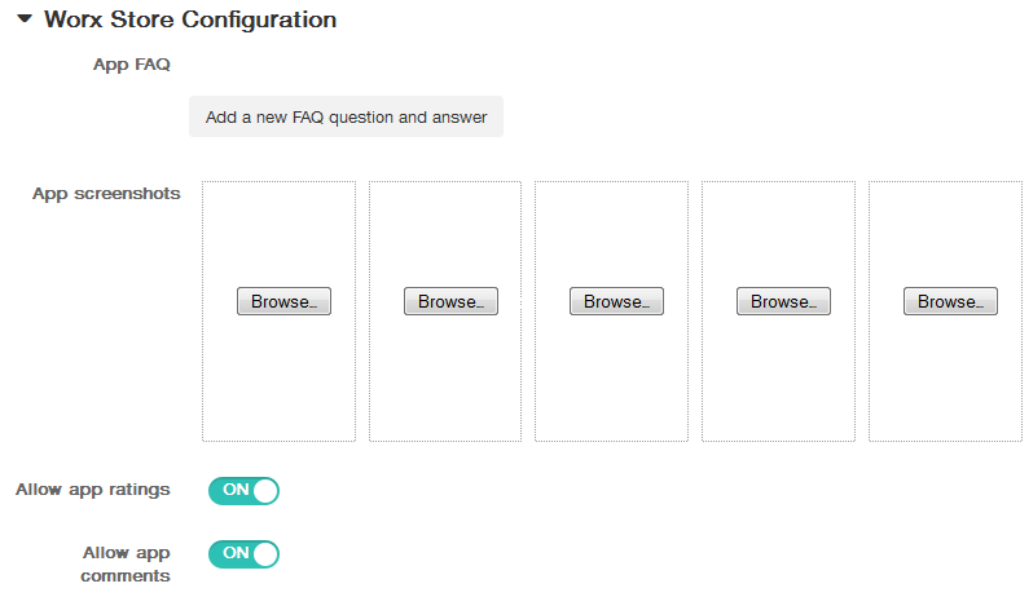


1. Geben Sie unter URL ggf. die Webadresse der App ein oder behalten Sie die Standardadresse bei.
2. Klicken Sie unter App is hosted in internal network auf ON, wenn die App auf einem Server im internen Netzwerk ausgeführt wird. Wenn Benutzer von einem Remotestandort aus eine Verbindung mit der internen Anwendung herstellen, muss dies über NetScaler Gateway erfolgen. Wenn Sie diese Option auf ON festlegen, wird das VPN-Schlüsselwort der App hinzugefügt, sodass Benutzer eine Verbindung über NetScaler Gateway herstellen können.
3. Klicken Sie in der Liste App category auf eine Kategorie.
4. Klicken Sie unter Enable user management for provisioning auf On. Wenn Sie den Connector Globalforce_SAML verwenden, müssen Sie Enable user management for provisioning aktivieren, um eine nahtlose SSO-Integration zu gewährleisten.

6. Klicken Sie auf Next. Die Seite Policies wird angezeigt.

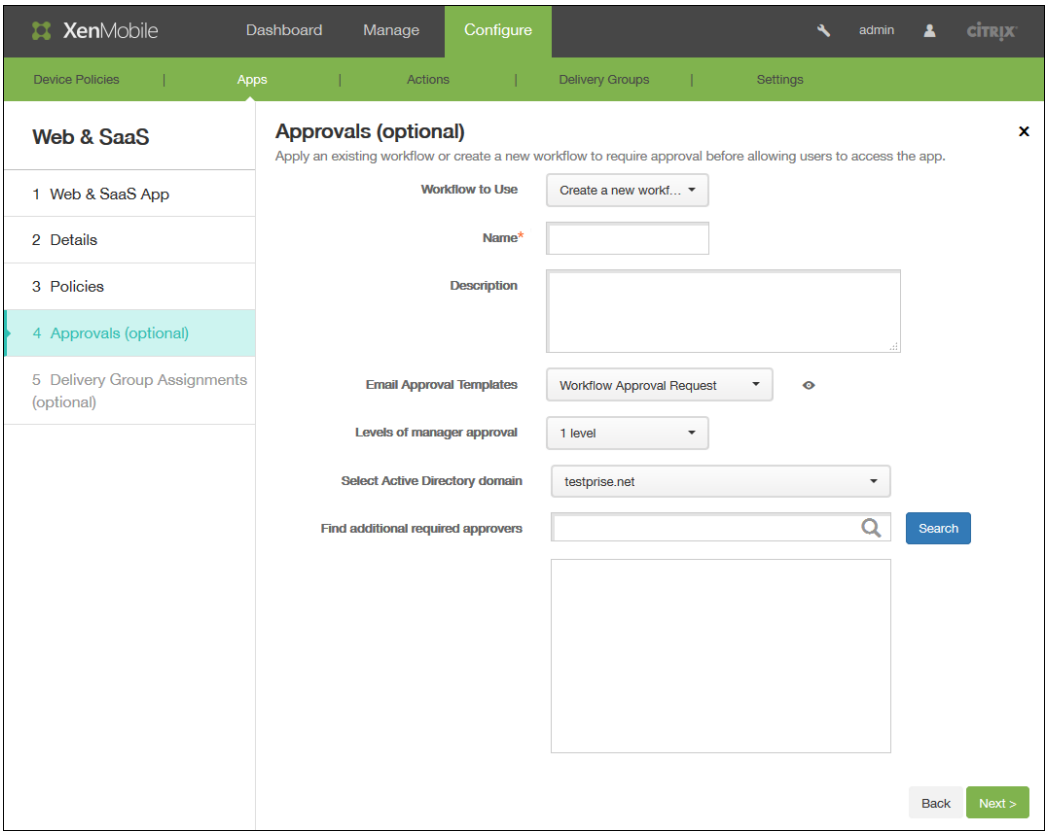


7. Klicken Sie unter Device Security für Block jailbroken or rooted auf ON.
8. Konfigurieren Sie unter Network Requirements die folgenden Einstellungen:
   1. Klicken Sie für WiFi required auf ON und geben Sie interne WiFi-Netzwerke an.
   2. Klicken Sie für Internal network required auf ON, wenn ein internes Netzwerk erforderlich ist, um die App auszuführen.
9. Erweitern Sie Worx Store Configuration, um FAQ für die App oder Bildschirmaufnahmen zur Klassifizierung des App im Worx Store hinzuzufügen. Die hochgeladene Grafik muss im PNG-Format sein. Sie können keine GIF- oder JPEG-Bilder hochladen.



Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.

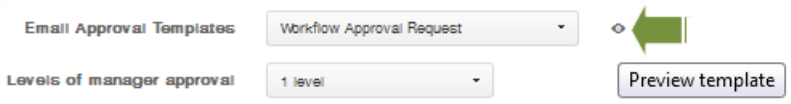
10. Klicken Sie unter Allow app comments auf ON, um eine Kommentierung der App durch die Benutzer zuzulassen.
11. Klicken Sie auf Next.
12. Klicken Sie auf der Seite Approvals in der Liste Workflow to use optional auf einen Workflow oder auf Create a new workflow.



13. Wenn Sie einen neuen Workflow erstellen, werden in der XenMobile-Konsole nun Konfigurationsoptionen für den Freigabeprozess angezeigt. Die betreffenden Felder werden in den nachfolgenden Schritten erläutert. Konfigurieren Sie

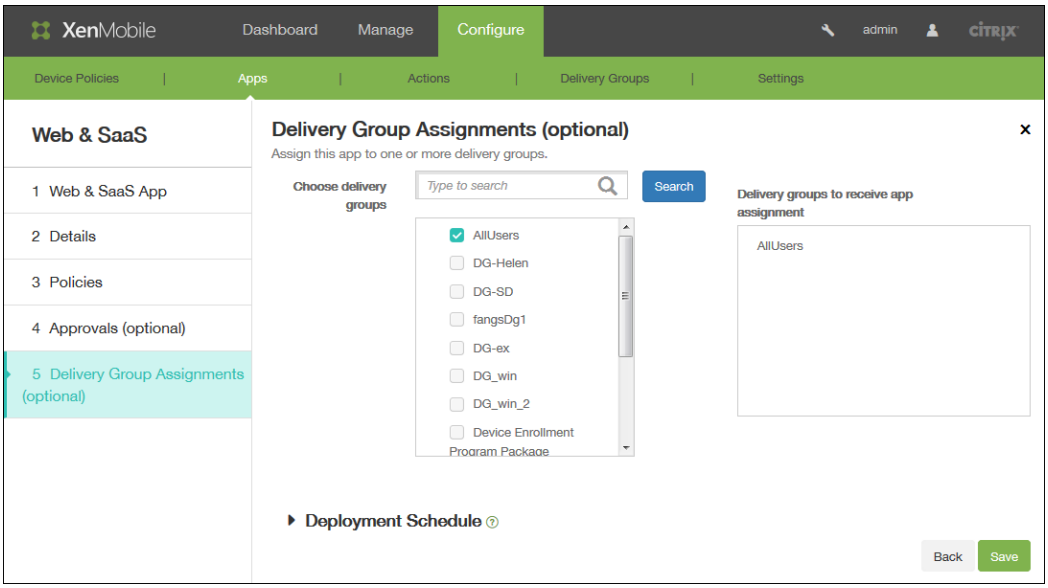
diese Felder, wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist.

1. Geben Sie unter **Name** einen Namen für den Workflow ein.
2. Geben Sie optional unter **Description** eine Beschreibung ein.
3. Klicken Sie unter **Email Approval Templates** auf eine Benachrichtigungsoption. Klicken Sie auf das **Augensymbol**, um eine Vorschau der ausgewählten Vorlage anzuzeigen.



4. Klicken Sie unter **Levels of manager approval** auf eine Stufe zwischen None und 3.
5. Klicken Sie unter **Select Active Directory domain** auf die Domäne.
6. Geben Sie unter Find additional required approvers optional weitere Freigabeberechtigte ein und klicken Sie auf Search.

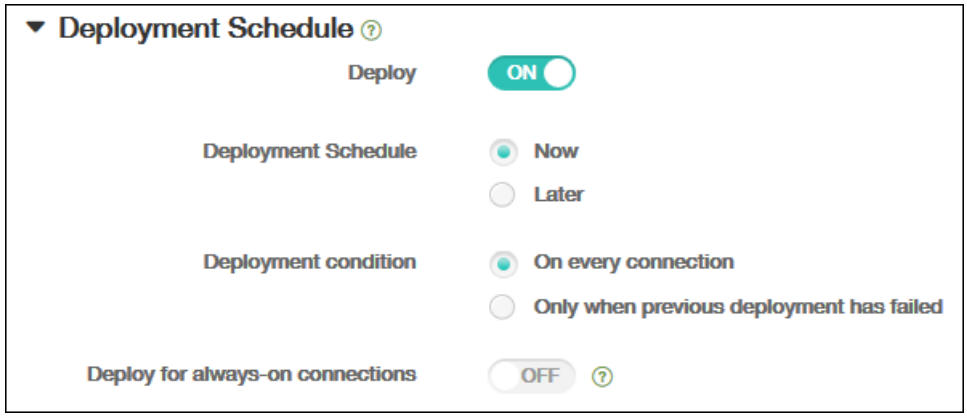
14. Klicken Sie auf Next.
15. Nehmen Sie optional auf der Seite **Delivery Groups Assignment** neben Choose delivery groups eine Eingabe vor, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste mindestens eine Bereitstellungsgruppe für die Zuweisung aus.
    Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



16. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
    3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
    4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
    5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
       Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im

Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



17. Klicken Sie auf **Speichern**.

Liste der Anwendungsconnectortypen

Nov 12, 2015

In der folgenden Tabelle finden Sie die Connectors und Connectortypen, die in XenMobile verfügbar sind. Die Tabelle enthält außerdem Angaben dazu, ob ein Connector die Benutzerkontenverwaltung unterstützt, mit der neue Konten automatisch oder mit einem Workflow erstellt werden können.

Connectorname	**Single Sign-On SAML**	**Unterstützt Benutzerkontenverwaltung**
Echosign_SAML	J	J
Globoforce_SAML		**Hinweis**: Wenn Sie diesen Connector verwenden, müssen Sie User Management für Provisioning aktivieren, um eine nahtlose SSO-Integration zu gewährleisten.
GoogleApps_SAML	J	J
GoogleApps_SAML _IDP	J	J
Lynda_SAML	J	J
Office365_SAML	J	J
Salesforce_SAML	J	J
Salesforce_SAML_SP	J	J
SandBox_SAML	J	
SuccessFactors_SAML	J	
ShareFile_SAML	J	
ShareFile_SAML_SP	J	
WebEx_SAML_SP	J	J

So fügen Sie XenMobile eine Unternehmensapp hinzu

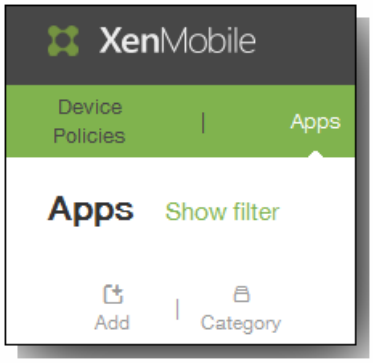
Nov 20, 2015

Unternehmensapps in XenMobile sind native Apps, die nicht mit dem MDX Toolkit umschlossen wurden und nicht die Richtlinien für MDX-Apps enthalten. Sie können Unternehmensapps mit der Registerkarte Apps der XenMobile-Konsole hochladen. Unternehmensapps unterstützen folgende Plattformen (und die entsprechenden Dateitypen):

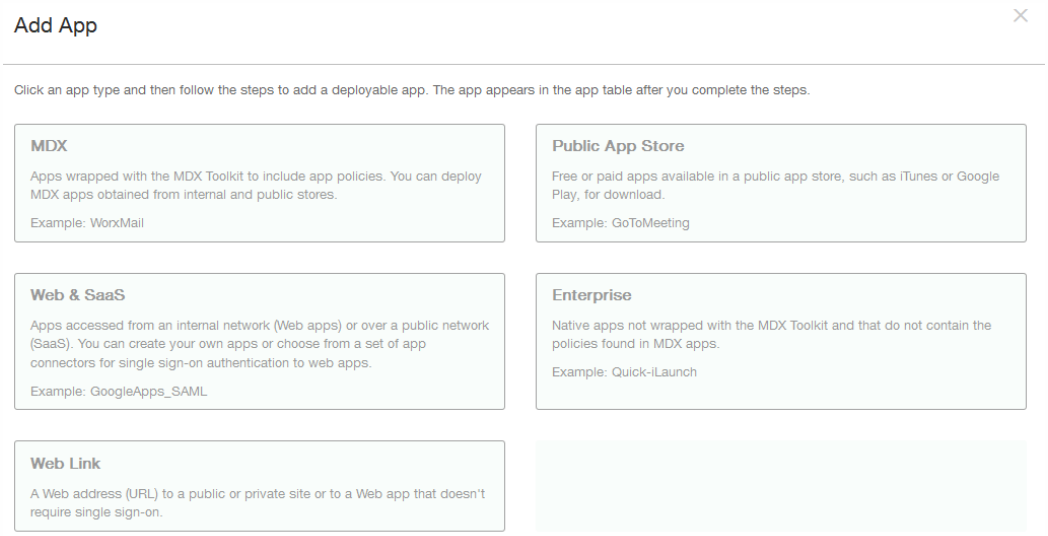
- iOS (.ipa)
- Android (.apk)
- Samsung KNOX (.apk)
- Android for Work (.apk)
- Windows Phone (.xap oder .appx)
- Windows Tablet (.appx)

So erstellen Sie eine Unternehmensapp

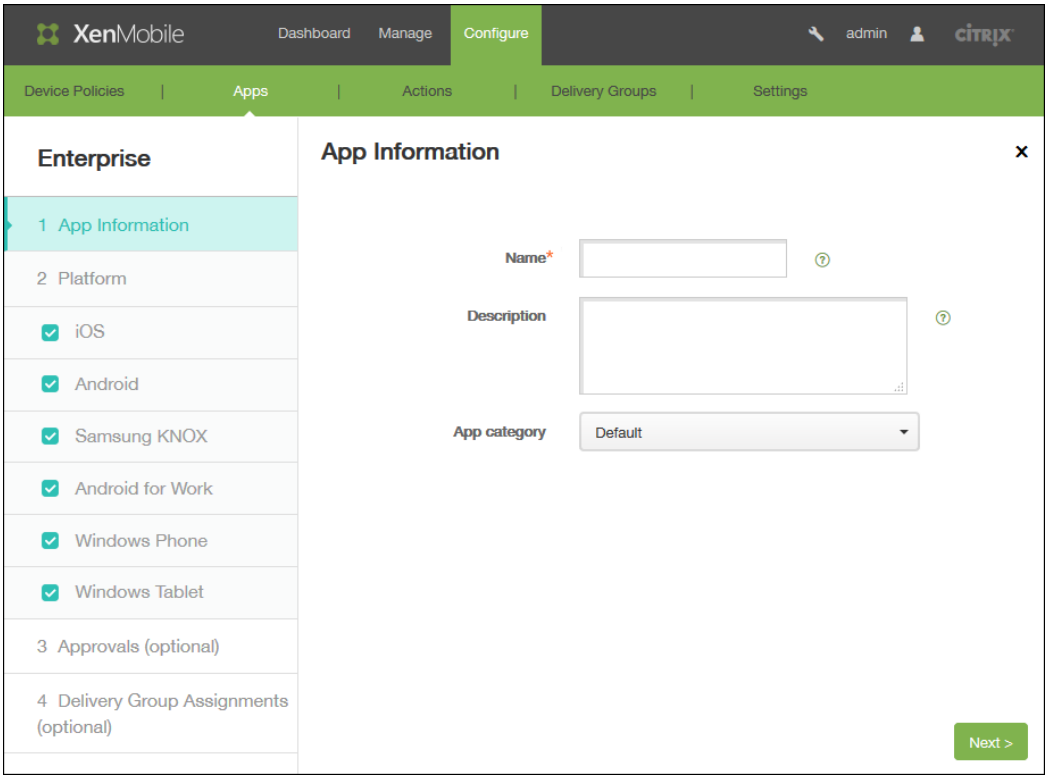
1. Klicken Sie in der XenMobile-Konsole auf Configure > Apps.
2. Klicken Sie auf der Seite "Apps" auf **Add**.



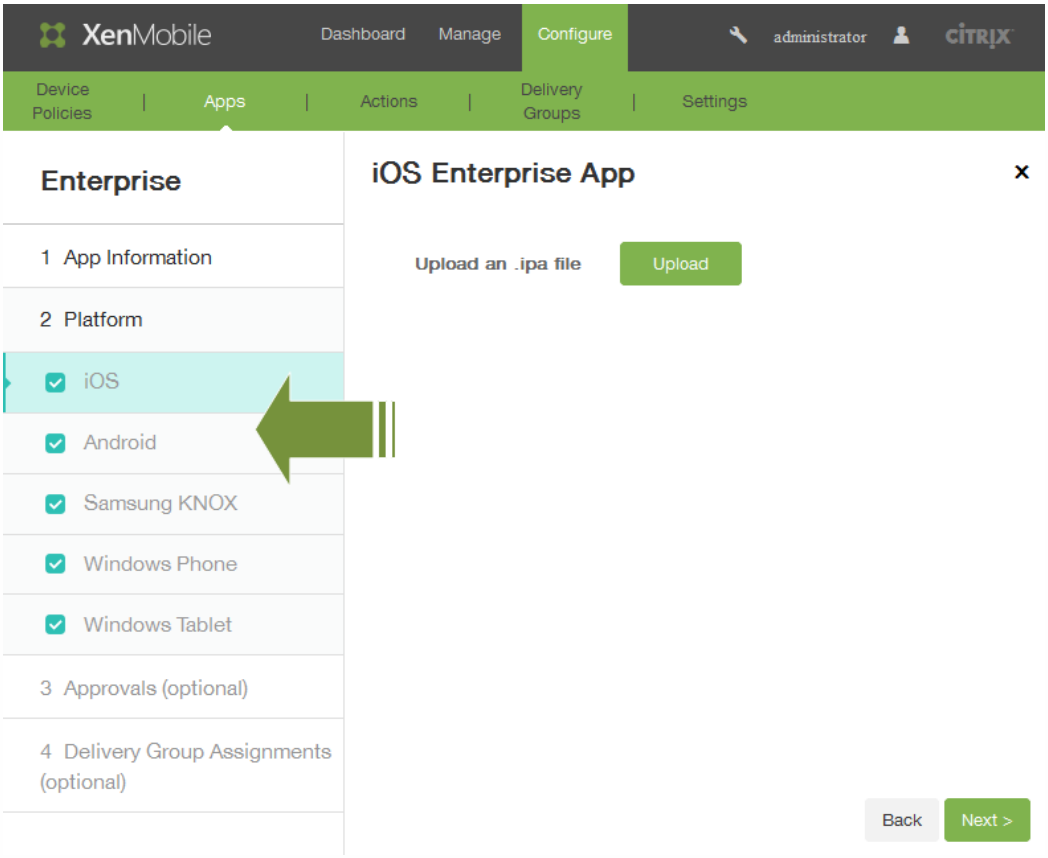
3. Klicken Sie auf der Seite Add App auf **Enterprise**.



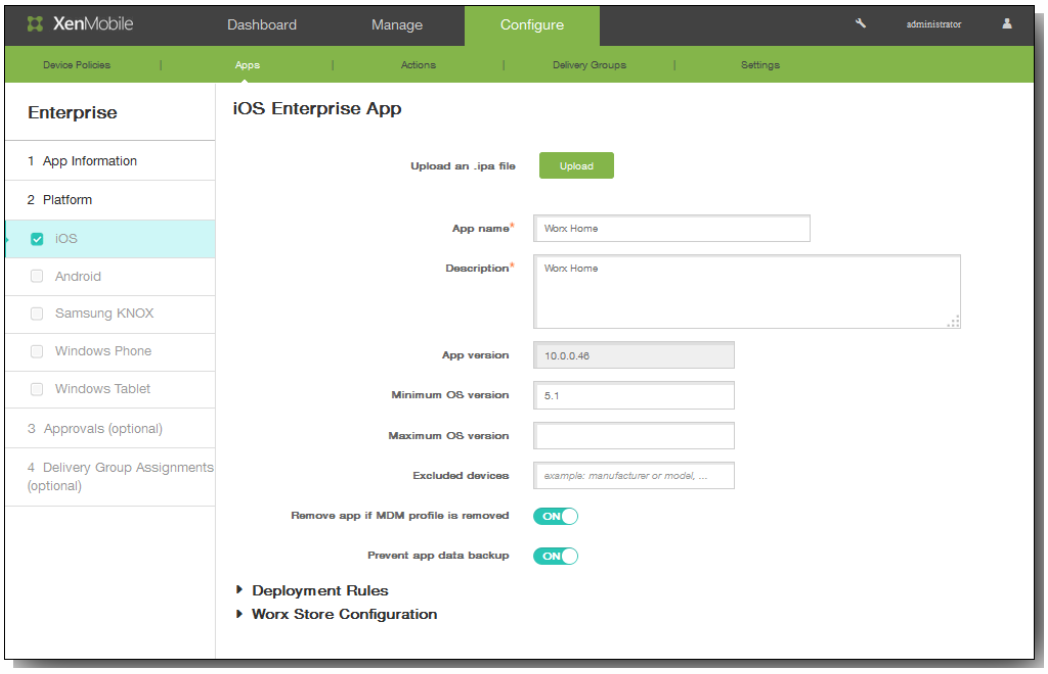
Die Seite App Information wird angezeigt.



4. Machen Sie auf der Seite App Information folgende Angaben:
   1. Name: Geben Sie einen Namen für die App ein.
   2. Description: Geben Sie eine Beschreibung für die App ein.
   3. Klicken Sie unter **App category** auf eine Kategorie und dann auf Next.
5. Wählen Sie im Bereich Platform links die Geräteplattformen aus, für die Sie die App hinzufügen möchten (z. B. iOS oder Android).

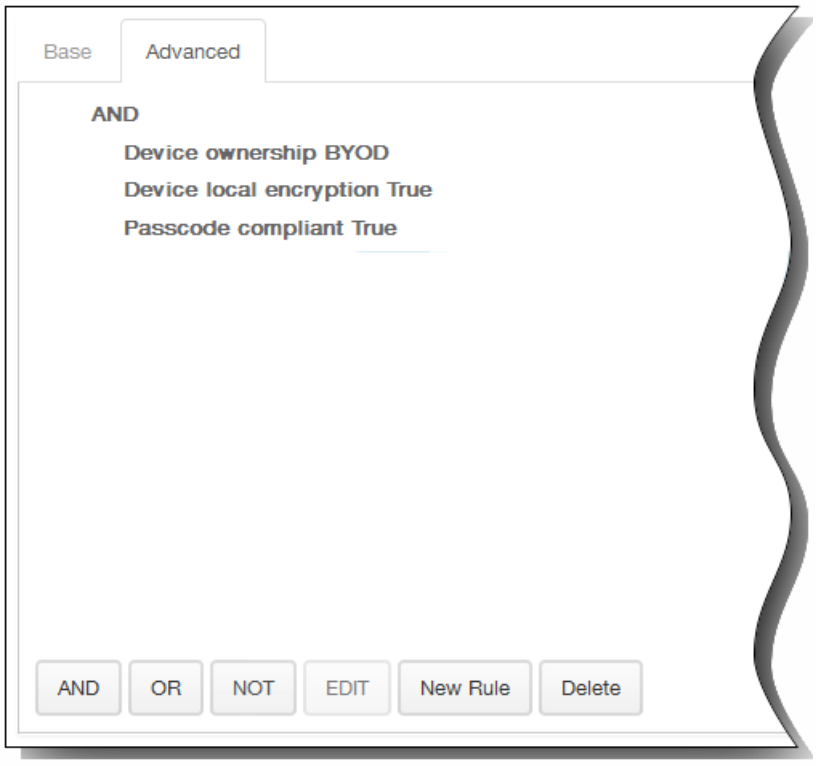


6. Klicken Sie auf Upload, navigieren Sie zum Speicherort der Datei und klicken Sie dann auf Next. Die Seite mit den App-Informationen für den Plattformtyp wird angezeigt. Die Felder enthalten bereits Informationen zu der gewählten App (einschließlich Name, Beschreibung, Versionsnummer und zugeordnetes Bild). Falls erforderlich, ändern Sie Namen und Beschreibung der App.



7. Klicken Sie unter Remove app if MDM profile is removed auf ON, wenn die App bei Entfernen des MDM-Profils auch entfernt werden soll. Standardmäßig ist diese Option auf ON festgelegt.
8. Klicken Sie unter Prevent app data backup auf ON, wenn Sie verhindern möchten, dass durch die App Daten gesichert werden. Standardmäßig ist diese Option auf ON festgelegt.
9. Erweitern Sie Deployment Rules. Standardmäßig wird die Registerkarte Base angezeigt.

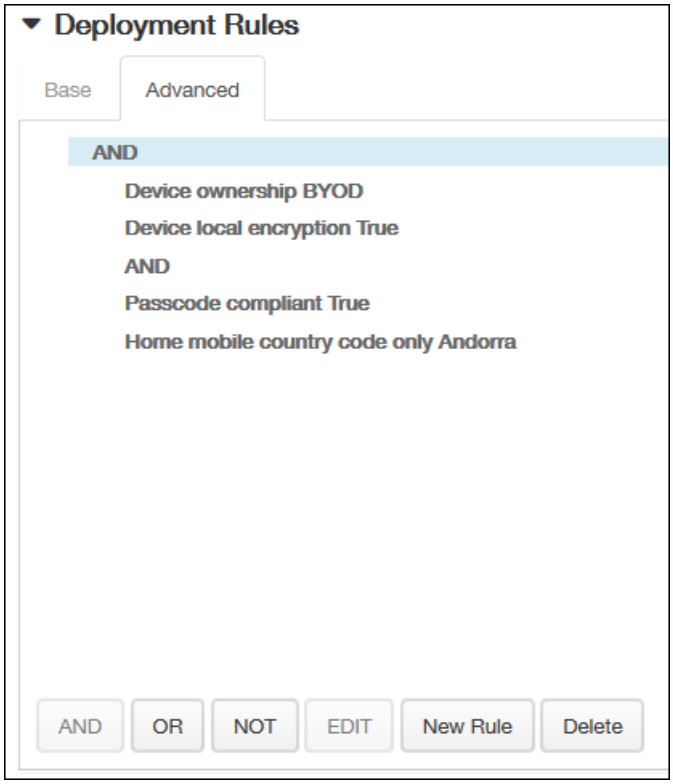
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die App bereitgestellt werden soll.
    1. Sie können die App bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



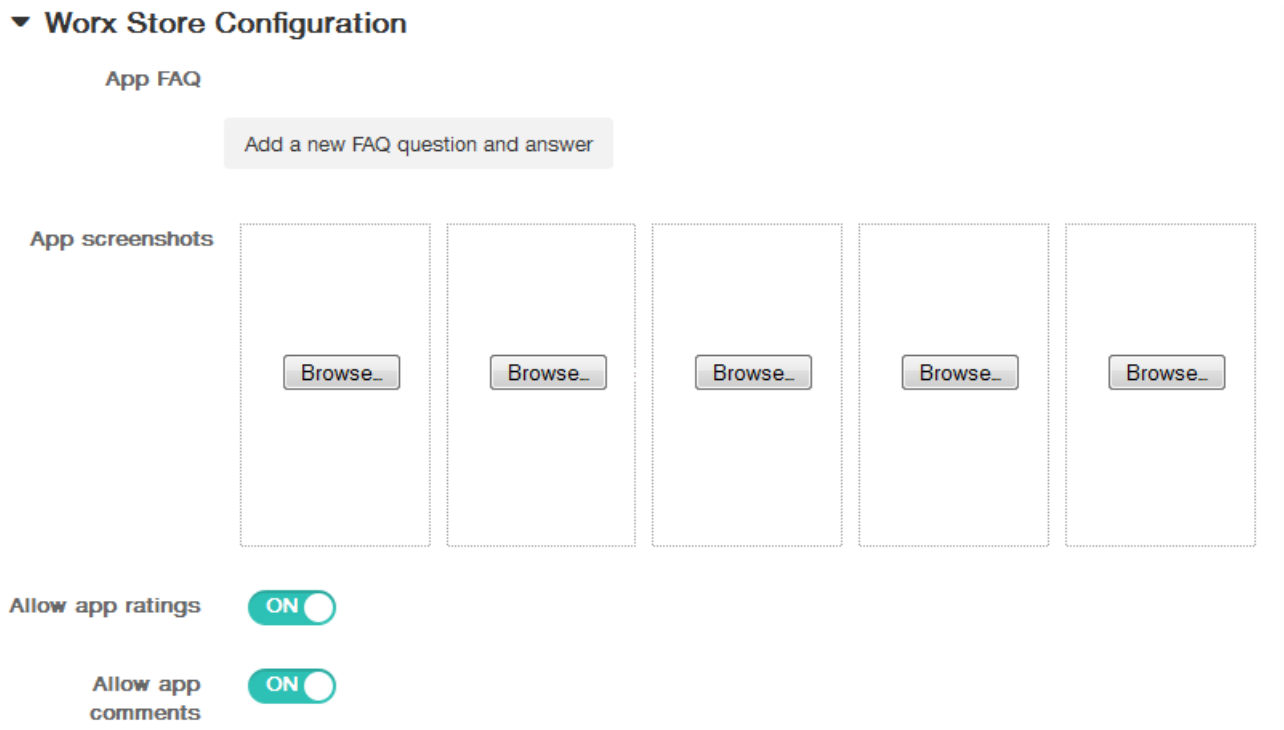
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.

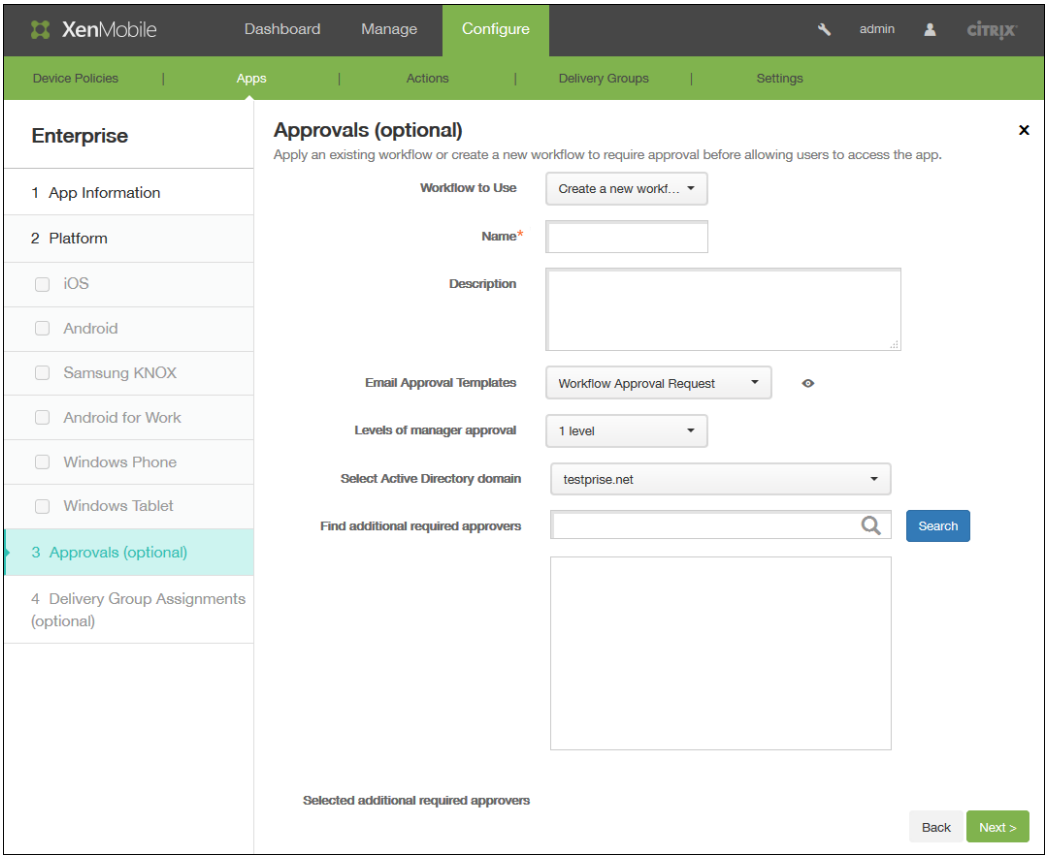


10. Erweitern Sie Worx Store Configuration, um FAQ für die App oder Bildschirmaufnahmen zur Klassifizierung des App im Worx Store hinzuzufügen. Die hochgeladene Grafik muss im PNG-Format sein. Sie können keine GIF- oder JPEG-Bilder hochladen.

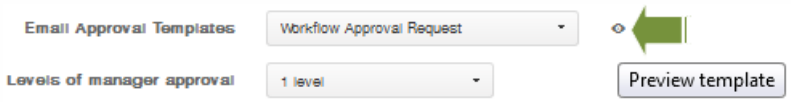


Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.

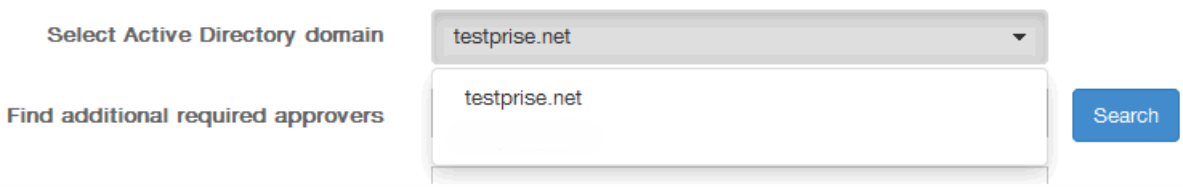
11. Klicken Sie unter Allow app comments auf ON, um eine Kommentierung der App durch die Benutzer zuzulassen.
12. Klicken Sie auf Next.
13. Klicken Sie auf der Seite Approvals in der Liste Workflow to use optional auf einen Workflow oder auf Create a new workflow.



14. Wenn Sie einen neuen Workflow erstellen, werden in der XenMobile-Konsole nun Konfigurationsoptionen für den Freigabeprozess angezeigt. Die betreffenden Felder werden in den nachfolgenden Schritten erläutert. Konfigurieren Sie diese Felder, wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist.
    1. Geben Sie unter **Name** einen Namen für den Workflow ein.
    2. Geben Sie optional unter **Description** eine Beschreibung ein.
    3. Klicken Sie unter **Email Approval Templates** auf eine Benachrichtigungsoption. Klicken Sie auf das Augensymbol, um eine Vorschau der ausgewählten Vorlage anzuzeigen.

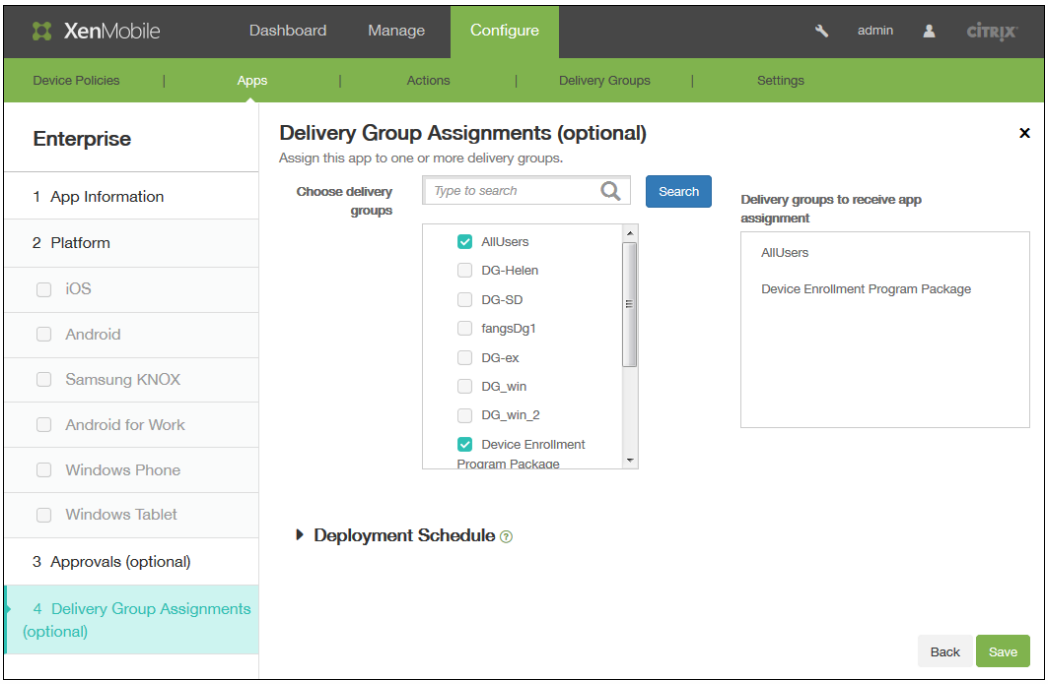


    4. Klicken Sie unter **Levels of manager approval** auf eine Stufe zwischen None und 3.
    5. Wählen Sie unter **Select Active Directory domain** die Domäne aus dem Dropdownmenü aus. Die Liste enthält nur Active Directory-Mitgliedsdomänen (z. B. testprise.net):



6. Geben Sie unter Find additional required approvers optional weitere Freigabeberechtigte ein und klicken Sie auf Search.

15. Weise Sie die App auf der Seite **Delivery Groups Assignment** optional einer oder mehreren Bereitstellungsgruppen zu.



16. Suchen Sie unter Choose delivery groups die Bereitstellungsgruppe(n). Aktivieren Sie das Kontrollkästchen **All Users**, um die App allen XenMobile-Benutzern zuzuweisen.
17. Erweitern Sie Deployment Schedule, um die Bereitstellungsgruppe näher zu definieren.
    1. Deploy: Klicken Sie auf ON, um einen Bereitstellungszeitplan zu aktivieren.
    2. Deployment Schedule: Klicken Sie auf Now oder Later, um den Bereitstellungszeitplan festzulegen.
    3. Deployment condition: Wählen Sie aus, ob die App bei jeder Verbindung oder bei Fehlschlagen der vorherigen Bereitstellung bereitgestellt werden soll.
    4. Klicken Sie unter Deploy for always-on connections auf ON, wenn die Bereitstellung erfolgen soll, wenn die Verbindungsrichtlinie "always-on" festgelegt ist.
       Hinweis: Diese Option wird angewendet, wenn Sie im Bereich Server Properties der XenMobile-Konsole unter Settings auch Schlüssel für die globale Bereitstellung im Hintergrund konfiguriert haben. Die Richtlinie "always-on" ist für iOS-Geräte nicht verfügbar.
18. Klicken Sie auf Save.

So fügen Sie XenMobile eine Weblink-App hinzu

Nov 12, 2015

In XenMobile können Sie eine Webadresse (URL) für eine öffentliche oder private Website oder eine Web-App, die kein Single Sign-On erfordert, einrichten.

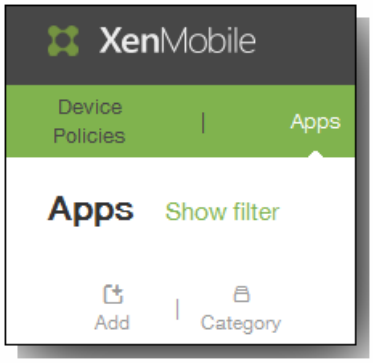
Sie können Weblinks über die Registerkarte Apps in der XenMobile-Konsole konfigurieren. Wenn Sie die Konfiguration des Weblinks abgeschlossen haben, wird der Link als Symbol in der Liste der App-Tabelle angezeigt. Der Link wird mit der Liste der verfügbaren Anwendungen und Desktops angezeigt, wenn Benutzer sich bei Worx Home anmelden.

Für den hinzuzufügenden Link müssen Sie die folgenden Informationen angeben:

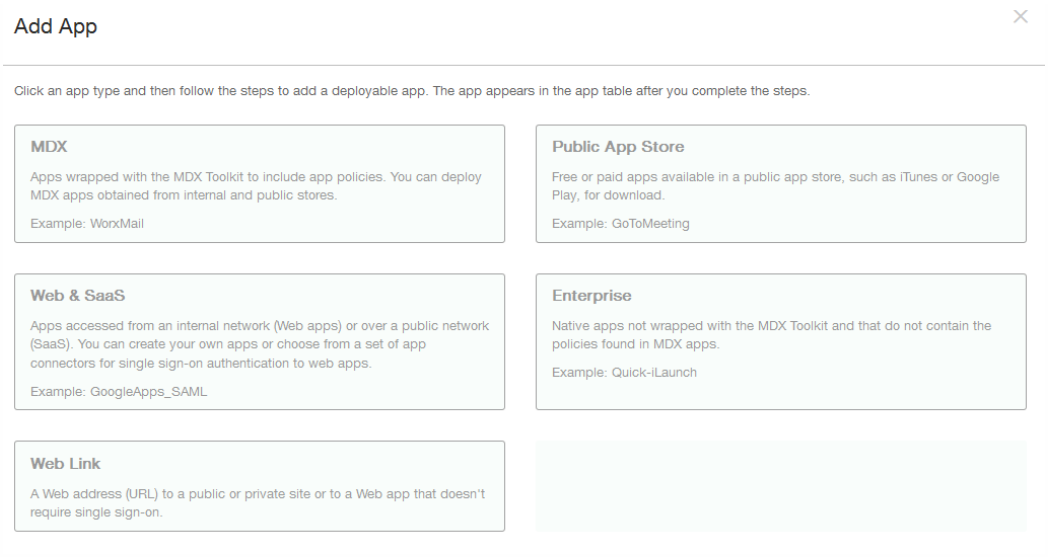
- Name für den Link
- Beschreibung des Links
- Webadresse (URL)
- Category
- Rolle
- Bild im PNG-Format (optional)

So fügen Sie in XenMobile einen Weblink hinzu

1. Configure > Apps. Die Seite Apps wird geöffnet.
2. Klicken Sie auf der Seite Apps auf Add.

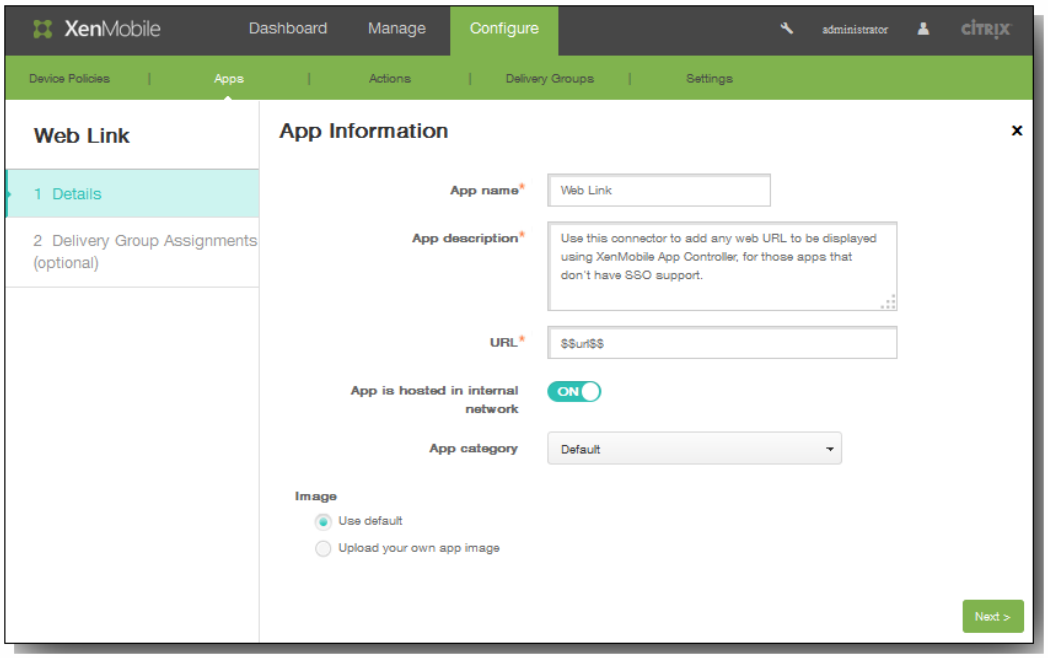


3. Klicken Sie auf der Seite Add App auf Web Link.

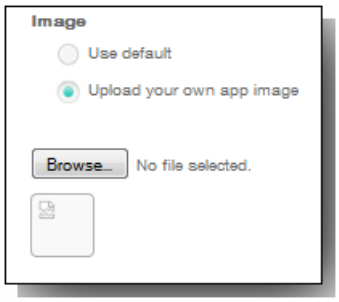


Die Seite App Information wird angezeigt.

4. Die Felder App name, Description und URL sind bereits ausgefüllt.

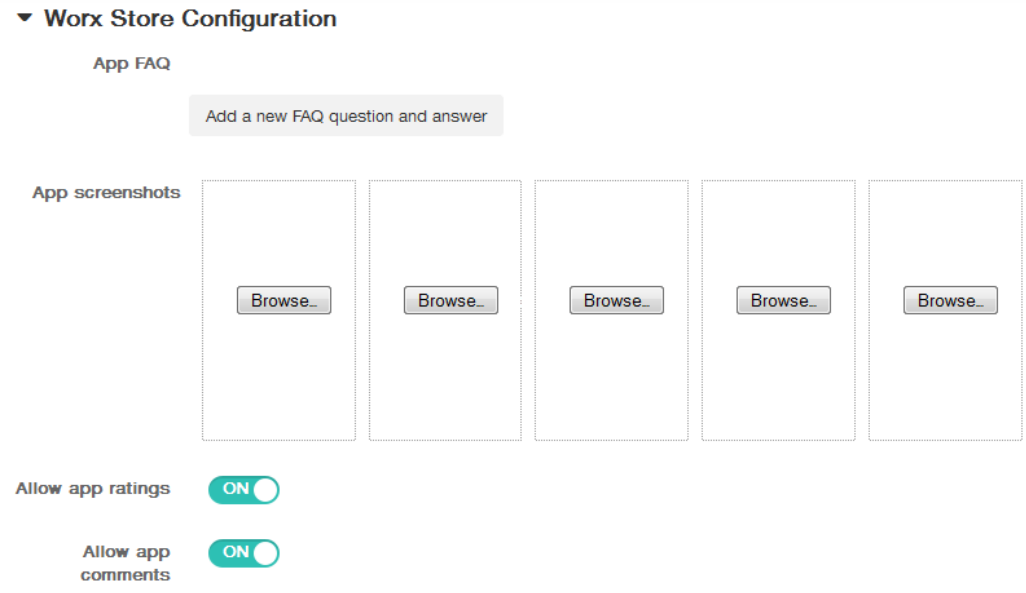


1. Geben Sie unter URL ggf. die Webadresse der App ein oder behalten Sie die Standardadresse bei.
2. Klicken Sie unter App is hosted in internal network auf ON, wenn die App auf einem Server im internen Netzwerk ausgeführt wird. Wenn Benutzer von einem Remotestandort aus eine Verbindung mit der internen Anwendung herstellen, muss dies über NetScaler Gateway erfolgen. Wenn Sie diese Option auf ON festlegen, wird das VPN-Schlüsselwort der App hinzugefügt, sodass Benutzer eine Verbindung über NetScaler Gateway herstellen können.
3. Klicken Sie in der Liste App category auf eine Kategorie.
4. Wenn Sie eine eigene Miniaturansicht zuweisen möchten, wählen Sie Upload your own app image aus. Klicken Sie auf Browse, um das gewünschte Bild zu suchen:



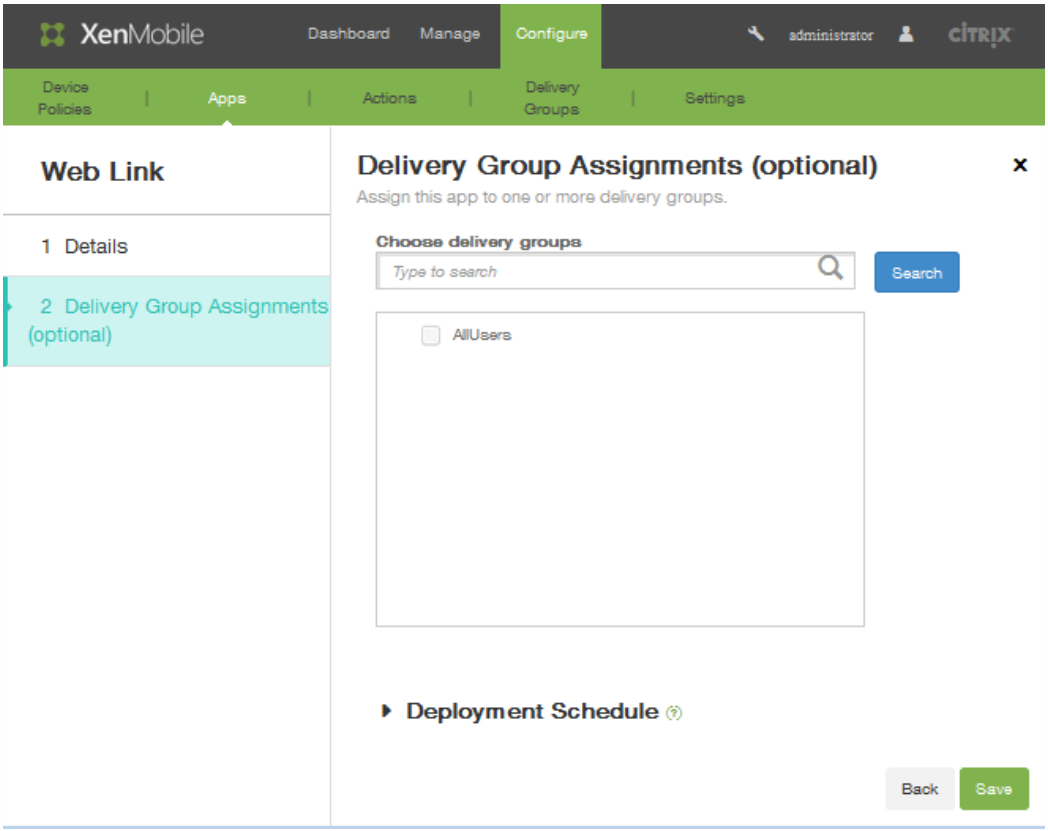
Bilder müssen im PNG-Format vorliegen.

5. Erweitern Sie Worx Store Configuration, um FAQ für die App oder Bildschirmaufnahmen zur Klassifizierung des App im Worx Store hinzuzufügen. Die hochgeladene Grafik muss im PNG-Format sein. Sie können keine GIF- oder JPEG-Bilder hochladen.

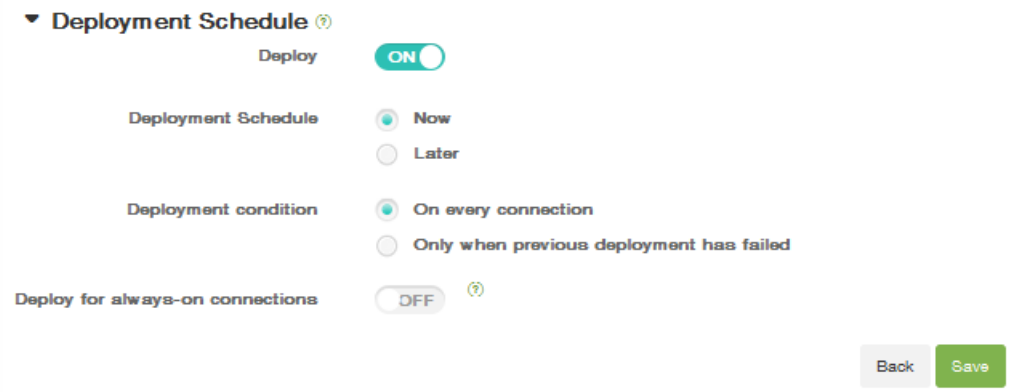


Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.

6. Klicken Sie unter Allow app comments auf ON, um eine Kommentierung der App durch die Benutzer zuzulassen.
7. Klicken Sie auf Next.
8. Weise Sie die App auf der Seite **Delivery Groups Assignment** optional einer oder mehreren Bereitstellungsgruppen zu.



9. Suchen Sie unter Choose delivery groups die Bereitstellungsgruppe(n). Aktivieren Sie das Kontrollkästchen **All Users**, um die App allen XenMobile-Benutzern zuzuweisen.
10. Erweitern Sie Deployment Schedule, um die Bereitstellungsgruppe näher zu definieren.



1. Deploy: Klicken Sie auf ON, um einen Bereitstellungszeitplan zu aktivieren.
2. Deployment Schedule: Klicken Sie auf Now oder Later, um den Bereitstellungszeitplan festzulegen.
3. Deployment condition: Wählen Sie aus, ob die App bei jeder Verbindung oder bei Fehlschlagen der vorherigen Bereitstellung bereitgestellt werden soll.
4. Klicken Sie unter Deploy for always-on connections auf ON, wenn die Bereitstellung erfolgen soll, wenn die Verbindungsrichtlinie "always-on" festgelegt ist.
   Hinweis: Diese Option wird angewendet, wenn Sie im Bereich Server Properties der XenMobile-Konsole unter Settings auch Schlüssel für die globale Bereitstellung im Hintergrund konfiguriert haben. Die Richtlinie "always-on" ist für iOS-Geräte nicht verfügbar.
11. Klicken Sie auf Speichern.

So erstellen und verwalten Sie Workflows

Nov 12, 2015

Sie können das Erstellen und Entfernen von Benutzerkonten mit Workflows verwalten. Damit ein Workflow verwendet werden kann, müssen Sie die Personen in Ihrer Organisation ermitteln, die zum Genehmigen von Benutzerkontenanforderungen berechtigt sind. Anschließend können Sie mit der Workflowvorlage Benutzerkontenanforderungen erstellen und genehmigen.

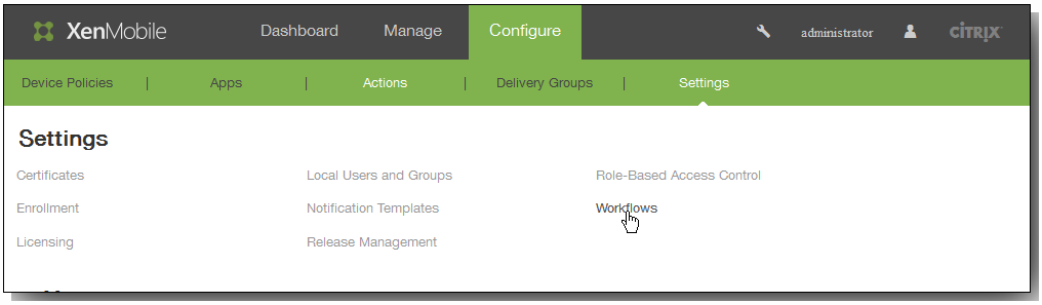
Bei der Erstkonfiguration von XenMobile werden auch die Einstellungen für Workflow-E-Mails konfiguriert. Diese Einstellungen müssen konfiguriert werden, damit Workflows verwendet werden können. Sie können die Einstellungen für Workflow-E-Mails jederzeit ändern. Diese Einstellungen umfassen E-Mail-Server, Port, E-Mail-Adresse und Angaben dazu, ob die Anforderung zum Erstellen des Benutzerkontos genehmigt werden muss.

Workflows können in XenMobile an zwei Stellen konfiguriert werden:

- Auf der Seite Workflows in der XenMobile-Konsole: Auf der Seite Workflows können Sie mehrere Workflows zur Verwendung mit App-Konfigurationen verwenden. Wenn Sie Workflows auf der Seite Workflows konfigurieren, können Sie den Workflow während des Konfigurierens der App auswählen.
- Wenn Sie einen Anwendungsconnector konfigurieren, geben Sie in der App einen Workflow-Namen an und konfigurieren anschließend die Personen, die die Benutzerkontoanforderung genehmigen können. Siehe Hinzufügen von Apps in XenMobile

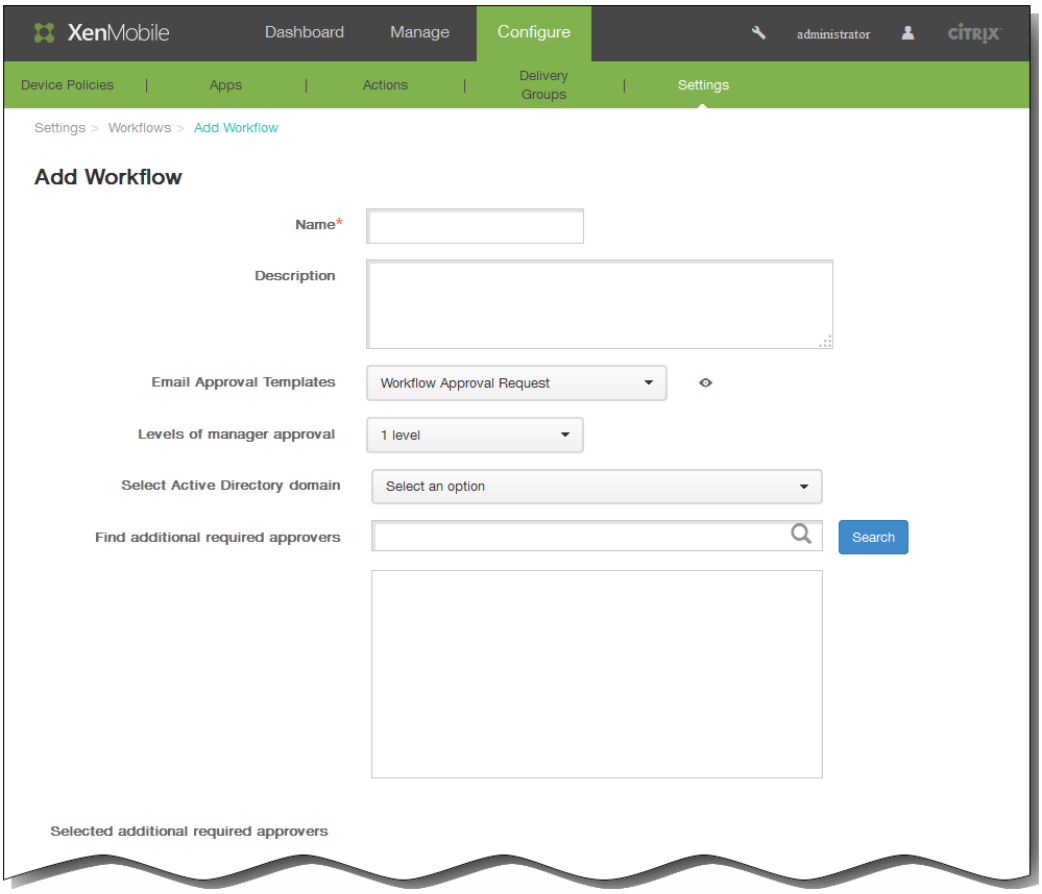
Sie können bis zu drei Ebenen für die Genehmigung von Benutzerkonten durch leitende Mitarbeiter zuweisen. Wenn noch weitere Personen zum Genehmigen eines Benutzerkontos berechtigt sein sollen, können Sie anhand des Namens oder der E-Mail-Adresse weitere genehmigende Personen suchen und auswählen. Wenn XenMobile die Person gefunden hat, können Sie sie zum Workflow hinzufügen. Alle Personen im Workflow erhalten E-Mails zum Genehmigen oder Ablehnen des neuen Benutzerkontos.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Workflows.



Die Seite Workflows wird angezeigt.

2. Klicken Sie auf der Seite Workflows auf Add. Die Seite Add Workflow wird angezeigt.



3. Geben Sie auf der Seite Add Workflow im Feld Name einen eindeutigen Namen für den Workflow ein.
4. Geben Sie unter Description optional eine Beschreibung für den Workflow ein.
5. Wählen Sie in der Liste Email Approval Templates die E-Mail-Genehmigungsvorlage aus, die zugewiesen werden soll. Sie erstellen E-Mail-Vorlagen im Bereich Notification Templates der XenMobile-Konsole unter Settings. Wenn Sie auf das Augensymbol rechts neben dem Feld klicken, wird der folgende Tipp angezeigt.

6. Wählen Sie in der Liste Levels of manager approval die Anzahl der Managergenehmigungsebenen für den Workflow aus.
7. Wählen Sie in der Liste Select Active Directory domain die für den Workflow zu verwendende Active Directory-Domäne aus.
8. Geben Sie neben Find additional required approvers den Namen der zusätzlich erforderlichen Person in das Suchfeld ein und klicken Sie dann auf Search. Für die Namen wird Active Directory verwendet.
9. Wenn der Name der Person im Feld angezeigt wird, aktivieren Sie das Kontrollkästchen daneben. Der Name und die E-

Mail-Adresse der Person werden im Feld Selected additional required approvers angezeigt. Zum Entfernen einer Person aus der Liste Selected additional required approvers führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf Search, um eine Liste aller Personen in der ausgewählten Domäne anzuzeigen.
- Geben Sie den Namen der Person vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf Search, um das Suchergebnis einzuschränken.

Die Namen der Personen in der Liste Selected additional required approvers sind im Suchergebnis mit einem Häkchen gekennzeichnet. Navigieren Sie durch die Liste und deaktivieren Sie die Kontrollkästchen aller Personen, die Sie entfernen möchten.

10. Klicken Sie auf Speichern.
    Der erstellte Workflow wird auf der Seite Workflows angezeigt.

Nach dem Erstellen des Workflows können Sie dessen Details und die mit ihm verbundenen Apps anzeigen oder den Workflow löschen. Ein einmal erstellter Workflow kann nicht mehr geändert werden. Wenn ein Workflow mit anderen Genehmigungsebenen oder Freigabeberechtigten benötigt wird, müssen Sie einen neuen erstellen.

