Info über XenMobile 10

Oct 13, 2016

In XenMobile 10 werden die XenMobile-Komponenten App Controller und Device Manager aus Version 9 und früheren Versionen zu einem einheitlichen Verwaltungstool zum Konfigurieren und Verwalten von Benutzergeräten und Apps zusammengefasst.

Hinweis: Der Remote Support-Client ist in XenMobile Cloud-Versionen 10.x für Windows CE- und Samsung Android-Geräte nicht verfügbar.

Bei der Planung einer XenMobile-Bereitstellung müssen viele Punkte berücksichtigt werden. Empfehlungen, Antworten auf allgemeine Fragen und Anwendungsfälle für XenMobile finden Sie in der XenMobile-Bereitstellungsdokumentation.

Neue Features

Eine Liste der in diesem Release behobenen Probleme finden Sie unter http://support.citrix.com/article/CTX141722 Eine Liste der bekannten Probleme in XenMobile 10.0 finden Sie unter Bekannte Probleme.

- **Einheitliche Infrastruktur**: Mobilgeräteverwaltung (MDM) und Mobilanwendungsverwaltung (MAM) wurden innerhalb einer einheitlichen Serverinfrastruktur zusammengefasst.
  - Schnellere Bereitstellung von XenMobile mit weniger Setupschritten.
  - Verwaltung von Apps und Geräten über einen virtuellen Server.
- **Neue, einheitliche XenMobile-Konsole:**
  - Die intuitive Benutzeroberfläche vereinfacht Verwaltungsaufgaben wie die Registrierung, Bereitstellung, Konfiguration und Problembehandlung der gesamten Mobilitätsumgebung.
  - Vereinfachte Richtlinienkonfiguration für Apps und Geräte. Konfigurieren Sie eine Richtlinie für alle verfügbaren Geräteplattformen.
- **Integration mit NetScaler Gateway über dieselbe Konsole:** Verwalten automatischer Konnektivitätsprüfungen für Systeme, die zur Mobilitätsumgebung gehören.
- **Unterstützung von Beacons außer Gebrauch:** Beacons werden nicht in XenMobile 10 unterstützt, auch wenn Optionen noch in der XenMobile-Konsole angezeigt werden. Citrix empfiehlt, dass Sie entweder die Verbindung zum XenMobile-Server über NetScaler Gateway herstellen oder von innerhalb der Firewall direkt zum XenMobile-Server.
- **Erweiterte Unterstützung für App-Authentifizierung:** Sichert die Verschlüsselung zwischen Geräten und dem internen Netzwerk, zwischen dem internen Netzwerk und dem XenMobile-Server und für XenMobile-Konsolenverbindungen.
  - Adaptive Authentifizierung mit RSA
  - Unterstützung für erweiterte Verschlüsselung mit FIPS 140.2

Erste Schritte mit XenMobile 10

Laden Sie als Erstes das virtuelle Image für XenMobile 10.0 Edition herunter und installieren Sie es auf einem Hypervisor, z. B. XenServer, VMware ESXi oder Hyper-V. Schließen Sie dann die Erstkonfiguration von XenMobile über die Befehlszeilenkonsole des Hypervisors ab. Weitere Informationen finden Sie unter Systemanforderungen, Installationscheckliste und Installieren von XenMobile.

Öffnen Sie als Nächstes die webbasierte XenMobile-Konsole mit dem Administratorkonto, das Sie während der

Erstkonfiguration eingerichtet haben.

Unter Erste Schritte mit der Konsole finden Sie Informationen zum weiteren Navigieren in der Konsole. Die Empfehlungen zu Beginn beziehen sich auf Ersteinstellungen, die Sie während der Installation möglicherweise übersprungen haben.

Architektur im Überblick

Oct 13, 2016

Welche XenMobile-Komponenten Sie in der XenMobile-Referenzarchitektur bereitstellen, hängt von den Anforderungen des Unternehmens an die Geräte- bzw. App-Verwaltung ab. Die Komponenten von XenMobile sind modular und bauen aufeinander auf. Beispielsweise könnten Sie beabsichtigen, Benutzern Remotezugriff auf mobile Apps zu erteilen und die Gerätetypen, mit denen Benutzer eine Verbindung herstellen, zu überwachen. In diesem Szenario würden Sie XenMobile mit NetScaler Gateway bereitstellen. In XenMobile verwalten Sie Apps und Geräte und NetScaler Gateway ermöglicht den Benutzern die Verbindung mit Ihrem Netzwerk.

Bereitstellen von XenMobile Komponenten: Für die Bereitstellung von XenMobile zur Verwendung von Ressourcen im internen Netzwerk durch die Benutzer gibt es folgende Möglichkeiten:

- Verbindungen mit dem internen Netzwerk: Benutzer außerhalb des Netzwerks können mit einer VPN- oder Micro VPN-Verbindung über NetScaler Gateway auf Apps und Desktops im internen Netzwerk zugreifen.
- Device enrollment: Benutzer können Mobilgeräte in XenMobile registrieren, damit Sie die Geräte, die eine Verbindung mit Netzwerkressourcen herstellen, in der XenMobile-Konsole verwalten können.
- Web-, SaaS- und Mobilanwendungen: Benutzer können auf ihre Web-, SaaS- und mobilen Apps von XenMobile über Worx Home zugreifen.
- Windows-basierte Anwendungen und virtuelle Desktops: Benutzer können eine Verbindung mit Citrix Receiver oder einem Webbrowser herstellen, um auf Windows-basierte Anwendungen und virtuelle Desktops von StoreFront oder Webinterface zuzugreifen.

Zur Bereitstellung einiger oder aller dieser Funktionen empfiehlt Citrix die Bereitstellung von XenMobile-Komponenten in der folgenden Reihenfolge:

- NetScaler Gateway: Sie können Einstellungen in NetScaler Gateway für die Kommunikation mit XenMobile, StoreFront oder dem Webinterface mit dem Konfigurationsassistenten konfigurieren. Vor der Verwendung des Konfigurationsassistenten in NetScaler Gateway müssen Sie XenMobile, StoreFront oder das Webinterface installieren, damit Sie die Kommunikation damit einrichten können.
- XenMobile: Nach der Installation von XenMobile können Sie Richtlinien und Einstellungen in der XenMobile-Konsole konfigurieren, mit denen Benutzer ihre Mobilgeräte registrieren können. Außerdem können Sie mobile, Web- und SaaS-Apps konfigurieren. Mobile Anwendungen können auch Apps aus dem Apple App Store oder Google Play sein. Die Benutzer können auch eine Verbindung mit mobilen Apps herstellen, die Sie mit dem MDX Toolkit umschließen und in die Konsole hochladen.
- MDX Toolkit: Mit dem MDX Toolkit können Sie in Ihrem Unternehmen erstellte Anwendungen und mobile, außerhalb des Unternehmens erstellte Apps (wie die Citrix Worx-Apps) sicher umschließen. Nach dem Umschließen einer App können Sie die App über die XenMobile-Konsole zu XenMobile hinzufügen und die Richtlinienkonfiguration nach Bedarf anpassen. Sie können außerdem App-Kategorien hinzufügen, Workflows anwenden und Apps für Bereitstellungsgruppen bereitstellen.
- StoreFront (optional): Sie können den Zugriff auf Windows-basierte Anwendungen und virtuelle Desktops von StoreFront über Verbindungen mit Receiver bereitstellen.
- ShareFile Enterprise (optional): Wenn Sie ShareFile bereitstellen, können Sie die Integration des Unternehmensverzeichnisses über XenMobile aktivieren, das als SAML-Identitätsanbieter (Security Assertion Markup Language) fungiert. Weitere Informationen zum Konfigurieren von Identitätsanbietern für ShareFile finden Sie auf der ShareFile-Supportsite.

In den folgenden Abschnitten werden verschiedene Referenzarchitekturen für die XenMobile-Bereitstellung beschrieben. Referenzarchitekturdiagramme finden Sie in den Abschnitten Reference Architecture for On-Premises Deployments und Reference Architecture for Cloud Deployments in der XenMobile-Bereitstellungsdokumentation. Eine vollständige Liste der Ports finden Sie unter Portanforderungen für XenMobile.

In einer Produktionsumgebung empfiehlt Citrix die Bereitstellung der XenMobile-Lösung in einer Clusterkonfiguration zur Gewährleistung von Skalierbarkeit und Serverredundanz. Die Nutzung der SSL-Offload-Funktion von NetScaler kann die Last für den XenMobile-Server weiter vermindern und den Durchsatz erhöhen. Weitere Informationen zum Einrichten von Clustering für XenMobile 10.x durch die Konfiguration von zwei virtuellen IP-Adressen zum Lastausgleich auf NetScaler finden Sie unter Konfigurieren von Clustering für XenMobile 10.

Mobilgeräteverwaltungsmodus (MDM-Modus)

XenMobile MDM Edition bietet Mobilgeräteverwaltung für iOS, Android, Amazon und Windows Phone (siehe Unterstützte Geräteplattformen in XenMobile 10). Stellen Sie XenMobile im MDM-Modus bereit, wenn Sie planen, nur die MDM-Features von XenMobile zu verwenden. Beispielsweise müssen Sie vom Unternehmen bereitgestellte Geräte per MDM verwalten, um Richtlinien und Apps bereitzustellen, Assetinventare abzurufen und Aktionen wie Löschvorgänge auf Geräten auszuführen.

Bei dem empfohlenen Modell befindet sich der XenMobile-Server in der DMZ, eine optionale Platzierung hinter einem NetScaler bietet zusätzlichen Schutz für XenMobile.

Mobilanwendungsverwaltungsmodus (MAM-Modus)

MAM unterstützt iOS- und Android-Geräte, aber keine Windows Phone-Geräte (weitere Informationen finden Sie unter Unterstützte Geräteplattformen in XenMobile 10). Stellen Sie XenMobile im MAM-Modus (bzw. Nur-MAM-Modus) bereit, wenn Sie planen, nur die MDM-Features von XenMobile zu verwenden und keine Geräte für MDM zu registrieren. Beispielsweise können Sie Apps und Daten auf BYO-Mobilgeräten sichern, mobile Unternehmens-Apps bereitstellen sowie Apps sperren und deren Daten löschen. Die Geräte dürfen nicht nicht für die Mobilgeräteverwaltung (MDM) registriert sein.

Bei diesem Bereitstellungsmodell befindet sich der XenMobile-Server hinter einem NetScaler Gateway, das zusätzlichen Schutz für XenMobile bietet.

MDM+MAM-Modus

Die Verwendung von MDM und MAM zusammen ermöglicht die Verwaltung mobiler Apps und Daten sowie von Mobilgeräten für iOS, Android und Windows Phone (weitere Informationen finden Sie unter Unterstützte Geräteplattformen in XenMobile 10). Stellen Sie XenMobile im ENT-Modus (Enterprise) bereit, wenn Sie planen, die MDM- und MAM-Features von XenMobile zu verwenden. Beispielsweise können Sie vom Unternehmen bereitgestellte Geräte per MDM verwalten, Richtlinien und Apps bereitzustellen, Assetinventare abrufen und Daten von Geräten löschen. Zudem können Sie mobile Unternehmens-Apps bereitstellen, Apps sperren und die Daten auf Benutzergeräten löschen.

Bei dem empfohlenen Bereitstellungsmodell befindet sich der XenMobile-Server in der DMZ hinter einem NetScaler Gateway, das zusätzlichen Schutz für XenMobile bietet.

Skalierung von XenMobile 10

Oct 12, 2015

Die Kenntnis der Größe der XenMobile-Infrastruktur ist ein wichtiger Faktor bei der Entscheidung darüber, wie Sie XenMobile bereitstellen und konfigurieren. Dieser Artikel enthält Antworten auf häufige Fragen zur Ermittlung der Anforderungen für kleine bis große Bereitstellungen.

Richtlinien für Leistung und Skalierbarkeit

Die Angaben in diesem Artikel dienen als Richtlinie zur Bestimmung von Leistung und Skalierbarkeit einer XenMobile-Infrastruktur. Die zwei wichtigsten Faktoren bei der Konfiguration von Server und Datenbank sind die Skalierbarkeit (maximale Benutzer-/Gerätezahl) und die Anmelderate.

- Skalierbarkeit ist die maximale Anzahl gleichzeitig arbeitender Benutzer, die eine definierte Arbeitslast ausführen. Informationen zu den Abläufen beim Laden der XenMobile-Infrastruktur finden Sie unter Arbeitslasten.
- Die Anmelderate bezieht sich auf das Onboarding neuer Benutzer und die Authentifizierung bestehender Benutzer.
  - Die Onboardingrate ist die maximale Anzahl Geräte, die erstmals in der Umgebung registriert werden können. Dieser im vorliegenden Artikel als Erstverwendung (Englisch auch FTU) bezeichnete Datenpunkt ist bei der Planung einer Implementierungsstrategie wichtig.
  - Die Rate vorhandener Benutzer ist die maximale Anzahl der bei der Umgebung authentifizierten Benutzer, die sich bereits registriert und eine Verbindung über ihr Gerät hergestellt haben. Diese Tests umfassten auch die Erstellung von Sitzungen für bereits registrierte Benutzer und die Ausführung von WorxMail- und WorxWeb-Apps.

Die folgende Tabelle enthält Skalierbarkeitsrichtlinien basierend auf den Testergebnissen für die entsprechende XenMobile-Umgebung.

Tabelle 1. XenMobile Enterprise mit Registrierung

Skalierbarkeit	Maximal 100.000 Geräte	
Anmelderaten	Onboarding (Erstverwendung)	Maximal 2.777 Geräte pro Stunde
	Vorhandene Benutzer	Maximal 16.667 Geräte pro Stunde
Konfiguration	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	XenMobile-Servercluster mit 10 Knoten
	Datenbank	Externe Microsoft SQL Server-Datenbank

Systemkonfiguration und Testergebnisse

In diesem Abschnitt werden die Hardwarekonfiguration für die Arbeitslast-Skalierbarkeitstests für Onboarding und vorhandene Benutzer sowie die Testergebnisse beschrieben.

Die nachstehende Tabelle enthält die Empfehlungen für Hardware und Konfiguration für XenMobile bei einer Skalierung zwischen 1000 und 100.000 Geräten. Diese Richtlinien basieren auf Testergebnissen und den zugehörigen Arbeitslasten. Bei den Empfehlungen wurde eine akzeptable Fehlerspanne angelegt (siehe Ausgangskriterien).

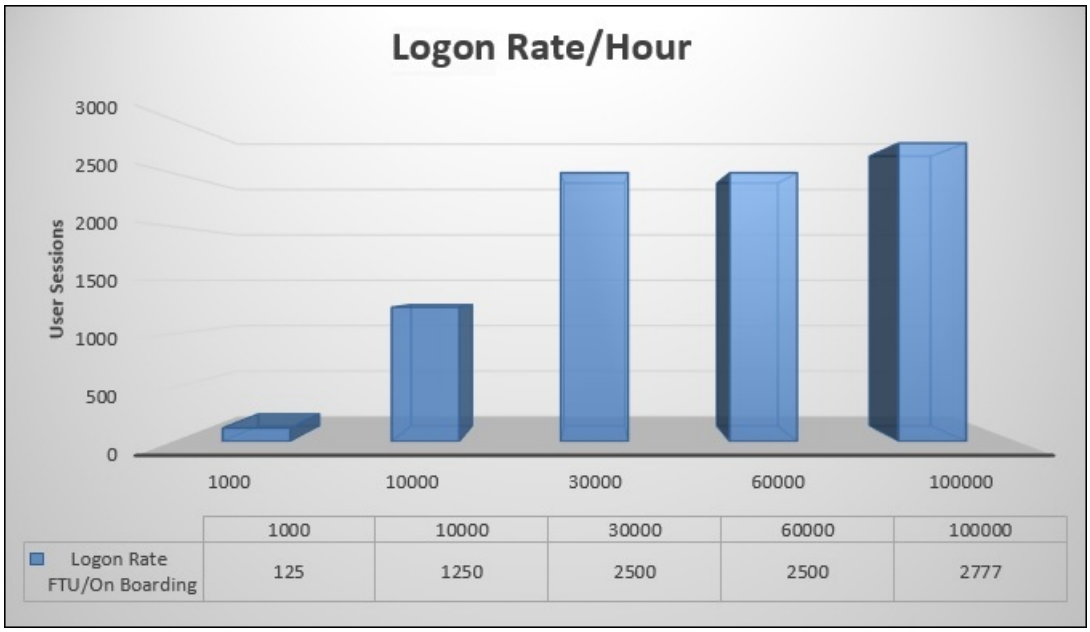
Die Analyse der Testergebnisse hat zu folgenden Schlussfolgerungen geführt:

- Die Anmelderate ist ein wichtiger Faktor beim Bestimmen der Skalierbarkeit eines Systems. Neben der Erstanmeldung hängen Anmelderaten auch von den in der Umgebung konfigurierten Timeoutwerten für die Authentifizierung ab. Wird der Timeoutwert z. B. zu niedrig gewählt, müssen Benutzer häufiger Anmeldeanforderungen durchführen. Es ist daher wichtig zu wissen, wie sich Timeouteinstellungen auf die Umgebung auswirken.
- Für die Tests wurde eine externe Datenbank (SQL Server) mit 128 GB RAM, 300 GB Speicherplatz und 24 virtuellen CPUs verwendet. Eine solche wird auch für Produktionsumgebungen empfohlen.
- Zur Erzielung einer maximalen Skalierbarkeit wurden CPU- und RAM-Ressourcen in XenMobile erhöht.
- Die Konfiguration mit 10 Clusterknoten war die größte geprüfte Konfiguration. Eine Skalierung über 10 Knoten hinaus erfordert eine zusätzliche XenMobile-Implementierung.

Tabelle 2. Skalierbarkeitsergebnisse für XenMobile Enterprise mit Registrierung

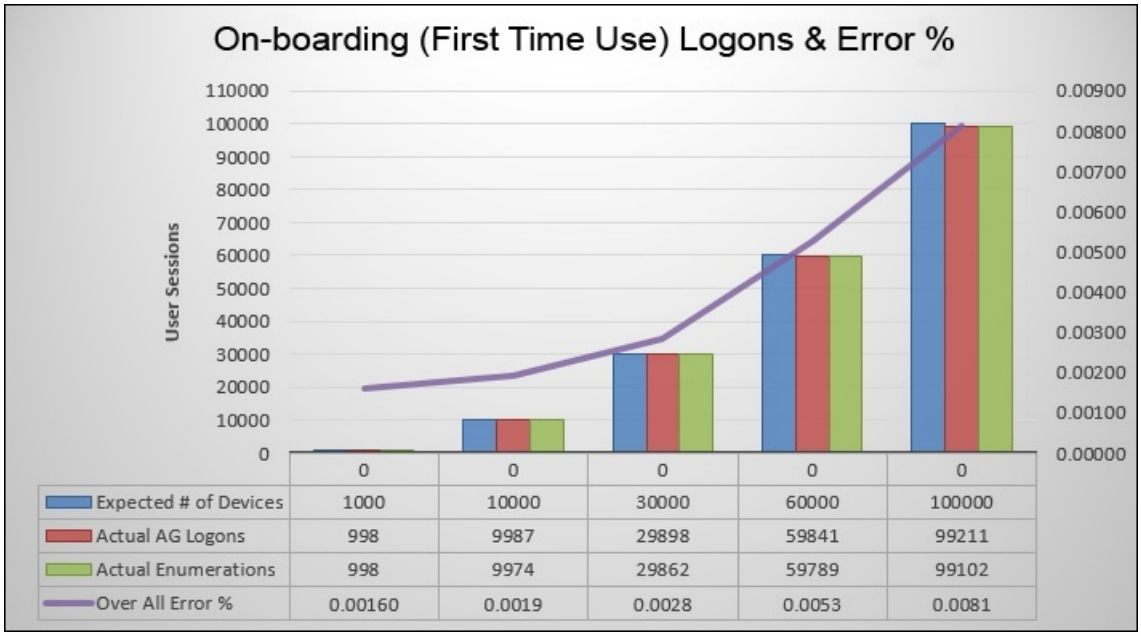
Anzahl der Geräte	**1.000**	**10.000**	**30.000**	**60.000**	**100.000**
Anmelderate					
Onboarding (Erstverwendung)	125	1.250	2.500	2.500	2.777
Vorhandene Benutzer	1.000	2.500	7.500	15.000	16.667
Konfiguration					
Referenzumgebung	VPX-XenMobile, eigenständig	MPX-XenMobile, eigenständig	MPX-XenMobile, Cluster (3)	MPX-XenMobile, Cluster (6)	MPX-XenMobile, Cluster (10)
NetScaler Gateway	VPX mit 2 GB RAM 2 virtuelle CPUs	MPX-10500		MPX-20500	
XenMobile-Modus	Eigenständig	Eigenständig	Cluster		
XenMobile-Cluster	nicht zutreffend	nicht zutreffend	3	6	10
XenMobile – virtuelles Gerät	8 GB RAM und 4 virtuelle CPUs	8 GB RAM und 4 virtuelle CPUs	8 GB RAM und 4 virtuelle CPUs	16 GB RAM und 4 virtuelle CPUs	16 GB RAM und 4 virtuelle CPUs
Datenbank	Externe Schicht				

Die Tabelle oben enthält die empfohlenen Raten für Onboarding und vorhandene Benutzer basierend auf XenMobile-Konfiguration NetScaler Gateway-Gerät, Clustereinstellungen und Datenbank. Anhand der Daten in dieser Tabelle können Sie einen optimalen Registrierungsplan für neue Bereitstellungen und einen Plan für die Raten wiederkehrender Benutzer/Geräte für vorhandene Bereitstellungen erstellen. Im Abschnitt "Konfiguration" werden Leistungsdaten für Registrierung und Anmeldung den entsprechenden Hardwareempfehlungen zugeordnet.



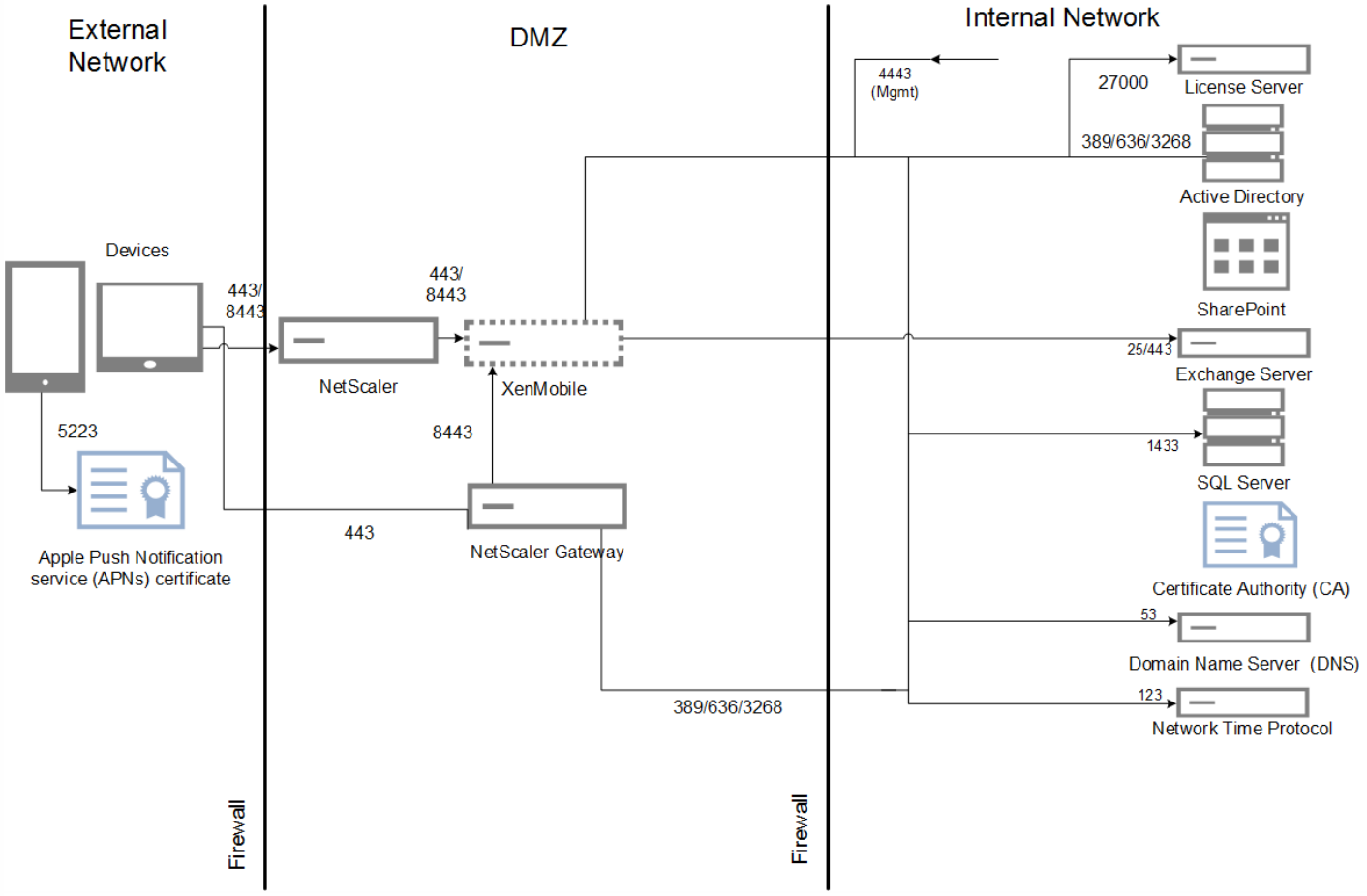
Hinweis: Wenn Sie bei der Dimensionierung des Systems die empfohlenen Raten überschreiten oder die Hardwareempfehlungen nicht beachten, treten die nachfolgenden Probleme auf.

- Registrierungs- bzw. Anmeldelatenz (Roundtripzeit)
  - Durchschnittliche Latenz insgesamt: > 1,5 Sekunden
  - Durchschnittliche Latenz bei NetScaler Gateway-Anmeldungen: > 440 ms
  - Durchschnittliche Latenz bei Worx Store-Anforderungen: > 3 Sekunden
- Bei Erreichen der Skalierbarkeitslimits wurden Beeinträchtigungen der physischen Leistung, z. B. Aufbrauchen von CPU und Speicher, bei Infrastrukturkomponenten beobachtet.
  - Ungültige Antworten bei NetScaler Gateway- und XenMobile-Geräten
  - Lange Antwortzeit bei der XenMobile-Konsole

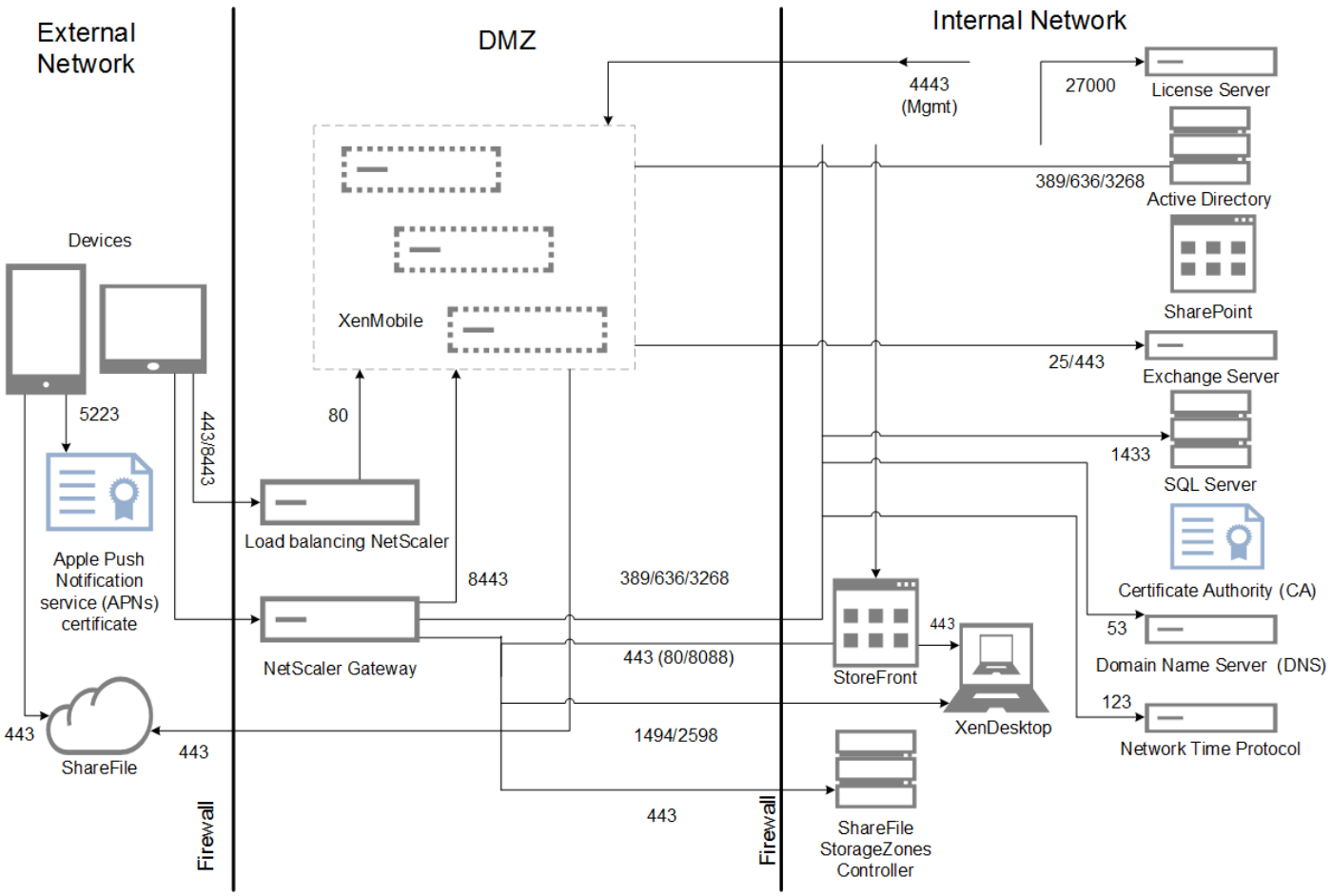


Der Fehlerprozentsatz in der Abbildung oben enthält Fehler insgesamt bei Anforderungen für alle Vorgänge und nicht nur für Anmeldungen. Der Fehlerprozentsatz ist für jeden Testlauf akzeptabel gemäß den im Abschnitt Ausgangskriterien aufgeführten Kriterien.

Die folgende Abbildung zeigt die Referenzarchitektur für eine kleine Bereitstellung. Es ist eine eigenständige Architektur für bis zu 10.000 Geräte.



Die folgende Abbildung zeigt die Referenzarchitektur für eine Unternehmensbereitstellung. Es ist eine Clusterarchitektur mit SSL-Offload für MDM über HTTP für 10.000 oder mehr Geräte.



Testmethode

Die Tests wurden an XenMobile Enterprise zur Benchmarkerstellung ausgeführt. Zum Testen sowohl kleiner und als auch großer Bereitstellungen wurden 1000 bis 10.0000 Geräten bei den Messungen verwendet.

Zur Simulation realer Anwendungsfälle wurden Arbeitslasten erstellt. Diese Arbeitslasten wurden für jeden Test ausgeführt, um die Auswirkungen auf Registrierungs- und Anmelderaten zu prüfen. Ziel der Tests war die Bestimmung der optimalen Anmelderate mit einer akzeptablen Fehlerspanne (siehe Ausgangskriterien). Anmelderaten sind ein wichtiger Faktor bei der Zusammenstellung von Empfehlungen für die Hardwarekonfiguration von Infrastrukturkomponenten.

Onboarding-Anmeldeanforderungen umfassten Vorgänge für automatische Ermittlung, Authentifizierung und Geräteregistrierung. Vorgänge für Abonnement, Installation und Starten von Apps waren gleichmäßig über den Testzeitraum verteilt. Damit wurde die beste Simulation realer Benutzeraktionen erzielt. Bei Testende erfolgte die Abmeldung der Sitzung. Anmeldeanforderungen für bestehende Benutzer umfassten nur Authentifizierungsanforderungen.

Arbeitslasten

Benutzerarbeitslasten werden wie folgt definiert:

Tabelle 3. Definition von Benutzerarbeitslasten

Benutzersitzungen/Geräte	Umfasst Anmeldungen bei NetScaler Gateway, Enumerationen, Geräteregistrierungen usw.

	für jede Sitzung.
Worx Store-Starts	Benutzer starten Worx Store mehrmals und abonnieren oder installieren jedes Mal mehrere Apps, unabhängig davon, ob es sich um eine mobile App (Web/SaaS/MDX) oder Windows-App (HDX) handelt.
Web-/SaaS-App, SSO pro Gerät	Startsequenz bei Web- und SaaS-Apps bis zu dem Punkt, an dem XenMobile das SSO abschließt und die tatsächliche App-URL zurückgibt. Es wurden keine Daten an die Apps selbst gesendet.
MDX-App-Downloads pro Gerät	Anzahl der MDX-App-Downloads (kann Worx Store-startübergreifend erfolgen). Bei iOS-Apps enthält dieser Wert außerdem die Automatisierung der App-Installation über Apple ITMS, bei der die neuen token/tms-Dienst-APIs von NetScaler Gateway genutzt werden.

On-Boarding (FTU)-Arbeitslast

Die Onboarding-Arbeitslast entsteht beim ersten Zugriff eines Benutzers auf die XenMobile-Umgebung. Diese Arbeitslast umfasste folgende Vorgänge:

- Automatische Ermittlung
- Enrollment
- Authentifizierung
- Geräteregistrierung
- App-Bereitstellung (Web-, SaaS- und mobile MDX-Apps)
  - App-Abonnement (einschließlich Download von Bildern und Symbolen)
  - Installation der abonnierten MDX-Apps
- App-Start (Web-, SaaS- und mobile MDX-Apps)
- Minimale WorxMail- und WorxWeb-Verbindungen (VPN-Tunnel): zwei Verbindungen
- Installation erforderlicher Apps über XenMobile

Arbeitslastparameter:

- 1 Geräteregistrierung pro Gerät
- 1 Enumeration pro Gerät
- 14 enumerierte Apps pro Gerät
- 4 Worx Store-Starts pro Gerät
- 4 Web-/SaaS-App-SSOs pro Gerät
- 1 MDX-App pro Gerät heruntergeladen
- 2 Downloads erforderlicher Apps

Arbeitslast für vorhandene Benutzer

In der folgenden Tabelle wird die Arbeitslast für vorhandene Benutzer aufgeführt. Diese Arbeitslast simulierte einen Benutzer mit WorxMail- und WorxWeb-Apps. Diese Simulation wurde zum Messen der Skalierbarkeit des NetScaler Gateway-Ports innerhalb der XenMobile-Konfiguration verwendet. Bei der WorxWeb-App erfolgte der Zugriff der Benutzer auf interne Websites, die kein XenMobile-SSO auslösen. Dieser Modus umfasste folgende Vorgänge:

- Authentifizierung (NetScaler Gateway und XenMobile)

- WorxMail- und WorxWeb-Verbindungen (VPN-Tunnel): vier Verbindungen

Worx-Apps-Verbindungsprofile

In der folgenden Tabelle werden die Arbeitslastparameter für bestehende Benutzer aufgeführt.

Tabelle 4. Worx-Apps-Verbindungsprofile

Geräteverbindung	Verbindungstyp	Gesendete Daten pro Sitzung[1]	Empfangene Daten pro Sitzung[1]
WorxMail-Verbindung 1	Typ 1[2]	4,1 MB	4,1 MB
WorxMail-Verbindung 2	Typ 1	6,3 MB	12,5 MB
WorxWeb-Verbindung 1	Typ 2[3]	5,2 MB	15,7 MB
WorxWeb-Verbindung 2	Typ 2	4,1 MB	3,4 MB
Pro Sitzung[1] übertragene Byte, gesamt		~ 19,7 MB	~ 40,7 MB

1. **Sitzung**: 8 Stunden

2. **Typ 1**: asymmetrisches Senden und Empfangen mit langlebigen Verbindungen (d. h. WorxMail mit einer dedizierten Microsoft Exchange-Postfachverbindung)

3. **Typ 2**: asymmetrische Senden und Empfangen mit Verbindungen, die nach Verzögerungen geschlossen und wieder geöffnet werden (d. h. WorxWeb-Verbindungen)

Hinweis: Änderungen an den Verbindungen wirken sich auf die Analyseergebnisse aus. Wenn beispielsweise die Zahl der Verbindungen pro Benutzer erhöht wird, sinkt möglicherweise die Zahl der unterstützten NetScaler Gateway-Sitzungen.

WorxMail- und WorxWeb-Profile

Die folgenden Tabellen zeigen die Daten der WorxMail- und WorxWeb-Profile.

Tabelle 5. WorxMail-Profil – mittlere Arbeitslast

Pro Tag gesendete Nachrichten	20
Pro Tag empfangene Nachrichten	80
Pro Tag gelesene Nachrichten	80
Pro Tag gelöschte Nachrichten	20

Durchschnittliche Nachrichtengröße (KB)	200

Tabelle 6. WorxWeb-Profil – mittlere Arbeitslast

Zahl gestarteter Web-Apps	10
Zahl manuell geöffneter Webseiten	10
Durchschnittliche Zahl der Anforderungs-/Antwortpaare pro Web-App	100
Durchschnittliche Anforderungsgröße (Byte)	300
Durchschnittliche Antwortgröße (Byte)	1000

Konfiguration und Parameter

Die folgenden Konfigurationen wurden für die Skalierbarkeitstests verwendet:

- NetScaler Gateway und virtuelle Lastausgleichsserver koexistierten auf demselben NetScaler Gateway-Gerät.
- In NetScaler Gateway wurde für SSL-Transaktionen ein 2048-Bit-Schlüssel verwendet.