So zeigen Sie Details an und löschen einen Workflow

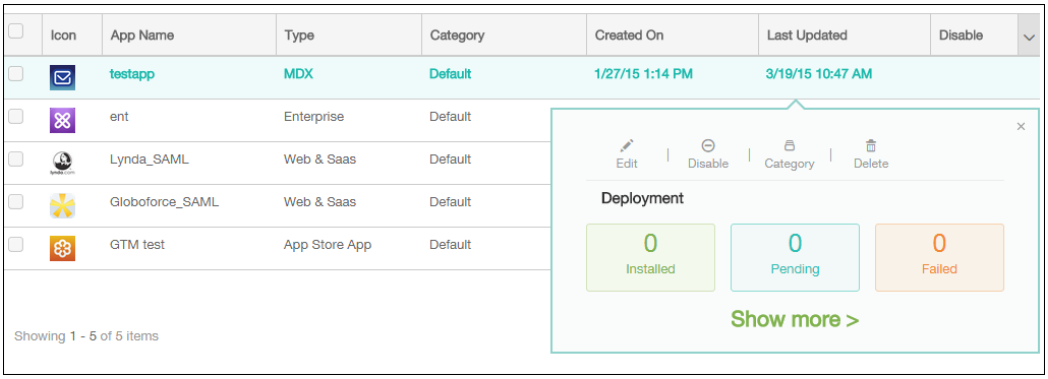
1. Wählen Sie auf der Seite Workflows in der Liste der Workflows einen Workflow durch Klicken auf die Zeile in der Tabelle oder Aktivieren des Kontrollkästchens neben dem Workflow aus.
2. Klicken Sie zum Löschen des Workflows auf Delete. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie noch einmal auf Delete.
   Wichtig: Sie können diesen Vorgang nicht rückgängig machen.

Aktualisieren einer App in XenMobile

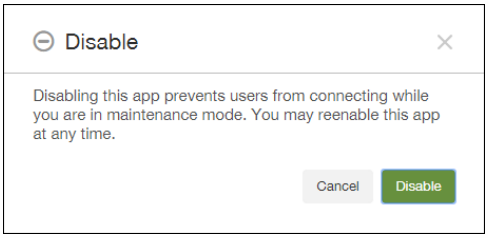
Nov 12, 2015

Zum Aktualisieren einer App in XenMobile deaktivieren Sie diese in der XenMobile-Konsole und laden die neue App-Version hoch.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Apps.
2. Fahren Sie bei verwalteten, d. h. bei XenMobile für die Mobilgeräteverwaltung registrierten Geräten mit Schritt 3 fort. Führen Sie für nicht verwaltete, d. h. bei XenMobile nur zum Zweck der App-Verwaltung registrierten Geräten die folgenden Schritte aus:
   1. Klicken Sie in der Tabelle der Apps auf die App, die Sie aktualisieren möchten, und klicken Sie in dem nun angezeigten Menü auf Disable.

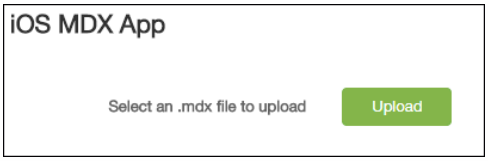


   2. Klicken Sie im Bestätigungsdialogfeld auf Disable.



   Als Status der App wird in der Tabelle nun Disabled angezeigt.

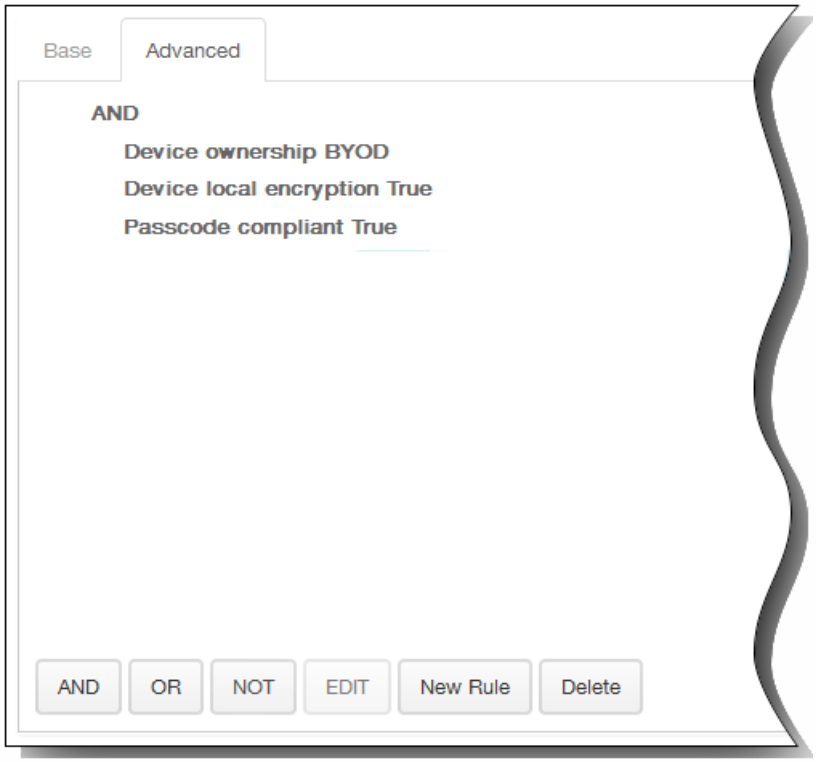
   Hinweis: Durch Deaktivieren werden Apps in den Wartungsmodus versetzt. Benutzer können nach der Abmeldung keine Verbindung mit deaktivierten Apps mehr herstellen. Das Deaktivieren von Apps ist optional, wird aber von Citrix empfohlen, um Probleme bei der App-Funktionalität zu vermeiden. Probleme können beispielsweise durch Richtlinienupdates auftreten, oder wenn ein Benutzer einen Download zur gleichen Zeit anfordert, zu der Sie die App in XenMobile hochladen.
3. Wählen Sie die App aus und klicken Sie in dem nun angezeigten Menü auf Edit. Die ursprünglich für die App ausgewählte Plattform ist ausgewählt.
4. Auf der Seite App Information ändern Sie optional die Angaben für Name, Description oder App category und klicken Sie auf Next.
5. Klicken Sie auf Upload, um die Datei, die Sie zum Ersetzen der aktuellen App hochladen möchten, auszuwählen, und klicken Sie auf Next.



Die Anwendung wird in XenMobile hochgeladen. Optional können Sie die App-Details und Richtlinieneinstellungen ändern.

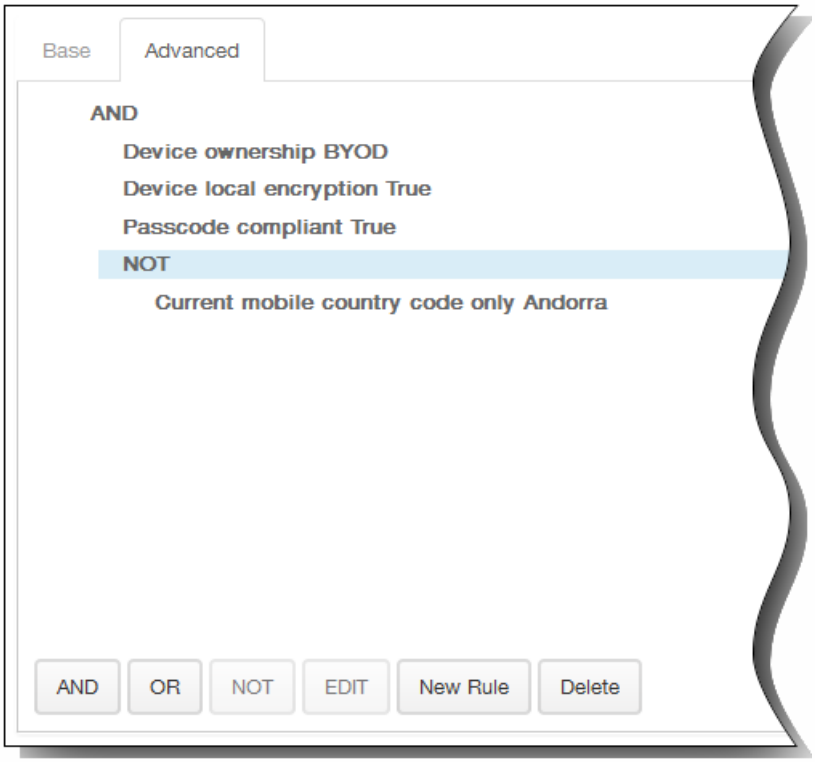
6. Klicken Sie auf Next und behalten Sie in den Schritten 8 bis 14 die Einstellungen bei, bzw. nehmen Sie Änderungen für das Upgrade vor.
7. Erweitern Sie Deployment Rules. Standardmäßig wird die Registerkarte Base angezeigt.

1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die App bereitgestellt werden soll.
    1. Sie können die App bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.

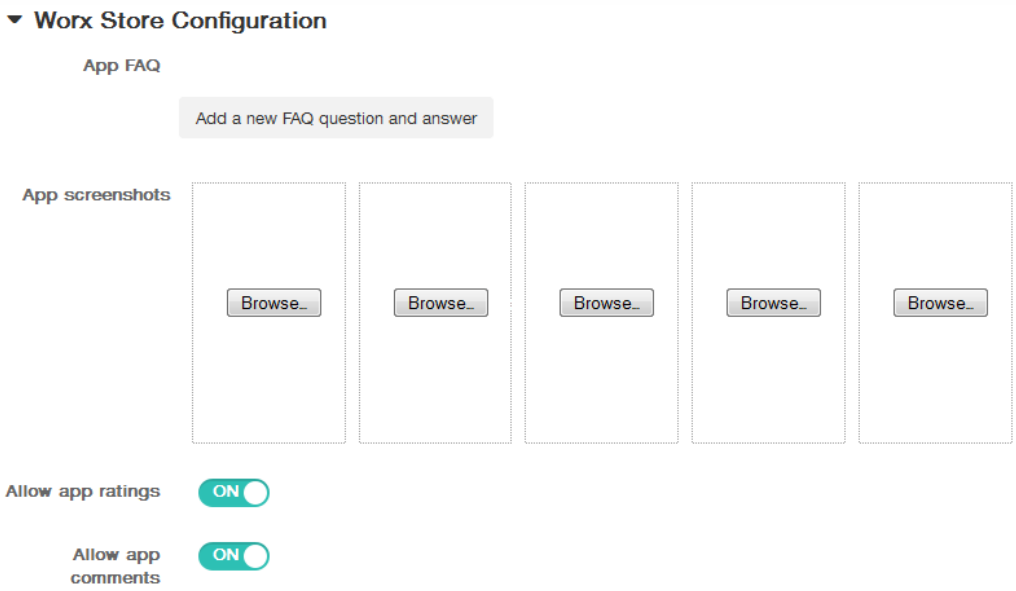


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

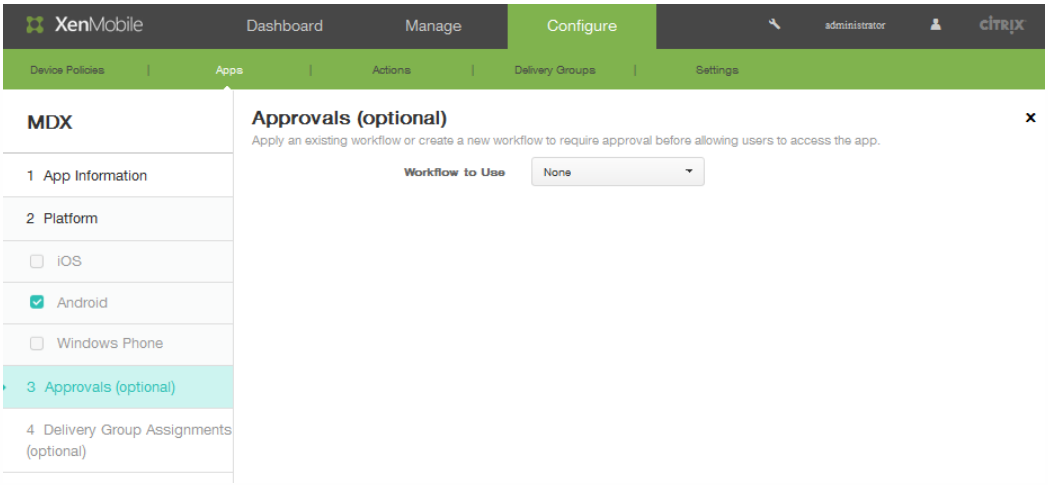
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.
   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



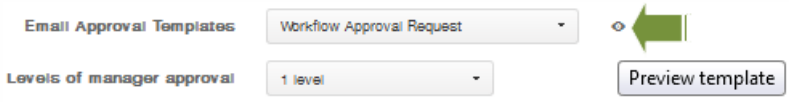
8. Erweitern Sie Worx Store Configuration, um FAQ für die App oder Bildschirmaufnahmen zur Klassifizierung des App im Worx Store hinzuzufügen. Die hochgeladene Grafik muss im PNG-Format sein. Sie können keine GIF- oder JPEG-Bilder hochladen.



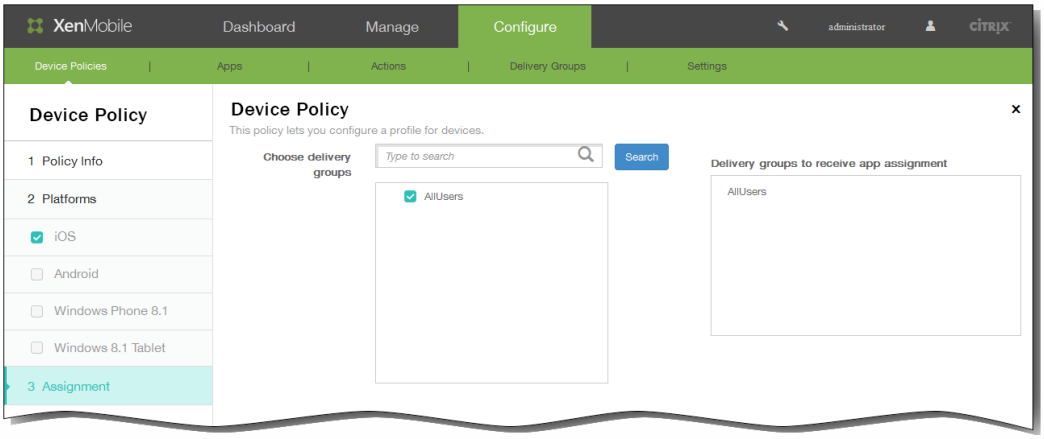
   Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.
9. Klicken Sie unter Allow app comments auf ON, um eine Kommentierung der App durch die Benutzer zuzulassen.
10. Klicken Sie auf Next. Die Seite Approvals wird angezeigt.



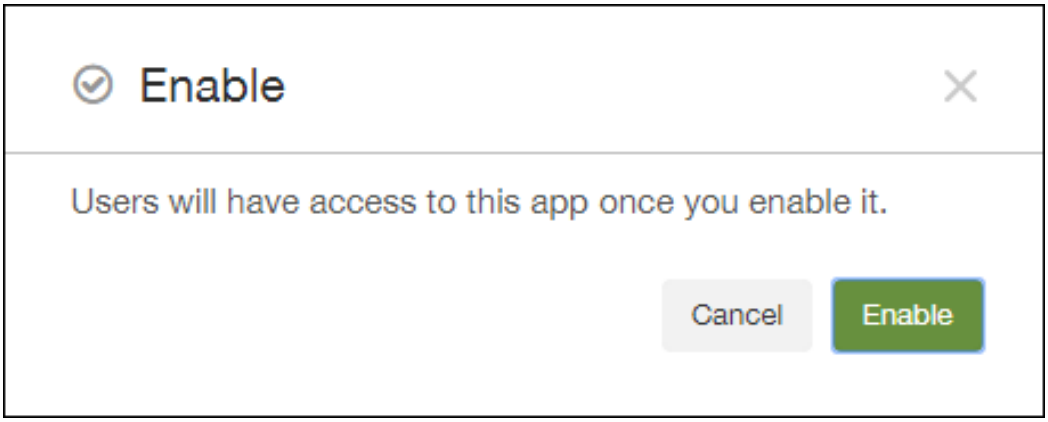
11. Wenn Sie einen neuen Workflow erstellen, werden in der XenMobile-Konsole nun Konfigurationsoptionen für den Freigabeprozess angezeigt. Die betreffenden Felder werden in den nachfolgenden Schritten erläutert. Konfigurieren Sie diese Felder, wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist.
    1. Geben Sie unter **Name** einen Namen für den Workflow ein.
    2. Geben Sie optional unter **Description** eine Beschreibung ein.
    3. Klicken Sie unter **Email Approval Templates** auf eine Benachrichtigungsoption. Klicken Sie auf das **Augensymbol**, um eine Vorschau der ausgewählten Vorlage anzuzeigen.



    4. Klicken Sie unter **Levels of manager approval** auf eine Stufe zwischen None und 3. .
    5. Klicken Sie unter **Select Active Directory domain** auf die Domäne.
    6. Geben Sie unter Find additional required approvers optional weitere Freigabeberechtigte ein und klicken Sie auf Search.
12. Klicken Sie auf Next.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



14. Klicken Sie auf Save. Die Seite Apps wird angezeigt.
15. Wenn Sie die App in Schritt 2 deaktiviert haben, führen Sie folgende Schritte aus:
    1. Klicken Sie in der Tabelle der Apps auf die App, die Sie aktualisiert haben, und klicken Sie in dem nun angezeigten Menü auf Enable.
    2. Klicken Sie in der daraufhin angezeigten Bestätigungsmeldung auf Enable.



Die Benutzer können jetzt auf die App zugreifen und erhalten eine Benachrichtigung mit der Aufforderung, die App zu aktualisieren.

MDX App-Richtlinien auf einen Blick

Apr 12, 2016

Eine Tabelle mit den MDX-App-Richtlinien für iOS, Android und Windows Phone einschließlich Hinweisen zu Einschränkungen und Empfehlungen von Citrix finden Sie unter MDX App-Richtlinien auf einen Blick in der Dokumentation zum MDX Toolkit.

Hinweis: Durch Worx Home werden Richtlinien bei bestimmten Aktionen aktualisiert. Weitere Informationen finden Sie unter Worx Home.

Konfigurieren von XenMobile und der ShareFile-App für Single Sign-On mit SAML

Oct 11, 2016

Sie können XenMobile und ShareFile so konfigurieren, dass diese mit Security Assertion Markup Language (SAML) Single Sign-On-Zugriff (SSO) für mobile ShareFile-Apps, die mit dem MDX Toolkit umschlossen wurden, sowie für nicht umschlossene ShareFile-Clients (z. B. Website, Outlook-Plug-In oder Synchronisierungsclients) bereitstellen.

- **Umschlossene ShareFile-Apps**: Benutzer, die sich bei ShareFile über die mobile ShareFile-App anmelden, werden zur Benutzerauthentifizierung und zum Abrufen eines SAML-Tokens an Worx Home weitergeleitet. Nach einer erfolgreichen Authentifizierung sendet die mobile ShareFile-App das SAML-Token an ShareFile. Nach der ersten Anmeldung können Benutzer über SSO auf die mobile ShareFile-App zugreifen und Dokumente aus ShareFile an WorxMail-E-Mails anhängen, ohne sich jedes Mal erneut anmelden zu müssen.
- **Nicht umschlossene ShareFile-Clients**: Benutzer, die sich bei ShareFile über einen Webbrowser oder einen anderen ShareFile-Client anmelden, werden zur Benutzerauthentifizierung und zum Abrufen eines SAML-Tokens an XenMobile weitergeleitet. Nach einer erfolgreichen Authentifizierung wird das SAML-Token an ShareFile gesendet. Nach der ersten Anmeldung können Benutzer auf ShareFile-Clients über SSO ohne erneute Anmeldung zugreifen.

Ein detailliertes Architekturdiagramm finden Sie im Artikel Reference Architecture for On-Premises Deployments in der XenMobile-Bereitstellungsdokumentation.

Voraussetzungen

Damit Sie Single Sign-On für XenMobile und ShareFile-Apps konfigurieren können, müssen die folgenden Voraussetzungen erfüllt sein:

- MDX Toolkit Version 9.0.4 oder höher (für mobile ShareFile-Apps)
- Erforderliche mobile ShareFile-Apps:
  - ShareFile für iPhone Version 3.0.x
  - ShareFile für iPad Version 2.2.x
  - ShareFile für Android Version 3.2.x
- Worx Home 9.0 (für mobile ShareFile-Apps)
  Installieren Sie die iOS- bzw. die Android-Version nach Bedarf.
- ShareFile-Administratorkonto

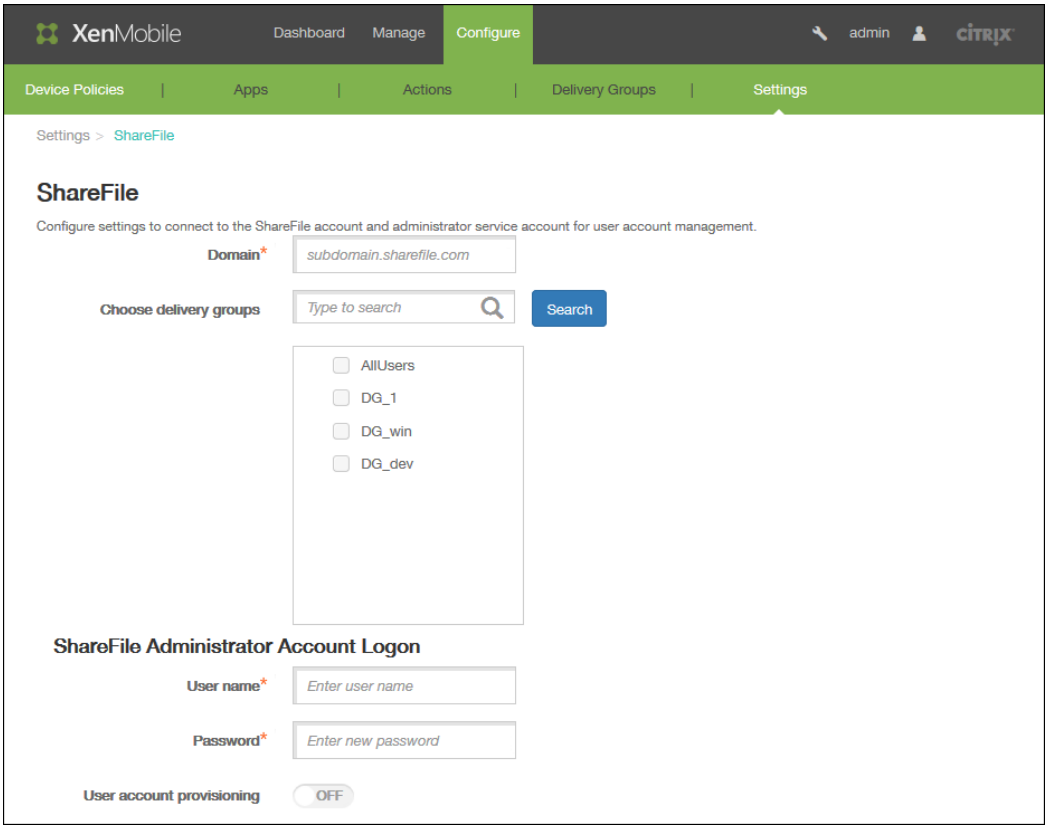
Stellen Sie sicher, dass XenMobile und ShareFile eine Verbindung herstellen können. Weitere Informationen zum Überprüfen der Konnektivität finden Sie unter Durchführen von Verbindungsüberprüfungen.

Konfigurieren des ShareFile-Zugriffs

Vor der Konfiguration von SAML für ShareFile geben Sie die ShareFile-Zugriffsinformationen wie folgt an:

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings. Die Seite Settings wird angezeigt.

2. Klicken Sie auf More und dann unter ShareFile auf ShareFile. Die Seite ShareFile wird angezeigt.



3. Konfigurieren Sie die folgenden Einstellungen:
   - Domain: Geben Sie den Namen Ihrer ShareFile-Unterdomäne an, z. B. example.sharefile.com.
   - Choose delivery groups: Wählen Sie die Bereitstellungsgruppen aus (bzw. suchen Sie sie), für die Sie die Verwendung von SSO mit ShareFile aktivieren möchten.
   - User name: Geben Sie den Namen des ShareFile-Administrators ein. Dieses Benutzerkonto muss über Administratorrechte verfügen.
   - Password Geben Sie das Kennwort des ShareFile-Administrators ein.
   - User account provisioning: Aktivieren Sie diese Option, wenn Sie das Benutzerprovisioning in XenMobile aktivieren möchten. Wenn Sie stattdessen das ShareFile User Management Tool verwenden möchten, lassen Sie die Option deaktiviert.
     Hinweis: Enthalten die ausgewählten Rollen einen Benutzer ohne ShareFile-Konto, wird in XenMobile automatisch ein ShareFile-Konto für diesen Benutzer bereitgestellt, wenn Sie User account provisioning aktivieren. Citrix empfiehlt die Verwendung einer Rolle mit wenigen Mitgliedern zum Testen der Konfiguration. So wird eine potenziell große Zahl von Benutzern ohne ShareFile-Konto vermieden.
4. Klicken Sie auf Speichern.

Konfigurieren von SAML für umschlossenen ShareFile MDX-Apps

Die folgenden Schritte gelten für iOS- und Android-Apps und -Geräte.

1. Umschließen Sie die mobile ShareFile-App mit dem MDX Toolkit. Informationen zum Umschließen von Apps mit dem MDX Toolkit finden Sie unter Umschließen von Apps mit dem MDX Toolkit.
2. Laden Sie die umschlossene mobile ShareFile-App in XenMobile hoch. Informationen zum Hochladen von MDX-Apps

finden Sie unter So fügen Sie XenMobile eine MDX-App hinzu.

3. Überprüfen Sie die SAML-Einstellungen, indem Sie sich bei ShareFile mit den Anmeldeinformationen des Administrators, die Sie beim Konfigurieren des ShareFile-Zugriffs festgelegt haben, anmelden.
4. Stellen Sie sicher, dass ShareFile und XenMobile für dieselbe Zeitzone konfiguriert sind.
   Hinweis: Unterschiedliche Zeitzonen können dazu führen, dass Zeitstempel nicht übereinstimmen und das SSO fehlschlägt.

Überprüfen der mobilen ShareFile-App

1. Falls noch nicht geschehen, installieren und konfigurieren Sie Worx Home auf dem Benutzergerät.
2. Laden Sie die mobile ShareFile-App aus dem Worx Store herunter und installieren Sie sie.
3. Starten Sie die mobile ShareFile-App.
   ShareFile wird ohne Anforderung von Benutzernamen und Kennwort gestartet.

Überprüfung über WorxMail

1. Falls noch nicht geschehen, installieren und konfigurieren Sie Worx Home auf dem Benutzergerät.
2. Laden Sie WorxMail aus dem Worx Store herunter, installieren und konfigurieren Sie es.
3. Öffnen Sie ein neues E-Mail-Formular und tippen Sie auf Von ShareFile anfügen.
   Die zum Anfügen verfügbaren Dateien werden ohne Anforderung von Benutzernamen und Kennwort angezeigt.

Konfigurieren von NetScaler Gateway für andere ShareFile-Clients

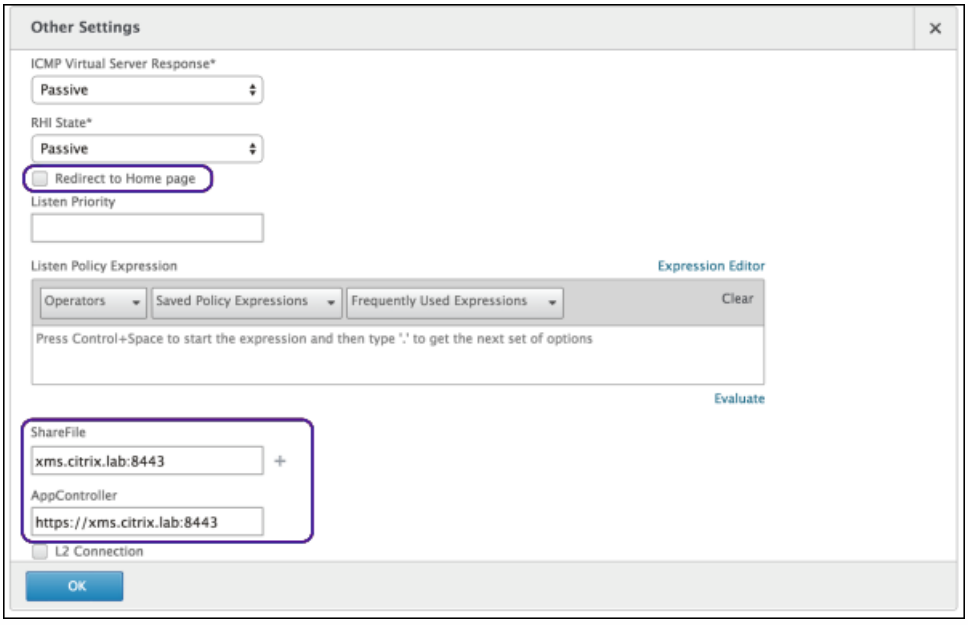
Wenn Sie den Zugriff für nicht umschlossene ShareFile-Clients (z. B. Website, Outlook-Plug-In oder Synchronisierungsclients) konfigurieren möchten, müssen Sie NetScaler Gateway folgendermaßen konfigurieren, damit es die Verwendung von XenMobile als SAML-Identitätsanbieter unterstützt:

- Deaktivieren Sie die Homepageumleitung.
- Erstellen Sie eine ShareFile-Sitzungsrichtlinie und ein Profil.
- Konfigurieren Sie Richtlinien auf dem virtuellen NetScaler Gateway-Server.

Deaktivieren der Homepageumleitung

Sie müssen die Standardverarbeitung von Anforderungen, die über den /cginfra-Pfad eingehen, deaktivieren, damit den Benutzern die ursprüngliche angeforderte interne URL anstelle der konfigurierten Homepage angezeigt wird.

1. Bearbeiten Sie die Einstellungen für den virtuellen NetScaler Gateway-Server, der für XenMobile-Anmeldungen verwendet wird. Navigieren Sie in NetScaler 10.5 zu Other Settings und deaktivieren Sie das Kontrollkästchen Redirect to Home Page.

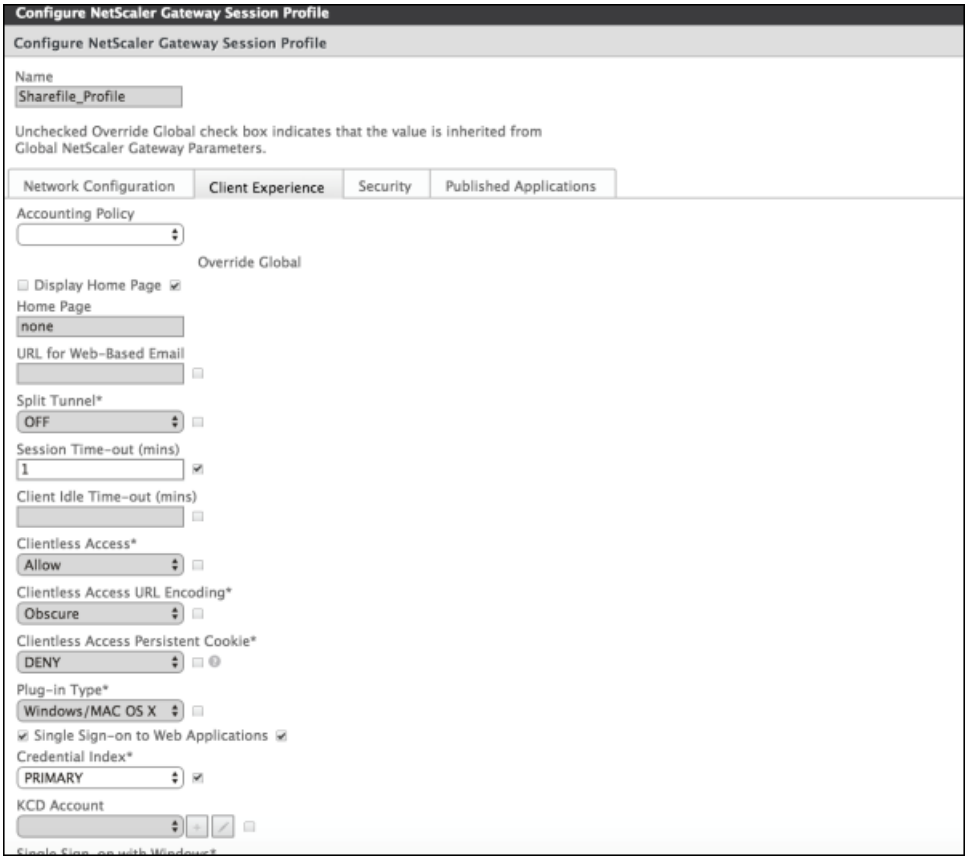


2. Geben Sie unter ShareFile den internen Namen des XenMobile-Servers und die Portnummer ein.
3. Geben Sie unter AppController die XenMobile-URL ein.
   Mit dieser Konfiguration werden Anforderungen an die über den /cginfra-Pfad eingegebene URL genehmigt.

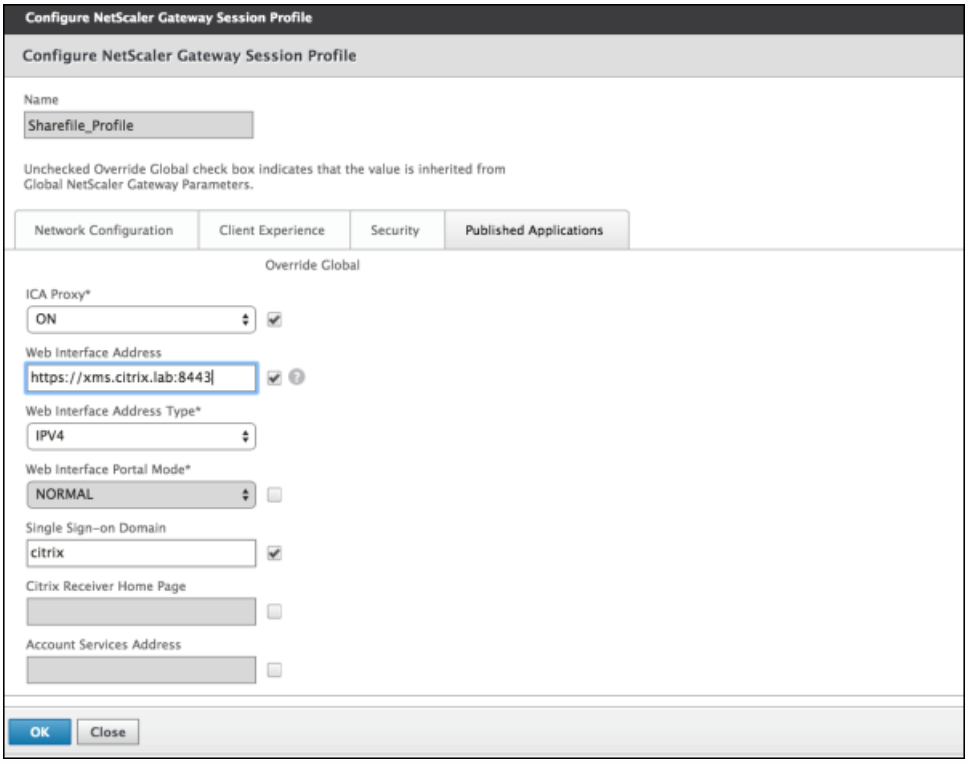
Erstellen einer ShareFile-Sitzungsrichtlinie und eines Anforderungsprofils

Konfigurieren Sie die folgenden Einstellungen zum Erstellen einer ShareFile-Sitzungsrichtlinie und eines Anforderungsprofils:

1. Klicken Sie im Konfigurationsprogramm für NetScaler Gateway im linken Navigationsbereich auf NetScaler GatewayPoliciesSession.
2. Erstellen Sie eine neue Sitzungsrichtlinie. Klicken Sie auf der Registerkarte Policies auf Add.
3. Geben Sie im Feld Name den Ausdruck ShareFile_Policy ein.
4. Erstellen Sie eine neue Aktion durch Klicken auf die +-Schaltfläche.
   Der Bildschirm Create NetScaler Gateway Session Profile wird angezeigt. Konfigurieren Sie die folgenden Einstellungen:

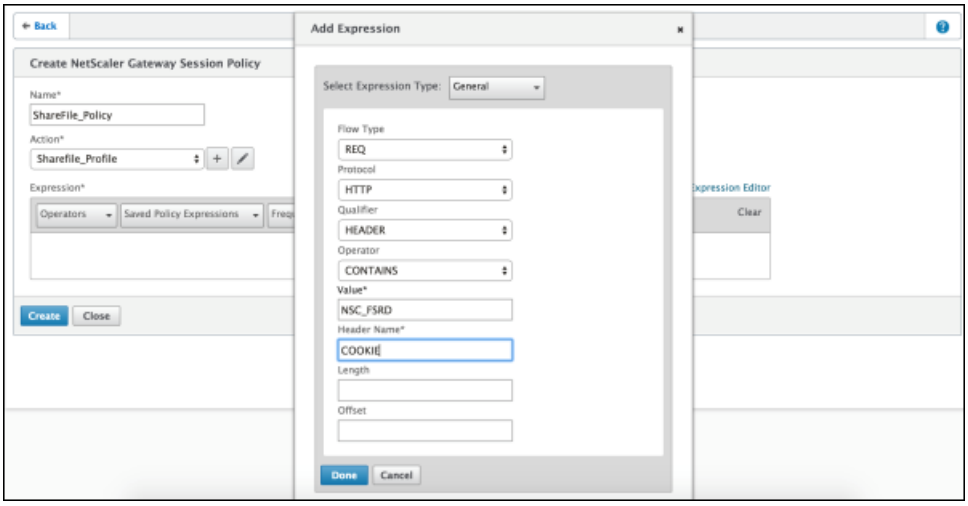


1. Name: Geben Sie ShareFile_Profile ein.
2. Klicken Sie auf die Registerkarte Client Experience und konfigurieren Sie dann die folgenden Einstellungen:
    1. Home Page: Geben Sie none ein.
    2. Session Time-out (mins): Geben Sie 1 ein.
    3. Single Sign-on to Web Applications: Wählen Sie diese Einstellung.
    4. Credential Index: Klicken Sie in der Liste auf PRIMARY.
3. Klicken Sie auf die Registerkarte Published Applications und konfigurieren Sie dann die folgenden Einstellungen:



1. ICA Proxy: Wählen Sie in der Liste ON aus.
2. Web Interface Address: Geben Sie die URL des XenMobile-Servers ein.
3. Single Sign-on Domain: Geben Sie den Namen Ihrer Active Directory-Domäne ein.
   Hinweis: Beim Konfigurieren des NetScaler Gateway-Sitzungsprofils muss das Domänensuffix für Single Sign-on Domain mit dem in LDAP festgelegten XenMobile-Domänenalias übereinstimmen.

5. Klicken Sie auf Create, um das Sitzungsprofil zu definieren.
6. Klicken Sie auf Expression Editor, und konfigurieren Sie dann die folgenden Einstellungen:



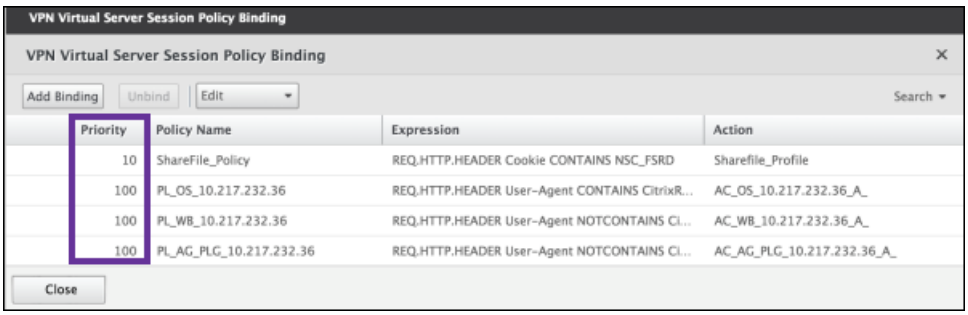
1. Value: Geben Sie NSC_FSRD ein.
2. Header Name: Geben Sie COOKIE ein.
3. Klicken Sie auf Done.

7. Klicken Sie auf Create und dann auf Close.

Konfigurieren von Richtlinien auf dem virtuellen NetScaler Gateway-Server

Konfigurieren Sie die folgenden Einstellungen auf dem virtuellen NetScaler Gateway-Server.

1. Klicken Sie im Konfigurationsprogramm für NetScaler Gateway im linken Navigationsbereich auf NetScaler Gateway > Virtual Servers.
2. Klicken Sie im Bereich Details auf den virtuellen NetScaler Gateway-Server.
3. Klicken Sie auf Edit.
4. Klicken Sie auf Configured policies > Session policies und dann auf Add binding.
5. Wählen Sie ShareFile_Policy aus.
6. Bearbeiten Sie die automatisch generierte Prioritätszahl unter Priority für die ausgewählte Richtlinie so, dass sie die höchste Priorität (die niedrigste Zahl) vor allen anderen aufgeführten Richtlinien hat (siehe folgende Abbildung).



7. Klicken Sie auf Done und speichern Sie die ausgeführte NetScaler-Konfiguration.

Konfigurieren von SAML für ShareFile-Apps ohne MDX

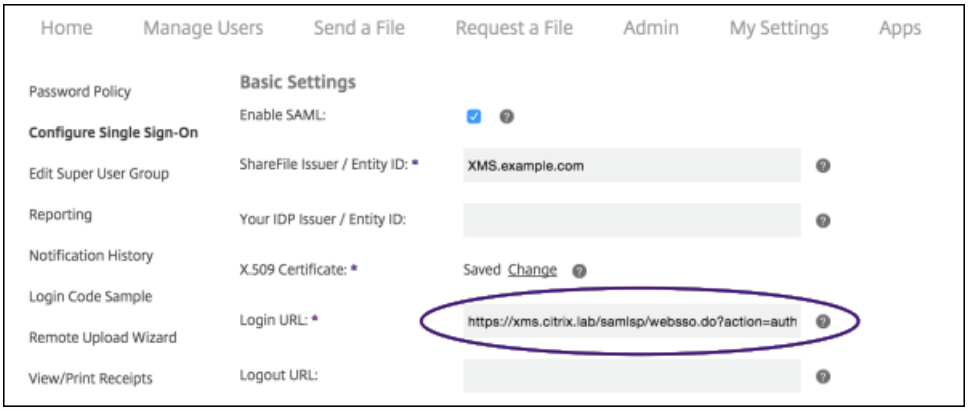
Ermitteln Sie anhand der folgenden Schritte den internen App-Namen für die ShareFile-Konfiguration.

1. Melden Sie sich bei dem Verwaltungstool für XenMobile unter Verwendung der URL https://:4443/OCA/admin/ an. Geben Sie dabei "OCA" unbedingt in Großbuchstaben ein.
2. Klicken Sie in der Liste View auf Configuration.

3. Klicken Sie auf Applications > Applications und notieren Sie den unter Application Name für die App angezeigten Namen mit dem unter Display Name angezeigten Anzeigenamen "ShareFile".

Ändern der SSO-Einstellungen für ShareFile.com

1. Melden Sie sich bei Ihrem ShareFile-Konto (https://.sharefile.com) als ShareFile-Administrator an.
2. Klicken Sie im ShareFile-Webinterface auf Admin und wählen Sie Configure Single Sign-on aus.
3. Bearbeiten Sie den Eintrag im Feld Login URL wie folgt:
   Der Eintrag im Feld Login URL sollte in etwa so aussehen: https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1.



1. Geben Sie den externen FQDN des virtuellen NetScaler Gateway-Servers plus "/cginfra/https/" vor dem FQDN des

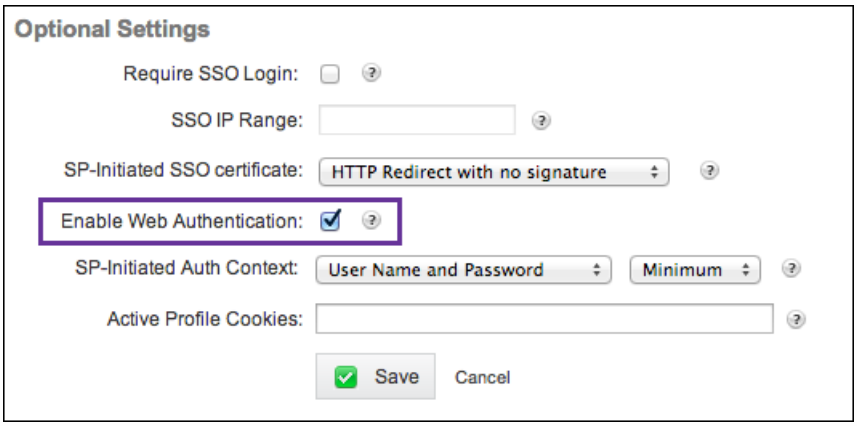
XenMobile-Servers und hinter dem FQDN des XenMobile-Servers "8443" ein.
Die URL sollte nun in etwa so aussehen:
https://**nsgateway.acme.com/cginfra/https**/xms.citrix.lab:**8443**/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1

2. Ändern Sie den Parameter **&app=ShareFile_SAML_SP** auf den in Schritt 3 beim Konfigurieren von SAML für ShareFile-Apps ohne MDX festgelegten internen ShareFile-Anwendungsnamen. Der interne Name lautet standardmäßig **ShareFile_SAML**. Jedes Mal, wenn Sie die Konfiguration ändern, wird jedoch eine Zahl an den internen Namen angehängt (ShareFile_SAML_2, ShareFile_SAML_3 usw.).
Die URL sollte nun in etwa so aussehen:
https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser**&app=ShareFile_SAML**&reqtype=1

3. Hängen Sie "&nssso=true" an das Ende der URL an.
Die geänderte URL sollte nun in etwa so aussehen::
https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1**&nssso=true**.

   Wichtig: Jedes Mal, wenn Sie die ShareFile-App bearbeiten oder neu erstellen oder die ShareFile-Einstellungen in der XenMobile-Konsole ändern, wird an den internen Anwendungsnamen eine neue Zahl angehängt. Sie müssen daher die Anmelde-URL für die ShareFile-Website dem neuen Anwendungsnamen entsprechend ändern.

4. Aktivieren Sie unter Optional Settings das Kontrollkästchen Enable Web Authentication.



5. Klicken Sie auf Speichern.

Überprüfen der Konfiguration

Überprüfen Sie die Konfiguration wie nachfolgend beschrieben.

1. Rufen Sie im Browser https://sharefile.com/saml/login auf.
Sie werden zum NetScaler Gateway-Anmeldungsformular umgeleitet. Erfolgt keine Umleitung, überprüfen Sie die oben aufgeführten Konfigurationseinstellungen.

2. Geben Sie die Anmeldeinformationen ein, die Sie für die NetScaler Gateway- bzw. XenMobile-Umgebung konfiguriert haben.
Die ShareFile-Ordner auf .sharefile.com werden angezeigt. Wenn keine ShareFile-Ordner angezeigt werden, prüfen Sie,

ob Sie die richtigen Anmeldeinformationen eingegeben haben.

Automatisierte Aktionen

Oct 29, 2015

Sie können in XenMobile automatisierte Aktionen zum Programmieren einer Reaktion auf Ereignisse, Benutzer- oder Geräteeigenschaften oder das Vorhandensein von Apps auf Benutzergeräten erstellen. Beim Erstellen einer automatisierten Aktion legen Sie auf der Basis von Auslösern die Auswirkungen auf den Geräten von Benutzern fest, wenn diese eine Verbindung mit XenMobile herstellen. Wenn ein Ereignis ausgelöst wird, können Sie eine Nachricht mit einer Aufforderung zur Problembeseitigung an den betroffenen Benutzer senden, bevor Maßnahmen ergriffen werden.
Wenn Sie beispielsweise Apps entdecken möchten, die Sie gesperrt haben (z. B. Words with Friends), können Sie einen Auslöser festlegen, der ein Gerät als nicht richtlinientreu einstuft, wenn darauf Words with Friends erkannt wird. Der Benutzer wird dann durch die Aktion benachrichtigt, dass er die App entfernen muss, damit sein Gerät wieder richtlinientreu wird. Sie können ein Zeitlimit festlegen, bis zu dem auf eine Korrekturmaßnahme seitens des Benutzers gewartet wird, nach dessen Ablauf Maßnahmen, etwa eine selektive Löschung von Daten, ergriffen werden.

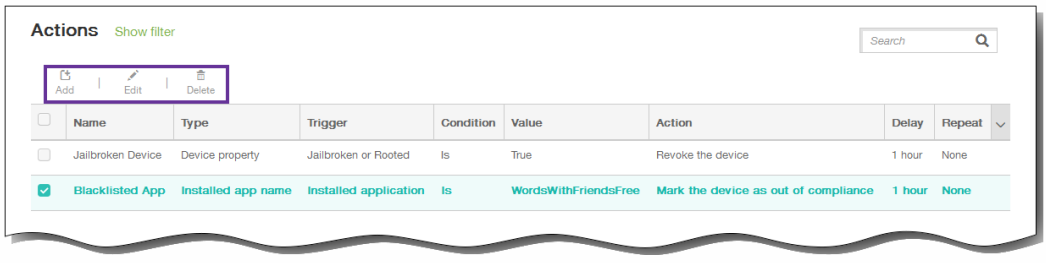
Sie können folgende automatische Auswirkungen festlegen:

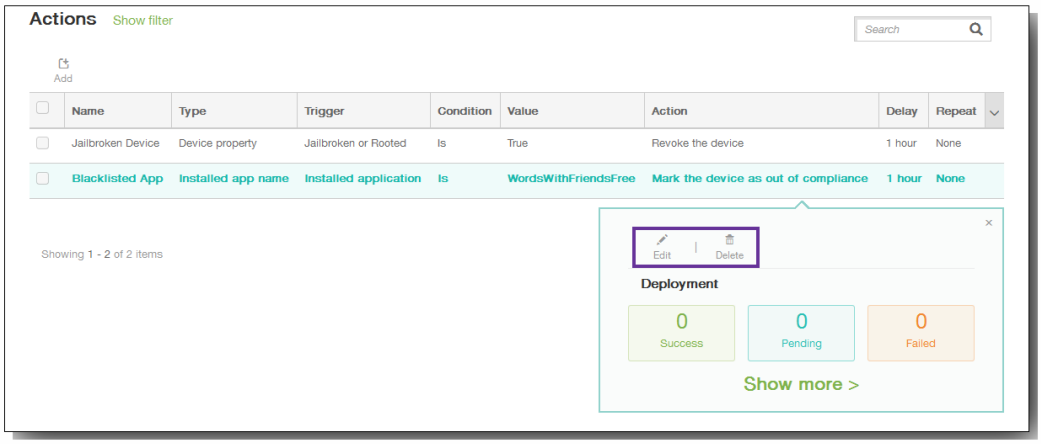
- Vollständige oder selektive Datenlöschung
- Einstufung von Geräten als nicht richtlinientreu
- Widerrufen von Geräten
- Senden einer Benachrichtigung an Benutzer mit der Aufforderung zur Problembehebung

Hinweis: Sie können Benutzer nur benachrichtigen, wenn Sie unter Settings Benachrichtigungsserver für SMTP und SMS konfiguriert haben, damit XenMobile Nachrichten senden kann (siehe Benachrichtigungen in XenMobile). Richten Sie, bevor Sie fortfahren, außerdem alle Benachrichtigungsvorlagen ein, die Sie verwenden möchten. Weitere Informationen über Benachrichtigungsvorlagen finden Sie unter So erstellen oder aktualisieren Sie Benachrichtigungsvorlagen in XenMobile.
In diesem Abschnitt wird erläutert, wie Sie automatisierte Aktionen in XenMobile hinzufügen, bearbeiten und filtern.

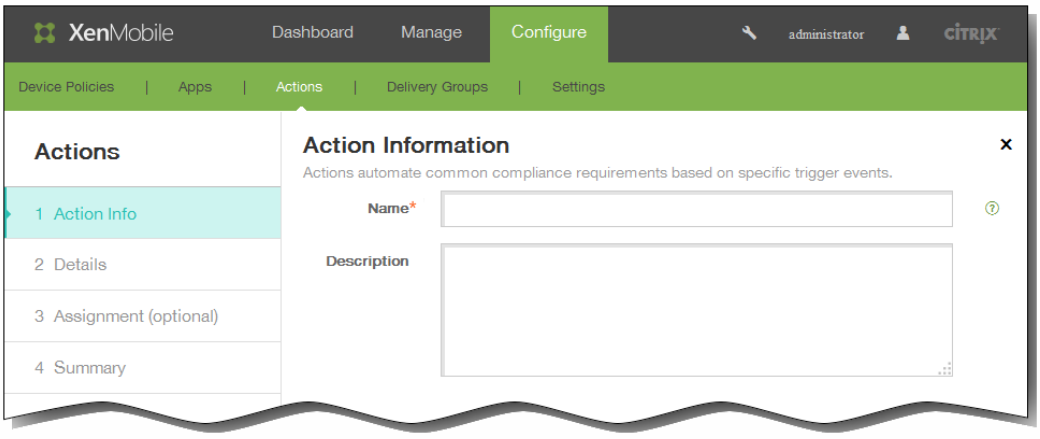
1. Klicken Sie in der XenMobile-Konsole auf Configure > Actions. Die Seite Actions wird angezeigt.

2. Führen Sie auf der Seite Actions einen der folgenden Schritte aus:
   - Klicken Sie auf Add, um eine neue Aktion hinzuzufügen.
   - Wählen Sie eine vorhandene Aktion zum Bearbeiten oder Löschen aus. Klicken Sie auf die gewünschte Option.
     Hinweis: Wenn Sie das Kontrollkästchen neben einer Aktion auswählen, wird das Menü mit den Optionen oberhalb der Liste der Aktionen eingeblendet. Wenn Sie auf eine andere Stelle im Eintrag klicken, wird es rechts neben dem Eintrag eingeblendet.

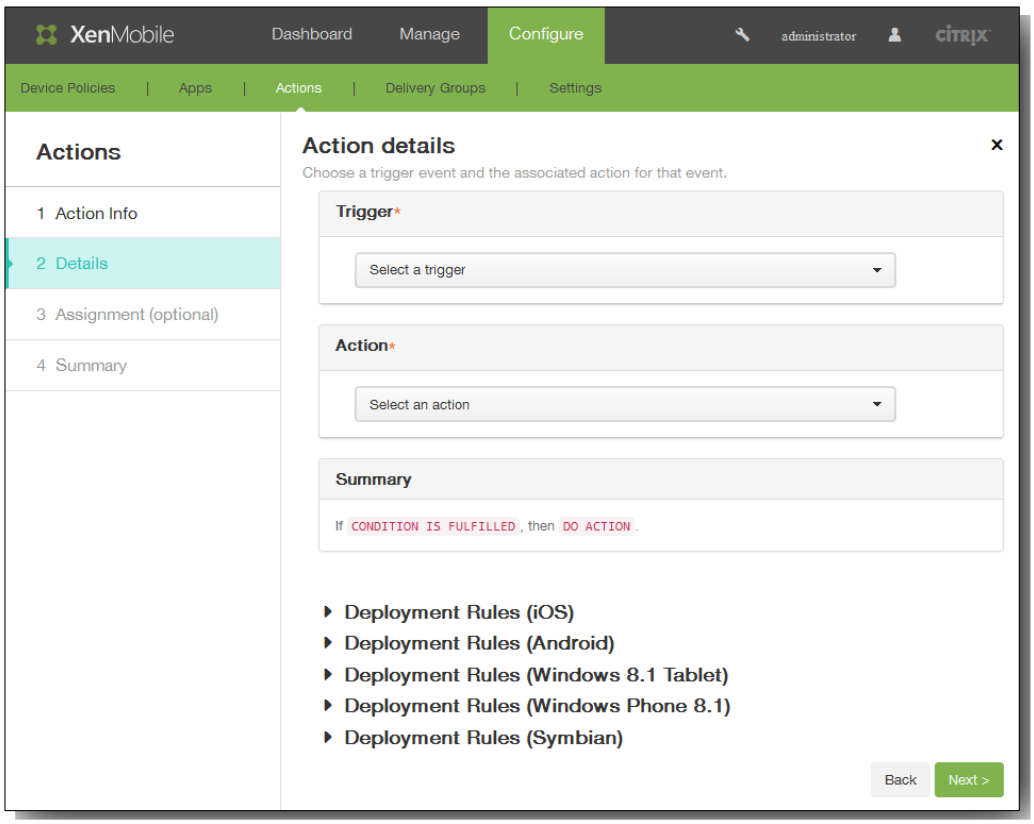




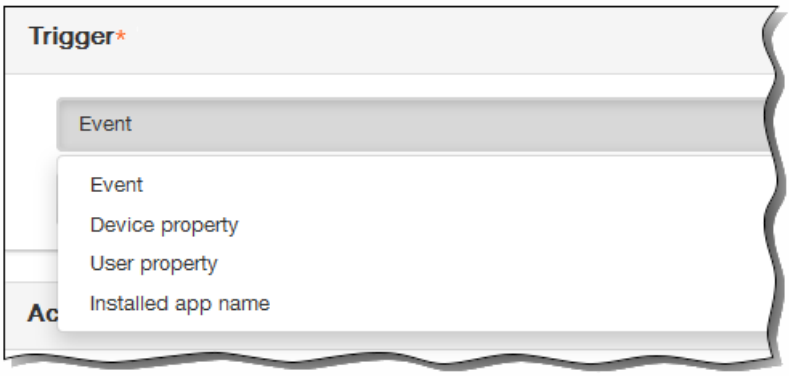
Die Seite Action Information wird angezeigt.



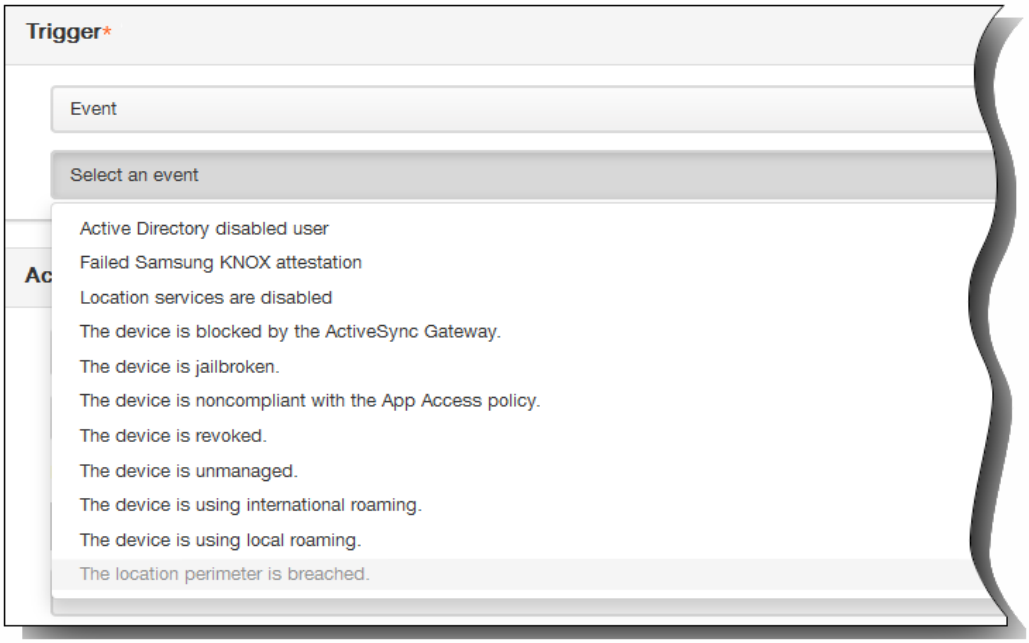
3. Konfigurieren Sie auf der Seite Action Information die folgenden Informationen:
   1. Name: Geben Sie einen Namen zur Identifizierung der Aktion ein. Diese Angabe ist erforderlich.
   2. Beschreibung: Geben Sie eine Beschreibung der Aktion ein.
4. Klicken Sie auf Next. Die Seite Action details wird angezeigt.
   Hinweis: Das folgende Beispiel zeigt, wie ein Ereignisauslöser eingerichtet wird. Wenn Sie einen anderen Auslöser auswählen, werden andere Optionen als die in der Abbildung angezeigt.



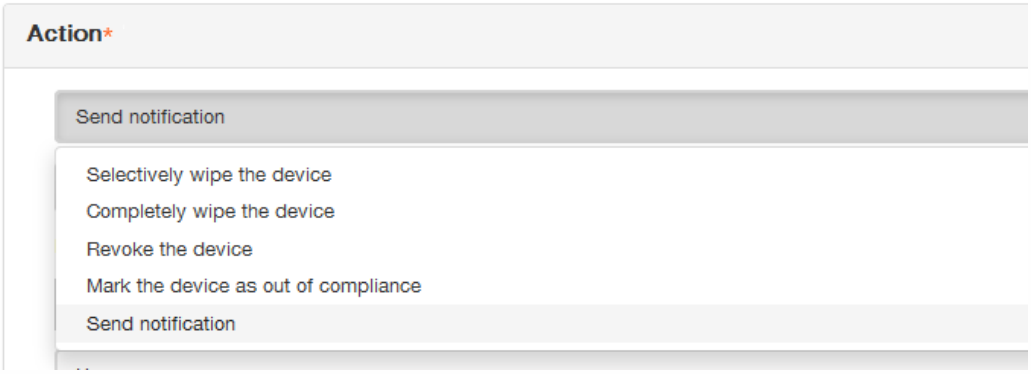
5. Konfigurieren Sie auf der Seite Action details die folgenden Informationen:
   1. Klicken Sie in der Liste Trigger auf den Auslösertyp für die Aktion. Es gibt folgende Auslöser:
      - Event: reagiert auf ein festgelegtes Ereignis.
      - Device property: prüft Geräte im MDM-Modus auf ein Attribut und reagiert entsprechend.
      - User property: reagiert auf ein Benutzerattribut, in der Regel aus Active Directory.
      - Installed app name: reagiert auf die Installation einer App. Hierfür muss die App-Bestandsrichtlinie auf dem Gerät aktiviert sein. Die App-Bestandsrichtlinie ist auf allen Plattformen standardmäßig aktiviert. Weitere Informationen finden Sie unter So fügen Sie eine App-Bestandsrichtlinie für Geräte hinzu.



   2. Klicken Sie in der nächsten Liste auf die Reaktion auf den Auslöser.

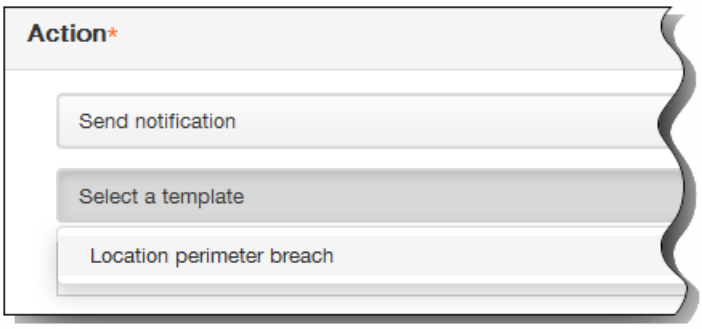


3. Klicken Sie in der Liste Action auf die Aktion, die ausgeführt werden soll, wenn das Auslöserkriterium erfüllt wird. Mit Ausnahme von Send notification können Sie für alle Optionen einen Zeitraum festlegen, in dem Benutzer das für den Auslöser ursächliche Problem beheben können. Wenn das Problem in diesem Zeitraum nicht behoben wird, wird die ausgewählte Aktion durchgeführt.



Bei den restlichen Schritten dieses Verfahrens wird erläutert, wie Sie eine Benachrichtigung senden.

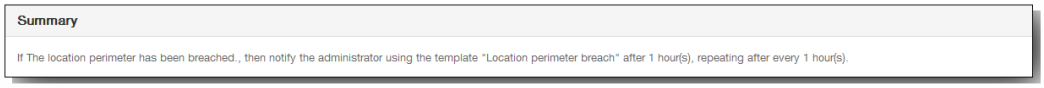
4. Wählen Sie in der nächsten Liste die Vorlage für die Benachrichtigung aus. Für das ausgewählte Ereignis relevante Benachrichtigungsvorlagen werden angezeigt.
   Hinweis: Sie können Benutzer nur benachrichtigen, wenn Sie unter Settings Benachrichtigungsserver für SMTP und SMS konfiguriert haben, damit XenMobile Nachrichten senden kann (siehe Benachrichtigungen in XenMobile). Richten Sie, bevor Sie fortfahren, außerdem alle Benachrichtigungsvorlagen ein, die Sie verwenden möchten. Weitere Informationen über Benachrichtigungsvorlagen finden Sie unter So erstellen oder aktualisieren Sie Benachrichtigungsvorlagen in XenMobile.