Ausgangskriterien

Anmelderaten bilden die Grundlage dieser Analyse. Sie liefern die Richtlinien für die Infrastrukturkomponenten und deren Konfiguration. Die Anmelderaten umfassen eine Fehlerspanne auf der Basis folgender Kriterien:

- Ungültige Antworten
  - Antworten mit dem Statuscode 401/404 anstatt 200 gelten als ungültig.
- Anforderungstimeouts
  - Eine Antwort muss innerhalb von 120 Sekunden erfolgen.
- Verbindungsfehler
  - Eine Verbindung wird zurückgesetzt.
  - Es kommt zu einem abrupten Verbindungsabbruch.

Die Anmelderate ist akzeptabel, wenn die Gesamtfehlerrrate unter einem Prozent der insgesamt von einem bestimmten Gerät gesendeten Anforderungen liegt. Die Fehlerrate umfasst Fehler, die die einzelnen Arbeitslastvorgänge betreffen, und solche, die die physische Leistung der Infrastrukturkomponente betreffen, z. B. Aufbrauchen von CPU oder Speicher.

Angaben zu Software und Hardware

Die folgende Tabelle enthält die XenMobile-Infrastruktursoftware, die bei den Tests verwendet wurde.

Tabelle 7. XenMobile-Infrastrukturkomponenten

Komponente	Version
NetScaler Gateway	10.5.55.8.nc
XenMobile	10.0.0.62300
Externe Datenbank	MS SQL Server 2008 R2 (128 GB RAM, 300 GB Speicherplatz, 24 virtuelle CPUs)

Die Skalierbarkeitstests wurden auf einer XenServer-Plattform durchgeführt (siehe folgende Tabelle).

Tabelle 8. XenServer-Hardware

Anbieter	GenuineIntel
Model	Intel Xeon CPU — E5645 @ 2,40 GHz (CPUs = 24)

Dies umfasst Kerndienste der Infrastruktur (z. B. Active Directory, Windows Domain Name Service, Zertifizierungsstelle, Microsoft Exchange usw.) sowie die XenMobile-Komponenten (virtuelles XenMobile-Gerät und virtuelles NetScaler Gateway-VPX-Gerät, sofern verwendet).

Weitere Produktinformationen und Antworten auf technische Fragen zu diesem Artikel oder den angeführten Produkten finden Sie auf Citrix.com. Die aktuelle Produktdokumentation finden Sie in der Dokumentation zu XenMobile. Alternativ wenden Sie sich an Ihren lokalen Citrix-Mitarbeiter.

Info über XenMobile Cloud

Aug 12, 2016

XenMobile Cloud ist ein Produktservice, der eine XenMobile Enterprise Mobility Management-Umgebung zur Verwaltung von Apps und Geräten sowie Benutzer und Benutzergruppen bietet. Bei XenMobile Cloud übernimmt die Cloud Operations-Gruppe von Citrix die Konfiguration und Pflege der Infrastruktur am Standort. So können Sie sich vollständig auf die Benutzererfahrung und die Verwaltung von Geräten, Richtlinien und Apps konzentrieren. Bei XenMobile Cloud werden Erwerb und Verwaltung von Lizenzen zudem durch ein Abonnement ersetzt.

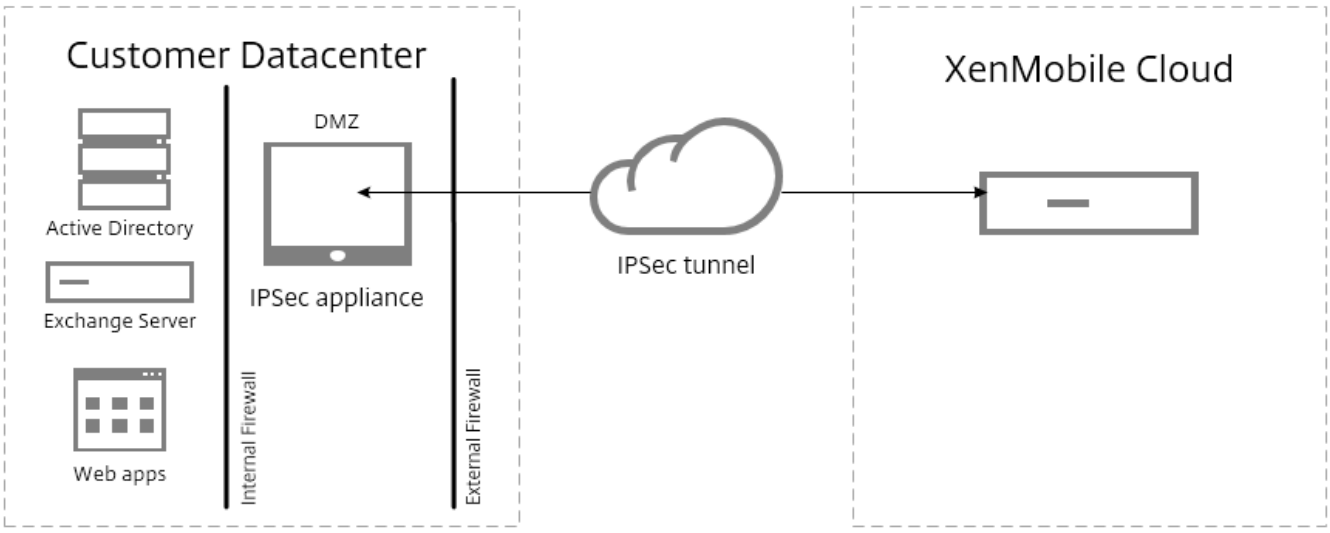
Cloud Operations-Administratoren kümmern sich um die Pflege und Konfiguration der Netzwerkkonnektivität und um die Integration von Citrix Produkten wie NetScaler, XenApp, XenDesktop, StoreFront und ShareFile. Die Cloud-Umgebung wird in weltweit verteilten Amazon-Datencentern gehostet, wodurch eine hohe Leistung, schnelle Reaktionszeiten und Support gewährleistet werden.

Für erste Schritte mit XenMobile Cloud besuchen Sie https://www.citrix.com/products/xenmobile/tech-info/cloud.html.

Hinweis

- Der Remote Support-Client ist in XenMobile Cloud-Versionen 10.x für Windows CE- und Samsung Android-Geräte nicht verfügbar.
- Die serverseitigen Komponenten von XenMobile Cloud sind nicht FIPS 140-2-konform.
- Citrix unterstützt keine Syslog-Integration in XenMobile Cloud mit einem lokalen Syslog-Server. Sie können die Protokolle von der Supportseite in der XenMobile-Konsole herunterladen. Klicken Sie zum Abrufen der Systemprotokolle auf "Download All". Weitere Informationen finden Sie unter Anzeigen und Analysieren von Protokolldateien in XenMobile.

Die grundlegende Architektur von XenMobile Cloud wird in der folgenden Abbildung dargestellt: Detaillierte Architekturdiagramme finden Sie im Abschnitt "Reference Architecture for On-Premises Deployments" in der XenMobile-Bereitstellungsdokumentation.



Sie können die XenMobile Cloud-Architektur in die vorhandene Infrastruktur integrieren, indem Sie Citrix CloudBridge installieren und bereitstellen oder ein vorhandenes IPsec-Gateway in Ihrem Datencenter verwenden.

Diese Architektur ermöglicht außerdem die Nutzung von NetScaler in der Cloud unter Steuerung durch die Cloud Operations-Gruppe oder in Ihrem Datencenter. Bei Verwendung im Datencenter bietet NetScaler eine zentrale Verwaltungsstelle zur Steuerung des Zugriffs und zum Beschränken von Aktionen in Sitzungen auf der Basis von Benutzeridentität und dem Endpunktgerät. Eine solche Bereitstellung bietet mehr Anwendungssicherheit und Datenschutz und eine bessere Compliance-Verwaltung.

Zum Herunterladen und Installieren von Citrix CloudBridge besuchen Sie https://www.citrix.com/downloads/cloudbridge.html.

Rollen in XenMobile Cloud

In XenMobile Cloud wird die gleiche rollenbasierte Zugriffssteuerung (RBAC) verwendet wie in lokalen XenMobile-Bereitstellungen. Der einzige Unterschied besteht darin, dass sich bei XenMobile Cloud die Citrix Cloud Operations-Gruppe um alle Rollen kümmert, einschließlich des Provisionings, die mit der Infrastruktur zu tun haben.

Die folgende Abbildung zeigt die RBAC-Konsole von XenMobile Cloud.

In XenMobile sind vier Standardbenutzerrollen für die logische Trennung des Zugriffs auf Systemfunktionen implementiert: Die Standardrollen sind folgende:

- **Administrator**: besitzt Vollzugriff auf das System.
- **Support**: besitzt Zugriff auf den Remotesupport.
- **Benutzer**: für Benutzer zur Registrierung von Geräten und für den Zugriff auf das Selbsthilfeportal.
- **Provisioning**: für Administratoren zur Bereitstellung aller Windows Mobile-/CE-Geräte als eine Gruppe mit dem Device Provisioning-Tool. Um diese Rolle kümmert sich die Cloud Operations-Gruppe.

Sie können die Standardrollen auch als Vorlagen verwenden, die Sie zum Erstellen von Benutzerrollen mit Berechtigungen für den Zugriff auf bestimmte (über die durch diese Standardrollen definierten Funktionen hinausgehende) Systemfunktionen verwenden.

Sie können Rollen lokalen Benutzern (auf Benutzerebene) oder Active Directory-Gruppen (alle Benutzer in der Gruppe haben dieselben Berechtigungen) zuweisen. 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

Folgende Rollen stehen Ihnen zur Zuweisung zur Verfügung. Um alle nicht in dieser Liste aufgeführten Rollen kümmert sich die Citrix Cloud Operations-Gruppe.

Hauptabschnitt	Abschnitt	Seite	Seite sichtbar für
Dashboard	ALL	ALL	IT-Verwaltung
Verwaltung	Geräte	ALL	IT-Verwaltung
Verwaltung	Registrierung	ALL	IT-Verwaltung
Konfigurieren	Geräterichtlinien	ALL	IT-Verwaltung
Konfigurieren	Apps	ALL	IT-Verwaltung
Konfigurieren	Aktionen	ALL	IT-Verwaltung
Konfigurieren	Bereitstellungsgruppen	ALL	IT-Verwaltung
Konfigurieren	Einstellungen	Zertifikate	Cloudadministrator und IT-Verwaltung
Konfigurieren	Einstellungen	Benachrichtigungsvorlagen	IT-Verwaltung
Konfigurieren	Einstellungen	Rollenbasierte Zugriffssteuerung	Cloudadministrator und IT-Verwaltung
Konfigurieren	Einstellungen	Registrierung	IT-Verwaltung
Konfigurieren	Einstellungen	Lokale Benutzer und Gruppen	Cloudadministrator und

			IT-Verwaltung
Konfigurieren	Einstellungen	Releasemanagement	Cloudadministrator und IT-Verwaltung
Konfigurieren	Einstellungen	Workflows	IT-Verwaltung
Konfigurieren	Einstellungen	Anmeldeinformationsanbieter	IT-Verwaltung
Konfigurieren	Einstellungen	PKI-Entitäten	IT-Verwaltung
Konfigurieren	Einstellungen	Clienteigenschaften	IT-Verwaltung
Konfigurieren	Einstellungen	NetScaler Gateway	Nur Cloudadministrator ODER IT-Verwaltung
Konfigurieren	Einstellungen	SMS-Gateway des Netzbetreibers	IT-Verwaltung
Konfigurieren	Einstellungen	Benachrichtigungsserver	Cloudadministrator und IT-Verwaltung
Konfigurieren	Einstellungen	ActiveSync Gateway	IT-Verwaltung
Konfigurieren	Einstellungen	iOS VPP	IT-Verwaltung
Support	Protokollvorgänge	Protokolleinstellungen	Cloudadministrator, IT-Verwaltung und technischer Support
Konfigurieren	Einstellungen	Servereigenschaften	Cloudadministrator, IT-Verwaltung und technischer Support
Konfigurieren	Einstellungen	Google Play-Anmeldeinformationen	IT-Verwaltung
Konfigurieren	Einstellungen	LDAP	IT-Verwaltung
Konfigurieren	Einstellungen	Netzwerkzugriffssteuerung (NAC)	IT-Verwaltung
Support	Support Bundle	Create Support Bundles	Cloudadministrator und technischer Support

Konfigurieren	Einstellungen	Registrierungsprogramm für iOS-Geräte	IT-Verwaltung
Konfigurieren	Einstellungen	Mobilfunkanbieter	IT-Verwaltung
Konfigurieren	Einstellungen	Samsung KNOX	IT-Verwaltung
Konfigurieren	Einstellungen	XenApp/ XenDesktop	IT-Verwaltung
Konfigurieren	Einstellungen	ShareFile	IT-Verwaltung
Support	Erweitert	Clusterinformationen	Cloudadministrator und technischer Support
Support	Erweitert	Garbage Collection	Cloudadministrator und technischer Support
Support	Erweitert	Java-Speichereigenschaften	Cloudadministrator und technischer Support
Support	Erweitert	Macros	IT-Verwaltung
FTU Wizard	Erstmalige Konfiguration	NetScaler Gateway	Nur Cloudadministrator ODER IT-Verwaltung
Konfigurieren	Einstellungen	Worx Home-Support	IT-Verwaltung
Konfigurieren	Einstellungen	Worx Store Branding	IT-Verwaltung
Support	Diagnose	NetScaler Gateway-Konnektivitätsprüfung	Cloudadministrator, IT-Verwaltung und technischer Support
Support	Diagnose	XenMobile-Konnektivitätsprüfung	Cloudadministrator, IT-Verwaltung und technischer Support
Support	Protokollvorgänge	Protokolle	Cloudadministrator, IT-Verwaltung und technischer Support

Support	Erweitert	Konfigurieren von PKI	Cloudadministrator und IT-Verwaltung
Support	Tools	Hilfsprogramm für APNs-Signierung	Kunde und technischer Support
Support	Tools	Citrix Insight Services	Cloudadministrator, IT-Verwaltung und technischer Support
FTU Wizard	Erstmalige Konfiguration	SSL-Zertifikat	Cloudadministrator und IT-Verwaltung
FTU Wizard	Erstmalige Konfiguration	Konfigurieren von LDAP	IT-Verwaltung
FTU Wizard	Erstmalige Konfiguration	Benachrichtigungsserver	Cloudadministrator und IT-Verwaltung
FTU Wizard	Erstmalige Konfiguration	Zusammenfassung	Cloudadministrator und IT-Verwaltung
Support	Verknüpfungen	Citrix Knowledge Center	Cloudadministrator, IT-Verwaltung und technischer Support
Support	Tools	NetScaler Connector-Status für Gerät	IT-Verwaltung
Support	Protokollvorgänge	Protokolleinstellungen->Protokollgröße	Cloudadministrator und technischer Support

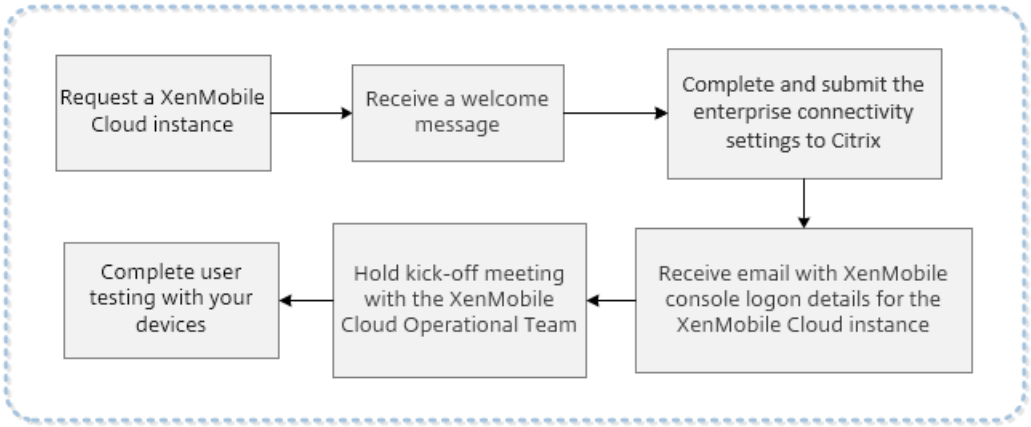
Schrittweise Anweisungen zum Anpassen von Rollen finden Sie unter Konfigurieren von Rollen mit RBAC.

Zum Anfordern eines Neustarts der Serverknoten wenden Sie sich an den technischen Support unter https://www.citrix.com/contact/technical-support.html.

XenMobile Cloud – Voraussetzungen und Verwaltung

May 05, 2016

Die Schritte des Onboarding-Prozesses von Ihrer Anforderung einer XenMobile Cloud-Instanz bis zu den Verwendungstests mit Geräten in Ihrem Unternehmen werden in der folgenden Abbildung dargestellt. Wenn Sie XenMobile Cloud bewerten oder erwerben, leistet das für den Betrieb von XenMobile Cloud verantwortliche Team Hilfe, um sicherzustellen, dass die grundlegenden XenMobile Cloud-Dienste ausgeführt werden und richtig konfiguriert sind.



Citrix hostet die XenMobile Cloud-Lösung und stellt sie bereit. Für die Verbindung zwischen der XenMobile Cloud-Infrastruktur und den Diensten in Ihrem Unternehmen gibt es jedoch einige Anforderungen in Bezug auf Kommunikation und Ports (z. B. Active Directory). Bereiten Sie Ihre XenMobile Cloud-Bereitstellung anhand der nachfolgenden Abschnitte vor.

IPSec-Tunnelgateways für XenMobile Cloud

Sie können unter Verwendung eines XenMobile Enterprise-Connectors eine Verbindung zwischen XenMobile Cloud und Infrastrukturdiensten des Unternehmens wie Active Directory über einen IPsec-Tunnel herstellen.

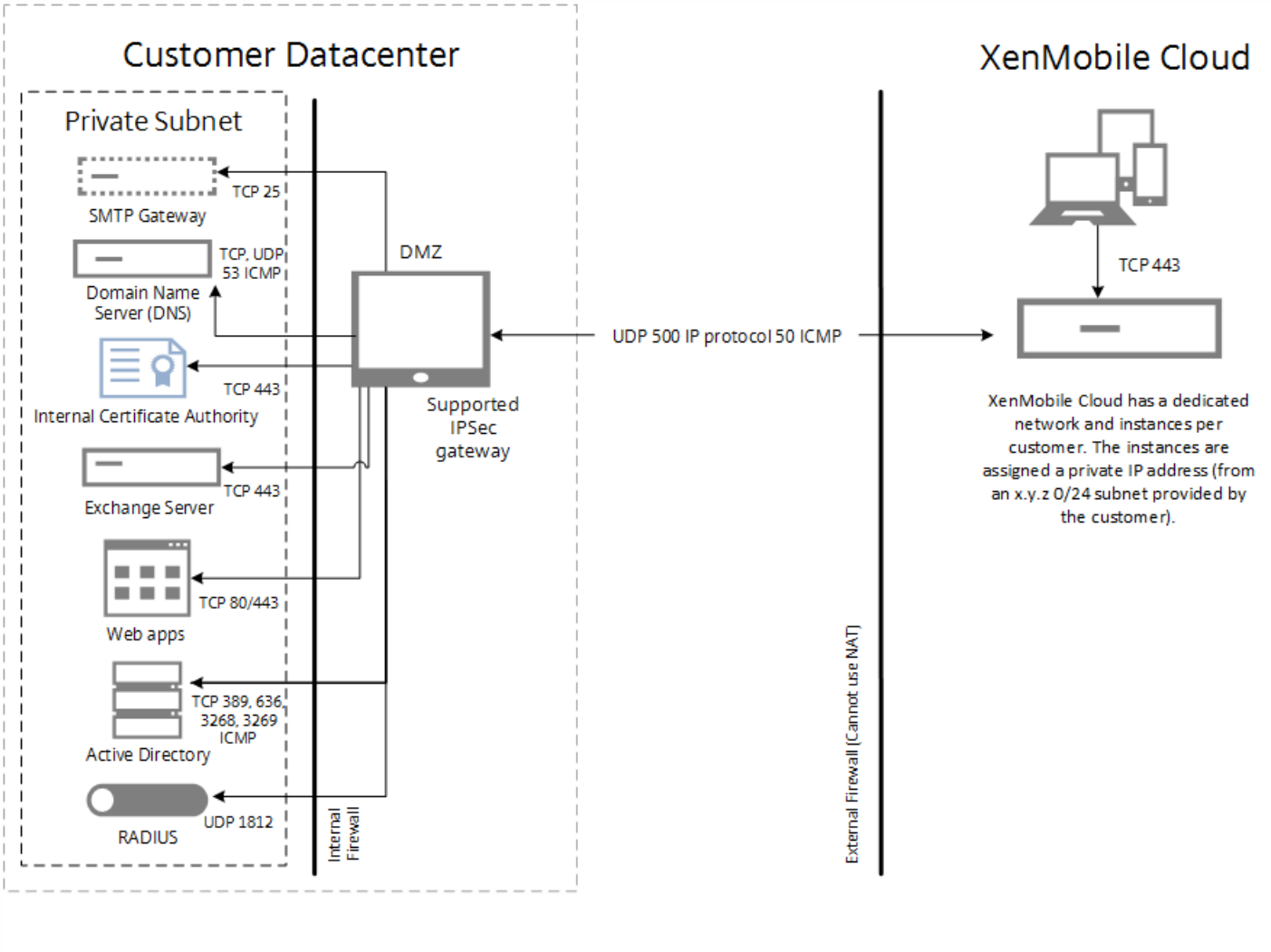
Die auf der folgenden Amazon Web Services-Website aufgeführten IPsec-Gateways sind offiziell getestet und werden für XenMobile Cloud unterstützt: http://aws.amazon.com/vpc/faqs/. Führen Sie einen Bildlauf zum Abschnitt "F: Welche Kunden-Gateway-Geräte kann ich für die Verbindung mit Amazon VPC verwenden?", um die Liste der unterstützten Gateways einzublenden.

> ## Hinweis
>
> Wenn Ihr IPsec-Gateway nicht in der Liste der genehmigten IPsec-Gateways aufgeführt ist, funktioniert es möglicherweise dennoch mit XenMobile Cloud, die Einrichtung kann jedoch länger dauern und es ist eventuell die Verwendung eines der offiziell unterstützten IPSec-Gateways als Ausweichmöglichkeit erforderlich.

Ihr IPsec-Gateway benötigt eine direkt zugewiesene öffentliche IP-Adresse, für die keine Netzwerkadressübersetzung

(NAT) verwendet werden darf.

Die folgende Abbildung zeigt die Konfiguration des IPsec-Tunnels in XenMobile Cloud für die Verbindung mit Unternehmensdiensten über verschiedene Ports.



Die folgende Tabelle enthält die Anforderungen im Hinblick auf Kommunikation und Ports für eine XenMobile Cloud-Bereitstellung einschließlich derer für den IPSec-Tunnel.

Quelle	Ziel	Protokolle	Port	Beschreibung
Externe (Rand-) Firewall – eingehende Regeln				
Öffentliche IP-Adressen von XenMobile Cloud (AWS) IPSec-VPN [1]	IPSec-Gerät des Kunden	UPD	500	IPSec-IKE-Konfiguration
Öffentliche IP-Adressen von	IPSec-Gerät des Kunden	IP-Protokoll-ID	50	IPSec-ESP-Protokoll

XenMobile Cloud (AWS) IPSec-VPN [1]				
Öffentliche IP-Adressen von XenMobile Cloud (AWS) IPSec-VPN [1]	IPSec-Gerät des Kunden	ICMP		Zur Problembehandlung (kann nach Einrichtung entfernt werden)
Externe (Rand-) Firewall – ausgehende Regeln				
Kunden-DMZ-Subnetz	Öffentliche IP-Adressen von XenMobile Cloud (AWS) IPSec-VPN [1]	UDP	500	IPSec-IKE-Konfiguration
Kunden-DMZ-Subnetz	Öffentliche IP-Adressen von XenMobile Cloud (AWS) IPSec-VPN [1]	IP-Protokoll-ID	50, 51	IPSec-ESP-Protokoll
Kunden-DMZ-Subnetz	Öffentliche IP-Adressen von XenMobile Cloud (AWS) IPSec-VPN [1]	ICMP		Zur Problembehandlung (kann nach Einrichtung entfernt werden)
Interne Firewall – eingehende Regeln				
Nicht genutztes und routbares /24-Kundensubnetz [2]	Interne DNS-Server im Datencenter des Kunden	TCP, UPP, ICMP	53	DNS-Auflösung
Nicht genutztes und routbares /24-Kundensubnetz [2]	Active Directory-Domänencontroller im Datencenter des Kunden	LDAP (TCP)	389, 636 3268, 3269	Für Active Directory-Authentifizierung der Benutzer und Verzeichnisanfragen an Domänencontroller
Nicht genutztes und routbares /24-Kundensubnetz [2]	Active Directory-Domänencontroller im Datencenter des Kunden	ICMP		Zur Problembehandlung (kann nach Abschluss der gesamten Einrichtung entfernt werden)
Nicht genutztes und routbares /24-Kundensubnetz [2]	Exchange-Server im Datencenter des Kunden	SMTP (TCP)	25	Optional für die XenMobile-E-Mail-Benachrichtigung

Nicht genutztes und routbares /24-Kundensubnetz [2]	Exchange-Server im Datencenter des Kunden	HTTP, HTTPS (TCP)	80, 443	Exchange ActiveSync – wird benötigt, wenn ActiveSync-Daten vom Gerät über den IPSec-Tunnel in die XenMobile Cloud-Infrastruktur an Exchange-Server gesendet werden. NICHT erforderlich, wenn Benutzergeräte mit einem öffentlichen ActiveSync-FQDN über das Internet kommunizieren, ohne dass eine Verbindung über den XenMobile-IPSec-Tunnel mit dem Exchange-Server erforderlich ist.
Nicht genutztes und routbares /24-Kundensubnetz [2]	Anwendungsserver, z. B. Intranet-/Webserver, SharePoint-Server usw.	HTTP, HTTPS (TCP)	80, 443	Zugriff auf Intranet- und/oder Anwendungsserver von Mobilgeräten über den XenMobile-IPSec-Tunnel. Jeder Anwendungsserver den Firewallregeln mit der für den Zugriff auf die Anwendung erforderlichen Portnummer (üblicherweise Port 80 und/oder 443) hinzugefügt werden.
Nicht genutztes und routbares /24-Kundensubnetz [2]	PKI-Server (falls eine lokale PKI verwendet wird)	HTTPS (TCP)	443	Optional (nicht in XenMobile-POCs verwendet): Hiermit kann eine Integration zwischen der XenMobile Cloud-Infrastruktur und einer lokalen PKI (z. B. Microsoft ZS) für die zertifikatbasierte Authentifizierung innerhalb von XenMobile hergestellt werden.
Nicht genutztes und routbares /24-Kundensubnetz [2]	RADIUS-Server	UDP	1812	Optional (nicht in XenMobile-POCs verwendet): Hiermit kann die Zweifaktorauthentifizierung innerhalb von XenMobile ermöglicht werden.
Interne Firewall – ausgehende Regeln				

Interne Subnetze des Kunden, von wo aus die XenMobile-Konsole verfügbar sein muss	Nicht genutztes und routbares /24-Kundensubnetz [2]	TCP	4443	XenMobile App Controller-Konsole (MAM) in der XenMobile Cloud-Infrastruktur

[1] Wird vom XenMobile Cloud-Team bei der Bereitstellung der XenMobile Cloud-Instanz und der IPSec-Komponenten in der XenMobile Cloud-Infrastruktur bekannt gegeben.

[2] Nicht genutztes, routbares /24-Subnetz, das der Kunde während des Bereitstellungsprozesses zur Verfügung stellt und das keine Konflikte mit internen Subnetzen im Datencenter des Kunden verursacht.

Wenn Sie XenMobile Mail Manager oder XenMobile NetScaler Connector für die native E-Mail-Filterung bereitstellen möchten, z. B. zum Blockieren oder Zulassen von Verbindungen von nativen E-Mail-Clients auf Mobilgeräten, gelten die nachfolgenden zusätzlichen Anforderungen.

APNs-Zertifikat von Apple für XenMobile

Wenn Sie iOS-Geräte in Ihrer XenMobile Cloud verwalten möchten, benötigen Sie ein APNs-Zertifikat von Apple. Besorgen Sie das Zertifikat vor dem Bereitstellen der XenMobile Cloud-Lösung. Schrittweise Anleitungen finden Sie unter Anfordern eines APNs-Zertifikats.

iOS-Pushbenachrichtigungszertifikat für WorxMail

Wenn Sie das Pushbenachrichtigungsfeature in Ihrer WorxMail-Bereitstellung nutzen möchten, beschaffen Sie ein APNS-Zertifikat von Apple für die iOS-Pushbenachrichtigung in WorxMail. Weitere Informationen finden Sie unter Pushbenachrichtigungen für WorxMail für iOS.

XenMobile MDX Toolkit

Das MDX Toolkit ist eine Technologie zum Umschließen von Apps, mit der diese für die sichere Bereitstellung mit XenMobile vorbereitet werden. Wenn Sie Apps wie Citrix WorxMail, WorxNotes, QuickEdit usw. umschließen möchten, müssen Sie das MDX Toolkit installieren. Weitere Informationen finden Sie unter Informationen zum MDX Toolkit.

Wenn Sie iOS-Apps umschließen möchten, brauchen Sie ein Apple Developer-Konto zur Erstellung der erforderlichen Apple-Verteilungsprofile. Weitere Informationen finden Sie im Abschnitt zu den Systemanforderungen für das MDX Toolkit und auf der Website für Apple Developer-Konten.

Wenn Sie Apps für Windows Phone 8.1-Geräte umschließen möchten, lesen Sie die Informationen unter Systemanforderungen.

XenMobile-Autodiscovery für die Windows Phone-

Registrierung

Wenn XenMobile-Autodiscovery für die Registrierung von Windows Phone 8.1-Geräten verwenden möchten, stellen Sie sicher, dass Sie ein öffentliches SSL-Zertifikat zur Verfügung haben. Weitere Informationen finden Sie unter Aktivieren von Autodiscovery für die Benutzerregistrierung in XenMobile.

Die XenMobile-Konsole

Für XenMobile Cloud wird die gleiche Webkonsole wie für eine lokale XenMobile-Bereitstellung verwendet. Daher werden alltägliche Verwaltungsaufgaben in XenMobile Cloud, z. B. Richtlinienverwaltung, App-Verwaltung, Geräteverwaltung usw., auf ähnliche Weise erledigt wie bei einer lokalen XenMobile-Bereitstellung. Informationen zur Verwaltung von Apps und Geräten in der XenMobile-Konsole finden Sie unter Erste Schritte mit der XenMobile-Konsole.

Geräteregistrierung bei XenMobile

Informationen zur Registrierung von Geräten der verschiedenen Plattformtypen bei XenMobile finden Sie unter Registrieren von Benutzern und Geräten.

XenMobile-Support

Informationen zum Zugriff auf entsprechende Informationen und Tools in der XenMobile-Konsole finden Sie unter Support und Wartung von XenMobile.

Unterstützen mobiler Plattformen in XenMobile Cloud

May 05, 2016

Nachdem Sie eine XenMobile Cloud-Instanz angefordert haben, können Sie, falls gewünscht, mit den Vorbereitungen für die Unterstützung von Android-, iOS- und Windows-Plattformen beginnen. Notieren Sie beim Ausführen der für Ihre Umgebung erforderlichen Schritte alle benötigten Informationen, damit sie Sie bei der Einrichtung der Einstellungen in der XenMobile-Konsole zur Verfügung haben.

Diese Anforderungen sind ein Teilsatz der Anforderungen an Verbindungen und Ports für das XenMobile Cloud-Onboarding. Weitere Informationen finden Sie unter XenMobile Cloud – Voraussetzungen und Verwaltung.

Android

- Erstellen Sie Google Play-Anmeldeinformationen. Informationen finden Sie unter Get Started with Publishing.
- Erstellen Sie ein Android for Work-Konto. Informationen finden Sie unter Verwalten von Geräten mit Android for Work in XenMobile.
- Lassen Sie Ihre Domäne von Google überprüfen. Informationen finden Sie unter Verify your domain for Google Apps.
- Aktivieren Sie APIs und erstellen Sie ein Dienstkonto für Android for Work. Informationen finden Sie unter Google for Work/Android.

iOS

- Erstellen Sie eine Apple-ID und ein Developer-Konto. Informationen finden Sie unter Apple Developer Program.
- Erstellen Sie ein APNs-Zertifikat. Informationen finden Sie unter Apple Push Certificates Portal.
- Erstellen Sie ein Unternehmenstoken für das Programm für Volumenlizenzen. Informationen finden Sie unter Apple Volume Purchasing Program.

Windows

- Erstellen Sie ein Entwicklerkonto für den Microsoft Windows-Store. Informationen finden Sie im Microsoft Dev Center.
- Beschaffen Sie eine Herausgeber-ID für den Microsoft Windows-Store. Informationen finden Sie im Microsoft Dev Center.
- Beschaffen Sie ein Unternehmenszertifikat von Symantec. Informationen finden Sie im Microsoft Dev Center.
- Erstellen Sie ein Anwendungsregistrierungstoken (AET). Informationen finden Sie im Microsoft Dev Center.

Systemanforderungen

Oct 13, 2016

Für die Ausführung von XenMobile 10 gelten die folgenden Mindestanforderungen:

- Eines der Folgenden:
  - XenServer (unterstützte Versionen: 6.2.x, 6.1.x und 6.0.x); weitere Details finden Sie unter XenServer
  - VMware (unterstützte Versionen: ESXi 5.5, ESXi 5.1 und ESXi 4.1); weitere Informationen finden Sie unter VMware.
  - Hyper-V (unterstützte Versionen: Windows Server 2008 R2, Windows Server 2012 und Windows Server 2012 R2); weitere Informationen finden Sie unter Hyper-V.
- Dual-Core-Prozessor
- 2 virtuelle CPUs
- 8 GB RAM
- 50 GB Speicherplatz auf der Festplatte

Empfohlene Konfiguration für 10.000 Geräte:

- Quad Core-Prozessor
- 8 GB RAM

Systemanforderungen für NetScaler Gateway

Für die Ausführung von NetScaler Gateway mit XenMobile 10 gelten die folgenden Mindestanforderungen:

- XenServer, VMWare oder Hyper-V
- 2 virtuelle CPUs
- 2 GB RAM
- 20 GB Speicherplatz auf der Festplatte

Außerdem ist die Kommunikation mit Active Directory und somit ein Dienstkonto erforderlich. Sie benötigen nur Abfrage- und Lesezugriff.

XenMobile 10-Datenbankanforderungen

Das XenMobile-Repository erfordert eine Microsoft SQL Server-Datenbank in einer der folgenden unterstützten Versionen:

- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008

Citrix XenMobile unterstützt die SQL-Verfügbarkeitsgruppe "Always on" und SQL-Clustering für hohe Datenbankverfügbarkeit. Citrix unterstützt nicht die Datenbankspiegelung für die hohe Verfügbarkeit der XenMobile-Datenbank. Hohe Datenbankverfügbarkeit wird im Aktiv/Aktiv- oder Aktiv/Passiv-Modus bei einer MS SQL-Clusterbereitstellung unterstützt.

Hinweis: Wenn die Datenbank offline ist, bedient der XenMobile-Server keine Verbindungen von Geräten, weil der XenMobile-Server in dem Fall auch offline ist.

Citrix empfiehlt die Remote-Verwendung von Microsoft SQL. PostgreSQL ist Teil von XenMobile und sollte lokal oder remote nur in Testumgebungen verwendet werden.

Hinweis: Das in XenMobile verwendete SQL Server-Dienstkonto muss die Rollenberechtigung "DBcreator" haben. Weitere Informationen über SQL Server-Dienstkonten finden Sie in den folgenden Seiten der Microsoft Developer Network-Site (diese Links verweisen auf Informationen für SQL Server 2014. Wenn Sie eine andere Version verwenden, wählen Sie sie in der Versionsliste aus):

- Serverkonfiguration – Dienstkonten
- Konfigurieren von Windows-Dienstkonten und -Berechtigungen
- Rollen auf Serverebene

XenMobile-Kompatibilität

Oct 13, 2016

> **Important**
>
> Ab Version 10.4 werden die mobilen Worx-Apps in XenMobile-Apps umbenannt. Die meisten XenMobile-Apps werden ebenfalls umbenannt. Weitere Informationen finden Sie unter Info über XenMobile-Apps.

In diesem Artikel werden die Versionen der unterstützten XenMobile-Komponenten zusammengefasst, die integriert werden können, einschließlich NetScaler Gateway und MDX Toolkit-Version (das Toolkit ist zum Umschließen, Konfigurieren und Verteilen mobiler Worx-Apps bzw. XenMobile-Apps erforderlich).

XenMobile 10.x

Unterstützte Versionen von NetScaler Gateway:

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

Citrix unterstützt die aktuelle Version und die zwei Vorversionen von XenMobile. Wenn die aktuelle Version beispielsweise XenMobile 10.4 ist, unterstützt Citrix ebenfalls XenMobile 10.3.6 (ein Service Pack und kein vollständiges Release) und XenMobile 10.3.5.

XenMobile-Clientkomponenten folgen diesen Kompatibilitätanforderungen:

- Die aktuellen Versionen von Secure Hub und dem MDX Toolkit sind mit der aktuellen Version und den letzten zwei Versionen von XenMobile-Server kompatibel.
- Die aktuelle Version von Secure Hub und die Version davor sind mit den aktuellen Versionen von MDX Toolkit und XenMobile-Apps kompatibel.
- Die aktuelle Version der XenMobile-Apps wurde mit der aktuellen Version von MDX Toolkit getestet.