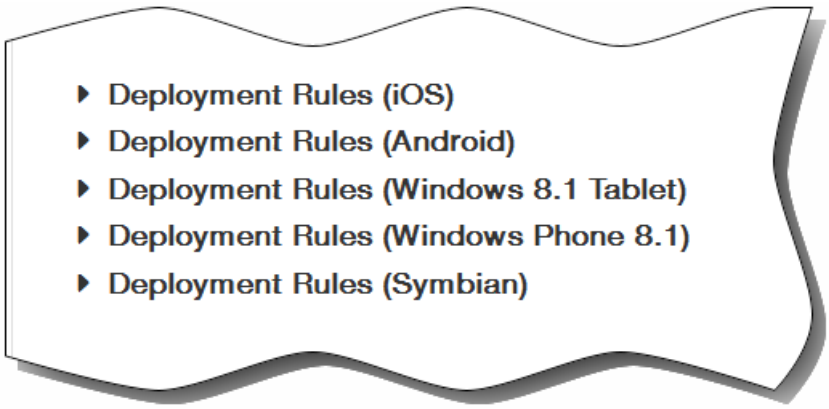
Hinweis: Nach Auswahl der Vorlage können Sie eine Vorschau davon anzeigen indem Sie auf Preview notification message klicken.

5. Geben Sie in den folgenden Feldern die Verzögerung in Tagen, Stunden oder Minuten bis zur Ausführung der Aktion an sowie das Intervall zur Wiederholung der Aktion bis der Benutzer das ursächliche Problem beseitigt.

6. Vergewissern Sie sich unter Summary, dass die automatisierte Aktion wie gewünscht konfiguriert wurde.

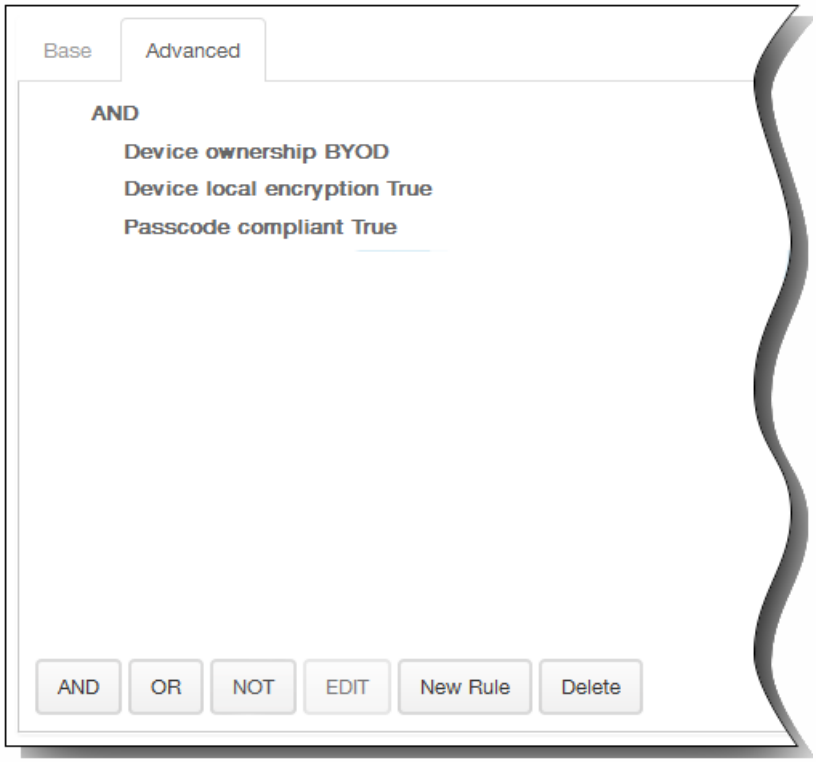


Nach dem Konfigurieren der Aktion können Sie für jede Plattform, d. h. iOS, Android, Windows 8.1 Tablet, Windows Phone 8.1 und Symbian, separat Bereitstellungsregeln festlegen. Führen Sie hierfür die Schritte 6 bis 9 für jede gewünschte Plattform aus.



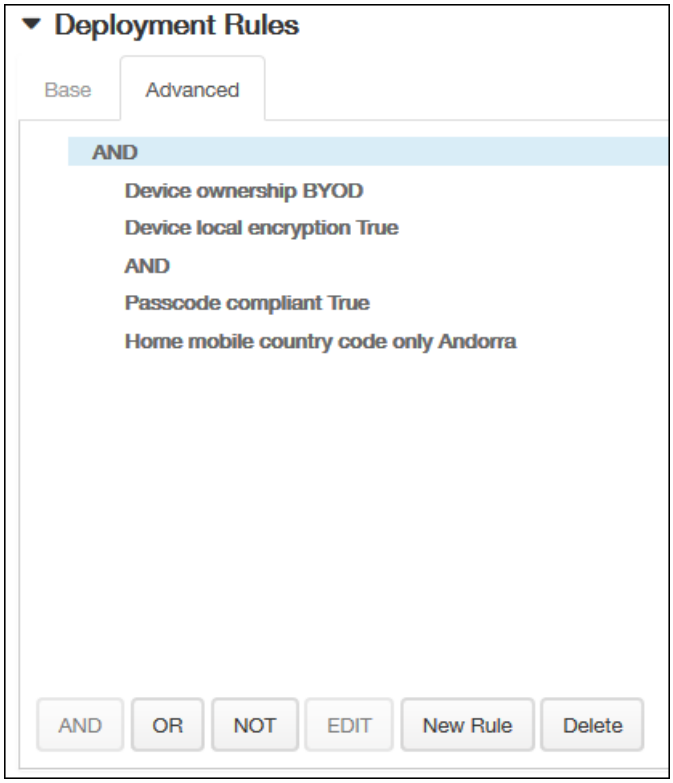
6. Erweitern Sie Deployment Rules. Standardmäßig wird die Registerkarte Base angezeigt.

1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Aktion bereitgestellt werden soll.
    1. Sie können die Aktion bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.

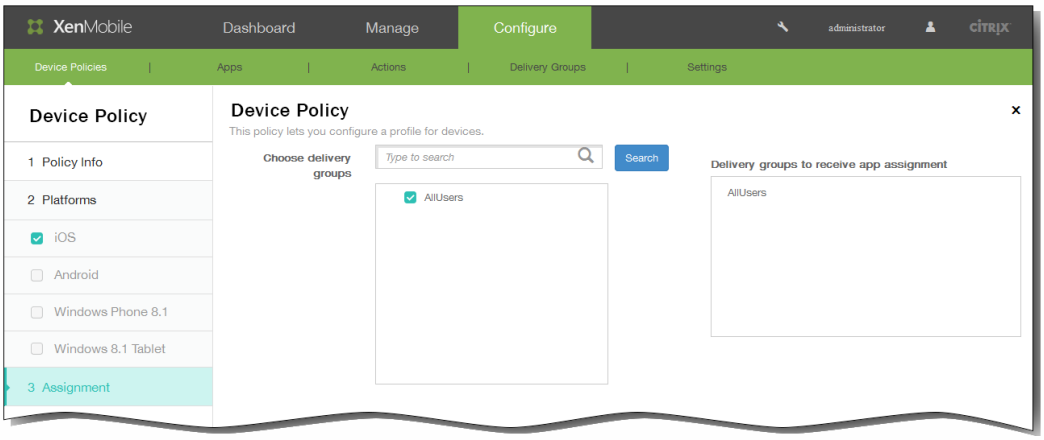


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf der rechten Seite, um die Bedingungen hinzuzufügen.
      Sie können jederzeit auf eine Bedingung und dann auf EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.
   3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
      In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



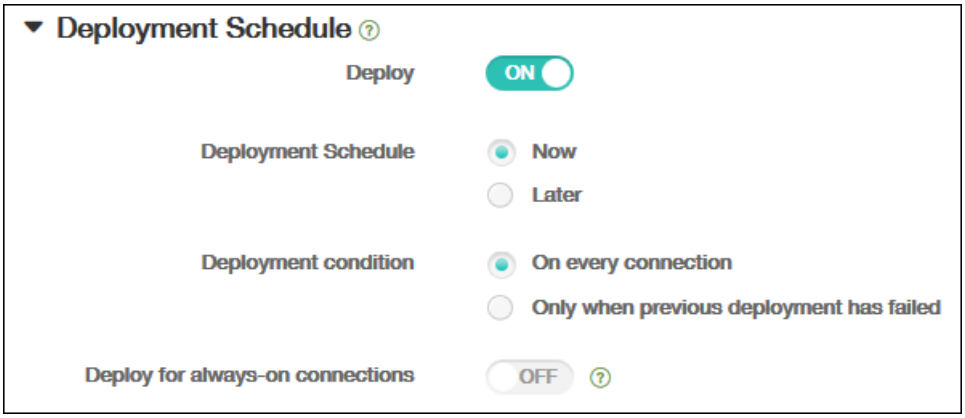
7. Nach dem Konfigurieren der Bereitstellungsregeln für die Aktion klicken Sie auf Next. Die Seite Actions wird angezeigt, auf der Sie die Aktion Bereitstellungsgruppen zuweisen können. Dieser Schritt ist optional.
8. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



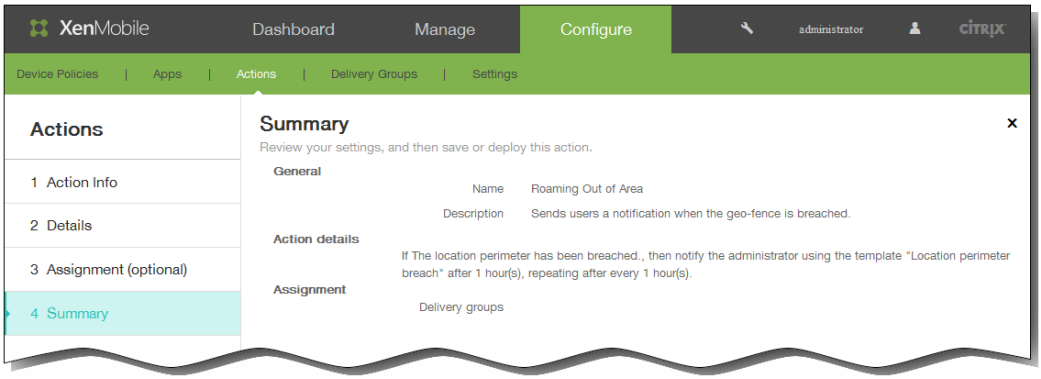
9. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
   1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert werden.
   2. Klicken Sie neben Deployment schedule auf Now oder Later. Die Standardeinstellung ist Now.
   3. Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

4. Klicken Sie neben Deployment condition auf On every connection oder auf Only when previous deployment has failed. Die Standardeinstellung ist On every connection.
5. Klicken Sie neben Deploy for always-on connection auf ON oder OFF. Die Standardeinstellung ist OFF.
   Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "always-on" ist für iOS-Geräte nicht verfügbar.

Hinweis: Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von Deploy for always on connection, denn diese Option gilt nicht für iOS.



10. Klicken Sie auf Next. Die Seite Summary wird angezeigt, auf der Sie die Konfiguration der Aktion prüfen können.



11. Klicken Sie auf Save, um die Aktion zu speichern.

XenMobile-Clienteinstellungen

Apr 12, 2016

Sie können die XenMobile-Clienteinstellungen über die XenMobile-Webkonsole konfigurieren.

1. Klicken Sie in der XenMobile-Konsole auf Configure und dann auf Settings.
   Die Seite Settings wird angezeigt.
2. Klicken Sie auf More.
3. Klicken Sie unter **Client** auf die Option, die Sie konfigurieren möchten.

Referenz der Clienteigenschaften

Jul 27, 2016

Die vordefinierten XenMobile-Clienteigenschaften und deren Standardeinstellungen sind wie folgt:

ENABLE_PASSCODE_AUTH

Anzeigename: Enable Worx PIN Authentication

Über diesen Schlüssel können Sie die Worx-PIN-Funktion aktivieren. Ist die Worx-PIN oder der Worx-Passcode aktiviert, werden die Benutzer aufgefordert, eine PIN zur Verwendung anstelle des Active Directory- Kennworts zu erstellen. Die Einstellung wird automatisch aktiviert, wenn ENABLE_PASSWORD_CACHING aktiviert ist oder wenn XenMobile die Zertifikatauthentifizierung verwendet.

Wenn Benutzer eine Offlineauthentifizierung durchführen, wird die Worx-PIN lokal validiert und die Benutzer können auf die gewünschte App bzw. den gewünschten Inhalt zugreifen. Wenn Benutzer eine Onlineauthentifizierung durchführen, wird mit der Worx-PIN oder dem Worx-Passcode das Active Directory-Kennwort bzw. -Zertifikat entsperrt und zur Authentifizierung bei XenMobile übertragen.

Mögliche Werte: true oder false

Standardwert: false

ENABLE_PASSWORD_CACHING

Anzeigename: Enable User Password Caching

Über diesen Schlüssel können Sie die lokale Zwischenspeicherung des Active Directory-Kennworts auf dem Mobilgerät zulassen. Wenn Sie diesen Schlüssel auf "true" setzen, werden die Benutzer aufgefordert, eine Worx-PIN oder einen Worx-Passcode festzulegen. Der Schlüssel ENABLE_PASSCODE_AUTH muss auf "true" gesetzt werden, wenn Sie diesen Schlüssel auf "true" setzen.

Mögliche Werte: true oder false

Standardwert: false

ENCRYPT_SECRETS_USING_PASSCODE

Anzeigename: Encrypt secrets using Passcode

Mit diesem Schlüssel können vertrauliche Daten auf Mobilgeräten in einem Geheimtresor statt in einem plattformbasierten systemeigenen Speicher (z. B. iOS-Schlüsselbund) gespeichert werden. Der Konfigurationsschlüssel ermöglicht eine starke Verschlüsselung von Schlüsselartefakten und erzeugt zudem Benutzerentropie (eine vom Benutzer generierte zufällige PIN, die nur dem Benutzer bekannt ist).

Citrix empfiehlt, dass Sie diesen Schlüssel aktivieren, um eine höhere Sicherheit auf den Benutzergeräten zu erzielen.

Hinweis: Die Aktivierung des Schlüssels wirkt sich auf die Benutzererfahrung in Form vermehrter Authentifizierungsaufforderungen für die Worx-PIN aus.

Mögliche Werte: true oder false

Standardwert: false

PASSCODE_TYPE

Anzeigename: Worx PIN Type

Dieser Schlüssel definiert, ob Benutzer eine numerische Worx-PIN oder einen alphanumerischen Worx-Passcode festlegen können. Wenn Sie "Numeric" auswählen, können Benutzer nur eine numerische Worx-PIN festlegen. Wenn Sie "Alphanumeric" auswählen, können Benutzer einen Worx-Passcode mit einer Kombination aus Buchstaben und Ziffern festlegen.

Hinweis: Wenn Sie die Einstellung ändern, werden die Benutzer zum Festlegen einer neuen Worx-PIN bzw. eines Passcodes aufgefordert, wenn sie sich das nächste Mal authentifizieren.

Mögliche Werte: Numeric oder Alphanumeric

Standardwert: Numeric

PASSCODE_EXPIRY

Anzeigename: Worx PIN Expiry Requirement

Dieser Schlüssel definiert, wie lange (in Tagen) die Worx-PIN bzw. der Worx-Passcode gültig ist. Nach diesem Zeitraum müssen die Benutzer die Worx-PIN bzw. den Passcode ändern. Wenn Sie diese Einstellung ändern, tritt der neue Wert erst in Kraft, wenn die aktuelle Worx-PIN bzw. der aktuelle Worx-Passcode eines Benutzers abläuft.

Mögliche Werte: 1-99

Standardwert: 90

PASSCODE_HISTORY

Anzeigename: Worx PIN History

Dieser Schlüssel definiert die Zahl der bereits verwendeten Worx-PINs/-Passcodes, die Benutzer beim Ändern nicht wiederverwenden können. Wenn Sie diese Einstellung ändern, tritt der neue Wert erst in Kraft, wenn ein Benutzer seine PIN bzw. seinen Passcode zurücksetzt.

Mögliche Werte: 1-99

Standardwert: 5

PASSCODE_MAX_ATTEMPTS

Anzeigename: Worx PIN Maximum Attempts

Dieser Schlüssel legt fest, wie viele Falscheingaben der Worx-PIN bzw. des Worx-Passcodes zulässig sind, bevor die Benutzer zu einer vollständigen Authentifizierung aufgefordert werden. Nach einer solchen vollständigen Authentifizierung werden die Benutzer aufgefordert, eine neue Worx-PIN bzw. einen neuen Worx-Passcode zu erstellen.

Mögliche Werte: beliebige Ganzzahl

Standardwert: 15

INACTIVITY_TIMER

Anzeigename: Inactivity Timer

Dieser Schlüssel definiert die Zeitdauer (in Minuten), die ein Gerät inaktiv sein darf, bevor Benutzer zur Eingabe von Worx-PIN bzw. -Passcode aufgefordert werden, wenn sie auf eine App zugreifen möchten. Zum Aktivieren dieser Einstellung für eine MDX-App müssen Sie die Einstellung App Passcode auf "Ein" festlegen. Wenn App Passcode auf "Aus" festgelegt ist, werden die Benutzer für eine vollständige Authentifizierung an Worx Home umgeleitet. Wenn Sie diese Einstellung ändern, tritt der neue Wert erst in Kraft, wenn ein Benutzer das nächste Mal zur Authentifizierung aufgefordert wird.

Hinweis: Für iOS steuert "Inactivity Timer" auch den Zugriff auf Worx Home und nicht nur den auf MDX-Apps.

Mögliche Werte: beliebige Ganzzahl

Standardwert: 15

PASSCODE_STRENGTH

Anzeigename: Worx PIN Strength Requirement

Dieser Schlüssel definiert die Sicherheit der Worx-PIN bzw. des Worx-Passcodes. Wenn Sie diese Einstellung ändern, werden die Benutzer zum Festlegen einer neuen Worx-PIN bzw. eines neuen Worx-Passcodes aufgefordert, wenn sie sich das nächste Mal authentifizieren.

Mögliche Werte: Low, Medium oder Strong

Standardwert: Medium

In der folgenden Tabelle werden die Kennwortregeln für die einzelnen Sicherheitseinstellungen nach der unter PASSCODE_TYPE ausgewählten Einstellung aufgeführt:

Passcodesicherheit	**Numerischer Passcode**	**Alphanumerischer Passcode**
Niedrig	Alle Ziffern, beliebige Reihenfolge zugelassen	Muss mindestens eine Ziffer und einen Buchstaben enthalten. **Nicht zulässig**: AAAaaa, aaaaaa, abcdef **Zulässig**: aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa
Mittel (Standardeinstellung)	1. Die Ziffern dürfen nicht alle gleich sein. Beispiel: 444444 ist nicht zulässig. 2. Es dürfen keine aufeinander folgenden Ziffern verwendet werden. Beispiel: 123456 oder 654321 ist nicht zulässig. **Zulässig:** 444333, 124567, 136790,	Zusätzlich zu den Regeln für die Passcodesicherheit "Low" gilt: 1. Buchstaben und Ziffern dürfen nicht alle gleich sein. Beispiel: aaaa11, aa11aa oder aaa111 sind nicht zulässig. 2. Es dürfen keine aufeinanderfolgenden Buchstaben und Ziffern verwendet werden.

	555556, 788888	Beispiel: abcd12, bcd123, 123abc, xy1234, xyz345 oder cba123 sind nicht zulässig. **Zulässig**: aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~
Strong	Wie Einstellung "Medium" für Worx-PIN	Der Passcode muss mindestens eine Ziffer, ein Sonderzeichen, einen Großbuchstaben und einen Kleinbuchstaben enthalten. **Nicht zulässig**: abcd12, Abcd12, dfgh12, jkrtA2 **Zulässig**: Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#

ENABLE_CRASH_REPORTING

Anzeigename: Enable Crash reporting

Mit diesem Schlüssel werden Absturzberichte für Worx-Apps mit Crashlytics aktiviert.

Mögliche Werte: true oder false

Standardwert: true

DISABLE_LOGGING

Anzeigename: Disable logging

Über diesen Schlüssel können Sie verhindern, dass Benutzer auf ihren Geräten Protokolle erstellen und hochladen. Die Protokollierung wird für Worx Home und alle installierten MDX-Apps deaktiviert. Die Benutzer können für keine App von der Supportseite Protokolle senden, obwohl das Dialogfeld zum Schreiben einer E-Mail angezeigt wird. Die Protokolle werden nicht angehängt, es wird jedoch eine Meldung angezeigt, dass die Protokollierung deaktiviert ist. Darüber hinaus können Sie Protokolleinstellungen für Worx Home und MDX-Apps, die Auswirkungen auf die Benutzergeräte haben, nicht in der XenMobile-Konsole ändern.

Wenn Sie diesen Schlüssel auf "true" festlegen, wird in Worx Home "Block application logs" auf "true" festgelegt, sodass die Protokollierung in MDX-Apps bei Anwenden der Richtlinie beendet wird.

Mögliche Werte: true oder false

Standardwert: false (Protokollierung nicht deaktiviert)

So erstellen Sie angepasstes Worx Store-Branding für iOS-Geräte

Jul 27, 2016

Sie können festlegen, wie Apps im WorxStore angezeigt werden, und Worx Home und dem WorxStore für mobile iOS- und Android-Geräte ein Logo hinzufügen.

Hinweis: Stellen Sie zu Beginn des Arbeitsgangs sicher, dass das benutzerdefinierte Bild bereitsteht.

- Die Datei muss im PNG-Format vorliegen.
- Verwenden Sie ein rein weißes Logo oder Text mit einem transparenten Hintergrund (72 dpi).
- Das Unternehmenslogo darf folgende Maße nicht überschreiten: 170 px x 25 px (1x) + 340 px x 50 px (2x).
- Benennen Sie die Datei Header.png und Header@2x.png.
- Erstellen Sie eine ZIP-Datei aus den Dateien direkt, nicht aus einem Ordner mit den Dateien.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > Worx Store Branding.
2. Wählen Sie neben Default store view die Option Category oder A-Z aus.
3. Wählen Sie neben Device option die Option Phone oder Tablet aus.
4. Klicken Sie neben Branding file auf Browse, um ein Bild bzw. eine ZIP-Datei mit Bildern für das Branding zu auszuwählen, und klicken Sie dann auf Save.

Zum Bereitstellen dieses Pakets auf den Geräten müssen Sie ein Bereitstellungspaket erstellen und bereitstellen.

So erstellen Sie Supportoptionen für Worx Home und GoToAssist

Nov 12, 2015

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > Worx Home Support.
2. Geben Sie auf der Seite Worx Home Support einen Wert in folgende Felder ein:
    1. Support email (IT help desk)
    2. Support phone (IT help desk)
    3. Token for GoToAssist chat
    4. GoToAssist support ticket email

Die Informationen für den Worx Home-Support werden in der Liste Client Properties in der XenMobile-Konsole mit der Zuweisung zu folgenden Schlüsseln angezeigt: SUPPORT_EMAIL, SUPPORT_PHONE, GTA_CHAT und GTA_TICKET.

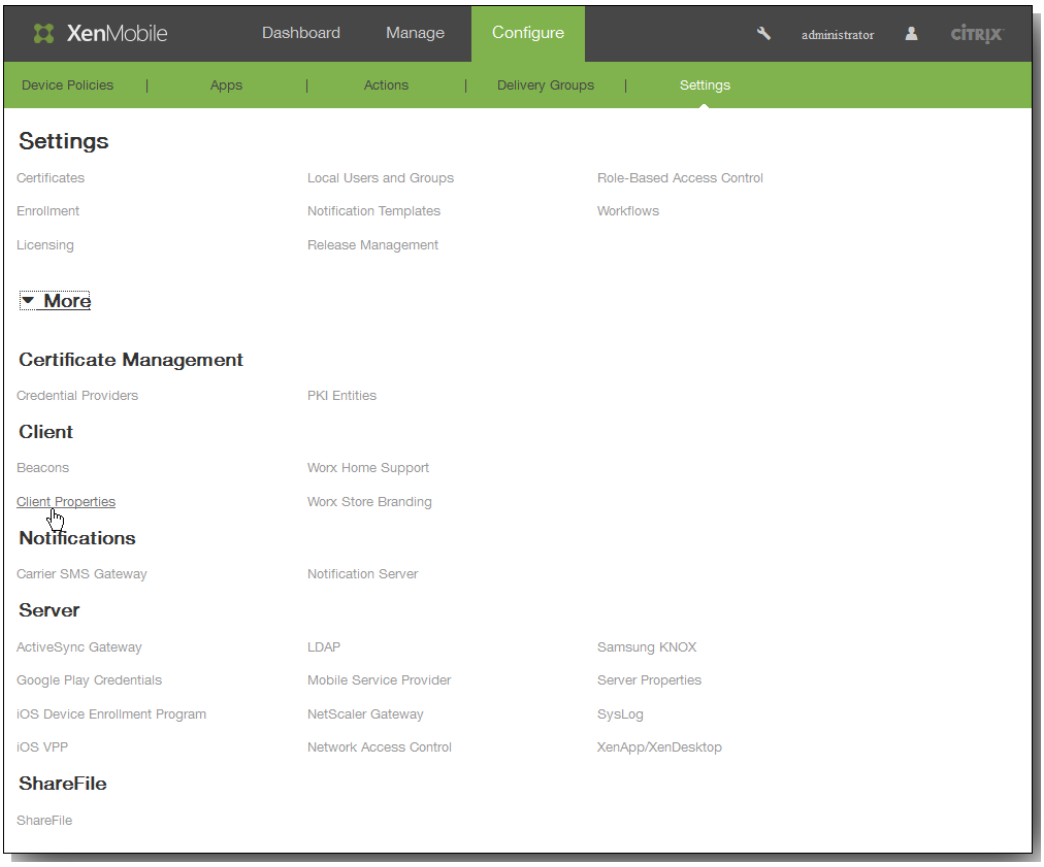
So erstellen, bearbeiten oder löschen Sie Clienteigenschaften

Nov 12, 2015

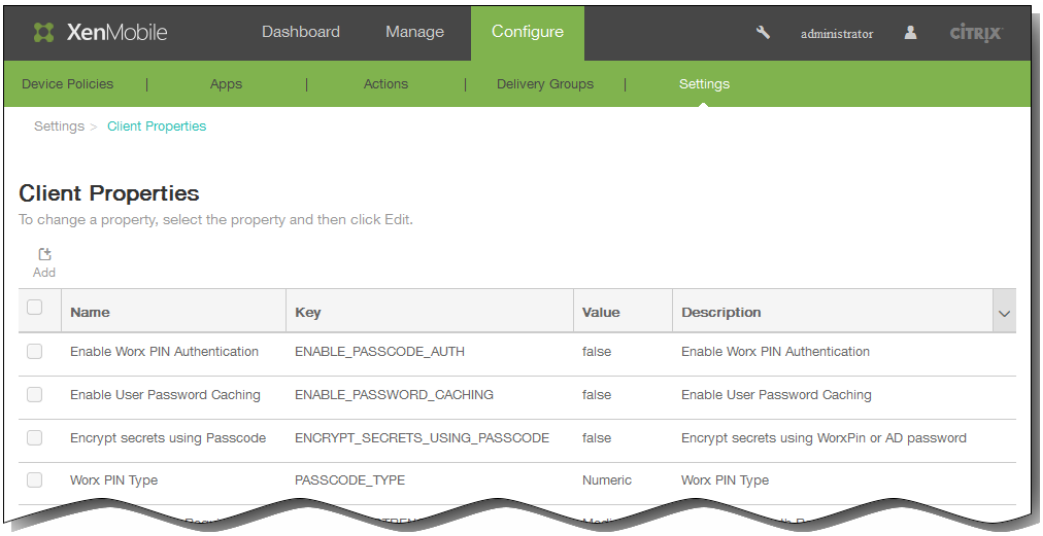
Clienteigenschaften enthalten Informationen, die direkt in Worx Home auf den Geräten der Benutzer bereitgestellt werden. Diese Eigenschaften werden zum Konfigurieren erweiterter Einstellungen, z. B. der Worx-PIN, verwendet. Clienteigenschaften sind beim Citrix Support erhältlich.

Hinweis: Clienteigenschaften können sich bei jedem neuen Release von Client-Apps, insbesondere Worx Home, ändern.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings> More > Client Properties.

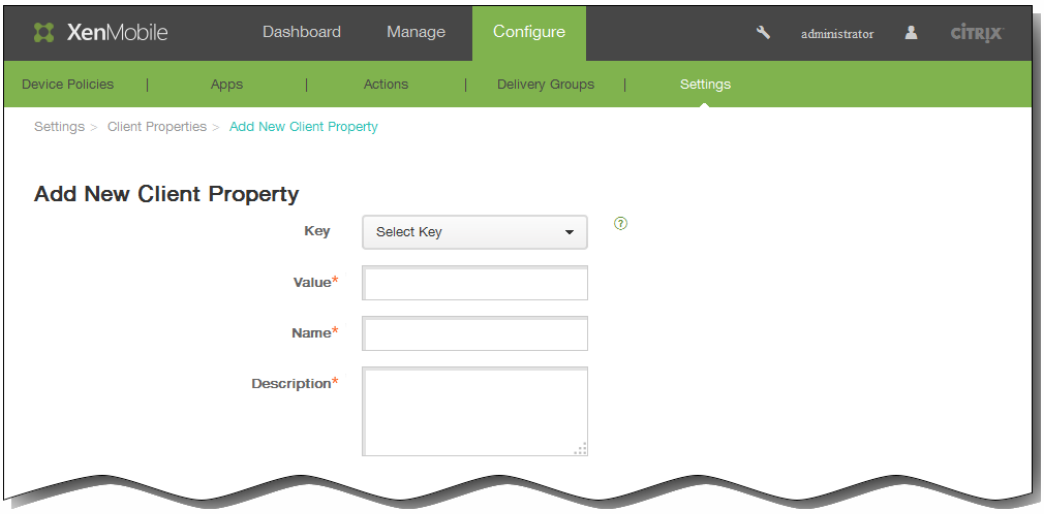


Die Seite Client Properties wird angezeigt. Auf dieser Seite können Sie die Clienteigenschaften hinzufügen, bearbeiten und löschen.



So fügen Sie eine Clienteigenschaft hinzu

1. Klicken Sie auf der Seite Client Properties auf Add. Die Seite Add New Client Property wird angezeigt.

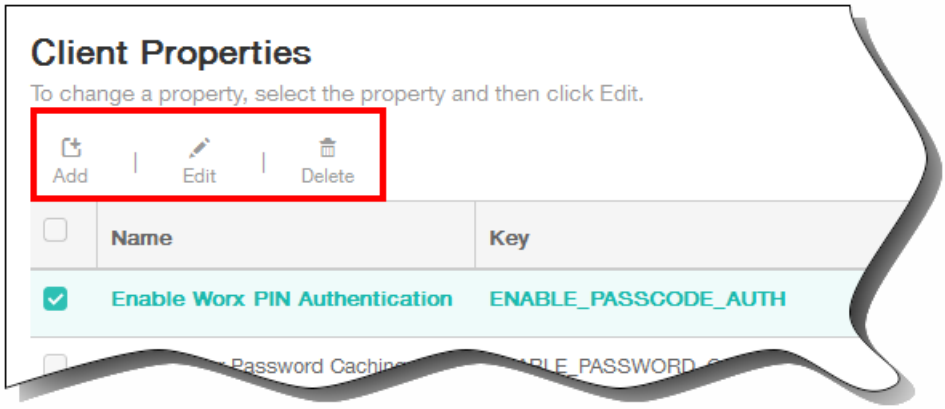


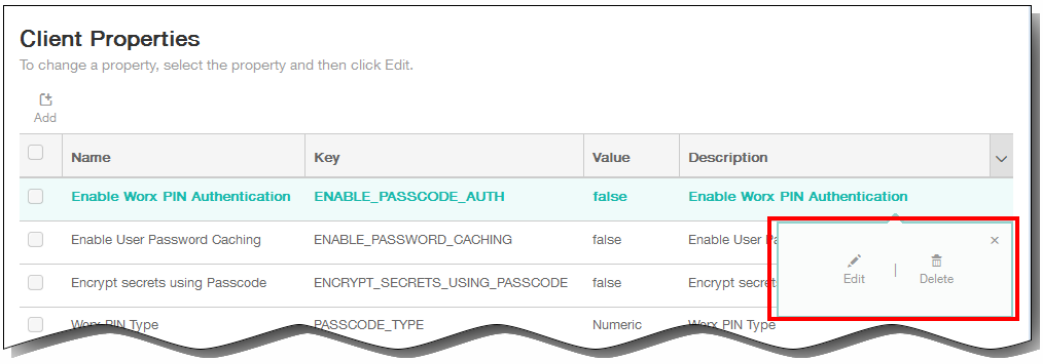
2. Geben Sie auf der Seite Add New Client Property die folgenden Informationen ein:
   Hinweis: Alle Felder müssen ausgefüllt werden.
   1. Key: Klicken Sie in der Liste auf den Eigenschaftsschlüssel, den Sie hinzufügen möchten.
      Wichtig: Wenden Sie sich an den Citrix Support, bevor Sie Änderungen vornehmen, oder fordern Sie einen speziellen Schlüssel an, um eine Änderung auszuführen.
   2. Value: Geben Sie den Wert der ausgewählten Eigenschaft ein.
   3. Name: Geben Sie einen Namen für die Eigenschaft ein.
   4. Description: Geben Sie eine Beschreibung für die Eigenschaft ein.

So bearbeiten Sie eine Clienteigenschaft

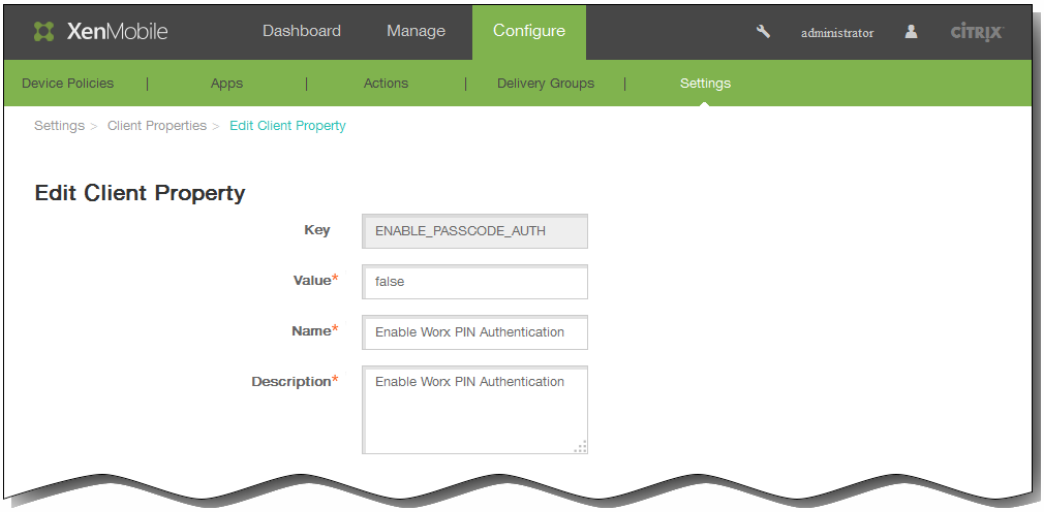
1. Wählen Sie in der Tabelle Client Properties die gewünschte Clienteigenschaft aus.
   Hinweis: Wenn Sie das Kontrollkästchen neben einer Clienteigenschaft auswählen, wird das Menü mit den Optionen oberhalb der Liste der Clienteigenschaften eingeblendet. Wenn Sie auf eine andere Stelle im Eintrag klicken, wird es

rechts neben dem Eintrag eingeblendet.





2. Klicken Sie auf Edit. Die Seite Edit Client Property wird angezeigt.



3. Ändern Sie nach Bedarf die folgenden Informationen:
   1. Value: Wert der ausgewählten Eigenschaft.
   2. Name: Name der Eigenschaft.

3. Description: Beschreibung der Eigenschaft.
4. Klicken Sie auf Save, um die Änderungen zu speichern oder auf Cancel, um die Clienteigenschaft unverändert zu lassen.

So löschen Sie eine Clienteigenschaft

1. Wählen Sie in der Tabelle Client Properties die gewünschte Clienteigenschaft aus.
   Hinweis: Sie können mehrere Eigenschaften auswählen, indem Sie die Kontrollkästchen daneben aktivieren.
2. Klicken Sie auf Delete. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie noch einmal auf Delete.

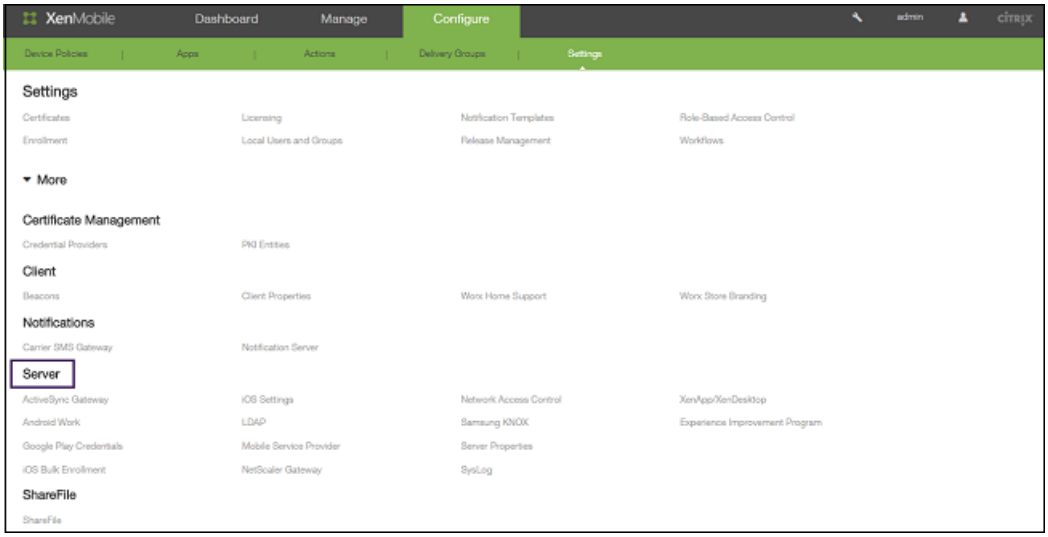
XenMobile-Servereinstellungen

Apr 12, 2016

In der XenMobile-Konsole werden folgende XenMobile-Servereinstellungen konfiguriert:

- ActiveSync Gateway
- Android for Work
- Google Play-Anmeldeinformationen
- iOS-Massenregistrierung
- iOS-Einstellungen
- LDAP
- Mobilfunkanbieter
- NetScaler Gateway
- Network Access Control
- Samsung KNOX
- Servereigenschaften
- SysLog
- XenApp/XenDesktop
- Programm zur Verbesserung der Benutzerfreundlichkeit

1. Klicken Sie in der XenMobile-Konsole auf Configure und dann auf Settings.
   Die Seite Settings wird angezeigt.



2. Klicken Sie auf More.
3. Klicken Sie unter **Server** auf die Option, die Sie konfigurieren möchten.

ActiveSync Gateway in XenMobile

Apr 12, 2016

ActiveSync ist ein Protokoll zur Synchronisierung mobiler Daten von Microsoft. ActiveSync synchronisiert Daten auf Handheld-Geräten und PC bzw. Laptops. Sie können ActiveSync Gateway-Regeln in XenMobile konfigurieren. Basierend auf diesen Regeln kann Geräten der Zugriff auf ActiveSync-Daten bewilligt oder verweigert werden. Wenn Sie beispielsweise die Regel "Missing Required Apps" aktivieren, prüft XenMobile per App-Zugriffsrichtlinie auf erforderliche Apps und verweigert den Zugriff auf ActiveSync-Daten, wenn die erforderlichen Apps fehlen.

XenMobile unterstützt die folgenden Regeln:

Anonymous Devices: Prüft, ob ein Gerät im anonymen Modus ist. Diese Prüfung ist verfügbar, wenn XenMobile bei einer Wiederverbindung den Benutzer des Geräts nicht erneut authentifizieren kann.

Failed Samsung KNOX attestation: Prüft, ob bei einem Gerät die Abfrage des Samsung KNOX-Nachweisservers fehlgeschlagen ist.

Forbidden Apps: Prüft, ob ein Gerät unzulässige Apps aufweist, die in einer App-Zugriffsrichtlinie definiert sind.

Implicit Allow and Deny: Dies ist die Standardaktion für das ActiveSync Gateway, das eine Liste aller Geräte erstellt, die keine der anderen Filterkriterien erfüllen. Verbindungen werden dann aufgrund dieser Liste zugelassen oder verweigert. Wenn keine Regel zutrifft, ist die Standardaktion "Implicit Allow".

Inactive Devices: Prüft, ob ein Gerät entsprechend dem unter "Inactivity Days Threshold" in den Servereigenschaften festgelegten Wert inaktiv ist.

Missing Required Apps: Prüft, ob auf einem Gerät Apps fehlen, die in einer App-Zugriffsrichtlinie definiert sind.

Non-suggested Apps: Prüft, ob ein Gerät nicht empfohlene Apps aufweist, die in einer App-Zugriffsrichtlinie definiert sind.

Noncompliant Password: Prüft, ob das Benutzerkennwort richtlinientreu ist. Auf iOS- und Android-Geräten kann XenMobile feststellen, ob das aktuelle Kennwort des Geräts die an das Gerät gesendete Kennwortrichtlinie erfüllt. Auf iOS-Geräten haben Benutzer beispielsweise 60 Minuten, um ein Kennwort festzulegen, wenn XenMobile eine Kennwortrichtlinie an das Gerät sendet. Bevor der Benutzer das Kennwort festlegt, ist das Kennwort u. U. nicht richtlinientreu.

Out of Compliance Devices: Prüft anhand der Eigenschaft für nicht richtlinientreue Geräte, ob ein Gerät richtlinientreu ist. Diese Eigenschaft wird normalerweise von automatisierten Aktionen geändert oder von einem Dritten durch Verwenden von XenMobile-APIs.

Revoked Status: Prüft, ob das Gerätezertifikat widerrufen worden ist. Ein widerrufenes Gerät kann erst erneut registriert werden, wenn es wieder autorisiert ist.

Rooted Android and Jailbroken iOS Devices: Prüft, ob auf einem Android- oder iOS-Gerät ein Jailbreak vorliegt.

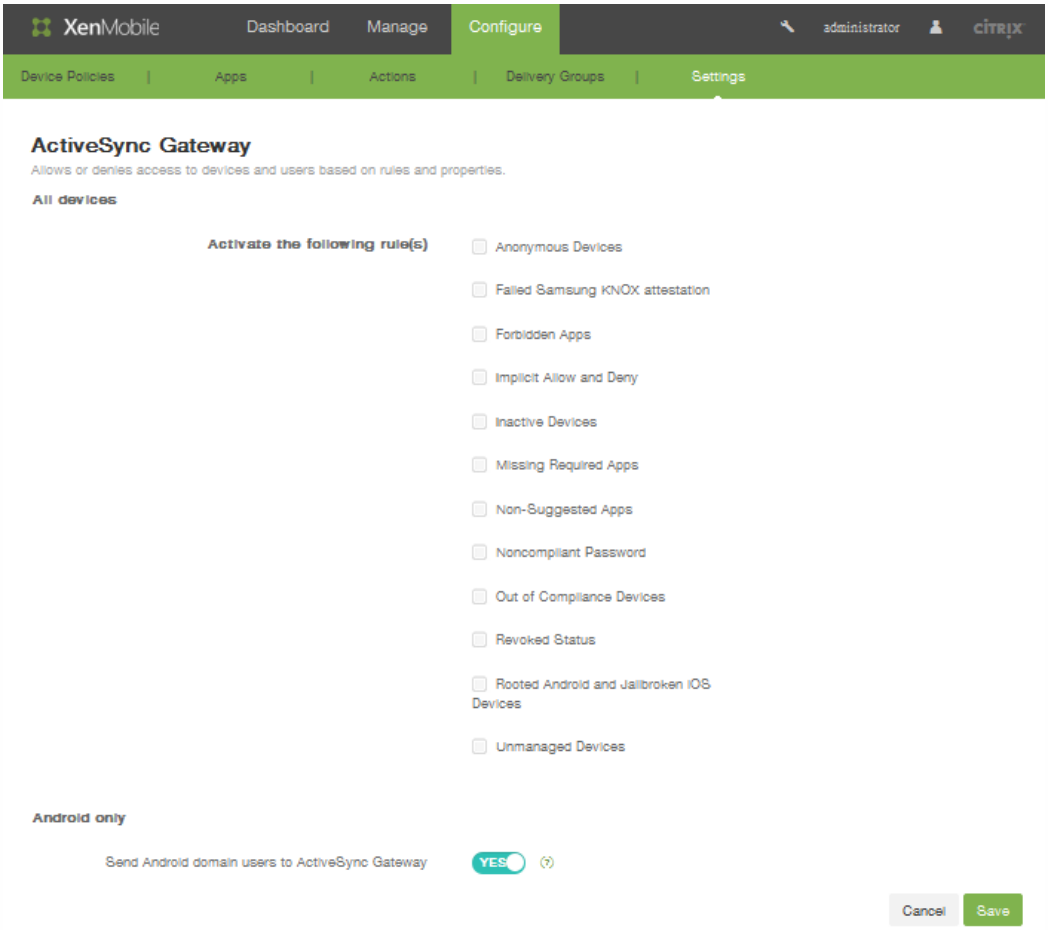
Unmanaged Devices: Prüft, ob ein Gerät verwaltet, d. h. von XenMobile kontrolliert wird. Beispielsweise ist ein Gerät im MAM-Modus oder ein nicht registriertes Gerät nicht verwaltet.

Send Android domain users to ActiveSync Gateway: Klicken Sie auf **YES**, damit XenMobile Android-Geräteinformationen an das ActiveSync Gateway sendet. Durch Aktivieren dieser Option wird sichergestellt, dass XenMobile Android-Geräteinformationen an das ActiveSync Gateway für den Fall sendet, dass XenMobile den ActiveSync-Bezeichner

für den Android-Gerätebenutzer nicht hat.

So konfigurieren Sie ein ActiveSync-Gateway in XenMobile

1. Klicken Sie in der XenMobile-Konsole auf **Configure > Settings > More > ActiveSync Gateway**. Die Seite **ActiveSync Gateway** wird angezeigt.



2. Wählen Sie unter **Activate the following rules** eine oder mehrere Regeln aus, die Sie aktivieren möchten.
3. Klicken Sie für **Android-only** unter **Send Android domain users to ActiveSync Gateway** auf **YES**, um sicherzustellen, dass XenMobile Android-Geräteinformationen an das Secure Mobile Gateway sendet.
4. Klicken Sie auf **Save**.

Google Play-Anmeldeinformationen

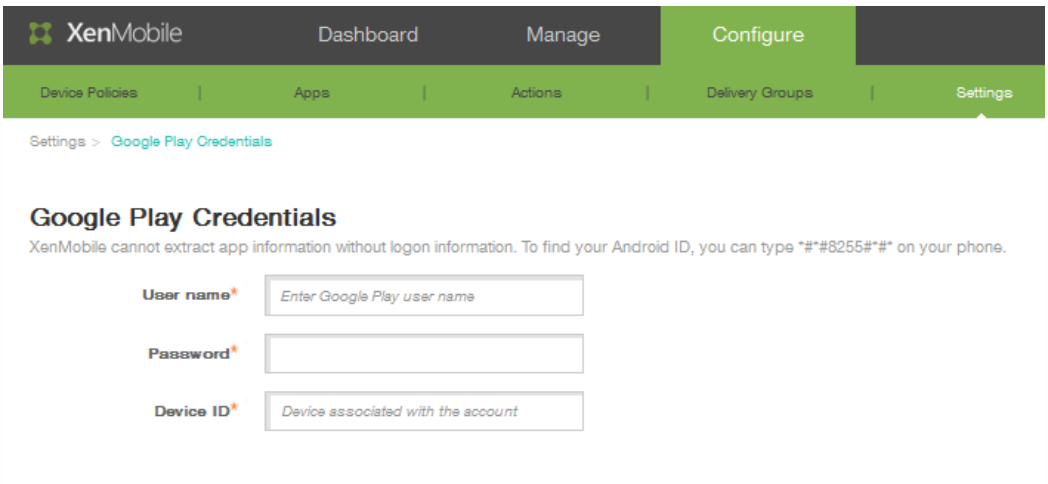
Apr 12, 2016

XenMobile verwendet Google Play-Anmeldeinformationen zum Extrahieren von App-Informationen für Geräte.

Hinweis: Zum Ermitteln der Android-ID geben Sie auf ihrem Telefon *#*#8255#*#* ein.
Wichtig: Damit XenMobile App-Informationen extrahieren kann, müssen Sie möglicherweise Ihr Gmail-Konto zum Zulassen unsicherer Verbindungen konfigurieren. Anweisungen hierzu finden Sie auf der Google-Supportsite.

So konfigurieren Sie XenMobile zur Verwendung von Google Play-Anmeldeinformationen

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > Google Play Credentials.
   Die Seite Google Play Credentials wird angezeigt.



2. Geben Sie in das Feld User name den Namen des Google Play-Kontos ein.
3. Geben Sie in das Feld Password das Kennwort des Benutzers ein.
4. Geben Sie in das Feld Device ID Ihre Android-ID ein.
   Zum Ermitteln der Android-ID geben Sie auf ihrem Telefon *#*#8255#*#* ein.
5. Klicken Sie auf Speichern.

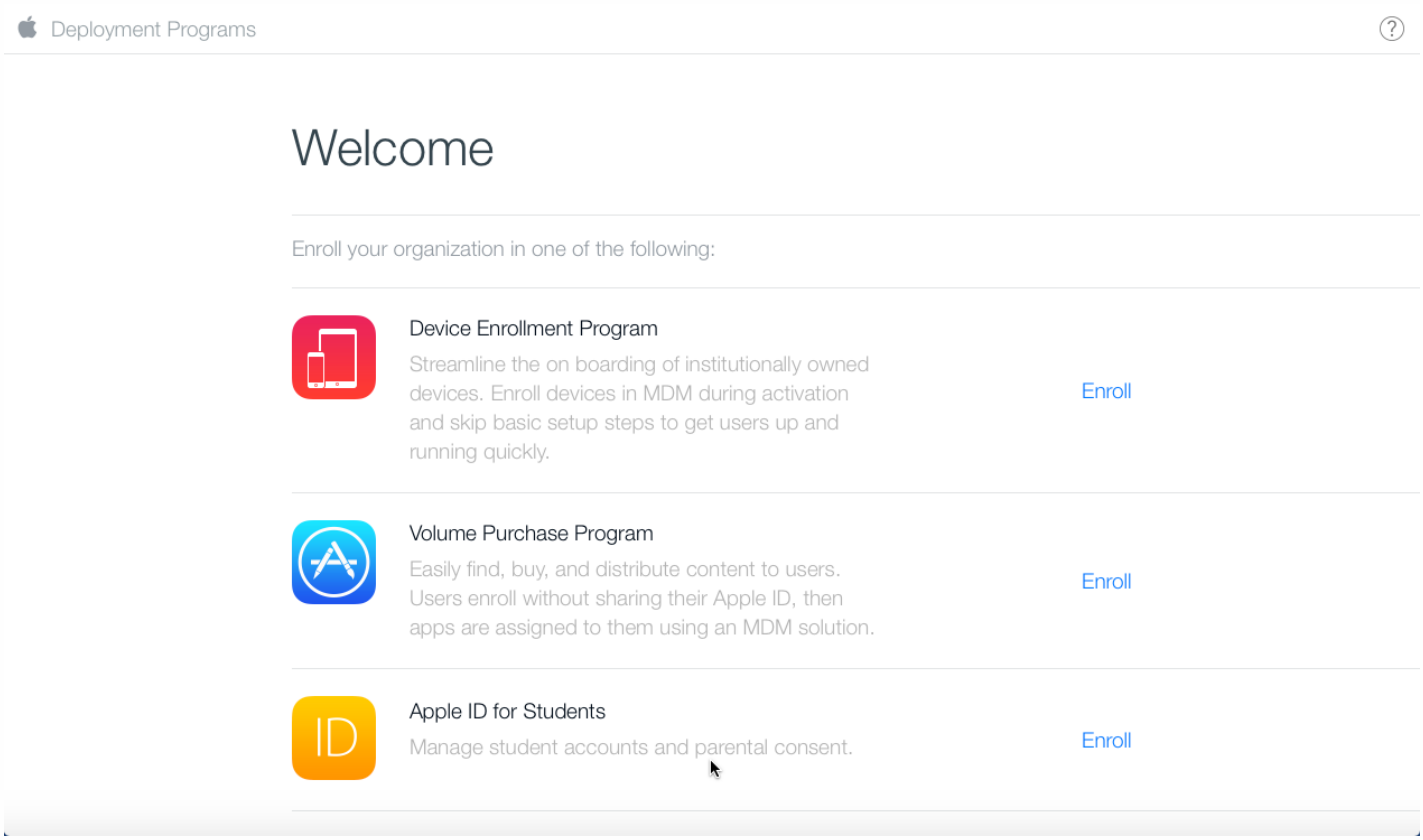
Registrierungsprogramm für iOS-Geräte

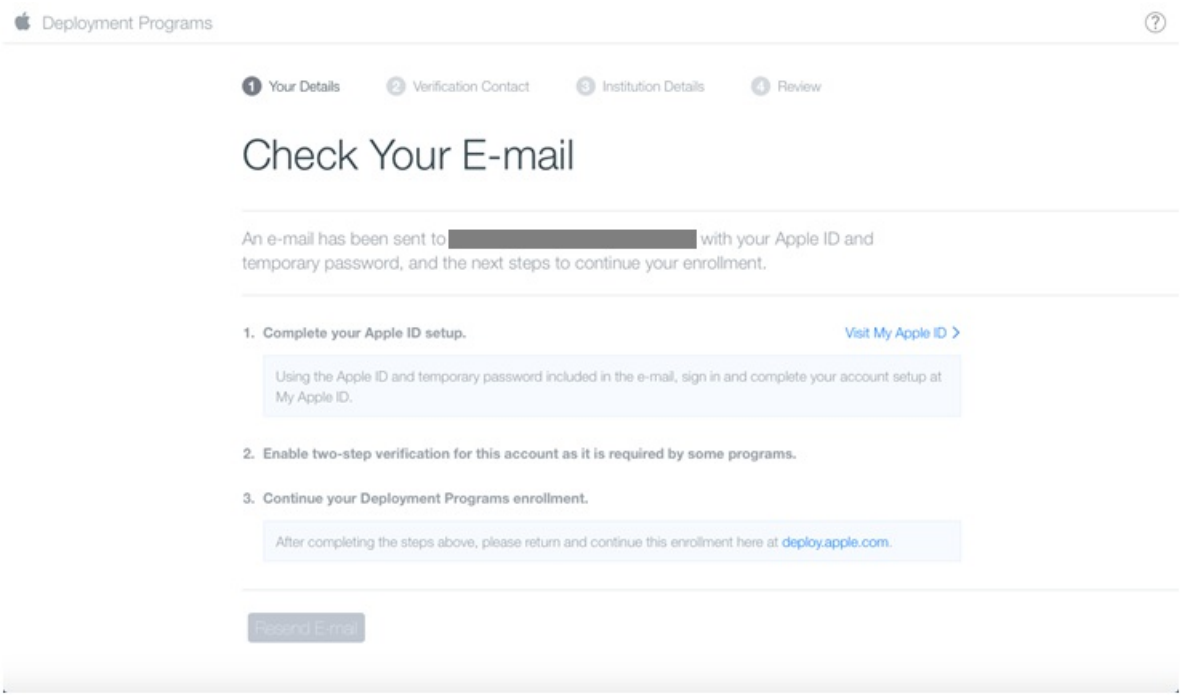
-
-

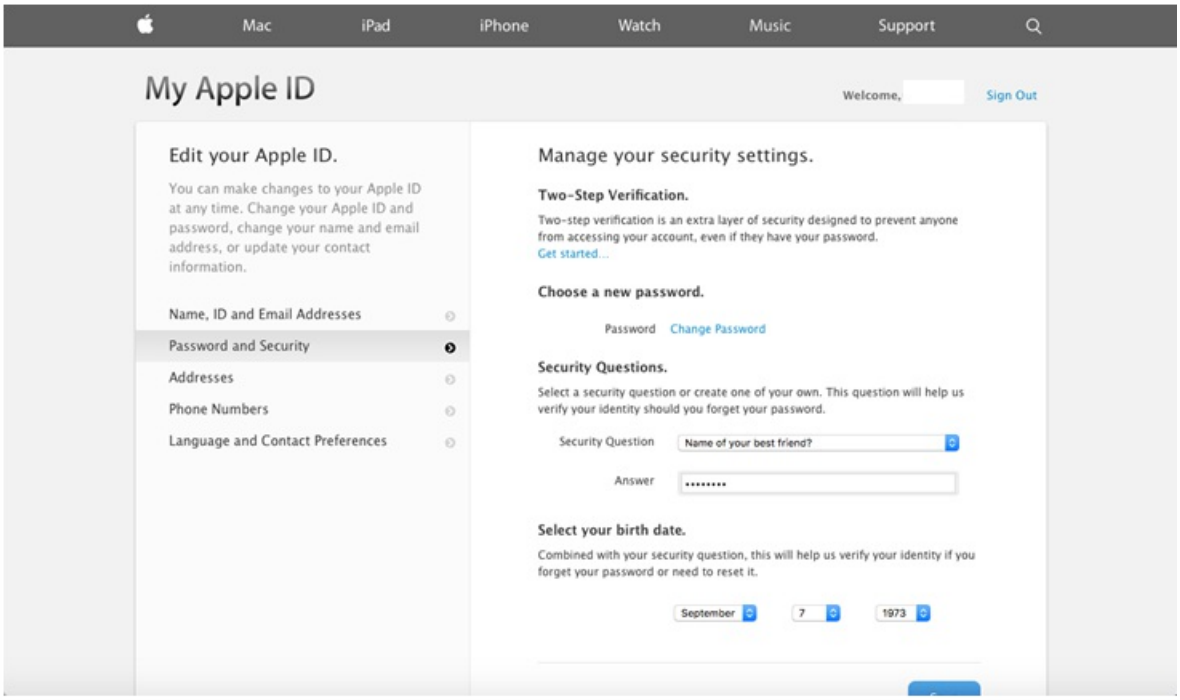
Bereitstellen von iOS-Geräten mit Apple DEP

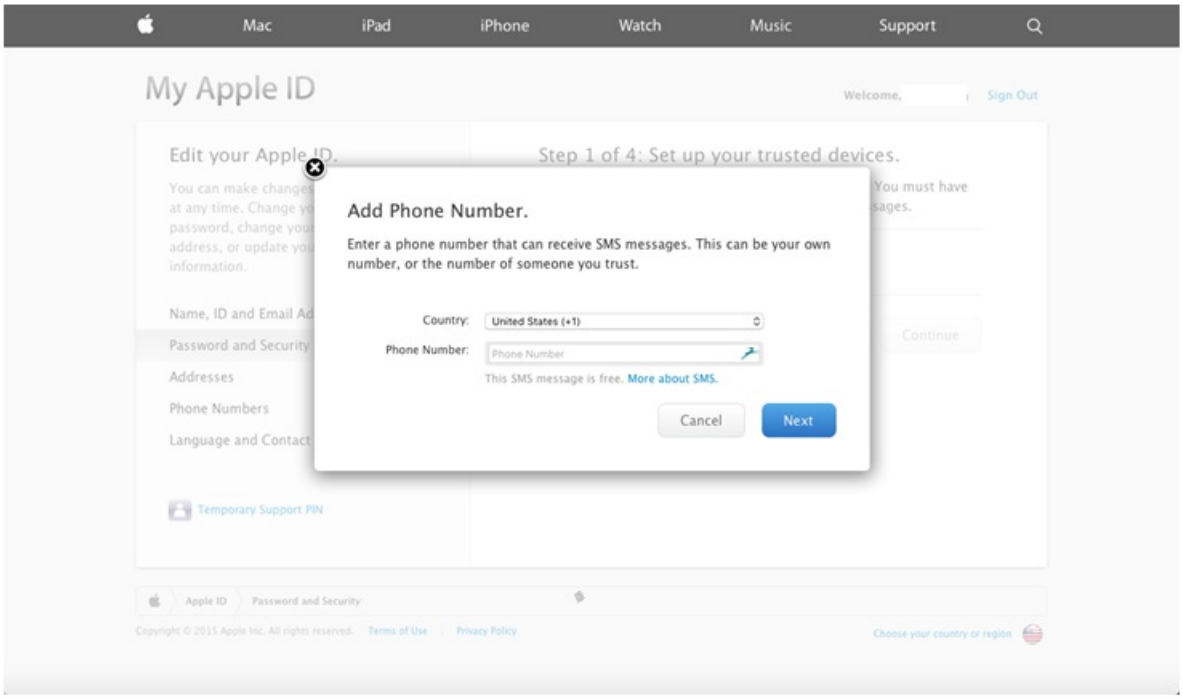
-
-
-
-

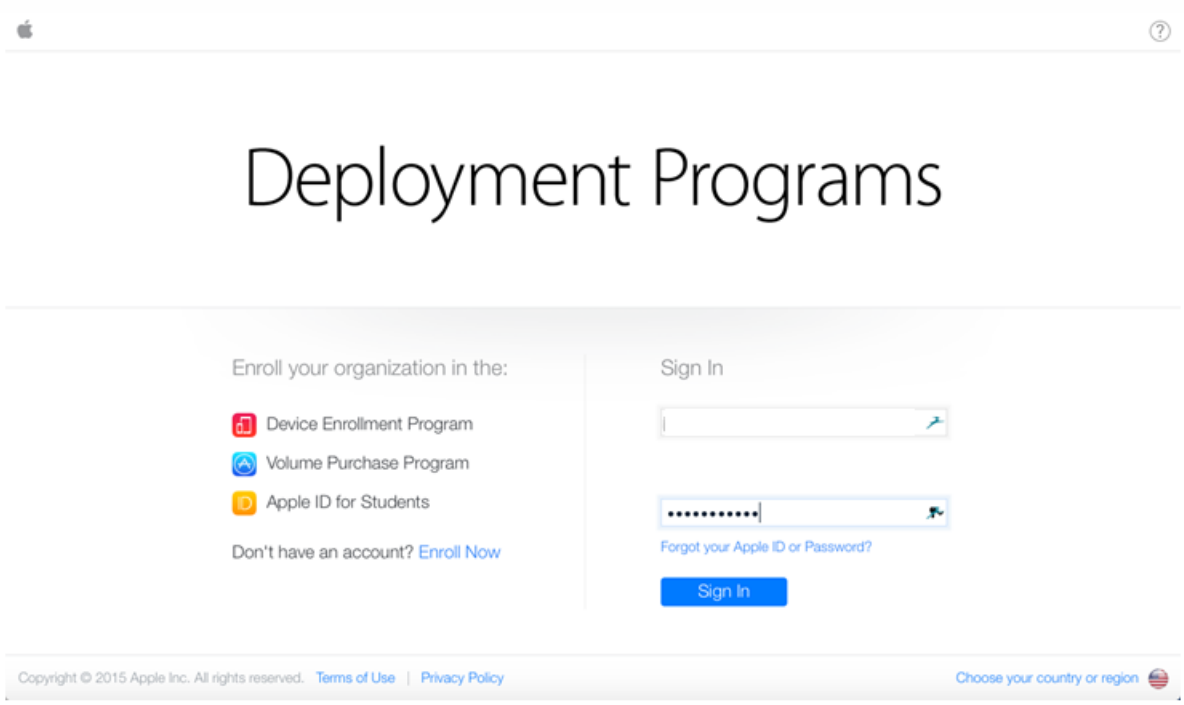
Beantragen eines Apple DEP-Kontos

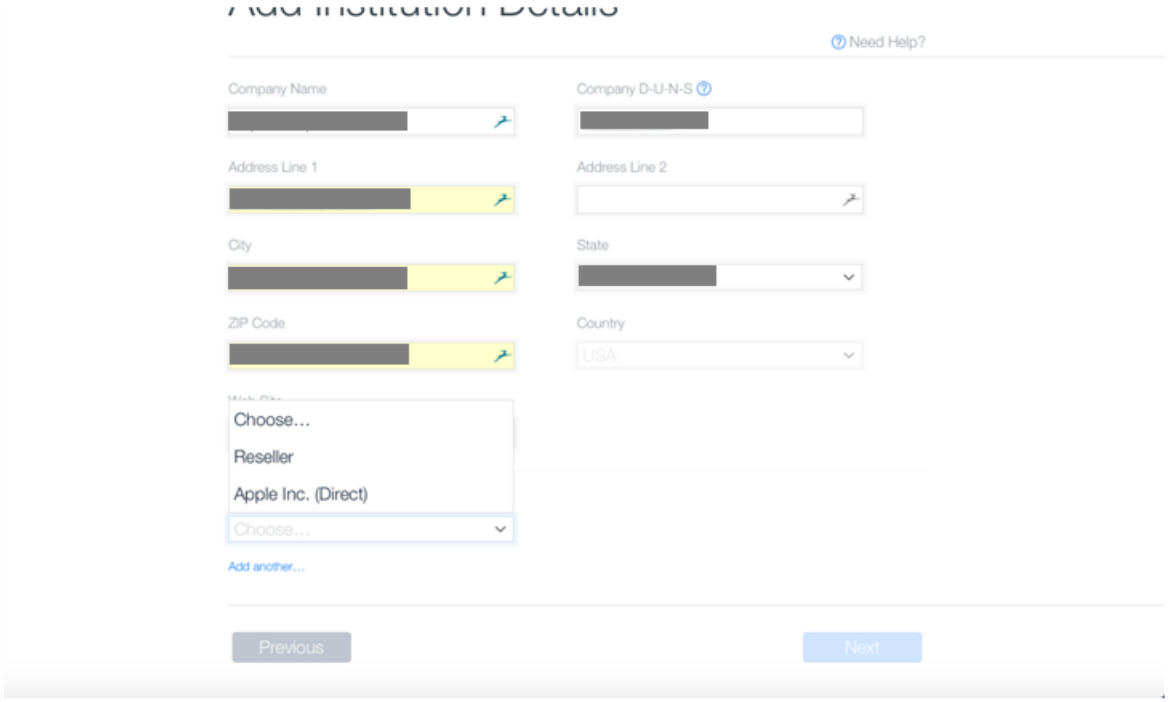


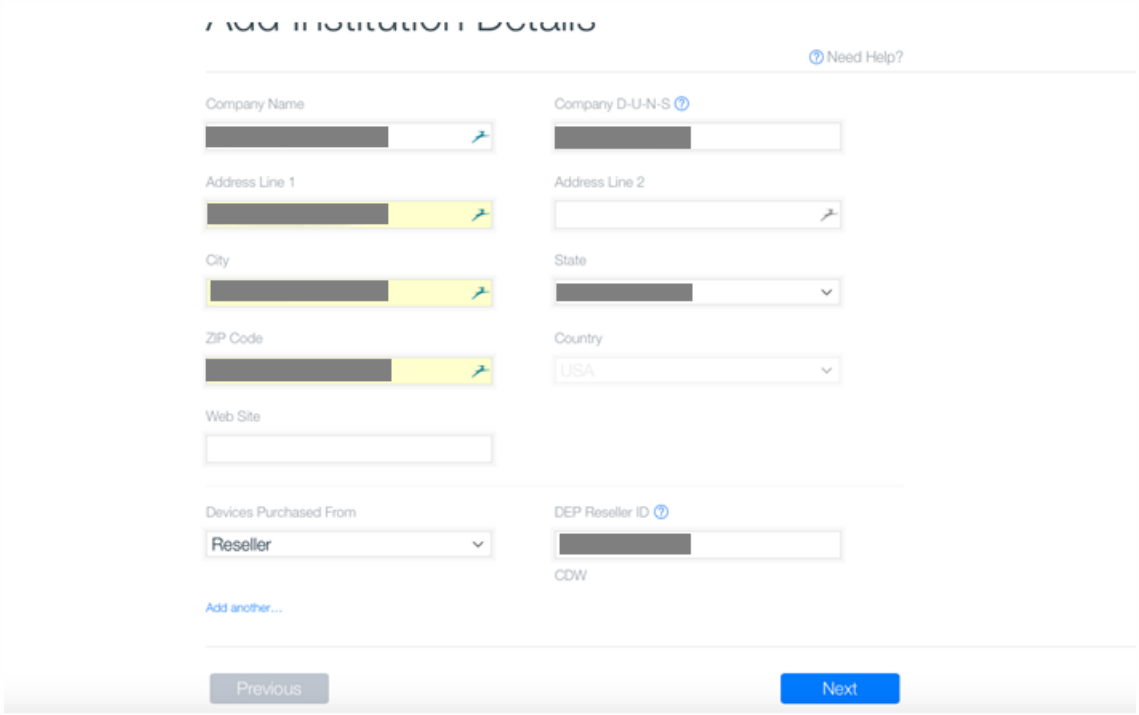


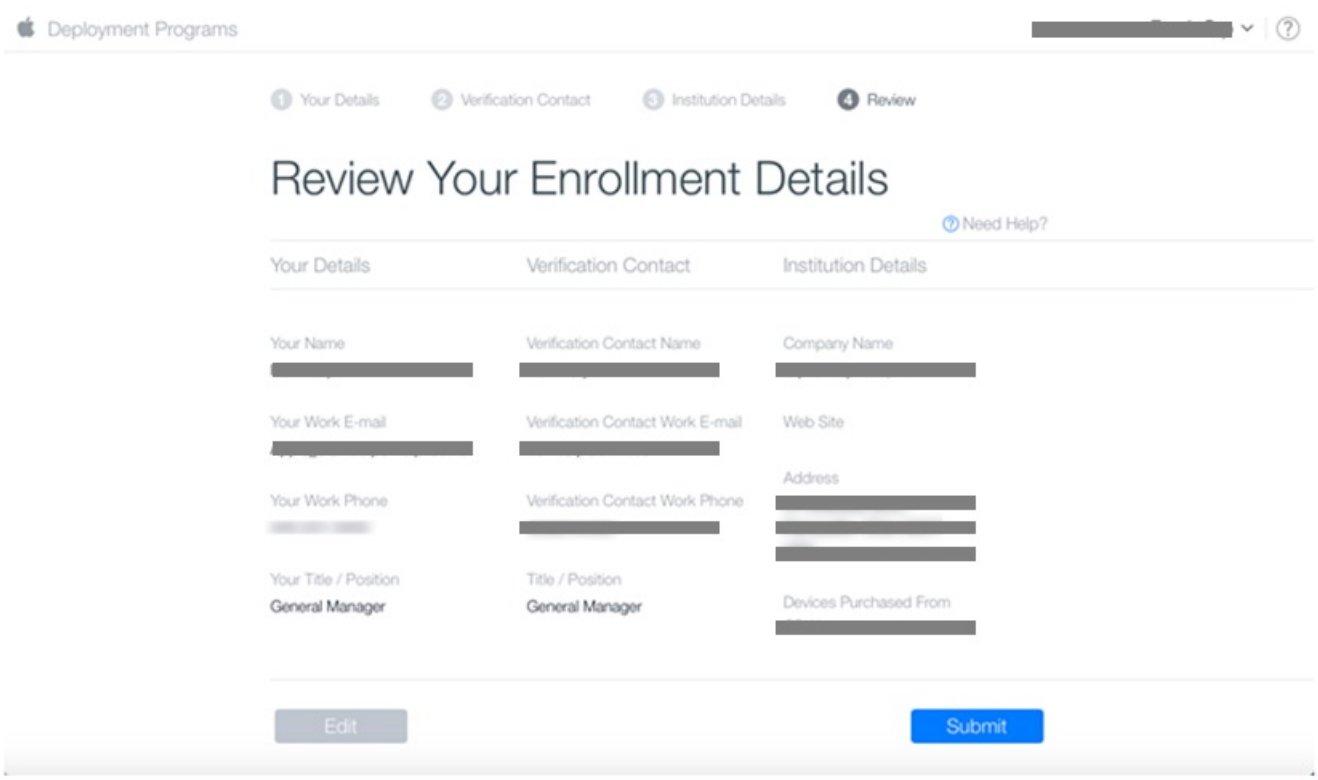


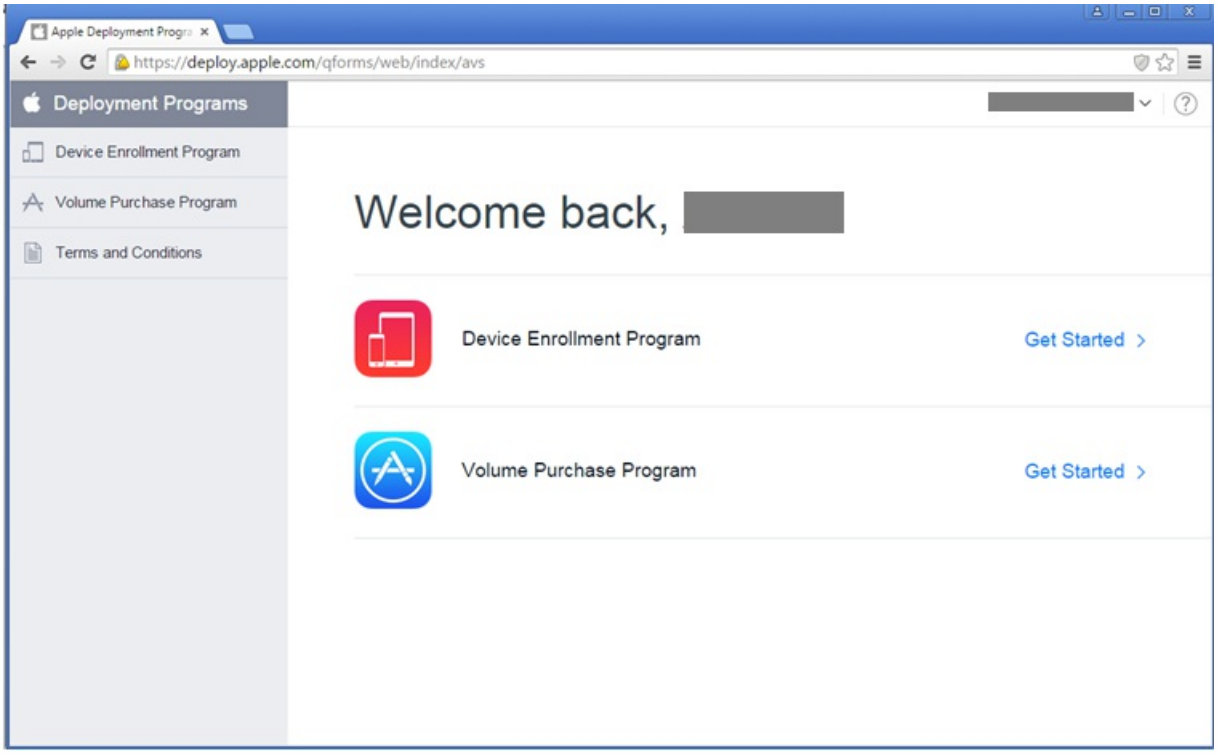




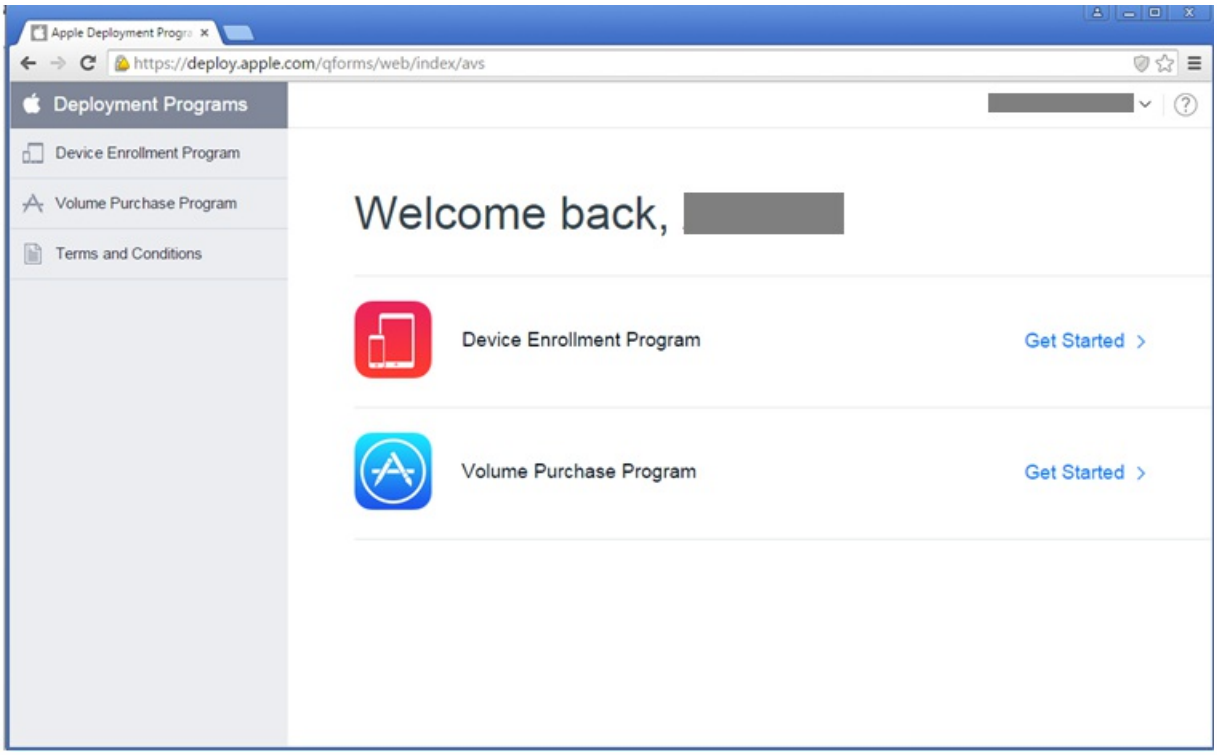


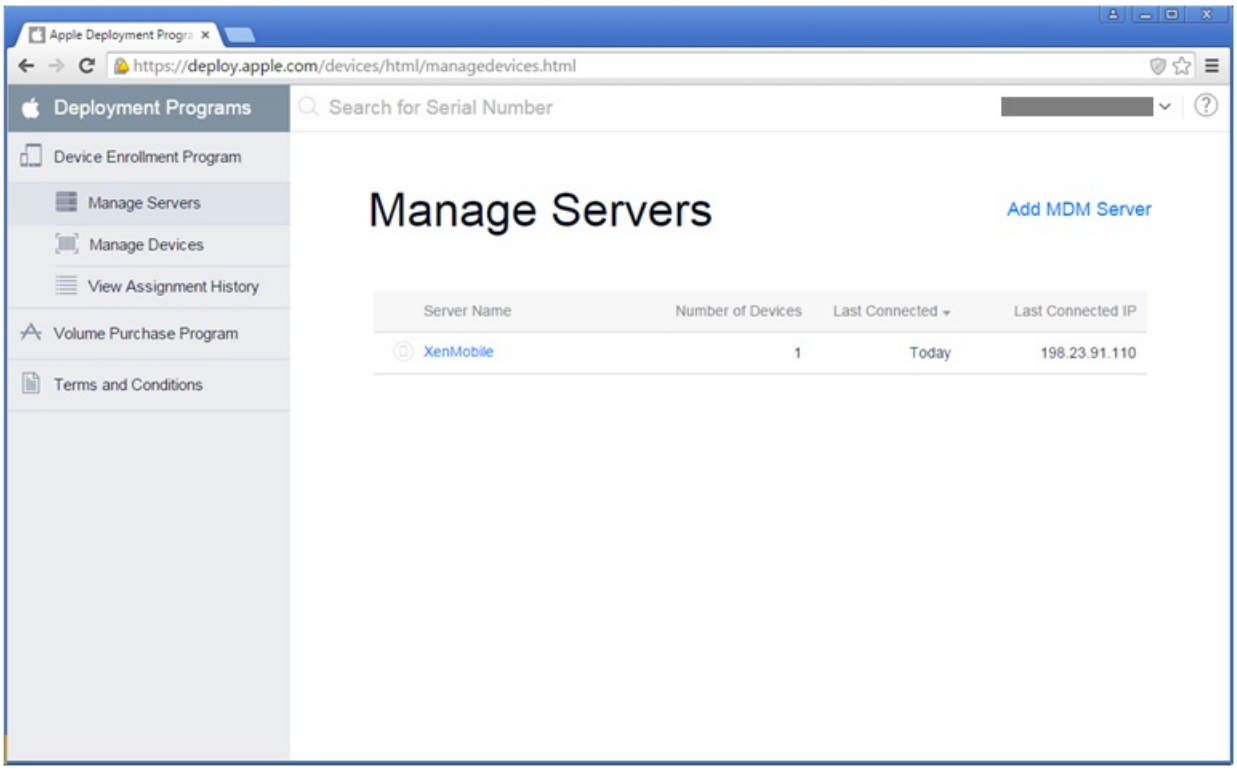


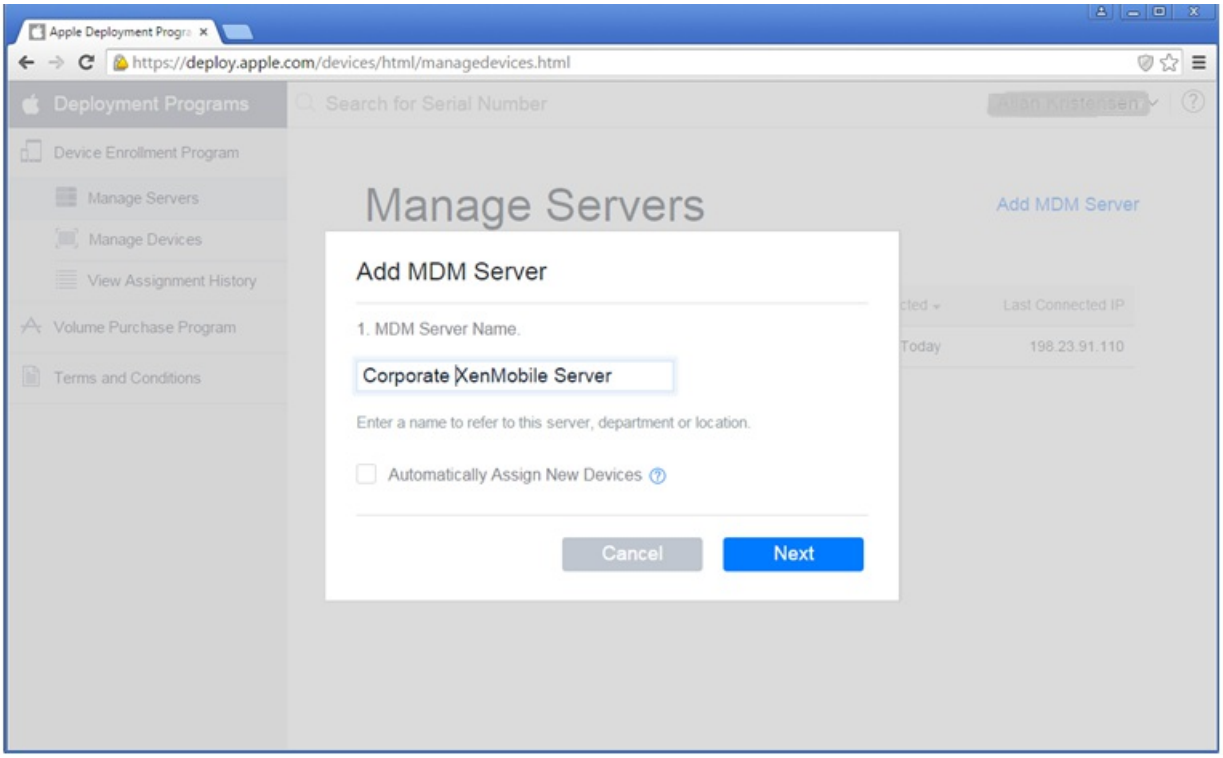


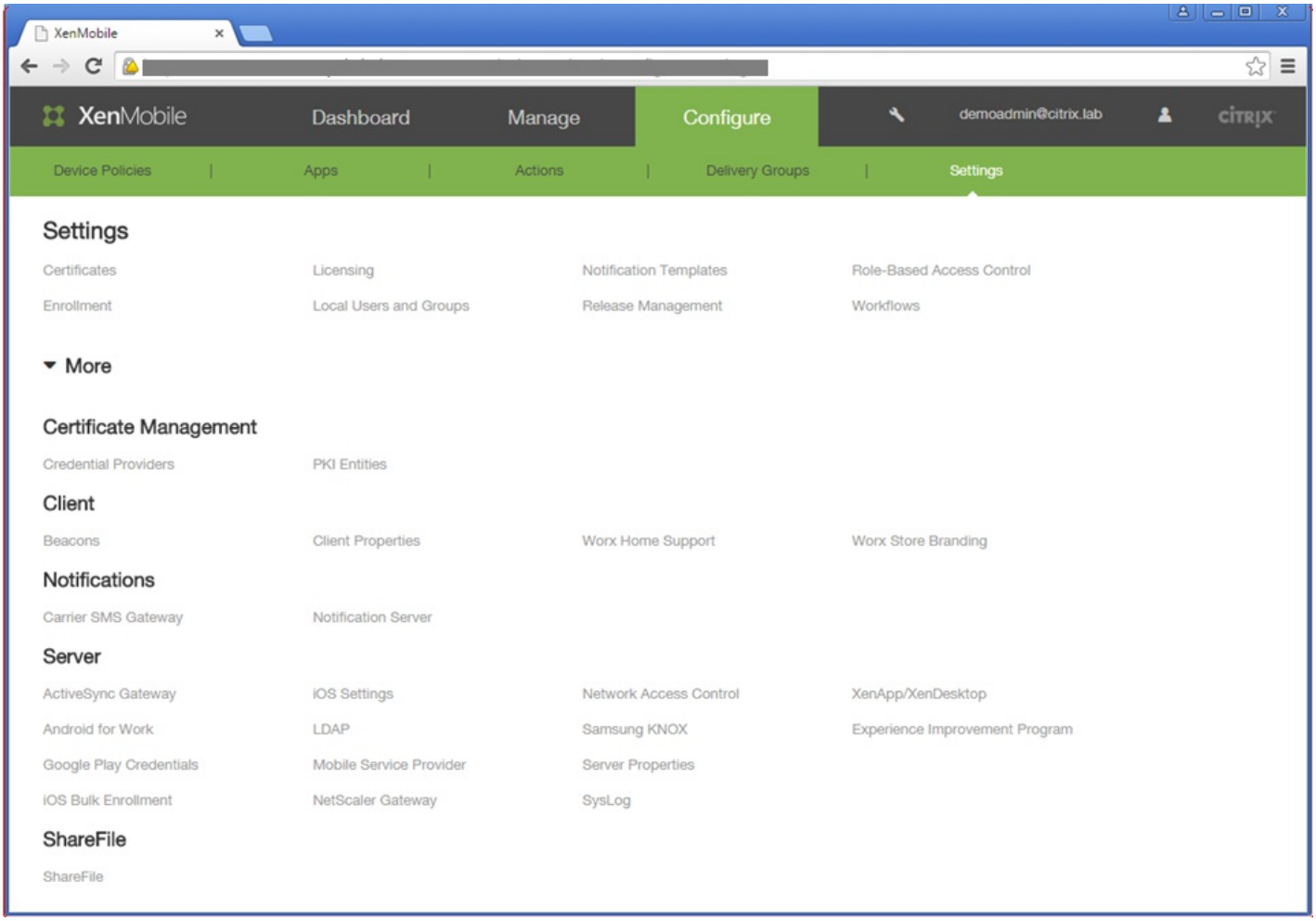


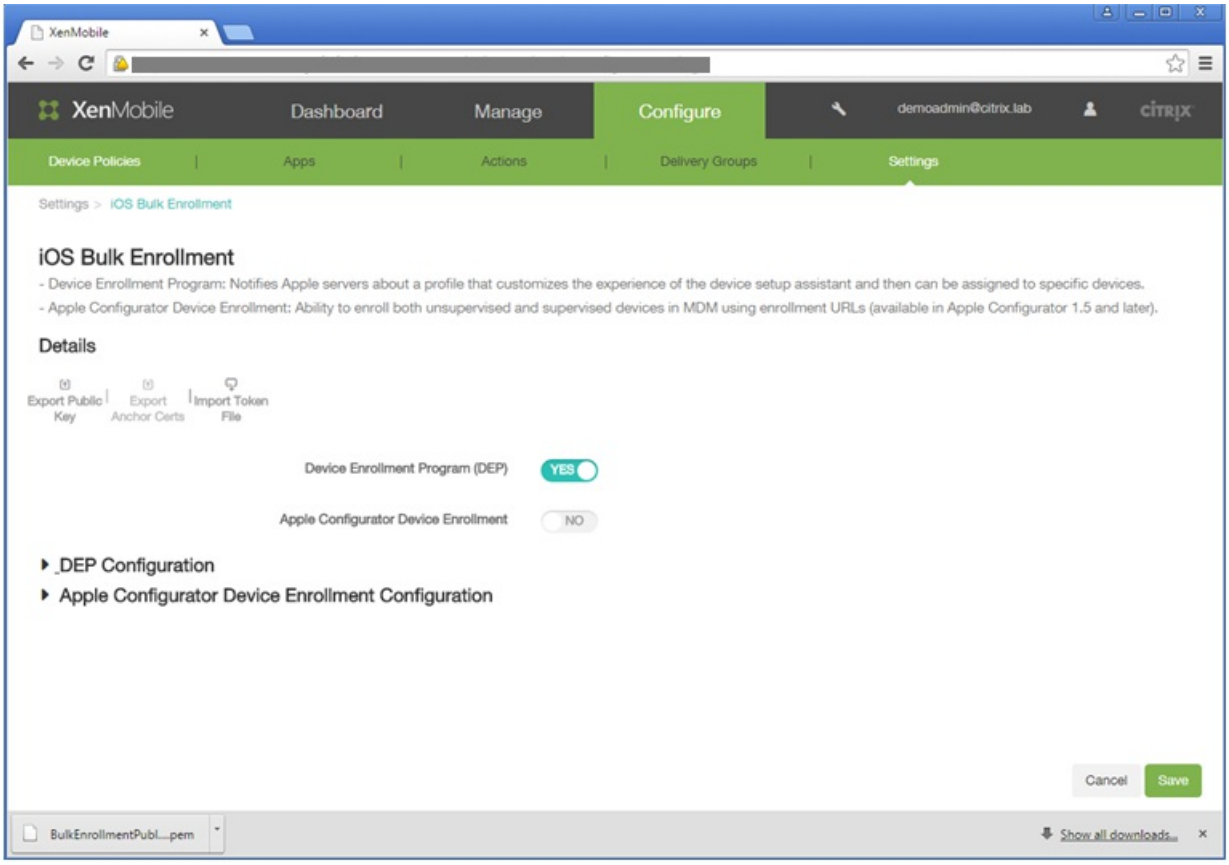
Integrieren des Apple DEP-Kontos mit XenMobile

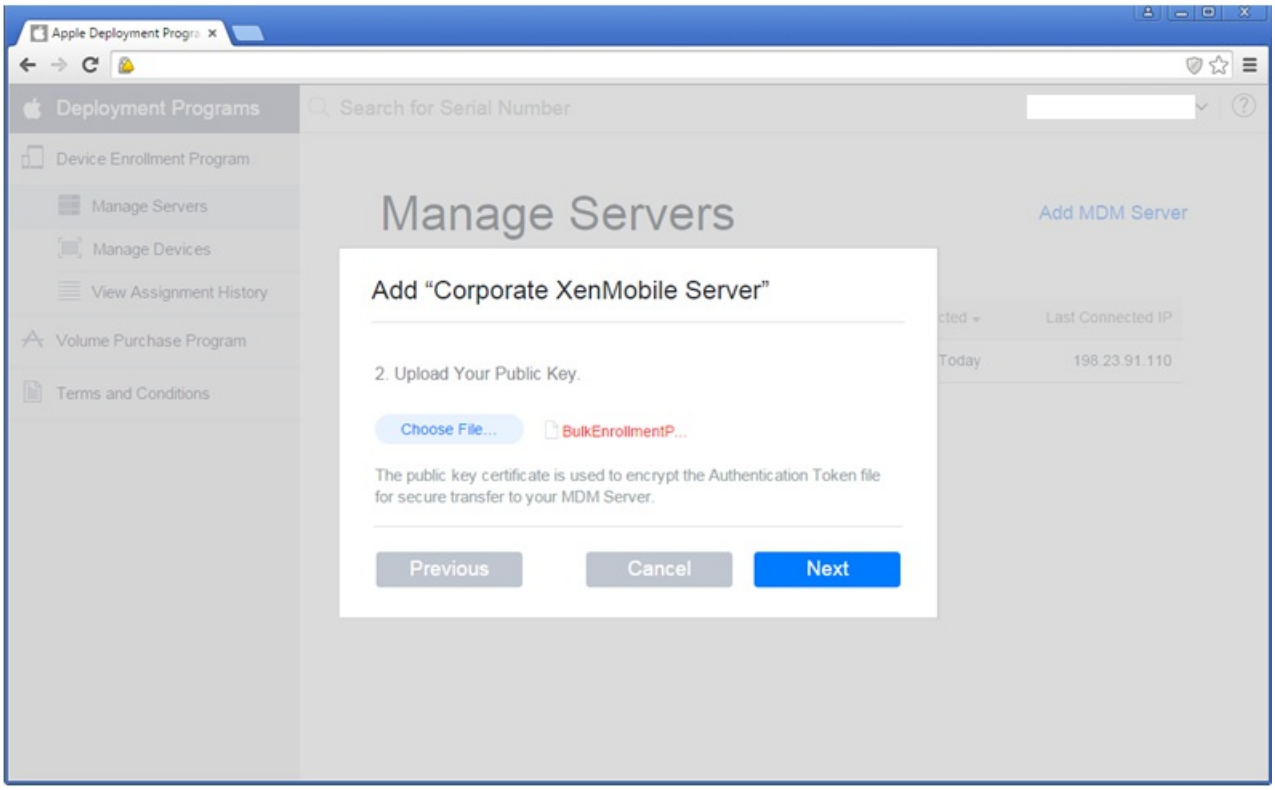


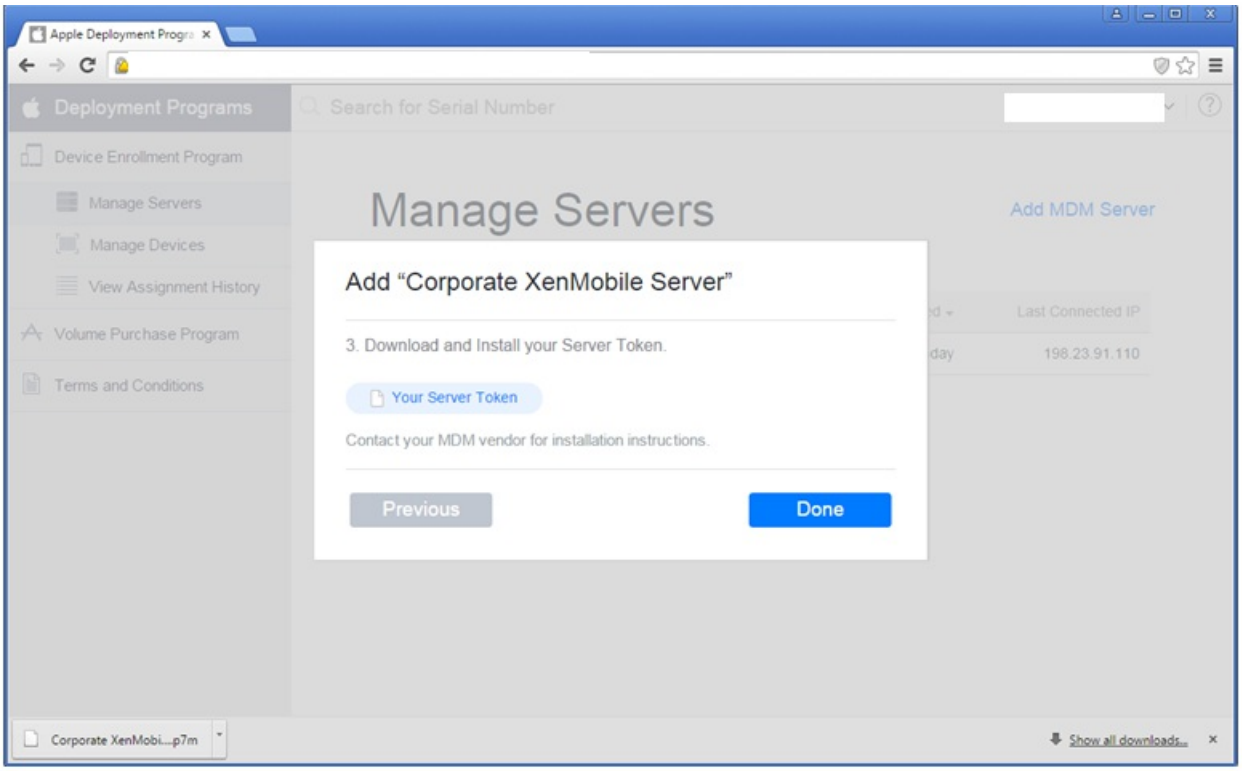


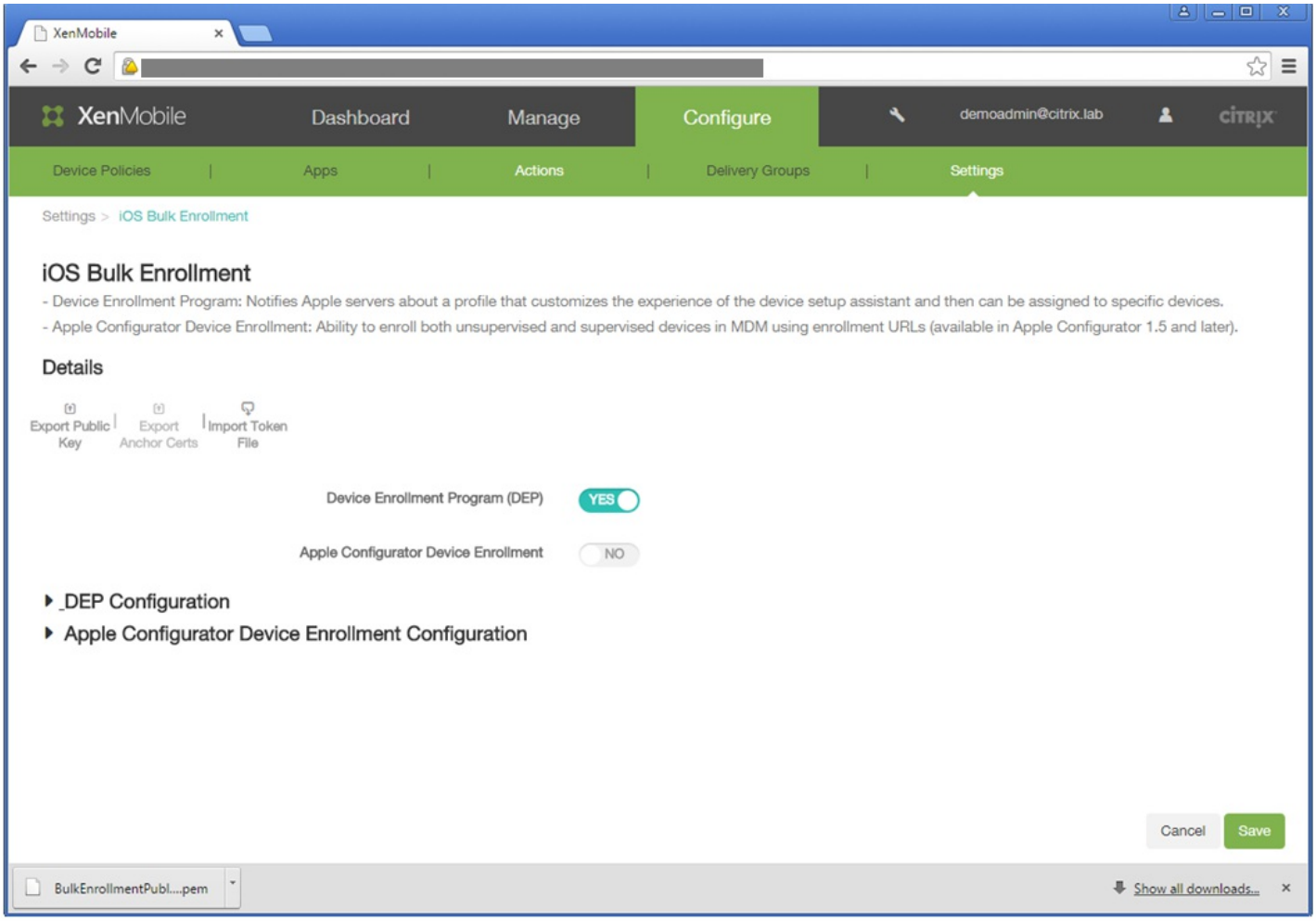


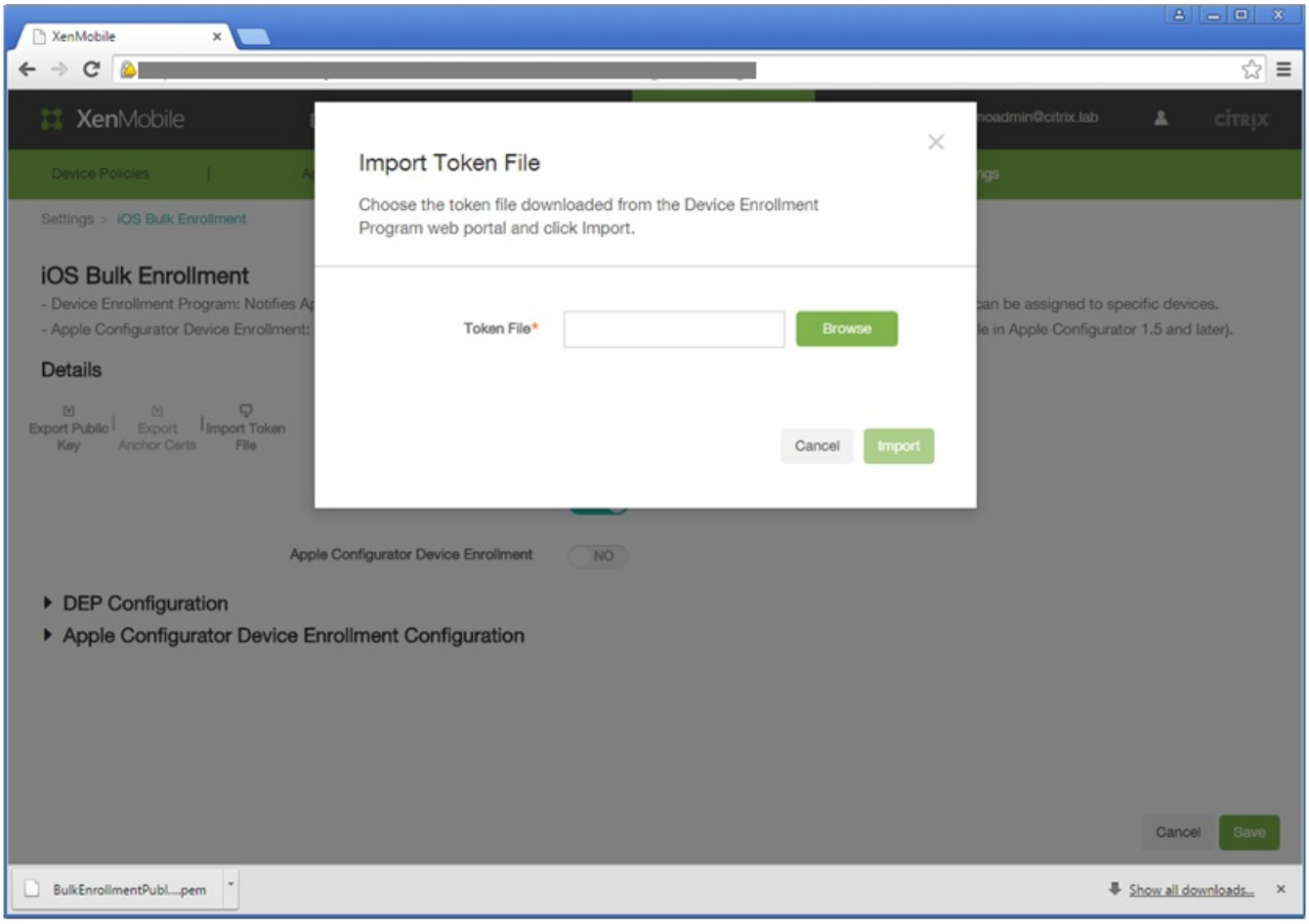


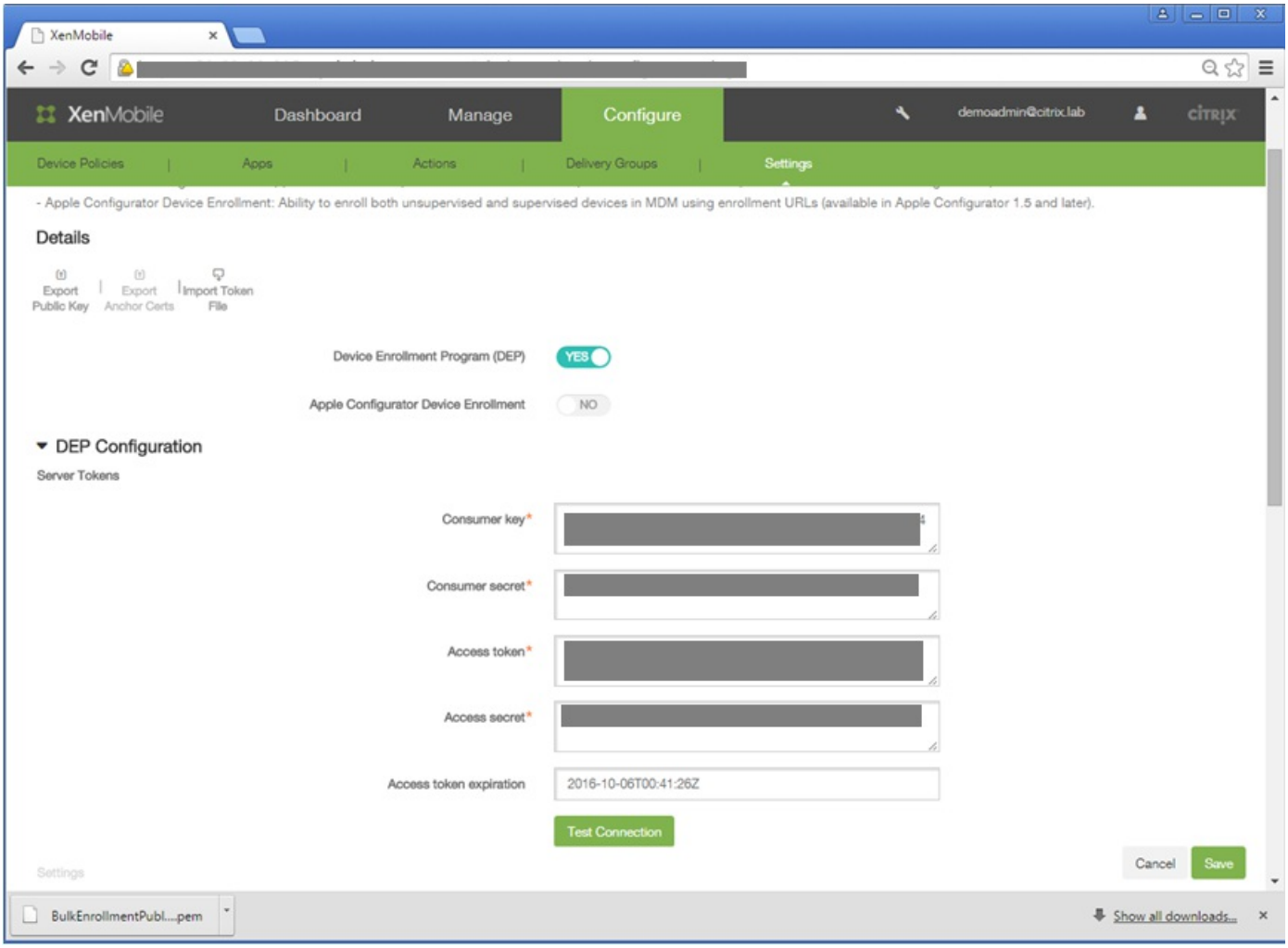


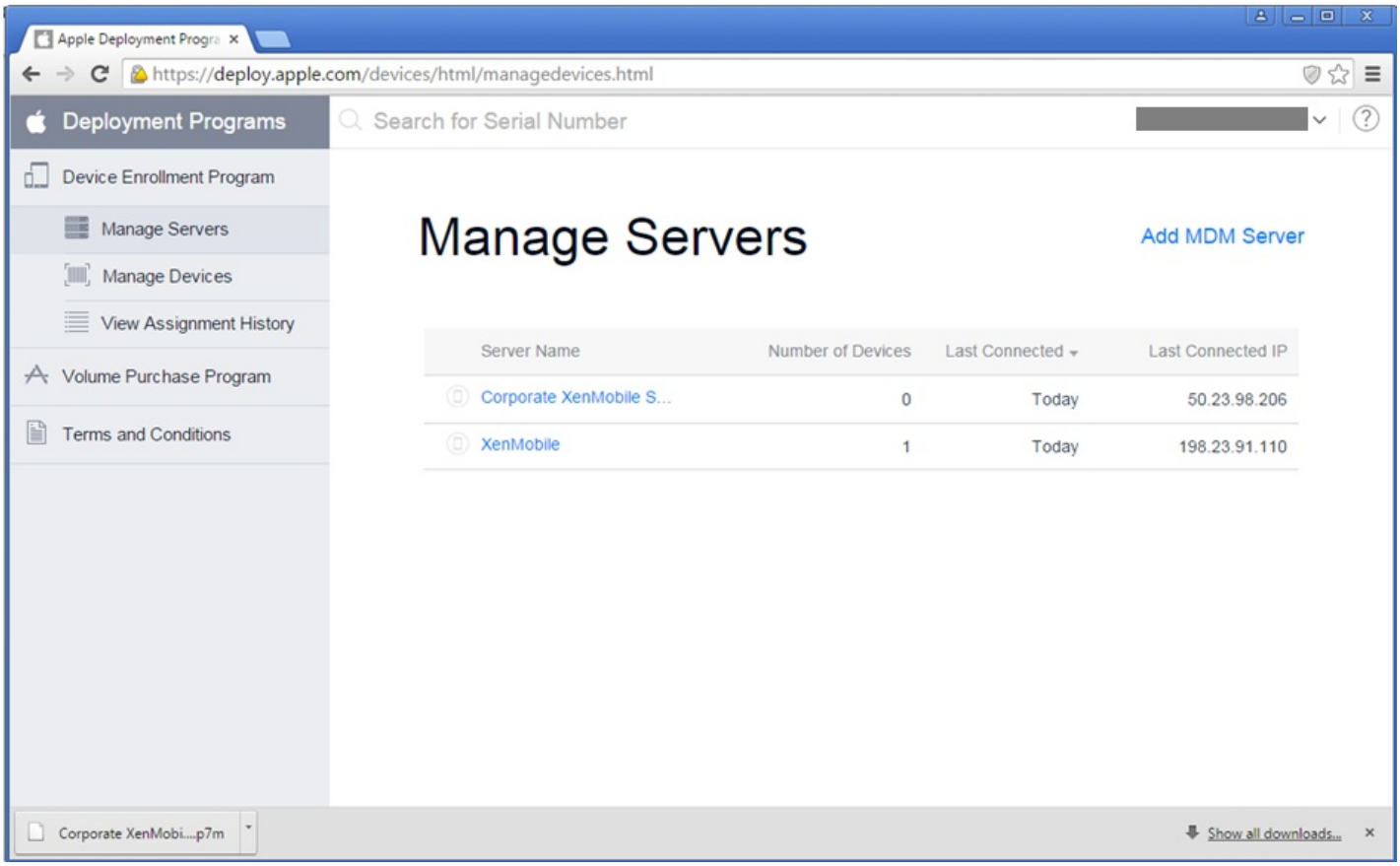






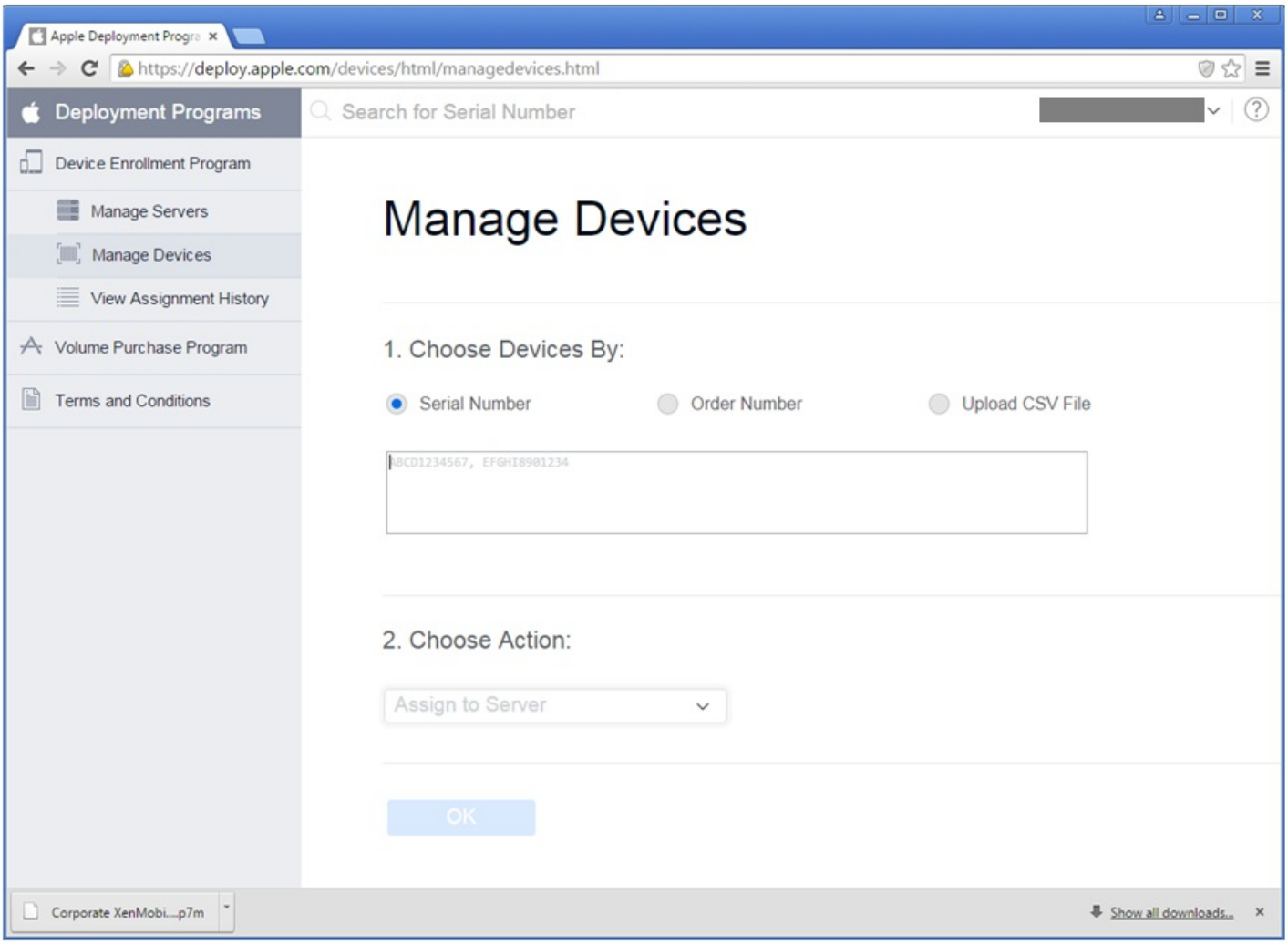


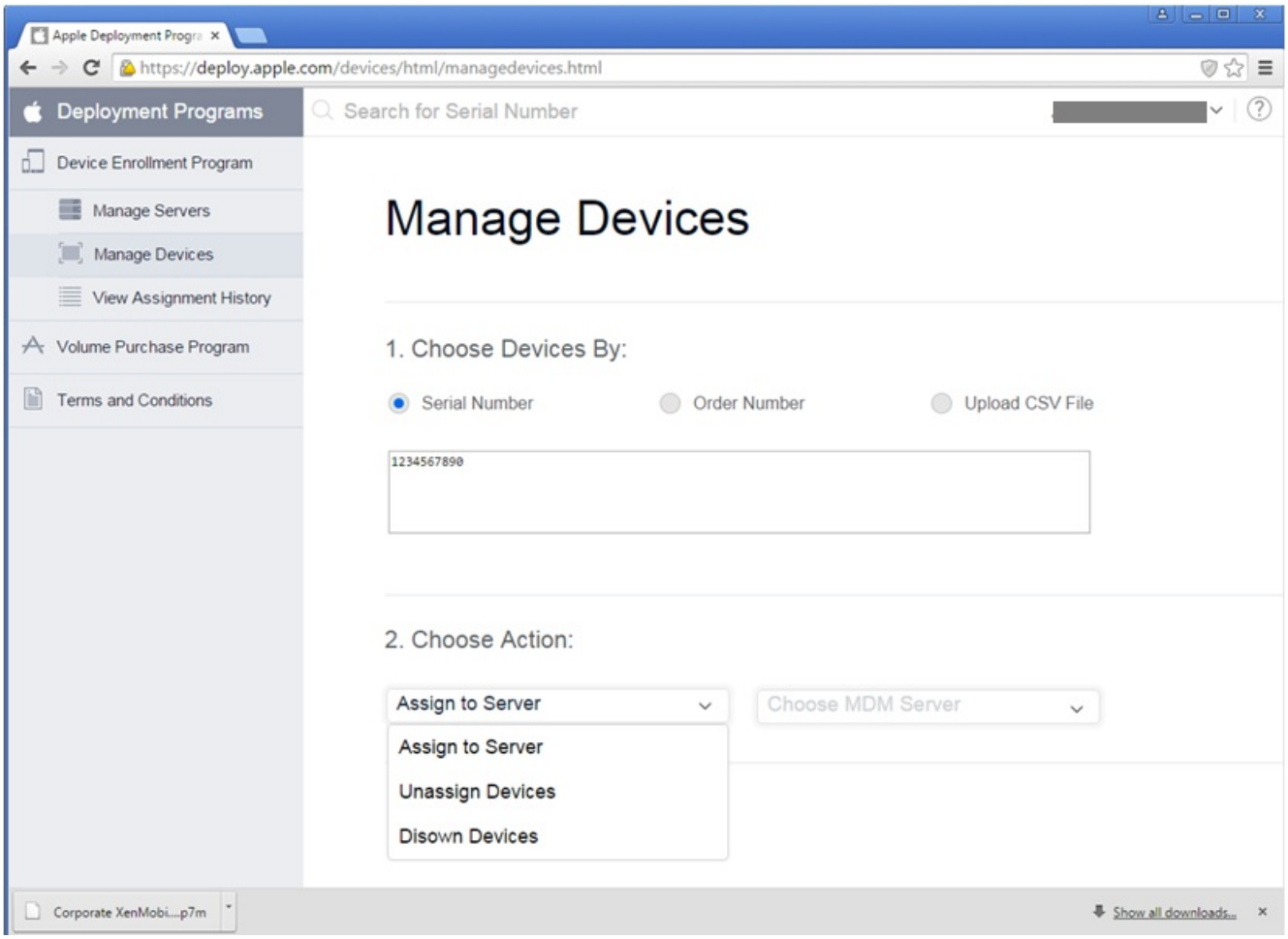


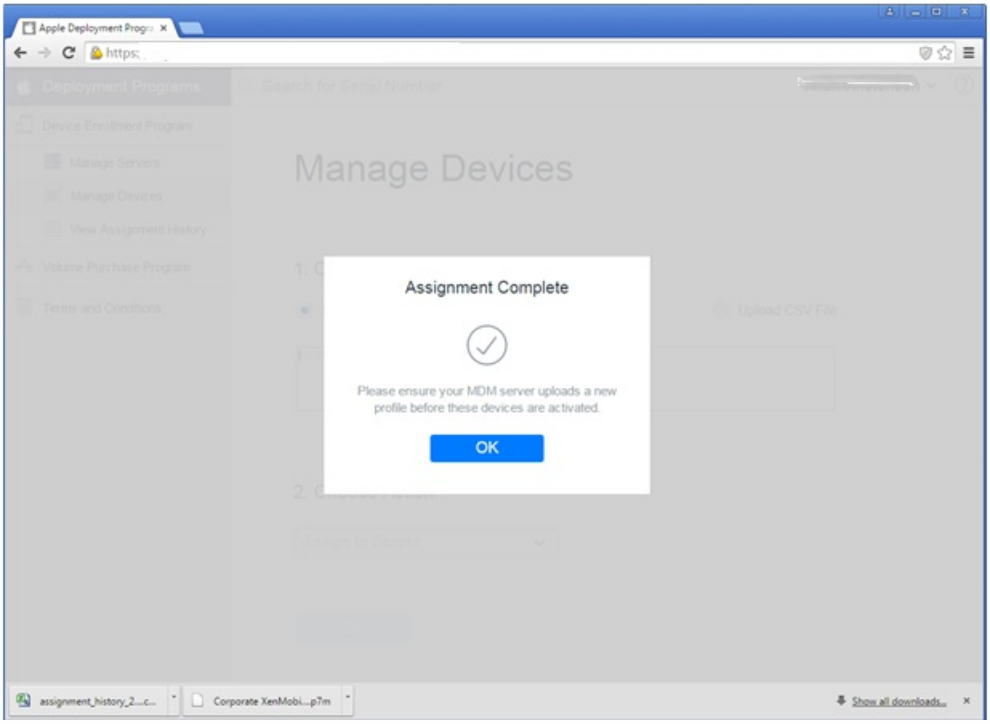


Bestellen von DEP-aktivierten Geräten

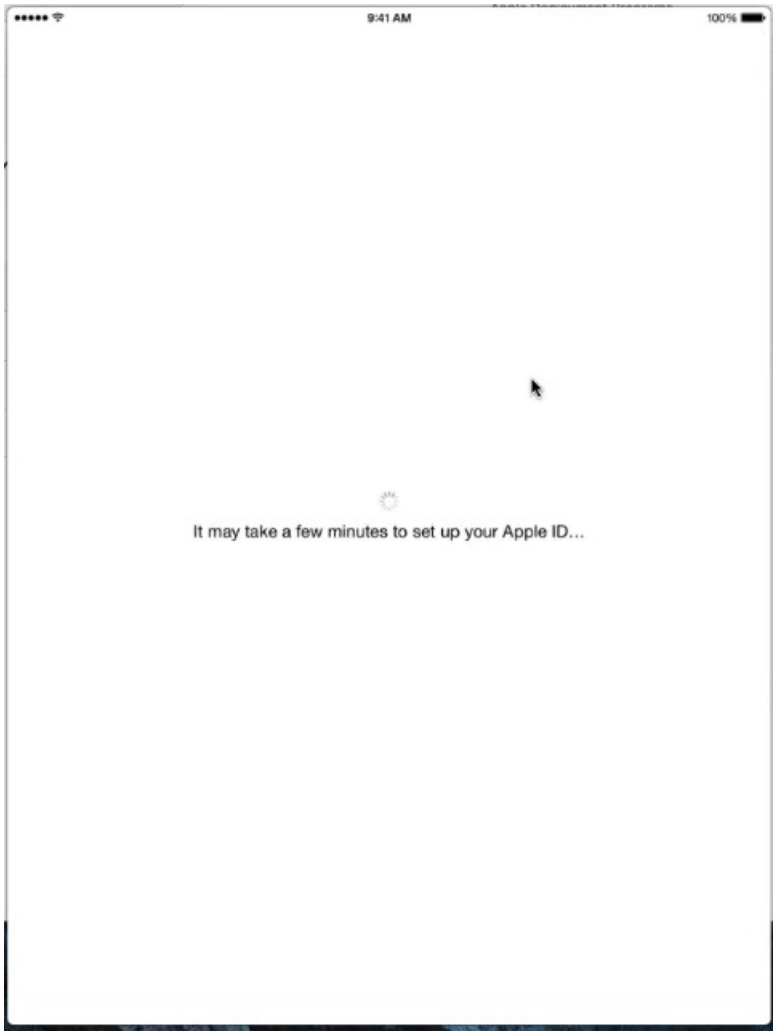
Verwalten von DEP-aktivierten Geräten

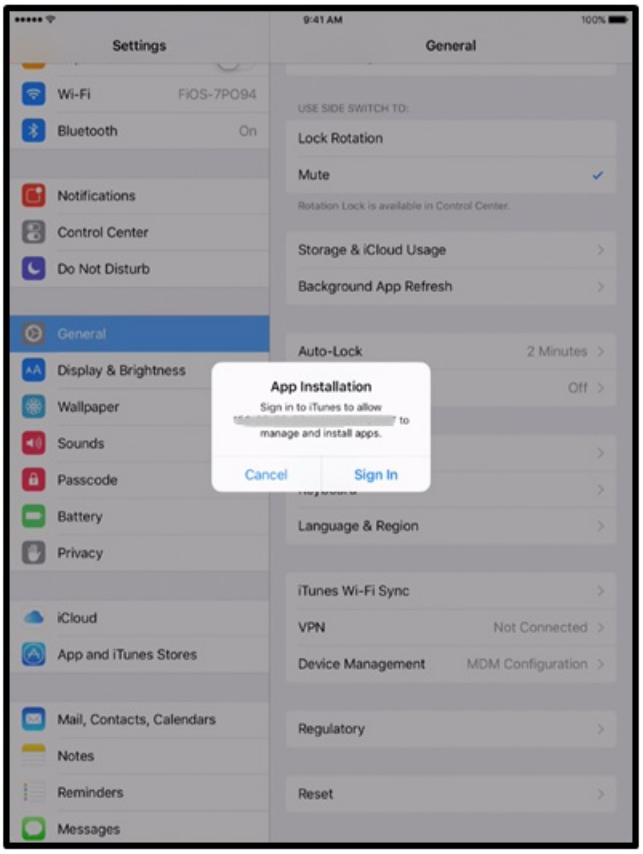




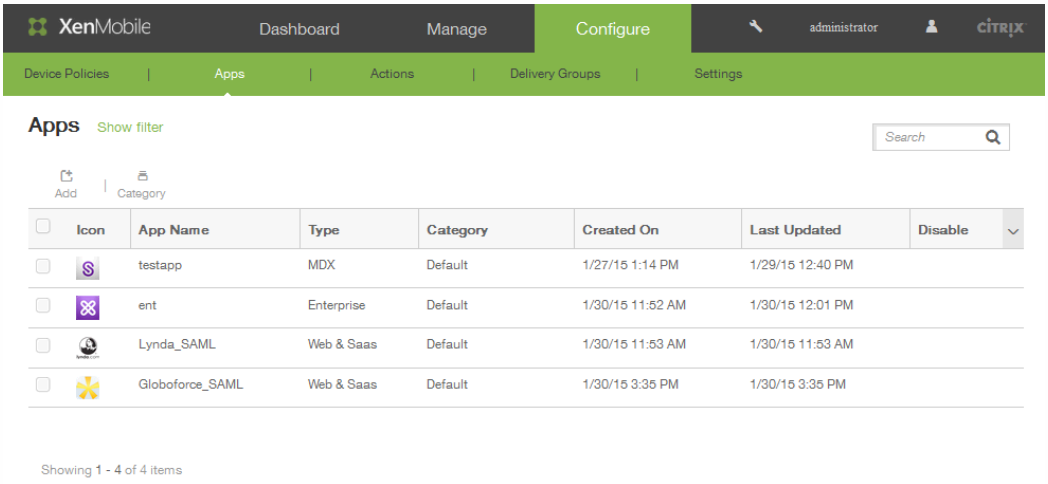


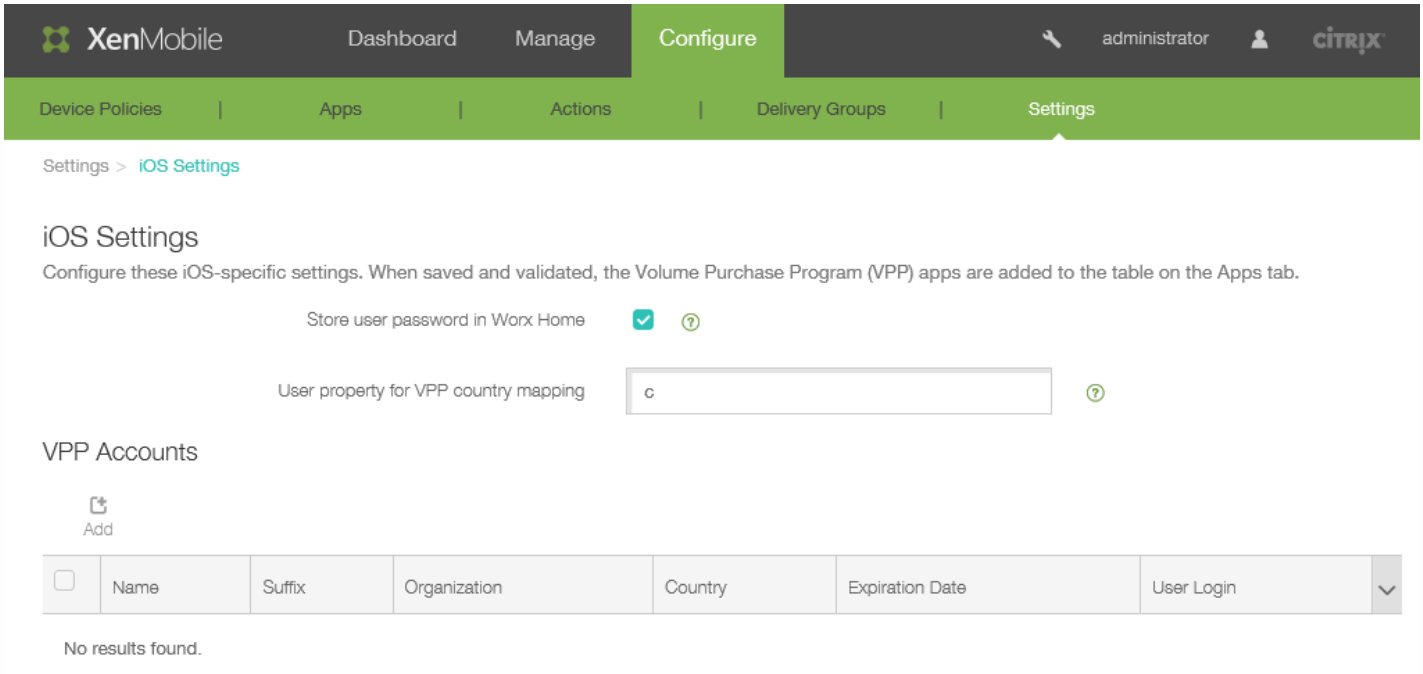
Benutzererfahrung beim Registrieren eines Apple DEP-aktivierten Geräts