Installieren Sie die neuesten Versionen des MDX Toolkits, von Secure Hub und den XenMobile-Apps, um die Vorteile der neuen Features, Problembehebungen und Richtlinienaktualisierungen zu nutzen.

Installieren Sie die neuesten Versionen des MDX Toolkits, von Worx Home und den mobilen Worx-Apps, um die Vorteile der neuen Features, Problembehebungen und Richtlinienaktualisierungen zu nut

MDX Toolkit-Versionen für iOS und Android	**Versionen von Worx Home/Secure Hub**	
	Android	**iOS**
10.4	10.4	10.4
10.3.10	10.3.10	10.3.10
10.3.9	10.3.9	10.3.9
10.3.6	10.3.8	10.3.8
10.3.5	10.3.6	10.3.6
10.3.1	10.3.5	10.3.5
10.2.1	10.3.1	10.3.1
10.0.7	10.3	
10.0.5	10.2.1	10.2.1
10.0.3	10.0.8	10.0.8
	10.0.3	10.0.3

MDX Toolkit für Windows Phone	**Kompatible Worx Home-Versionen***
10.0.7	10.0.3
10.0.5 - 10.0.3	10.0.3
10.0.0	10.0.0

*Worx Home-Versionen vor 10.0.3 sind kompatibel, aber sie werden nicht unterstützt.

> **Hinweis**
>
> Windows Phone 10 wird zurzeit nur von XenMobile 10 und 10.3.x unterstützt. Es wird nicht von XenMobile 10.1 unterstützt. Bei XenMobile 9 müssen Sie ein Patch installieren, damit die Apps richtig funktionieren. Weitere Informationen finden Sie unter CTX215497.

XenMobile 10.x unterstützt die in der folgenden Tabelle aufgeführten Versionen der mobilen Worx-Apps bzw. XenMobile-Apps.

App	Android	iOS	Windows Phone 8.1/10[1]
Secure Hub	10.4	10.4	
Worx Home	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3.1 10.2.1 10.0.8 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2.1 10.0.8 10.0.3 10.0.0	10.0.3 10.0.0
Secure Forms		10.4 10.3.10 10.3.9 10.3.8 10.3.6	
Secure Mail	10.4	10.4	
WorxMail	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.7
Secure Notes	10.4	10.4	
Worx Notes	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.0	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.0	
Secure Tasks	10.4	10.4	
WorxTasks	10.3.10	10.3.10	

	10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7	10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7	
Secure Web	10.4	10.4	
WorxWeb	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.3
QuickEdit[2]	6.3.1	6.4	
ShareConnect	3.6	3.7	
ShareFile	4.9	4.7	

1 Windows Phone 10 wird unter XenMobile 10.1 nicht unterstützt.

2 Nur die aktuellen Versionen von QuickEdit, ShareConnect und ShareFile werden unterstützt.

Browserunterstützung

XenMobile 10.x unterstützt die folgenden Browser:

- Internet Explorer, jedoch nicht Version 9 oder ältere Versionen
- Chrome
- Firefox
- Safari auf Mobilgeräten zur Verwendung mit dem Selbsthilfeportal.

XenMobile 10.x ist kompatibel mit der aktuellen Version des Browsers und der Version vor der aktuellen Version.

XenMobile 9

XenMobile 9 umfasst Device Manager 9.0 und App Controller 9.0.

Unterstützte Versionen von NetScaler Gateway:

- 11.0.64
- 10.5.x.e
- 10.5.x MR
- 10.1.x.e
- 10.1.x MR

XenMobile-Clientkomponenten folgen in der Regel diesen Kompatibilitätanforderungen:

- Die aktuelle Version vom Secure Hub und das MDX Toolkit sind mit den letzten zwei Versionen von XenMobile-Server kompatibel.
- Die aktuelle Version des MDX Toolkits ist mit der aktuellen Version der XenMobile-Apps kompatibel.
- Aktuelle MDX Toolkit-Versionen sind kompatibel mit den folgenden Versionen von Secure Hub:

	Versionen von Worx Home/Secure Hub*

MDX Toolkit-Versionen für iOS und Android	Android	iOS
10.4	10.4	10.4
10.3.6	10.3.6	10.3.6
10.3.5	10.3.5	10.3.5
10.3.1	10.3.1	
10.3	10.3	10.3
10.2.1	10.2.1	10.2.1
10.0.7	10.0.8	10.0.8
10.0.5	10.0.3	10.0.3
10.0.3		

MDX Toolkit für Windows Phone 10[1]	Kompatible Secure Hub Versionen
10.4	10.4
10.3.5	10.3.5
10.3.1	10.3
10.3	10.3
10.2	10.2

[1]In XenMobile 9 erfordert Windows 10 ein Patch, das hier erhältlich ist.

MDX Toolkit für Windows Phone 8.1	Kompatible Secure Hub-Versionen*
10.3.5	10.3.5
10.3.1	10.3
10.3	10.3
10.2.1	10.2.1
10.0.5 - 10.0.3	10.0.3
10.0.0	10.0.0

*Secure Hub-Versionen vor 10.0.3 sind kompatibel, aber sie werden nicht unterstützt.

XenMobile 9 unterstützt die in der folgenden Tabelle aufgeführten Versionen der mobilen Worx-Apps bzw. XenMobile-Apps.

App	Android	iOS	Windows Phone 8.1
Secure Hub	10.4	10.4	

Worx Home	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3.1 10.2.1 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2.1 10.0.8 10.0.3 10.0.0	10.0.3 10.0.0
Secure Mail	10.4	10.4	
WorxMail	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.7
Secure Notes	10.4	10.4	
WorxNotes*	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.0	
Secure Tasks	10.4	10.4	
WorxTasks	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2	

		10.0.7	
Secure Web	10.4	10.4	
WorxWeb	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.3
QuickEdit[1]	6.0.2	6.3.10	
ShareConnect	3.2	3.6	
ShareFile	4.6.5	4.5	

[1]Nur die aktuellen Versionen von QuickEdit, ShareConnect und ShareFile werden unterstützt.

* MDX Toolkit 2.3 und 2.2.1 unterstützen WorxNotes/Secure Notes nicht.

Unterstützte Geräteplattformen

Oct 13, 2016

XenMobile unterstützt folgende Geräteplattformen für Enterprise Mobility Management einschließlich der Verwaltung von Apps und Geräten. Aufgrund von Plattformeinschränkungen und Sicherheitsfeatures werden nicht alle Funktionen auf allen Plattformen unterstützt:

Informationen zur Unterstützung von älteren Betriebssystemversionen für Mobilgeräte, wie Android 4.1 und iOS 7, finden Sie im Artikel CTX204192 im Citrix Support Knowledge Center.

Die Informationen zu den unterstützten Geräteplattformen in diesem Artikel gelten auch für XenMobile Mail Manager und XenMobile NetScaler Connector.

> ## Hinweis
>
> - Citrix unterstützt mindestens die aktuelle Version und die Vorversion jeder gängigen Betriebssystemplattform. Nicht alle Features der neueren XenMobile-Versionen funktionieren auf älteren Plattformen. In diesem Artikel wird detailliert aufgeführt, welche Versionen Citrix zurzeit für die jeweiligen Betriebssysteme unterstützt. Der Artikel enthält auch von Citrix getestete Gerätemodelle. Wenn Sie Probleme mit anderen Gerätemodellen haben, wenden Sie sich an den Support von Citrix.
> - Ab Version 10.4 werden alle mobilen Worx-Apps in XenMobile-Apps umbenannt. Die meisten XenMobile-Apps werden ebenfalls umbenannt. Weitere Informationen finden Sie unter Info über XenMobile-Apps.

Android

XenMobile 10.4 und 10.3.x

Für alle Modi unterstützte Betriebssysteme: Android 4.4.x, 5.x, 6.x, 7

Für den Nur-MDM-Modus unterstützte Betriebssysteme: Android 4.1.x, 4.2.x, 4.3

Worx Home/Secure Hub wird auf x86-basierten Android-Geräten für MDM-Funktionen unterstützt.

Mit MDX umschlossene Worx-Apps/XenMobile-Apps werden auf x64-basierten Android-Geräten unterstützt.

Unter anderem wurden folgende Android-Geräte mit den zuvor aufgeführten Betriebssystemen unter XenMobile 10.3.x und 10.4 getestet:

- Nexus 6, 7, 9, 10
- Samsung Galaxy S4 und Note 3, 4, 5
- Galaxy Tablet P750
- Galaxy Tab-A
- Galaxy Tab 2 - S3, S4, S5
- HTC One
- Samsung Tablet P750
- Samsung S6, S6 Edge und S7
- OnePlus X
- Xiaomi Mi 4

- Huawei Honor 6
- Huawei Ascend Mate 7
- HTC One M9
- Motorola Moto-X
- Sony Experia Z
- Note 2, 3, 4

XenMobile 10 und 10.1

Für alle Modi unterstützte Betriebssysteme: 4.4.x, 5.x, 6.x, 7

Für den Nur-MDM-Modus unterstützte Betriebssysteme: 4.1.x

Android 4.2 und 4.3 werden nicht unterstützt.

Worx Home wird auf x86-basierten Android-Geräten für MDM Funktionen unterstützt. Die App-Verwaltung ist nur bei Android-Geräten mit ARM-basierten Prozessoren möglich. Mit MDX umschlossene Apps werden auf x86-basierten Android-Geräten nicht unterstützt.

Mit MDX umschlossene Worx-Apps werden auf x64-basierten Android-Geräten unterstützt.

Unter anderem wurden folgende Android-Geräte mit den oben genannten Betriebssystemen unter XenMobile 10 und 10.1 getestet:

- Nexus 10, 7, 5, 9
- Galaxy S4 und Note 2, 3
- Galaxy Tablet 2, S3, S4, S5
- Moto X
- HTC One
- HTC Desire, LG
- Samsung Tablet P750

SAFE und KNOX

Auf kompatiblen Samsung-Geräten bietet XenMobile 10.x Unterstützung und Erweiterung von Samsung for Enterprise- (SAFE) und Samsung KNOX-Richtlinien. 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.

Für HTC-spezifische Richtlinien unterstützt XenMobile die HTC API-Version 0.5.0. Für Sony-spezifische Richtlinien unterstützt XenMobile Sony Enterprise SDK 2.0.

iOS

Hinweis: Alle Worx-Apps/XenMobile-Apps sind ab Version 10.3.10 und höher mit iOS 10 kompatibel. Sie müssen das MDX Toolkit 10.3.10 oder höher verwenden, um mobile Apps oder Unternehmensapps zu umschließen, damit die Kompatibilität mit iOS 10 gewährleistet ist. Weitere Informationen finden Sie in diesem Artikel im Support Knowledge Center.

XenMobile 10.3.x und 10.4

- iOS 10

- iOS 9.x
- iOS 8.x (Worx Home/Secure Hub nur in Nur-MDM-Bereitstellungen)

Unter anderem werden folgende iOS-Geräte unter XenMobile 10.3.x und 10.4 unterstützt:

- iPhone 6, 6+, 6S, 6S+, 5s, 5, 5c
- iPad 2, 3
- iPad Air , iPad Air-2, iPad Mini-3, Mini-2
- iPad Pro
- Mac OS X
  - MacBook, Air, Mini, Mini Retina 10.9.5, 10.10, 10.11

XenMobile 10 und 10.1

- iOS 10
- iOS 9.x
- iOS 8.x (Worx Home nur in Nur-MDM-Bereitstellungen)

Unter anderem werden folgende iOS-Geräte unter XenMobile 10 und 10.1 unterstützt:

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

Windows Phone und Tablet

XenMobile 10.3.x und 10.4

- Windows 10 und 8.1 Tablet
  - Windows 10 Tablet wird bei Ausführung von XenMobile im Nur-MAM-Modus nicht unterstützt.
- Windows Tablet Surface Pro 3, Surface 2, RT
- Windows Phone 10, 8.1
  - Sie müssen für Windows Phone 10 einen Patch von der XenMobile-Downloadseite herunterladen.
  - Windows Phone 8.1 und 10 werden bei Ausführung von XenMobile im Nur-MAM-Modus nicht unterstützt.
- Kompatibilität von Windows Phone 8.1 mit Worx Home:
  - Worx Home 10.0, wenn XenMobile im Enterprise-Modus ist
  - Worx Home 9.1.0, wenn XenMobile im Nur-MDM-Modus ist.
- Windows 8.1 Pro und Enterprise Edition (32 Bit und 64 Bit)
- Windows RT 8.1
- Windows Mobile/CE
  - Windows CE wird bei Ausführung von XenMobile im Nur-MAM-Modus nicht unterstützt.

Unter anderem werden folgende Windows-Geräte unter XenMobile 10.3 unterstützt:

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

XenMobile 10 und 10.1

- Windows 10-Tablet
- Windows Phone 8.1 / 10:
  - Windows Phone 8.1 wird bei Ausführung von XenMobile im Nur-MAM-Modus nicht unterstützt.
  - Windows Phone 10 wird unter XenMobile 10.3 und höher unterstützt.
  - Windows Phone 10 wird unter XenMobile 9 unterstützt. Sie müssen jedoch einen Device Manager Rolling Patch installieren, wie in diesem Artikel im Support Knowledge Center erläutert. Beachten Sie zudem den Patch für das Windows 10 Anniversary Update Version 1607 für Windows Phones. Weitere Informationen finden Sie in diesem Artikel im Support Knowledge Center.
- Kompatibilität von Windows Phone 8.1 mit Worx Home:
  - Worx Home 10.0, wenn XenMobile im Enterprise-Modus ist
  - Worx Home 9.0.3, wenn XenMobile im MDM-Modus ist
- Windows 8.1 Pro und Enterprise Edition (32 Bit und 64 Bit)
- Windows RT 8.1
- Windows Mobile: XenMobile 10.1 unterstützt keine Windows Mobile-Geräte. Benutzer mit Geräten mit Windows Mobile oder Windows CE müssen weiterhin XenMobile 9 verwenden.

Unter anderem werden folgende Windows-Geräte unter XenMobile 10 und 10.1 unterstützt:

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

Die Verwaltung von Windows Phone 7-Geräten ist über XenMobile Mail Manager möglich. Weitere Informationen finden Sie unter Installieren von XenMobile Mail Manager.

Symbian

XenMobile 10.3.x und 10.4

XenMobile 10.3.x und 10.4 unterstützen Symbian nicht.

XenMobile 10 und 10.1

Unter anderem werden folgenden Symbian-Geräte unter XenMobile 10.1 und 10 unterstützt. Unter XenMobile 10 werden sie nur für die Geräteverwaltung unterstützt:

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

BlackBerry

Die Verwaltung von BlackBerry-Geräten erfolgt durch XenMobile Mail Manager. Weitere Informationen finden Sie unter Installieren von XenMobile Mail Manager.

Portanforderungen

Oct 13, 2016

Damit Geräte und Apps mit XenMobile kommunizieren können, müssen bestimmte Ports in den Firewalls geöffnet werden. Die folgenden Tabellen enthalten eine Liste der Ports, die geöffnet sein müssen.

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

Zum Ermöglichen von Benutzerverbindungen über Worx Home, Citrix Receiver und das NetScaler Gateway-Plug-In über NetScaler Gateway mit XenMobile, StoreFront, XenDesktop, den XenMobile NetScaler Connector und andere interne Netzwerkressourcen, z. B. Intranet-Websites, müssen Sie die folgenden Ports öffnen. Weitere Informationen über NetScaler Gateway finden Sie unter Configuration Settings for your XenMobile Environment in der Dokumentation für NetScaler Gateway. Weitere Informationen über NetScaler-eigene IP-Adressen, wie die NetScaler-IP-Adresse (NSIP), virtuelle Server-IP-Adresse (VIP) und Subnetz-IP-Adresse (SNIP), finden Sie unter How a NetScaler Communicates with Clients and Servers in der NetScaler-Dokumentation.

TCP-Port	Beschreibung	Quelle	Ziel
21 oder 22	Dient zum Senden von Supportpaketen an einen FTP- oder SCP-Server.	XenMobile	FTP oder SCP-Server
53	Wird für DNS-Verbindungen verwendet.	NetScaler Gateway XenMobile	DNS-Server
80	NetScaler Gateway leitet die VPN-Verbindung mit der internen Netzwerksressource durch die zweite Firewall. Dies passiert in der Regel, wenn Benutzer sich mit dem NetScaler Gateway-Plug-In anmelden.	NetScaler Gateway	Intranet-Websites
80 oder 8080 443	XML- und Secure Ticket Authority-Port (STA) für Enumeration, Ticketing und Authentifizierung. Citrix empfiehlt, Port 443 zu verwenden.	XML-Netzwerkdatenverkehr mit StoreFront und Webinterface NetScaler Gateway-STA	XenDesktop bzw. XenApp
123	Wird für Network Time Protocol-Dienste (NTP) verwendet.	NetScaler Gateway	NTP-Server

389	Wird für unsichere LDAP-Verbindungen verwendet.	NetScaler Gateway XenMobile	LDAP-Authentifizierungsserver oder Microsoft-Active Directory
443	Wird für Verbindungen zwischen StoreFront und Citrix Receiver und zwischen Receiver für Web und XenApp/XenDesktop verwendet.	Internet	NetScaler Gateway
	Wird für Verbindungen mit XenMobile zur Bereitstellung von Web-, Mobil- und SaaS-Apps verwendet.	Internet	NetScaler Gateway
	Wird für die allgemeine Gerätekommunikation mit XenMobile-Server verwendet.	XenMobile	XenMobile
	Wird für Verbindungen von mobilen Geräten zu XenMobile für die Registrierung verwendet.	Internet	XenMobile
	Wird für Verbindungen von XenMobile zum XenMobile NetScaler Connector verwendet.	XenMobile	XenMobile NetScaler Connector
	Wird für Verbindungen von XenMobile NetScaler Connector zu XenMobile verwendet.	XenMobile NetScaler Connector	XenMobile
	Wird für die Rückruf-URL in Bereitstellungen ohne Zertifikatauthentifizierung verwendet.	XenMobile	NetScaler Gateway
514	Wird für Verbindungen zwischen XenMobile und einem syslog-Server verwendet.	XenMobile	syslog-Server
636	Wird für sichere LDAP-Verbindungen verwendet.	NetScaler Gateway XenMobile	LDAP-Authentifizierungsserver oder Active Directory
1494	Wird für ICA-Verbindungen mit Windows-basierten Anwendungen im internen Netzwerk verwendet. Citrix empfiehlt, diesen Port geöffnet zu lassen.	NetScaler Gateway	XenApp oder XenDesktop

1812	Wird für RADIUS-Verbindungen verwendet.	NetScaler Gateway	RADIUS-Authentifizierungsserver
2598	Wird für Verbindungen mit Windows-basierten Anwendungen im internen Netzwerk unter Einsatz der Sitzungszuverlässigkeit verwendet. Citrix empfiehlt, diesen Port geöffnet zu lassen.	NetScaler Gateway	XenApp oder XenDesktop
3268	Wird für unsichere LDAP-Verbindungen mit dem globalen Microsoft-Katalog verwendet.	NetScaler Gateway XenMobile	LDAP-Authentifizierungsserver oder Active Directory
3269	Wird für sichere LDAP-Verbindungen mit dem globalen Microsoft-Katalog verwendet.	NetScaler Gateway XenMobile	LDAP-Authentifizierungsserver oder Active Directory
9080	Wird für HTTP-Datenverkehr zwischen NetScaler und dem XenMobile NetScaler Connector verwendet.	NetScaler	XenMobile NetScaler Connector
9443	Wird für HTTPS-Datenverkehr zwischen NetScaler und dem XenMobile NetScaler Connector verwendet.	NetScaler	XenMobile NetScaler Connector
45000 80	Wird in Clusterbereitstellungen für die Kommunikation zwischen zwei XenMobile-VM verwendet.	XenMobile	XenMobile
8443	Wird für die Registrierung, XenMobile Store und die Mobilanwendungsverwaltung (MAM) verwendet.	XenMobile NetScaler Gateway Geräte Internet	XenMobile
4443	Wird von Administratoren für den Zugriff auf die XenMobile-Konsole über einen Browser verwendet.	Zugriffspunkt (Browser)	XenMobile
	Dient zum Herunterladen von Protokollen und Supportpaketen für alle XenMobile-	XenMobile	XenMobile

	Clusterknoten von einem Knoten aus.		
27000	Standardport für den Zugriff auf den externen Citrix Lizenzserver	XenMobile	Citrix Lizenzserver
7279	Standardport zum Ein- und Auschecken von Citrix Lizenzen	XenMobile	Citrix Vendor Daemon

Öffnen von XenMobile-Ports zum Verwalten von Geräten

Sie müssen die folgenden Ports öffnen, damit XenMobile im Netzwerk kommunizieren kann.

TCP-Port	Beschreibung	Quelle	Ziel
25	Standard-SMTP-Port für den XenMobile-Benachrichtigungsdienst Wenn Ihr SMTP-Server einen anderen Port verwendet, stellen Sie sicher, dass die Firewall diesen Port nicht sperrt.	XenMobile	SMTP-Server
80 und 443	Verbindung zwischen dem firmeninternen App-Store und dem Apple iTunes-App-Store (ax.itunes.apple.com), Google Play (muss 80 verwenden) oder Windows Phone Store. Wird zum Veröffentlichen von Apps aus den App-Stores über Citrix Mobile Self-Serve unter iOS, Worx Home für Android oder Worx Home für Windows Phone verwendet.	XenMobile	Apple iTunes App Store (ax.itunes.apple.com und *.mzstatic.com) Apple-Programm für Volumenlizenzen (vpp.itunes.apple.com) Für Windows Phone: login.live.com und *.notify.windows.com Google Play (play.google.com)
80 oder 443	Wird für ausgehende Verbindungen zwischen XenMobile und Nexmo SMS Notification Relay verwendet.	XenMobile	Nexmo SMS Relay-Server
443	Wird für ausgehende Verbindungen zum AutoDiscovery-Server verwendet.	XenMobile	https://discovery.mdm.zenprise.com
443	Wird für die Registrierung und das Agent-Setup für Android und Windows Mobile verwendet.	Internet	XenMobile
	Wird für die Registrierung und das Agent-Setup für	Internes	

TCP-Port	Beschreibung	Quelle	Ziel
	Android- und Windows-Geräte, die XenMobile-Webkonsole und den MDM-Client für Remotesupport verwendet.	LAN und WiFi	
1433	Wird standardmäßig für Verbindungen mit einem Remotedatenbankserver verwendet (optional).	XenMobile	SQL Server
2195	Wird für ausgehende Verbindungen vom Apple Dienst für Pushbenachrichtigungen (APNs) zu gateway.push.apple.com für iOS-Gerätebenachrichtigungen und die Push-Anwendung von Geräterichtlinien verwendet.	XenMobile	Internet (APNs-Hosts mit öffentlicher IP-Adresse 17.0.0.0/8)
2196	Wird für ausgehende APNs-Verbindungen mit feedback.push.apple.com für die iOS-Gerätebenachrichtigung und die Push-Anwendung von Geräterichtlinien verwendet.		
5223	Wird für ausgehende APNs-Verbindungen von iOS-Geräten in WiFi-Netzwerken zu *.push.apple.com verwendet.	iOS-Geräte in WiFi-Netzwerken	Internet (APNs-Hosts mit öffentlicher IP-Adresse 17.0.0.0/8)
8443	Für die Registrierung von iOS- und Windows Phone-Geräten.	Internet	XenMobile
		LAN und WiFi	

Portanforderungen für die Verbindung mit Auto Discovery Service

Diese Portkonfiguration gewährleistet, dass auf Android-Geräten mit Worx Home für Android 10.2 über das interne Netzwerk auf Citrix Auto Discovery Service (ADS) zugegriffen werden kann. Der Zugriff auf den ADS ist zum Herunterladen von Sicherheitsupdates wichtig, die über diesen Dienst zur Verfügung gestellt werden.

Hinweis: ADS-Verbindungen funktionieren eventuell nicht mit dem vorhandenen Proxyserver. Lassen Sie in diesem Fall zu, dass ADS-Verbindungen den Proxyserver umgehen.

Für das Zertifikatpinning müssen die folgenden Voraussetzungen erfüllt sein:

- **Sammeln von XenMobile- und NetScaler-Zertifikaten**: Die Zertifikate müssen im PEM-Format und öffentlich, d. h. nicht der private Schlüssel sein.
- **Öffnen Sie einen Supportfall beim Citrix Support zum Aktivieren von Zertifikatpinning**: Bei diesem Prozess werden Ihre Zertifikate angefordert.

Die neuen Verbesserungen beim Zertifikatpinning erfordern, dass Geräte vor der Registrierung eine Verbindung mit ADS herstellen. Damit wird sichergestellt, dass Worx Home über die aktuellen Sicherheitsinformationen für die Umgebung verfügt, in der das Gerät registriert wird. Kann ein Gerät ADS nicht erreichen, lässt wird es von Home nicht registriert. Daher ist die Aktivierung des Zugriffs auf ADS im internen Netzwerk erforderlich, damit Geräte registriert werden können.

Damit der Zugriff auf ADS für Worx Home 10.2 für Android möglich ist, öffnen Sie Port 443 für die folgenden IP-Adressen und FQDNs:

FQDN	IP-Adresse
discovery.mdm.zenprise.com	54.225.219.53
	54.243.185.79
	107.22.184.230
	107.20.173.245
	184.72.219.144
	184.73.241.73
	54.243.233.48
	204.236.239.233
	107.20.198.193

FIPS 140-2-Richtlinientreue

May 05, 2016

Die FIPS-Norm (Federal Information Processing Standard) des US-Instituts für Normung (National Institute of Standards and Technologies, NIST) schreibt die Sicherheitsanforderungen für kryptographische Module in Sicherheitssystemen vor. FIPS 140-2 ist die zweite Version dieser Norm. Informationen zu NIST-geprüften FIPS 140-Modulen finden Sie unter http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf.

Wichtig: Sie können den XenMobile FIPS-Modus nur bei der ersten Installation aktivieren.
Hinweis: XenMobile für die Mobilgeräteverwaltung, XenMobile für die Verwaltung mobiler Apps und XenMobile Enterprise sind alle FIPS-konform, sofern keine HDX-Apps verwendet werden.
Für alle kryptographischen Vorgänge an ruhenden und in der Übertragung befindlichen Daten unter iOS werden FIPS-zertifizierte kryptographische Module von OpenSSL und Apple verwendet. Unter Android werden für alle kryptographischen Vorgänge an ruhenden und in der Übertragung vom Mobilgerät an NetScaler Gateway befindlichen Daten FIPS-zertifizierte kryptographische Module von OpenSSL verwendet.

Für Mobile Device Management (MDM) unter Windows RT, Microsoft Surface, Windows 8 Pro und Windows Phone 8 werden für alle kryptographischen Vorgänge an ruhenden und in der Übertragung befindlichen Daten FIPS-zertifizierte kryptographische Module von Microsoft verwendet.

Für alle kryptographischen Vorgänge an ruhenden und in der Übertragung befindlichen Daten in XenMobile Device Manager werden FIPS-zertifizierte kryptographische Module von OpenSSL verwendet. In Kombination mit den oben für Mobilgeräte bzw. zwischen Mobilgeräten und NetScaler Gateway beschriebenen kryptographischen Vorgängen werden für sämtliche Vorgänge an allen ruhenden und in der Übertragung von und zu MDM befindlichen Daten FIPS-konforme kryptographische Module verwendet.

Für alle kryptographischen Vorgänge an in der Übertragung von iOS-, Android- und Windows Mobile-Geräten an NetScaler Gateway befindlichen Daten werden FIPS-zertifizierte kryptographische Module verwendet. XenMobile nutzt ein in einer DMZ gehostetes NetScaler FIPS Edition-Gerät mit einem zertifizierten FIPS-Modul zum Sichern dieser Daten. Weitere Informationen finden Sie in der FIPS-Dokumentation zu NetScaler.

MDX-Apps werden unter Windows Phone 8.1 unterstützt und verwenden kryptographische Bibliotheken und APIs, die unter Windows Phone 8 FIPS-konform sind. Alle ruhenden Daten von MDX-Apps unter Windows Phone 8.1 sowie alle in der Übertragung zwischen Windows Phone 8.1-Geräten und NetScaler Gateway befindlichen Daten werden mit diesen Bibliotheken und APIs verschlüsselt.

MDX Vault verschlüsselt mit MDX umschlossene Apps und zugehörige ruhende Daten auf iOS- und Android-Geräten mit FIPS-zertifizierten kryptographischen Modulen von OpenSSL.

Die vollständige Erklärung zur FIPS 140-2-Konformität von XenMobile einschließlich der jeweils verwendeten Module erhalten Sie bei Ihrem Citrix Repräsentanten.

Sprachunterstützung für XenMobile

May 05, 2016

Citrix Worx-Apps und die XenMobile-Konsole sind für Englisch und für andere Sprachen ausgelegt. Dies umfasst die Unterstützung von erweiterten Zeichen und Tastatureingaben, auch wenn die App nicht in der bevorzugten Sprache des Benutzers lokalisiert ist.

Sprachunterstützung für Worx-Apps

Die folgende Tabelle führt die Sprachen auf, in die die Worx-Apps übersetzt wurden. Mit X gekennzeichnete Sprachen werden unterstützt.

Sprachen für die Benutzeroberfläche	Japanisch	Vereinfachtes Chinesisch	Deutsch	Französisch	Spanisch	Koreanisch	Portugiesisch	Niederländisch	Italienisch	Dänisch	Schwedisch	Hebräisch
Apple iPhone/iPad												
Worx Home	X	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X				
Android Phone/Tablet												
Worx Home	X	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X				
Windows Phone												
Worx Home			X	X	X				X	X	X	
WorxMail			X	X	X				X	X	X	
WorxWeb			X	X	X				X	X	X	

Vollständige Informationen zum Globalisierungsstatus von Citrix Produkten finden Sie im Citrix Knowledge Center.

Sprachunterstützung für die XenMobile-Konsole

In der folgenden Tabelle wird der Übersetzungsstatus für die XenMobile-Konsole aufgeführt, wobei mit X gekennzeichnete Sprachen verfügbar sind.

Sprachen für die Benutzeroberfläche	Vereinfachtes Chinesisch	Deutsch	Französisch	Koreanisch	Portugiesisch
XenMobile-Konsole	X	X	X	X	X

Unterstützung für Schreibrichtung von rechts nach links

In der folgenden Tabelle wird für jede App aufgeführt, welche Sprachen des Nahen Ostens unterstützt werden. Ein **X** bedeutet, dass das Feature für die Plattform verfügbar ist.

App	iOS	Android	Windows Phone
Worx Home	X	X	

WorxMail	X	X	
WorxWeb	X	X	
WorxTasks	X	X	
WorxNotes	X	X	
QuickEdit	X	X	

Checkliste vor der Installation

May 05, 2016

Diese Checkliste enthält die Voraussetzungen und Einstellungen für die Installation von XenMobile 10. Jede Aufgabe/Anmerkung enthält eine Spalte mit der Komponente bzw. Funktion, für die die Anforderung gilt. Installationsinformationen finden Sie unter Installieren von XenMobile.

Grundlegende Netzwerkeinstellungen

Nachfolgend sind die für XenMobile erforderlichen Netzwerkeinstellungen aufgeführt.

•	**Voraussetzung oder Einstellung**	**Komponente oder Funktion**	**Einstellung notieren**
	Notieren Sie den vollqualifizierten Domänennamen (FQDN) mit dem Remote-Benutzer eine Verbindung herstellen.	XenMobile NetScaler Gateway	
	Notieren Sie die öffentliche und lokale IP-Adresse. Sie brauchen diese IP-Adressen beim Konfigurieren der Firewall für die Netzwerkadressübersetzung (NAT).	XenMobile NetScaler Gateway	
	Notieren Sie die Subnetzmaske.	XenMobile NetScaler Gateway	
	Notieren Sie die DNS-IP-Adressen.	XenMobile NetScaler Gateway	
	Notieren Sie die WINS-Server-IP-Adressen (falls zutreffend).	NetScaler Gateway	
	Notieren Sie den Hostnamen von NetScaler Gateway. Hinweis: Dies ist nicht der vollqualifizierte Domänenname (FQDN). Der FQDN ist in dem signierten Serverzertifikat enthalten, der an den virtuellen Server gebunden ist und mit dem Benutzer die Verbindung herstellen. Sie können den Hostnamen mit dem Setupassistenten in NetScaler Gateway konfigurieren.	NetScaler Gateway	
	Notieren Sie die IP-Adresse von XenMobile.	XenMobile	

	Voraussetzung oder Einstellung	Komponente oder Funktion	Einstellung notieren
	Reservieren Sie eine IP-Adresse, wenn Sie eine Instanz von XenMobile installieren. Wenn Sie einen Cluster konfigurieren, notieren Sie alle benötigten IP-Adressen.		
	• Eine öffentliche IP-Adresse, die auf NetScaler Gateway konfiguriert ist • Einen externen DNS-Eintrag für NetScaler Gateway	NetScaler Gateway	
	Notieren Sie die IP-Adresse des Web-Proxyservers, den Port, die Proxy-Hostliste sowie Benutzername und Kennwort des Administrators. Diese Einstellungen sind optional, wenn Sie einen Proxyserver im Netzwerk bereitstellen. Hinweis: Zum Konfigurieren des Benutzernamens für den Web-Proxy können Sie den sAMAccountName oder den UPN (User Principal Name) verwenden.	XenMobile NetScaler Gateway	
	Notieren Sie die IP-Adresse des Standardgateways.	XenMobile NetScaler Gateway	
	Notieren Sie die System-IP-Adresse (NSIP) und Subnetzmaske.	NetScaler Gateway	
	Notieren Sie die Subnetz-IP-Adresse (NSIP) und Subnetzmaske.	NetScaler Gateway	
	Notieren Sie die IP-Adresse und den FQDN des virtuellen NetScaler Gateway-Servers aus dem Zertifikat. Wenn Sie mehrere virtuelle Server konfigurieren müssen, notieren Sie alle virtuellen IP-Adressen und FQDNs aus den Zertifikaten.	NetScaler Gateway	
	Notieren Sie die internen Netzwerke, auf die Benutzer über NetScaler Gateway zugreifen können. Beispiel: 10.10.0.0/24 Geben Sie alle internen Netzwerke und Netzwerksegmente an, auf die Benutzer zugreifen müssen, wenn sie eine Verbindung mit Worx Home oder dem NetScaler Gateway Plug-In herstellen und Split-Tunneling auf On gesetzt ist.	NetScaler Gateway	
	Stellen Sie sicher, dass zwischen XenMobile-Server, NetScaler Gateway, dem externen Microsoft SQL Server-Computer und dem DNS-Server Netzwerkkonnektivität besteht.	XenMobile NetScaler Gateway	

Lizenzierung

Für XenMobile müssen Sie Lizenzierungsoptionen für NetScaler Gateway und XenMobile erwerben. Informationen über die Citrix Lizenzierung finden Sie auf der Website zum Citrix Lizenzprogramm.

	Voraussetzung	Komponente	Speicherort notieren
	Beschaffen Sie universelle Lizenzen von der Citrix Website. Weitere Informationen finden Sie unter Installing NetScaler Gateway Licenses.	NetScaler Gateway XenMobile Citrix Lizenzserver	

Zertifikate

XenMobile und NetScaler Gateway erfordern Zertifikate für Verbindungen mit anderen Citrix Produkten und Anwendungen auf Benutzergeräten. Details finden Sie unter Zertifikate in XenMobile.

	Voraussetzung	Komponente	Hinweise
	Beschaffen und installieren Sie die erforderlichen Zertifikate.	XenMobile NetScaler Gateway	

Ports

Sie müssen Ports öffnen, um die Kommunikation mit XenMobile-Komponenten zu ermöglichen. Eine vollständige Liste der Ports, die geöffnet werden müssen, finden Sie unter Portanforderungen für XenMobile.

	Voraussetzung	Komponente	Hinweise
	Öffnen der Ports für XenMobile	XenMobile NetScaler Gateway	

Datenbank

Sie müssen eine Datenbankverbindung konfigurieren. Für das XenMobile-Repository muss eine Microsoft SQL Server-Datenbank einer der folgenden unterstützten Versionen ausgeführt werden: Microsoft SQL Server 2014, SQL Server 2012, SQL Server 2008 R2 oder SQL Server 2008. Citrix empfiehlt die Remote-Verwendung von Microsoft SQL. PostgreSQL ist Teil von XenMobile und sollte lokal oder remote nur in Testumgebungen verwendet werden.

	Voraussetzung	Komponente	Einstellung notieren
	IP-Adresse und Port des Microsoft SQL Server-Computers.	XenMobile	

	Voraussetzung	Komponente	Einstellung notieren
	Das in XenMobile verwendete SQL Server-Dienstkonto muss die Rollenberechtigung "DBcreator" haben.		

Active Directory-Einstellungen

	Voraussetzung	Komponente	Einstellung notieren
	Notieren Sie die Active Directory-IP-Adresse und den Port des primären und sekundären Servers. Wenn Sie Port 636 verwenden, installieren Sie ein Stammzertifikat von einer Zertifizierungsstelle in XenMobile und ändern Sie die Option Use secure connections auf Yes.	XenMobile NetScaler Gateway	
	Notieren Sie den Domänennamen für Active Directory.	XenMobile NetScaler Gateway	
	Notieren Sie das Active Directory-Dienstkonto (erfordert Benutzer-ID, Kennwort und Domänenalias). XenMobile verwendet das Dienstkonto für Active Directory-Abfragen.	XenMobile NetScaler Gateway	
	Notieren Sie den Benutzerbasis-DN. Dies ist die Verzeichnisebene, die Benutzer enthält, z. B. cn=users, dc=ace, dc=com. NetScaler Gateway und XenMobile verwenden dies für Active Directory-Abfragen.	XenMobile NetScaler Gateway	
	Notieren Sie den Gruppenbasis-DN. Dies ist die Verzeichnisebene, die Gruppen enthält. NetScaler Gateway und XenMobile verwenden dies für Active Directory-Abfragen.	XenMobile NetScaler Gateway	

Verbindungen zwischen XenMobile und NetScaler Gateway

	Voraussetzung	Komponente	Einstellung notieren
	Notieren Sie den XenMobile-Hostnamen.	XenMobile	
	Notieren Sie den FQDN oder die IP-Adresse von XenMobile.	XenMobile	
	Identifizieren Sie die Apps, auf die Benutzer zugreifen können.	NetScaler Gateway	

	Voraussetzung	Komponente	Einstellung notieren
	Notieren Sie die Callback-URL.	XenMobile	

Benutzerverbindungen: Zugriff auf XenDesktop, XenApp und Worx Home

Citrix empfiehlt, dass Sie Einstellungen für Verbindungen zwischen XenMobile und NetScaler Gateway und zwischen XenMobile und Worx Home mit dem Konfigurationsassistenten in NetScaler konfigurieren. Sie erstellen einen zweiten virtuellen Server, damit Benutzer Verbindungen von Receiver und Webbrowsern mit Windows-basierten Anwendungen und virtuellen Desktops in XenApp und XenDesktop herstellen können. Citrix empfiehlt, dass Sie auch diese Einstellungen mit dem Konfigurationsassistenten in NetScaler konfigurieren.

	Voraussetzung	Komponente	Einstellung notieren
	Notieren Sie den Hostnamen und die externe URL von NetScaler Gateway. Die externe URL ist die Webadresse, über die sich Benutzer verbinden.	XenMobile	
	Notieren Sie die NetScaler Gateway Callback-URL.	XenMobile	
	Notieren Sie die IP-Adressen und Subnetzmasken des virtuellen Servers.	NetScaler Gateway	
	Notieren Sie den Pfad für Program Neighborhood Agent oder eine XenApp Services-Site.	NetScaler Gateway XenMobile	
	Notieren Sie den FQDN oder die IP-Adresse des XenApp- oder XenDesktop-Servers, auf dem Secure Ticket Authority (STA) ausgeführt wird (nur für ICA-Verbindungen).	NetScaler Gateway	
	Notieren Sie den öffentlichen FQDN von XenMobile.	NetScaler Gateway	
	Notieren Sie den öffentlichen FQDN von Worx Home.	NetScaler Gateway	

Bekannte Probleme

May 05, 2016

Nachfolgend sind bekannte Probleme bei XenMobile 10.0 aufgeführt.

Eine Liste der in diesem Release behobenen Probleme finden Sie unter http://support.citrix.com/article/CTX141722.

- In Worx Home werden möglicherweise graue Platzhalter statt Symbole angezeigt, wenn ein iOS-Gerät von iOS 7 auf iOS 8 aktualisiert und dann neu gestartet wird. Dies ist ein Drittanbieterproblem. [#502879]
- Bei der Registrierung treten bei iOS-Geräten möglicherweise Fehler während oder nach der Installation von Profilen für die Mobilgeräteverwaltung (MDM) auf. Auf Geräten mit iOS 8.1 wird möglicherweise der Fehler "Cocoa error 4097" und auf Geräten, auf denen frühere Versionen von iOS ausgeführt werden, ein Fehler bei der Profilentschlüsselung gemeldet. Wenn dieses Problem auftritt, sollten Benutzer eine erneute Registrierung versuchen. In manchen Fällen sind mehrere Versuche erforderlich. [#507948]
- Sie können keine SOAP-Aufrufe "checkUserPassword" und "addGroup" in der Gruppenklasse USER in XenMobile 10 ausführen. Die Benutzer-API-Änderungen werden in der Datenbank, aber nicht auf Gerätebenutzeroberflächen angezeigt. [#511551, #511822]
- Es ist nicht möglich, über die XenMobile-Webkonsole die Bereitstellungsreihenfolge der Ressourcen von Bereitstellungsgruppen zu ändern. Wenn Sie die Bereitstellungsreihenfolge steuern möchten, benennen Sie die Ressourcen entsprechend dem von XenMobile verwendeten Bereitstellungsprotokoll um: numerisch (1, 2, 3, ...), Großbuchstaben (A, B, C, ...) und Kleinbuchstaben (a, b, c, ...). Eine Ressource, deren Name mit "24" beginnt, wird vor einer Ressource bereitgestellt, deren Name mit "WM" beginnt, und beide Ressourcen werden vor einer Ressource bereitgestellt, deren Name mit "tw" beginnt. [#512566]
- SafeSearch ist deaktiviert und auf Windows Phone 8.1-Geräten auf "Mittel" eingestellt, wenn der Filter für jugendgefährdenden Inhalt aktiviert ist. [#513605]
- Bei der Bereitstellung von Geräterichtlinien für Windows 8.1-Tablets werden die Richtlinien möglicherweise in der XenMobile-Konsole auf der Registerkarte Deployed unter Device details angezeigt, bevor XenMobile eine Bestätigung vom Gerät erhalten hat, dass die Richtlinie ausgeführt wurde. [#514749]
- Erneute Geräteregistrierungen können fehlschlagen, wenn sie zu schnell nach einer Aufhebung der Registrierung erfolgen. [#516567]
- Wenn Benutzer sich erneut bei Worx Home registrieren, wird manchmal eine zwischengespeicherte SSL-Sitzung aktiviert und der Bildschirm zur Registrierung erneut angezeigt. Wenn dieses Problem auftritt, sollten Benutzer eine erneute Registrierung durchführen. [#517301]
- Die App-Enumeration schlägt fehl, wenn Bereitstellungsgruppen mit Active Directory-Gruppen in übergeordneten und untergeordneten Domänen mit dem Operator AND definiert werden. Zur Problemumgehung verwenden Sie den Operator OR beim Definieren von Bereitstellungsgruppen. [#518084]
- Wenn Sie in der XenMobile-Konsole eine Einstellung oder Richtlinie konfigurieren und in diese eine Datei (Zertifikat, PDF, Schriftart usw.) hochladen, wird der Dateiname nicht angezeigt, wenn Sie später die Einstellungs- bzw. Richtliniendetails anzeigen. [#519552]
- XenMobile unterstützt bei iOS- und Android-Geräten im MAM-Modus (Mobilanwendungsverwaltung) keine Authentifizierung mit PIN. Wenn Sie diesen Modus als Standard in der XenMobile-Konsole konfigurieren, müssen Benutzer ihre Anmeldeinformationen in Worx Home zweimal eingeben. [#519572]
- Wenn Sie "AllUsers" als Bereitstellungsgruppe in der XenMobile-Konsole deaktivieren, können Benutzer, die zu keiner Bereitstellungsgruppe gehören, kein Gerät registrieren. Sie können sich jedoch beim für das Selbsthilfeportal anmelden. [#521393]
- Worx Home für Windows Phone 8.x, unterstützt im Mobilgeräteverwaltungsmodus nur Apps von öffentlichen Stores,

wenn diese als optional bereitgestellt werden. Wenn solche Apps einer Bereitstellungsgruppe als erforderlich hinzugefügt werden, werden sie in Worx Home nicht angezeigt. [#521524]

- Auf der Infoseite der rollenbasierten Zugriffssteuerung (RBAC) sind Änderungen an der Standard-Admin-Vorlage möglich. Hier oder anderswo vorgenommene Änderungen werden jedoch nicht in der Standard-Admin-Vorlage gespeichert. Die Standard-Admin-Vorlage ist nicht zur Bearbeitung vorgesehen. [#521540]
- Auf iOS-Geräten ist die Bereitstellung des SAML-Tokens bei der Registrierung von Benutzern in Worx Home und bei der Konfiguration von ShareFile-Konten u. U. nicht synchron. Benutzer umgehen dieses Problem, indem sie sich bei Worx Home ab- und wieder anmelden und sich dann an der ShareFile-App anmelden, um die Anforderung des SAML-Tokens erneut auszulösen. [#521934]
- Bei den meisten Android-Geräten werden beim Antippen des Menüsymbols die Optionen zum Akzeptieren und Ablehnen angezeigt, mit denen die Benutzer die Registrierung fortsetzen können. Bei einigen Geräten mit einem Betriebssystem vor Version 4.0 (z. B. Samsung-Tablet GT-P7510) wird das Menüsymbol nicht auf der Seite Terms and Conditions angezeigt und die Benutzer können die Registrierung nicht abschließen. Als Workaround können Sie die Geräte von der Terms and Conditions-Bereitstellung ausnehmen. [#524039]
- Zwischen Worx Home auf iOS-Geräten und dem Worx Store ist keine Verbindung möglich, wenn der Standardname des Stores auf der Seite Beacons in der XenMobile-Konsole (Configure > Settings > More > Beacons) geändert wird. Der Standardwert ist Store. Wenn diese Einstellung geändert wird, tritt im Discoverydienst bei der Benutzeranmeldepunkts ein Fehler auf und der Worx Store wird nicht gefunden. Zur Vermeidung dieses Fehlers behalten Sie auf der Seite Beacons die Einstellung Store für Store name bei. [#523306]
- Wenn Sie SAML-Apps in einer XenMobile-Konfiguration mit Load Balancing und SSL-Offload konfigurieren, müssen alle Referenzen zum XenMobile-Server auf Port 8443 statt 443 verweisen, damit Single Sign-On (SSO) funktioniert, wenn Benutzer WorxWeb installieren und eine vom Dienstanbieter initiierte App öffnen. [#528680]
- Bei der Konfiguration der Einstellung Lock device after (minutes of activity) für eine Samsung KNOX-Passcoderichtlinie erfolgt die Sperre durch den Server nach dem eingestellten Wert in Sekunden, obwohl die Einstellung in der Konsole in Minuten angegeben wird. [#531204]
- Sie können in XenMobile 10 keinen eigenen SAML-Dienst und Identitätsanbieter für die Authentifizierung von Benutzern und Geräten konfigurieren. [#530892]
- Sie können kein einzelnes BlackBerry- oder Windows-Gerät in der XenMobile-Konsole hinzufügen. [#532844]
- Wenn Sie SAML-Token App mit Nummernzeichen (#) im Namen konfigurieren, funktioniert Single Sign-On (SSO) über Worx Home nicht und eine Fehlermeldung wird angezeigt. [#533078]
- Wenn Sie eine generische PKI-Entität (GPKI) in der XenMobile-Konsole hinzufügen, können Sie die WSDL-URL-Adapterverbindung während der Konfiguration nicht testen. [#533871]
- Kennwortrichtlinien für Windows-Tablets treten nicht sofort auf den Geräten in Kraft und Aktualisierungen der Mindestkennwortlänge werden uneinheitlich umgesetzt. Dies ist ein Drittanbieterproblem. [#534088]
- Wenn Benutzer ein iOS-Gerät im Mobilgeräteverwaltungsmodus (MDM) registrieren, werden die Optionen für Security in der XenMobile-Konsole auf der Seite Manage > Devices zum Orten und Verfolgen von Geräten nicht sofort angezeigt. Nach einer kurzen Verzögerung werden die Optionen angezeigt. [#534672]
- Wenn Sie im Anzeigenamen des StoreFront-Delivery Controllers ein Sonderzeichen (z. B. einen Punkt) verwenden, können Benutzer keine Apps mit XenApp über Worx Home abonnieren und öffnen. Es wird dann gemeldet, dass die Anforderung nicht erfüllt werden kann. Um dieses Problem zu umgehen, entfernen Sie Sonderzeichen aus dem Namen. [#535497]
- Wenn Sie Apps hinzufügen und konfigurieren und einen Wert im Feld Excluded devices in der XenMobile-Konsole eingeben, werden die Apps für iOS-Geräte vor iOS 8 nicht im Worx Store angezeigt. Als Workaround können Sie eine Bereitstellungsregel konfigurieren, um die Geräte festzulegen, die die App installieren können. [#537631]
- Wenn Sie Verbindungen zwischen NetScaler Gateway und XenMobile für einen anderen Port als den Standardport 443 konfigurieren, schlägt die Registrierung für die Mobilanwendungsverwaltung (MAM) auf iOS-Geräten und für Worx Home auf Windows-Geräten fehl. [#537368]

- Sonderzeichen, wie $, @ und ", werden in Kennwörtern für die Befehlszeilenschnittstelle bei der Installation von XenMobile 10 und für zugewiesene Zertifikate nicht erkannt. Das Sonderzeichen und alle nachstehenden Zeichen werden ignoriert und die Anmeldung schlägt fehl. Nach der Installation kann das Kennwort für die Befehlszeilenschnittstelle nicht geändert werden, um Sonderzeichen einzuschließen. [#541997] [#542436]
- Ein Fehler für eine ungültiges Profil wird angezeigt, wenn Sie das iOS-Device Enrollment Program in der XenMobile-Konsole zu konfigurieren versuchen. Dies ist ein Drittanbieterproblem. [#608213]

Nachfolgend sind bekannte Probleme bei XenMobile Mail Manager 10.0 aufgeführt.

- 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.

Installieren von XenMobile

Oct 13, 2016

Virtuelle XenMobile-Maschine (VM) werden unter Citrix XenServer, VMware ESXi oder Microsoft Hyper-V ausgeführt. Sie können XenMobile über die XenCenter oder vSphere Management Console installieren.

Vorbereitungen: Bei der Planung einer XenMobile-Bereitstellung müssen viele Punkte berücksichtigt werden. Empfehlungen, Antworten auf allgemeine Fragen und Anwendungsfälle für XenMobile finden Sie in der XenMobile-Bereitstellungsdokumentation. Lesen Sie zunächst die Artikel Systemanforderungen für XenMobile 10 und Installationscheckliste für XenMobile 10.
Hinweis: Stellen Sie sicher, dass der Hypervisor mit der richtigen Uhrzeit konfiguriert ist, da diese von XenMobile verwendet wird.
XenServer- bzw. VMware ESXi-Voraussetzungen: Vor der Installation von XenMobile unter XenServer oder VMware ESXi müssen Sie die nachfolgenden Schritte ausführen. Weitere Informationen finden Sie in der Dokumentation zu XenServer bzw. VMware.

- Installieren Sie XenServer oder VMware ESXi auf einem Computer mit geeigneten Hardwareressourcen.
- Installieren Sie XenCenter oder vSphere auf einem separaten Computer. Der Hostcomputer von XenCenter oder vSphere muss über das Netzwerk mit dem Host von XenServer oder VMware ESXi verbunden sein.

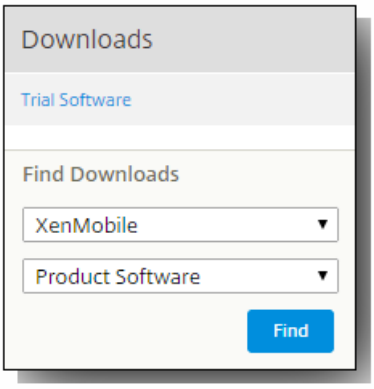
Hyper-V-Voraussetzungen: Vor der Installation von XenMobile unter Hyper-V müssen Sie die nachfolgenden Schritte ausführen. Weitere Informationen finden Sie in der Dokumentation zu Hyper-V.

- Installieren Sie Windows Server 2008 R2, Windows Server 2012 oder Windows Server 2012 mit aktiviertem Hyper-V und aktivierten Rollen auf einem Computer mit ausreichenden Systemressourcen. Beim Installieren der Hyper-V-Rolle müssen Sie die Netzwerkschnittstellenkarten (NICs) auf dem Server angeben, den Hyper-V zum Erstellen von virtuellen Netzwerken verwenden wird. Sie können einige NICs für den Host reservieren.

FIPS 140-2-Modus: Wenn Sie beabsichtigen, XenMobile-Server im FIPS-Modus zu installieren, müssen die in Konfigurieren von FIPS mit XenMobile erläuterten Voraussetzungen erfüllt sein.

Download der XenMobile-Produktsoftware

Sie können Produktsoftware von der Citrix Website herunterladen. Melden Sie sich bei der Citrix Website an und klicken Sie auf den Link Downloads. Sie können das Produkt und den Downloadtyp auswählen. Die folgende Abbildung zeigt beispielsweise die Auswahl von "XenMobile" und "Product Software":



Wenn Sie auf Find klicken, wird eine Seite mit einer Liste der verfügbaren Downloads angezeigt. Die aktuelle Version steht ganz oben auf der Liste. Sie können die gewünschte Software in der Liste der verfügbaren Optionen auswählen.

So laden Sie die Software für XenMobile herunter

1. Gehen Sie zur Citrix Website.
2. Klicken Sie auf My Account und melden Sie sich an.
3. Klicken Sie auf Downloads.
4. Klicken Sie unter Find Downloads in der Produktliste auf XenMobile.
5. Klicken Sie unter Find Downloads in der Downloadtypenliste auf Product Software und anschließend auf Find.
6. Klicken Sie auf der Seite XenMobile Product Software auf die XenMobile 10.0-Edition, die Sie herunterladen möchten.
7. Klicken Sie auf der Seite XenMobile 10.0 Edition für das entsprechende virtuelle Image (XenServer, VMware oder Hyper-V) auf Download, um XenMobile zu installieren.
8. Folgen Sie den Anweisungen auf dem Bildschirm, um die Software herunterzuladen.

So laden Sie die Software für NetScaler Gateway herunter

Mit diesen Schritten können Sie das virtuelle NetScaler Gateway-Gerät oder Softwareupgrades für das vorhandene NetScaler Gateway-Gerät herunterladen.

1. Gehen Sie zur Citrix Website.
2. Klicken Sie auf My Account und melden Sie sich an.
3. Klicken Sie auf Downloads.
4. Klicken Sie unter Find Downloads in der Produktliste auf NetScaler Gateway.
5. Klicken Sie unter Find Downloads in der Downloadtypenliste auf Product Software und anschließend auf Find.
   Hinweis: Sie können auch Virtual Appliances auswählen, um NetScaler VPX herunterzuladen. Wenn Sie diese Option auswählen, sehen Sie eine Liste mit Software für die virtuellen Maschinen für jeden Hypervisor.
6. Erweitern Sie auf der NetScaler Gateway-Seite den Eintrag 10.5(4).
7. Klicken Sie auf die Gerätesoftwareversion, die Sie herunterladen möchten.
8. Klicken Sie auf der Gerätesoftwareseite für die Version, die Sie herunterladen möchten, auf Download für das gewünschte virtuelle Gerät.
9. Folgen Sie den Anweisungen auf dem Bildschirm, um die Software herunterzuladen.

Konfigurieren von XenMobile für die Erstverwendung

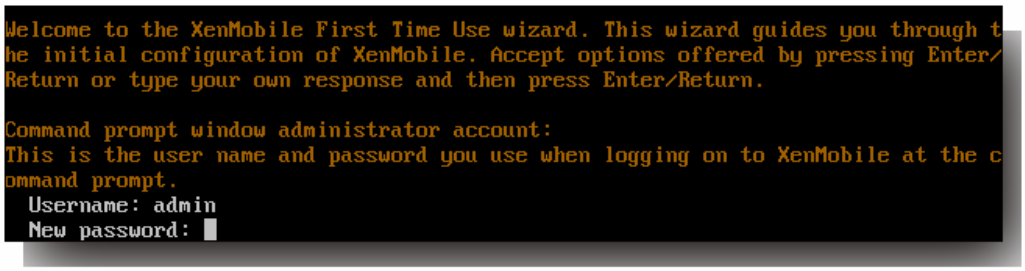
Die anfängliche Konfiguration von XenMobile ist ein zweiteiliger Prozess.

1. Konfigurieren Sie IP-Adresse, Subnetzmaske, Standardgateway und DNS-Server für XenMobile über die XenCenter- oder vSphere-Befehlszeilenkonsole.
2. Melden Sie sich bei der XenMobile-Verwaltungskonsole an und folgen Sie den Anweisungen der Bildschirme für die Erstanmeldung.

> **Hinweis**
>
> Bei Verwendung eines vSphere-Webclients wird empfohlen, die Netzwerkeigenschaften nicht bei der Bereitstellung der OVF-Vorlage über die Seite zum Anpassen der Vorlage zu konfigurieren. Dadurch vermeiden Sie in einer Umgebung mit hoher Verfügbarkeit ein Problem mit der IP-Adresse, das beim Klonen und Neustarten der zweiten virtuellen XenMobile-Maschine auftreten würde.

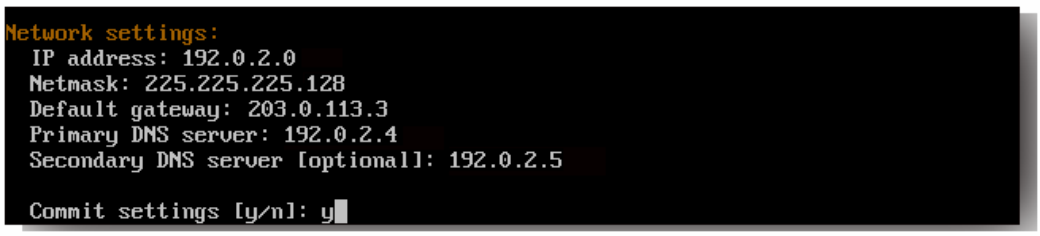
Konfigurieren von XenMobile im Eingabeaufforderungsfenster

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.



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

4. Geben Sie Folgendes ein:
    1. IP-Adresse
    2. Netzwerkmaske
    3. Standardgateway
    4. Primärer DNS-Server
    5. Sekundärer DNS-Server (optional)



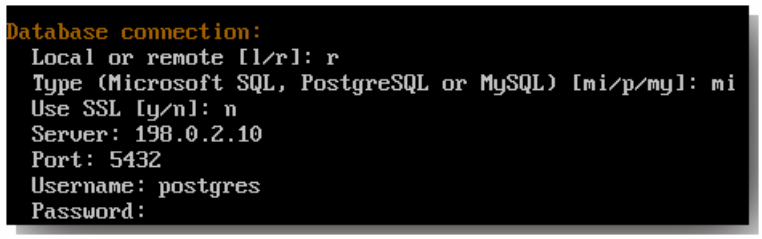
Hinweis: Die abgebildeten Adressen sind nicht funktionsfähig und dienen nur als Beispiel.

5. Geben Siey ein, um die Sicherheit zu erhöhen, indem Sie eine zufällige Passphrase generieren lassen, odern , um Ihre eigene Passphrase anzugeben. 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 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. Konfigurieren Sie die Datenbankverbindung. Sie können eine lokale oder remote Datenbank verwenden. Bei Anzeige der Frage Local or remote geben Sie Folgendes ein:r oderl.
   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.



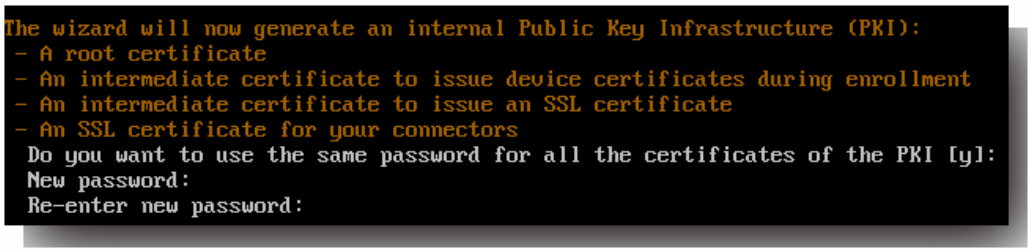
   Wichtig: Der Standardport für PostgreSQL ist 5432.

   Hinweis: Die abgebildeten Adressen sind nicht funktionsfähig und dienen nur als Beispiel.
8. Geben Sie den vollqualifizierten Domänennamen (FQDN) des Servers ein, auf dem XenMobile gehostet wird. Dieser Hostserver wird sowohl für die Geräteverwaltung als auch für die App-Verwaltung verwendet.

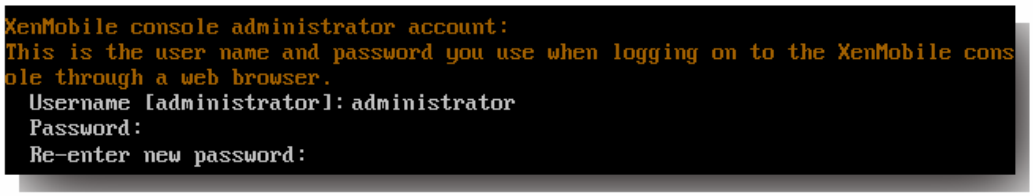
   Wichtig: Sie können den FQDN nicht ändern, ohne den Server komplett neu zu installieren.

9. 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.

10. Sie werden aufgefordert, Kennwörter für alle Public Key-Infrastruktur-Serverzertifikate anzugeben, und können auswählen, ob dasselbe Kennwort für alle Zertifikate verwendet werden soll. 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.



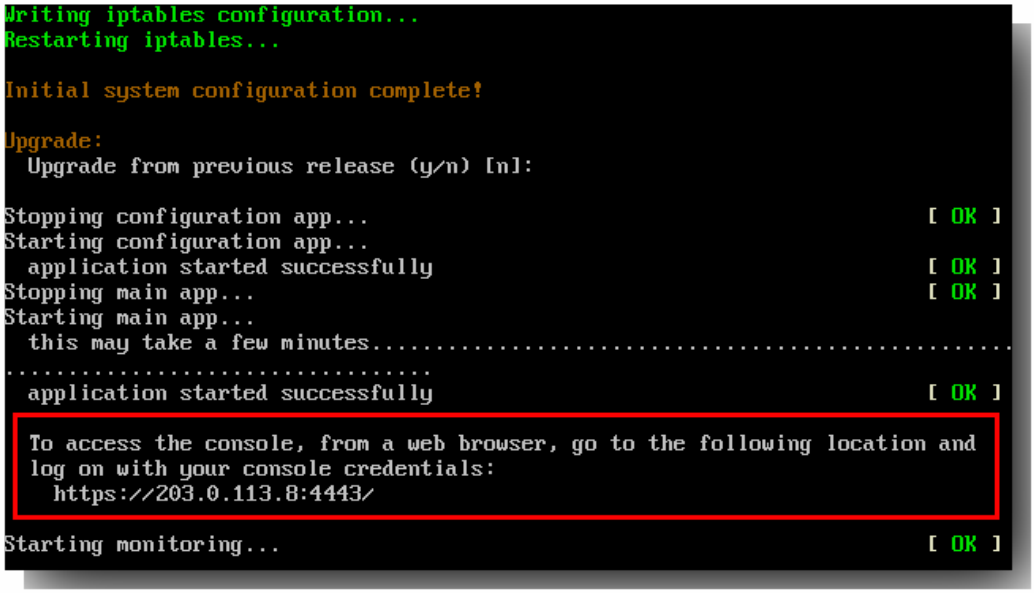
    Hinweis: Bei der Eingabe des neuen Kennworts werden keine Zeichen (Sternchen o. Ä.) angezeigt. Es wird nichts angezeigt.
11. Erstellen Sie ein Administratorkonto für die Anmeldung bei der XenMobile-Konsole mit einem Webbrowser. Diese Anmeldeinformationen sind zur späteren Verwendung aufzubewahren.



    Hinweis: Bei der Eingabe des neuen Kennworts werden keine Zeichen (Sternchen o. Ä.) angezeigt. Es wird nichts angezeigt.
12. Geben Sie zur Beantwortung der Frage, ob es sich um ein Upgrade handelt,n ein, da Sie eine Neuinstallation vornehmen.

13. Kopieren Sie die vollständige nun angezeigte URL und setzen Sie die Erstkonfiguration von XenMobile in Ihrem

Webbrowser fort.



Konfigurieren von XenMobile in einem Webbrowser

Nach Abschließen des erstens Teil der XenMobile-Konfiguration im Eingabeaufforderungsfenster des Hypervisors setzen Sie das Verfahren im Webbrowser fort.

1. Navigieren Sie im Webbrowser zu der zuletzt im Eingabeaufforderungsfenster angezeigten URL.
2. Geben Sie die Anmeldeinformationen des XenMobile-Konsolenadministratorkontos ein, die Sie zuvor im Eingabeaufforderungsfenster festgelegt haben.

3. Klicken Sie auf der Seite "Get Started" auf Start. Die Seite "Licensing" wird angezeigt.
4. Konfigurieren Sie die Lizenz. XenMobile enthält eine Evaluierungslizenz für 30 Tage. Informationen zum Hinzufügen und Konfigurieren von Lizenzen und zum Konfigurieren von Ablaufbenachrichtigungen finden Sie unter Lizenzierung von XenMobile.
   Wichtig: Wenn Sie Knoten oder Instanzen von XenMobile in Clustern verwenden möchten, müssen Sie die Citrix Lizenzierung auf einem Remoteserver verwenden.

5. Klicken Sie auf der Seite Certificate auf Import. Das Dialogfeld Import wird angezeigt.
6. Importieren Sie das APNs- und SSL Listener-Zertifikat. Informationen zur Arbeit mit Zertifikaten finden Sie unter Zertifikate in XenMobile.
   Hinweis: Das SSL-Listener-Zertifikat erfordert einen Serverneustart.
7. Konfigurieren Sie NetScaler Gateway, wenn die Umgebung dies erfordert. Informationen zur Konfiguration von NetScaler Gateway finden Sie unter NetScaler Gateway und XenMobile und Configuring Settings for Your XenMobile Environment.
   Hinweis: Sie können NetScaler Gateway am Rand des internen Netzwerks (Intranet) Ihres Unternehmens bereitstellen, sodass ein zentraler Zugriffspunkt auf alle Server, Anwendungen und andere Netzwerkressourcen im internen Netzwerk entsteht. In dieser Bereitstellung müssen alle Remotebenutzer eine Verbindung mit NetScaler Gateway herstellen, bevor sie auf Ressourcen im internen Netzwerk zugreifen können.
   Hinweis: Obwohl NetScaler Gateway eine optionale Einstellung ist, müssen Sie, wenn Sie auf der Seite Daten eingegeben haben, alle erforderlichen Felder ausfüllen oder leeren, um die Seite verlassen zu können.
8. Führen Sie die LDAP-Konfiguration für den Zugriff auf Benutzer und Gruppen aus Active Directory durch. Informationen zum Konfigurieren der LDAP-Verbindung finden Sie unter Konfigurieren von LDAP.
9. Konfigurieren Sie den Benachrichtigungsserver zum Senden von Nachrichten an Benutzer. Informationen zum Konfigurieren des Benachrichtigungsservers finden Sie unter Benachrichtigungen in XenMobile.

Konfigurieren von FIPS mit XenMobile

May 05, 2016

Zur Unterstützung von Kunden wie Behörden in den USA wird durch den FIPS-Modus (Federal Information Processing Standards) in XenMobile sichergestellt, dass der Server für alle Verschlüsselungsvorgänge ausschließlich FIPS 140-2-zertifizierte Bibliotheken verwendet. Durch die Installation des FIPS-Modus auf Ihrem XenMobile-Server wird sichergestellt, dass alle ruhenden und in der Übertragung befindlichen Daten für den XenMobile-Client und den -Server die Anforderungen von FIPS 140-2 erfüllen.

Bevor Sie einen XenMobile-Server im FIPS-Modus installieren, müssen die folgenden Voraussetzungen erfüllt werden.

- Sie müssen eine externe SQL Server 2012- oder SQL Server 2014-Datenbank als XenMobile-Datenbank verwenden. Der SQL Server muss für sichere SSL-Kommunikation konfiguriert sein. Anleitungen zum Konfigurieren von sicherer SSL-Kommunikation zum SQL Server finden Sie in den SQL Server Books Online.
- Für die sichere SSL-Kommunikation muss ein SSL-Zertifikat auf dem SQL Server installiert werden. Das SSL-Zertifikat kann ein öffentliches Zertifikat von einer kommerziellen Zertifizierungsstelle oder ein selbstsigniertes Zertifikat von einer internen Zertifizierungsstelle sein. SQL Server 2014 akzeptiert keine Platzhalterzertifikate. Citrix empfiehlt, dass Sie ein SSL-Zertifikat mit dem FQDN des SQL Servers anfordern.
- Wenn Sie ein selbstsigniertes Zertifikat für SQL Server verwenden, benötigen Sie eine Kopie des Stammzertifizierungsstellenzertifikats, von dem das selbstsignierte Zertifikat ausgestellt wurde. Das Stammzertifizierungsstellenzertifikat muss während der Installation in den XenMobile-Server importiert werden.

Konfigurieren des FIPS-Modus

Sie können den FIPS-Modus nur bei der Erstinstallation des XenMobile-Servers aktivieren. Nach der Installation kann FIPS nicht mehr aktiviert werden. Wenn Sie planen, den FIPS-Modus zu verwenden, müssen Sie daher von Anfang an den XenMobile-Server mit dem FIPS-Modus installieren. Wenn Sie einen XenMobile-Cluster haben, muss FIPS zudem auf allen Clusterknoten aktiviert sein. Eine Mischung von XenMobile-Servern mit und ohne FIPS im selben Cluster ist nicht zulässig.

Die Option **Toggle FIPS mode** in der XenMobile-Befehlszeilenschnittstelle ist nicht für eine Verwendung in der Produktion gedacht. Die Option ist für die Diagnose gedacht und wird auf einem XenMobile-Produktionsserver nicht unterstützt.

1. Aktivieren Sie **FIPS mode** während der Erstinstallation.

2. Laden Sie das Stammzertifizierungsstellenzertifikat für den SQL Server hoch. Wenn Sie ein selbstsigniertes SSL-Zertifikat statt eines öffentlichen Zertifikats für den SQL Server verwenden, wählen Sie für diese Option **Yes** und führen Sie einen der folgenden Vorgänge aus:

    a. Kopieren Sie das Zertifizierungsstellenzertifikat und fügen Sie es ein.

    b. Importieren Sie das Zertifizierungsstellenzertifikat. Um das Zertifizierungsstellenzertifikat zu importieren, müssen Sie das Zertifikat auf einer Website bereitstellen, auf die vom XenMobile-Server über eine HTTP-URL zugegriffen werden kann. Weitere Informationen finden Sie unter Importieren von Zertifikaten weiter unten in diesem Artikel.

3. Geben Sie den Namen und Port des SQL Servers an sowie die Anmeldeinformationen für den SQL Server und den Namen der für XenMobile zu erstellenden Datenbank.

Hinweis: Sie können eine SQL-Anmeldung oder ein Active Directory-Konto für den Zugriff auf den SQL Server verwenden.

Die Anmeldeinformationen müssen über eine DBcreator-Rolle verfügen.

4. Wenn Sie ein Active Directory-Konto verwenden, geben Sie die Anmeldeinformationen im Format domäne\benutzername ein.

5. Wenn Sie diese Schritte ausgeführt haben, fahren Sie mit der Ersteinrichtung von XenMobile fort.

Melden Sie sich an der XenMobile-Befehlszeilenschnittstelle an, um zu prüfen, ob der FIPS-Modus erfolgreich konfiguriert wurde. Im Anmeldebanner sollte die Meldung **In FIPS Compliant Mode** angezeigt werden.

Importieren von Zertifikaten

Mit den folgenden Schritten konfigurieren Sie FIPS auf XenMobile durch Importieren des Zertifikats, das erforderlich ist, wenn Sie ein VMware-Hypervisor verwenden.

Voraussetzungen für SQL

1. Die Verbindung zwischen der SQL-Instanz und XenMobile muss sicher sein und es muss sich um SQL Server Version 2012 oder SQL Server 2014 handeln. Anleitungen zum Sichern der Verbindung finden Sie unter How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console.

2. Wenn der Dienst nicht richtig neu startet, überprüfen Sie Folgendes: Öffnen Sie **Services.msc**.

   a. Kopieren Sie die Anmeldekontoinformationen für den SQL Server-Dienst.

   b. Öffnen Sie MMC.exe auf dem SQL Server.

   c. Gehen Sie zu **Datei** > **Snap-In hinzufügen/entfernen** und doppelklicken Sie auf das Zertifikatelement, das Sie dem Zertifikat-Snap-In hinzufügen möchten. Wählen Sie das Computerkonto und den lokalen Computer auf den zwei Seiten des Assistenten aus.

   d. Klicken Sie auf **OK**.

   e. Erweitern Sie **Zertifikate - Lokaler Computer** > **Persönlich** > **Zertifikate** und suchen Sie das importierte SSL-Zertifikat.

   f. Klicken Sie mit der rechten Maustaste auf das importierte Zertifikat, das Sie im SQL Server-Konfigurations-Manager ausgewählt haben, und klicken Sie dann auf **Alle Aufgaben** > **Private Schlüssel verwalten**.

   g. Klicken Sie unter **Gruppen- oder Benutzernamen** auf **Hinzufügen**.

   h. Geben Sie den Kontonamen des SQL-Diensts ein, den Sie zuvor kopiert haben.

   i. Deaktivieren Sie die Option **Vollzugriff**. Standardmäßig erhält das Dienstkonto Vollzugriffs- und Leseberechtigungen, aber es muss nur den privaten Schlüssel lesen können.

   j. Schließen Sie **MMC** und starten Sie den SQL-Dienst.

3. Stellen Sie sicher, dass der SQL-Dienst richtig startet.

Voraussetzungen für Internetinformationsdienste (IIS)

1. Laden Sie das Stammzertifikat herunter (Base 64).

2. Kopieren Sie das Stammzertifikat in die Standardsite auf dem IIS-Server, C:\inetpub\wwwroot.

3. Aktivieren Sie das Kontrollkästchen **Authentifizierung** für die Standardsite.

4. Legen Sie **Anonym** auf **aktiviert** fest.

5. Aktivieren Sie das Kontrollkästchen für die Regeln beim Fehlschlagen der Auftragsüberwachung.

6. Stellen Sie sicher, dass die Zertifikatdatei (.cer) nicht blockiert ist.

7. Navigieren Sie vom lokalen Server aus im Internet Explorer-Browser zum Speicherort der CER-Datei: http://localhost/certname.cer. Der Text des Stammzertifikats sollte im Browser angezeigt werden.