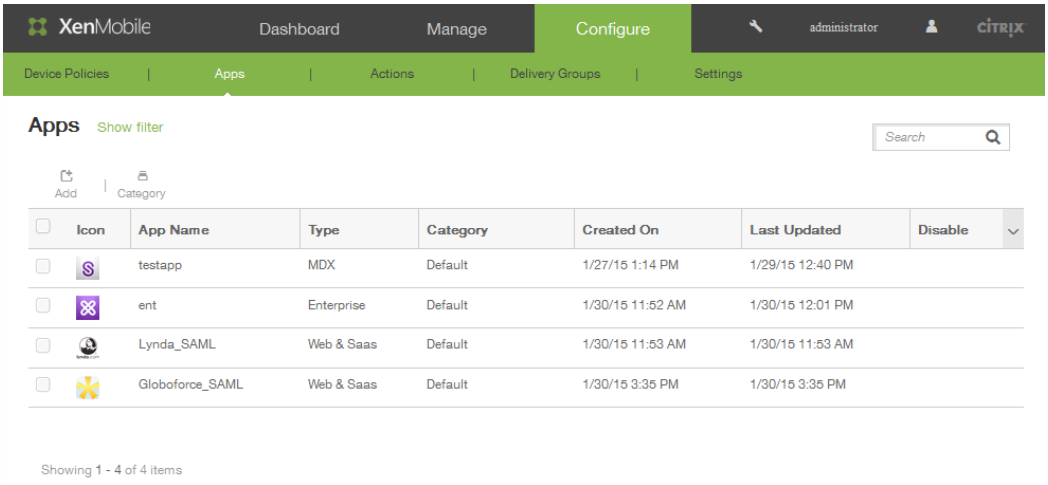




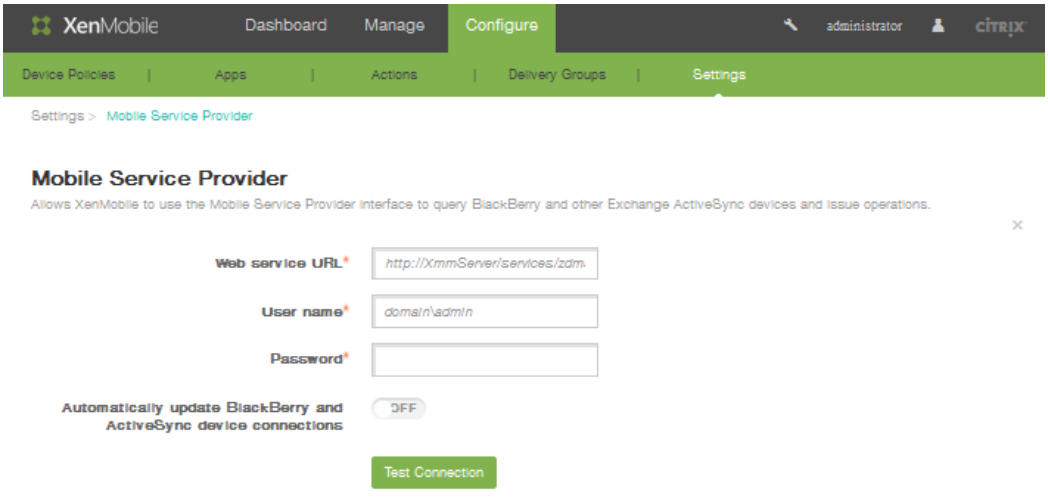
iOS VPP





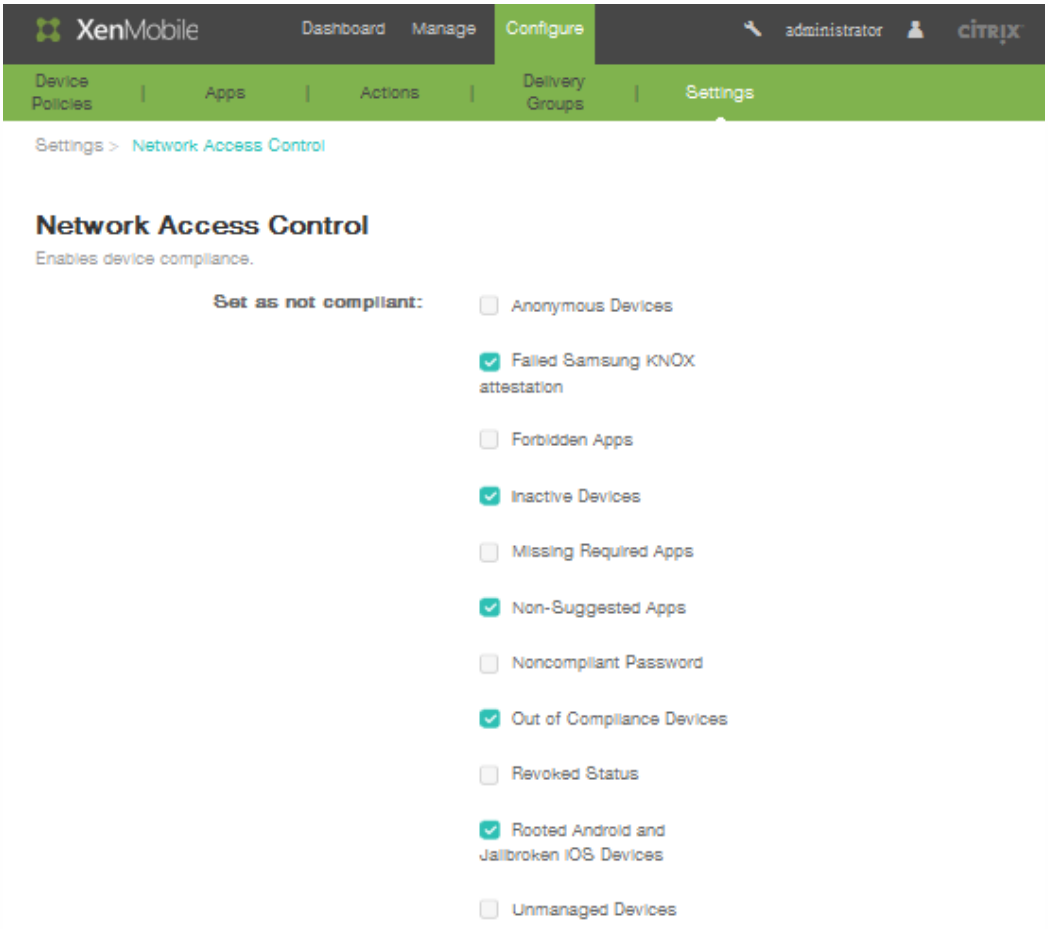


Mobilfunkanbieter

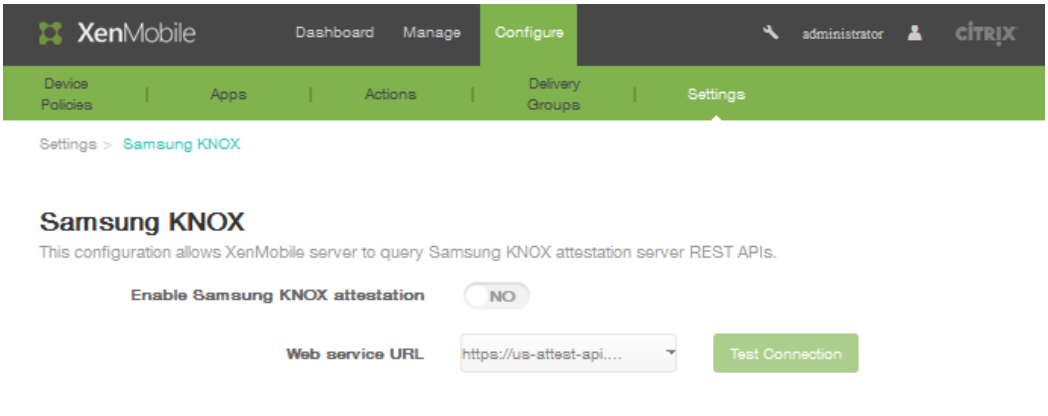


Network Access Control

Hinweis



Samsung KNOX

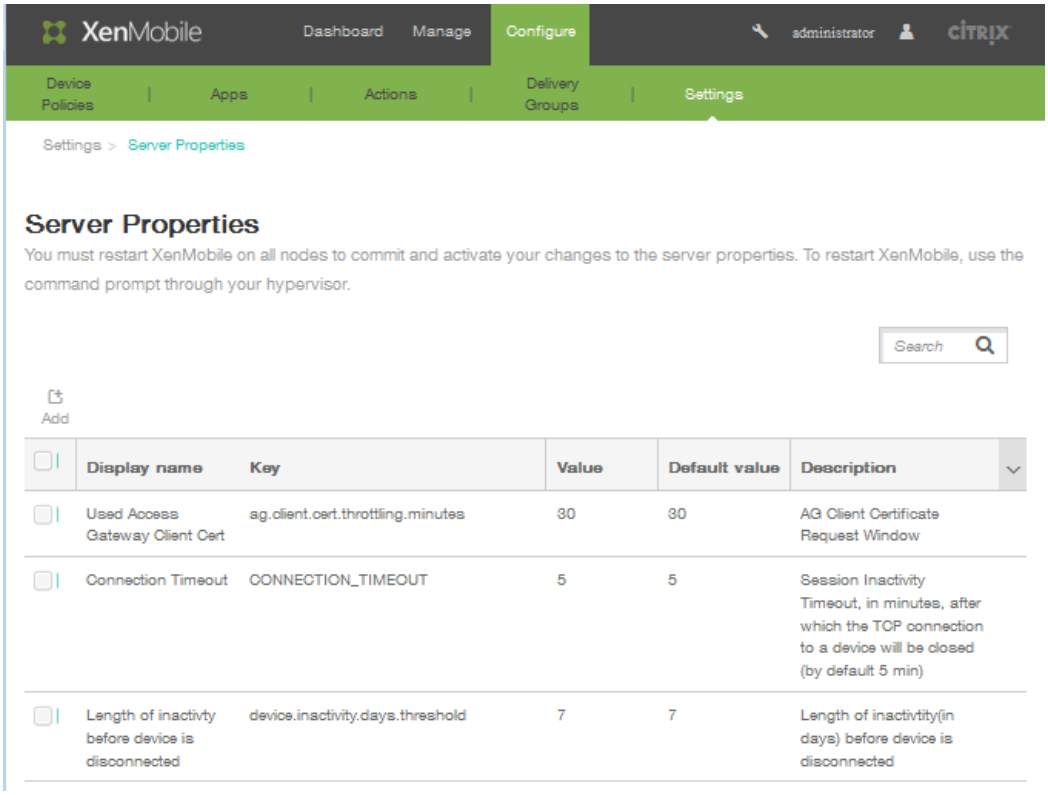


Servereigenschaften

Servereigenschaften – Definitionen

Hinzufügen, Bearbeiten oder Löschen von Servereigenschaften

> Hinweis



-
-

-
-
-

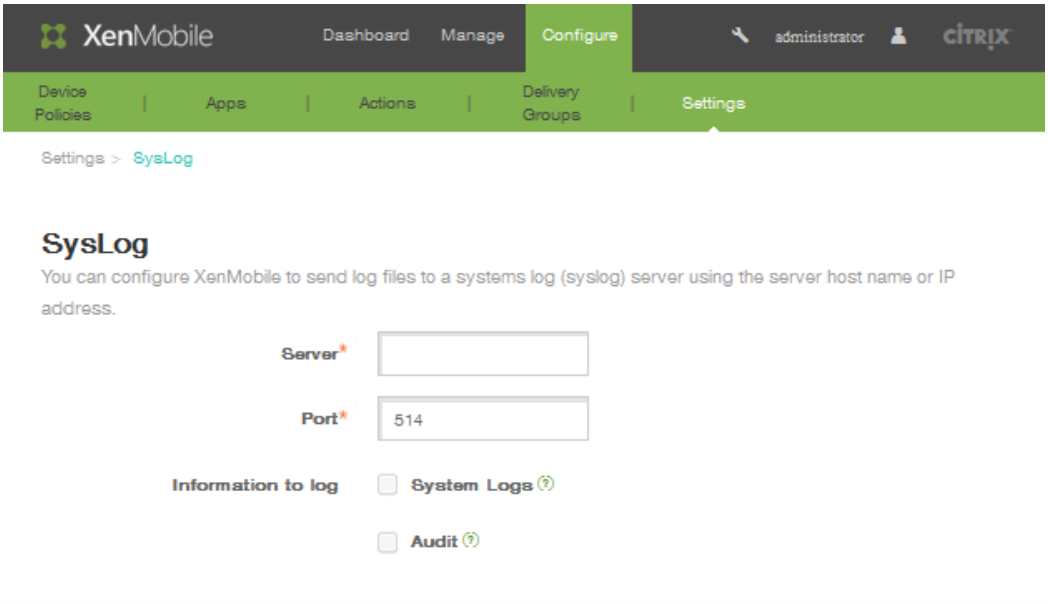
Konfigurieren des effektiven Servermodus in XenMobile

SysLog

-
-

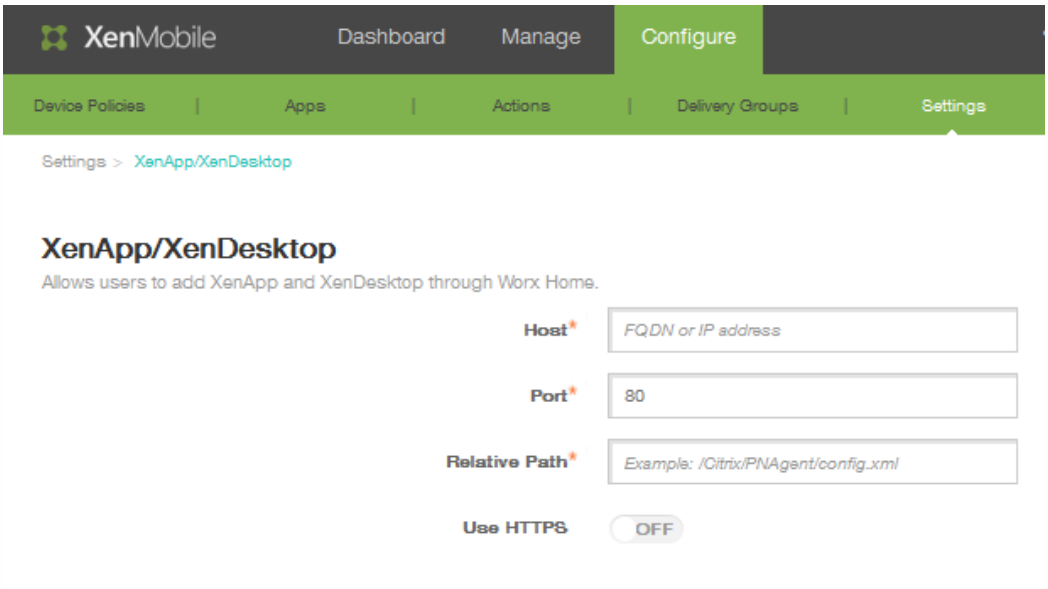
-
-
-
-
-

> Hinweis



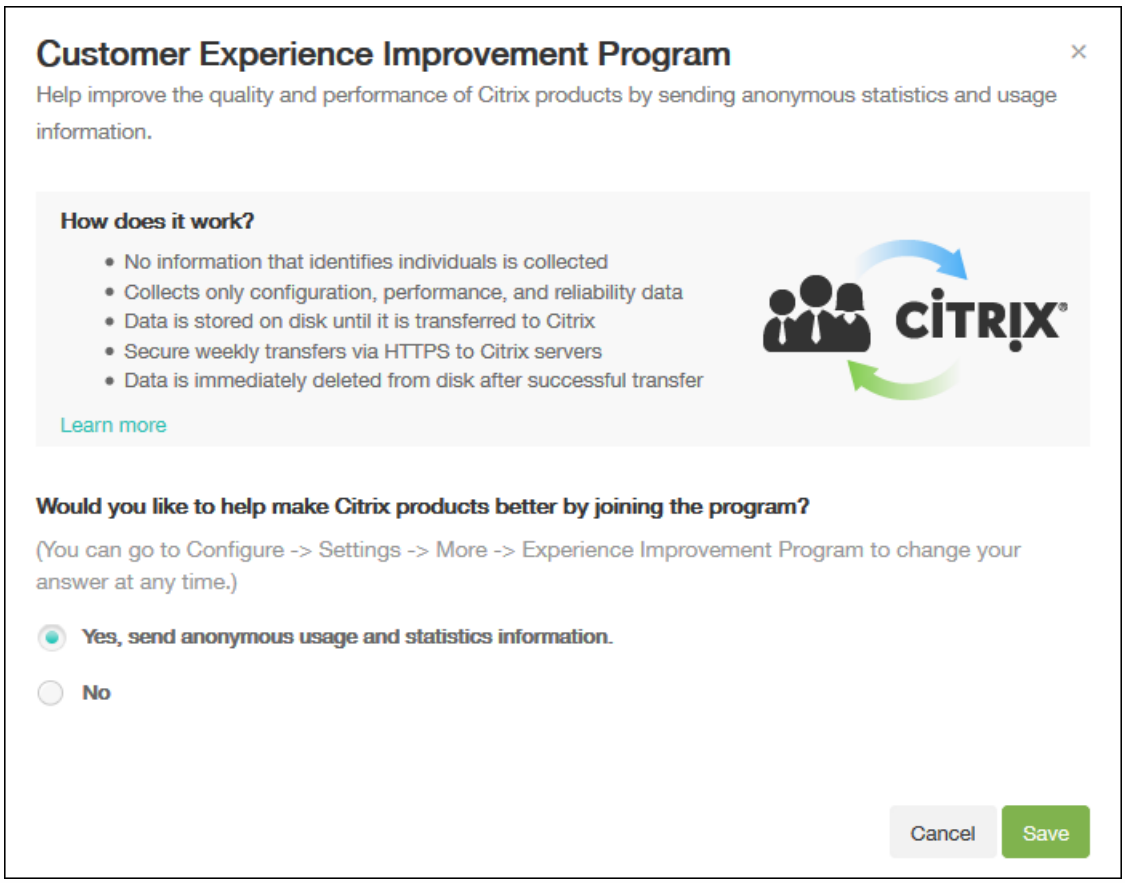
-
-

So konfigurieren Sie XenApp und XenDesktop

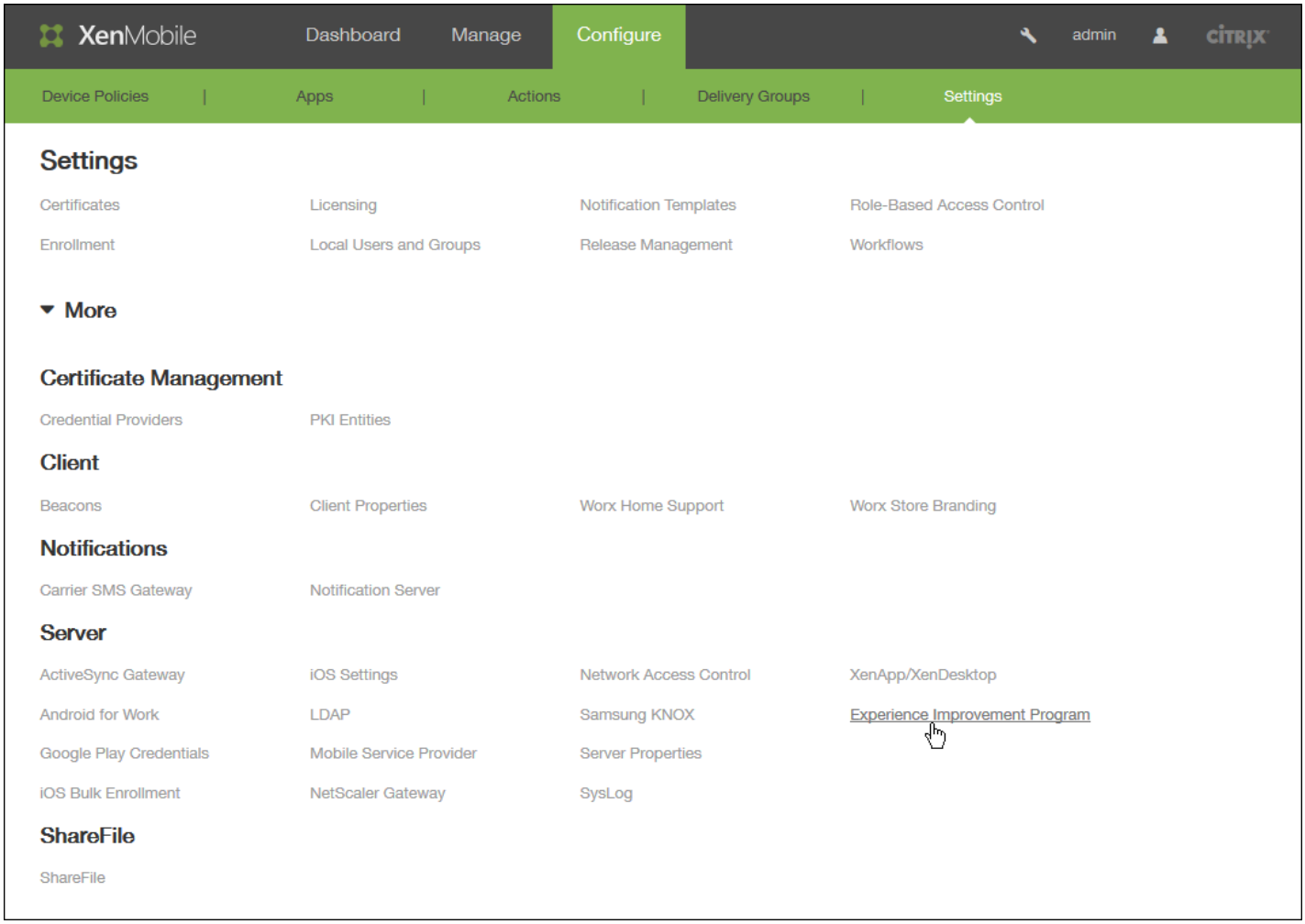


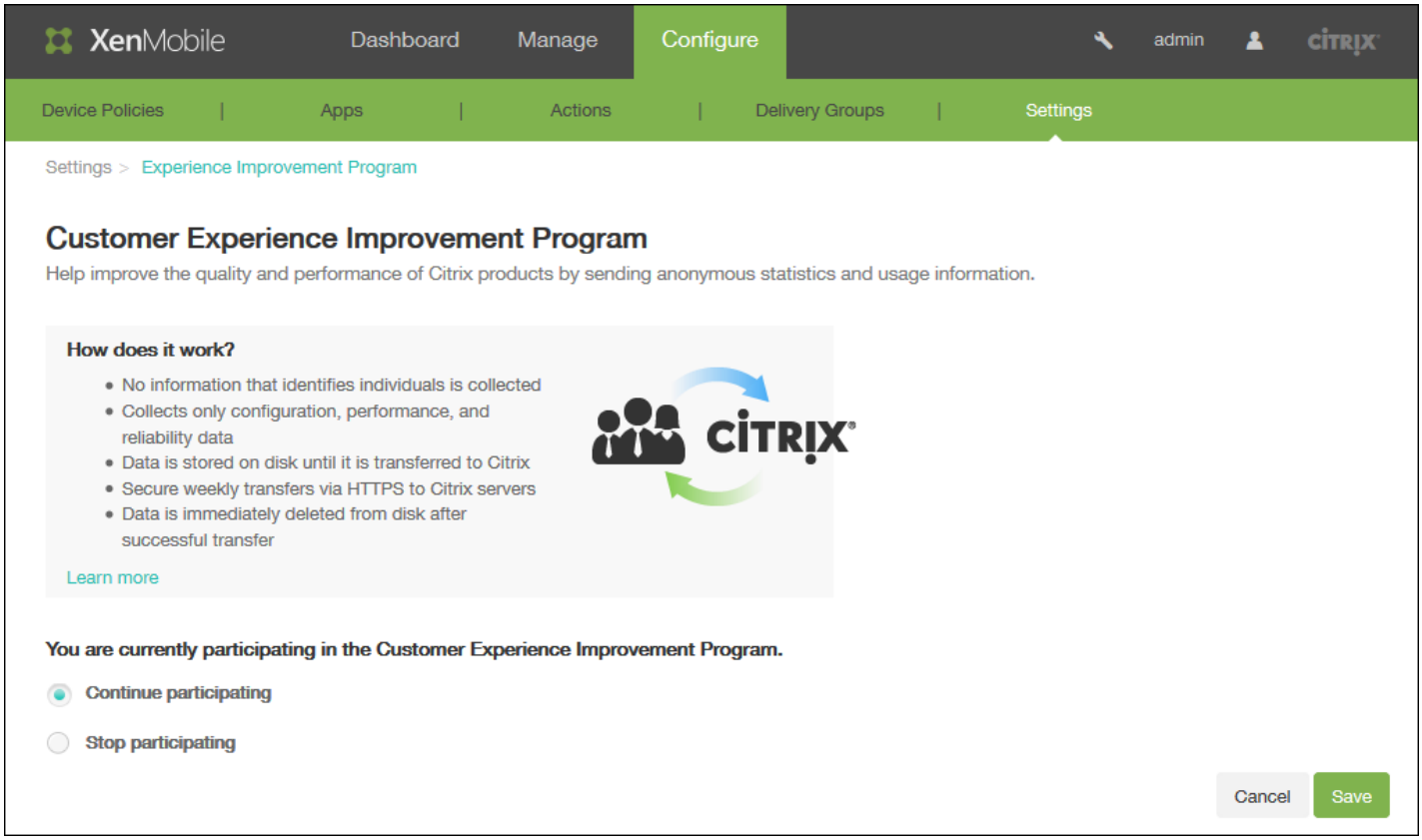
Programm zur Verbesserung der Benutzerfreundlichkeit

CEIP beim Installieren oder Aktualisieren von XenMobile

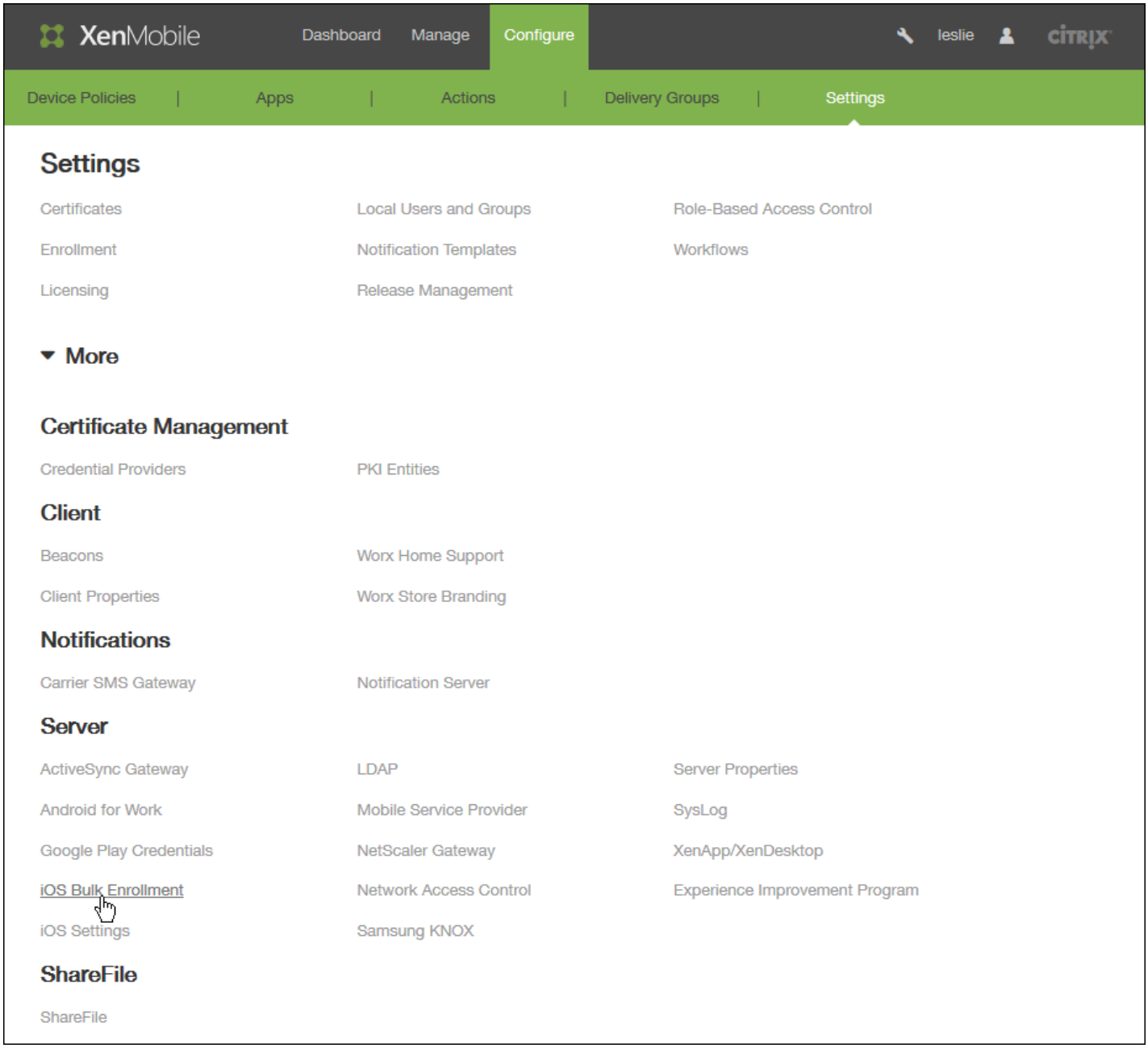


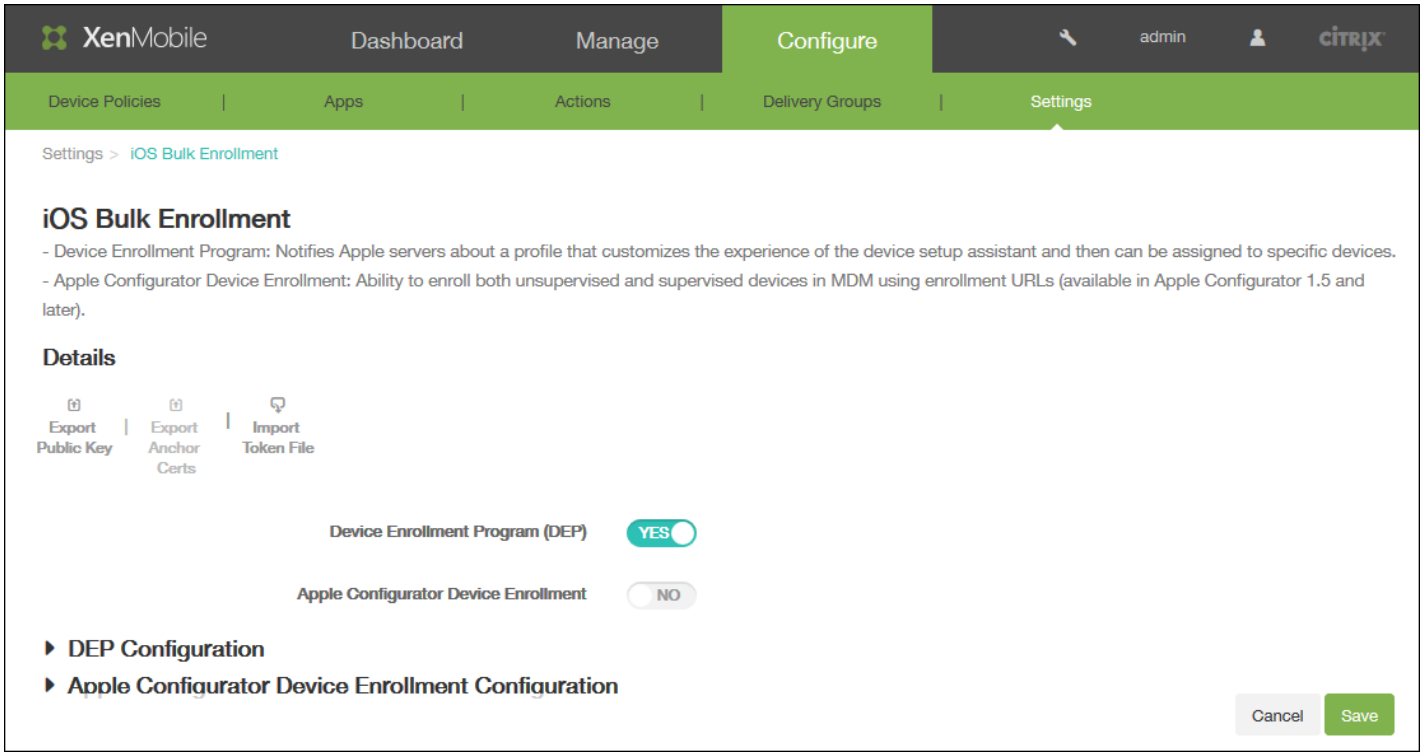
Ändern der Einstellung zur Teilnahme am CEIP



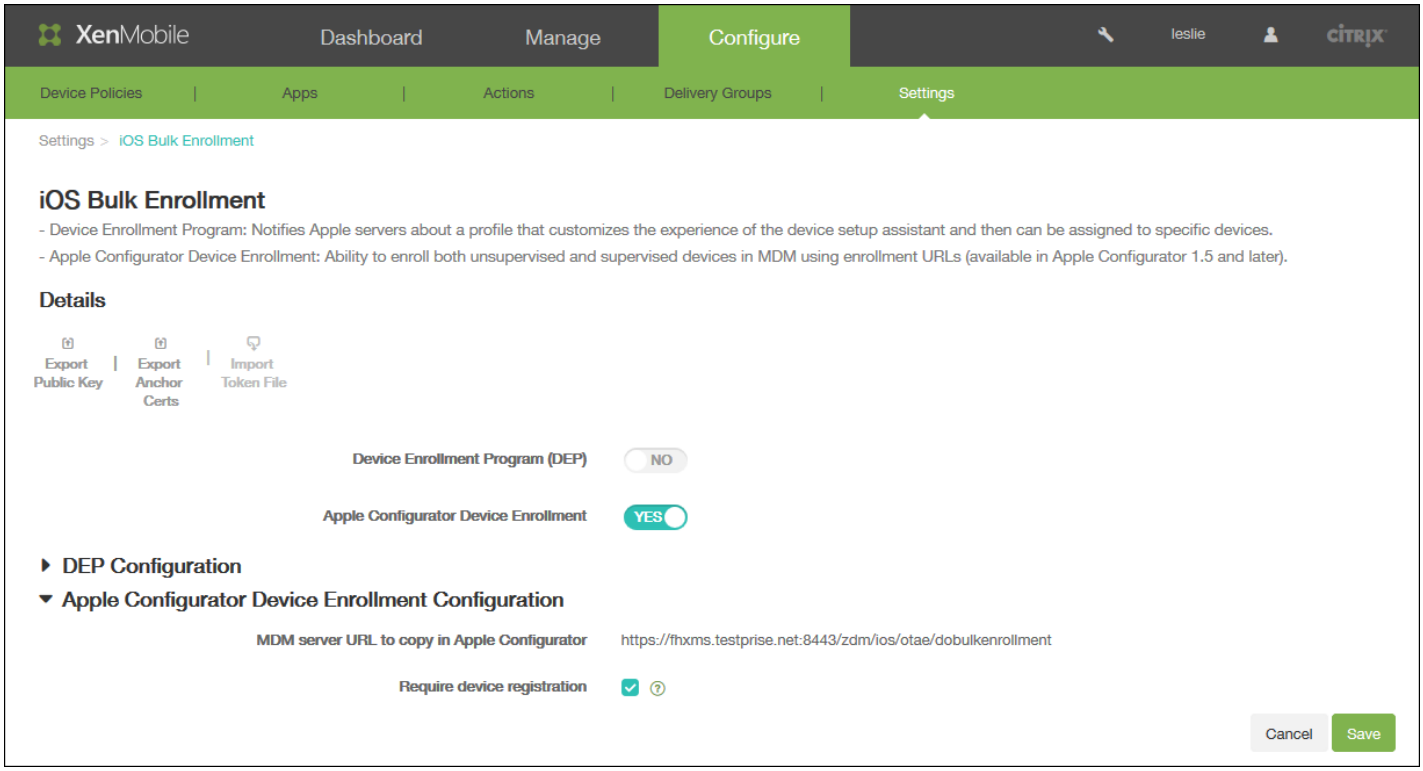


Massenregistrierung von iOS-Geräten





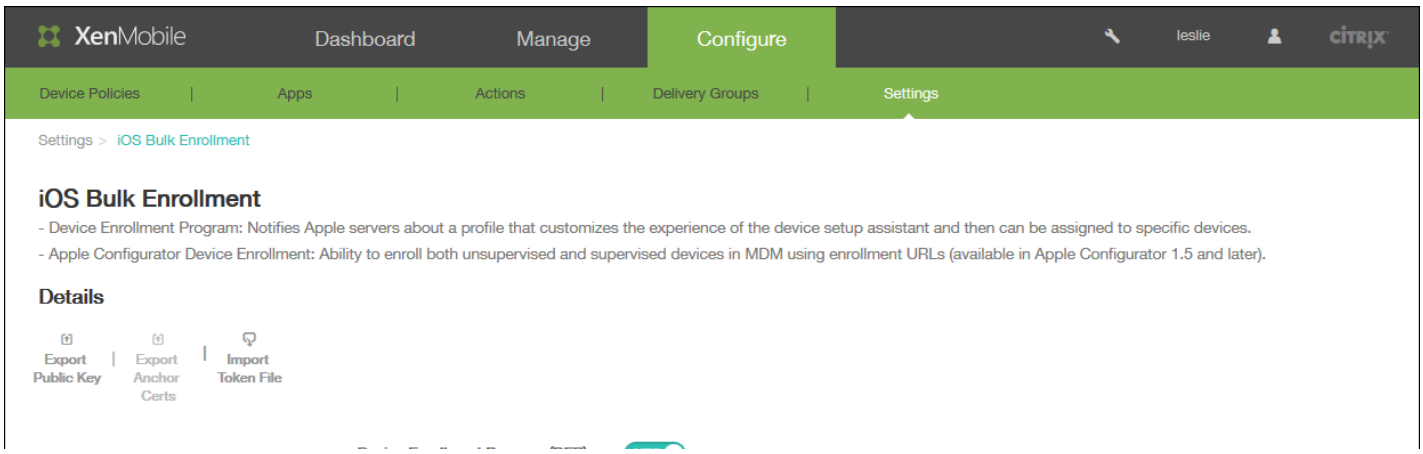
Konfigurieren von Apple Configurator-Einstellungen

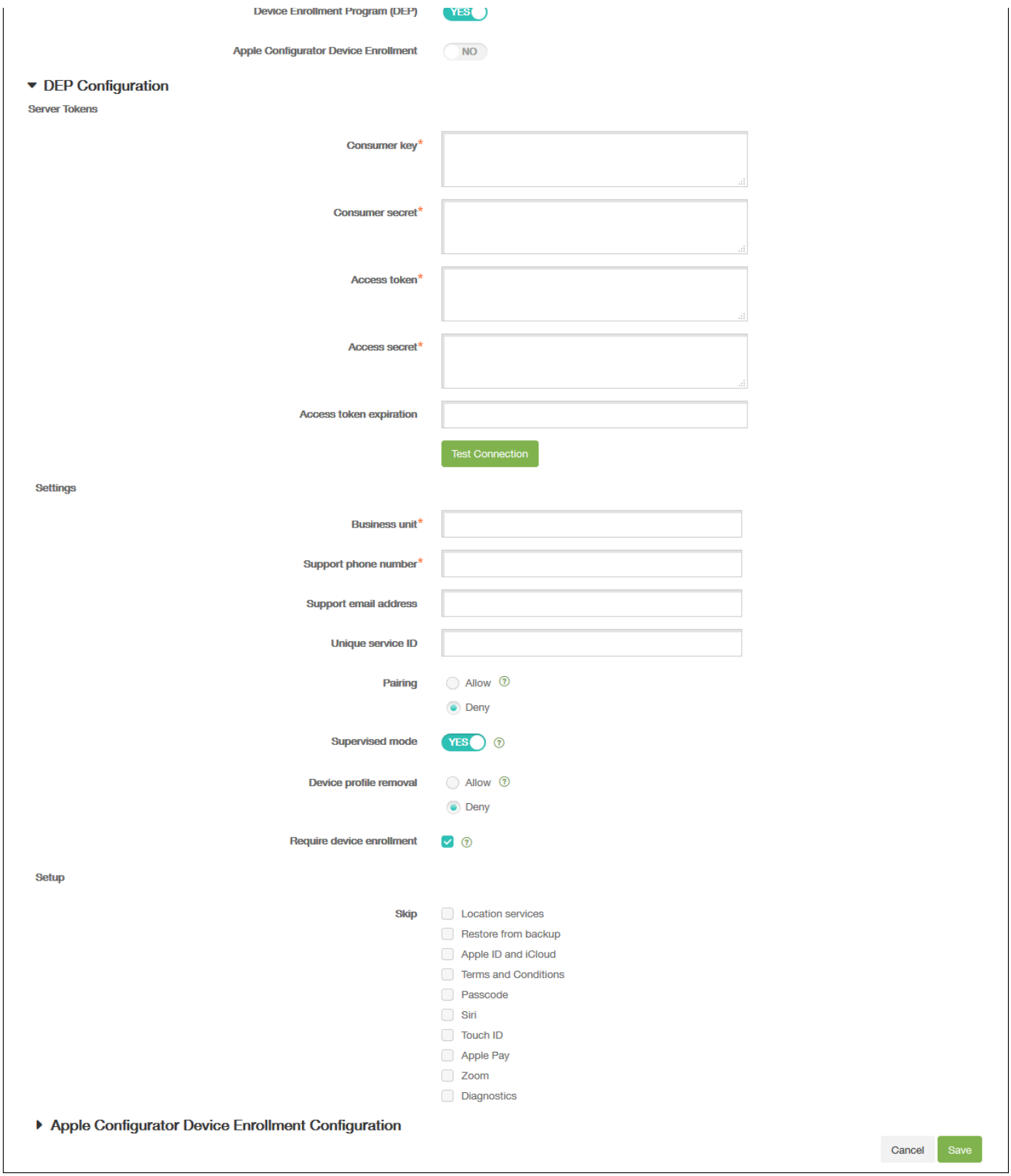


-
-

> Hinweis

Konfigurieren von DEP-Einstellungen





-
-
-
-
-

-
-
-
-
-

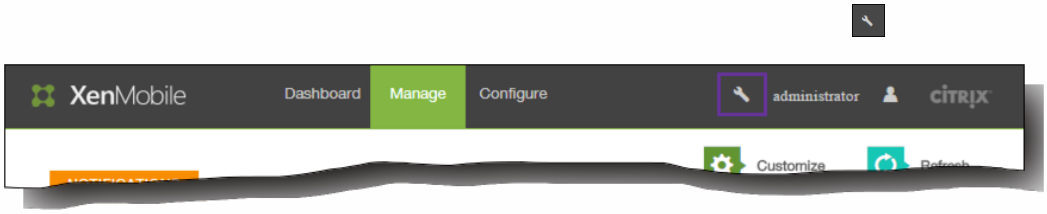
-

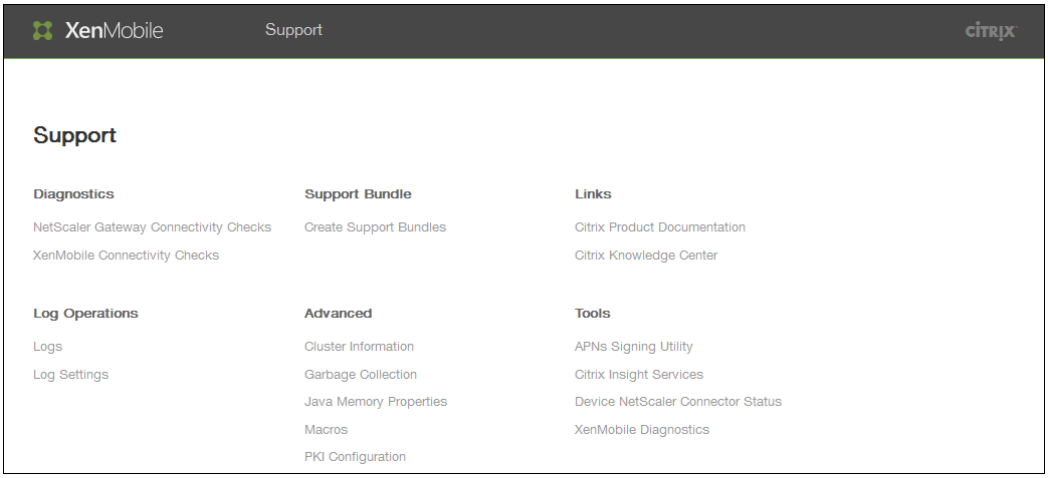
-

-

-
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -

Support und Wartung von XenMobile





-
-
-
-
-
-

Referenz zur XenMobile REST-API

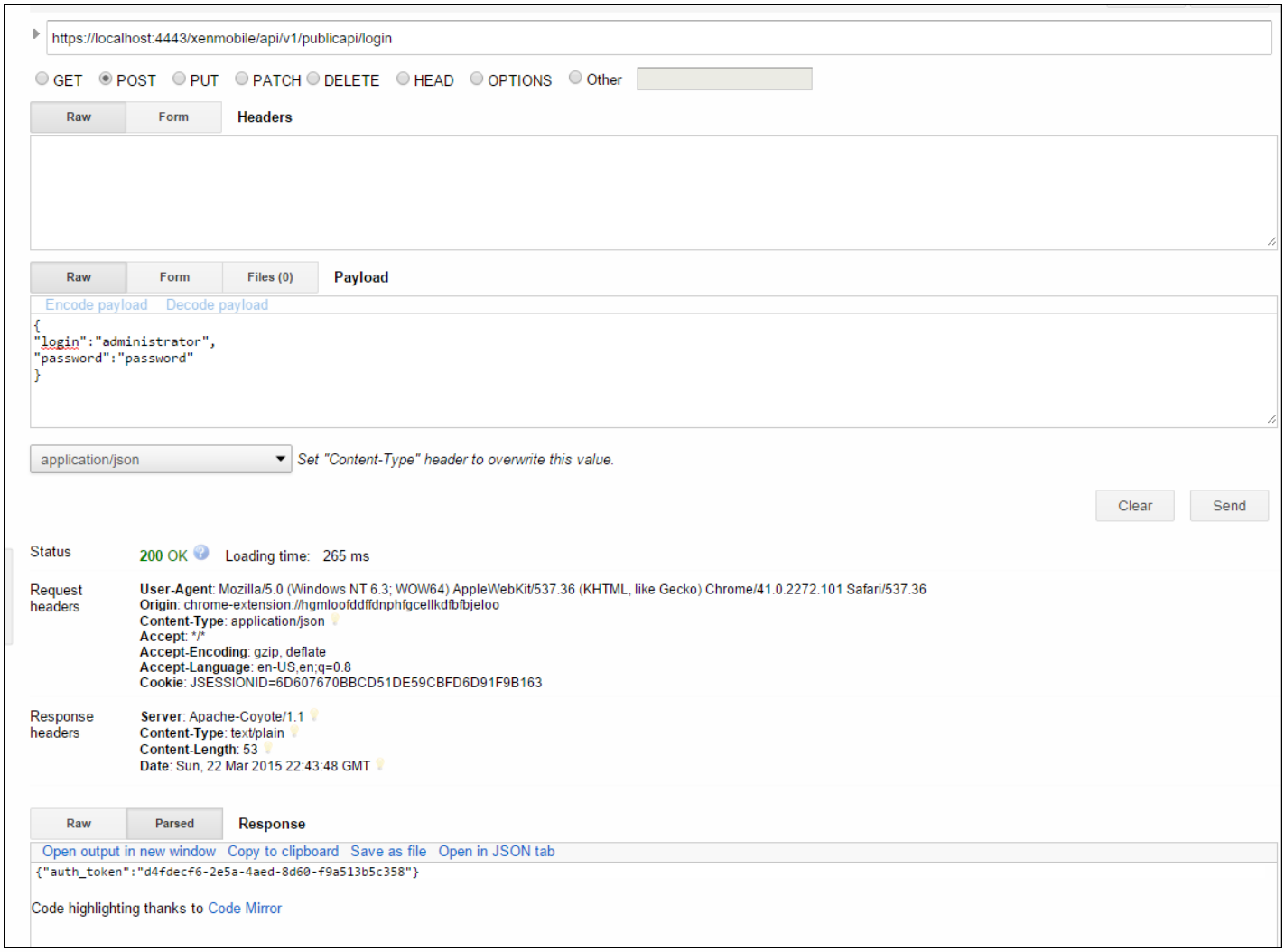
-
-

So rufen Sie REST-API-Dienste auf

> Hinweis

Verwenden eines REST-Clients

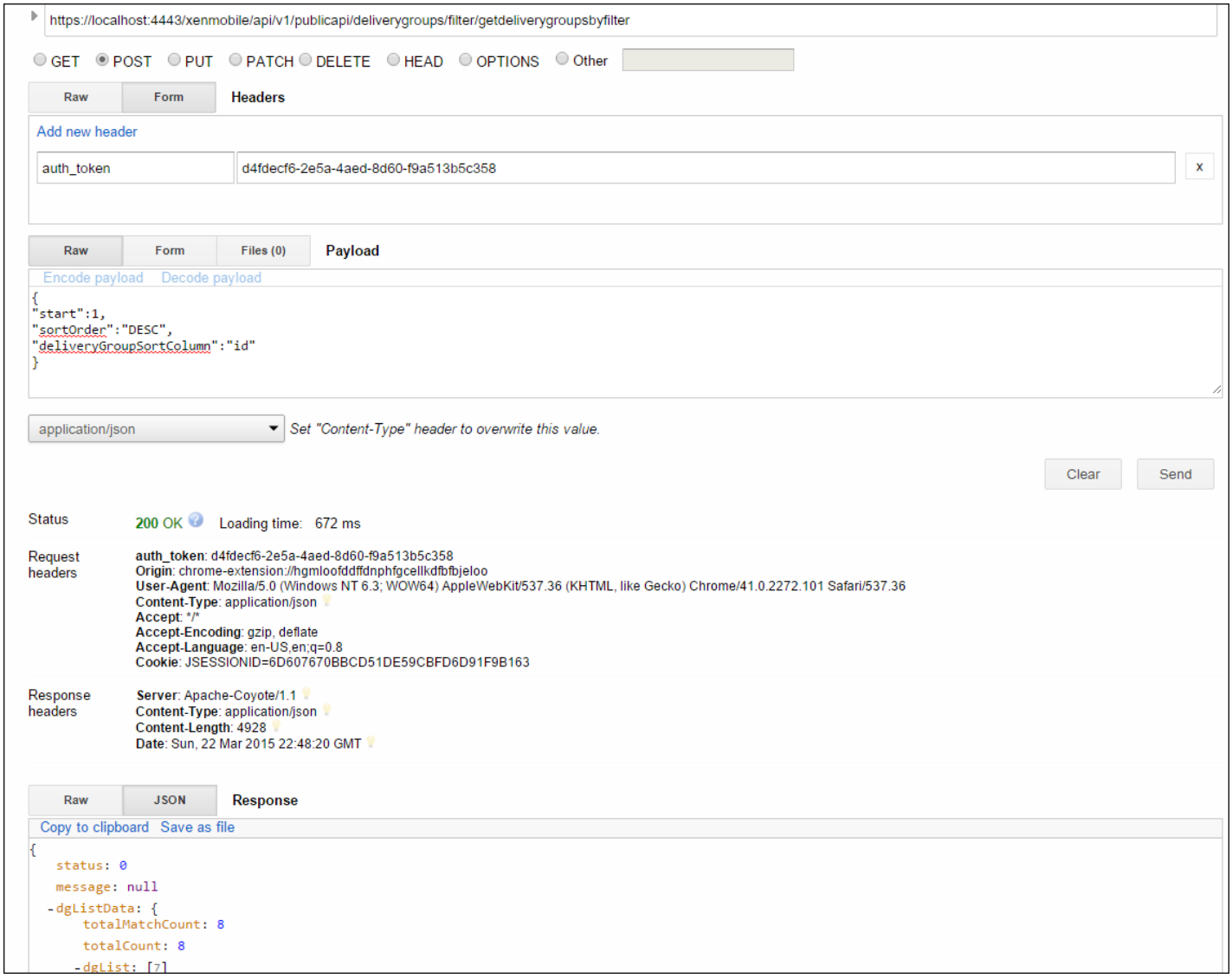
Login



Abruf von Bereitstellungsgruppen per Filter

Anforderung: KOPIEREN

```
{

        "start": 1,

        "sortOrder": "DESC",

        "deliveryGroupSortColumn":"id",

        "search":"add"

}
```



Öffentliche API REST-Dienste

REST-API-Definitionen

So melden Sie sich bei der öffentlichen API an

Anforderungsparameter KOPIEREN

```
{ "login":"administrator", "password":"password" }
```

Beispielantwort KOPIEREN

```
{

    "auth-token":"q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"

}
```

So melden Sie sich von der öffentlichen API ab

Anforderungsparameter KOPIEREN

```
{“login”:”administrator”}
```

Beispielantwort KOPIEREN

```
{"Status":"user administrator logged out successfully."}
```

So verwalten Sie Zertifikate

Get all certificates

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": null,
    "certificate": [
```

```
{
    "name": "ent-root-ca",
    "description": "test description server 1",
    "validFrom": "2012-02-22",
    "validTo": "2017-02-21",
    "type": "chain",
    "isActive": false,
    "privateKey": "false",
    "ca": null,
    "id": 4656,
    "certDetails": {
        "signatureAlgo": "SHA1WithRSAEncryption",
        "version": null,
        "serialNum": "348237881800118418457268346483687164l3",
        "issuerName": {
            "certString": "DC=com,DC=example,CN=ent-root-ca",
            "emailAddress": null,
            "commonName": "ent-root-ca",
            "orgUnit": null,
```



```
                "org": null,
                "locality": null,
                "state": null,
                "country": null,
                "description": null
            },
            "subjectName": {
                "certString": "DC=com,DC=example,CN=ent-root-ca",
                "emailAddress": null,
                "commonName": "ent-root-ca",
                "orgUnit": null,
                "org": null,
                "locality": null,
                "state": null,
                "country": null,
                "description": null
            }
        }
    }
],
```



```
    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```

Delete certificates

Anforderungsparameter KOPIEREN

```
{“certificateIds”:[“<certificate_id_1>”,”<certificate_id_2>”, ..., "<certificate_id_n>"]}
```

Import certificate as SAML certificate

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'saml',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
```

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

}
```


Import certificate as server certificate

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
```

```
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
        },
        "certificate": null,
        "apnsCheckObj": {
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
        }
}
```


Import certificate as listener certificate

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'listener',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null
```

```
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Create certificate

Anforderungsparameter KOPIEREN

```
{

    "isSelfSign":true,

    "csrRequest":{

    "commonName":"your certificate name",

    "description":"certificate description",

    "org":"organization",

    "orgUnit":"organization unit",

    "locality":"location",

    "state":"CA",

    "country":"US",

    "isSelfSign":true

    },

"validDays":"60",

"keyLength":"1024",

"useAs":"none"

}
```

Beispielantwort KOPIEREN

```
{
    status: 0
    message: "Success"
    csrRequest: ""
    apnsCheck: null
    certificate: null
    apnsCheckObj:
    {
    topicNameMismatch: false
    certExpired: false
    certNotYetValid: false
    malformed: false
    }
}
```

Export certificate

Anforderungsparameter

KOPIEREN

```
{
    "id": "300",
    "password": "1111",
    "exportPrivateKey": true
}
```

So verwalten Sie Schlüsselspeicher

Import a server keystore

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
```

```
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Import SAML keystore

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
}
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
```

```
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Import APNs keystore

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':apns,
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
```

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Import SSL listener keystore

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':"listener",
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

Beispielantwort KOPIEREN

```
{
    "status": 0
```

```
        "status": 0,
        "message": "Success",
        "csrRequest": null,
        "apnsCheck": {
                "topicNameMismatch": false,
                "certExpired": false,
                "certNotYetValid": false,
                "malformed": false
        },
    "certificate": null,
    "apnsCheckObj": {
                "topicNameMismatch": false,
                "certExpired": false,
                "certNotYetValid": false,
                "malformed": false
        }
    }
```


So verwalten Sie Lizenzen

Get license information

Beispielantwort KOPIEREN


```
{
    status: 0
    message: "Success"
    cpLicenseServer: {
        serverAddress: "192.0.2.20"
        localPort: 0
        remotePort: 27000
        serverType: "remote"
        licenseType: "none"
        isServerConfigured: true
        gracePeriodLeft: 0
        isRestartLpeNeeded: null
        isScheduleNotificationNeeded: null
            licenseList: []
```



```
{
    sadate: "2015.1210"
    notice: "Example Systems Inc."
    vendorString: ";LT=Retail;GP=720;UDM=U;LP=90;CL=STD,ADV,ENT;SA=1;ODP=0"
    licensesInUse: 0
    licensesAvailable: 102
    overdraftLicenseCount: 2
    p_E_M: "CXM_ENTU_UD"
    serialNumber: "cxmretailent1000user"
    licenseType: "Retail"
    expirationDate: "01-DEC-2015"
}
licenseNotification:
{
    id: 1
    notificationEnabled: false
    notifyFrequency: 7
    notifyNumberDaysBeforeExpire: 60
    recepientList: ""
    emailContent: "License expiry notice"
```

```
            }

        }

    }
```

Save license information

Anforderungsparameter KOPIEREN

```
{

    "serverAddress": "192.0.2.20",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": "remote",

    "licenseType": "none",

    "isServerConfigured": true,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": true,

    "isScheduleNotificationNeeded": true
```

```
"isScheduleNotificationNeeded": true,
    "licenseList": [],
    "licenseNotification": {
        "id": 1,
        "notificationEnabled": true,
        "notifyFrequency": 20,
        "notifyNumberDaysBeforeExpire": 60,
        "recepientList": "justa.name123@example.com",
        "emailContent": "Licenseexpirynotice"
    }
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success"
}
```

Upload license file

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success"
}
```

Activate license

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success"
    "cpLicenseServer": null
}
```

Remove all licenses

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "isConnected": null
}
```

Test license server

Anforderungsparameter KOPIEREN

```
{
    "serverAddress": "192.0.2.7",
    "localPort": 0,
    "remotePort": 27000,
    "serverType": null,
    "licenseType": null,
    "isServerConfigured": null,
    "gracePeriodLeft": 0,
    "isRestartLpeNeeded": null,
    "isScheduleNotificationNeeded": null,
    "licenseList": [],
    "licenseNotification": null
}
```


Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "isConnected": true
}
```


Get earliest expiration date

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "expiredDate": 1448956800000,
    "daysBeforeExpire": 229,
    "daysInPOC": 0
}
```


So verwalten Sie LDAP-Konfigurationen

List LDAP configuration

Beispielantwort KOPIEREN

```
{
    “result”: [
    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"aaa@example.com","password":"1.pwd","userBaseDN":"dc=
    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"test@xmexample.com","password":"1.pwd","userBaseDN":"d
    ]
}
```


Add new LDAP configuration

Anforderungsparameter KOPIEREN

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```


Beispielantwort KOPIEREN


```
{
    “status”: 0,
    “message”: “LDAP configuration created”
}
```

Edit LDAP configuration

Anforderungsparameter KOPIEREN

```
{
    "primaryHost":"192.0.2.7",
    "secondaryHost":"",
    "port":"389",
    "username":"aaa@example.com",
    "password":"1.pwd",
    "userBaseDN":"dc=example,dc=com",
    "groupBaseDN":"dc=example,dc=com",
    "lockoutLimit":"0",
    "lockoutTime":"1",
    "useSecure":"false",
    "userSearchBy":"upn",
    "domain":"example.com",
    "domainAlias":"exampleAlias",
    "globalCatalogPort":"0",
    "gcRootContext":""
}
```

Set default LDAP configuration

Delete LDAP configuration

List all NetScaler Gateway configurations

Beispielantwort KOPIEREN

```
{

    “result”: [

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false","id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        },

        { "name":"displayName",

        "alias":"",
```

```
            "url":"https://externalURl.com",

            "passwordRequired":"false",

            "logonType":"domain",

            "default":"false",

            "id":"",

            “callback”: [{“callbackUrl”:http://example.com,

            “ip”:”192.0.2.8”}]

            }

      ]

}
```

Add new NetScaler Gateway configuration

Anforderungsparameter KOPIEREN

```
{

    "name":"displayName",

    "alias":"",

    “default”:true, "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “callback”: [{“callbackUrl”:http://example.com,

    “ip”:”192.0.2.8”}]

}
```

Edit NetScaler Gateway configuration

Anforderungsparameter KOPIEREN

```
{

    "name":"displayName",

    "alias":"",

    "url":"https://externalURI.com",

    "passwordRequired":"false",

    "logonType":"domain",

    “default”: true,

    “callback”: [{“callbackUrl”:http://ag.com,

    “ip”:”192.0.2.8”}]

}
```

Delete NetScaler Gateway configuration

Set default NetScaler Gateway configuration

So verwalten Sie die Konfiguration des SMS- und des SMTP-Benachrichtigungsservers

List all SMS and SMTP servers

Beispielantwort KOPIEREN

```
{

    “result”: [

        { "name":"serverName","serverType":"SMS,"active":"true","id":"10"},

        { "name":"serverName2","serverType":"SMTP,"active":"true","id":"10"},

        { "name":"serverName3","serverType":"SMS,"active":"false","id":"10"}

    ]

}
```

Get server details

Beispielantwort SMS KOPIEREN

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Beispielantwort SMTP

KOPIEREN

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.12",

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false",

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Add SMS server configuration

Anforderungsparameter KOPIEREN

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false",

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Edit SMS server configuration

Anforderungsparameter KOPIEREN

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Add SMTP server configuration

Anforderungsparameter KOPIEREN

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false",

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Edit SMTP configuration

Anforderungsparameter KOPIEREN

```
{

    name":"displayName",

    "description":"Edited description",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false",

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Delete server configuration

Set default SMS configuration

Set default SMTP configuration

So verwalten Sie lokale Benutzer und Gruppen

Get all users

Beispielantwort KOPIEREN

```
{
```

```
"status": 0,

"message": "Success",

"result": [

        {

                "userid": 8,

                "username": "admin",

                "password": null,

                "confirmPassword": null,

                "groups": [],

                "attributes": {

                        "company": "example"

                },

                "role": "ADMIN",

                "roles": null,

                "createdOn": "1/10/15 11:42 AM",

                "lastAuthenticated": "1/10/15 11:42 AM",

                "domainName": null,

                "adUser": false,

                "vppUser": false

        }
```



```
    ]

}
```

Get one user

Beispielantwort KOPIEREN

```
{

    "status": 0,

    "message": "Success",

    "result": {

            "userid": 8,

            "username": "admin",

            "password": null,

            "confirmPassword": null,

            "groups": [],

            "attributes": {

                "company": "example"
```

```
                company": "example"

            },

            "role": "ADMIN",

            "roles": null,

            "createdOn": "1/10/15 11:42 AM",

            "lastAuthenticated": "1/10/15 11:42 AM",

            "domainName": null,

            "adUser": false,

            "vppUser": false

        }

}
```

Add user

Anforderungsparameter KOPIEREN

```
{

    "attributes": {

            "badpwdcount": "4",

            "asuseremail": "justa.name@example.com",

            "company": "example",

            "mobile": "4695557854"

            },

    "groups": [

            "MSP"

            ],

    "role": "USER",

    "username": "justaname_XX",

    "password": "password"

}
```

Beispielantwort KOPIEREN

```
{

    "status": 0,
```

```
"message": "Success",
"user": {
    "userid": 0,
    "username": "justaname_XX",
    "password": "password",
    "confirmPassword": null,
    "groups": [
        "MSP"
    ],
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
    },
    "role": "USER",
    "roles": null,
    "createdOn": null,
    "lastAuthenticated": null,
    "domainName": null,
```



```
            "adUser": false,

            "vppUser": false

        }

}
```

Update user

Anforderungsparameter KOPIEREN

```
{

    "attributes": {

            "badpwdcount": "4",

            "asuseremail": "justa.name@example.com",

            "company": "example",

            "mobile": "4695557854"

            },

    "groups": [

            "MSP"

            ],

    "role": "USER",

    "username": "justaname_XX",

    "password": "password"

}
```

Beispielantwort KOPIEREN

```
{

    "status": 0,
```

```
"message": "Success",
"user": {
    "userid": 108,
    "username": "justaname_XX",
    "password": null,
    "confirmPassword": null,
    "groups": [
        "MSP"
    ],
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
    },
    "role": "USER",
    "roles": null,
    "createdOn": "3/27/15 1:10 PM",
    "lastAuthenticated": "3/27/15 1:10 PM",
    "domainName": null,
```



```
            "adUser": false,

            "vppUser": false

        }

}
```

Change user password

Anforderungsparameter KOPIEREN

```
{

    "username": “administrator”,

    “password”: “newPassword”

}
```

Beispielantwort KOPIEREN

Response Errors:

1250 – User id not found

1252 – Failed to reset the password

Password can also be changed in the update local user call.

Delete users

Anforderungsparameter KOPIEREN

```
{ justaname XX }
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```


Delete one user

Beispielantwort KOPIEREN


```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Import provisioning file

Anforderungsparameter KOPIEREN

```
importdata={"fileType:"user"}

uploadfile=<file to be uploaded.csv>
```

Beispielantwort KOPIEREN

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

So verwalten Sie Apps

Get all apps by filter

Anforderungsparameter KOPIEREN

```
{
    "start": 0,
    "limit": 10,
    "orderBy": "name",
    "sortOrder": "desc",
    "searchStr": "justaserver1"
}
```

Get mobile apps by container

Beispielantwort KOPIEREN

```
{
```

```
"status": 0,

"message": "Success",

"result": {

        "id": 14,

        "name": "testApp",

        "description": "",

        "createdOn": null,

        "lastUpdated": null,

        "disabled": false,

        "nbSuccess": 0,

        "nbFailure": 0,

        "nbPending": 0,

        "schedule": {

                "enableDeployment": true,

                "deploySchedule": "NOW",

                "deployScheduleCondition": "EVERYTIME",

                "deployDate": null,

                "deployTime": null,

                "deployInBackground": false

        },
```



```
"iconData": "",
"appType": "MDX",
"categories": [
    "Default"
],
"roles": [],
"workflow": null,
"ios": {
    "displayName": "GoToMeeting",
    "description": "G2MW_IOS_5.3.3_075_01",
    "paid": false,
    "removeWithMdm": true,
    "preventBackup": true,
    "appVersion": "5.3.3.075",
    "minOsVersion": "",
    "maxOsVersion": "",
    "excludedDevices": "",
    "avppParams": null,
    "avppTokenParams": null,
```



```
"rules": null,
"appType": "mobile_ios",
"uuid": "8e69d397-48bb-4f29-a95c-dd7b16665c1c",
"id": 0,
"store": {
    "rating": {
        "rating": 0,
        "reviewerCount": 0
    },
    "screenshots": [],
    "faqs": [],
    "storeSettings": {
        "rate": true,
        "review": true
    }
},
"policies": [
    {
        "policyName": "ReauthenticationPeriod",
        "policyValue": "480",
```



```
            "policyType": "integer",
            "policyCategory": "Authentication",
            "title": "Reauthentication period (minutes)",
            "description": "\nDefines the period before a user is challenged to authenticate again. ",
            "units": "minutes",
            "explanation": null
        },
        {
            "policyName": "BlockJailbrokenDevices",
            "policyValue": "true",
            "policyType": "boolean",
            "policyCategory": "Device Security",
            "title": "Block jailbroken or rooted",
            "description": "\nIf On, the application is locked when the device is jailbroken or rooted.",
            "units": null,
            "explanation": null
        },
        {
            "policyName": "CertificateLabel",
            "policyValue": "",
```



```
                        "policyType": "string",
                        "policyCategory": "Network Access",
                        "title": "Certificate label",
                        "description": "\nThe label for the certificate.\n                                    Default value is empty.\n
                        "units": null,
                        "explanation": null
                    }
                ]
            },
            "android": null,
            "android_knox": null,
            "android_work": null,
            "windows": null,
            "windows_tab": null
        }
    }
```


Get SaaS apps by container

Get public store apps by container

Get Web link apps by container

Delete app container

So verwalten Sie Bereitstellungsgruppenkonfigurationen

Get delivery groups by filter

Anforderungsparameter KOPIEREN

```
{
    "start": 1,
    "sortOrder": "DESC",
    "deliveryGroupSortColumn": "id",
    “limit”:10,
    "search": "add"
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "dgListData": {
        "totalMatchCount": 7,
        "totalCount": 10,
        "dgList": [
```

```
dgList": [

    {

        "id": null,

        "name": "add delivery group 6.0",

        "description": "testing add delivery group 6.0",

        "groups": [

            {

                "id": 1,

                "userListId": 1,

                "name": "MSP",

                "uniqueName": "MSP",

                "uniqueId": "MSP",

                "domainName": "local",

                "primaryToken": 0

            }

        ],

        "zoneId": null,

        "zoneDomain": null,

        "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\":\"001-restrictU

        "disabled": false,
```



```
"lastUpdated": 1427144713353,
"anonymousUser": true,
"roledefLangVersionId": 1,
"applications": [
    {
        "name": "Web Link",
        "required": false
    },
    {
        "name": "GoogleApps_SAML",
        "required": true
    }
],
"devicePolicies": [
    "test terms conditions"
],
"smartActions": [
    "shankar ganesh"
],
"nbSuccess": 0,
```



```
        "nbFailure": 0,
        "nbPending": 0
    },
    {
        "id": null,
        "name": "add delivery group 5.0",
        "description": "testing add delivery group 5.0",
        "groups": [
            {
                "id": 1,
                "userListId": 1,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP",
                "domainName": "local",
                "primaryToken": 0
            }
        ],
        "zoneId": null,
        "zoneDomain": null,
```



```
"rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\":\"001-restrictU

"disabled": false,

"lastUpdated": 1426891345698,

"anonymousUser": true,

"roledefLangVersionId": 1,

"applications": [

    {

        "name": "GoogleApps_SAML",

        "required": true

    },

    {

        "name": "Web Link",

        "required": false

     }

],

"devicePolicies": [

    "test terms conditions"

],

"smartActions": [

    "shankar ganesh"
```



```
                        ],
                        "nbSuccess": 0,
                        "nbFailure": 0,
                        "nbPending": 0
                    }
                ]
            }
}
```

Get delivery group by name

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": null,
```

```
"name": "AllUsers",
"description": "default role",
"groups": [],
"zoneId": null,
"zoneDomain": null,
"rules": null,
"disabled": false,
"lastUpdated": null,
"anonymousUser": false,
"roledefLangVersionId": 1,
"applications": [
    {
        "name": "test mdx",
        "required": false
    },
    {
        "name": "test all",
        "required": false
    },
```



```
        {
            "name": "justa test",
            "required": false
        },
        {
            "name": "test enterprise",
            "required": false
        },
        {
            "name": "name test",
            "required": false
        }
    ],
    "devicePolicies": [
        "test terms conditions"
    ],
    "smartActions": [
        "justa name"
    ],
    "nbSuccess": 0,
```



```
            "nbFailure": 0,

            "nbPending": 0

        }

}
```

Edit delivery group

Anforderungsparameter KOPIEREN

```
{

    "name": "add delivery group 2",

    "description": "Changing the description of the delivery group xxx",

    "groups": [

        {

            "name": "MSP",

            "uniqueName": "MSP",

            "uniqueId": "MSP",

            "domainName": "local"
```

```
        },
        {
            "name":"CN=Users,CN=Builtin,DC=example,DC=com",
            "uniqueName": "Users",
            "uniqueId":"a4169204-45f6-48fb-8a0d-847a3200d47e",
            "domainName": "example.com"
        }
        ],
    "disabled": false,
    "anonymousUser": false,
    "applications": [
        {
            "name": "GoogleApps_SAML",
            "required": true
        },
        {
            "name": "test mdx",
            "required": false
        }
        ],
```

```
    "devicePolicies": [
        {
            "name":"test terms conditions",
            "priority":-1
        }
        ],
    "smartActions": [
        {
            "name":"Smart Action Name 1",
            "priority":-1
        }
        ],
    "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"justa.name@example.com\"},\"ruleId\":\"001-restrictUserPropEmail\"}]
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
```

```
"role": {
        "id": null,
        "name": "add delivery group 2",
        "description": "Changing the description of the delivery group xxx",
        "groups": [
            {
                "id": null,
                "userListId": null,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP",
                "domainName": "local",
                "primaryToken": null
            },
            {
                "id": null,
                "userListId": null,
                "name": "CN=Users,CN=Builtin,DC=example,DC=com",
                "uniqueName": "Users",
```

```
                "uniqueId": "a4169204-45f6-48fb-8a0d-847a3200d47e",
                "domainName": "example.com",
                "primaryToken": null
            }
        ],
    "zoneId": null,
    "zoneDomain": null,
    "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"justa.name@example.com\"},\"ruleId\":\"001-restrictUserPropEm
    "disabled": false,
    "lastUpdated": null,
    "anonymousUser": false,
    "roledefLangVersionId": null,
    "applications": [
        {
         "name": "GoogleApps_SAML",
                "required": true
        },
        {
                "name": "test mdx",
                "required": false
```



```
                }

                ],

            "devicePolicies": [

                "test terms conditions"

                 ],

            "smartActions": [

                "justa name"

                ],

            "nbSuccess": 0,

            "nbFailure": 0,

            "nbPending": 0

        }

}
```

Add delivery group

Anforderungsparameter KOPIEREN

```
{
    "name": "add delivery group 4.0",
    "description": "testing add delivery group 4.0",
    "anonymousUser": true,
    "devicePolicies": [
        {
            "name":"test terms conditions",
            "priority":-1
        }
        ],
        "applications": [
            {
                "name": "GoogleApps_SAML",
                "required": true
            },
            {
                "name": "Web Link",
                "required": false
            }
```

```
        ],
    "devicePolicies": [
        {
            "name":"test terms conditions",
            "priority":-1
        }
        ],
     "smartActions": [
        {
            "name":"Smart Action Name 1",
            "priority":-1
        }
        ],
    "groups": [
        {
            "uniqueName": "MSP",
            "domainName": "local",
            "name": "MSP",
            "uniqueId": "MSP"
        }
```

```
            ],
        "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\"justa.name@exa
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": 16,
        "name": "add delivery group 11.0",
        "description": "testing add delivery group 4.0",
        "groups": [
            {
                "id": null,
                "userListId": null,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP"
```

```
            "uniqueId": "MSP",
            "domainName": "local",
            "primaryToken": null
        }
      ],
    "zoneId": null,
    "zoneDomain": null,
    "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\"justa.name@
    "disabled": false,
    "lastUpdated": null,
    "anonymousUser": true,
    "roledefLangVersionId": null,
    "applications": [
        {
            "name": "GoogleApps_SAML",
            "required": true
        },
        {
            "name": "Web Link",
            "required": false
```



```
                }

                ],

            "devicePolicies": [

                "test terms conditions"

                ],

            "smartActions": [

                "justa name"

                ],

            "nbSuccess": 0,

            "nbFailure": 0,

            "nbPending": 0

        }

}
```


Delete delivery group

Anforderungsparameter KOPIEREN

```
[ "add delivery group 11.0" ]
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "roleNames": [
        "add delivery group 11.0"
    ]
}
```

So verwalten Sie Servereigenschaften

Get all server properties

Beispielantwort KOPIEREN

```
{
```

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": [
        {
            "id": 1,
            "name": "ios.mdm.pki.ca-root.certificatefile",
            "value": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",
            "displayName": "ios.mdm.pki.ca-root.certificatefile",
            "description": "",
            "defaultValue": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",
            "displayFlag": false,
            "editFlag": true,
            "deleteFlag": false,
            "markDeleted": false
        } ,
        {
            "id": 2,
            "name": "ios.mdm.https.host",
            "value": "192.0.2.4",
```



```
        "displayName": "ios.mdm.https.host",
        "description": "",
        "defaultValue": "192.0.2.4",
        "displayFlag": false,
        "editFlag": false,
        "deleteFlag": false,
        "markDeleted": false
    },
    {
        "id": 3,
        "name": "ios.mdm.enrolment.checkRemoteAddress",
        "value": "false",
        "displayName": "iOS Device Management Enrollment - Check Remote Address",
        "description": "",
        "defaultValue": "false",
        "displayFlag": true,
        "editFlag": true,
        "deleteFlag": false,
        "markDeleted": false
    },
```



```
    ]

}
```

Get server properties by filter

Anforderungsparameter KOPIEREN

```
{

    "start": 0,

    "limit": 1000,

    "orderBy": "name",

    "sortOrder": "desc",

    "searchStr": "justaserver1"

}
```

Beispielantwort KOPIEREN

```
{
```

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": [
        {
            "id": 154,
            "name": "justaserver123",
            "value": "justaserver1",
            "displayName": "justarserver display name",
            "description": "justaserver description",
            "defaultValue": "justaserver1",
            "displayFlag": true,
            "editFlag": true,
            "deleteFlag": true,
            "markDeleted": false
        }
    ]
}
```


Add server property

Anforderungsparameter KOPIEREN

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 1",
    "description": "Description 1"
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": null
}
```


Edit server properties

Anforderungsparameter KOPIEREN

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 2",
    "description": "Description 2"
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Reset server properties

Anforderungsparameter KOPIEREN

```
{

    "names": [,

        "justaname7"

        ]

}
```