8. Wenn das Stammzertifikat nicht im Internet Explorer-Browser angezeigt wird, stellen Sie wie folgt sicher, dass ASP auf dem IIS-Server aktiviert ist.

   a. Öffnen Sie Server-Manager**.**

   b. Navigieren Sie zum Assistenten mit **Verwalten** > **Rollen und Features hinzufügen**.

   c. Erweitern Sie in den Serverrollen **Webserver (IIS)**, **Webserver**, **Anwendungsentwicklung**, und wählen Sie **ASP**.

   d. Klicken Sie auf **Weiter**, bis die Installation abgeschlossen ist.

9. Öffnen Sie Internet Explorer und navigieren Sie zu http://localhost/cert.cer.

Weitere Informationen finden Sie unter Internet Information Services (IIS) 8.5.

> **Hinweis**
>
> Verwenden Sie die IIS-Instanz der Zertifizierungsstelle für diesen Vorgang.

Importieren des Stammzertifikats während der FIPS-Erstkonfiguration

Wenn Sie die Erstkonfiguration von XenMobile in der Befehlszeilenkonsole durchführen, müssen Sie die folgenden Einstellungen festlegen, um das Stammzertifikat zu importieren. Ausführliche Installationsanleitungen finden Sie unter Installieren von XenMobile.

- Enable FIPS: Yes
- Upload Root Certificate: Yes
- Copy(c) or Import(i): i
- Geben Sie die HTTP-URL für den Import ein: http://*FQDN des IIS-Servers*/cert.cer
- Server: *FQDN des SQL-Servers*
- Port: 1433
- User name: Dienstkonto, das die Berechtigungen zum Erstellen der Datenbank besitzt (domäne\benutzername).
- Password: Das Kennwort für das Dienstkonto.
- Database Name: Geben Sie der Datenbank einen Namen.

XenMobile 10 MDM Upgrade Tool

May 05, 2016

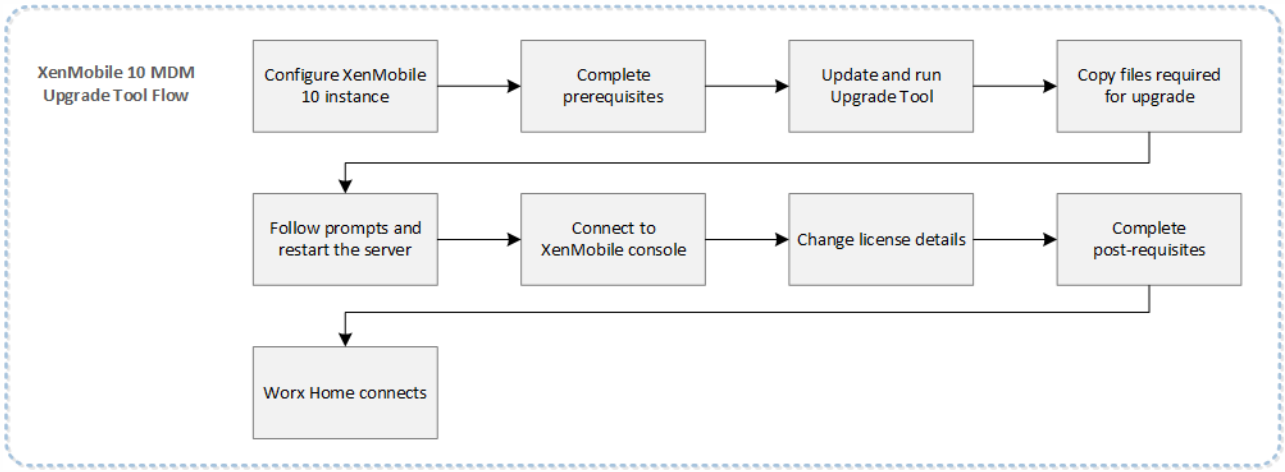
> ## Hinweis
>
> Citrix empfiehlt, die aktuelle Version Upgrade Tools zu verwenden. Mit der aktuellen Version können Sie die MAM-, MDM- und Enterprise-Modi Ihrer XenMobile 9.0-Umgebung mit einem Tool aktualisieren. Das Upgrade Tool können Sie von der Seite Citrix.com downloads herunterladen.

Sie verwenden das XenMobile 10 MDM Upgrade Tool zum Durchführen des Upgrades von XenMobile 9.0 auf XenMobile 10. Das Tool wird für das Upgrade von XenMobile MDM Edition-Bereitstellungen unterstützt.

Wichtig: Die Verwendung des Tools für Upgrades von XenMobile App Edition oder XenMobile Enterprise Edition wird nicht unterstützt. Das Tool kann auch nicht für Upgrades von XenMobile 8.6 oder 8.7 auf XenMobile 10 verwendet werden. Ist die Multi-Tenant Console (MTC) unter XenMobile 9.0 aktiviert, kann sie nicht nach XenMobile 10 migriert werden.
Wenn Ihr XenMobile 9.0-Setup auf benannten SQL-Instanzen basiert, müssen Sie bestimmten Schritten folgen. Weitere Informationen finden Sie unter Unterstützung für benannte SQL-Instanzen.

Das Upgrade Tool ist integraler Bestandteil der virtuellen XenMobile 10-Maschine. Sie aktivieren den Assistenten für die einmalige Verwendung über die Befehlszeilenkonsole bei der ersten Installation von XenMobile 10.

Die folgende Abbildung zeigt die grundlegenden Schritte beim Upgrade von XenMobile 9.0 auf XenMobile 10.



Lesen Sie vor der Migration auf XenMobile 10 die Abschnitte Voraussetzungen und Bekannte Probleme.

Vom Upgrade Tool migrierte Elemente

Das XenMobile MDM Upgrade Tool 10 migriert Konfigurations- und Benutzerdaten vom XenMobile 9.0-Server in eine neue Instanz von XenMobile 10 mit demselben vollqualifizierten Domänennamen (FQDN).

Sie können auswählen, ob Sie das Upgrade testen oder ein vollständiges Produktionsupgrade durchführen möchten. Bei

Auswahl von Test Drive werden nur Konfigurationsdaten, jedoch keine Geräte- oder Benutzerdaten nach XenMobile 10 migriert. Mit dieser Option können Sie XenMobile 9.0 und XenMobile 10 ohne Auswirkungen auf die Produktionsumgebung vergleichen.

Bei Auswahl von Production Upgrade werden sämtliche Konfigurations-, Geräte- und Benutzerdaten migriert. Wenn Sie sich nach dem Upgrade bei der XenMobile 10-Konsole anmelden, sehen Sie alle Benutzer- und Gerätedaten, die von XenMobile 9 migriert wurden.

Hinweis: Dies ist keine In-place-Migration, denn alle Daten werden nicht in XenMobile 10 verschoben sondern *kopiert*. Alle Daten bleiben in XenMobile 9.0 bestehen, bis Sie den XenMobile 10-Server in die Produktion übernehmen. Wenn Benutzer in einer Produktionsumgebung eine Verbindung mit XenMobile 10 herstellen und Sie aus irgendeinem Grund ein Downgrade auf XenMobile 9.0 durchführen möchten, müssen die Benutzer sich bei XenMobile 9.0 erneut registrieren.
Um XenMobile 10 nach einem erfolgreichen Produktionsupgrade in die Produktionsumgebung zu übernehmen, müssen Sie die folgenden Schritte ausführen:

1. Aktualisieren Sie den DNS-Eintrag, um den XenMobile 9.0-FQDN der neuen XenMobile 10-Server-IP-Adresse zuzuweisen.
2. Wenn NetScaler einen Lastausgleich der XenMobile Device Manager-Server durchführt, müssen Sie den XenMobile 9.0-Dienst auf den XenMobile 10-Dienst umschalten.

Vom Upgrade Tool nicht migrierte Elemente

Die folgenden Informationen werden mit dem Upgrade Tool **nicht** nach XenMobile 10 migriert:

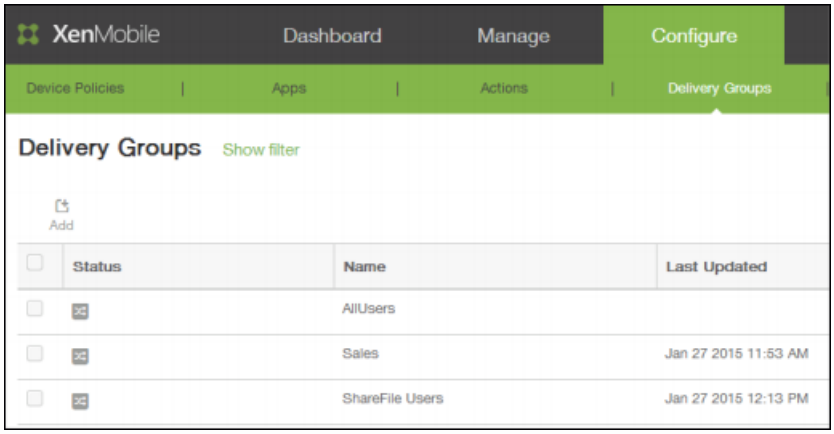
- Lizenzinformationen
- Berichtdaten
- Automatisierte Aktionen
- Servergruppenrichtlinien und zugeordnete Bereitstellungen
- MSP-Gruppe
- Richtlinien und Pakete für Windows CE und Windows 8.0
- Bereitstellungspakete, die nicht in Gebrauch sind, z. B., wenn ihnen keine Benutzer oder Gruppen zugewiesen sind
- Jegliche anderen Konfigurations- oder Benutzerdaten (siehe Datei migration.log)
- CXM Web (durch Citrix WorxWeb ersetzt)
- DLP-Richtlinien (durch Citrix ShareFile ersetzt)
- Benutzerdefinierte Active Directory-Attribute
- Wenn Sie mehrere Branding-Richtlinien konfiguriert haben, werden diese nicht migriert. XenMobile 10 unterstützt nur eine Branding-Richtlinie. Es darf daher nur eine Branding-Richtlinie in XenMobile 9.0 verbleiben, damit sie erfolgreich nach XenMobile 10 migriert werden kann.
- Alle Einstellungen in der Datei auth.jsp in XenMobile 9.0, die den Zugriff auf die Konsole einschränken. Zugriffseinschränkungen auf die Konsole in XenMobile 10 sind Firewalleinstellungen, die Sie in der Befehlszeilenschnittstelle konfigurieren können.

Für XenMobile 10 gelten außerdem die folgenden Änderungen:

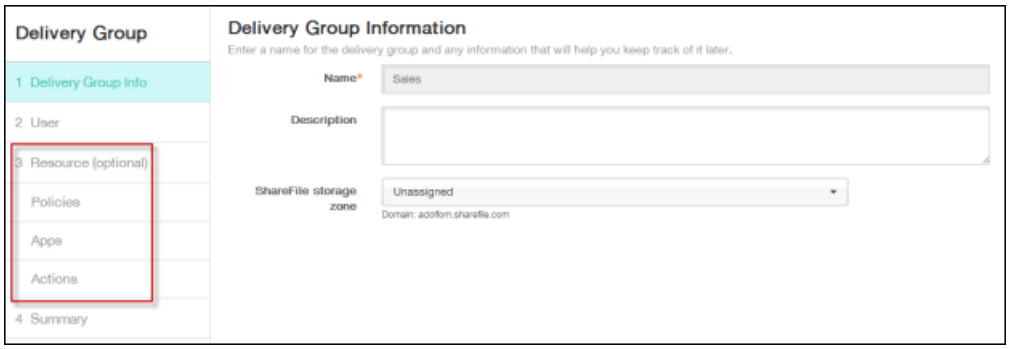
- XenMobile 10 unterstützt keine Active Directory-Benutzer, die lokalen Gruppen zugewiesen sind.
- Die Hierarchie der lokalen Gruppen ist flach.

Geänderte Terminologie bei XenMobile 10

Nach einem Upgrade werden Bereitstellungspakete in Device Manager als Bereitstellungsgruppen bezeichnet (siehe folgende Abbildung). Weitere Informationen finden Sie unter Verwalten von Bereitstellungsgruppen.



Innerhalb der Bereitstellungsgruppe können Sie die für Benutzergruppen, die Ressourcen benötigen, erforderlichen Richtlinien, Aktionen und Apps anzeigen.

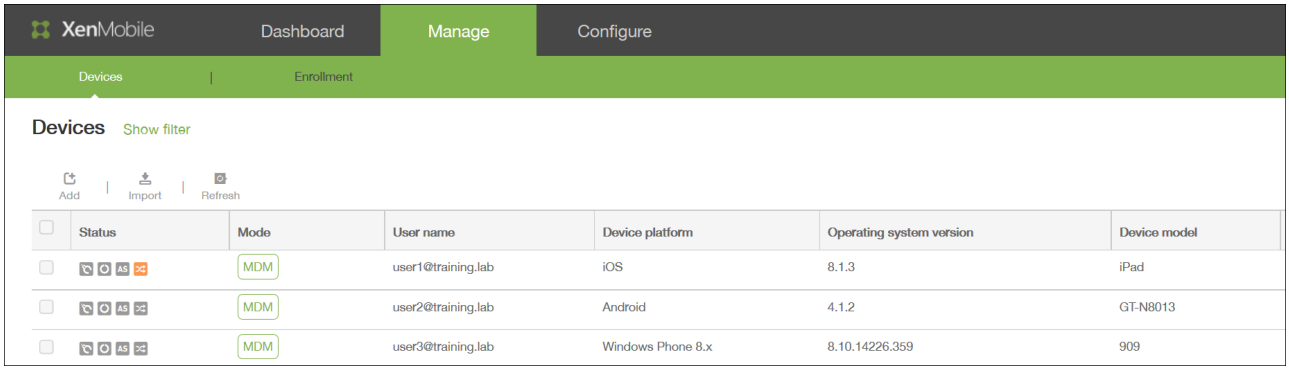


Geräteregistrierung nach dem Upgrade

Benutzer müssen ihre Geräte nach dem Upgrade auf XenMobile 10 nicht erneut registrieren. Die Geräte sollten basierend auf dem Taktintervall automatisch eine Verbindung mit dem XenMobile 10-Server herstellen.

Soll ein Gerät sofort mit XenMobile 10 verbunden werden, verwenden Sie auf dem Gerät WorxHome > Device Info > Refresh Policy.

Nach dem Verbinden der Benutzergeräte vergewissern Sie sich, dass Sie die Geräte in der XenMobile-Konsole wie in der folgenden Abbildung dargestellt sehen.



Voraussetzungen

May 05, 2016

Vor der Ausführung des XenMobile 10 MDM Upgrade Tools müssen die folgenden Voraussetzungen erfüllt werden.

Citrix Lizenzserver

Installieren Sie Version 11.12.1 des Citrix Lizenzservers (verfügbar auf der Seite Citrix Licensing) und konfigurieren Sie den Server mit der aktuellen V6-Lizenz für die ausschließliche Mobilgeräteverwaltung (MDM). Stellen Sie sicher, dass die Lizenzserverports 27000 und 7279 für den Server geöffnet sind. Dieser Schritt ist wichtig, um ein versehentliches Upgrade von Benutzergeräten auf den XenMobile Enterprise-Modus zu verhindern, wodurch Lizenzverstöße möglich wären und eine erneute Registrierung der Geräte von Benutzern erforderlich würde.

Datenbank

Die Migration ist nur zwischen Datenbanken desselben Typs möglich. Beispiel:

Unterstützt

- PostgreSQL nach PostgreSQL
- MSSQL nach MSSQL

Nicht unterstützt

- MSSQL nach PostgreSQL
- PostgreSQL nach MSSQL

Bei der Datenmigration muss XenMobile auf die unter XenMobile 9.0 Device Manager implementierte Datenbanklösung zugreifen können. Beispielsweise müssen die folgenden Ports geöffnet sein:

- Standardport für Microsoft SQL Server ist 1433.
- Standardport für PostgreSQL ist 5432.

Zum Ermöglichen von Remoteverbindungen mit PostgreSQL müssen Sie die folgenden Schritte ausführen:

1. Öffnen Sie die Datei pg_hba.conf und suchen Sie die folgende Zeile: "host all all 127.0.0.1/32 md5"
2. Fügen Sie eine neue Zeile ein: host all all [XMS-Adresse/externe Adresse]/32 md5
3. Speichern Sie die Datei.
4. Halten Sie den Dienst an und starten Sie ihn wieder.
5. Suchen und öffnen Sie die Datei postgresql.conf und ändern die Zeile
   "#listen_addresses = 'localhost'"

   in

   "listen_addresses = '*'"

   Hinweis: Die Zeile darf nicht auskommentiert sein. Hier kann eine Einschränkung konfiguriert werden, sodass nur von den IP-Adressen von XenMobile 9.0- und XenMobile 10-Servern Zugriff auf die PostgreSQL-Datenbank besteht (listen_addresses = '10.x.x.1,10.x.x.2').
6. Halten Sie den PostgreSQL-Dienst an und starten Sie ihn wieder, damit die Änderungen wirksam werden.
7. Stellen Sie sicher, dass XMS und die Datenbank miteinander kommunizieren. (Damit wird auch sichergestellt, dass die Datenbank Remoteverbindungen empfangen kann.)

Wenn der Datenbanklösung ein benutzerdefinierter Port zugewiesen wurde, muss dieser in der Firewall, die XenMobile 9.0 Device Manager schützt, geöffnet und zulässig sein. Dadurch kann XenMobile 10 eine Verbindung mit der Datenbank herstellen und die erforderlichen Informationen migrieren.

Externes SSL-Zertifikat

Externe SSL-Zertifikate müssen die unter How to Configure an External SSL Certificate aufgeführten Bedingungen erfüllen. Überprüfen Sie die Datei pki.xml vor der Migration, um sicherzustellen, dass das SSL-Zertifikat diese Bedingungen erfüllt.

Administratorkonto- Benutzername

Der Benutzername des Administratorkontos, das für die Anmeldung bei der XenMobile 10-Konsole verwendet wird, darf nur Kleinbuchstaben enthalten, andernfalls können Sie sich nach der Migration nicht bei der XenMobile 10-Konsole anmelden. Erstellen Sie ein Administratorkonto unter ausschließlicher Verwendung von Kleinbuchstaben und mit allen Berechtigungen, damit Sie sich nach der Migration mit diesem Konto bei der XenMobile 10-Konsole anmelden können.

Bereitstellungspaketnamen mit Sonderzeichen

Bereitstellungspaketnamen in XenMobile 9.0 mit Sonderzeichen (!, $, (), #, % , +, *, ~, ?, |, {} und []) werden migriert, die entsprechenden Bereitstellungsgruppen können nach der Migration jedoch nicht in XenMobile 10 bearbeitet werden. Außerdem verursachen lokale Benutzer und lokale Gruppen, die in XenMobile 9.0 erstellt wurden und deren Name eine eckige Klammer links ([) enthält, Probleme in XenMobile 10 beim Erstellen von Registrierungseinladungen. Entfernen Sie vor der Migration alle Sonderzeichen aus Bereitstellungspaketnamen und alle eckigen Klammern links aus den Namen lokaler Benutzer und lokaler Gruppen.

Kopieren von Dateien von XenMobile 9.0 Device Manager

Vorausgesetzt, dass Device Manager im Standardverzeichnis installiert ist (C:\Programme Files(x86)\Citrix\XenMobile Device Manager\tomcat), kopieren Sie die folgenden Dateien in einen temporären Ordner:

Aus dem Ordner "C:\Programme (x86)\Citrix\XenMobile Device Manager\tomcat\conf":

- server.xml
- https.p12
- cacerts.pem.jks
- pki-ca-root.p12
- pki-ca-devices.p12
- pki-ca-servers.p12

Hinweis: Wenn auf dem Server mit Device Manager benutzerdefinierte Server-SSL-Serverzertifikate (.p12) verwendet wurden, kopieren Sie anstelle der Datei https.p12 das Zertifikat in den temporären Ordner.
Kopieren Sie die folgenden Dateien aus dem Ordner "C:\Programme (x86)\Citrix\XenMobile Device Manager\tomcat\webapps\zdm\WEB-INF\classes\" in denselben temporären Ordner:

- ew-config.properties
- pki.xml
- variables.xml

Nachdem Sie alle Dateien kopiert haben, öffnen Sie den temporären Ordner und komprimieren die Dateien in einer ZIP-Datei. Komprimieren Sie nicht den Ordner, sondern die Dateien. Die komprimierten Dateien werden während des Upgrades hochgeladen.

Wenn Sie sich über alle bekannten Probleme informiert und alle Voraussetzungen erfüllt haben, können Sie mit dem Upgrade

beginnen. Details finden Sie unter Aktivieren und Ausführen des XenMobile 10 MDM Upgrade Tools

Bekannte Probleme

May 05, 2016

Nachfolgend sind bekannte Probleme bei XenMobile 10 MDM Upgrade Tool aufgeführt.

- XenMobile-Grenzwert für Sperrung wird nicht migriert. Legen Sie den Wert nach der Migration erneut fest. [#545770]
- Optionen der rollenbasierten Zugriffssteuerung (RBAC) werden nicht einwandfrei migriert. Prüfen Sie nach der Migration die RBAC-Rollen und nehmen Sie alle erforderlichen Änderungen vor. [#543183]
- Protokolleinstellungen werden nicht migriert. Konfigurieren Sie nach der Migration die Protokolleinstellungen in der XenMobile-Konsole neu. [#541869]
- Wenn mehrere LDAP- Konfigurationen, bei denen nur eine verschachtelte Gruppen unterstützen soll, migriert werden, ist die Unterstützung verschachtelter Gruppen nach der Migration für alle LDAP-Konfigurationen aktiviert. Außerdem werden Gruppen beim Serverstart auf allen LDAP-Servern synchronisiert. [#540713]
- Wenn eine Geräterichtlinie für die Webinhaltsfilterung eine URL ohne HTTP/HTTPS enthält, wird die URL gelöscht, wenn Benutzer sie bearbeiten und dann den Vorgang abbrechen. Stellen Sie nach der Migration sicher, dass alle URLs HTTP oder HTTPS enthalten, um zu verhindern, dass sie beim Abbrechen einer Bearbeitung gelöscht werden. [#540025]
- Wenn Richtlinien, Apps oder Aktionen in mehreren Paketen mit unterschiedlichen Regeln enthalten sind, werden Bereitstellungsregeln nicht migriert. Dieses Verhalten ist beabsichtigt. [#539517]
- Der XenMobile 9.0-Administrator kann sich nach einer erfolgreichen Migration nicht bei der XenMobile 10-Konsole anmelden, wenn sein Benutzername einen Großbuchstaben enthält. Erstellen Sie vor der Migration ein Administratorkonto unter ausschließlicher Verwendung von Kleinbuchstaben und mit allen Berechtigungen, damit Sie sich nach der Migration mit diesem Konto bei der XenMobile 10-Konsole anmelden können. [#547422]
- Wenn die Multi-Tenant Console (MTC) unter XenMobile 9 aktiviert ist, kann sie nicht nach XenMobile 10 migriert werden. [#549969]
- Mit einer in XenMobile 9.0 erstellten Super Admin-Rolle werden mehrere Berechtigungen für Einstellung und Zuweisung nicht nach XenMobile 10 migriert. Navigieren Sie nach der Migration in der XenMobile 10-Konsole zu Configure > Settings > Role Based Access Control und erstellen Sie die XenMobile 9.0-Super Admin-Rolle mit Berechtigungen aus der XenMobile 10-Admin-Rolle neu. [#553079]

- In XenMobile 9.0 erstellte Bereitstellungspaketnamen mit Sonderzeichen (!, $, (), #, % , +, *, ~, ?, |, {} und []) können nach der Migration nicht bearbeitet werden. Außerdem verursachen lokale Benutzer und lokale Gruppen, die in XenMobile 9.0 erstellt wurden und deren Name eine eckige Klammer links ([) enthält, Probleme in XenMobile 10 beim Erstellen von Registrierungseinladungen. Entfernen Sie vor der Migration alle Sonderzeichen aus Bereitstellungspaketnamen und alle eckigen Klammern links aus den Namen lokaler Benutzer und lokaler Gruppe. [#538639]

Aktivieren und Ausführen des XenMobile 10 MDM Upgrade Tools

May 05, 2016

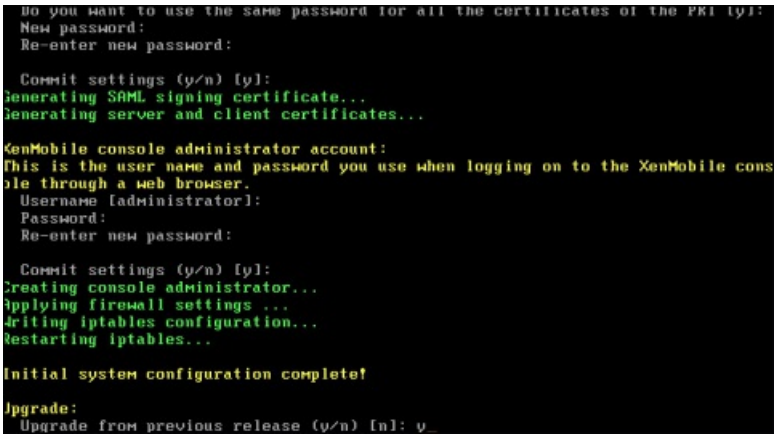
Die grundlegenden Schritte beim Upgrade von XenMobile 9.0 auf XenMobile 10 sind folgende:

1. Konfigurieren der XenMobile 10-Instanz über die Befehlszeilenkonsole
2. Erfüllen aller Upgrade Tool-Voraussetzungen. Details finden Sie unter Voraussetzungen.
3. Aktualisieren des Upgrade Tools auf die aktuelle Version
   Wichtig: Leeren des Browsercache nach dem Neustart des Systems
4. Starten des Upgrade Tools in Firefox oder Chrome
5. Upload der kopierten XenMobile 9.0-Dateien in das Upgrade Tool
6. Eingeben des Zertifikatkennworts für XenMobile 9.0
7. Ausführen des Upgrade Tools
8. Neustarten des XenMobile 10-Servers
9. Anmelden bei der XenMobile 10-Konsole
10. Konfigurieren von Lizenzen unter XenMobile 10, damit Benutzer eine Verbindung herstellen können
11. Produktionsupgrade: Ändern des externen DNS für XenMobile zum Verweis auf den neuen XenMobile 10-Server
12. Produktionsupgrade bei Verwendung von NetScaler für Lastausgleich: Entfernen der XenMobile 9.0-Server-IP und Hinzufügen der XenMobile 10-Server-IP

So installieren Sie eine Instanz von XenMobile 10 und aktivieren das Upgrade Tool

Sie aktivieren das Upgrade Tool über die Befehlszeilenkonsole bei der Erstinstallation von XenMobile 10 (siehe folgende Abbildung).

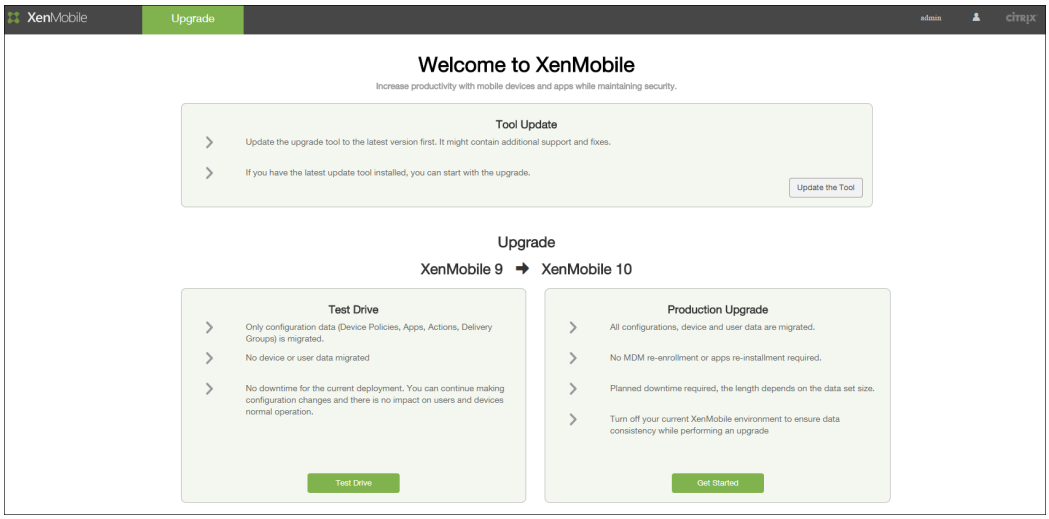
Wichtig: Wenn Sie einen Snapshot des Systems erstellen möchten, tun Sie dies nach der anfänglichen XenMobile 10-Konfiguration und *vor* dem Zugriff auf das Upgrade Tool.



Wenn Sie **y** eingeben, um das Upgrade durchzuführen, wird das Upgrade Tool zur einmaligen Verwendung aktiviert. Sie greifen dann auf das Upgrade Tool über https:///uw/ zu.

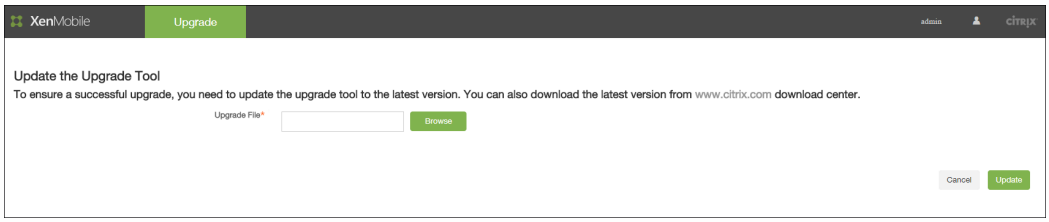
Tipp: Citrix empfiehlt die Verwendung von Firefox oder Chrome für den Zugriff auf das Upgrade Tool. Internet Explorer wird nicht empfohlen.
Beim Migrieren auf den neuen Server stellen Sie sicher, dass der Hostname des neuen Servers mit dem Hostnamen des Quellservers der Migration übereinstimmt. Dadurch wird sichergestellt, dass Worx Home mit XenMobile 10 über denselben

Hostnamen eine Verbindung herstellen kann wie zuvor mit XenMobile 9.0. Die Benutzer müssen sich so in XenMobile 10 nicht erneut registrieren.



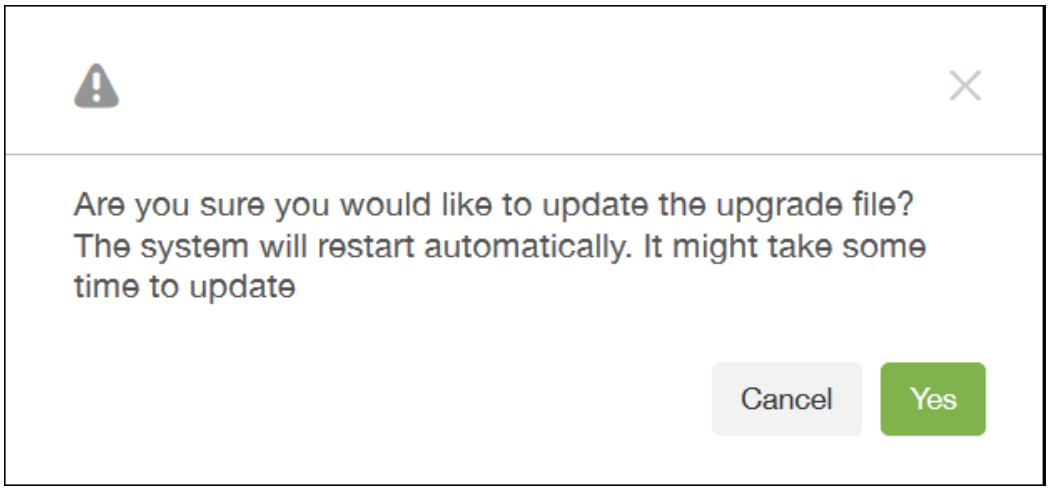
So aktualisieren Sie das Upgrade Tool und beginnen die Migration

Updates für das Upgrade Tool finden Sie auf der XenMobile-Downloadseite. Für eine MDM-Migration müssen Sie das aktuelle Tool verwenden, das Sie von Citrix.com herunterladen können.



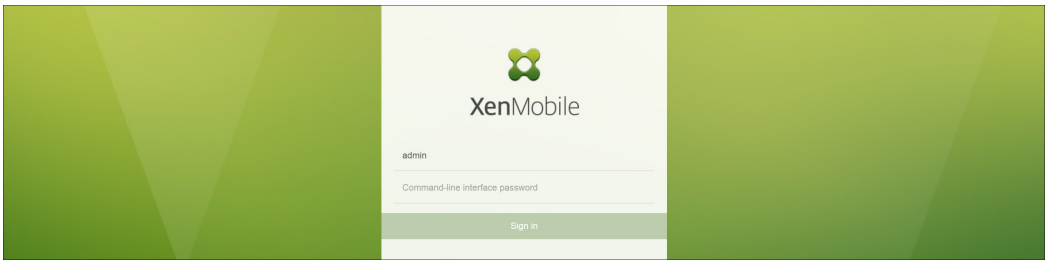
Die folgende Meldung wird zur Bestätigung des Starts des Updateprozesses angezeigt.

Hinweis: Nachdem Sie auf Yes geklickt haben, wird keine Fortschrittsanzeige angezeigt, Sie können jedoch in der Befehlszeilenschnittstelle beobachten, wann das System neu gestartet wird. Das Update dauert ca. 30 Sekunden.

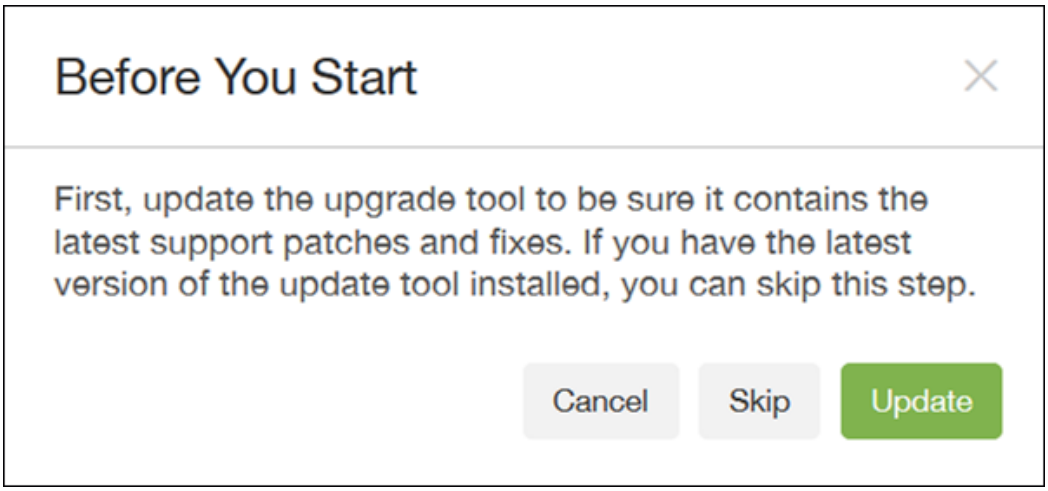


Hinweis:

- Nach dem Neustart des Systems leeren Sie den Browsercache, bevor Sie auf das Upgrade Tool unter der URL https:///uw zugreifen.
- Wenn Sie nicht den Standardport für die Kommunikation über HTTPS (443) verwenden, lautet die Upgrade Tool-URL https://:/uw.



Nach der Anmeldung beim Upgrade Tool können Sie in diesem Fall auf **Skip** klicken, da Sie das Upgrade Tool bereits aktualisiert haben.



Wählen Sie Test Drive oder Production Upgrade aus und führen Sie dann die Migration durch.

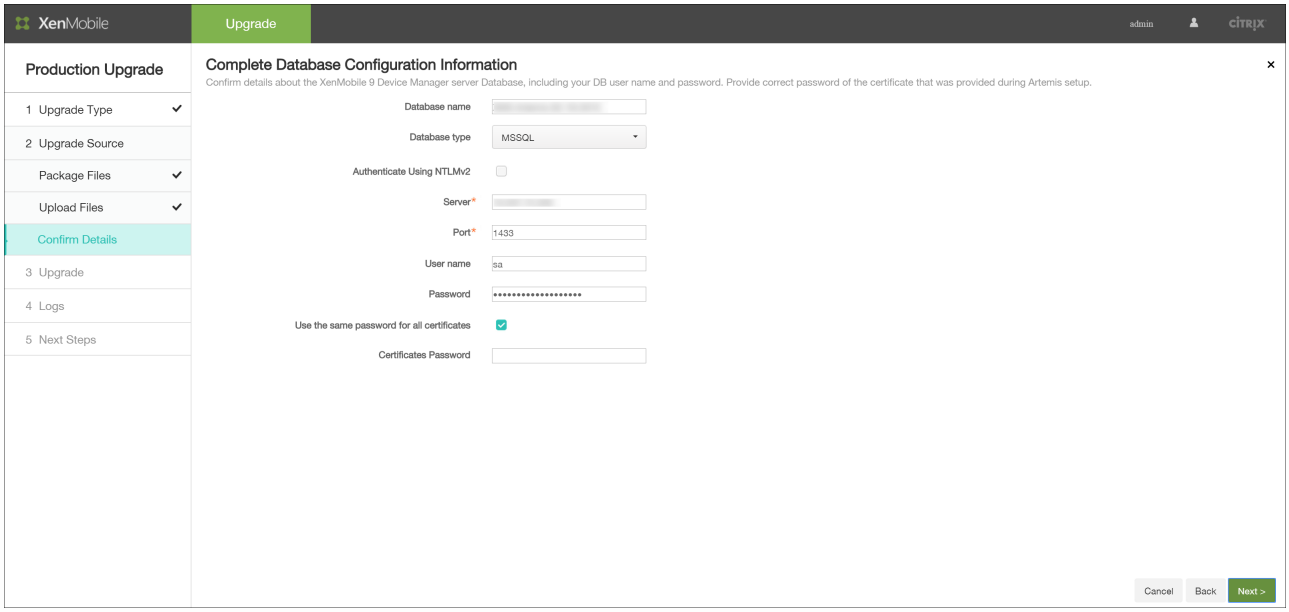
Wenn das Upgrade Tool geöffnet wird, können Sie auswählen, ob Sie alle Daten oder nur die Konfigurationsdaten migrieren möchten. Wenn Sie Configuration Data only auswählen, müssen die Benutzer ihre Geräte erneut registrieren. Klicken Sie auf Next, um die als Voraussetzung in den temporären Ordner kopierten und komprimierten Dateien hochzuladen.

Klicken Sie nach Abschluss des Uploads auf Next.

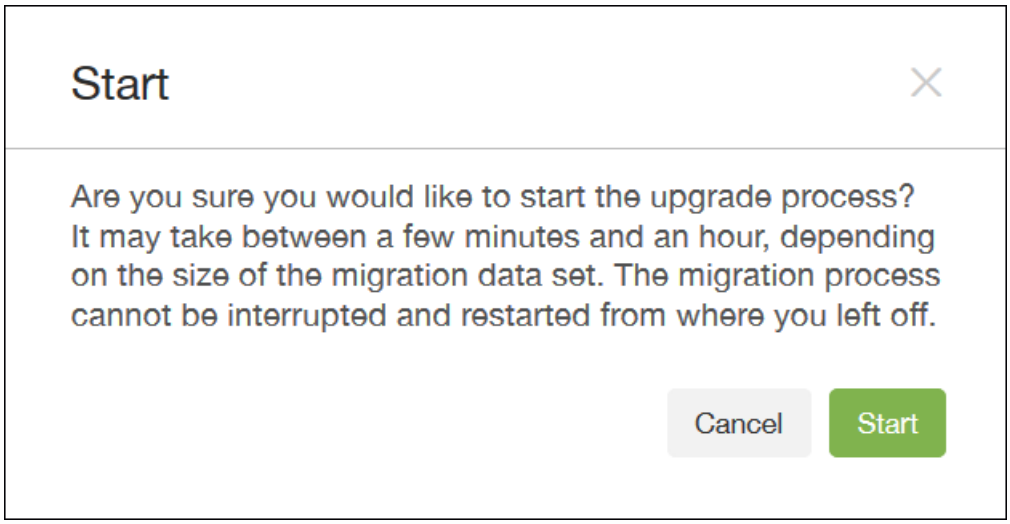
Wenn Sie eine PostgreSQL-Datenbank migrieren und der Servernamen lautet "localhost", müssen Sie "localhost" in die Server IP-Adresse ändern.

Vergewissern Sie sich, dass die von XenMobile 9.0 Device Manager gesammelten Informationen richtig sind. Sie müssen auch das Zertifikatkennwort eingeben.

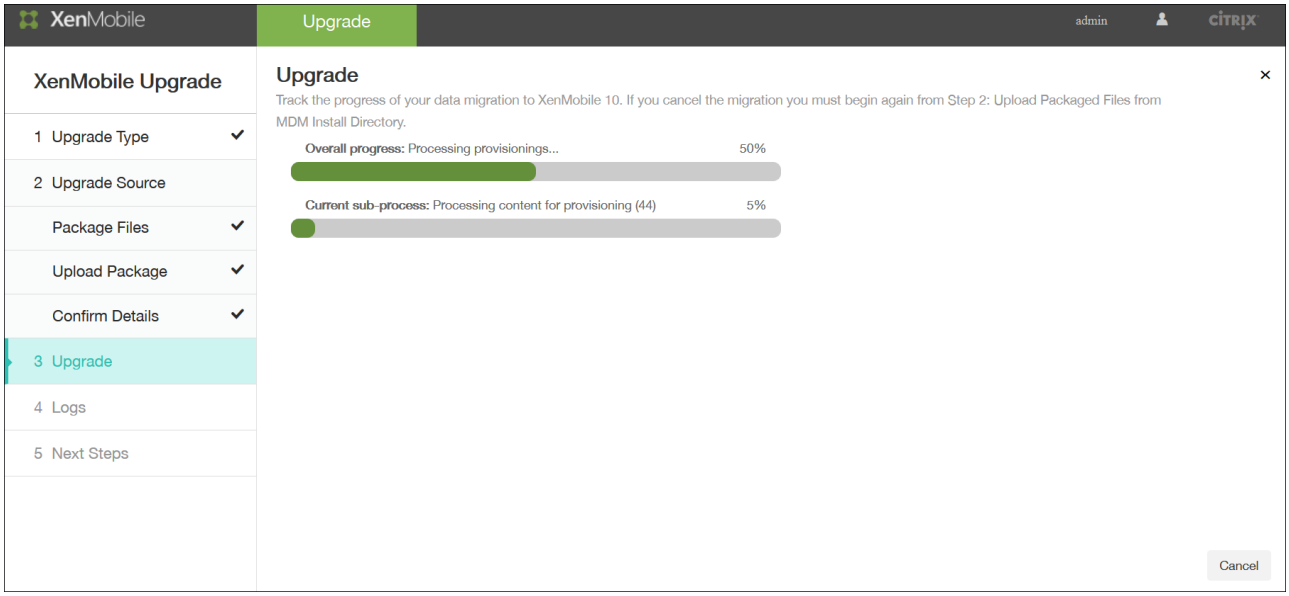
Wichtig: Alle Zertifikatkennwörter müssen richtig eingegeben werden, ansonsten schlägt die Migration fehl.

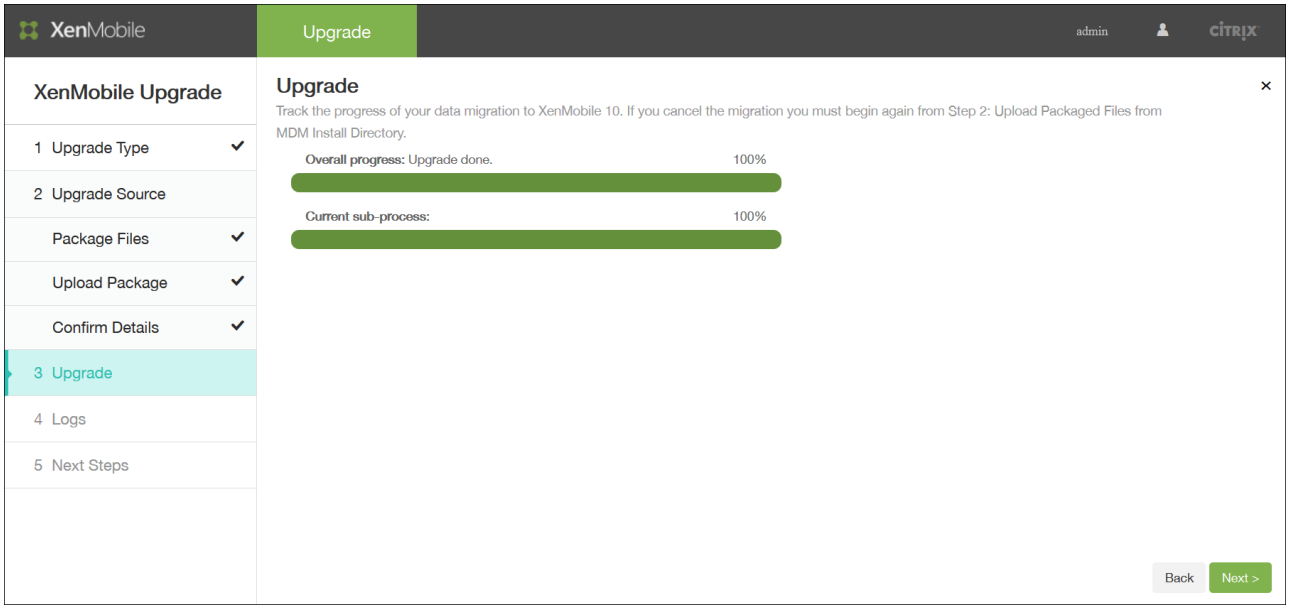


Wenn Sie auf Next klicken, wird die folgende Bestätigungsmeldung angezeigt.



Die als Nächstes angezeigte Seite Upgrade enthält Fortschrittsanzeigen, anhand derer Sie die Datenmigration von XenMobile 9.0 beobachten können.



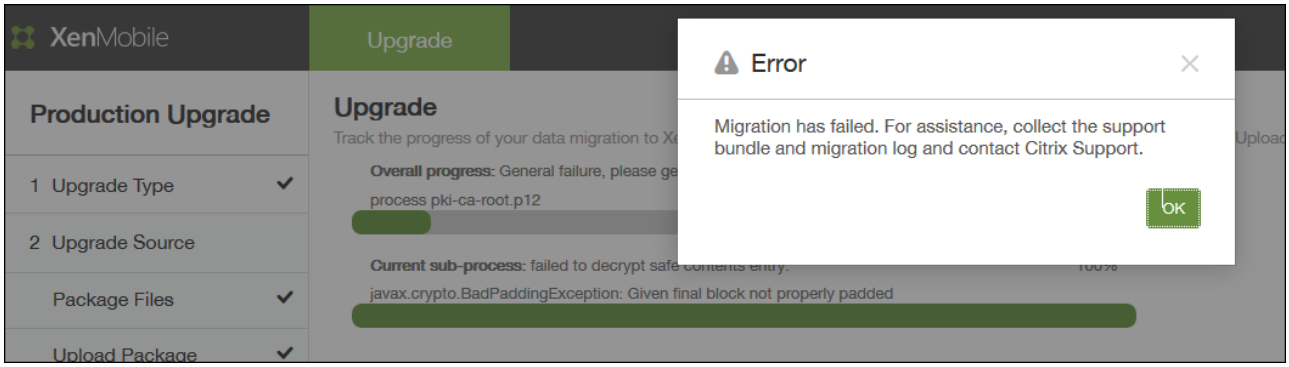


Wenn Sie nicht alle erforderlichen Device Manager-Dateien in die ZIP-Datei kopiert haben, werden die fehlenden Dateien im Upgrade Tool angezeigt. Die Ausführung des Tools wird fortgesetzt, wenn Sie erforderlichen Dateien hinzugefügt haben.

Wenn Sie ein Problem nicht beheben können, wird eine Fehlermeldung angezeigt, in der Sie zum Erstellen eines XenMobile-Supportpakets, zum Sammeln des Migrationsprotokolls und zum Verständigen des technischen Supports von Citrix aufgefordert werden.

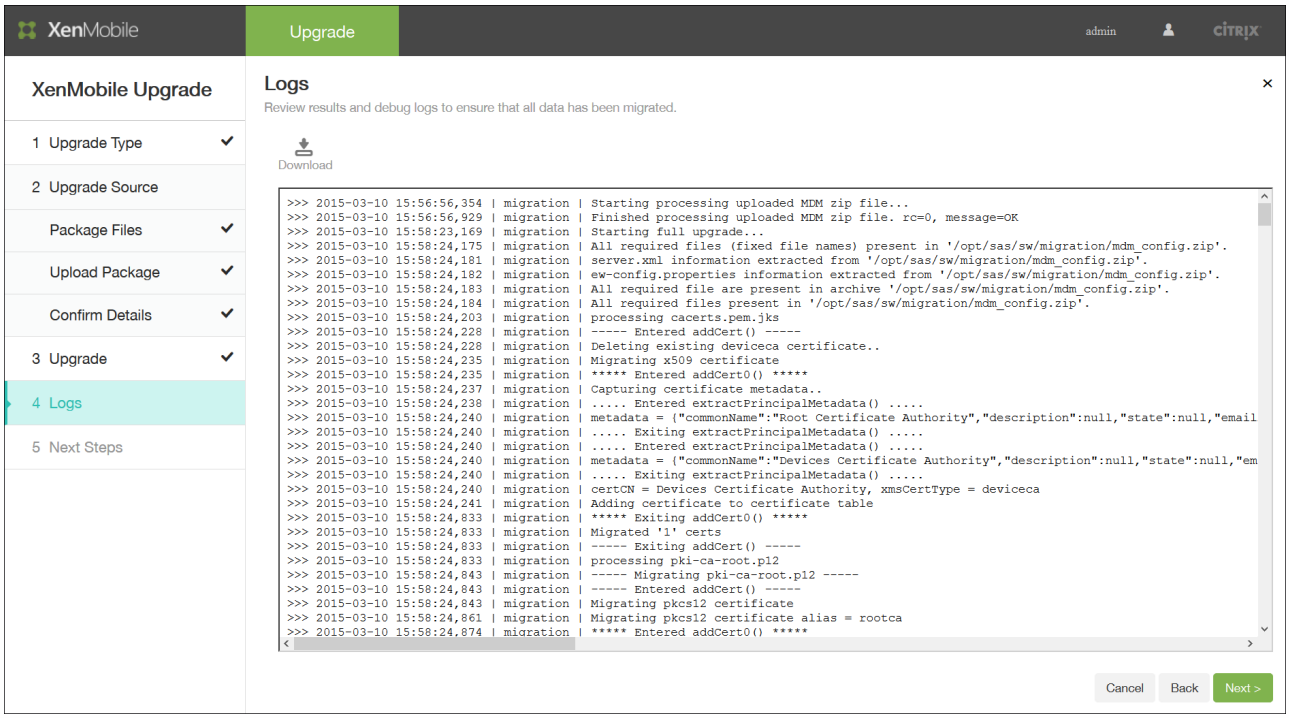
Hinweis:

- Wenn Migration fehlschlägt, müssen Sie eine neue XenMobile 10-Instanz importieren und die Migration dann neu starten.
- Wenn die Migration abgeschlossen ist (erfolgreich oder mit Fehlern), können Sie keine Informationen mehr mit der Schaltfläche Back korrigieren. Sie müssen dann eine neue XenMobile 10-Instanz importieren und die Migration neu starten.



Anzeigen der Upgrade Tool-Protokolle

Nach dem Upgrade auf XenMobile 10 können Sie die Protokolldatei migration.log des XenMobile Upgrade Tools herunterladen und prüfen (siehe folgende Abbildung). Citrix empfiehlt, dass Sie anhand der Datei prüfen, ob Richtlinien, Einstellungen, Benutzerdaten usw. einwandfrei nach XenMobile 10 migriert wurden.



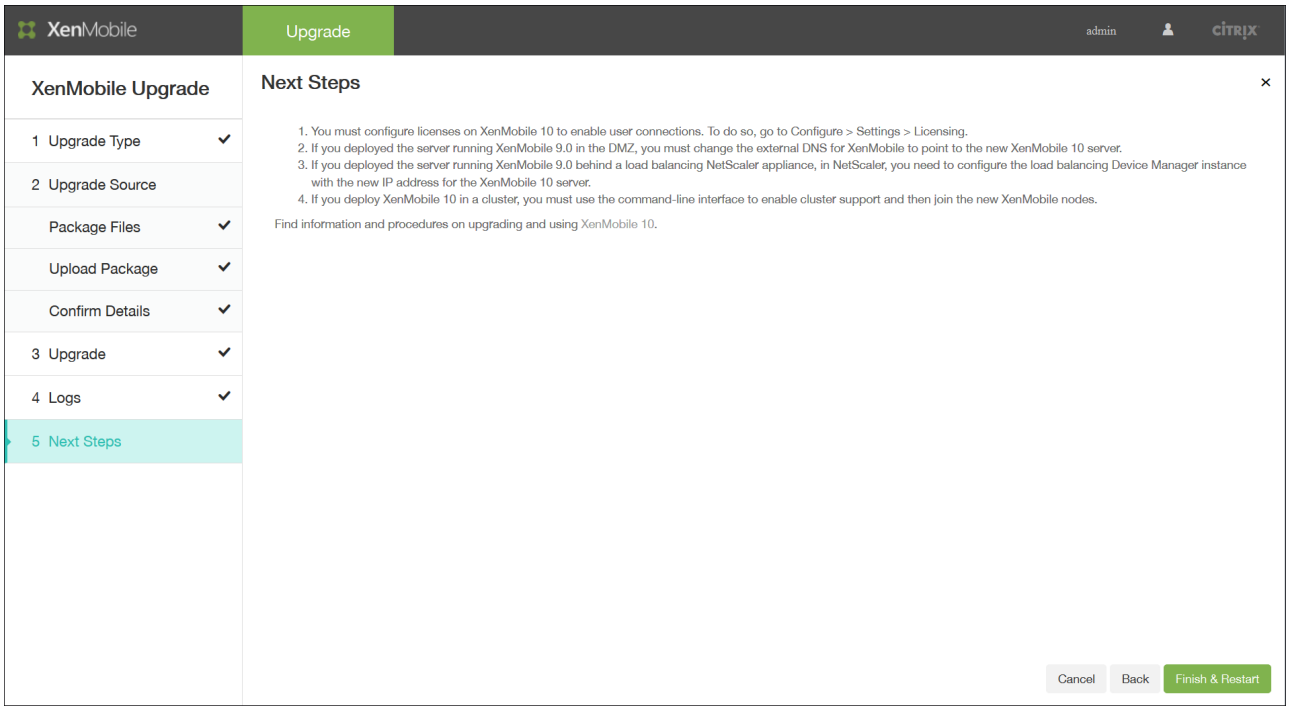
Klicken Sie nach dem Download und Prüfen des Migrationsprotokolls auf Next um mit den nächsten Schritten fortzufahren. Weitere Informationen finden Sie unter Voraussetzungen für das Upgrade Tool.

Nachbereitung eines Upgrades

May 05, 2016

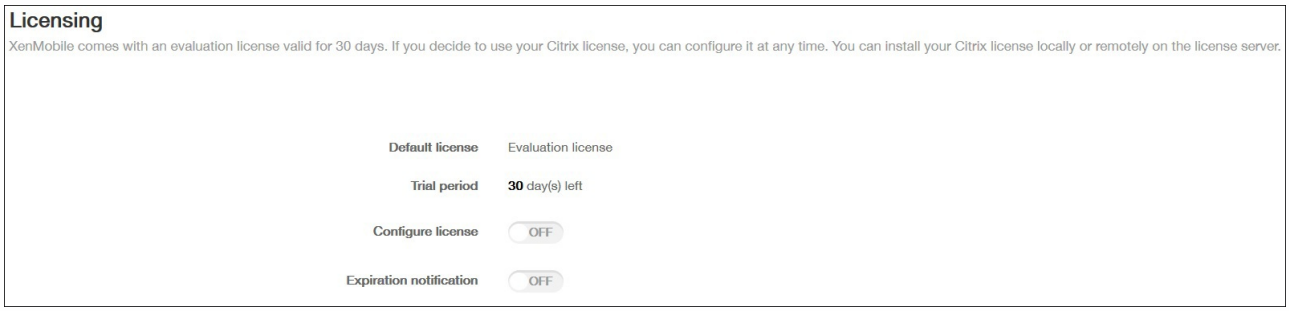
Nachdem Sie ein Upgrade durchgeführt haben müssen Sie die folgenden Nachbereitungsschritte ausführen, von denen einige auch auf der letzten Seite des Upgrade Tools angegeben sind. Wenn Sie auf Finish & Restart klicken, wird der Server neu gestartet.

Hinweis: Melden Sie sich bei der XenMobile unter https://: 4443 mit Ihren Administratoranmeldeinformationen ein.



Lizenzierung

XenMobile 10 unterstützt nur die Citrix V6-Lizenzierung. Legen Sie die lokale oder Remote-Lizenzkonfiguration in der XenMobile-Konsole wie in der folgenden Abbildung dargestellt fest und laden Sie die Lizenzdatei von Citrix Licensing herunter. Weitere Informationen finden Sie unter Lizenzierung von XenMobile.



Sie müssen Lizenzen in XenMobile 10 konfigurieren, damit Benutzer eine Verbindung herstellen können. Navigieren Sie hierfür zu **Configure** > **Settings** > **Licensing**. Bei einem eigenständigen Server mit XenMobile 10 können Sie die Lizenz für die ausschließliche Mobilgeräteverwaltung in die XenMobile-Konsole hochladen.

DNS

Hinweis: Dieser Nachbereitungsschritt ist für Produktionsupgrades erforderlich. Wenn Sie den Server mit XenMobile 9.0 in der DMZ bereitgestellt haben, müssen Sie das externe DNS für XenMobile dahingehend ändern, dass es auf den neuen XenMobile 10-Server verweist.

IP-Adresse von NetScaler für den Lastausgleich

Hinweis: Dieser Nachbereitungsschritt ist für Produktionsupgrades erforderlich. Wenn Sie den Server mit XenMobile 9.0 hinter einem NetScaler-Gerät für den Lastausgleich bereitgestellt haben, müssen Sie die Lastausgleich-Device Manager-Instanz in NetScaler mit der neuen IP-Adresse des XenMobile 10-Servers konfigurieren.

Clustering

Wenn Sie XenMobile 10 in einem Cluster bereitstellen, müssen die Clusterunterstützung mit der Befehlszeilenoberfläche aktivieren und die neuen XenMobile-Knoten anfügen. Sie können die IP-Adressen der XenMobile 9.0-Knoten wiederverwenden, indem Sie die neue XenMobile 10-Instanz mit denselben IP-Adressen konfigurieren und sie dann dem Knoten "Admin/Oldest" anfügen.

Aktualisieren nicht migrierter Informationen

Aktualisieren Sie die folgenden Elemente nach Bedarf:

- Automatisierte Aktionen
- Servergruppenrichtlinien und zugeordnete Bereitstellungen
- MSP-Gruppe
- Benutzerdefinierte Active Directory-Attribute
- XenMobile-Grenzwert für Sperrung
- RBAC-Rollen
- Protokolleinstellungen
- URLs ohne HTTP oder HTTPS
- Jegliche in der Datei migration.log aufgeführten Konfigurations- oder Benutzerdaten

Unterstützung für benannte SQL-Instanzen

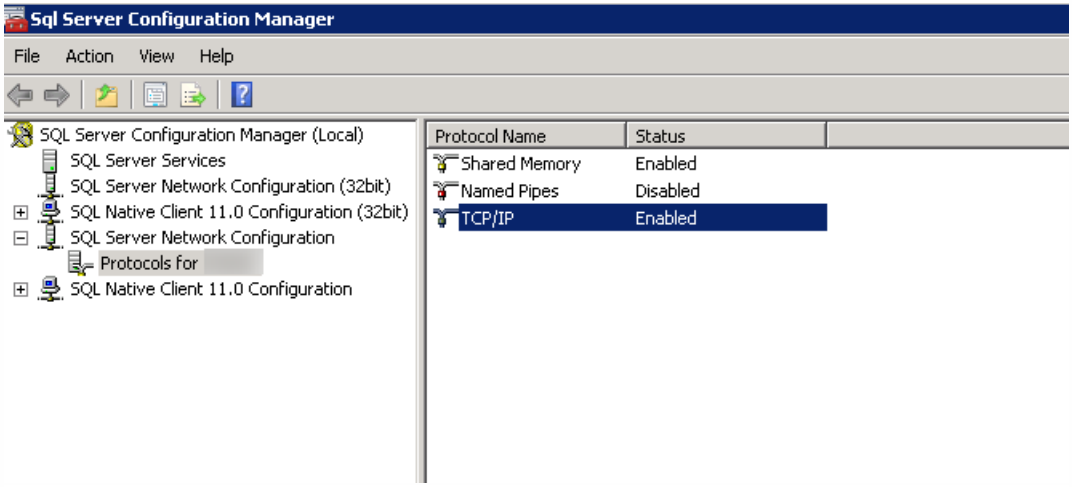
May 05, 2016

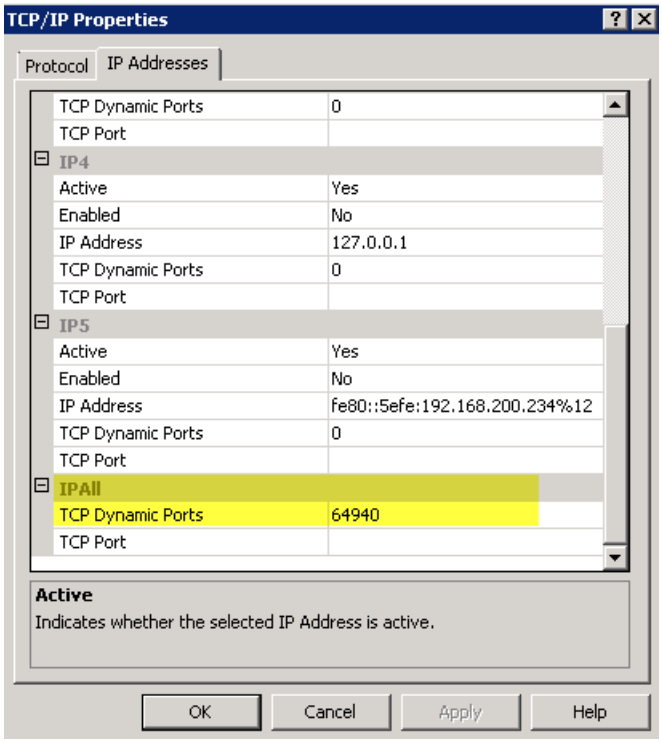
Mit dem Upgrade Tool können Sie Upgrades von XenMobile 9 auf XenMobile 10 und von XenMobile 9 auf XenMobile 10.1 durchführen. Wenn Ihr XenMobile 9-Setup auf benannten SQL-Instanzen basiert, müssen Sie bestimmten Schritten folgen. Wenn Ihre XenMobile 9-Umgebung die folgenden Voraussetzungen erfüllt, folgen Sie den Anleitungen in diesem Artikel, um das Upgrade durchzuführen.

- Setup von XenMobile 9 MDM Edition oder Enterprise Edition mit einer externen SQL Server-Datenbank.
- Die SQL Server-Datenbank wird auf einer nicht standardmäßigen benannten Instanz ausgeführt.
- Die benannte SQL Server-Instanz hört einen statischen oder dynamischen TCP-Port ab. Sie können diese Voraussetzung bestätigen, indem Sie die IP-Adressen des TCP/IP-Protokolls der benannten Instanz überprüfen (siehe Abbildungen unten).

Hinweis

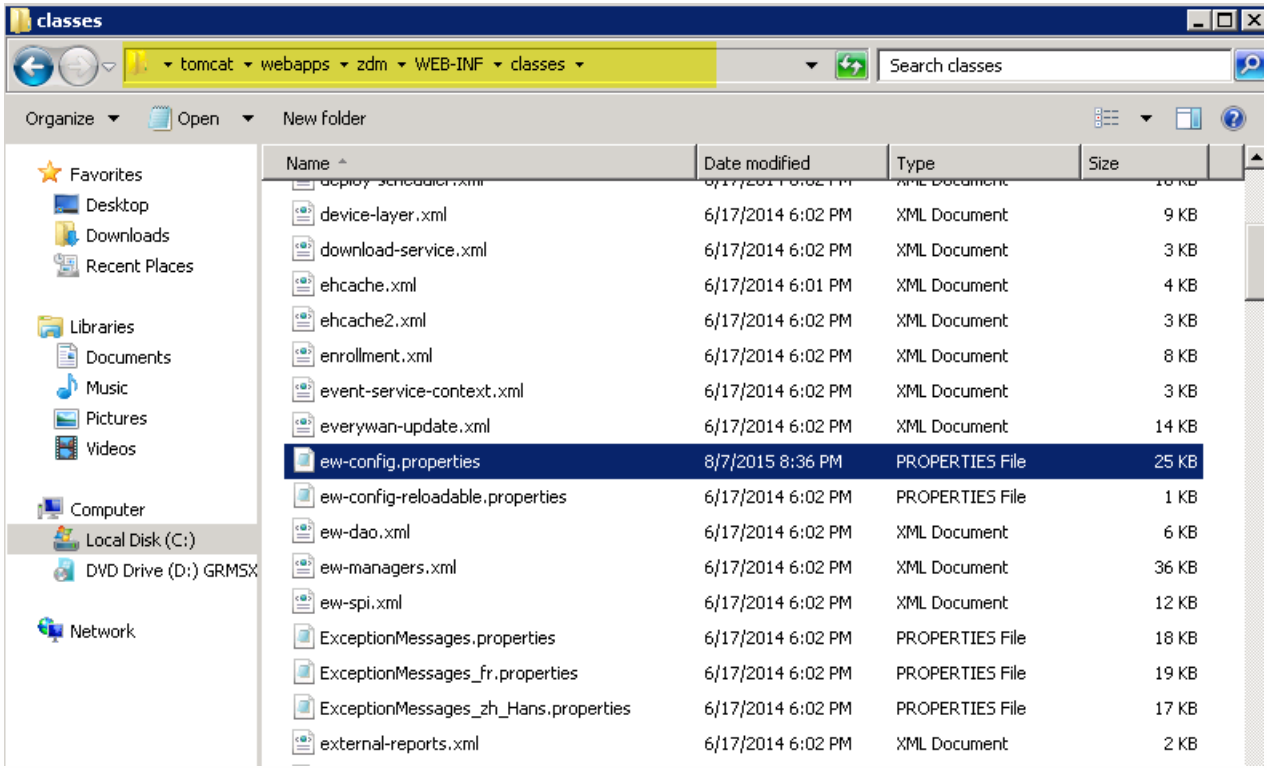
Citrix empfiehlt, die SQL Server-Datenbankinstanz immer auf einem statischen Port auszuführen, weil der XenMobile-Server kontinuierlichen Zugriff auf die Datenbank benötigt. Diese Verbindung erfolgt im Allgemeinen durch eine Firewall. Sie müssen daher den entsprechenden Port in der Firewall öffnen und deswegen muss die Datenbankinstanz auf einem statischen Port ausgeführt werden.





Schritte zum Upgrade von XenMobile mit einer benannten SQL Server-Instanz

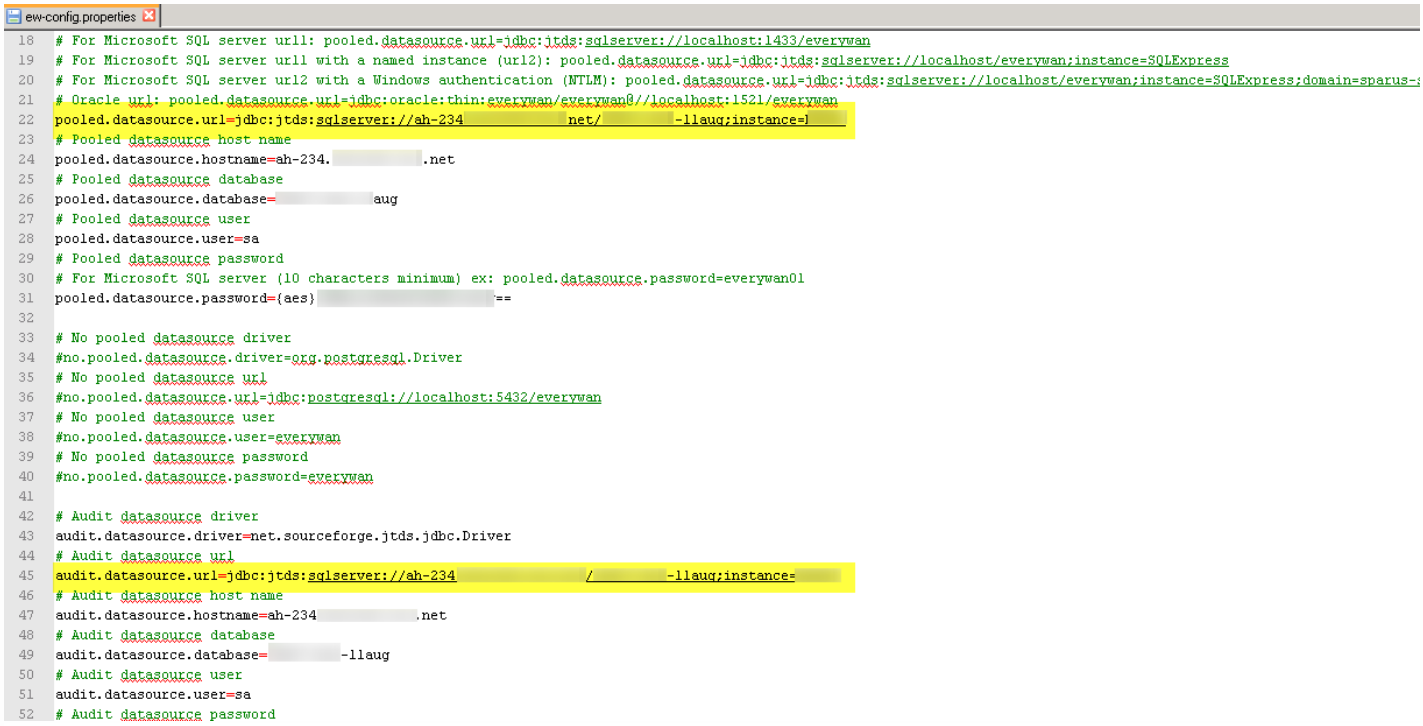
1. Navigieren Sie zum Installationsverzeichnis des Device Managers und öffnen Sie die Datei ew-config.properties. Diese Datei ist in tomcat/webapps/zdm/WEB-INF/classes.



2. Suchen Sie in der Datei ew-config.properties im DATASOURCE-Konfigurationsbereich die folgenden URLs:

pooled.datasource.url= jdbc:jtds:sqlserver:///;instance=

audit.datasource.url= jdbc:jtds:sqlserver:///;instance=



3. Entfernen Sie den Instanznamen aus den aufgeführten URLs und fügen Sie den Port sowie den FQDN des SQL Servers hinzu. In diesem Fall ist 64940 der erforderliche Port.

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

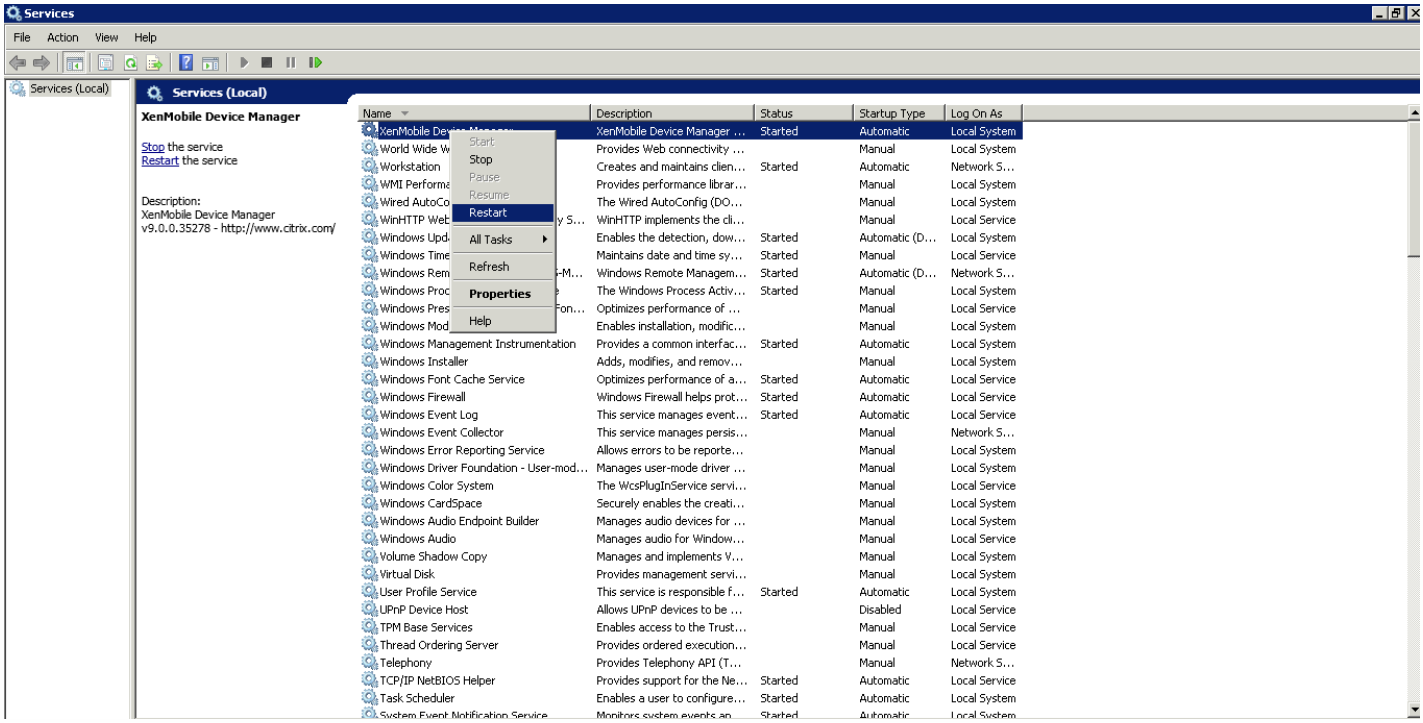
audit.datasource.url=jdbc:jtds:sqlserver:// :64940/

> ## Hinweis
>
> Citrix empfiehlt, eine Datensicherung durchzuführen, eine Kopie zu erstellen oder genau aufzuschreiben, welche Änderungen Sie in der Datei ew-config.properties vornehmen. Diese Informationen sind nützlich, falls ein Fehler bei der Migration auftritt.