Beispielantwort KOPIEREN

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```

Delete server properties

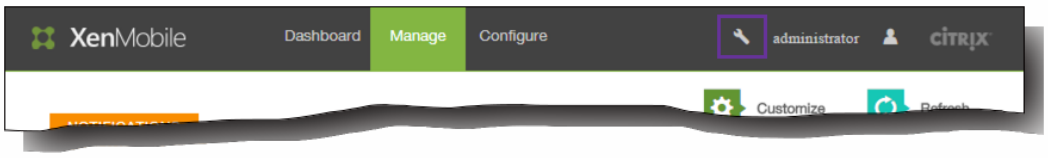
Anforderungsparameter KOPIEREN

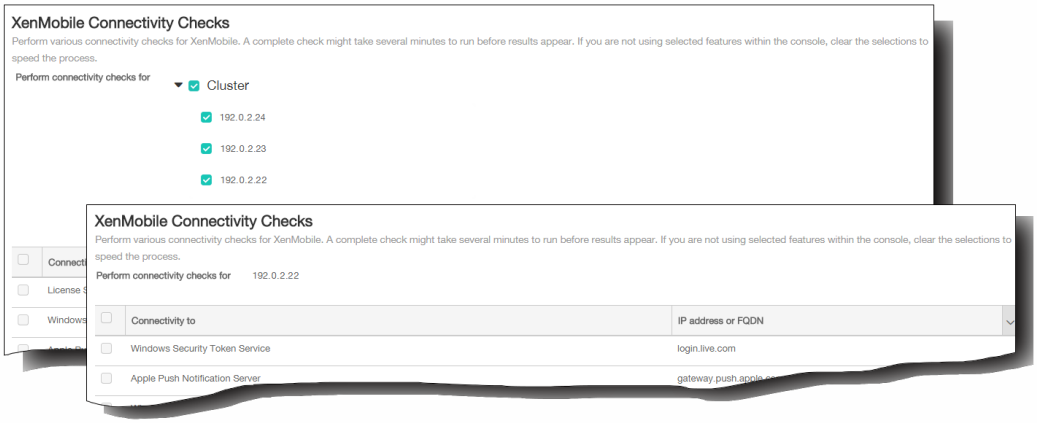
```
{
    "justaname3",
    "justaname4"
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Durchführen von Verbindungsüberprüfungen

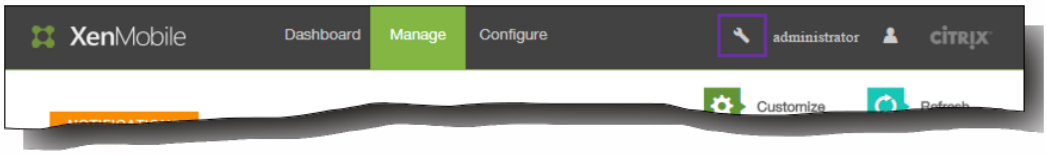


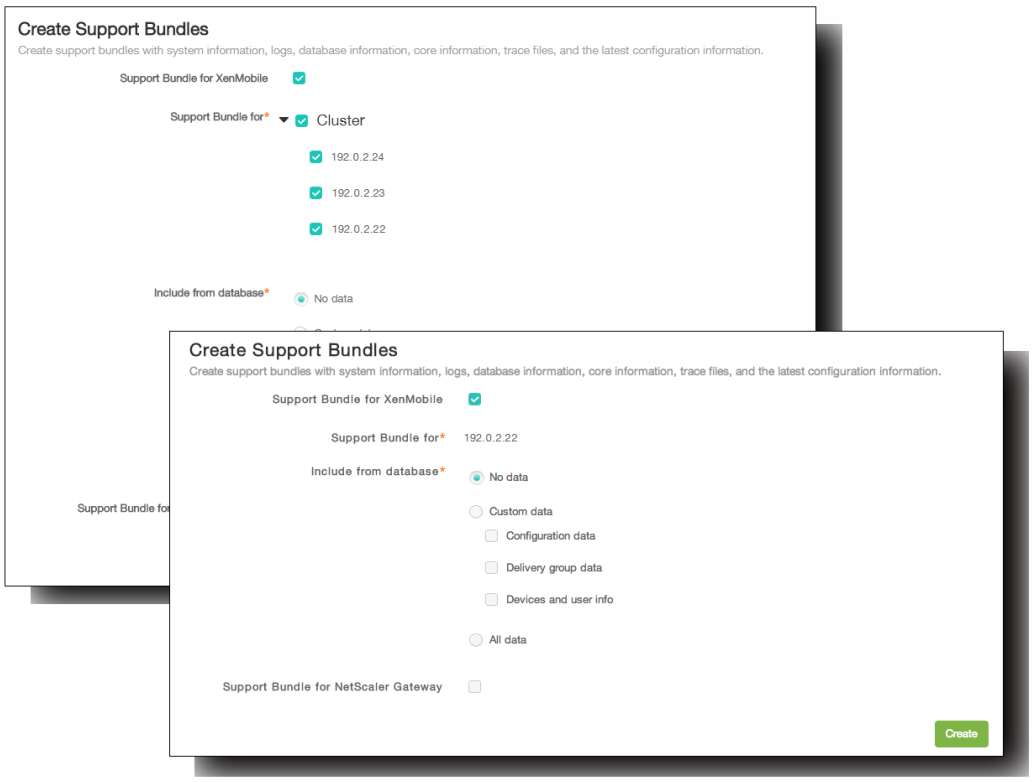


Prüfen von XenMobile-Verbindungen

Prüfen von NetScaler Gateway-Verbindungen

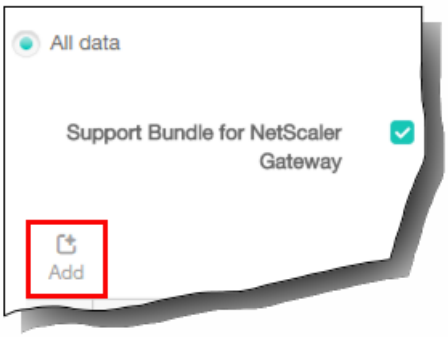
Erstellen von Supportpaketen in XenMobile

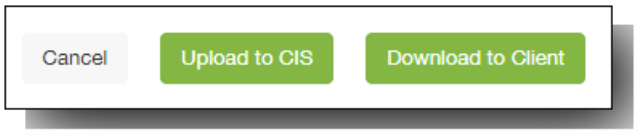




-

-
  -
  -
  -
-

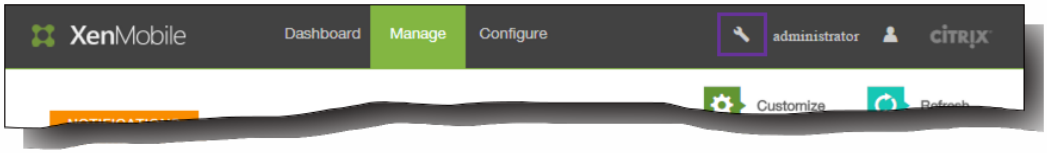


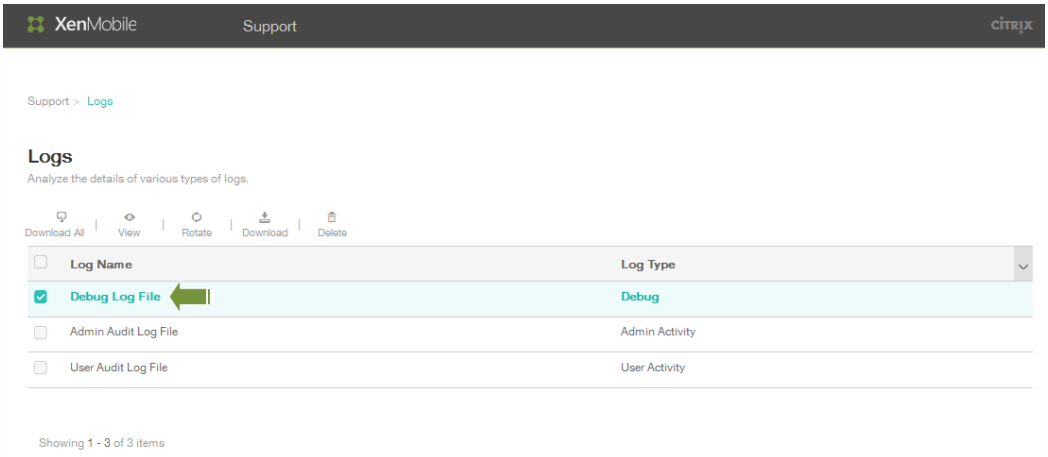


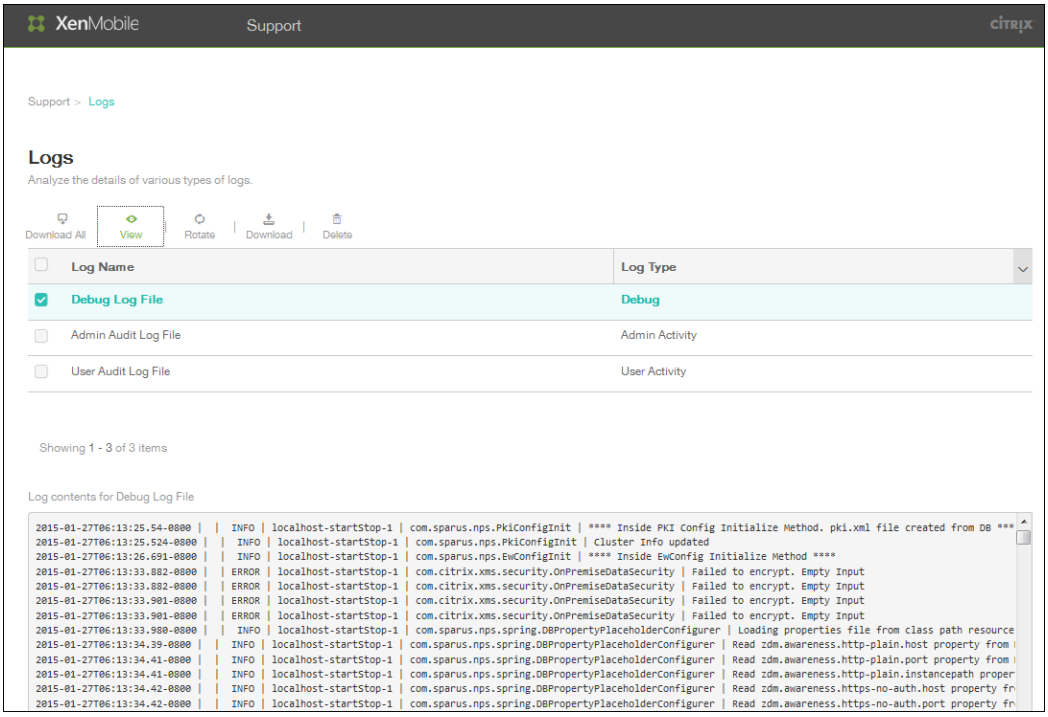
Hochladen von Supportpaketen an Citrix Insight Services

Herunterladen von Supportpaketen auf einen Client

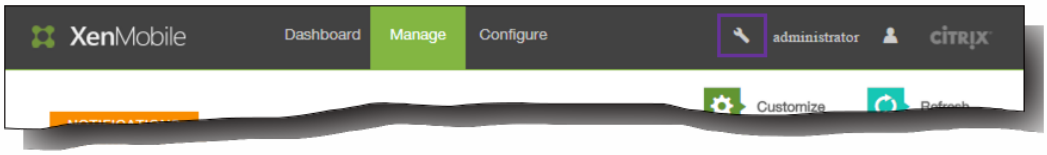
So zeigen Sie die Debugprotokolldatei an

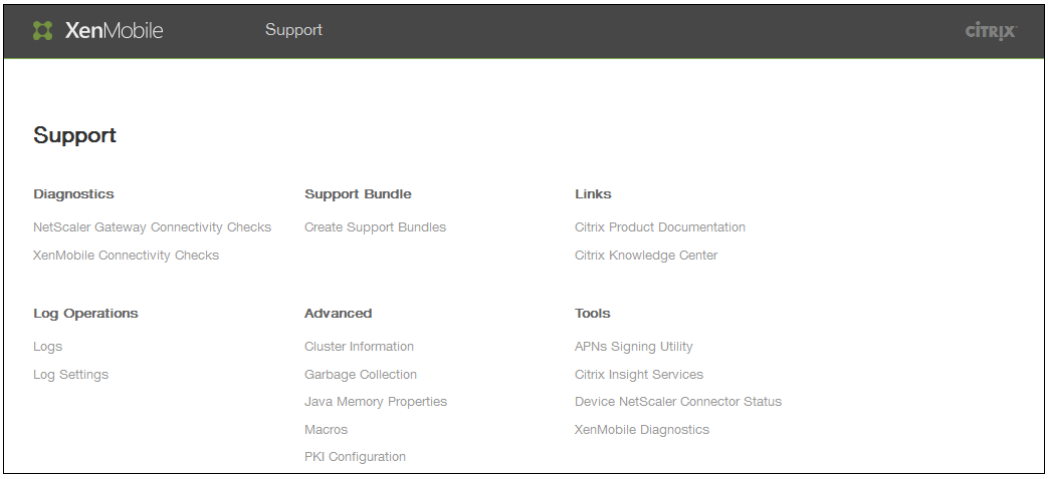






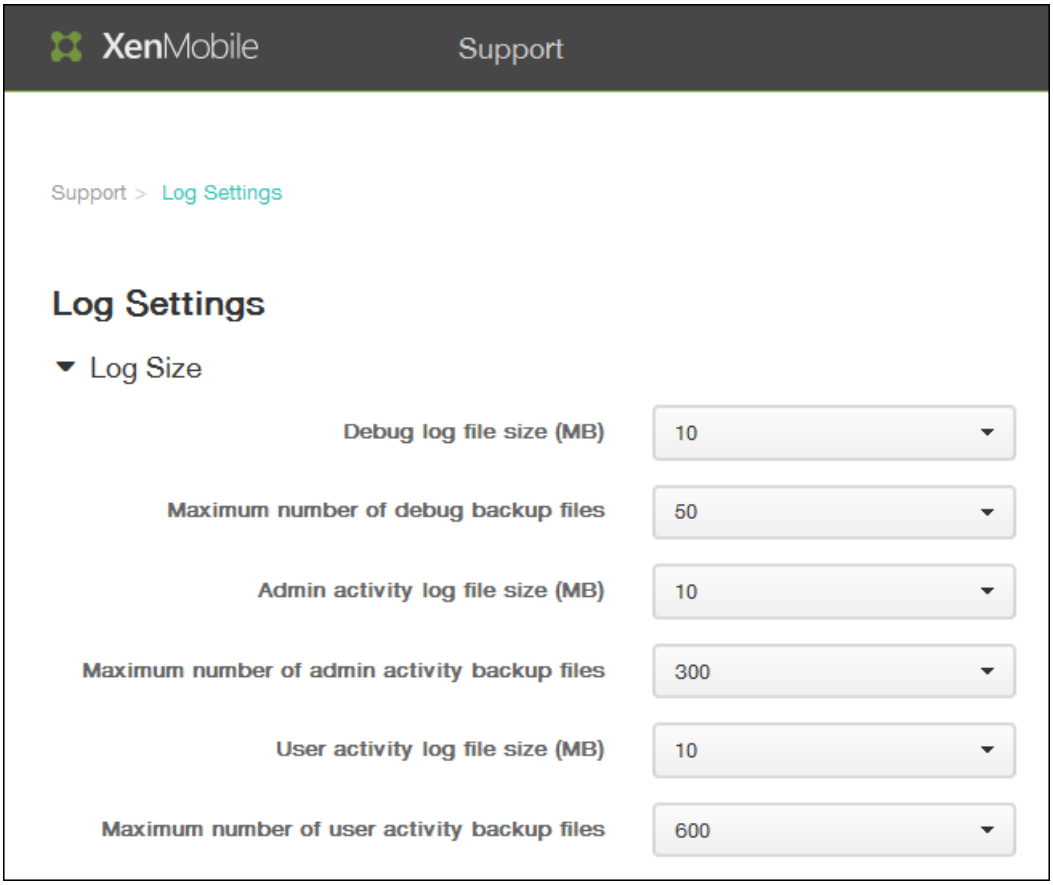
So konfigurieren Sie die Einstellungen für Protokolle



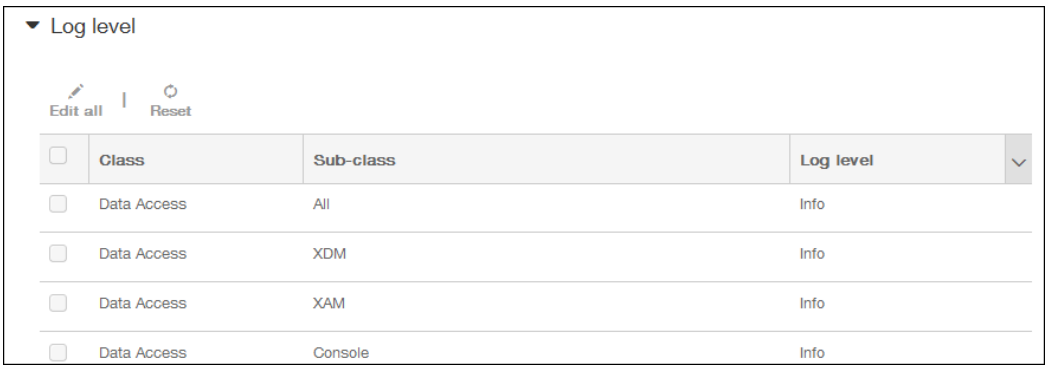


-
-
-

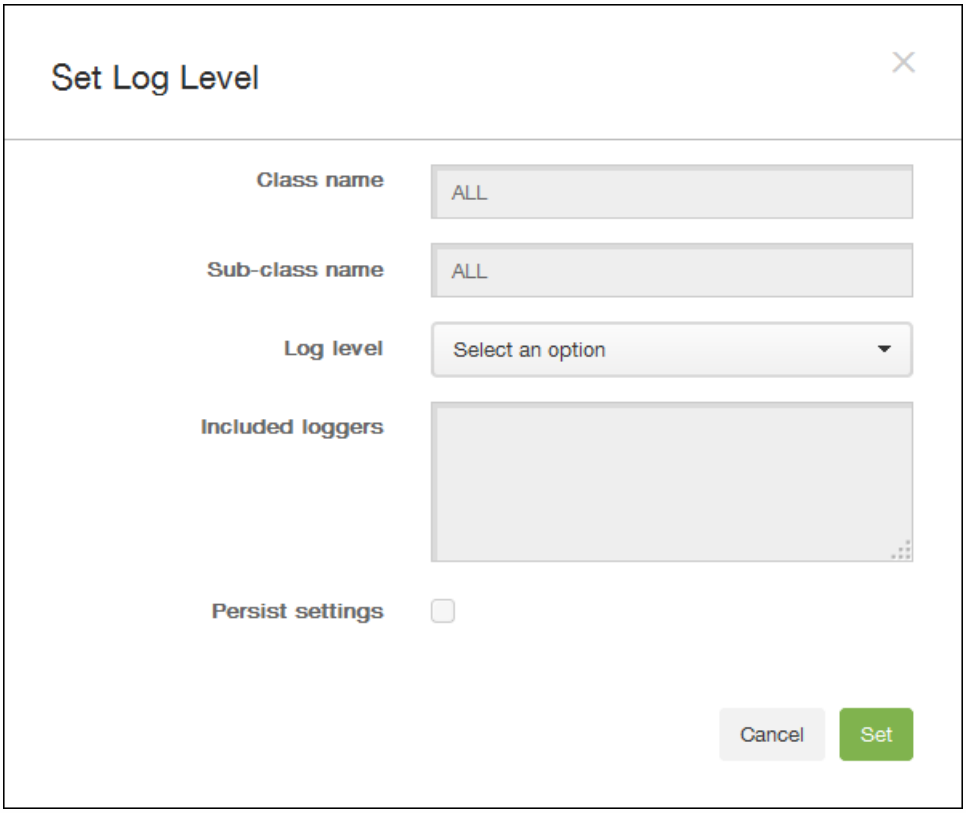
So konfigurieren Sie die Protokollgrößenoptionen



So konfigurieren Sie die Protokollebene

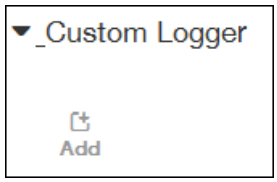


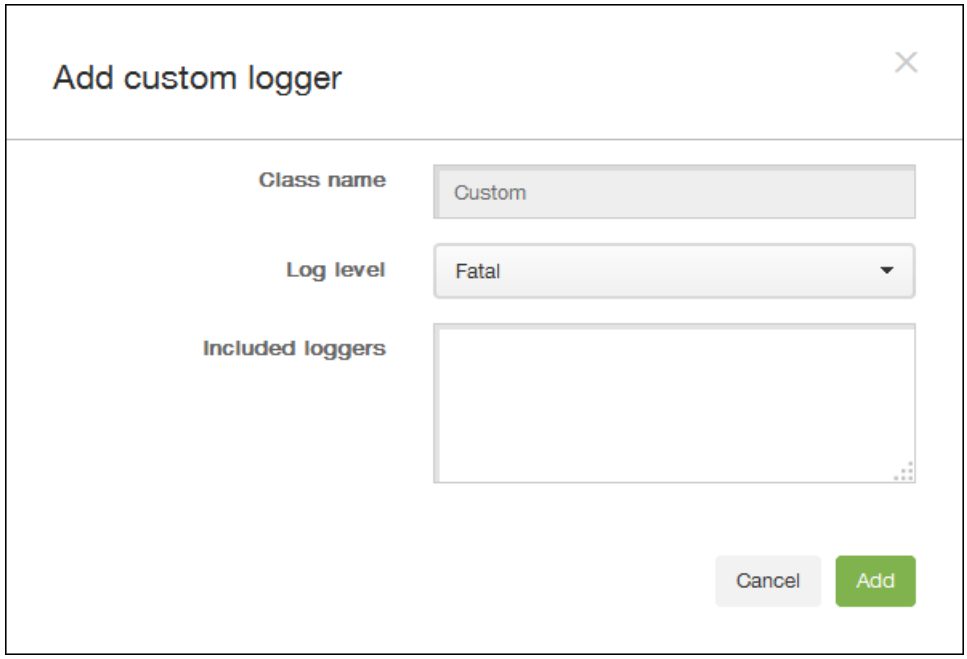
-
-



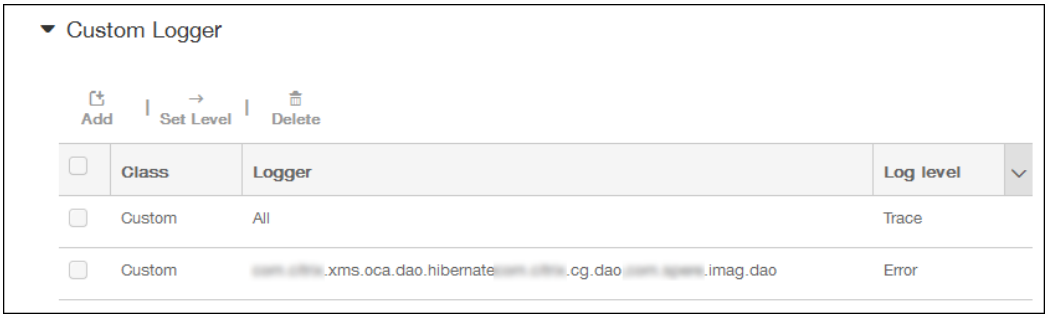
-
-
-
-
-
-
-

So fügen Sie eine benutzerdefinierte Protokollierung hinzu



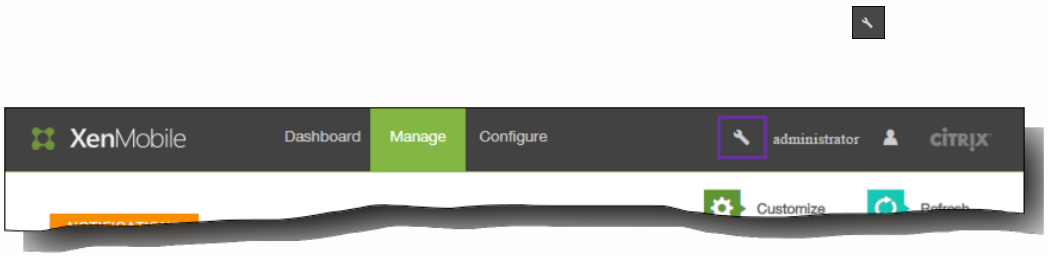


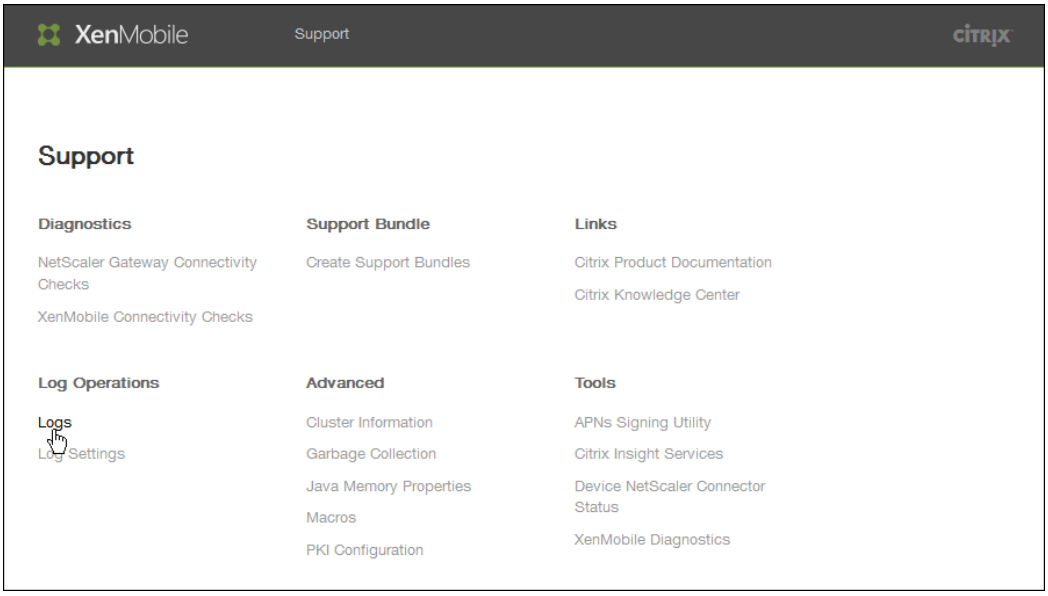
-
-
-
-
-
-
-

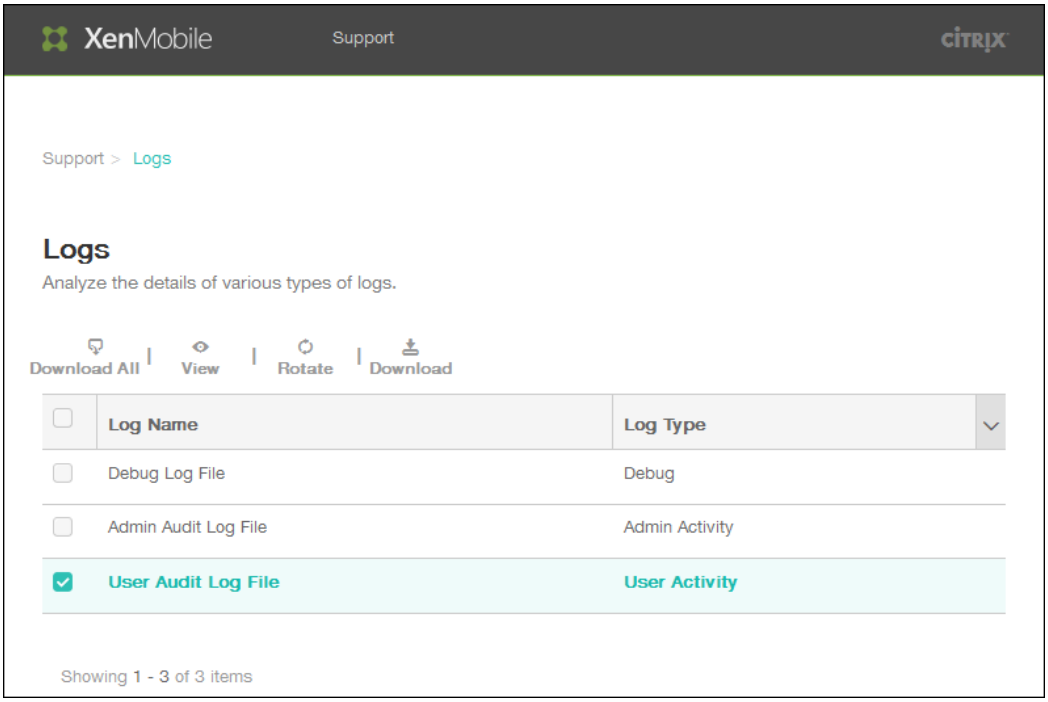


So löschen Sie eine benutzerdefinierte Protokollierung

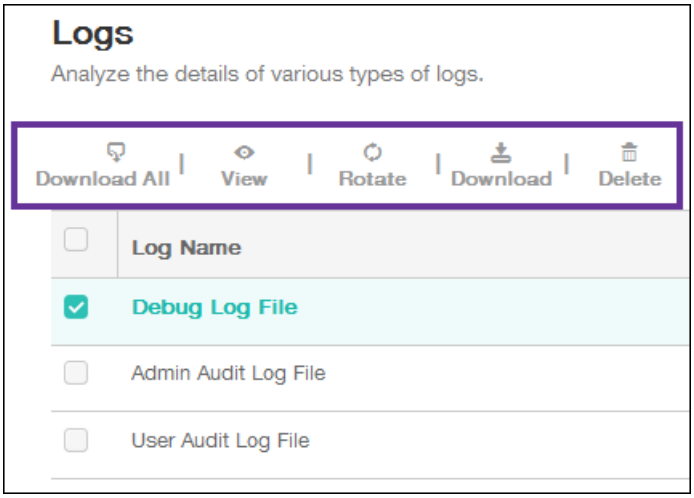
Anzeigen und Analysieren von Protokolldateien in XenMobile



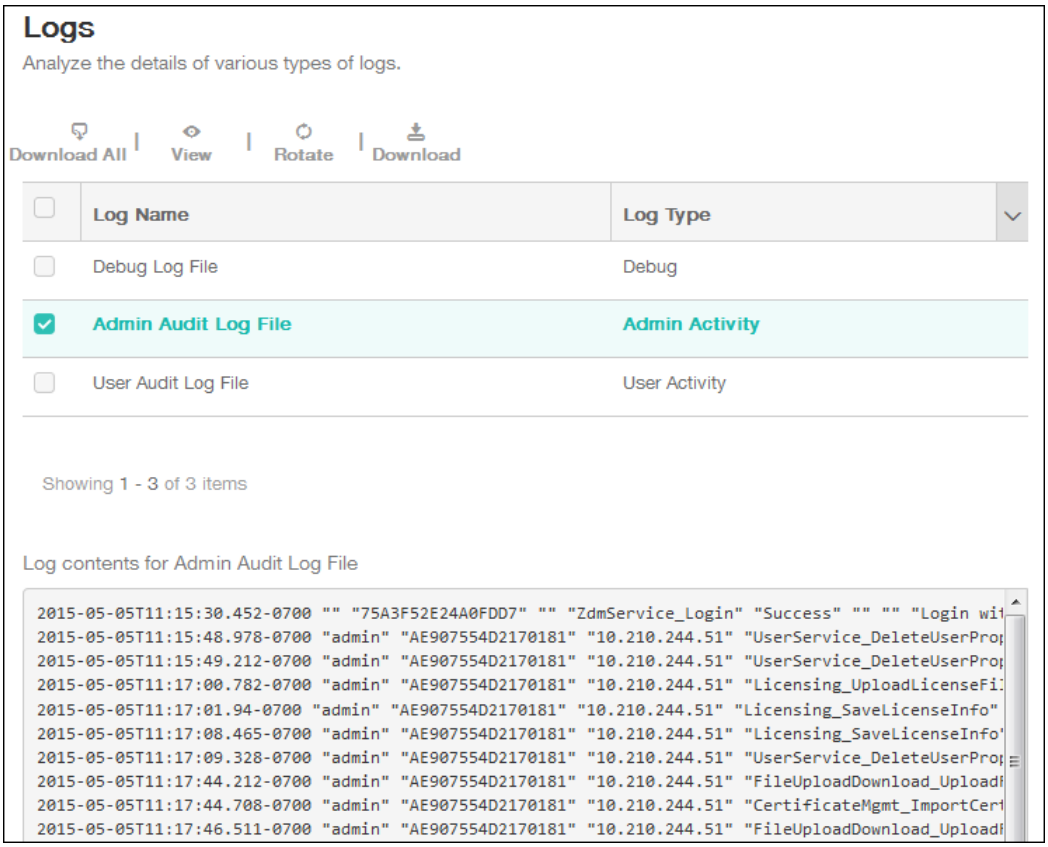


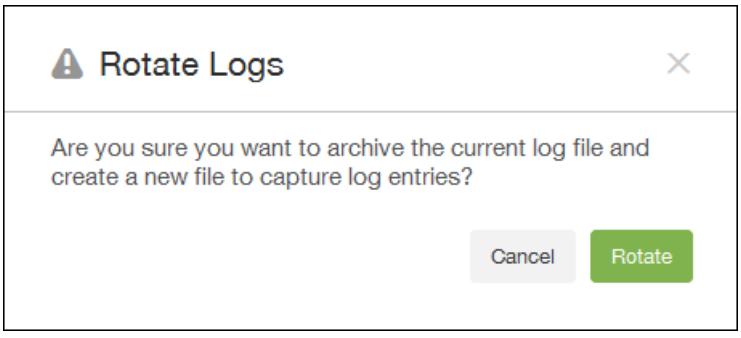


-
-
-
-
-



-

- 

- 

-
-

Optionen für die XenMobile-Befehlszeilenschnittstelle

Hauptmenü

---

[0] Configuration

[1] Clustering

[2] System

[3] Troubleshooting

[4] Help

[5] Log Out

Choice: [0 - 5]

Optionen des Menüs "Configuration"

[0] Back to Main Menu

[1] Network

[2] Firewall

[3] Database

[4] Listener Ports

Choice: [0 - 4]

Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:

- comma separated list of hosts or networks

- e.g. 10.20.5.3, 10.20.6.0/24

- an empty value means no access restriction

- enter c as value to clear list

HTTP service

Port: 80

Enable access (y/n) [y]:

Management HTTPS service

Port: 4443

Enable access (y/n) [y]:

SSH service

Port [22]:

Enable access (y/n) [y]:

Access white list []:

Management API (for initial staging) HTTPS service

Port [30001]:

Enable access (y/n) [y]:

Access white list []:

Remote Support-Tunnel

Port [8081]:

Enable access (y/n) [n]:

Type: [mi]

Use SSL (y/n) [y]:

Upload Root Certificate (y/n) [y]:

Copy or Import (c/i) [c]:

Optionen des Menüs "Clustering"

[0] Back to Main Menu

[1] Show Cluster Status

[2] Enable/Disable cluster

[3] Cluster member white list

[4] Enable or Disable SSL offload

[5] Display Hazelcast Cluster

Choice: [0 - 5]

To enable realtime communication between cluster members, please open port 80 using the Firewall menu option in CLI menu. Also configure Access white list under Firewall settings for restricted access.

You have chosen to disable clustering. Access to port 80 is not needed. Please disable it.

Cluster is disabled. Please enable it.

Current White List:

- comma separated list of hosts or network

- e.g. 10.20.5.3, 10.20.6.0/24

- an empty value means no access restriction

Please enter hosts or networks to be white listed:

Enabling SSL offload will open port 80 for everyone. Please configure Access white list under Firewall settings for restricted access.

Hazlecast Cluster Members:

[IP address listed]

NOTE: If an configured node is not part of the cluseter, please reboot that node.

Optionen des Menüs "System"

---

[0] Back to Main Menu

[1] Display System Date

[2] Set Time Zone

[3] Display System Disk Usage

[4] Update Hosts File

[5] Proxy Server

[6] Admin (CLI) Password

[7] Restart Server

[8] Shutdown Server

[9] Advanced Settings

Choice: [0 - 9]

Optionen des Menüs "Troubleshooting"

---

[0] Back to Main Menu

[1] Network Utilities

[2] Logs

[3] Support Bundle

Choice: [0 - 3]

Choice: [0 - 7]

Logs Menu

---

[0] Back to Troubleshooting Menu

[1] Display Log File

Choice: [0 - 1]

XenMobile APIs

Nov 12, 2015

Sie können in XenMobile für die Mobilgeräteverwaltung die folgenden Webdienst-APIs verwenden. APIs und SDKs für XenMobile können Sie von der XenMobile Developer Community-Website herunterladen.

WSDL-Name (Web Service Definition Language)	Aufruf
EveryWanDevice	addDevice
	addDevice
	authenticateUser
	authorize
	canCreateUser
	clearDeploymentHisto
	corporateDataWipeDevice
	createUser
	deploy
	deviceExists
	disableTrackingDevice
	enableTrackingDevice
	findDeviceByUdid
	getAllDevices
	getDeploymentHisto
	getDeploymentHisto
	getDeviceInfo
	getDeviceInformationForUser
	getDeviceProperties
	getLastUser
	getManagedStatus

WSDL-Name (Web Service Definition Language)	Aufruf
	getMasterKeyList
	getSoftwareInventory
	getStrongID
	getUserDevices
	isEnforceSSL
	isEnforceStrongAuthentication
	locateDevice
	lockDevice
	putDeviceProperties
	registerDeviceForUser
	removeDevice
	resetDeploymentState
	revoke
	unlockDevice
	wipeDevice
	addDevice
CiscoISE/NAC	action/pinlock
	/mdminfo
	/devices/0/all
	/devices/0/macaddress/
	/batchdevices/0/macaddress/all
OTPServices	createOTP
	getAvailableEnrollmentModes
	getOtpInfo
	triggerNotification

XenMobile Mail Manager 10

Apr 12, 2016

XenMobile Mail Manager bietet die Funktionalität, die die Funktionen von XenMobile auf folgenden Weise erweitert:

- Dynamische Zugriffssteuerung für Exchange ActiveSync-Geräte (EAS). EAS-Geräten kann der Zugriff auf Exchange-Dienste automatisch erlaubt oder verweigert werden.
- Zugriff von XenMobile auf durch Exchange bereitgestellte EAS-Gerätepartnerschaftsinformationen.
- Funktionalität für EAS-Löschen des mobilen Geräts durch XenMobile.
- Zugriff von XenMobile auf Informationen über Blackberry-Geräte und Steuerungsvorgäng wie Löschen und Kennwort zurücksetzen.

Die folgenden bekannten Probleme wurden im aktuellen Release von XenMobile Mail Manager 10.0 behoben. Zum Herunterladen von XenMobile Mail Manager navigieren Sie auf Citrix.com zum Abschnitt "Server Components" unter XenMobile 10 Server.

- Die installierte Version von XenMobile Mail Manager wird während des Upgrades auf XenMobile Mail Manager 10 immer als 8.5 angezeigt. Das Upgrade auf XenMobile Mail Manager erfolgt jedoch. [#539520]
- Die Erfassung von "devices found" im kleineren Snapshot kann zu Verwirrung führen. Die gleichen Geräte werden in den aufeinanderfolgenden Zusammenfassungen für kleinere Snapshots möglicherweise als "new" erfasst, wenn kleinere Snapshots nach dem Start eines großen Snapshots ausgeführt werden.

Power Shell/Exchange-Verwaltung

In bestimmten Microsoft Exchange-Umgebungen (primär Office 365) gibt es eine Einschränkung für XenMobile Mail Manager, die die Bandbreite limitiert und verhindert, dass Apps PowerShell-Anfragen oder -Befehle ausgeben. Sie können jetzt einen anderen PowerShell-Cmdlet-Pfad auf der Registerkarte für die Exchange-Konfiguration verwenden, wodurch XenMobile Mail Manager in einen alternativen Snapshotmodus versetzt wird, der den ursprünglichen Datenpfad umgeht.

Ein neues Flag ermöglicht das Verfügbarmachen des Flags **AllowRedirection** für andere Umgebungen als Microsoft Office 365. Verwenden Sie die Registerkarte für die Exchange-Konfiguration zum Aktivieren dieses Flags.

Regelverwaltung

Lokale LDAP-Regeln unterstützen jetzt eine unbegrenzte Zahl Gruppen für große Active Directory-Umgebungen.

XenMobile dupliziert Geräteinformationen für WorxMail-Clients. Zur Beseitigung dieses Problems müssen Sie die Unterstützung für reguläre Ausdrücke im Bereich "Managed Service Provider" (MSP) von XenMobile Mail Manager aktivieren, damit die an XenMobile zurückgegebenen Datensätze gefiltert werden. Geräte, die dem Filter entsprechen, werden nicht an XenMobile zurückgegeben.

MSP

Benutzer, die aus der BlackBerry Enterprise Server-Datenbank entfernt werden, werden nun auch aus der lokalen Datenbank entfernt.

Benutzeroberfläche

Sie können jetzt eine Fortschrittsdialogfeld-Klasse für Szenarios verwenden, bei denen ein persistenter Prozess abläuft. Bei einem solchen Prozess sendet XenMobile Mail Manager den Benutzern Feedback und ermöglicht ihnen ggf. den Vorgang abzubrechen.

Der Standardwert für neue Microsoft Exchange-Instanzen ist jetzt *Shallow*.

Installer

Komponenten, die auf Zenprise verweisen, wurden für XenMobile Mail Manager entsprechend geändert.

Der Installer bleibt hängen, wenn er den Installationspfad nicht findet.

Support-Binärdateien und -Skripts residieren jetzt nach der Installation im Ordner "Support".

Im Windows-Startmenü residieren XenMobile Mail Manager-Verknüpfungen jetzt im Ordner "\Citrix\XenMobile Mail Manager".

Support

Das Supportmodell bietet die Möglichkeit der Aktivierung der Problembehandlungsfunktionen durch Hinzufügen einer config.xml-Datei. Mit dieser Datei können Sie Citrix bei der Problembehandlung helfen. In diesem Release von XenMobile Mail Manager gelten diese Funktionen nur für die Bildschirme Add und Edit der Microsoft Exchange-Konfiguration.
Hinweis: Sie können die Problembehandlungsfunktionen auch aktivieren, indem Sie beim Öffnen des Hilfsprogramms für die Konfiguration die Umschalttaste gedrückt halten.

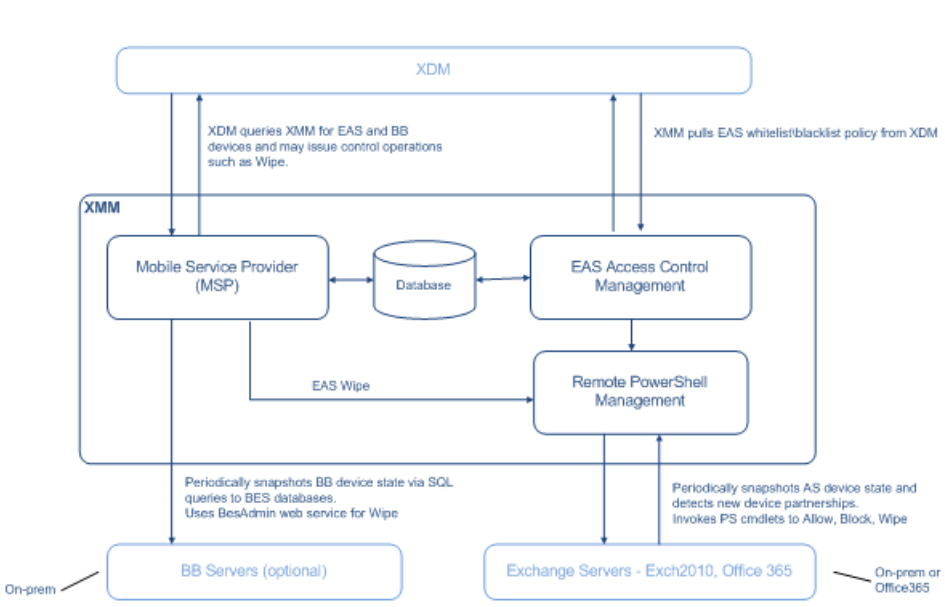
Protokollierung

Von PowerShell zurückgegebene Fehlermeldungen haben jetzt eine GUID. Verwenden Sie diesen Wert, um zu steuern, was auf der Registerkarte mit den Snapshot History-Details angezeigt wird.

Architektur

Oct 11, 2016

Die folgende Abbildung zeigt die wichtigsten Komponenten von XenMobile Mail Manager. Ein detailliertes Architekturdiagramm finden Sie im Artikel Reference Architecture for On-Premises Deployments in der XenMobile-Bereitstellungsdokumentation.



Die drei Hauptkomponenten sind folgende:

- **Exchange ActiveSync Access Control Management**: Ruft eine Exchange ActiveSync-Richtlinie bei XenMobile ab und führt diese mit lokal definierten Richtlinien zusammen, um zu bestimmen, welche Exchange ActiveSync-Geräte Zugriff auf Exchange erhalten sollen. Lokale Richtlinien ermöglichen die Erweiterung der Richtlinienregeln für die Zugriffssteuerung auf der Basis von Active Directory-Gruppe, Benutzer, Gerätetyp oder Gerätebenutzer-Agent (im Allgemeinen die Version der mobilen Plattform).
- **Remote PowerShell Management**: Verantwortlich für das Planen und Aufrufen von Remote-PowerShell-Befehlen für die Anwendung der über Exchange ActiveSync Access Control Management kompilierten Richtlinie. Erstellt in regelmäßigen Abständen einen Snapshot der Exchange ActiveSync-Datenbank zur Erkennung neuer oder geänderter Exchange ActiveSync-Geräte.
- Mobile Service Provider: Bietet eine Webdienstschnittstelle, sodass XenMobile Exchange ActiveSync- und/oder BlackBerry-Geräte abfragen und Vorgänge zu deren Steuerung, etwa die Löschung von Daten, ausgeben kann.

Systemanforderungen und Voraussetzungen

Apr 12, 2016

Die folgenden Mindestsystemanforderungen müssen für XenMobile Mail Manager erfüllt verwenden:

- Windows Server 2008 R2 (muss ein auf Englisch basierender Server sein)
- Microsoft SQL Server 2008, SQL Server 2012, SQL Server Express 2008, SQL Server 2012 oder Microsoft SQL Server 2012 Express LocalDB
- Microsoft .NET Framework 4.5
- Blackberry Enterprise Service, Version 5 (optional)

Mindestens unterstützte Versionen von Microsoft Exchange Server

- Microsoft Office 365
- Exchange Server 2013
- Exchange Server 2010 SP2

- Windows Management Framework installiert
  - PowerShell V4, V3 und V2
- Die PowerShell-Ausführungsrichtlinie muss über Set-ExecutionPolicy RemoteSigned auf RemoteSigned festgelegt werden.
- TCP-Port 80 muss zwischen dem Computer mit XenMobile Mail Manager und dem Remote-Computer mit Exchange Server geöffnet sein.

Anforderungen für lokale Computer mit Exchange

- **Berechtigungen**: Die rollenbasierte Zugriffssteuerung (RBAC) für Exchange geht über den Rahmen dieser Dokumentation hinaus. Prinzipiell muss das im Konfigurations-UI für Exchange festgelegte Konto in der Lage sein, eine Verbindung mit Exchange Server herzustellen und vollständigen Zugriff zum Ausführen der folgenden Exchange-spezifischen PowerShell-Cmdlets erhalten:
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
- Wenn XenMobile Mail Manager zur Anzeige der kompletten Gesamtstruktur konfiguriert ist, muss die Berechtigung zum Ausführen gewährt werden für: Set-AdServerSettings -ViewEntireForest $true
- Die angegebenen Anmeldeinformationen müssen zu einer Verbindung mit Exchange Server über die Remote-Shell berechtigt sein. Standardmäßig hat der Benutzer, der Exchange installiert, diese Berechtigung.
- Laut http://technet.microsoft.com/en-us/library/dd315349.aspx müssen die Anmeldeinformationen zum Herstellen einer Remoteverbindung und Ausführen von Remotebefehlen einem Benutzer entsprechen, der auf dem Remotecomputer Administratorrechte hat. Laut dem Blog http://blogs.msdn.com/b/powershell/archive/2009/11/23/you-don-t-have-to-be-an-administrator-to-run-remote-powershell-commands.aspx kann Set-PSSessionConfiguration verwendet werden, um diese Anforderung zu umgehen, eine Erläuterung dieses Befehls geht jedoch über den Rahmen des vorliegenden Dokuments hinaus.

- Exchange Server muss für die Unterstützung von Remote-PowerShell-Anfragen über HTTP konfiguriert sein. Normalerweise ist nur ein Administrator erforderlich, der folgenden PowerShell-Befehl auf dem Exchange Server ausführt: WinRM quickconfig.
- Exchange hat zahlreiche Einschränkungsrichtlinien. Eine davon steuert, wie viele gleichzeitige PowerShell-Verbindungen pro Benutzer zugelassen sind. In Exchange 2010 ist die Standardzahl gleichzeitiger Verbindungen pro Benutzer 18. Wenn dieses Limit erreicht ist, kann XenMobile Mail Manager keine Verbindung mit Exchange Server herstellen. Es gibt Methoden zum Ändern der Zahl der maximal zulässigen gleichzeitigen Verbindungen über PowerShell, dies geht jedoch über den Rahmen der vorliegenden Dokumentation hinaus. Bei entsprechendem Interesse lesen Sie die Exchange-Dokumentation zu Einschränkungsrichtlinien für die Remoteverwaltung per PowerShell.

Anforderungen für Office 365 Exchange

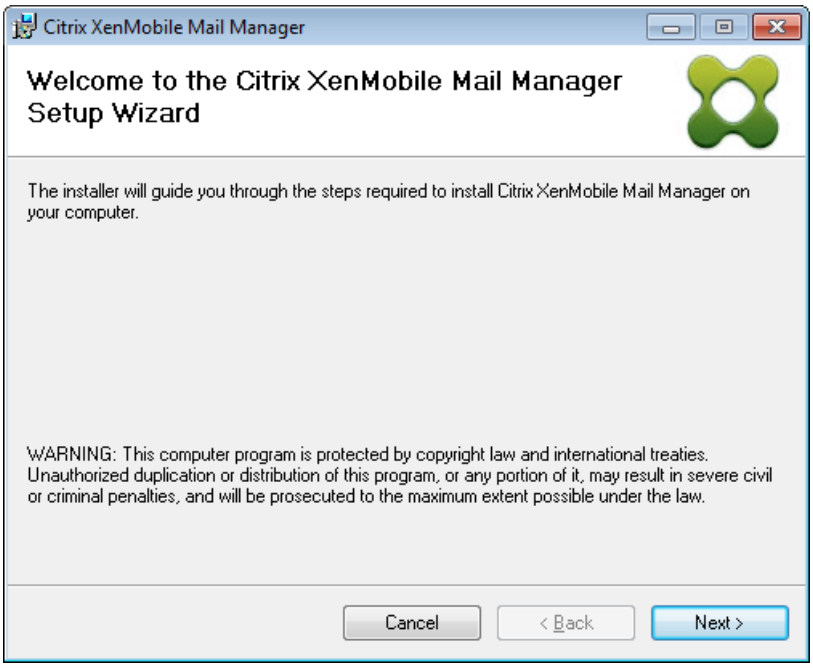
- **Berechtigungen**: Die rollenbasierte Zugriffssteuerung (RBAC) für Exchange geht über den Rahmen dieser Dokumentation hinaus. Prinzipiell muss das im Konfigurations-UI für Exchange festgelegte Konto in der Lage sein, eine Verbindung mit Office 365 herzustellen und vollständigen Zugriff zum Ausführen der folgenden Exchange-spezifischen PowerShell-Cmdlets erhalten:
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
- Die angegebenen Anmeldeinformationen müssen zu einer Verbindung mit dem Office 365-Server über die Remote-Shell berechtigt sein. Standardmäßig besitzt der Office 365-Onlineadministrator die erforderlichen Rechte.
- Exchange hat zahlreiche Einschränkungsrichtlinien. Eine davon steuert, wie viele gleichzeitige PowerShell-Verbindungen pro Benutzer zugelassen sind. In Office 365 ist die Standardzahl gleichzeitiger Verbindungen pro Benutzer 3. Wenn dieses Limit erreicht ist, kann XenMobile Mail Manager keine Verbindung mit Exchange Server herstellen. Es gibt Methoden zum Ändern der Zahl der maximal zulässigen gleichzeitigen Verbindungen über PowerShell, dies geht jedoch über den Rahmen der vorliegenden Dokumentation hinaus. Bei entsprechendem Interesse lesen Sie die Exchange-Dokumentation zu Einschränkungsrichtlinien für die Remoteverwaltung per PowerShell.

Installation und Konfiguration

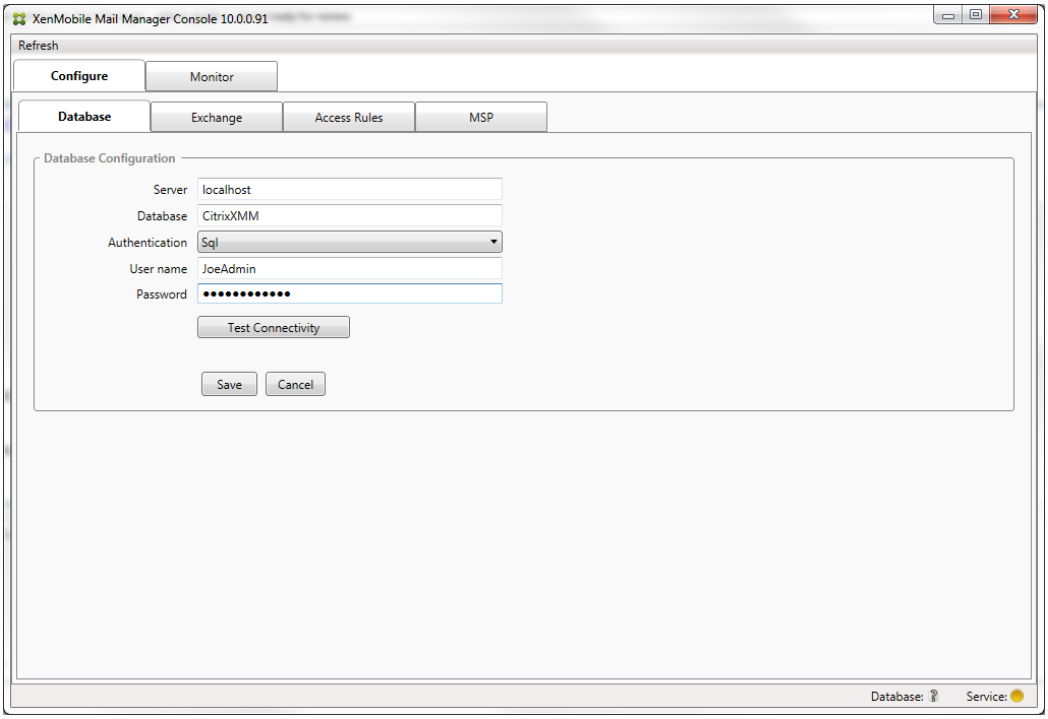
Nov 20, 2015

Führen Sie die folgenden Schritte für die Installation und Konfiguration von XenMobile Mail Manager aus. Lesen Sie vorher die Informationen zu Systemanforderungen und Voraussetzungen. Einzelheiten finden Sie unter Systemanforderungen und Voraussetzungen für XenMobile Mail Manager.

1. Klicken Sie auf die Datei XmmSetup.msi und folgen Sie den Anweisungen des Installers zum Installieren von XenMobile Mail Manager.

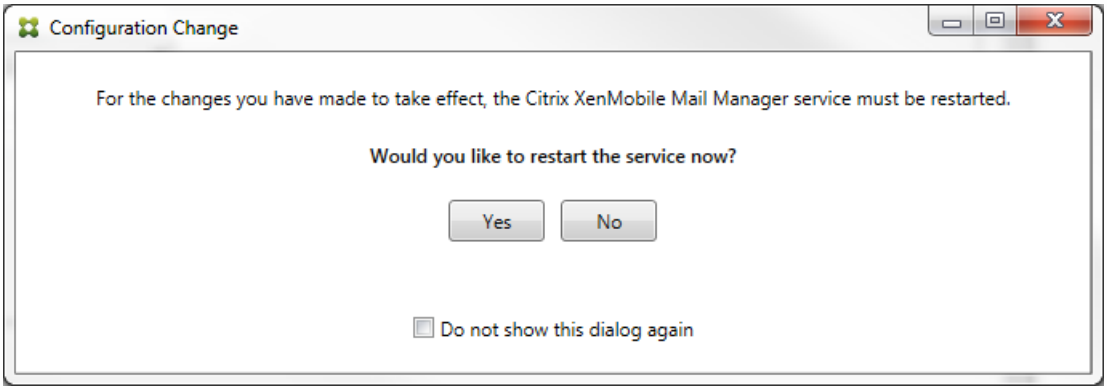


2. Öffnen Sie XenMobile Mail Manager über das Startmenü .
3. Konfigurieren Sie die folgenden Datenbankeigenschaften:
   1. Wählen Sie die Registerkarte Configure > Database.
   2. Geben Sie den Namen des SQL Server-Computers ein (standardmäßig "localhost").
   3. Behalten Sie den Standarddatenbanknamen "CitrixXmm" bei.
   4. Wählen Sie einen der folgenden für SQL verwendeten Authentifizierungsmodi aus:
      - Sql: Geben Sie den Benutzernamen und das Kennwort eines gültigen SQL-Benutzers ein.
      - Windows Integrated: Wenn Sie diese Option auswählen, müssen die Anmeldeinformationen des XenMobile Mail Manager-Diensts in ein Windows-Konto geändert werden, das Zugriff auf den SQL Server-Computer hat. Öffnen Sie hierfür Systemsteuerung > Verwaltung > Dienste, klicken Sie mit der rechten Maustaste auf den XenMobile Mail Manager-Diensteintrag und klicken Sie auf die Registerkarte Anmelden.
        Hinweis: Wenn "Windows Integrated" auch für die BlackBerry-Datenbankverbindung ausgewählt wird, muss dem hier angegebenen Windows-Konto Zugriff auf die BlackBerry-Datenbank erteilt werden.

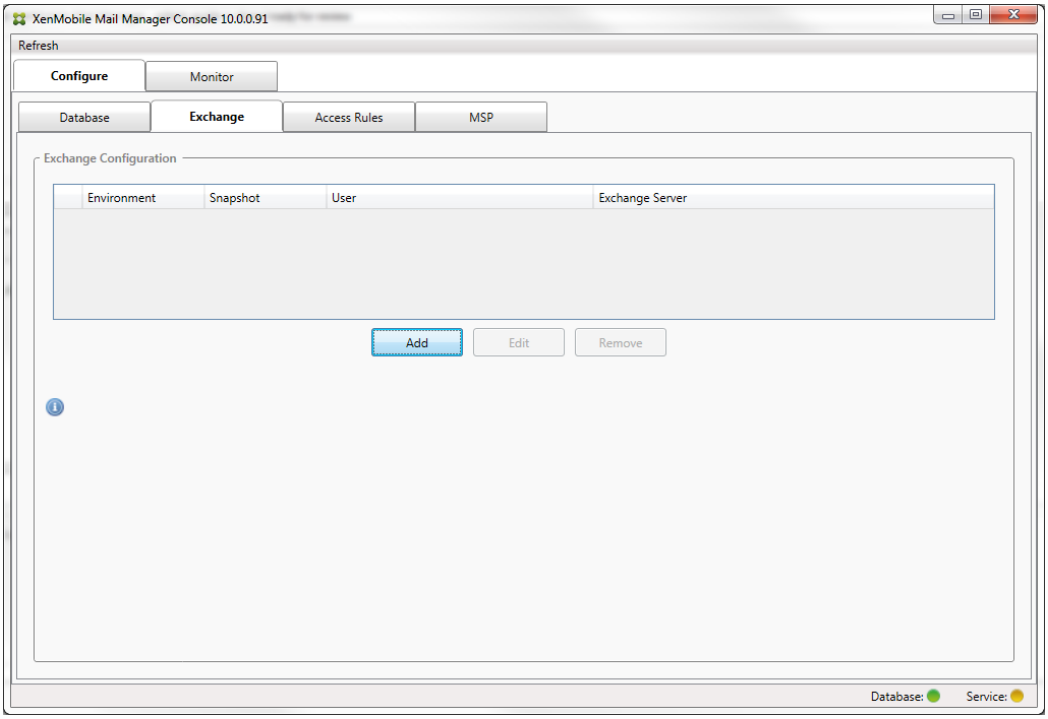


5. Klicken Sie auf Test Connectivity, um zu prüfen, ob eine Verbindung mit dem SQL Server-Computer hergestellt werden kann, und klicken Sie auf Save.

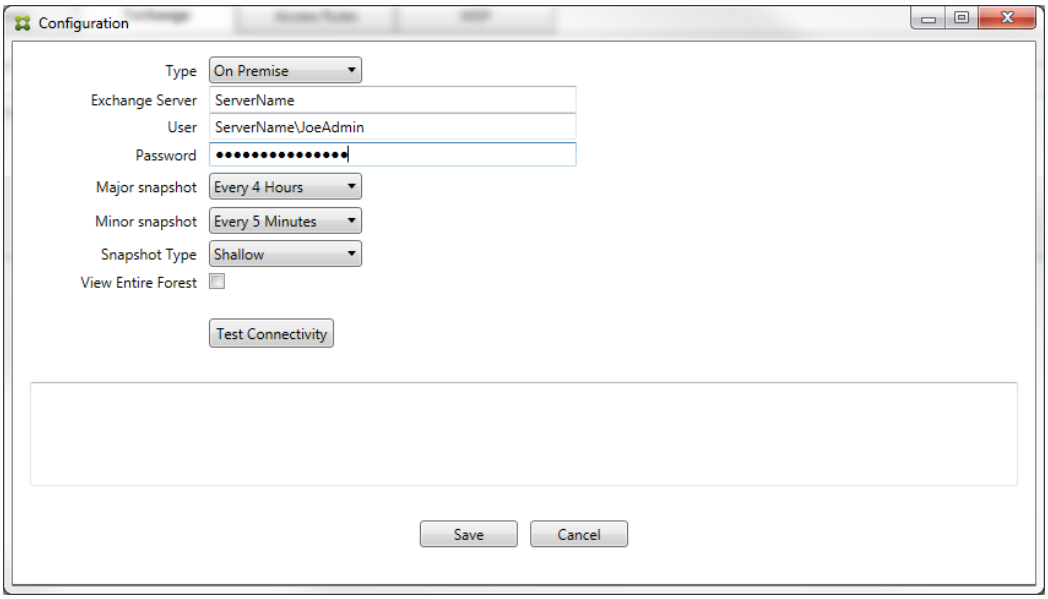
4. Eine Meldung fordert Sie zum Neustarten des Diensts auf. Klicken Sie auf Yes.



5. Konfigurieren Sie einen oder mehrere Exchange Server:
   1. Wenn Sie eine einzelne Exchange-Umgebung verwalten, müssen Sie nur einen Server angegeben. Wenn Sie mehrere Exchange-Umgebungen verwalten, müssen Sie für jede einen separaten Exchange Server-Computer festlegen.
   2. Wählen Sie die Registerkarte Configure > Exchange.



3. Klicken Sie auf Add.
4. Wählen Sie den Typ der Exchange Server-Umgebung aus: entweder On Premise oder Office 365.

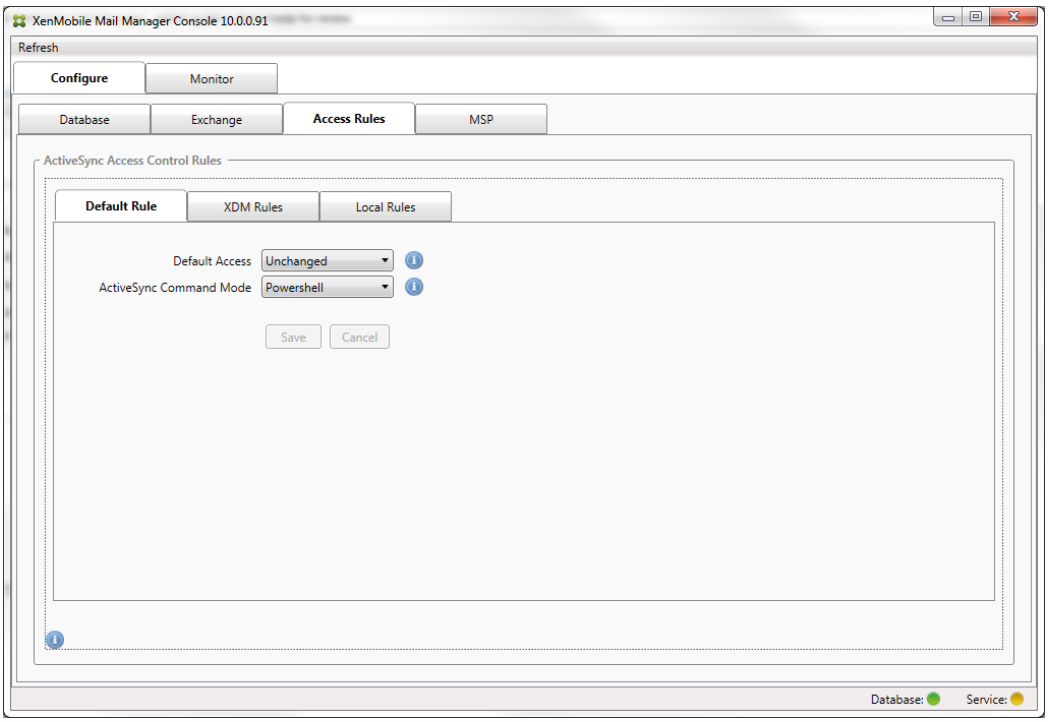


5. Wenn Sie On Premise auswählen, geben Sie den Namen des für Remote-PowerShell-Befehle verwendeten Exchange-Servers ein.
6. Geben Sie den Benutzernamen einer Windows-Identität ein, die die unter "Anforderungen" aufgeführten Berechtigungen auf dem Exchange Server-Computer hat.
7. Geben Sie für Password das Kennwort des Benutzers ein.
8. Wählen Sie den Zeitplan zum Ausführen größerer Snapshots. Bei einem größeren Snapshot wird jede Exchange ActiveSync-Partnerschaft ermittelt.
9. Wählen Sie den Zeitplan zum Ausführen kleinerer Snapshots. Bei einem kleineren Snapshot werden neu erstellte Exchange ActiveSync-Partnerschaften ermittelt.
10. Wählen Sie den Snapshottyp aus: Deep oder Shallow. Flache Snapshots (Shallow) werden in der Regel viel schneller

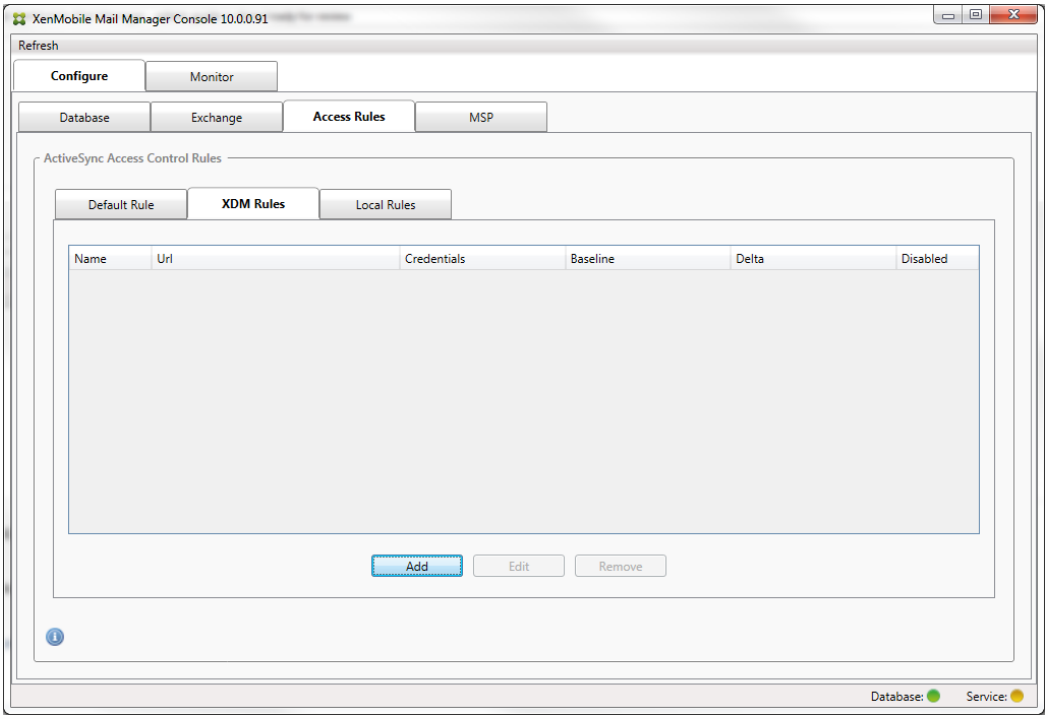
erstellt und reichen zur Ausführung aller Funktionen der Exchange ActiveSync-Zugriffssteuerung von XenMobile Mail Manager aus. Tiefe Snapshots (Deep) brauchen wesentlich länger und sind nur erforderlich, wenn Mobile Service Provider für ActiveSync aktiviert ist (dadurch kann XenMobile nicht verwaltete Geräte abfragen).

11. Klicken Sie auf Test Connectivity, um zu prüfen, ob eine Verbindung mit dem Exchange Server-Computer hergestellt werden kann, und klicken Sie auf Save.
12. Eine Meldung fordert Sie zum Neustarten des Diensts auf. Klicken Sie auf Yes.

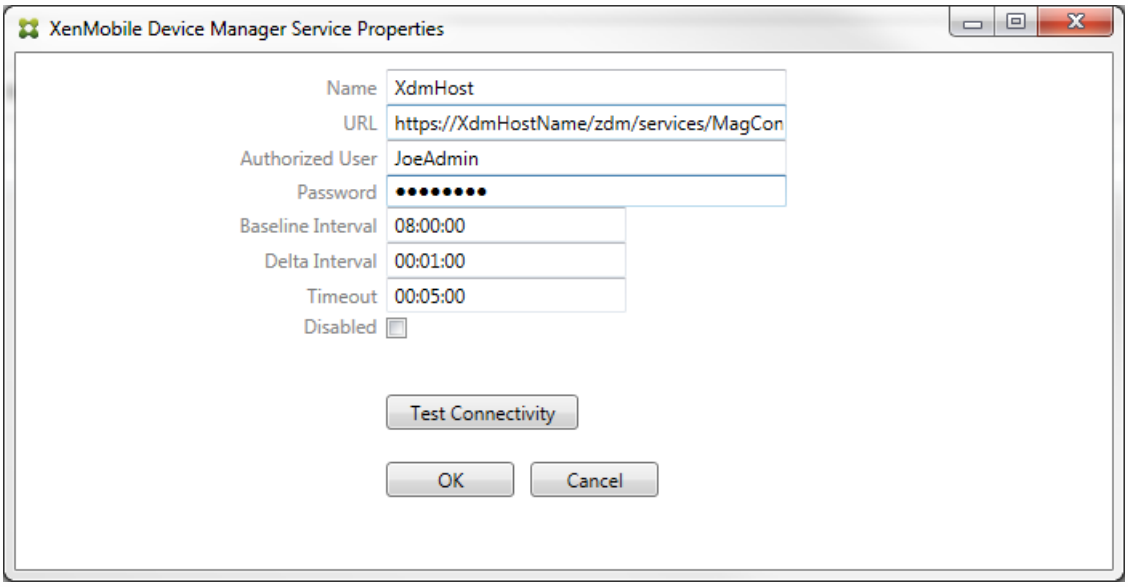
6. Konfigurieren Sie die Zugriffsregeln:
   1. Wählen Sie die Registerkarte Configure > Access Rules.



   2. Wählen Sie den Standardzugriff aus: Allow, Block oder Unchanged. Hierdurch wird gesteuert, wie Geräte behandelt werden, die keine der Kriterien von XenMobile-Regeln oder lokalen Regeln erfüllen. Wenn Sie die Option Allow auswählen, erhalten all diese Geräte ActiveSync-Zugriff, wenn Sie Block auswählen, wird der Zugriff verweigert und wenn Sie Unchanged auswählen, erfolgt keine Änderung.
   3. Wählen Sie für ActiveSync Command Mode eine Option aus: PowerShell oder Simulation.
      - Im PowerShell-Modus gibt XenMobile Mail Manager die PowerShell-Befehle für die gewünschte Zugriffssteuerung aus.
      - Im Simulationsmodus werden von XenMobile Mail Manager keine PowerShell-Befehle ausgegeben, sondern stattdessen beabsichtigte Befehle und Ergebnisse in der Datenbank protokolliert. Im Simulationsmodus kann der Benutzer dann auf der Registerkarte Monitor sehen, was passiert wäre, wenn der PowerShell-Modus aktiviert gewesen wäre.
   4. Klicken Sie auf Speichern.
7. Klicken Sie auf die Registerkarte XDM Rules.



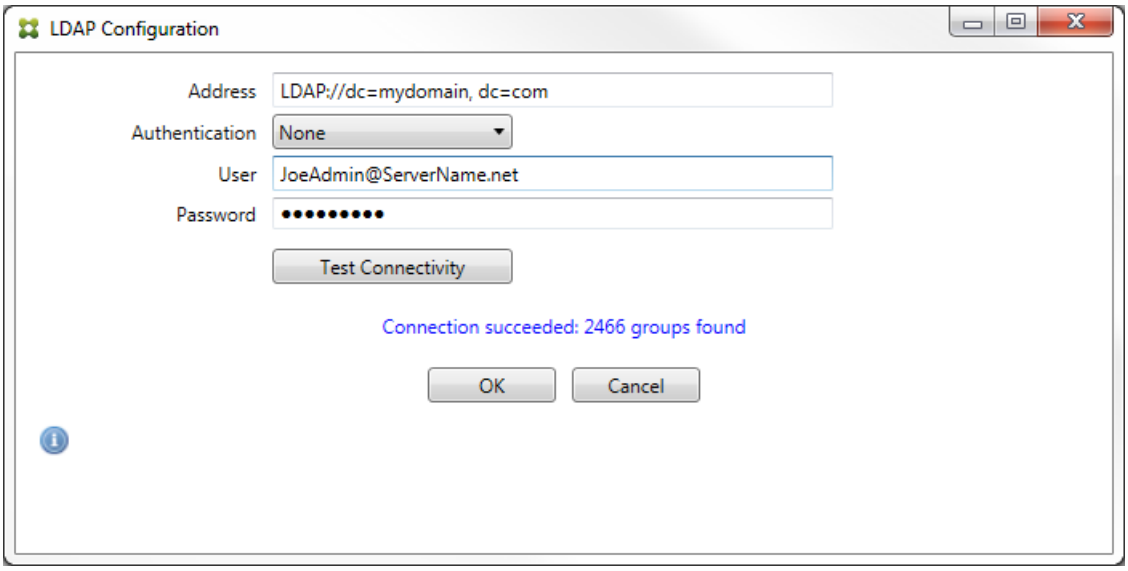
1. Klicken Sie auf Add.
2. Geben Sie einen Namen für die XDM-Regel ein, z. B. "XdmHost".



3. Ändern Sie die URL in eine Zeichenfolge, die auf den XenMobile-Server verweist. Lautet der Servername beispielsweise "XdmHost", geben Sie "http://XdmHostName/zdm/services/MagConfigService" ein.
4. Geben Sie einen auf dem Server berechtigten Benutzer an.
5. Geben Sie das Kennwort des Benutzers ein.
6. Übernehmen Sie die Standardwerte für Baseline Interval, Delta Interval und Timeout values.
7. Klicken Sie auf Test Connectivity, um die Verbindung zu dem Server zu testen.
   Hinweis: Wenn das Kontrollkästchen "Disabled" aktiviert ist, ruft der XenMobile Mail-Dienst keine Richtlinie vom XenMobile-Server ab.
8. Klicken Sie auf OK.

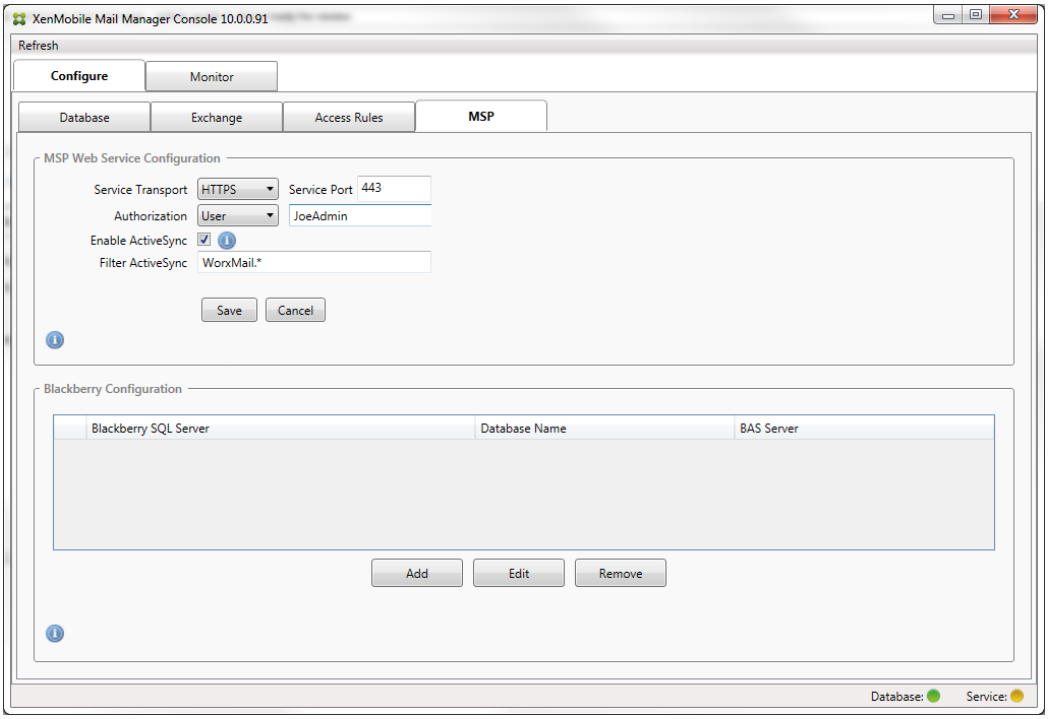
8. Klicken Sie auf die Registerkarte Local Rules.

1. Wenn Sie lokale Regeln für Active Directory-Gruppen erstellen möchten, klicken Sie auf Configure LDAP und konfigurieren Sie dann die LDAP-Verbindungseigenschaften.



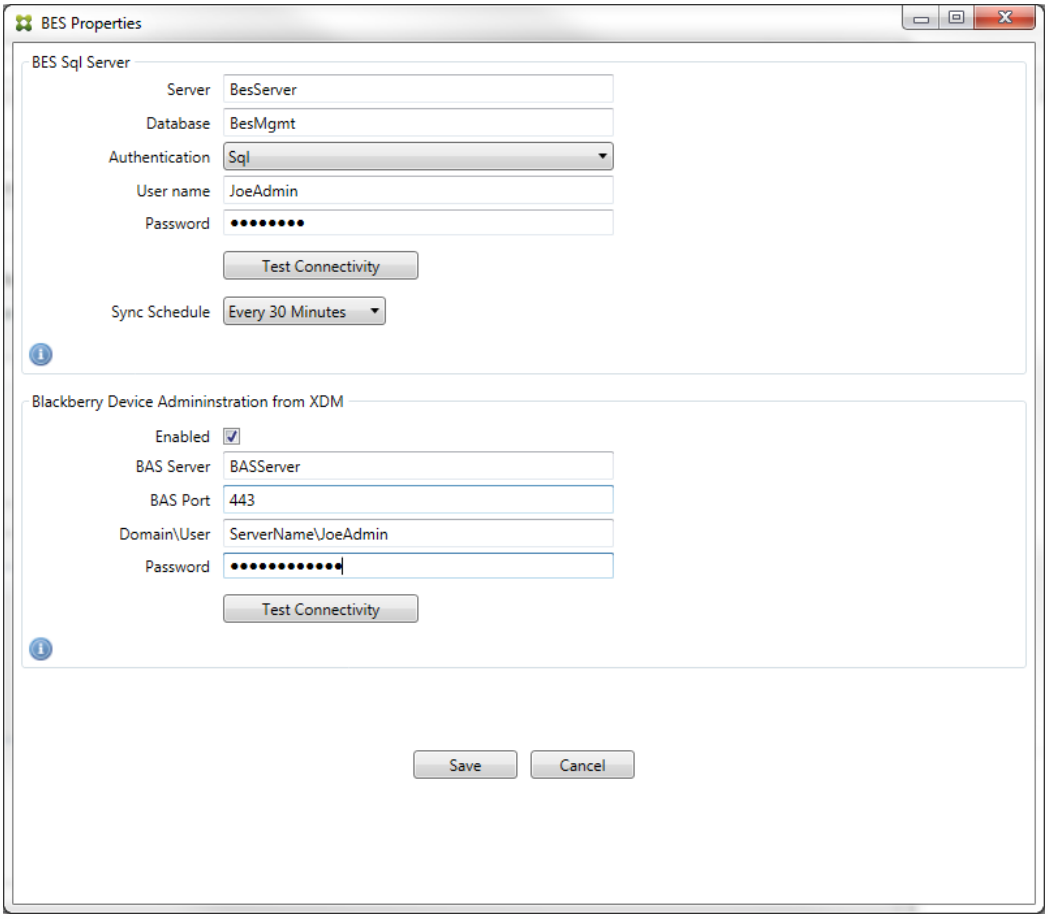
2. Sie können lokale Regeln basierend auf den Parametern ActiveSync Device ID, Device Type, AD Group, User oder UserAgent hinzufügen. Wählen Sie in der Liste den geeigneten Schlüssel aus. Weitere Informationen finden Sie unter Zugriffsregeln in XenMobile Mail Manager.
3. Geben Sie Text oder Textteile in das Textfeld ein. Klicken Sie optional auf die Schaltfläche "Query", um die Entsprechungen für die Textteile anzuzeigen.
   Hinweis: Bei allen Typen mit Ausnahme von Group verwendet das System die in einem Snapshot gefundenen Geräte. Wenn Sie gerade erst anfangen und noch keinen Snapshot erstellt haben, ist daher noch nichts verfügbar.
4. Wählen Sie einen Textwert aus und klicken Sie auf Allow oder Deny, um ihn rechts dem Bereich Rule List hinzuzufügen. Mit den Schaltflächen rechts neben Rule List können Sie die Reihenfolge der Regeln ändern oder diese entfernen. Die Reihenfolge ist wichtig, weil die Regeln für jeden Benutzer bzw. jedes Gerät in der angegebenen Reihenfolge bewertet werden und eine Übereinstimmung bei einer höher stehenden Regel dazu führt, dass darunter stehende Regeln wirkungslos bleiben. Beispiel: Wenn Sie eine Regel zum Zulassen aller iPads und darunter eine Regel zum Blockieren des Benutzers "Matthias" erstellen, dann wird das iPad des Benutzers Matthias zugelassen, da die iPad-Regel Priorität vor der Matthias-Regel hat.
5. Zum Durchführen einer Analyse der Regeln in der Liste auf mögliche Außerkraftsetzungen, Konflikte oder zusätzliche Konstrukte klicken Sie auf Analyze.
6. Klicken Sie auf Speichern.

9. Konfigurieren des Mobile Service Provider-Diensts
   Hinweis: Der Mobile Service Provider-Dienst ist optional und nur erforderlich, wenn auch XenMobile für die Verwendung der Mobile Service Provider-Schnittstelle für die Abfrage nicht verwalteter Geräte konfiguriert ist.
   1. Wählen Sie die Registerkarte ConfigureMSP.



2. Legen Sie den Dienst-Transporttyp für den Mobile Service Provider-Dienst auf HTTP oder HTTPS fest.
3. Legen Sie den Port (normalerweise 80 oder 443) für den Mobile Service Provider-Dienst fest.
   Hinweis: Wenn Sie Port 443 verwenden, muss an den Port in IIS ein SSL-Zertifikat gebunden sein.
4. Legen Sie die Autorisierungsgruppe bzw. den Autorisierungsbenutzer fest. Dies ist die Gruppe bzw. der Benutzer, die bzw. der in XenMobile eine Verbindung mit dem Mobile Service Provider-Dienst herstellen kann.
5. Legen Sie fest, ob ActiveSync-Abfragen aktiviert sein sollen.
   Hinweis: Wenn ActiveSync-Abfragen für den XenMobile-Server aktiviert werden, muss der Snapshottyp für den bzw. die Exchange Server auf Deep eingestellt werden, was eine starke Leistungsminderung bei der Erstellung von Snapshots nach sich ziehen kann.
6. Standardmäßig werden ActiveSync-Geräte, die dem regelmäßigen Ausdruck "WorxMail.*" entsprechen, nicht an XenMobile gesendet. Zum Ändern dieses Verhaltens ändern Sie das Feld Filter ActiveSync nach Bedarf.
   Hinweis: Ein leeres Feld bedeutet, dass alle Geräte an XenMobile weitergeleitet werden.
7. Klicken Sie auf Speichern.

10. Konfigurieren Sie nach Wunsch einen oder mehrere BlackBerry Enterprise Server (BES):
    1. Klicken Sie auf Add.
    2. Geben Sie den Servernamen des BES SQL-Servers ein.



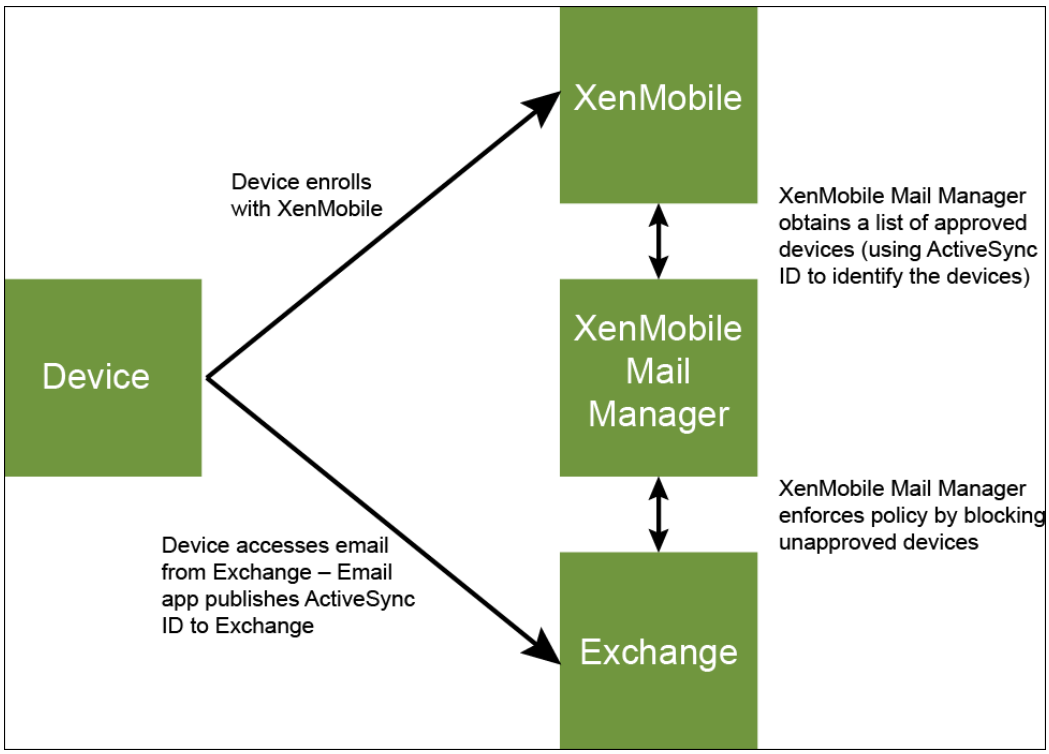
3. Geben Sie den Namen der BES-Verwaltungsdatenbank ein.
4. Wählen Sie den Authentifizierungsmodus aus. Bei Auswahl von "Windows Integrated" wird das Benutzerkonto des XenMobile Mail Manager-Diensts für die Verbindung mit dem BES SQL-Server verwendet.
   Hinweis: Wenn "Windows Integrated" auch für die XenMobile Mail Manager-Datenbankverbindung ausgewählt wird, muss dem hier angegebenen Windows-Konto Zugriff auf die XenMobile Mail Manager-Datenbank erteilt werden.
5. Wenn Sie SQL authentication auswählen, geben Sie Benutzernamen und Kennwort ein.
6. Legen Sie den Parameter Sync Schedule fest. Nach diesem Zeitplan erfolgt eine regelmäßige Verbindung mit dem BES SQL-Server zur Prüfung auf Aktualisierungen an Geräten.
7. Klicken Sie auf Test Connectivity, um die Verbindung mit dem SQL-Server zu prüfen.
   Hinweis: Wurde "Windows Integrated" ausgewählt, wird bei dem Test das Konto des aktuell angemeldeten Benutzers anstelle des XenMobile Mail Manager-Dienstkontos verwendet und die SQL-Authentifizierung daher nicht richtig getestet.
8. Wenn Sie das Remotelöschen und/oder das Zurücksetzen des Kennworts auf BlackBerry-Geräten von XenMobile aus unterstützen möchten, aktivieren Sie das Kontrollkästchen Enabled.
   1. Geben Sie den vollqualifizierten Domänennamen (FQDN) des BES ein.
   2. Geben Sie den BES-Port für den Verwaltungswebdienst ein.
   3. Geben Sie den vollständig qualifizierten Benutzernamen und das Kennwort für den BES-Dienst ein.
   4. Klicken Sie auf Test Connectivity, um die Verbindung zum BES zu testen.
   5. Klicken Sie auf Speichern.

Erzwingen von E-Mail-Richtlinien mit ActiveSync-IDs

Nov 20, 2015

Die E-Mail Richtlinie Ihres Unternehmens schreibt möglicherweise vor, dass bestimmte Geräte nicht für Unternehmens-E-Mails verwendet werden dürfen. Für die Einhaltung dieser Richtlinie müssen Sie sicherstellen, dass Benutzer über solche Geräte keinen Zugriff auf Unternehmens-E-Mail haben. XenMobile Mail Manager und XenMobile sorgen zusammen für die Einhaltung einer solchen E-Mail-Richtlinie. In XenMobile wird die Richtlinie für den Zugriff auf Unternehmens-E-Mail festgelegt, und wenn ein nicht genehmigtes Gerät bei XenMobile registriert wird, erzwingt XenMobile Mail Manager die Einhaltung der Richtlinie.

Der E-Mail-Client eines Geräts kündigt sich bei Exchange Server (oder Office 365) mit der Geräte-ID an. Die Geräte-ID wird auch als ActiveSync-ID bezeichnet und ermöglicht die eindeutige Identifizierung des Geräts. Worx Home ruft eine ähnliche ID ab und sendet sie XenMobile, wenn das Gerät registriert wird. Durch den Vergleich der beiden Geräte-IDs kann XenMobile Mail Manager ermitteln, ob ein bestimmtes Gerät auf Unternehmens-E-Mail zugreifen darf. Das Konzept wird in folgender Abbildung dargestellt:



Wenn XenMobile eine andere ActiveSync-ID an XenMobile Mail Manager sendet als die, die das Gerät an Exchange gibt, dann kann XenMobile Mail Manager Exchange nicht anzeigen, wie mit dem Gerät verfahren werden soll.

Das Zuordnen von ActiveSync-IDs funktioniert zuverlässig auf den meisten Plattformen. Bei einigen Android-Implementierungen hat Citrix jedoch festgestellt, dass sich die ActiveSync-ID des Geräts von der ID unterscheidet, die der E-Mail-Client Exchange ankündigt. Auf folgende Weise mindern Sie das Problem:

- Auf der Samsung SAFE-Plattform stellen Sie die ActiveSync-Konfiguration von XenMobile per Push auf dem Gerät bereit.
- Auf allen anderen Android-Plattformen stellen Sie die Touchdown-App und die Touchdown-ActiveSync-Konfiguration von XenMobile per Push bereit.

Dadurch wird jedoch nicht verhindert, dass ein Mitarbeiter einen anderen E-Mail-Client als Touchdown auf einem Android-Gerät installiert. Um sicherzustellen, dass die Zugriffsrichtlinie für Unternehmens-E-Mail richtig durchgesetzt wird, können Sie eine defensive Sicherheitsstrategie anwenden und E-Mails blockieren, indem Sie in XenMobile Mail Manager die statische Richtlinie auf Deny by default festlegen. Wenn ein Mitarbeiter dann einen anderen E-Mail-Client als Touchdown auf einem Android-Gerät konfiguriert und die ActiveSync-ID-Erkennung nicht ordnungsgemäß funktioniert, wird dem Mitarbeiter der Zugriff auf Unternehmens-E-Mail verweigert.

Regeln für die Zugriffssteuerung

Nov 20, 2015