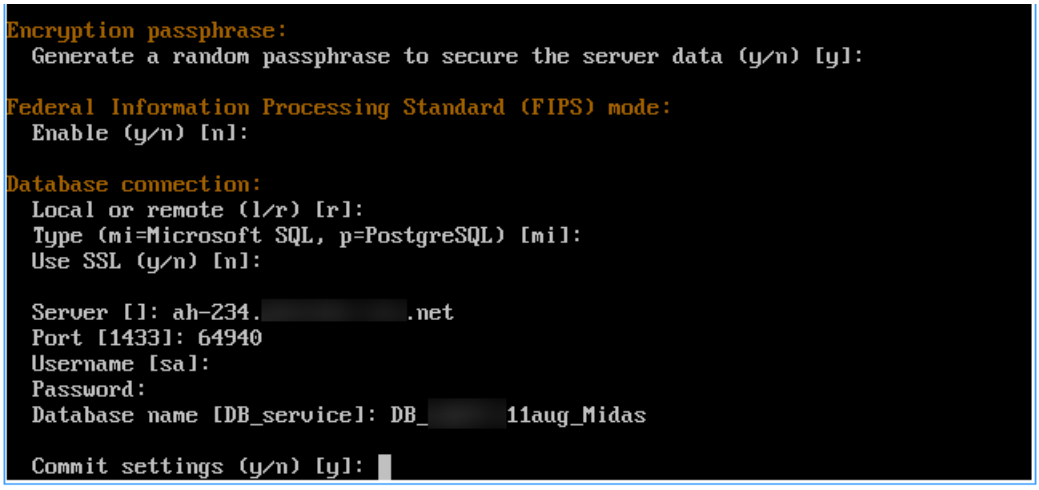
ew-config.properties

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

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

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

4. Starten Sie den Device Manager-Dienst neu. Aktualisieren Sie die Geräteverbindungen, wenn die Device Manager-Instanz wieder angezeigt wird.



5. Ermitteln Sie, ob der XenMobile 10-Server ebenfalls benannte SQL-Instanzen verwendet. Wenn dies der Fall ist, identifizieren Sie den Port, auf dem die benannte Instanz ausgeführt wird. Wenn es sich um einen dynamischen Port handelt, empfiehlt Citrix, dass Sie den Port in einen statischen Port umwandeln. Konfigurieren Sie dann den statischen Port auf dem neuen XenMobile-Server als Teil des Datenbanksetups.



6. Folgen Sie den Anleitungen in den unten genannten Artikeln für weitere Upgrades Ihrer XenMobile-Umgebung:

- Für Upgrades von XenMobile 9.0 App Edition oder Enterprise Edition auf XenMobile 10.1 verwenden Sie das XenMobile Server App Edition und Enterprise Edition Upgrade Tool. Details finden Sie unter Aktivieren und Ausführen des XenMobile 10.1 MDM Upgrade Tools
- Informationen zum Upgrade von XenMobile 9.0 MDM Edition auf XenMobile 10.1 finden Sie unter XenMobile 10 MDM Upgrade Tool.

Upgrade von XenMobile über die XenMobile-Konsole

May 05, 2016

Sobald neue Versionen der XenMobile-Software verfügbar sind, können Sie ein Upgrade durchführen. Sie verwenden die Seite "Release Management" der XenMobile-Konsole zum Installieren neuer XenMobile-Versionen, Service Packs und Systempatches.

Hinweis: Sobald eine neue Version oder ein wichtiges Update verfügbar wird, wird sie bzw. es auf Citrix.com veröffentlicht und eine Meldung an die als Kontaktperson verzeichnete Person bei den Kunden gesendet.

Wichtig:

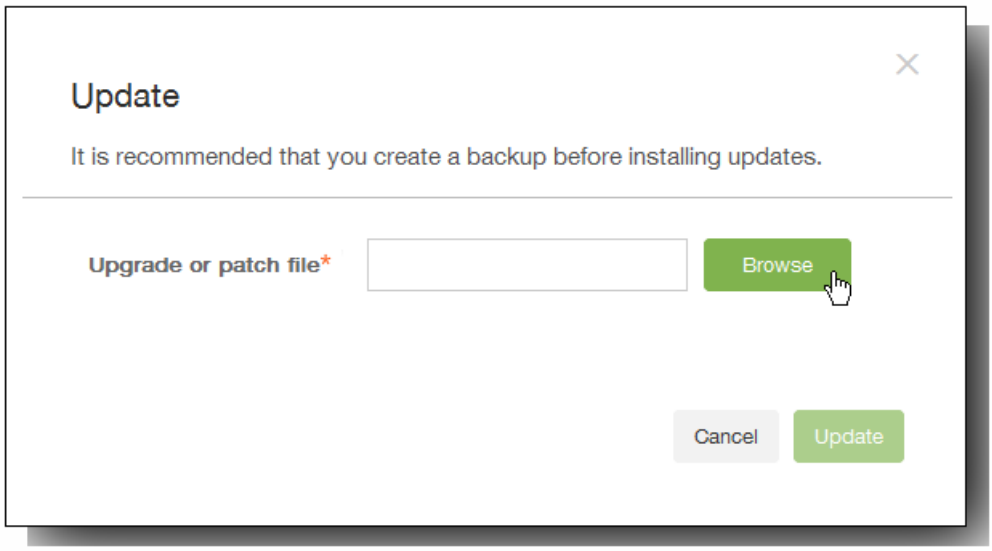
- Vor der Installation eines XenMobile-Updates verwenden Sie die Funktionen der virtuellen Maschine (VM) zum Erstellen eines Systemsnapshots.
- Sichern Sie die Konfigurationsdatenbank des Systems.
- Wenn Sie auf dem MDM Server Samsung KNOX Attestation aktiviert haben und ein Upgrade auf XenMobile 10.0 planen, müssen Sie die neuen benutzerdefinierten KNOX Attestation-Domänen hinzufügen, bevor Sie das Upgrade durchführen. Weitere Informationen zum Aktivieren von Samsung KNOX Attestation finden Sie unter Samsung KNOX. Die neuen Attestation-Domänen sind folgende:
  - Region China: china-attest-api.secb2b.com.cn
  - Europäische Region: eu-attest-api.secb2b.com
  - Region USA: us-attest-api.secb2b.com

So aktualisieren Sie XenMobile

1. Melden Sie sich mit Ihrem Konto auf der Citrix Website an und laden Sie die XenMobile-Upgradedatei (.bin) an einen geeigneten Speicherort herunter.
2. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Certificates.

   Die Seite Release Management wird angezeigt. Sie enthält die Version der aktuell installierten Software sowie eine Liste aller Updates, Patches und Upgrades, die Sie bereits hochgeladen haben.

3. Klicken Sie unter Updates auf Update. Das Dialogfeld Update wird angezeigt.



4. Klicken Sie auf Browse, navigieren Sie zu dem Speicherort, an dem Sie die von Citrix.com heruntergeladene XenMobile-Upgradedatei gespeichert haben, und wählen Sie dann die Datei aus.
5. Klicken Sie auf Update und starten Sie XenMobile neu, wenn Sie dazu aufgefordert werden.
   Hinweis: Möglicherweise muss XenMobile nicht neu gestartet werden, nachdem das Update installiert wurde. In diesem Fall zeigt eine Meldung an, dass das Update erfolgreich installiert wurde. Wenn ein Neustart erforderlich ist, müssen Sie die Befehlszeile verwenden.
   Wichtig: Wenn das System im Clustermodus konfiguriert ist, führen Sie die folgenden Schritte aus, um jeden Knoten zu aktualisieren:
   - Fahren Sie alle Knoten bis auf einen herunter.
   - Aktualisieren Sie den Knoten.
   - Vergewissern Sie sich, dass der Dienst ausgeführt wird, bevor Sie den nächsten Knoten aktualisieren.

   Falls das Update nicht erfolgreich durchgeführt werden kann, wird eine Fehlermeldung zu dem Problem angezeigt. Das System wird in den Zustand vor dem Update zurückgesetzt.

Konfigurieren von Clustering für XenMobile 10

Oct 13, 2016

XenMobile 10 integriert XenMobile 9 Device Manager und App Controller. In früheren Versionen von XenMobile konfigurieren Sie Device Manager als Cluster und App Controller als ein hochverfügbares Paar. Hohe Verfügbarkeit triff nicht auf XenMobile 10 zu. Um Clustering für XenMobile 10 zu konfigurieren, müssen Sie daher die folgenden beiden virtuellen IP-Adressen für den Lastausgleich in NetScaler konfigurieren.

- **Mobile device management (MDM) load balancing virtual IP address**: Eine virtuelle IP-Adresse für den MDM-Lastausgleich ist für die Kommunikation mit den XenMobile-Knoten erforderlich, die in einem Cluster konfiguriert sind. Dieser Lastausgleich ist im SSL-Brückenmodus.
- **Mobile app management (MAM) load balancing virtual IP address**: Virtuelle IP-Adressen für den MAM-Lastausgleich sind erforderlich für die Kommunikation von NetScaler Gateway mit XenMobile-Knoten, die in einem Cluster konfiguriert sind. In XenMobile 10 wird standardmäßig der gesamte Netzwerkverkehr von NetScaler Gateway an die virtuellen IP-Adressen für den Lastausgleich auf Port 8443 geleitet.

In diesem Artikel wird erläutert, wie Sie eine neue XenMobile-VM (virtuelle Maschine) erstellen und die neue VM mit einer vorhandenen VM zusammenführen, um dadurch ein Clustersetup zu erstellen.

Voraussetzungen

- Sie haben den erforderlichen XenMobile-Knoten vollständig konfiguriert.
- Sie haben zwei freie IP-Adressen, die Sie als virtuelle IP-Adressen für den Lastausgleich verwenden können.
- Serverzertifikate
- Sie haben eine freie IP für die virtuelle IP-Adresse von NetScaler.

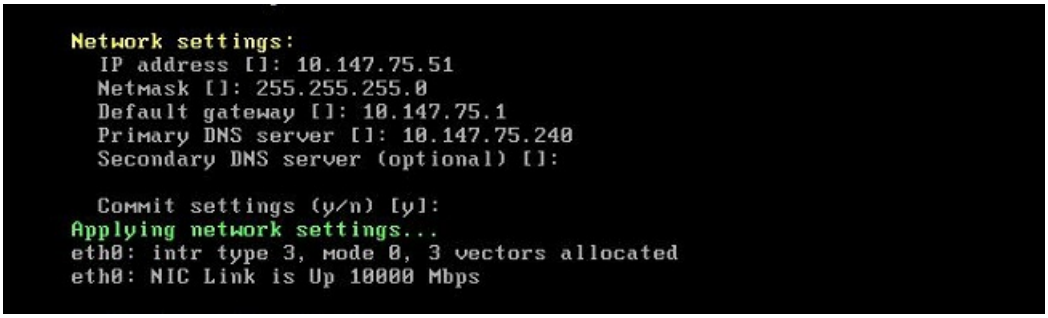
Referenzarchitekturdiagramme für XenMobile 10.x in Clusterkonfigurationen finden Sie unter Architektur im Überblick.

Installieren der XenMobile-Clusterknoten

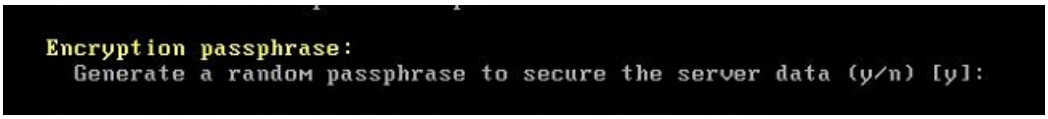
Basierend auf der Anzahl der erforderlichen Knoten erstellen Sie neue XenMobile-VMs. Sie verweisen die neuen VMs auf die gleiche Datenbank und die gleichen PKI-Zertifikatkennwörter.

1. Öffnen Sie die Befehlszeilenkonsole der neuen VM und geben Sie das neue Kennwort für das Administratorkonto ein.

2. Geben Sie die Details der Netzwerkkonfiguration wie in der folgenden Abbildung dargestellt an.

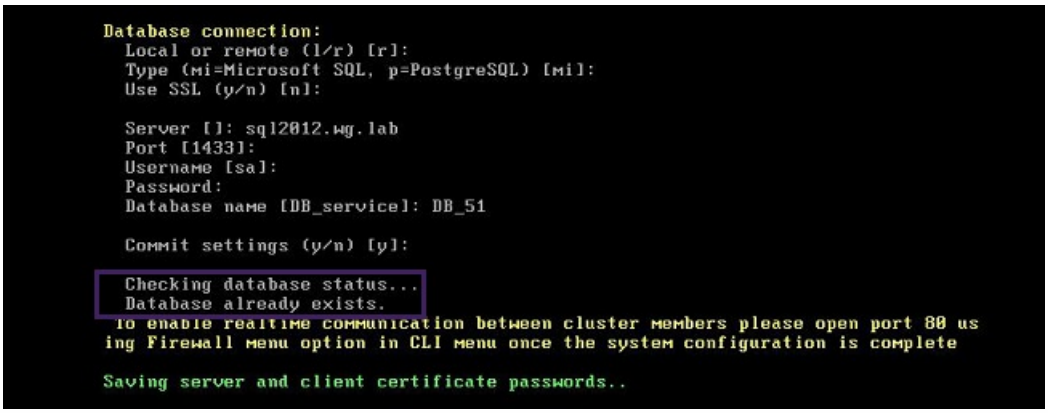


3. Wenn Sie das Standardkennwort für den Schutz von Daten verwenden möchten, geben Sie **y** ein. Sonst geben Sie **n** ein und geben Sie ein neues Kennwort an. **Hinweis:** Wenn Sie nicht dem Cluster manuell weitere Knoten hinzuzufügen und die anfängliche XenMobile-VM nicht klonen wollen, müssen Sie hier manuell ein neues Kennwort eingeben. Für die sequenziellen Knoten ist der gleiche Passcode erforderlich. Wenn Sie nicht die gleichen Passcodes verwenden, schlägt der Prozess beim Hinzufügen des zweiten Knotens fehl. In dem Fall können Sie die VM klonen, aber das Angeben eines neuen Kennworts verhindert den Fehler.

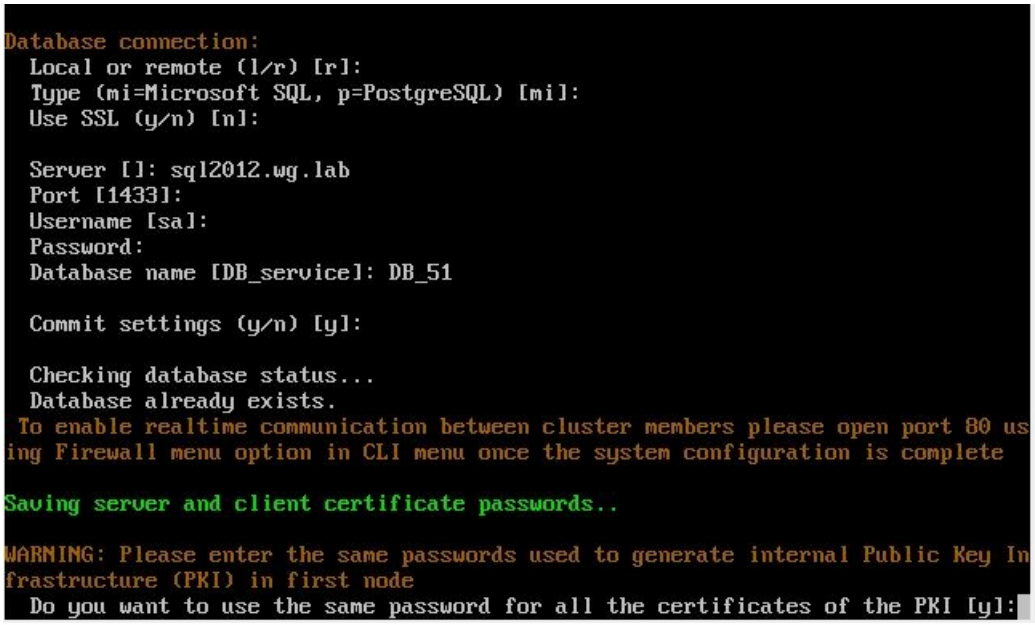


4. Wenn Sie FIPS verwenden möchten, geben Sie **y** oder **n** an.

5. Konfigurieren Sie die Datenbank so, dass sie auf die gleiche Datenbank verweist, wie die vorherige vollständig konfigurierte VM. Sie sehen eine Meldung, dass die Datenbank bereits vorhanden ist.

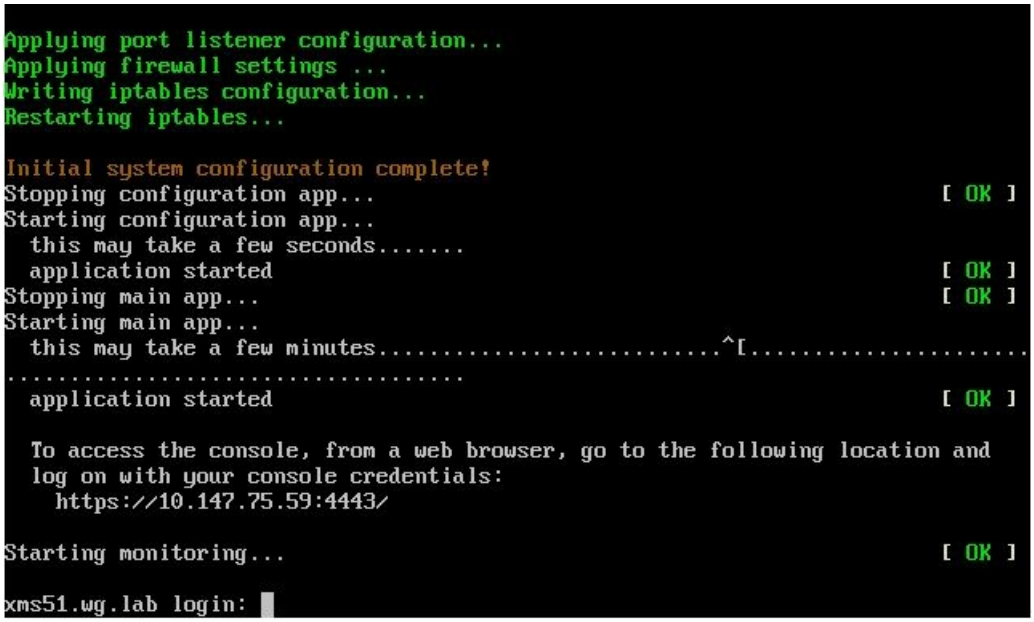


6. Geben Sie die gleichen Kennwörter für die Zertifikate an, wie für die erste VM.



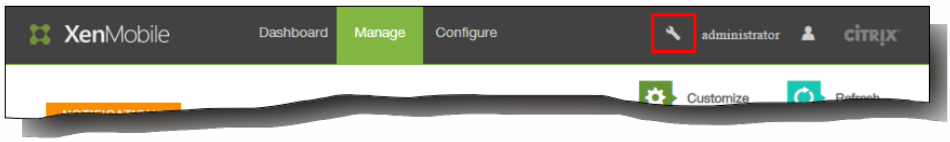
Nachdem Sie das Kennwort eingegeben haben, wird die anfängliche Konfiguration auf dem zweiten Knoten abgeschlossen.

7. Der Server wird neu gestartet nachdem die Konfiguration abgeschlossen ist und Sie sehen das Anmeldedialogfeld.

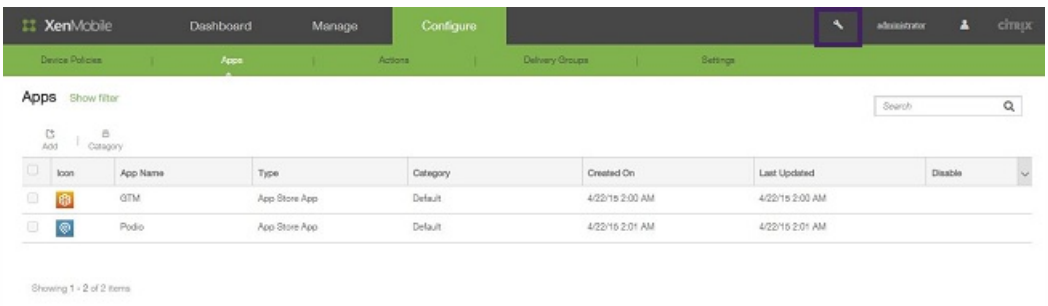


Hinweis: Das Anmeldedialogfeld ist das gleiche wie für die erste VM. Die Übereinstimmung zeigt Ihnen, dass beide VMs den gleichen Datenbankserver verwenden.

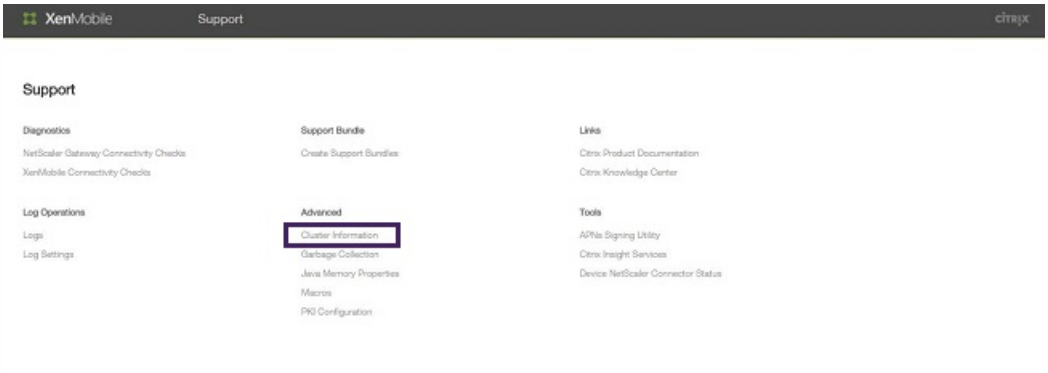
8. Verwenden Sie den vollqualifizierten Domänennamen (FQDN) von XenMobile, um die XenMobile-Konsole in einem Webbrowser zu öffnen.
9. Klicken Sie im Dashboard auf das Toolsymbol oben rechts auf dem Bildschirm.



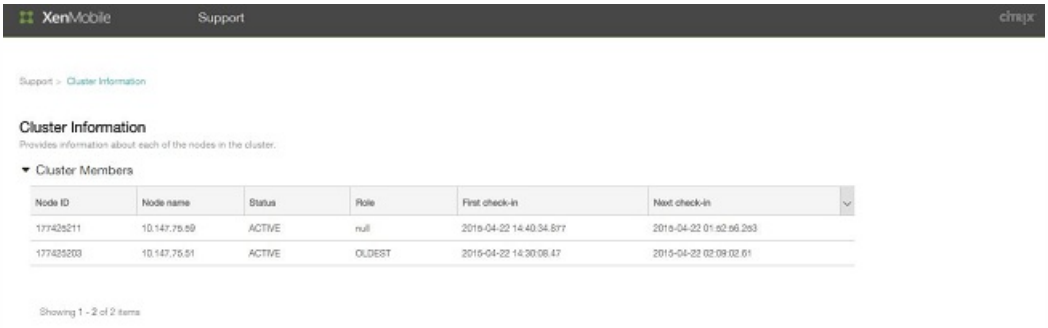
Die Seite "Support" wird geöffnet.



10. Klicken sie unter Advanced auf Cluster Information.



Alle Informationen über den Cluster werden angezeigt, einschließlich Informationen zu Clustermitgliedern, Geräteverbindungen, Aufgaben usw.



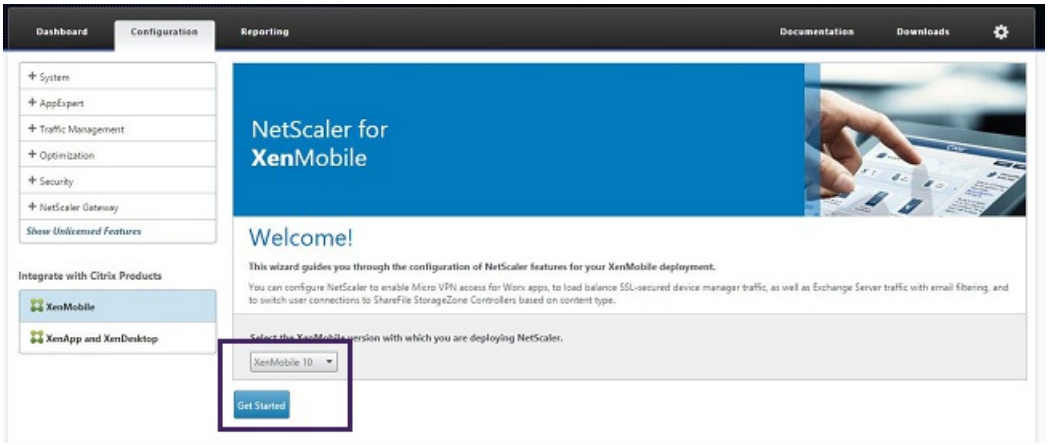
Der neue Knoten gehört nun zu dem Cluster. Sie können auf die gleiche Weise noch weitere Knoten hinzufügen.

So konfigurieren Sie den Lastausgleich für den XenMobile-Cluster in NetScaler

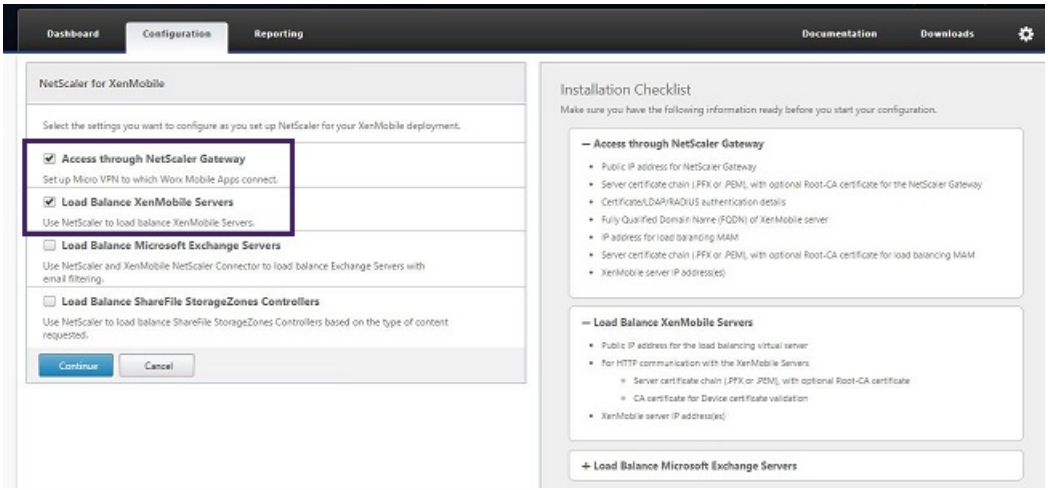
Nachdem Sie die erforderlichen Knoten als Mitglieder des XenMobile-Clusters hinzugefügt haben, müssen Sie für die Knoten den Lastausgleich durchführen, um auf die Cluster zuzugreifen. Der Lastausgleich geschieht, indem Sie den XenMobile-Assistent in NetScaler 10.5.x ausführen. Folgen Sie diesen Schritten, um den XenMobile-Lastausgleich über den Assistenten einzurichten.

1. Melden Sie sich an NetScaler an.

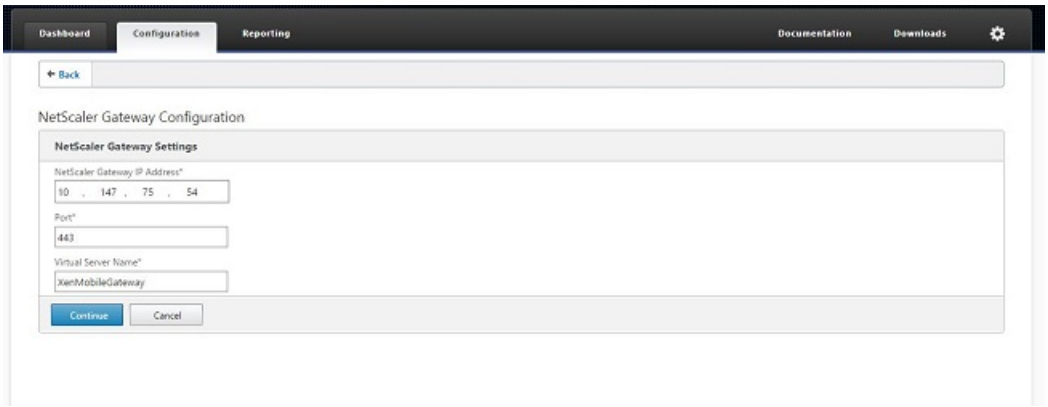
2. Klicken Sie auf der Registerkarte Configuration auf XenMobile und dann auf Get Started.



3. Wählen Sie die Kontrollkästchen Access through NetScaler Gateway und Load Balance XenMobile Servers. Klicken Sie dann auf Continue.

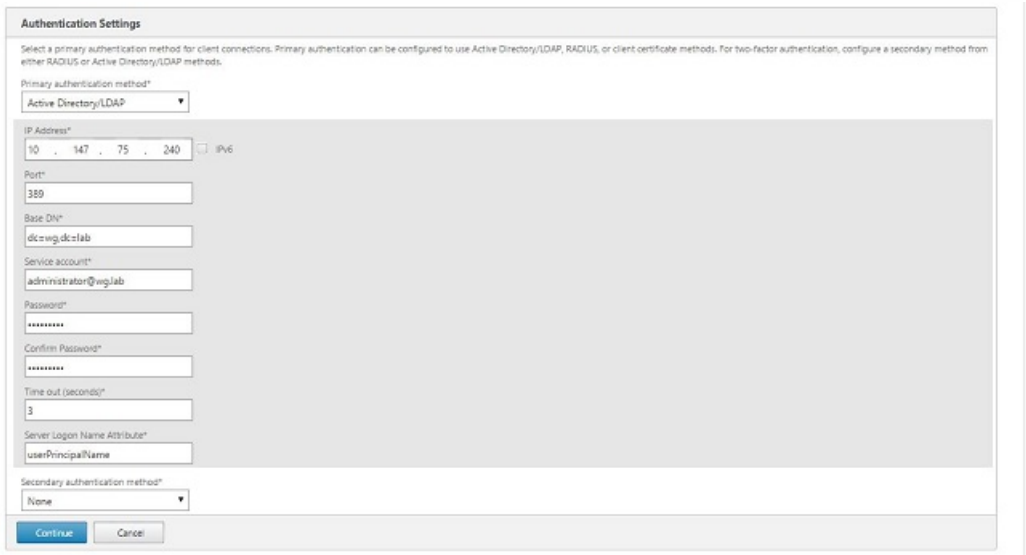


4. Geben Sie die IP-Adresse für NetScaler Gateway ein und klicken Sie auf Continue.



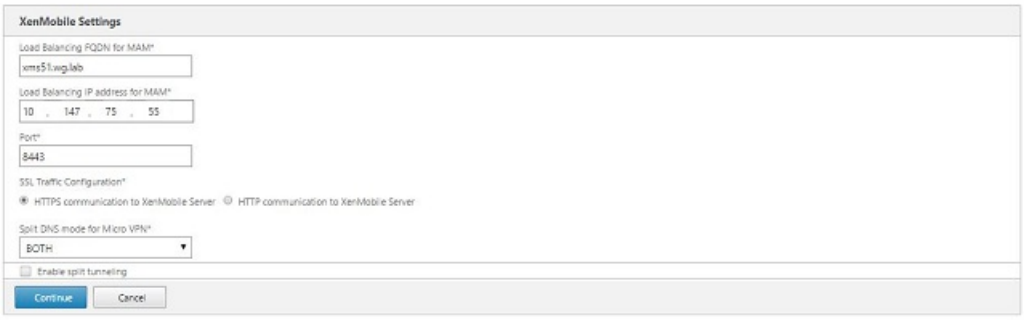
5. Binden Sie mit einer der folgenden Methoden das Serverzertifikat an die virtuelle IP-Adresse von NetScaler Gateway und klicken Sie dann auf Continue.
   - Wählen Sie unter Use existing certificate das Serverzertifikat aus der Liste.
   - Klicken Sie auf die Registerkarte Install Certificate, um ein neues Serverzertifikat hochzuladen.

6. Geben Sie die Authentifizierungsserverdetails an und klicken Sie dann auf Continue.



Hinweis: Stelle Sie sicher, dass Server Logon Name Attribute mit dem übereinstimmt, was Sie in der XenMobile-LDAP-Konfiguration angegeben haben.

7. Geben Sie unter XenMobile settings den vollqualifizierten Domänennamen für Load Balancing FQDN for MAM ein und klicken Sie dann auf Continue.



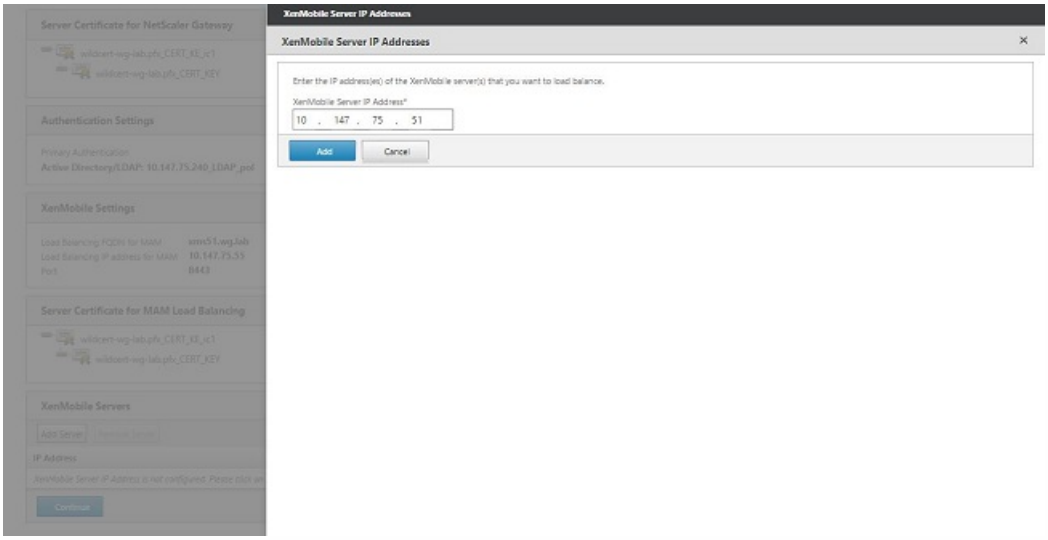
Hinweis: Stellen Sie sicher, dass der vollqualifizierte Domänenname (FQDN) der virtuellen IP-Adresse für den MAM-Lastausgleich und der FQDN von XenMobile gleich sind.

8. Wenn Sie den SSL-Brückenmodus (HTTPS) verwenden möchten, wählen Sie HTTPS communication to XenMobile Server. Wenn Sie aber SSL-Offload verwenden möchten, wählen Sie HTTP communication to XenMobile Server, wie in der voranstehenden Abbildung dargestellt. Für die Zwecke dieses Artikels nehmen wir SSL-Brückenmodus (HTTPS).

9. Binden Sie das Serverzertifikat für virtuelle IP-Adresse für den MAM-Lastausgleich und klicken Sie auf Continue.

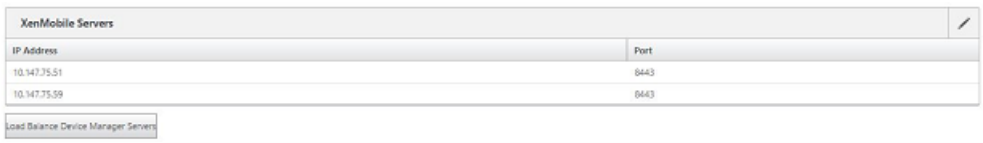
10. Klicken Sie unter XenMobile Servers auf Add Server, um die XenMobile-Knoten hinzuzufügen.

11. Geben Sie die IP-Adresse des XenMobile-Knotens ein und klicken Sie auf Add.

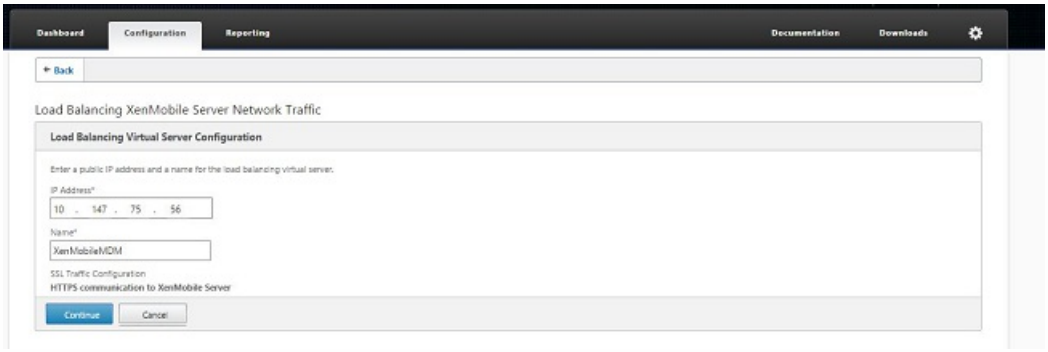


12. Wiederholen die Schritte 10 und 11, um weitere XenMobile-Knoten hinzuzufügen, die Teil des XenMobile-Clusters sind. Sie sehen dann alle XenMobile-Knoten, die Sie hinzugefügt haben. Klicken Sie auf Continue.

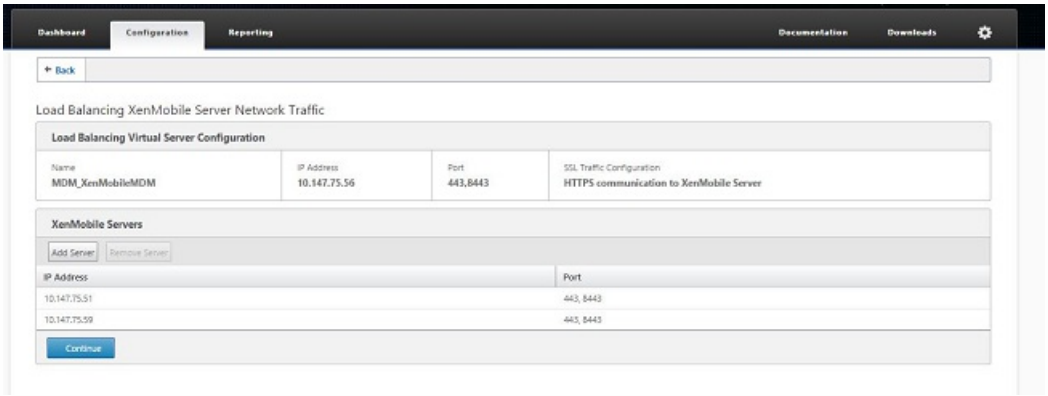
13. Klicken Sie auf Load Balance Device Manager Servers, um mit der Konfiguration des MDM-Lastausgleichs fortzufahren.