XenMobile Mail Manager bietet eine regelbasierte Methode zur dynamischen Konfiguration der Zugriffssteuerung für Exchange ActiveSync-Geräte. XenMobile Mail Manager-Zugriffsregeln bestehen aus zwei Teilen: einem Abgleichausdruck und dem gewünschten Zugriffszustand (Zulassen oder Blockieren). Eine Regel kann gegen ein Exchange ActiveSync-Gerät ausgewertet werden, um zu ermitteln, ob die Regel auf das Gerät zutrifft, d. h. ob der Abgleichausdruck auf das Gerät zutrifft. Es gibt mehrere Arten von Abgleichausdrücken, eine Regel kann beispielsweise auf alle Geräten eines bestimmten Typs, eine bestimmte Exchange ActiveSync-Geräte-ID, alle Geräte eines bestimmten Benutzers usw. zutreffen.
Beim Hinzufügen, Entfernen und Umordnen von Regeln in der Regelliste kann die Liste jederzeit mit einem Klick auf die Schaltfläche Cancel auf den Zustand zurückgesetzt werden, den sie beim ersten Öffnen hatte. Wenn Sie nicht auf Schaltfläche Save klicken, gehen jegliche Änderungen in diesem Fenster verloren, wenn Sie das Konfigurationstool schließen.

XenMobile Mail Manager bietet drei Regeltypen: lokale Regeln, XDM-Regeln und die Standardzugriffsregel.

Lokale Regeln: Diese haben die höchste Priorität, d. h. sobald eine lokale Regel auf ein Gerät zutrifft, wird die Regelauswertung eingestellt. Es werden weder die XDM-Regeln noch die Standardzugriffsregel konsultiert. Lokale Regeln werden in Bezug auf XenMobile Mail Manager lokal über die Registerkarte Configure/Access Rules/Local Rules konfiguriert. Der Abgleich basiert auf der Mitgliedschaft von Benutzern bei einer bestimmten Active Directory-Gruppe. Der Abgleich basiert auf regelmäßigen Ausdrücken in folgenden Feldern:

- ActiveSync Device ID
- ActiveSync Device Type
- User Principal Name (UPN)
- ActiveSync User Agent (normalerweise die Geräteplattform oder der E-Mail Client)

Sofern ein größerer Snapshot durchgeführt und Geräte gefunden wurden, müsste es möglich sein, eine normale Regel oder eine solche mit regelmäßigen Ausdrücken hinzuzufügen. Wenn kein größerer Snapshot durchgeführt wurde, können Sie nur Regeln mit regelmäßigen Ausdrücken hinzufügen.

XDM-Regeln: XDM-Regeln sind Verweise auf einen externen XenMobile-Server, der Regeln zu verwalteten Geräten bereitstellt. Der XenMobile-Server kann mit eigenen allgemeinen Regeln konfiguriert werden, bei denen Geräte basierend auf in XenMobile bekannten Eigenschaften (z. B. Vorliegen von Jailbreak oder Vorhandensein verbotener Apps) zugelassen oder blockiert werden. XenMobile wertet die allgemeinen Regeln aus und generiert eine Liste zulässiger bzw. blockierter ActiveSync-Geräte-IDs, die dann an XenMobile Mail Manager gesendet werden.

Standardzugriffsregel: Die Besonderheit der Standardzugriffsregel besteht darin, dass sie theoretisch auf jedes Gerät zutreffen kann und immer als letzte ausgewertet wird. Die Regel dient als Auffangnetz für alle Geräte; trifft bei einem Gerät weder eine lokale noch eine MDM-Regel zu, wird der gewünschte Zugriffszustand durch die Standardzugriffsregel bestimmt.

- Default Access – Allow: Geräte, auf die weder eine lokale noch eine XDM-Regel zutrifft, werden alle zugelassen.
- Default Access – Block: Geräte, auf die weder eine lokale noch eine XDM-Regel zutrifft, werden alle blockiert.
- Default Access - Unchanged: Bei Geräten, auf die weder eine lokale noch eine XDM-Regel zutrifft, wird der Zugriffszustand von XenMobile Mail Manager nicht geändert. Wurde ein Gerät beispielsweise durch Exchange in den Quarantänemodus versetzt, erfolgt keine Aktion. Das Gerät kann nur aus dem Quarantänemodus genommen werden, wenn es eine explizite lokale oder XDM-Regel gibt, die die Quarantäne außer Kraft setzt.

Auswertung von Regeln

Für jedes Gerät, das Exchange an XenMobile Mail Manager meldet, werden die Regeln beginnend bei der Regel mit der höchsten bis zu der Regel mit der niedrigsten Priorität in folgender Reihenfolge ausgewertet:

- Lokale Regeln
- Standardzugriffsregel
- XDM-Regeln

Sobald eine Regel zutrifft, wird die Auswertung beendet. Trifft beispielsweise eine lokale Regel auf ein Gerät zu, erfolgt für dieses keine Auswertung der XDM-Regeln oder der Standardzugriffsregel. Das gleiche Prinzip gilt für die Regeln desselben Regeltyps. Beispiel: Treffen mehrere lokale Regeln auf ein Gerät zu, wird die Auswertung beendet, sobald die erste Übereinstimmung gefunden wird.

XenMobile Mail Manager wiederholt die Auswertung eines vorliegenden Regelsatzes, wenn Geräteeigenschaften sich ändern, wenn Geräte hinzugefügt oder entfernt werden oder wenn die Regeln selbst sich ändern. Bei größeren Snapshots werden Änderungen an Eigenschaften und Entfernungen von Geräten in konfigurierbaren Intervallen ermittelt. Bei kleineren Snapshots werden Hinzufügungen von Geräten in konfigurierbaren Intervallen ermittelt.

Exchange ActiveSync umfasst ebenfalls Regeln für den Zugriff. Es ist wichtig, zu wissen, wie diese Regeln im Zusammenhang mit XenMobile Mail Manager funktionieren. In Exchange können Regeln dreierlei Ebenen konfiguriert werden: persönliche Ausnahmen, Geräteregeln und Organisationseinstellungen. XenMobile Mail Manager automatisiert die Zugriffssteuerung durch programmgesteuerte Remote PowerShell-Anforderungen, die sich auf die Listen der persönlichen Ausnahmen auswirken. Bei diesen handelt es sich um Listen zulässiger oder blockierter Exchange ActiveSync-Geräte-IDs eines Postfachs. Wird XenMobile Mail Manager bereitgestellt, übernimmt es die Verwaltung der Ausnahmelistenfunktion in Exchange. Weitere Informationen finden Sie in diesem Microsoft-Artikel.

Eine Analyse ist besonders dann nützlich, wenn mehrere Regeln für das gleiche Feld definiert wurden. Sie können die Beziehungen zwischen Regeln auf Konflikte untersuchen. Die Analyse erfolgt aus der Perspektive der Regelfelder, d. h. Regeln werden beispielsweise in Gruppen nach abgeglichenen Feld (ActiveSync Device ID, ActiveSync Device Type, User, User Agent usw.) analysiert.

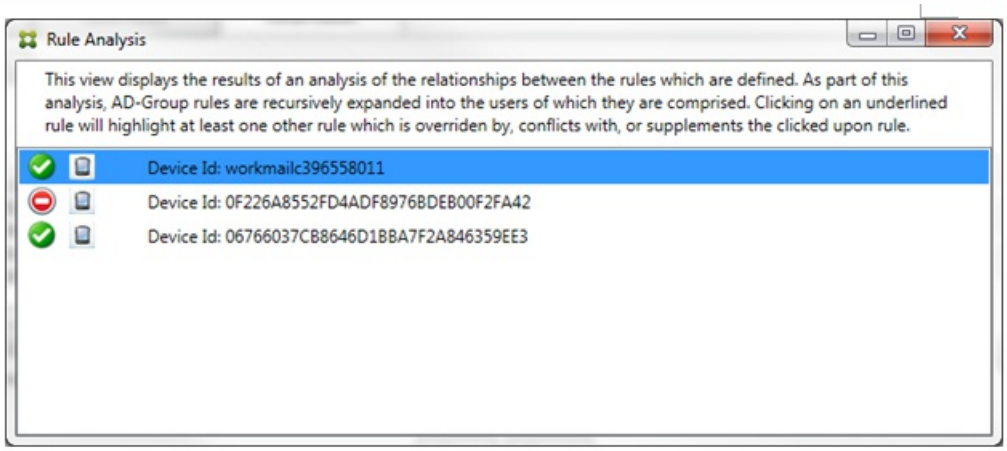
Terminologie:

- **Overriding rule** (außer Kraft setzende Regel): Eine Außerkraftsetzung tritt auf, wenn mehr als eine Regel auf ein Gerät zutreffen. Da Regeln nacheinander gemäß Priorität ausgewertet werden, werden zutreffende Regeln weiter unten in der Liste möglicherweise nie ausgewertet.
- **Conflicting rule** (Konflikt verursachende Regel): Ein Konflikt tritt auf, wenn mehrere Regeln auf ein Gerät zutreffen, der Zugriffszustand (Zulassen/Blockieren) jedoch nicht übereinstimmt. Handelt es sich nicht um Regeln mit regelmäßigen Ausdrücken, folgt aus einem Konflikt grundsätzlich eine Außerkraftsetzung.
- **Supplemental rule** (Ergänzungsregeln): Eine Ergänzung tritt auf, wenn mehrere Regeln regelmäßige Ausdrücke enthalten und daher sichergestellt werden muss, dass die regelmäßigen Ausdrücke sich entweder zu einem einzigen zusammenfassen lassen, oder aber keine Funktionalität duplizieren. Eine Ergänzungsregel kann auch beim Zugriffszustand (Zulassen/Blockieren) einen Konflikt verursachen.
- **Primary rule** (primäre Regel): Die primäre Regel ist diejenige, auf die im Dialogfeld geklickt wurde. Sie wird durch einen durchgehenden Rahmen optisch hervorgehoben. Für diese Regel werden auch ein oder zwei nach oben oder unten weisende grüne Pfeile angezeigt. Ein nach oben weisender Pfeil zeigt an, dass es Nebenregeln gibt, die vor der primären Regel stehen. Ein nach unten weisender Pfeil zeigt an, dass es Nebenregeln gibt, die nach der primären Regel stehen. Es kann immer nur eine primäre Regel aktiv sein.

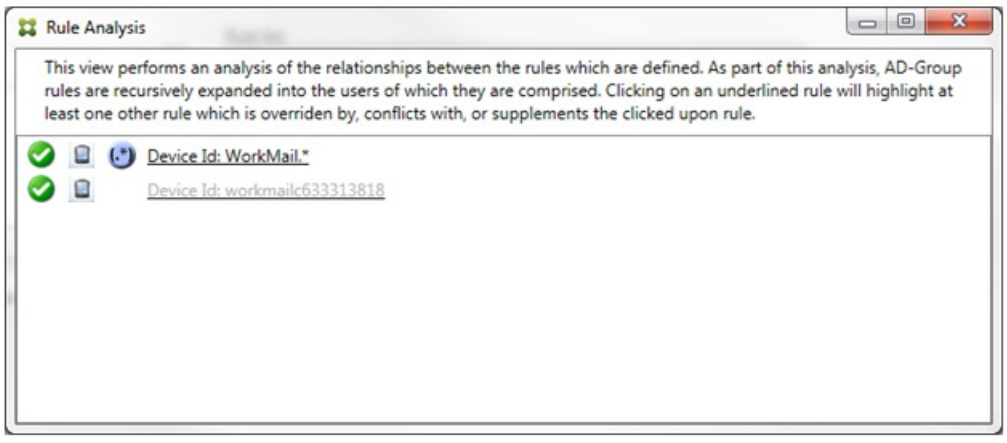
- **Ancillary rule** (Nebenregel): Eine Nebenregel hängt durch eine Außerkraftsetzung, einen Konflikt oder eine Ergänzungsbeziehung mit einer primären Regel zusammen. Solche Regeln werden durch einen gestrichelten Rahmen optisch hervorgehoben. Jede primäre Regel kann beliebig viele Nebenregeln haben. Wenn Sie auf einen unterstrichenen Eintrag klicken, erfolgt die Hervorhebung der Nebenregeln immer aus der Sicht der primären Regel. Beispiel: Die Nebenregel wird durch die primäre Regel außer Kraft gesetzt und/oder die Nebenregel verursacht einen Konflikt beim Zugriffszustand mit der primären Regel und/oder die Nebenregel ergänzt die primäre Regel.

Darstellung des Regeltyps im Dialogfeld zur Regelanalyse

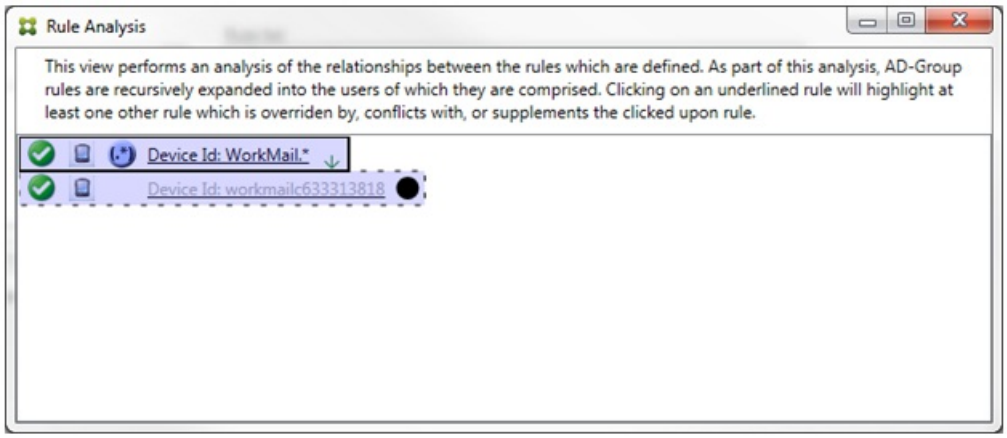
Wenn keine Konflikte, Außerkraftsetzungen oder Ergänzungen vorliegen, enthält das Dialogfeld Rule Analysis keine unterstrichenen Einträge. Das Klicken auf Elemente hat keine Auswirkung, es wird z. B. normal angezeigt, welches Element ausgewählt ist.



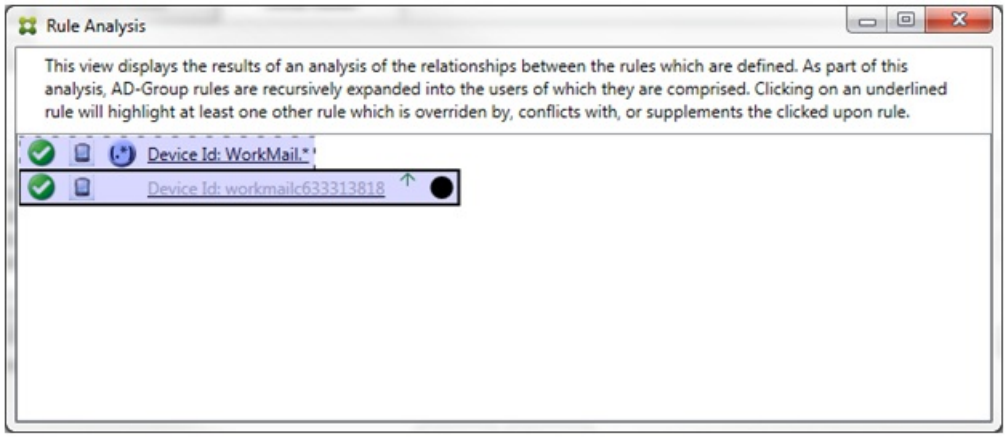
Wenn eine Außerkraftsetzung vorliegt, werden mindestens zwei Regeln unterstrichen dargestellt: die primäre Regel und die Nebenregel(n). Mindestens eine Nebenregel erscheint in einer helleren Schrift, um anzuzeigen, dass sie durch eine höhere Regel außer Kraft gesetzt wird. Sie können auf die außer Kraft gesetzte Regel klicken, um zu ermitteln, durch welche Regel(n) sie außer Kraft gesetzt wird. Neben außer Kraft gesetzten Primär- oder Nebenregeln wird, sobald sie ausgewählt werden, ein schwarzer Punkt als deutliches Zeichen dafür angezeigt, dass die jeweilige Regel nicht aktiv ist. Beispiel: Bevor Sie auf eine Regel klicken, wird das Dialogfeld folgendermaßen angezeigt:



Wenn Sie auf die Regel mit der höchsten Priorität klicken, wird es folgendermaßen angezeigt:



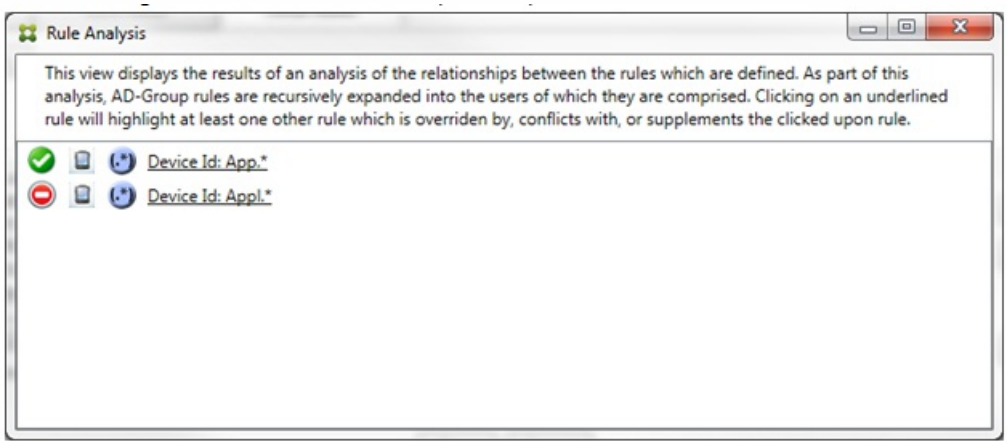
In diesem Beispiel ist die Regel mit regelmäßigen Ausdrücken WorkMail.* die primäre Regel (angezeigt durch den durchgehenden Rahmen) und die normale Regel workmailc633313818 ist eine Nebenregel (angezeigt durch den gestrichelten Rahmen). Der schwarze Punkt neben der Nebenregel weist deutlich darauf hin, dass die Regel inaktiv ist (d. h. niemals ausgewertet wird), da ihr die Regel mit den regelmäßigen Ausdrücken voransteht und eine höhere Priorität hat. Nach dem Klicken auf die außer Kraft gesetzte Regel wird das Dialogfeld folgendermaßen angezeigt:



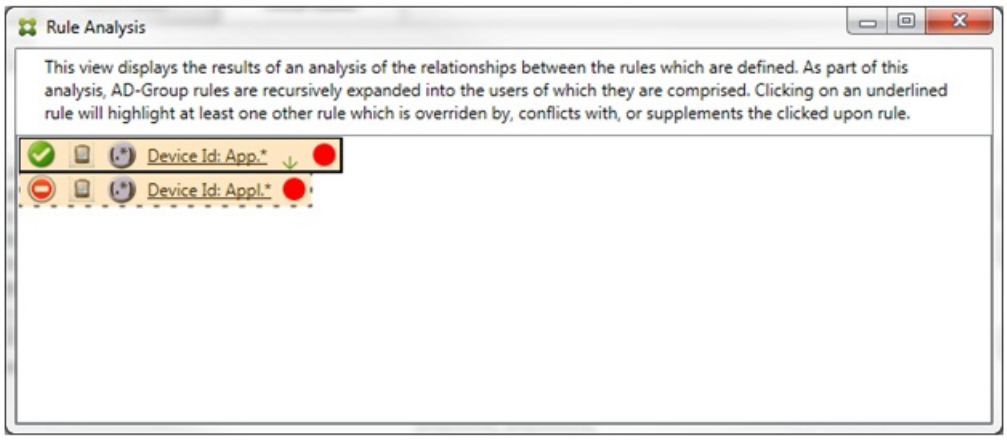
Im vorherigen Beispiel ist die Regel mit regelmäßigen Ausdrücken WorkMail.* die Nebenregel (angezeigt durch den gestrichelten Rahmen) und die normale Regel workmailc633313818 ist eine primäre Regel (angezeigt durch den durchgehenden Rahmen). In diesem einfachen Beispiel ist der Unterschied nicht groß. Ein etwas vielschichtigeres Beispiel finden Sie weiter unten in der Beschreibung komplexer Ausdrücke. In einem Szenario mit vielen definierten Regeln lässt sich durch einen Klick auf eine außer Kraft gesetzte Regel schnell herausfinden, welche Regel(n) sie außer Kraft setzen.

Wenn ein Konflikt vorliegt, werden mindestens zwei Regeln unterstrichen dargestellt: die primäre Regel und die Nebenregel(n). Die widersprüchlichen Regeln werden mit einem roten Punkt gekennzeichnet. Ein reiner Konflikt ist nur möglich, wenn mindestens zwei Regeln mit regelmäßigen Ausdrücken definiert wurden. Bei allen anderen Szenarios liegt

nicht nur ein Konflikt vor, sondern auch eine Außerkraftsetzung. Vor dem Klicken auf eine der Regeln in diesem einfachen Beispiel sieht das Dialogfeld folgendermaßen aus:

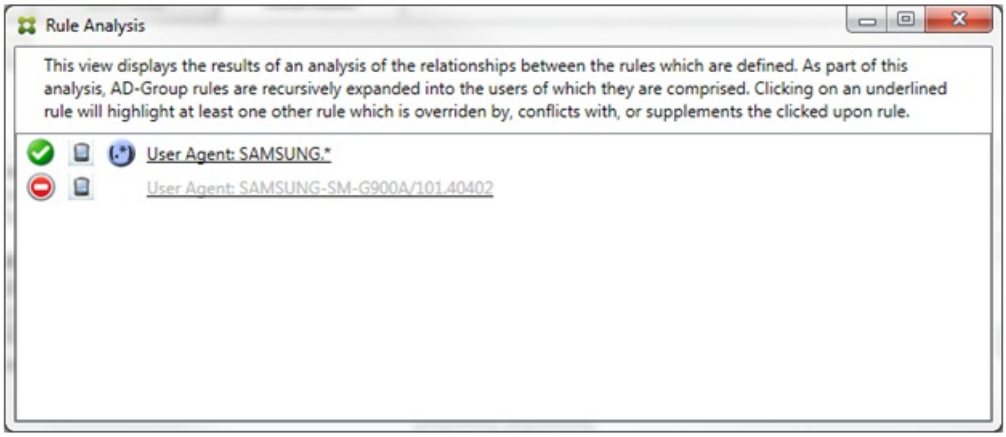


Eine Untersuchung der beiden Regeln mit regelmäßigen Ausdrücken ergibt, dass die erste alle Geräte, deren ID "App" enthält, zulässt und die zweite alle Geräte, deren ID "Appl" enthält, blockiert. Obwohl die zweite Regel alle Geräte, deren ID "Appl" enthält, blockiert, wird kein Gerät, auf das die Regel zutrifft, je blockiert, da die zulassende Regel eine höhere Priorität hat. Nach dem Klicken auf die erste Regel wird das Dialogfeld folgendermaßen angezeigt:



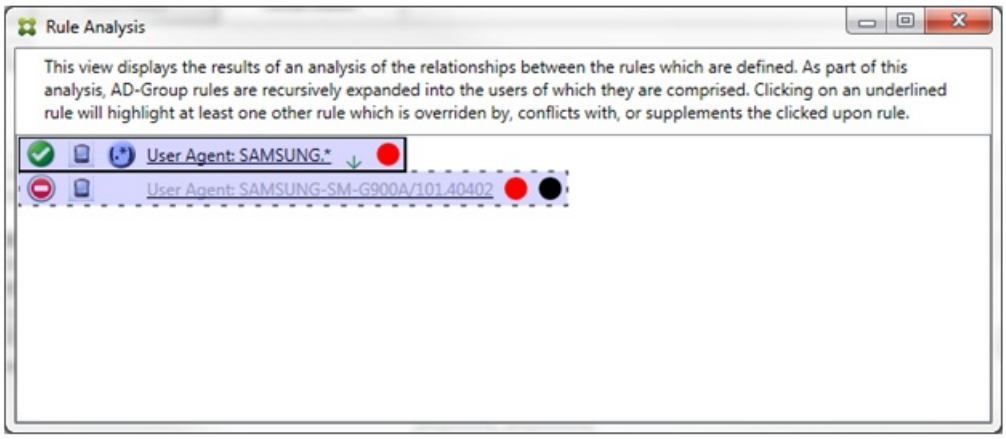
Im vorherigen Szenario wird sowohl die primäre Regel (mit dem regelmäßigen Ausdruck "App.*") und die Nebenregel (mit dem regelmäßigen Ausdruck "Appl.*") gelb markiert angezeigt. Dies ist ein einfacher optischer Warnhinweis auf den Umstand, dass mehrere Regeln mit regelmäßigem Ausdruck für ein einzelnes Feld angewendet wurden, was eine Redundanz oder ein schwerwiegenderes Problem bedeuten kann.

In einem Szenario mit Konflikt und Außerkraftsetzung wird sowohl die primäre Regel (mit dem regelmäßigen Ausdruck "App.*") und die Nebenregel (mit dem regelmäßigen Ausdruck "Appl.*") gelb markiert angezeigt. Dies ist ein einfacher optischer Warnhinweis auf den Umstand, dass mehrere Regeln mit regelmäßigem Ausdruck für ein einzelnes Feld angewendet wurden, was eine Redundanz oder ein schwerwiegenderes Problem bedeuten kann.



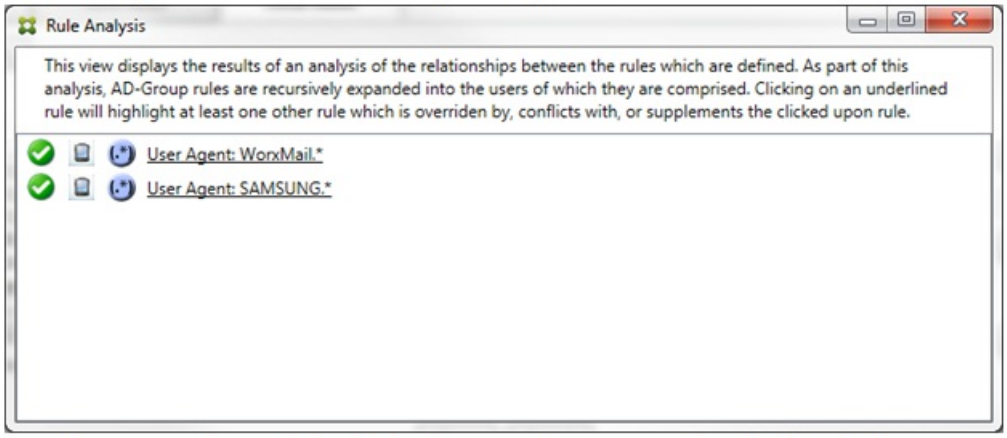
Im vorherigen Beispiel ist leicht zu erkennen, dass die erste Regel (mit dem regelmäßigen Ausdruck SAMSUNG.*) die nächste Regel (normale Regel SAMSUNG-SM-G900A/101.40402) außer Kraft setzt und überdies ein Konflikt beim Zugriffszustand (primäre Regel = Zulassen, Nebenregel = Blockieren) vorliegt. Die zweite Regel (normale Regel SAMSUNG-SM-G900A/101.40402) wird in einer helleren Schrift dargestellt, um darauf hinzuweisen, dass sie aufgrund einer Außerkraftsetzung inaktiv ist.

Nach dem Klicken auf die Regel mit dem regelmäßigen Ausdruck wird das Dialogfeld folgendermaßen angezeigt:

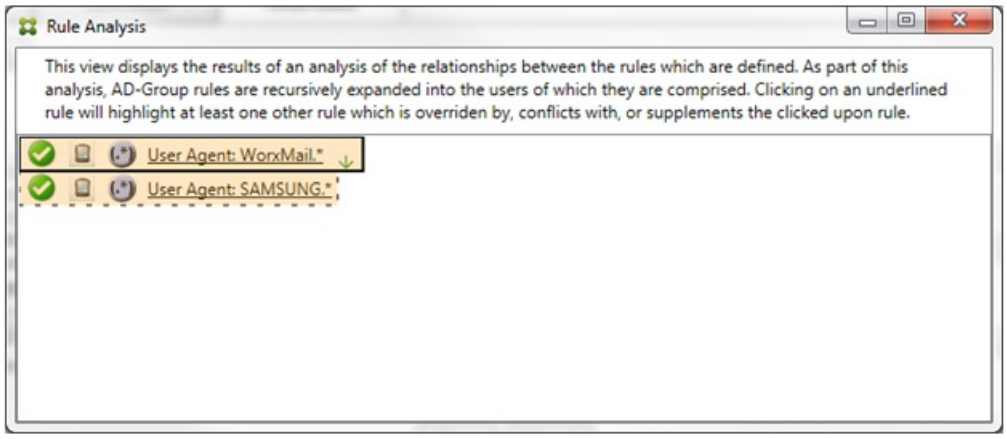


Die primäre Regel (mit dem regelmäßigen Ausdruck SAMSUNG.*) ist mit einem roten Punkt gekennzeichnet, um anzuzeigen, dass ihr Zugriffszustand im Widerspruch mit dem von mindestens einer Nebenregel steht. Die Nebenregel (normale Regel SAMSUNG-SM-G900A/101.40402) ist mit einem roten Punkt gekennzeichnet, um anzuzeigen, dass ihr Zugriffszustand im Widerspruch mit dem der primären Regel steht und mit einem schwarzen Punkt, um anzuzeigen, dass sie außer Kraft gesetzt und daher inaktiv ist.

Mindestens zwei Regeln werden unterstrichen dargestellt: die primäre Regel und die Nebenregel(n). Regeln, die nur einander ergänzen, können nur solche mit regelmäßigen Ausdrücken sein. Wenn Regeln einander ergänzen, werden durch eine gelbe Überlagerung gekennzeichnet. Vor dem Klicken auf eine der Regeln in diesem einfachen Beispiel sieht das Dialogfeld folgendermaßen aus:



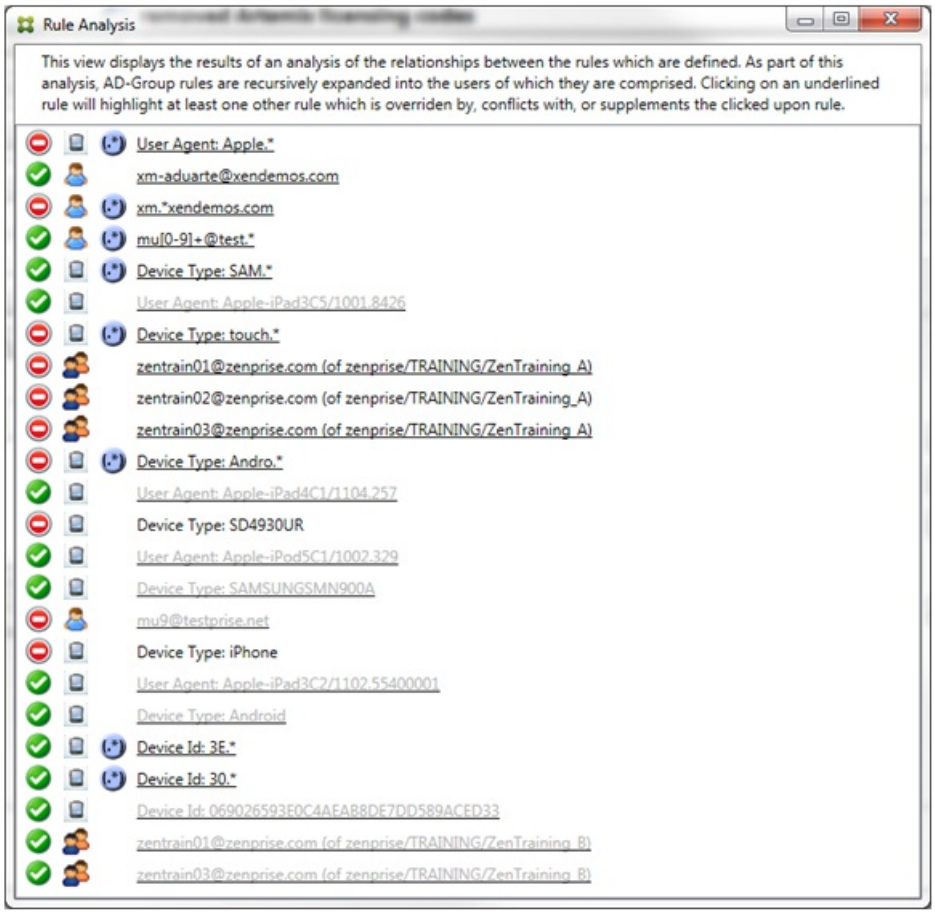
Es ist leicht zu erkennen, dass beide Regeln solche mit regelmäßigen Ausdrücken sind, und beide auf das Feld "ActiveSync device ID" in XenMobile Mail Manager angewendet werden. Nach dem Klicken auf die erste Regel sieht das Dialogfeld folgendermaßen aus:



Die primäre Regel (mit dem regelmäßigen Ausdruck WorxMail.*) ist mit einer gelben Überlagerung gekennzeichnet, um anzuzeigen, dass es mindestens eine weitere Nebenregel mit einem regelmäßigen Ausdruck gibt. Die Nebenregel (mit dem regelmäßigen Ausdruck SAMSUNG.*) ist mit einer gelben Überlagerung gekennzeichnet, um anzuzeigen, dass sowohl sie selbst als auch die primäre Regel als Regel mit einem regelmäßigen Ausdruck auf dasselbe Feld in XenMobile Mail Manager (ActiveSync device ID) angewendet werden. Dabei überschneiden die regelmäßigen Ausdrücke einander möglicherweise. Sie müssen entscheiden, ob die regelmäßigen Ausdrücke richtig konfiguriert wurden.

Beispiel für einen komplexen Ausdruck

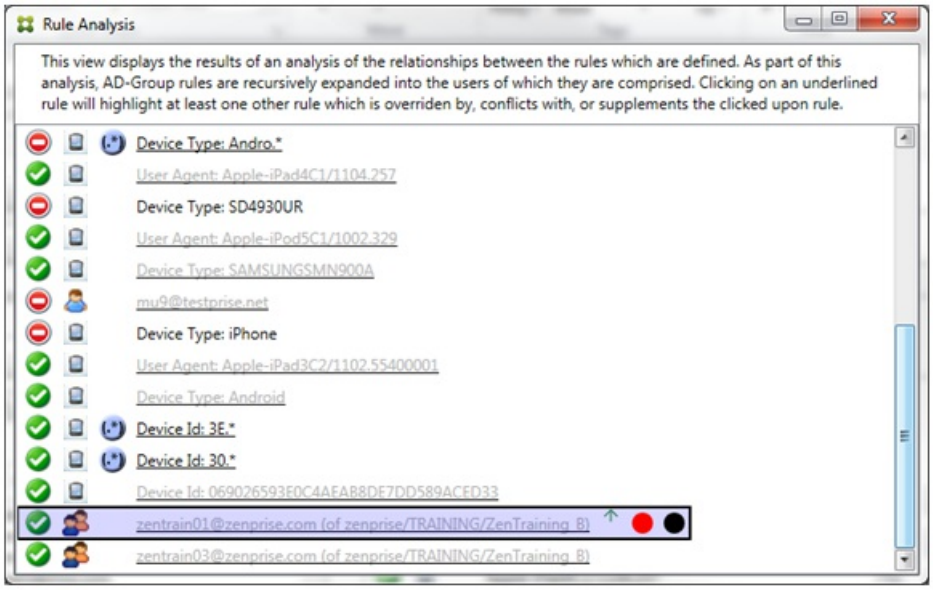
Es sind viele Außerkraftsetzungen, Konflikte oder Ergänzungen möglich, die hier nicht alle mit einem Beispiel vorgestellt werden können. Im Folgenden werden anhand eines Negativbeispiels die immensen Vorzüge des visuellen Konstrukts der Regelanalyse gezeigt. Die meisten Elemente in der folgenden Abbildung sind unterstrichen. Viele Elemente werden in einer helleren Schrift dargestellt, wodurch angezeigt wird, dass die jeweilige Regel durch eine höhere Regel außer Kraft gesetzt wurde. Die Liste enthält auch eine Reihe von Regeln mit regelmäßigen Ausdrücken, die durch das Symbol (.*) gekennzeichnet sind.



Analysieren einer Außerkraftsetzung

Um zu sehen, welche Regeln eine bestimmte Regel außer Kraft setzen, klicken Sie auf die Regel.

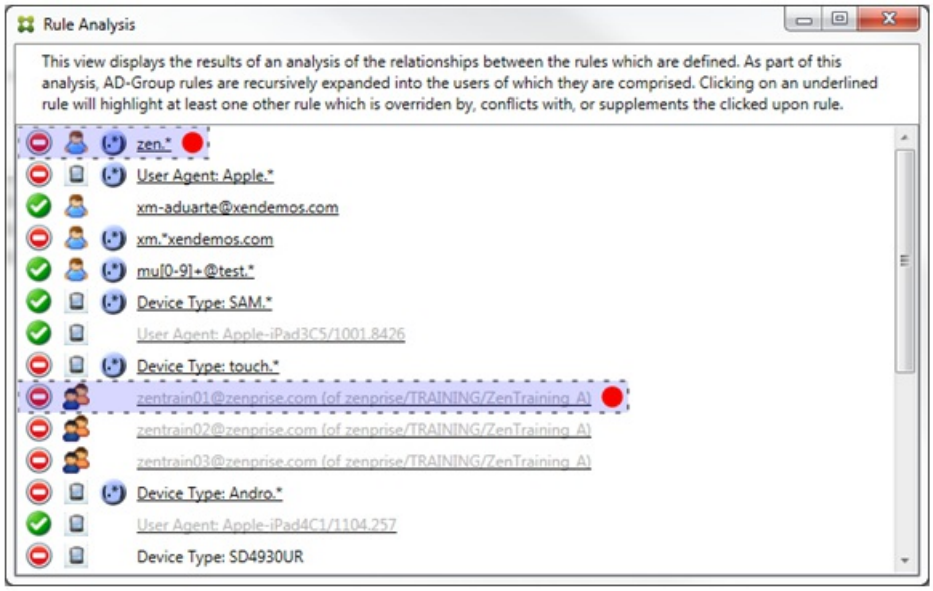
Beispiel 1: In diesem Beispiel wird untersucht, warum zentrain01@zenprise.com außer Kraft gesetzt wurde.



Die primäre Regel (AD-Gruppenregel zenprise/TRAINING/ZenTraining B, bei der zentrain01@zenprise.com Mitglied ist) hat die folgenden Merkmale:

- Sie ist blau unterlegt und wird von einem durchgehenden Rahmen umgeben.
- Sie hat einen nach oben weisenden grünen Pfeil, was anzeigt, dass alle Nebenregeln weiter oben sind.
- Sie ist mit einem roten und einem schwarzen Punkt gekennzeichnet, um anzuzeigen, dass erstens mindestens eine Nebenregel einen widersprüchlichen Zugriffszustand hat und zweitens die primäre Regel außer Kraft gesetzt und somit inaktiv ist.

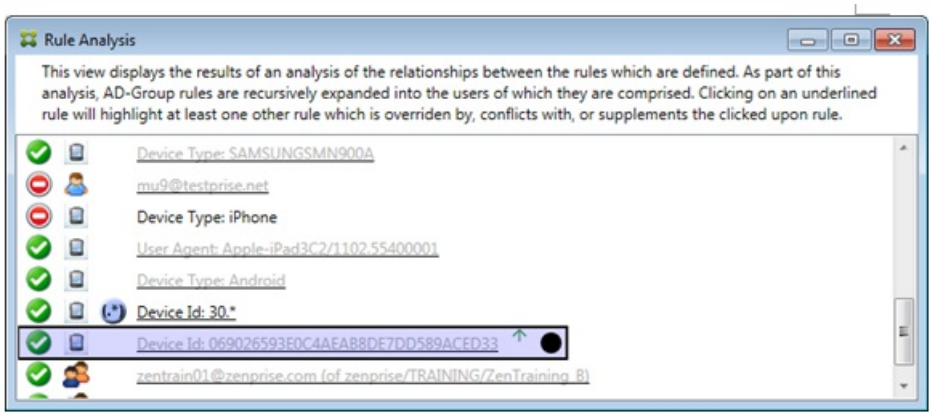
Wenn Sie einen Bildlauf nach oben durchführen, wird Folgendes angezeigt:



In diesem Fall gibt es zwei Nebenregeln, die die primäre Regel außer Kraft setzen: die Regel mit regelmäßigem Ausdruck zen.* und die normale Regel zentrain01@zenprise.com (von zenprise/TRAINING/ZenTraining A). Bei der letzteren Nebenregel

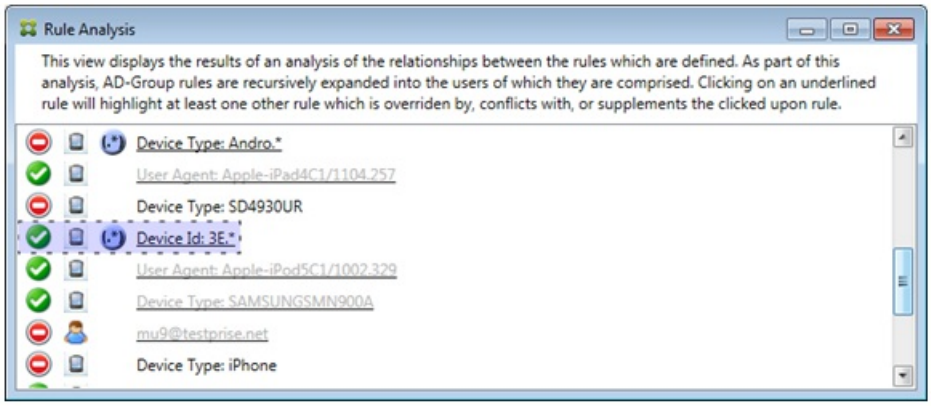
besteht das Problem darin, dass die Active Directory-Gruppenregel ZenTraining A den Benutzer zentrain01@zenprise.com enthält, die Active Directory-Gruppenregel ZenTraining B diesen Benutzer jedoch auch enthält. Da die Nebenregel eine höhere Priorität hat als die primäre Regel, wird die primäre Regel außer Kraft gesetzt. Der Zugriffszustand der primären Regel ist Zulassen und weil der Zugriffszustand beider Nebenregeln Blockieren ist, werden alle mit einem roten Punkt gekennzeichnet, um auf den Konflikt hinzuweisen.

Beispiel 2: Dieses Beispiel zeigt, warum die Regel zu dem Gerät mit der ActiveSync-Geräte-ID 069026593E0C4AEAB8DE7DD589ACED33 außer Kraft gesetzt wurde:



Die primäre Regel (normale Regel mit Geräte-ID 069026593E0C4AEAB8DE7DD589ACED33) hat die folgenden Merkmale:

- Sie ist blau unterlegt und wird von einem durchgehenden Rahmen umgeben.
- Sie hat einen nach oben weisenden grünen Pfeil, was anzeigt, dass die Nebenregel weiter oben ist.
- Sie ist mit einem schwarzen Punkt gekennzeichnet, um anzuzeigen, dass sie von einer Nebenregel außer Kraft gesetzt und somit deaktiviert wurde.

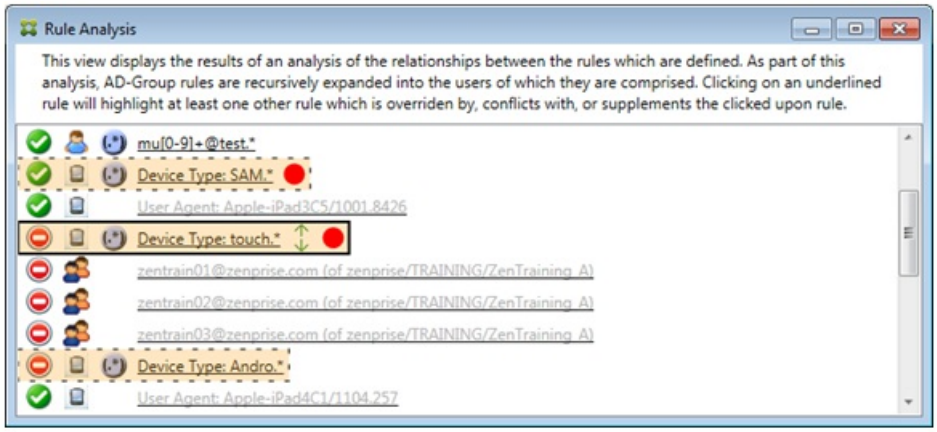


In diesem Fall wird die primäre Regel von einer einzigen Nebenregel außer Kraft gesetzt: der Regel mit der ActiveSync Geräte-ID und dem regelmäßigen Ausdruck 3E.*. Da der regelmäßige Ausdruck 3E.* auf 069026593E0C4AEAB8DE7DD589ACED33 zutrifft, würde die primäre Regel niemals ausgewertet.

Analysieren einer Ergänzung und eines Konflikts

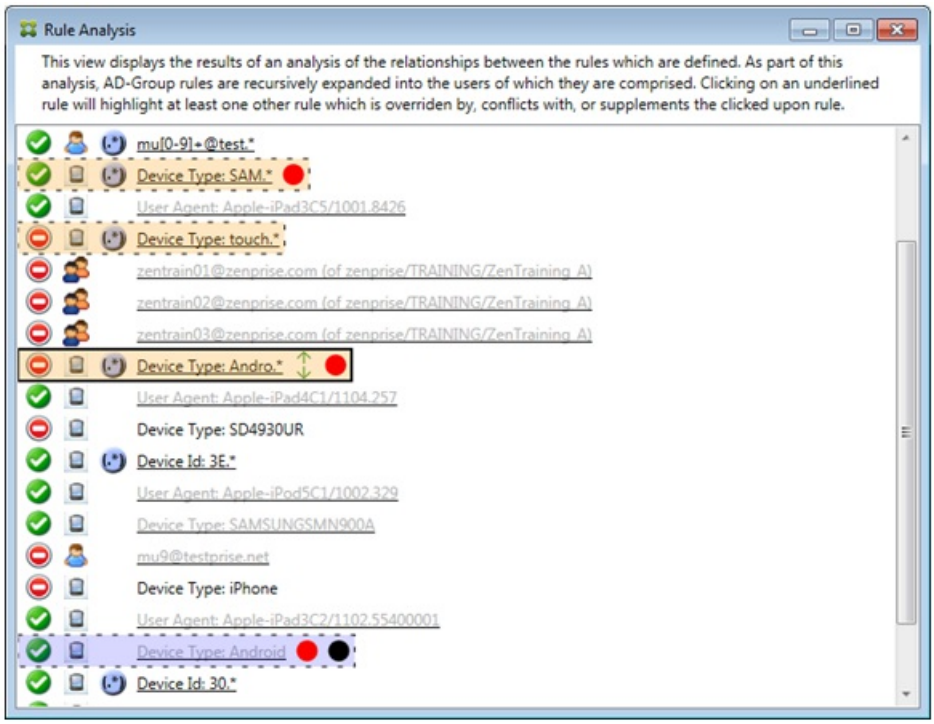
In diesem Beispiel ist die primäre Regel die ActiveSync-Gerätetypregel mit dem regelmäßigen Ausdruck touch.* Sie hat folgende Merkmale:

- Sie ist von einem durchgehenden Rahmen umgeben und mit einer gelben Überlagerung gekennzeichnet, welche anzeigt, dass mehrere Regeln mit regelmäßigen Ausdrücken auf das gleiche Feld abzielen (in diesem Fall "ActiveSync device type").
- Ein nach oben und ein nach unten weisender Pfeil geben an, dass es mindestens eine Nebenregel mit höherer Priorität und mindestens eine Nebenregel mit niedrigerer Priorität gibt.
- Der rote Punkt zeigt an, dass bei mindestens einer Nebenregel der Zugriffszustand auf Zulassen festgelegt ist und somit ein Konflikt mit der primären Regel besteht, bei welcher der Zugriffszustand auf Blockieren festgelegt ist.
- Es gibt zwei Nebenregeln: die ActiveSync-Gerätetypregel mit dem regelmäßigen Ausdruck SAM.* und die ActiveSync-Gerätetypregel mit dem regelmäßigen Ausdruck Andro.*.
- Beide Nebenregeln sind von einem gestrichelten Rahmen umgeben, welcher anzeigt, dass es sich um Nebenregeln handelt.
- Beide Nebenregeln haben eine gelbe Überlagerung, die anzeigt, dass sie ergänzend auf das Regelfeld "ActiveSync device type" angewendet werden.
- In einem solchen Szenario sollten Sie sicherstellen, dass die Regeln mit regelmäßigen Ausdrücken nicht redundant sind.



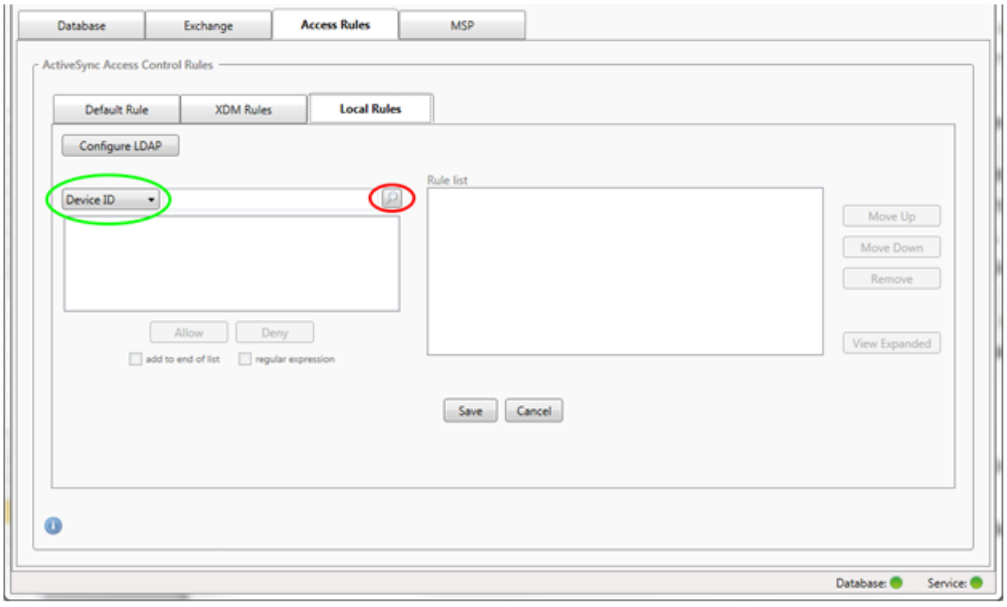
Weitere Analyse von Regeln

In diesem Beispiel wird demonstriert, dass Regelbeziehungen immer aus der Sicht der primären Regel dargestellt werden. Im vorherigen Beispiel wurde gezeigt, was beim Klicken auf die Gerätetypregel mit dem regelmäßigen Ausdruck touch.* angezeigt wird. Wird auf die Nebenregel Andro.* geklickt, werden andere Nebenregeln markiert.



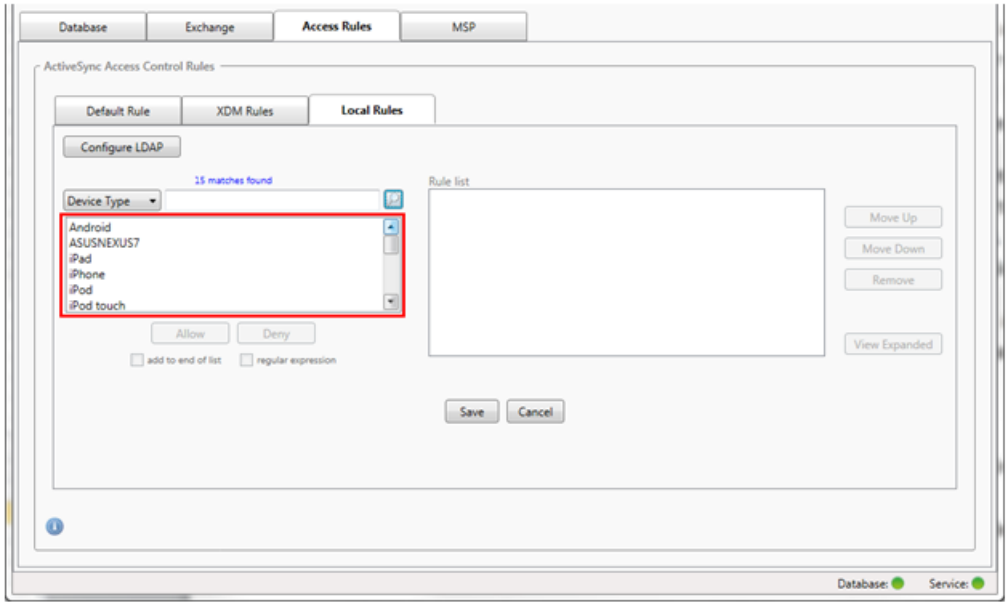
In diesem Beispiel wird eine außer Kraft gesetzte Regel, die Teil der Regelbeziehung ist, gezeigt. Diese Regel ist die normale ActiveSync-Gerätetypregel "Android", die außer Kraft gesetzt ist (sichtbar an der helleren Schrift und dem schwarzen Punkt) und deren Zugriffszustand mit dem der primären ActiveSync-Gerätetypregel mit regelmäßigem Ausdruck Andro.* einen Konflikt verursacht; letztere war vor dem Anklicken eine Nebenregel. Im vorherigen Beispiel wurde die normale ActiveSync-Gerätetypregel "Android" nicht als Nebenregel angezeigt, da sie aus Sicht der primären Regel (der ActiveSync-Gerätetypregel mit regelmäßigem Ausdruck touch.*) nicht mit dieser in Beziehung stand.

1. Klicken Sie auf die Registerkarte Access Rules.



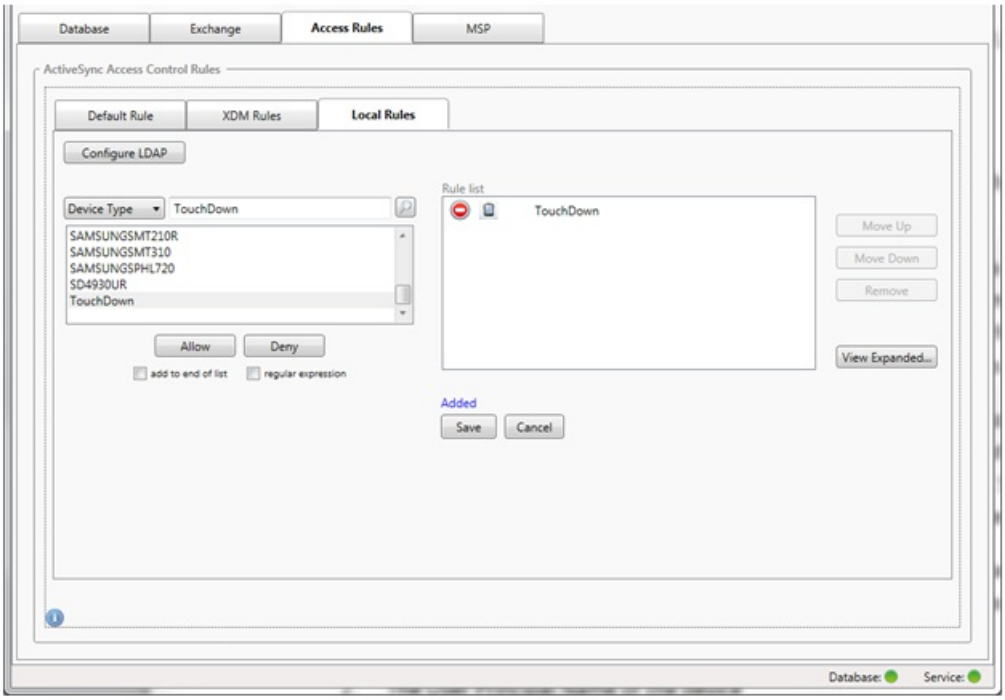
2. Wählen Sie in der Liste Device ID das Feld aus, für das Sie die lokale Regel erstellen möchten.

3. Klicken Sie auf das Lupensymbol, um alle eindeutigen Übereinstimmungen für das ausgewählte Feld einzublenden. In diesem Beispiel wurde das Feld Device Type ausgewählt, die Übereinstimmungen werden unterhalb des Listenfelds angezeigt.



4. Klicken Sie auf einen der Einträge in der Ergebnisliste und dann auf eine der folgenden Optionen:
   - Allow, sodass Exchange den ActiveSync-Datenverkehr für alle Benutzergeräte, auf welche die Regel zutrifft, zulässt.
   - Deny, sodass Exchange den ActiveSync-Datenverkehr für alle Benutzergeräte, auf welche die Regel zutrifft, verweigert.

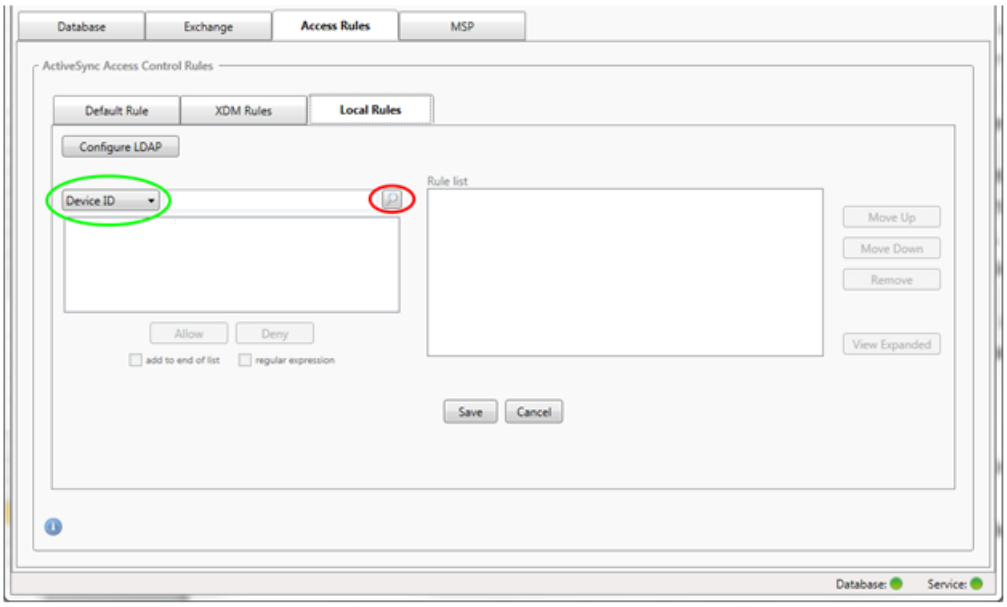
   In diesem Beispiel wird der Zugriff für alle Geräte des Typs TouchDown verweigert.



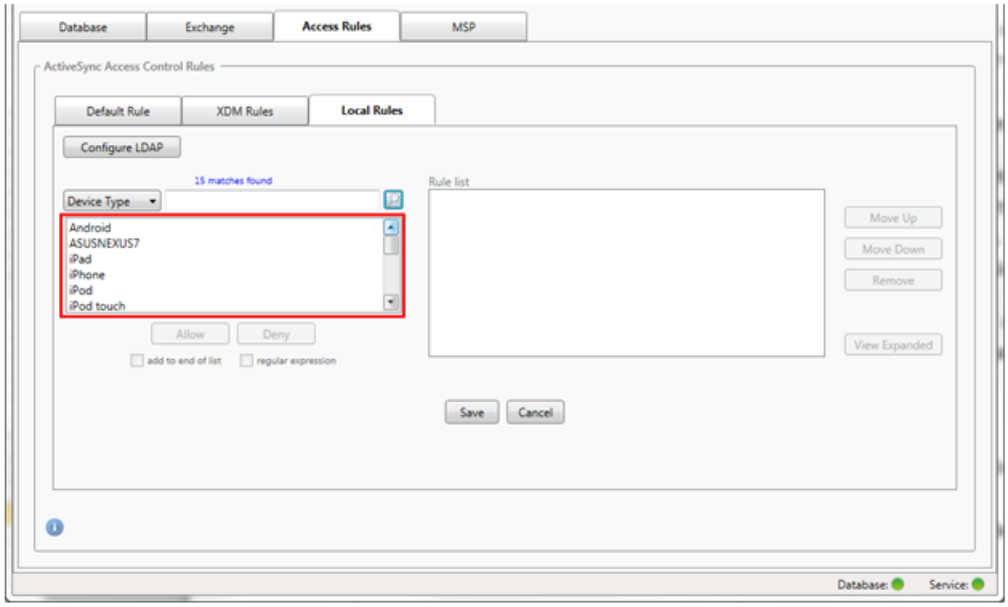
Lokale Regeln mit regelmäßigen Ausdrücken sind an dem Symbol (.*) zu erkennen. Zum Hinzufügen einer Regel mit regelmäßigem Ausdruck können Sie entweder einen Wert aus der Ergebnisliste für ein spezifisches Feld als Grundlage verwenden (sofern bereits ein größerer Snapshot durchgeführt wurde) oder den regelmäßigen Ausdruck selbst eingeben.

Erstellen eines regelmäßigen Ausdrucks mit einem vorhandenen Feldwert

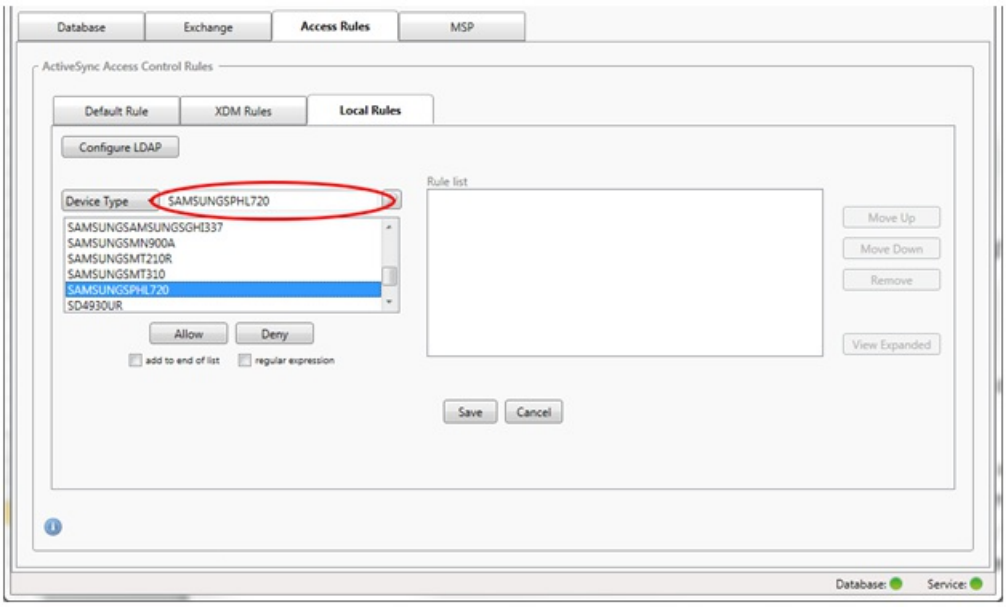
1. Klicken Sie auf die Registerkarte Access Rules.



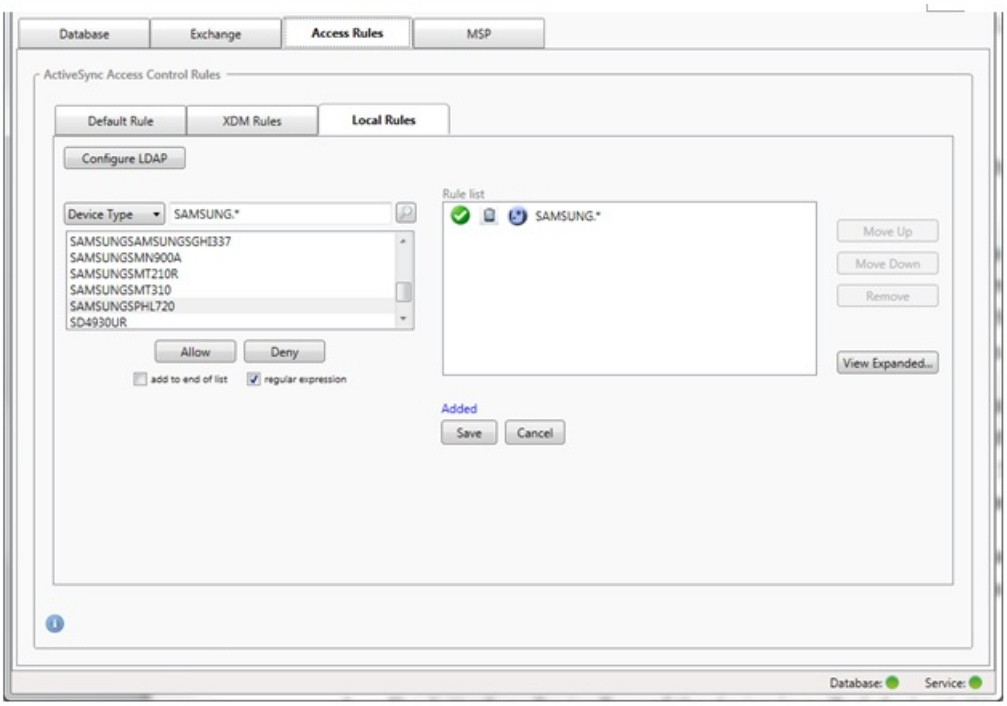
2. Wählen Sie in der Liste Device ID das Feld aus, für das Sie die lokale Regel mit einem regelmäßigen Ausdruck erstellen möchten.
3. Klicken Sie auf das Lupensymbol, um alle eindeutigen Übereinstimmungen für das ausgewählte Feld einzublenden. In diesem Beispiel wurde das Feld Device Type ausgewählt, die Übereinstimmungen werden unterhalb des Listenfelds angezeigt.



4. Klicken Sie auf einen der Einträge in der Ergebnisliste. In diesem Beispiel wurde SAMSUNGSPHL720 ausgewählt und erscheint im Textfeld neben Device Type.

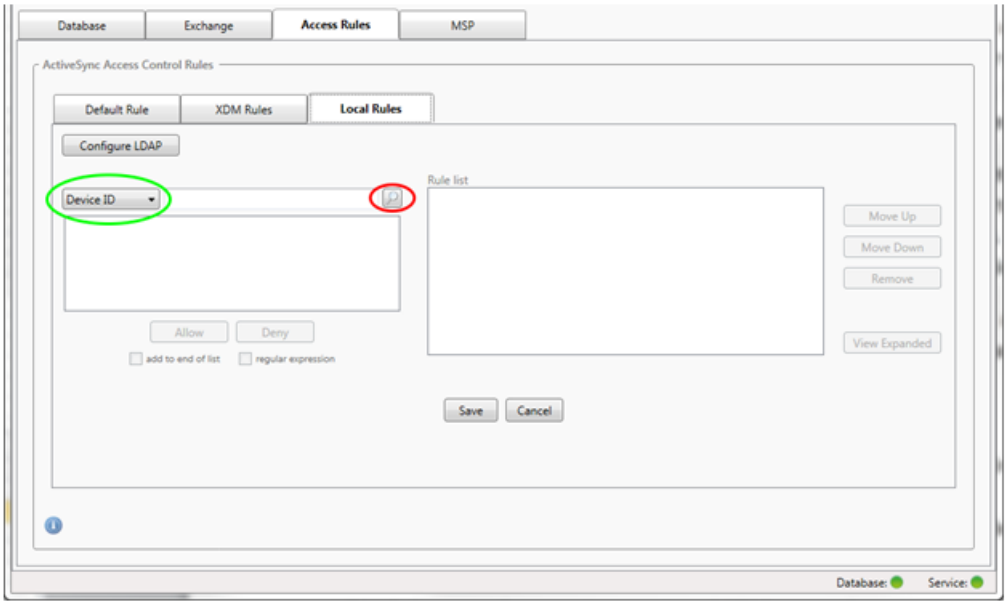


5. Damit alle Gerätetypen, deren Gerätetypwert "Samsung" enthält, zugelassen werden, fügen Sie eine Regel mit regelmäßigem Ausdruck wie folgt hinzu:
   1. Klicken Sie in das Textfeld des ausgewählten Elements.
   2. Ändern Sie den Text SAMSUNGSPHL720 in SAMSUNG.*
   3. Stellen Sie sicher, dass das Kontrollkästchen regular expression aktiviert ist.
   4. Klicken Sie auf Allow.

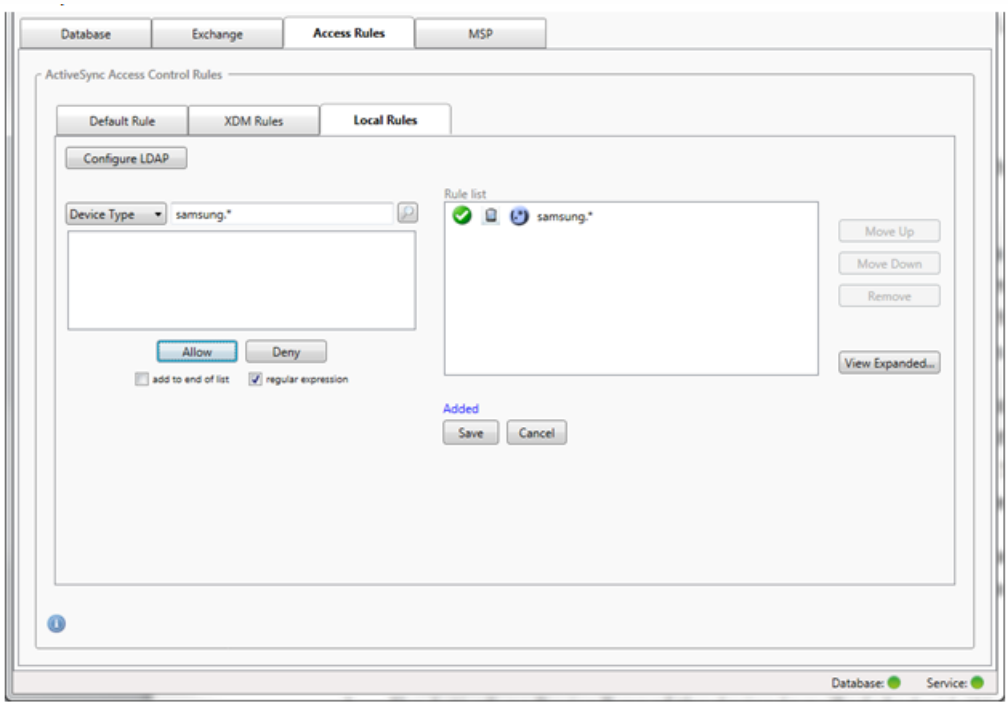


1. Klicken Sie auf die Registerkarte Local Rules.
2. Zum Eingeben des regelmäßigen Ausdrucks müssen Sie die Geräte-ID-Liste und das Textfeld des ausgewählten Elements

verwenden.



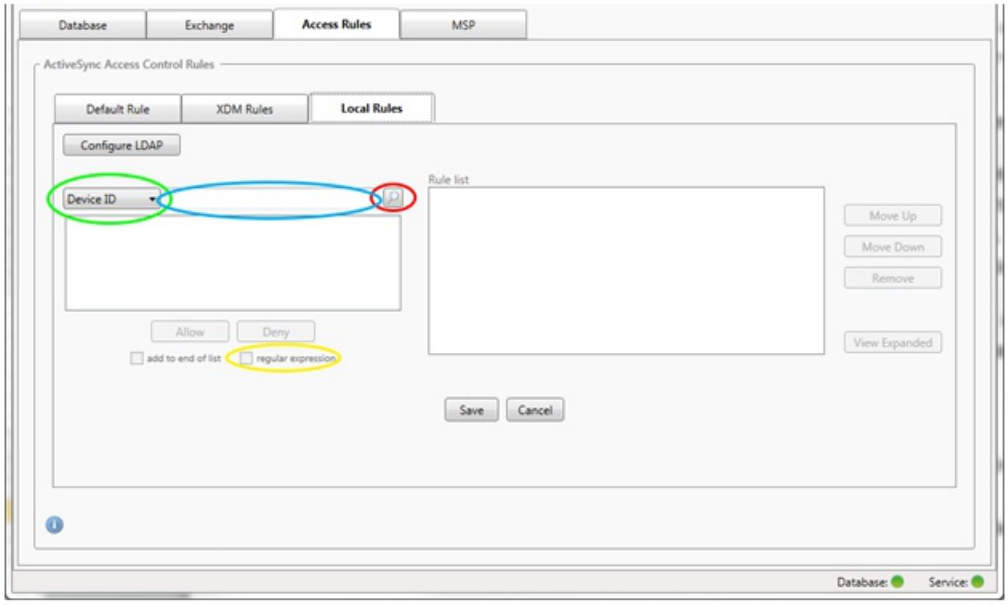
3. Wählen Sie das Feld aus, gegen das der Abgleich stattfinden soll. In diesem Beispiel ist dies Device Type.
4. Geben Sie den regelmäßigen Ausdruck ein. In diesem Beispiel ist diessamsung.*
5. Stellen Sie sicher, dass das Kontrollkästchen regular expression aktiviert ist, und klicken Sie auf Allow oder Deny. In diesem Beispiel lautet die Auswahl Allow und das Endergebnis ist wie folgt:



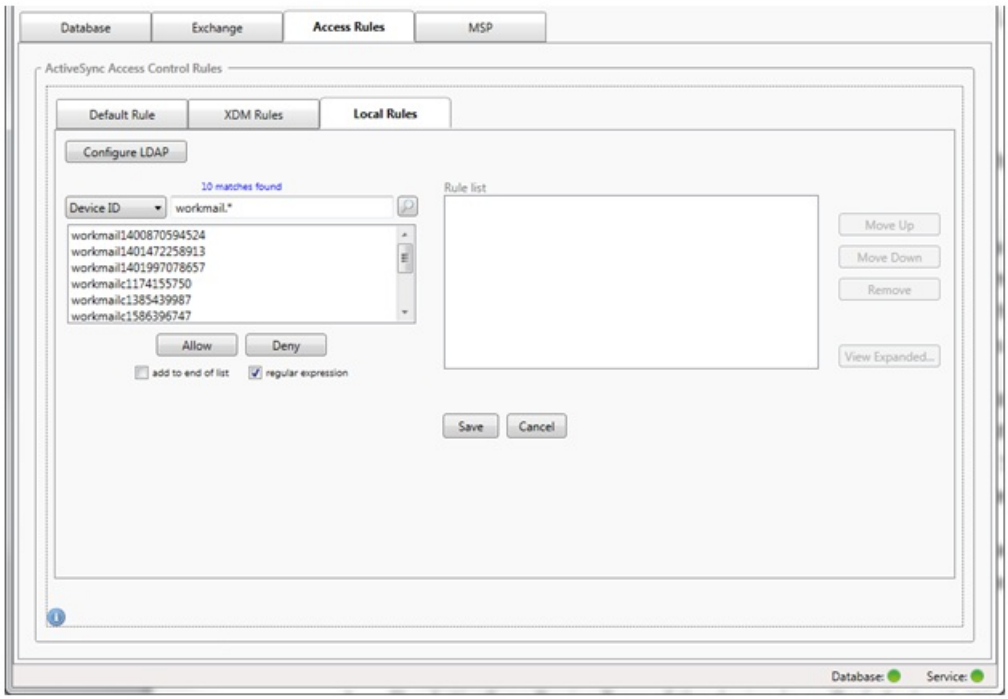
Durch Aktivieren des Kontrollkästchens "regular expression" können Sie Geräte, die dem angegebenen Ausdruck entsprechen, suchen. Dieses Feature steht nur zur Verfügung, wenn ein größerer Snapshot erfolgreich durchgeführt wurde. Sie können das Feature nutzen, selbst wenn Sie keine Verwendung regelmäßiger Ausdrücke planen. Beispiel: Sie möchten alle Geräte suchen, deren ActiveSync-Geräte-ID den Text "workmail" enthält. Gehen Sie hierfür wie nachfolgend

beschrieben vor.

1. Klicken Sie auf die Registerkarte Access Rules.
2. Stellen Sie sicher, dass die Abgleichfeldauswahl auf Device ID (Standardeinstellung) festgelegt ist.

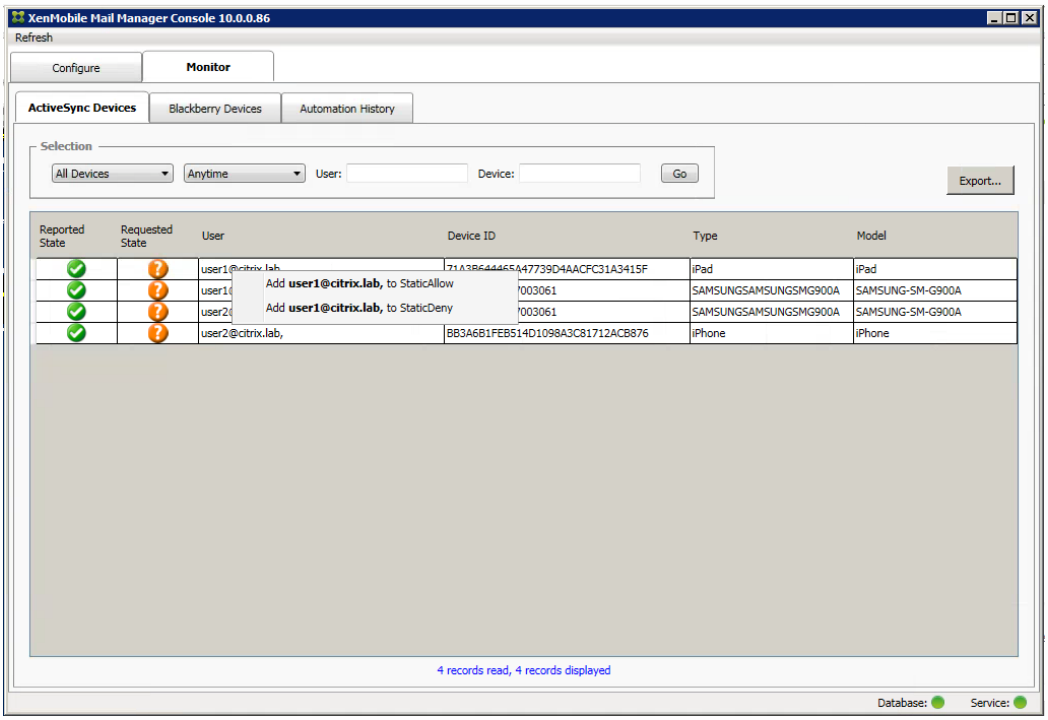


3. Klicken Sie in das Textfeld des ausgewählten Elements (blau in der Abbildung oben) und geben Sieworkmail.*ein.
4. Stellen Sie sicher, dass das Kontrollkästchen regular expression aktiviert ist, und klicken Sie auf das Lupensymbol, damit Übereinstimmungen angezeigt werden (siehe folgende Abbildung).



Sie können statische Regeln basierend auf Benutzern, Geräte-IDs oder Gerätetypen auf der Registerkarte ActiveSync Devices hinzufügen.

1. Klicken Sie auf die Registerkarte ActiveSync Devices.
2. Klicken Sie in der Liste mit der rechten Maustaste auf einen Benutzer, ein Gerät oder einen Gerätetyp und wählen Sie aus, ob dieser bzw. dieses zugelassen oder verweigert werden soll.
   Die folgende Abbildung zeigt die Allow-/Deny-Option für user1.



Geräteüberwachung

Nov 20, 2015

Die Registerkarte Monitor in XenMobile Mail Manager ermöglicht das Durchsuchen der erkannten Exchange ActiveSync- und BlackBerry-Geräte sowie des Verlaufs automatisch ausgegebener PowerShell-Befehle. Die Registerkarte Monitor enthält die folgenden drei Registerkarten:

- ActiveSync Devices:
  - Sie können die angezeigten ActiveSync-Geräte exportieren, indem Sie auf die Schaltfläche Export klicken.
  - Sie können lokale (statische) Regeln hinzufügen, indem Sie mit der rechten Maustaste auf die Spalte User, Device ID oder Type klicken und den entsprechenden Regeltyp zum Blockieren oder Zulassen auswählen.
  - Zum Reduzieren einer erweiterten Zeile drücken Sie die STRG-Taste und klicken Sie darauf.
- Blackberry Devices
- Automation History

Die Registerkarte Configure zeigt den Verlauf aller Snapshots. Der Snapshot-Verlauf zeigt an, wann ein Snapshot erstellt wurde, wie lange er dauerte, wie viele Geräte erkannt wurden und ggf. welche Fehler aufgetreten sind.

- Klicken Sie auf der Registerkarte Exchange auf das Info-Symbol für den gewünschten Exchange-Server.
- Klicken Sie auf der Registerkarte MSP auf das Info-Symbol für den gewünschten Blackberry-Server.

Problembehandlung und Diagnose

Nov 20, 2015

In folgender Protokolldatei von XenMobile Mail Manager werden Fehler und andere Betriebsinformationen aufgezeichnet: \log\XmmWindowsService.log. Von XenMobile Mail Manager werden auch wichtige Ereignisse im Windows-Ereignisprotokoll protokolliert.

Beispiele für verbreitete Fehler:

XenMobile Mail Manager-Dienst startet nicht

Prüfen Sie die Protokolldatei und das Windows-Ereignisprotokoll auf Fehler. Typische Ursachen:

- Der XenMobile Mail Manager-Dienst hat keinen Zugriff auf den SQL Server-Computer. Dafür kann Folgendes Ursache sein:
  - Der SQL Server-Dienst wird nicht ausgeführt.
  - Die Authentifizierung schlägt fehl.

  Wenn die integrierte Windows-Authentifizierung konfiguriert ist, muss das Benutzerkonto von XenMobile Mail Manager als zulässige SQL-Anmeldung konfiguriert sein. Standardmäßig ist das Konto des XenMobile Mail Manager-Diensts das lokale System, es kann aber in jedes beliebige Konto, das über lokale Administratorprivilegien verfügt, geändert werden. Wenn die SQL-Authentifizierung konfiguriert ist, muss die SQL-Anmeldung in SQL richtig konfiguriert sein.
- Der für den Mobile Service Provider konfigurierte Port ist nicht verfügbar. Es muss ein Überwachungsport verwendet werden, der von keinem anderen Prozess des Systems verwendet wird.

XenMobile kann keine Verbindung mit dem Mobile Service Provider herstellen

Stellen Sie auf der Registerkarte Configure> MSP der XenMobile Mail Manager-Konsole sicher, dass der Port und Transport für den Mobile Service Provider-Dienst ordnungsgemäß konfiguriert sind. Stellen Sie sicher, dass die Autorisierungsgruppe bzw. der Benutzer richtig eingestellt ist.
Wenn HTTPS konfiguriert ist, muss ein gültiges SSL-Serverzertifikat installiert sein. Wenn IIS installiert ist, kann IIS-Manager verwendet werden, um das Zertifikat zu installieren. Wenn IIS nicht installiert ist, konsultieren Sie den Artikel http://msdn.microsoft.com/en-us/library/ms733791.aspx zur Installation von Zertifikaten.

XenMobile Mail Manager enthält ein Hilfsprogramm zum Testen der Verbindung mit dem Mobile Service Provider-Dienst. Führen Sie das Programm MspTestServiceClient.exe aus, legen Sie die URL und die Anmeldeinformationen auf Werte fest, die in XenMobile konfiguriert werden, und klicken Sie dann auf Test Connectivity. Dies simuliert die vom XenMobile-Dienst ausgehenden Webdienstanfragen. Wenn HTTPS konfiguriert ist, müssen Sie den Hostnamen des Servers (den im SSL-Zertifikat angegebenen Namen) verwenden.

Hinweis: Für **Test Connectivity** muss mindestens ein ActiveSyncDevice-Datensatz vorhanden sein, sonst schlägt der Test möglicherweise fehl.

XenMobile NetScaler Connector

Oct 11, 2016

XenMobile NetScaler Connector bietet einen Authentifizierungsdienst auf Geräteebene für ActiveSync-Clients bei NetScaler, der als Reverseproxy für das Exchange ActiveSync-Protokoll fungiert. Die Autorisierung wird durch eine Kombination von Richtlinien, die Sie in XenMobile definieren, und lokal in XenMobile NetScaler Connector definierten Regeln gesteuert.

Weitere Informationen finden Sie in den folgenden Artikeln:

- XenMobile NetScaler Connector
- ActiveSync Gateway in XenMobile

Ein detailliertes Architekturdiagramm finden Sie im Artikel Reference Architecture for On-Premises Deployments in der XenMobile-Bereitstellungsdokumentation.