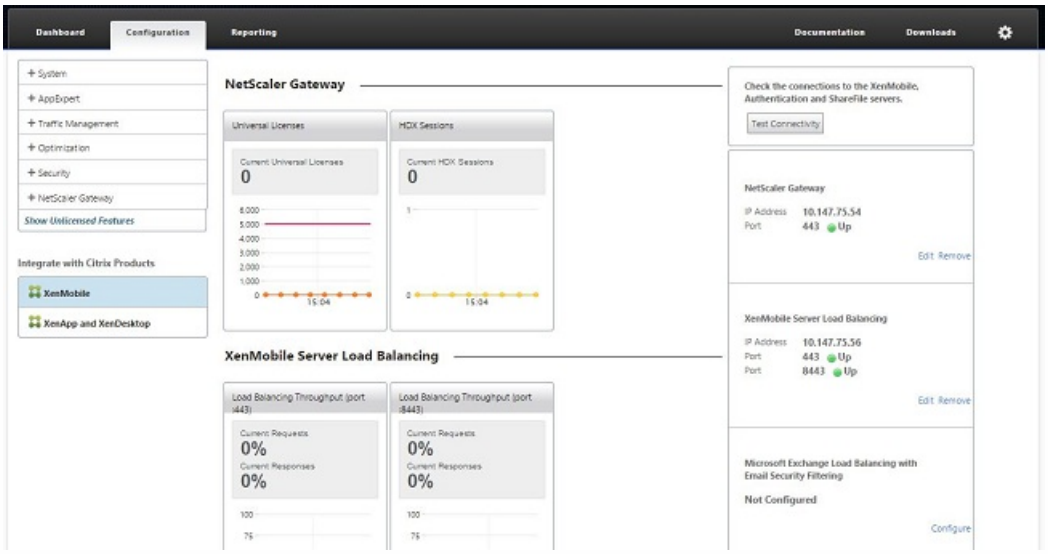
14. Geben Sie die IP-Adresse ein, die für den MDM-Lastausgleich verwendet werden soll und klicken Sie auf Continue.



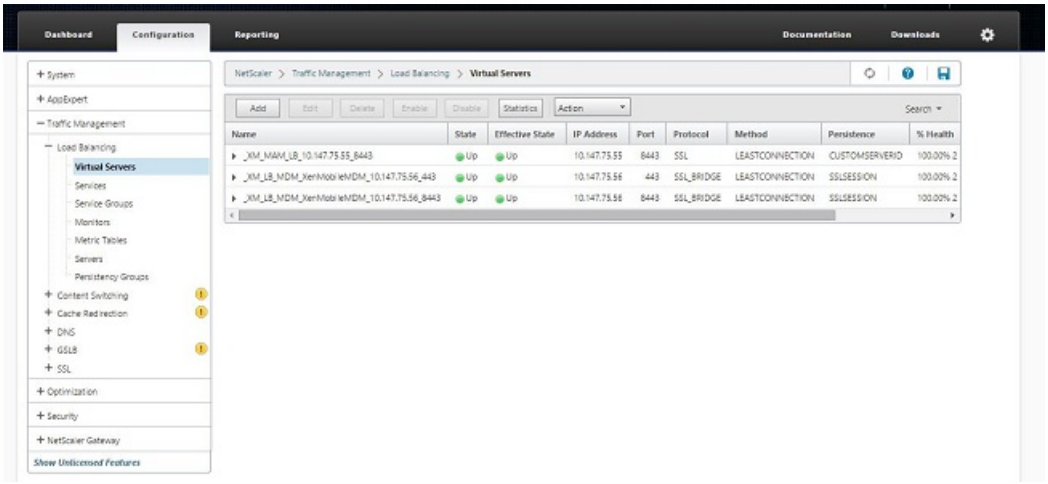
15. Sobald Sie die XenMobile-Knoten in der Liste sehen, klicken Sie auf Continue und dann auf click Done, um den Vorgang abzuschließen.



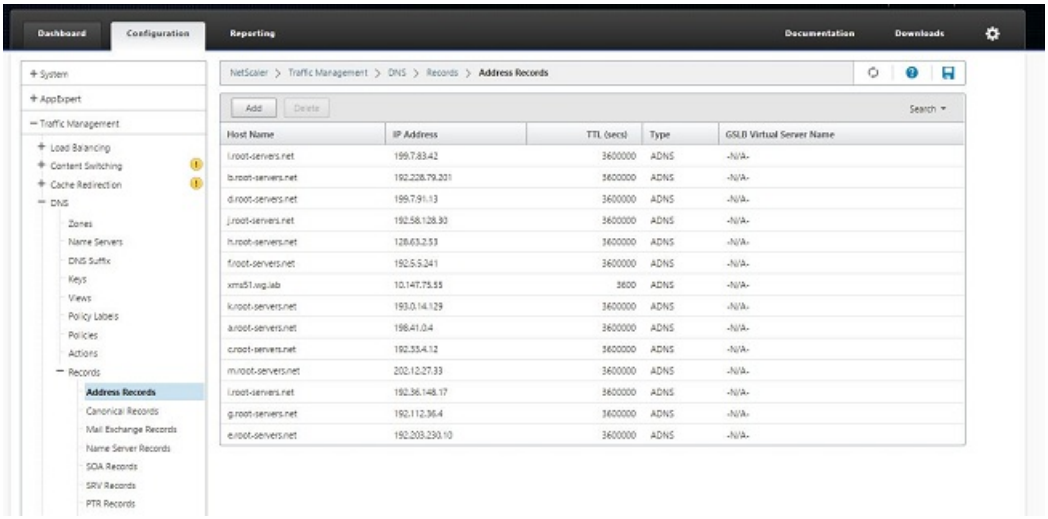
Sie sehen den Status der virtuellen IP-Adresse auf der Seite XenMobile.



16. Sie bestätigen, dass die virtuellen IP-Adressen funktionieren, indem Sie auf der Registerkarte Configuration zu Traffic Management > Load Balancing > Virtual Servers navigieren.



Sie sehen auch, dass der DNS-Eintrag in NetScaler auf die virtuelle IP-Adresse für den MAM-Lastausgleich verweist.

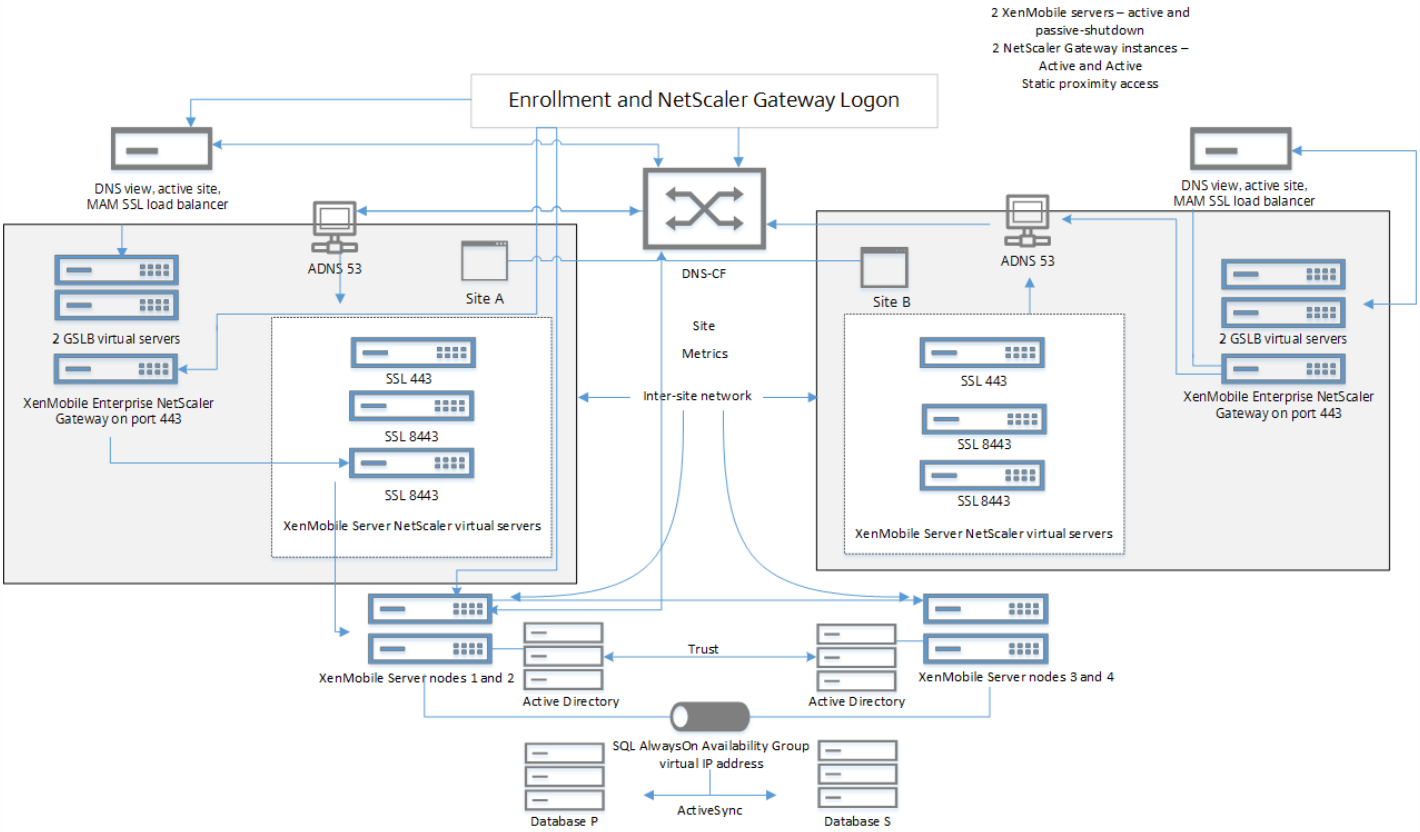


Disaster Recovery Guide für XenMobile

May 05, 2016

Diese Anleitung zur Notfallwiederherstellung ist als PDF verfügbar und erläutert die Konfiguration von XenMobile 10 Enterprise Edition für ein Notfallwiederherstellungsbereitstellung.

Die Architektur für diese Bereitstellung ist im folgenden Diagramm dargestellt und ist ebenfalls als PDF verfügbar.



PDF XenMobile Disaster Recovery Guide

PDF XenMobile Disaster Recovery – Architekturdiagramm

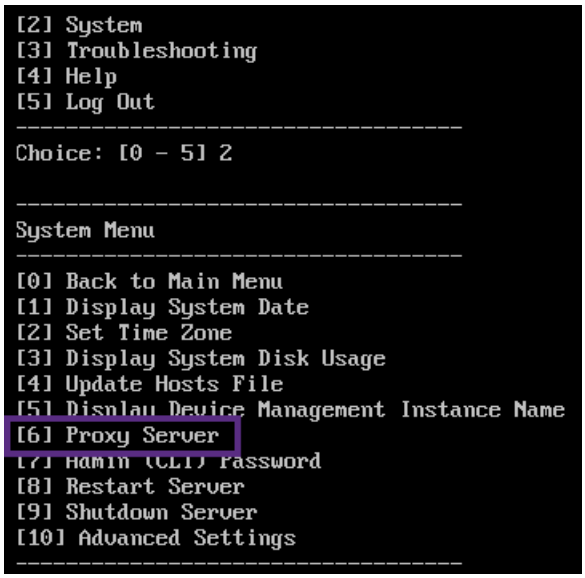
Aktivieren von Proxyservern in XenMobile

May 05, 2016

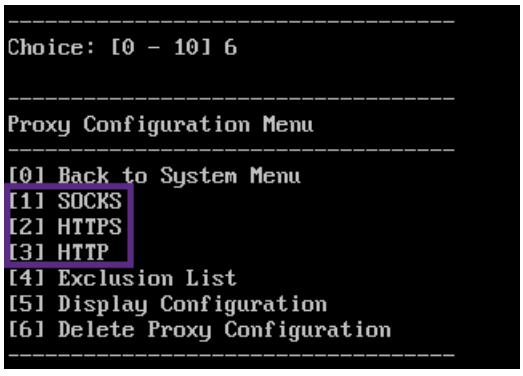
Zum Steuern von ausgehendem Internetverkehr können Sie in XenMobile einen Proxyserver für den Verkehr einrichten. Dazu müssen Sie den Proxyserver über die Befehlszeilenschnittstelle (CLI) einrichten. Zum Einrichten des Proxyservers müssen Sie das System neu starten.

1. Geben Sie im Hauptmenü der XenMobile-Befehlszeilenschnittstelle **2** ein, um das Systemmenü auszuwählen.

2. Geben Sie im Systemmenü **6** ein, um das Menü für Proxyserver auszuwählen.



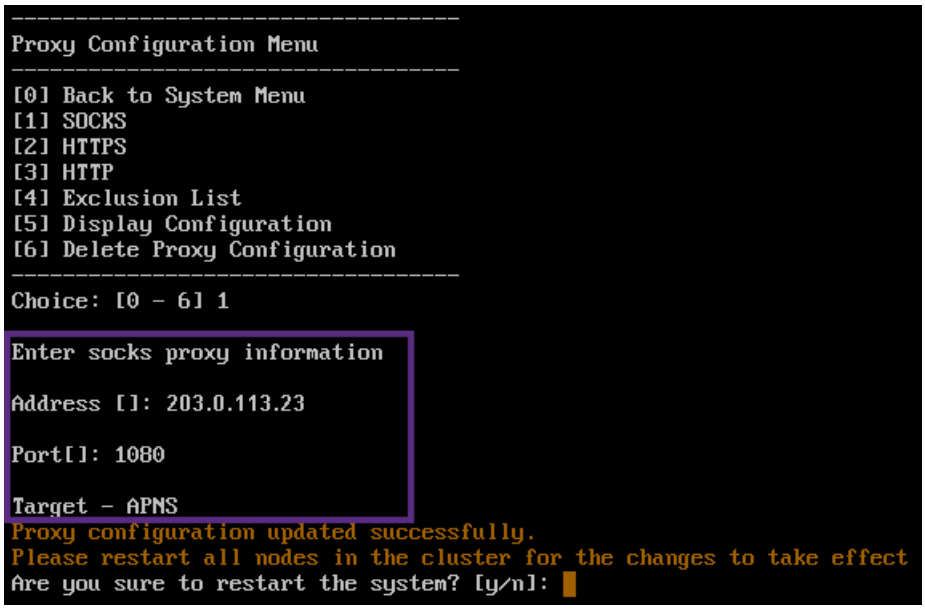
3. Geben Sie im Menü für die Proxykonfiguration **1** für die Auswahl von SOCKS ein, **2** für die Auswahl von HTTPS oder **3** für die Auswahl von HTTP.



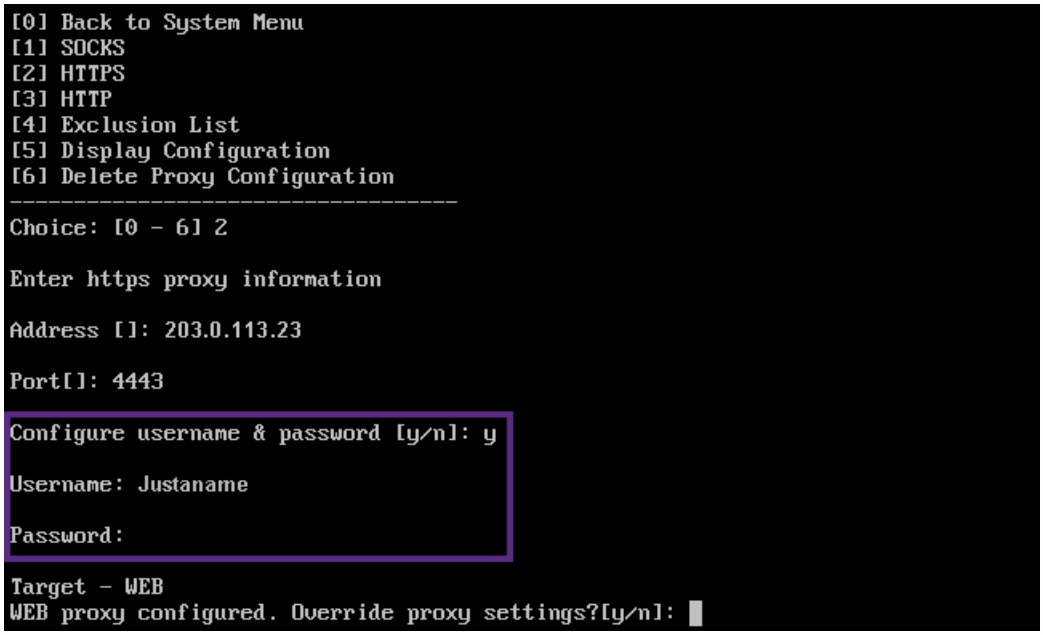
4. Geben Sie IP-Adresse, Portnummer und Ziel des Proxyservers ein. In der folgenden Tabelle sind die für die Proxyservertypen unterstützten Zieltypen aufgeführt.

Proxytyp	Unterstützte Ziele

SOCKS	APNS
HTTP	APNS, Web PKI
HTTPS	Web, PKI
HTTP mit Authentifizierung	Web, PKI
HTTPS mit Authentifizierung	Web, PKI



5. Wenn Sie einen Benutzernamen und ein Kennwort für die Authentifizierung auf dem HTTP- oder HTTPS-Proxyserver konfigurieren möchten, geben Sie **y** ein und dann den Benutzernamen und das Kennwort.



6. Geben Sie **y** ein, um die Einrichtung des Proxyservers abzuschließen.

Lizenzierung

May 05, 2016

XenMobile und NetScaler Gateway erfordern eine Lizenz. Informationen zur Lizenzierung von NetScaler Gateway finden Sie unter Installing Licenses on NetScaler Gateway.
Bei XenMobile wird die Citrix Lizenzierung zum Verwalten von Lizenzen verwendet. Informationen über die Citrix Lizenzierung finden Sie auf der Website zum Citrix Lizenzprogramm.

Nach dem Erwerb von XenMobile erhalten Sie per E-Mail eine Bestellbestätigung mit Anweisungen zum Aktivieren der Lizenzen. Neue Kunden müssen sich für ein Lizenzprogramm registrieren, bevor sie eine Bestellung machen können. Weitere Informationen über XenMobile-Lizenzierungsmodelle und -Programme finden Sie unter XenMobile-Lizenzierung.

Sie müssen vor dem Herunterladen der XenMobile-Lizenzen die Citrix Lizenzierung installieren. Der Name des Servers, auf dem Sie die Citrix Lizenzierung installiert haben, ist zum Generieren der Lizenzdatei erforderlich. Wenn Sie XenMobile installieren, wird die Citrix Lizenzierung standardmäßig auf dem Server installiert. Alternativ können Sie eine vorhandene Bereitstellung der Citrix Lizenzierung zum Verwalten der XenMobile-Lizenzen verwenden. Weitere Informationen zur Installation, Bereitstellung und Verwaltung der Citrix Lizenzierung finden Sie unter Lizenzieren des Produkts.
Hinweis: XenMobile 10 erfordert den Citrix Lizenzserver 11.12.1 oder höher, ältere Versionen funktionieren nicht mit XenMobile 10.
Wichtig: Wenn Sie Knoten oder Instanzen von XenMobile in Clustern verwenden möchten, müssen Sie die Citrix Lizenzierung auf einem Remoteserver verwenden.
Citrix empfiehlt, eine lokale Kopie aller Lizenzdateien aufzubewahren, die Sie erhalten. Wenn Sie eine Sicherungskopie der Konfigurationsdatei speichern, sind alle Lizenzdateien darin enthalten. Wenn Sie jedoch XenMobile erneut installieren, ohne zuvor die Konfigurationsdatei zu sichern, brauchen Sie die Originallizenzdateien.

Informationen zur XenMobile-Lizenzierung

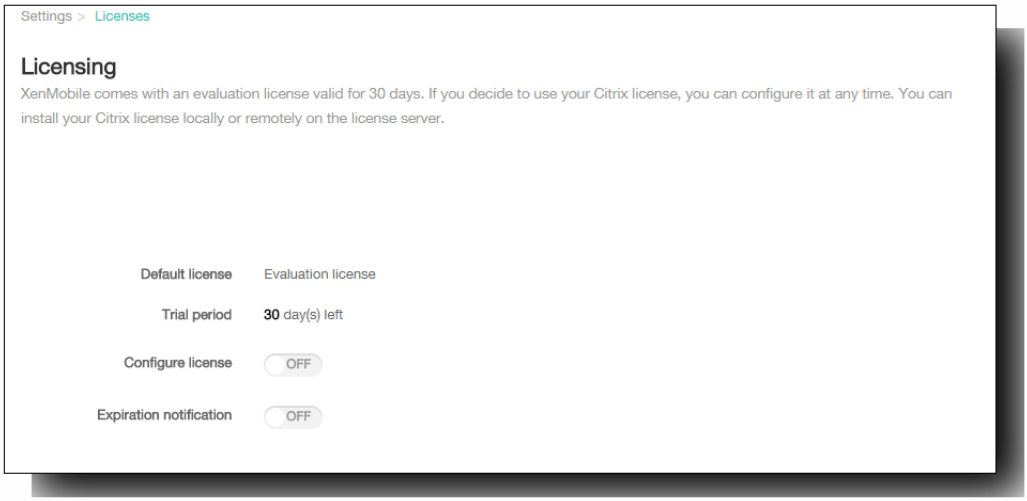
Ohne Lizenz kann XenMobile zu Evaluierungszwecken voll funktionsfähig für einen Zeitraum von 30 Tagen ausgeführt werden. Der Testmodus ist nur einmal möglich, der 30-tägige Kulanzzeitraum beginnt mit der Installation. Der Zugriff auf die XenMobile-Webkonsole ist nie gesperrt, unabhängig davon, ob eine gültige XenMobile-Lizenz verfügbar ist.

In XenMobile können zwar mehrere Lizenzen hochgeladen werden, es kann aber nur eine Lizenz aktiviert werden.

Läuft eine XenMobile-Lizenz ab, sind keinerlei Geräteverwaltungsfunktionen mehr verfügbar. Neue Benutzer oder Geräte können dann beispielsweise nicht registriert werden und auf registrierten Geräten bereitgestellte Apps und Konfigurationen können nicht aktualisiert werden.

So finden Sie die Lizenzierungsseite in der XenMobile-Konsole

Wenn die Lizenzierungsseite nach der Installation von XenMobile zum ersten Mal angezeigt wird, ist standardmäßig der 30-tägige Testmodus aktiviert und die Lizenz ist noch nicht konfiguriert. Sie können auf dieser Seite Lizenzen hinzufügen und konfigurieren.



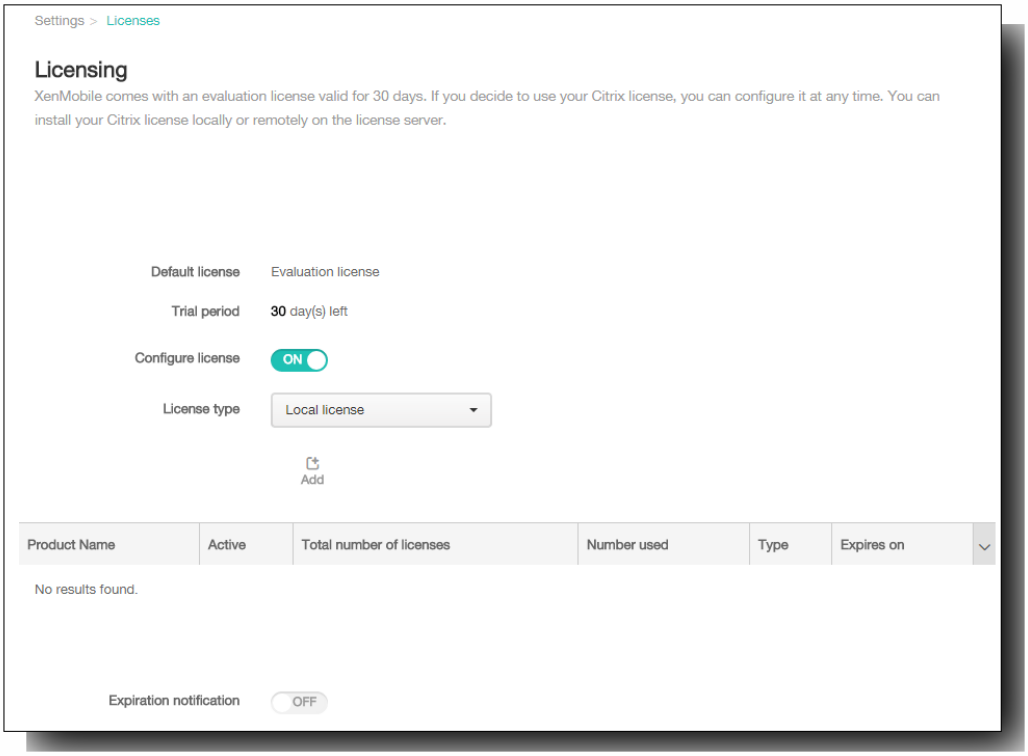
1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings.
2. Klicken Sie auf Licensing. Die Seite Licensing wird angezeigt.

So fügen Sie eine lokale Lizenz hinzu

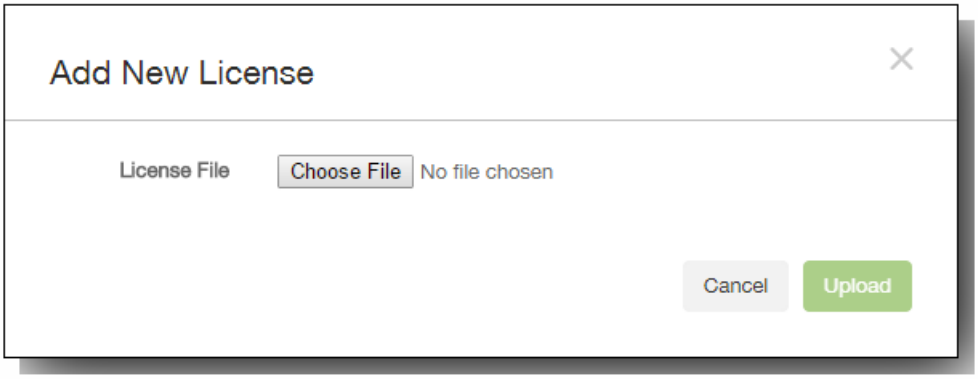
Wenn Sie neue Lizenzen hinzufügen, werden diese in der Tabelle angezeigt. Die zuerst hinzugefügte Lizenz wird automatisch aktiviert. Wenn Sie mehrere Lizenzen derselben Kategorie (z. B. Enterprise) und desselben Typs (z. B. Gerät) hinzufügen, werden diese in einer einzigen Tabellenzeile angezeigt. In diesen Fällen verstehen sich die Angaben unter Total number of license und Number used in ihrer Kombination als Gesamtzahl der Lizenzen. Das Datum unter Expires on ist das Ablaufdatum der aktuellsten Lizenz.

Sie können alle lokalen Lizenzen über die XenMobile-Konsole verwalten.

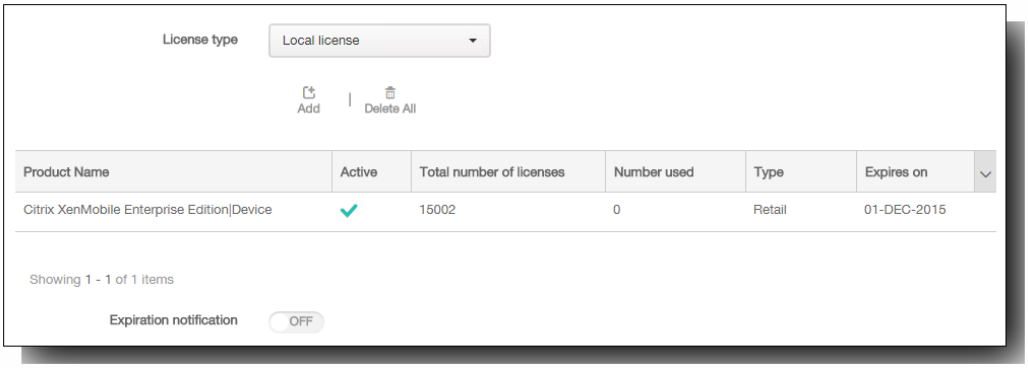
1. Eine Lizenzdatei erhalten Sie über den Simple License Service, die License Administration Console oder direkt über Ihr Konto auf Citrix.com. Einzelheiten hierzu finden Sie unter Abrufen der Lizenzdateien.
2. Klicken Sie in der Konsole auf Configure > Settings > Licenses. Die Seite Licensing wird angezeigt.
3. Legen Sie für Configure license den Wert On fest. Es werden die Liste License type, die Schaltfläche Add und die Lizenztabelle angezeigt. Die Lizenztabelle enthält die Lizenzen, die Sie mit XenMobile verwendet haben. Wenn Sie noch keine Citrix Lizenz hinzugefügt haben, ist die Tabelle leer.



4. Stellen Sie sicher, dass License type auf Local license festgelegt ist, und klicken Sie auf Add. Das Dialogfeld Add New License wird angezeigt.



5. Klicken Sie im Dialogfeld Add New License auf Choose File und navigieren Sie zu der Lizenz.
6. Klicken Sie auf Upload. Die Lizenz wird lokal hochgeladen und in der Tabelle angezeigt.

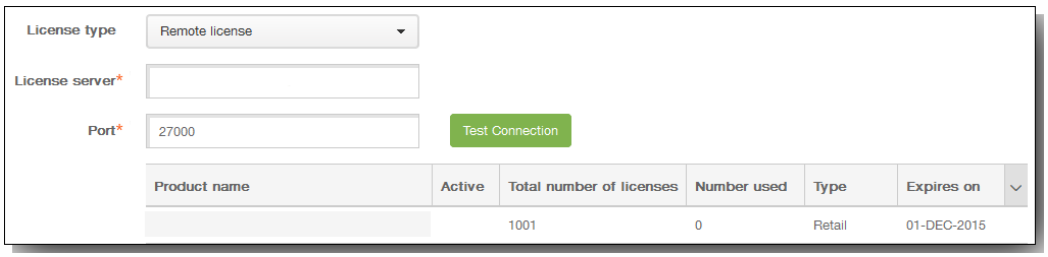


7. Wenn die Lizenz in der Tabelle auf der Seite License angezeigt wird, aktivieren Sie sie. Wenn dies die erste Lizenz in der Tabelle ist, wird sie automatisch aktiviert.

So fügen Sie eine Remote-Lizenz hinzu

Wenn Sie den Remoteserver der Citrix Lizenzierung verwenden, verwenden Sie diesen zum Verwalten aller Lizenzierungsaktivitäten. Weitere Informationen finden Sie unter Lizenzieren des Produkts.

1. Legen Sie auf der Seite Licensing den Wert für Configure license auf On fest. Es werden die Liste License type, die Schaltfläche Add und die Lizenztabelle angezeigt. Die Lizenztabelle enthält die Lizenzen, die Sie mit XenMobile verwendet haben. Wenn Sie noch keine Citrix Lizenz hinzugefügt haben, ist die Tabelle leer.
2. Legen Sie für License type den Wert Remote license fest. Die Schaltfläche Add wird durch die Felder License server und Port und die Schaltfläche Test Connection ersetzt.



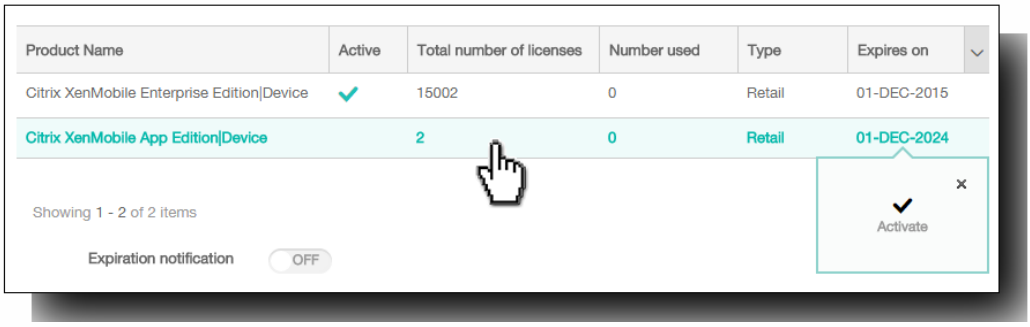
3. Geben Sie für License server die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Remoteservers für die Lizenzierung ein.
4. Übernehmen Sie im Feld Port den Standardport oder geben Sie die Portnummer für die Kommunikation mit dem Lizenzserver ein.
5. Klicken Sie auf Test Connection. Wenn die Verbindung erfolgreich hergestellt wird, stellt XenMobile eine Verbindung mit dem Lizenzserver her und die Lizenztabelle wird mit den verfügbaren Lizenzen aufgefüllt. Wenn die Verbindung fehlschlägt, stellen Sie sicher, dass Sie die richtigen Informationen angegeben haben und alle Verbindungen aktiv sind. Hinweis: Gibt es nur eine Lizenz, wird diese automatisch aktiviert.

So aktivieren Sie eine andere Lizenz

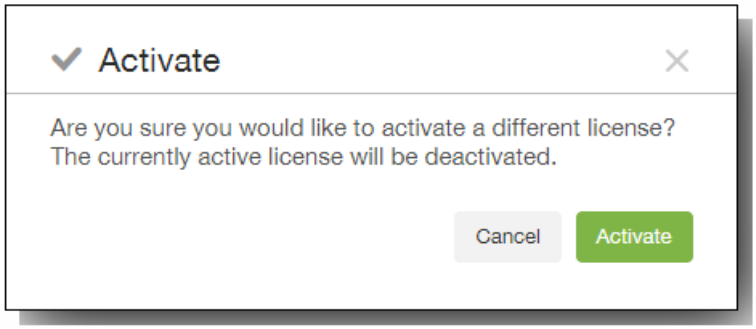
Wenn Sie mehrere Lizenzen haben, können Sie die gewünschte Lizenz zur Aktivierung auswählen. Es kann jedoch immer nur eine Lizenz aktiv sein.

1. Klicken Sie auf der Seite Licensing in der Lizenztabelle auf die Zeile der Lizenz, die Sie aktivieren möchten. Neben der Zeile

wird zur Bestätigung das Feld Activate eingeblendet.



2. Klicken Sie auf Activate. Das Dialogfeld Activate wird angezeigt.

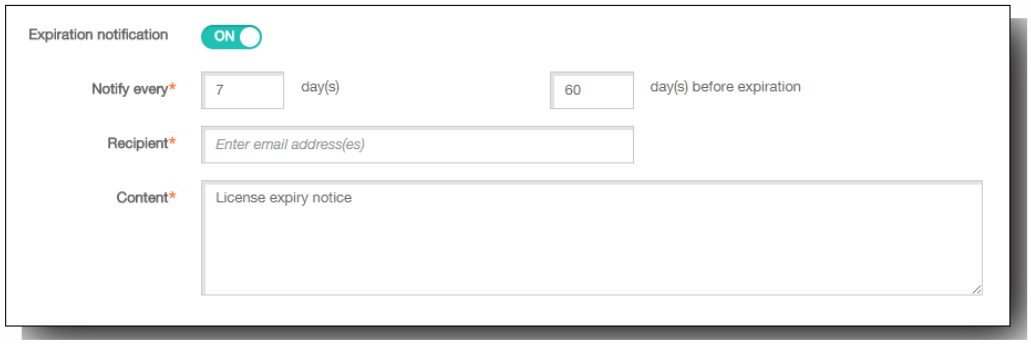


3. Klicken Sie auf Activate.
   Wichtig: Wenn Sie die ausgewählte Lizenz aktivieren, wird die bisher aktive Lizenz deaktiviert.
   Die ausgewählte Lizenz wird aktiviert.

So richten Sie eine automatische Ablaufbenachrichtigung ein

Nach Aktivierung einer Remote- oder lokalen Lizenz können Sie XenMobile so konfigurieren, dass Sie oder eine andere Person automatisch über das Nahen des Ablaufdatums benachrichtigt werden.

1. Legen Sie auf der Seite Licensing den Wert für Expiration notification auf On fest. Es werden Felder für die Benachrichtigung eingeblendet.



2. Geben Sie für Notify every Folgendes an:
   - Häufigkeit, mit der Benachrichtigungen gesendet werden, z. B. alle 7 Tage.
   - Wann der Versand von Benachrichtigung beginnen soll, z. B. 60 Tage vor Lizenzablauf.
3. Geben Sie im Feld Recipient Ihre E-Mail-Adresse oder die der für die Lizenzierung zuständigen Person ein.
4. Geben Sie im Feld Content den Text der Ablaufbenachrichtigung ein.
5. Klicken Sie auf Speichern. Zu dem festgelegten Datum vor dem Ablauf der Lizenz beginnt XenMobile mit dem Versand von E-Mail-Nachrichten mit dem von Ihnen angegebenen Text an den von Ihnen festgelegten Empfänger. Der Versand der Benachrichtigungen wird mit der von Ihnen vorgegebenen Häufigkeit wiederholt.

Erste Schritte mit der XenMobile-Konsole

May 05, 2016

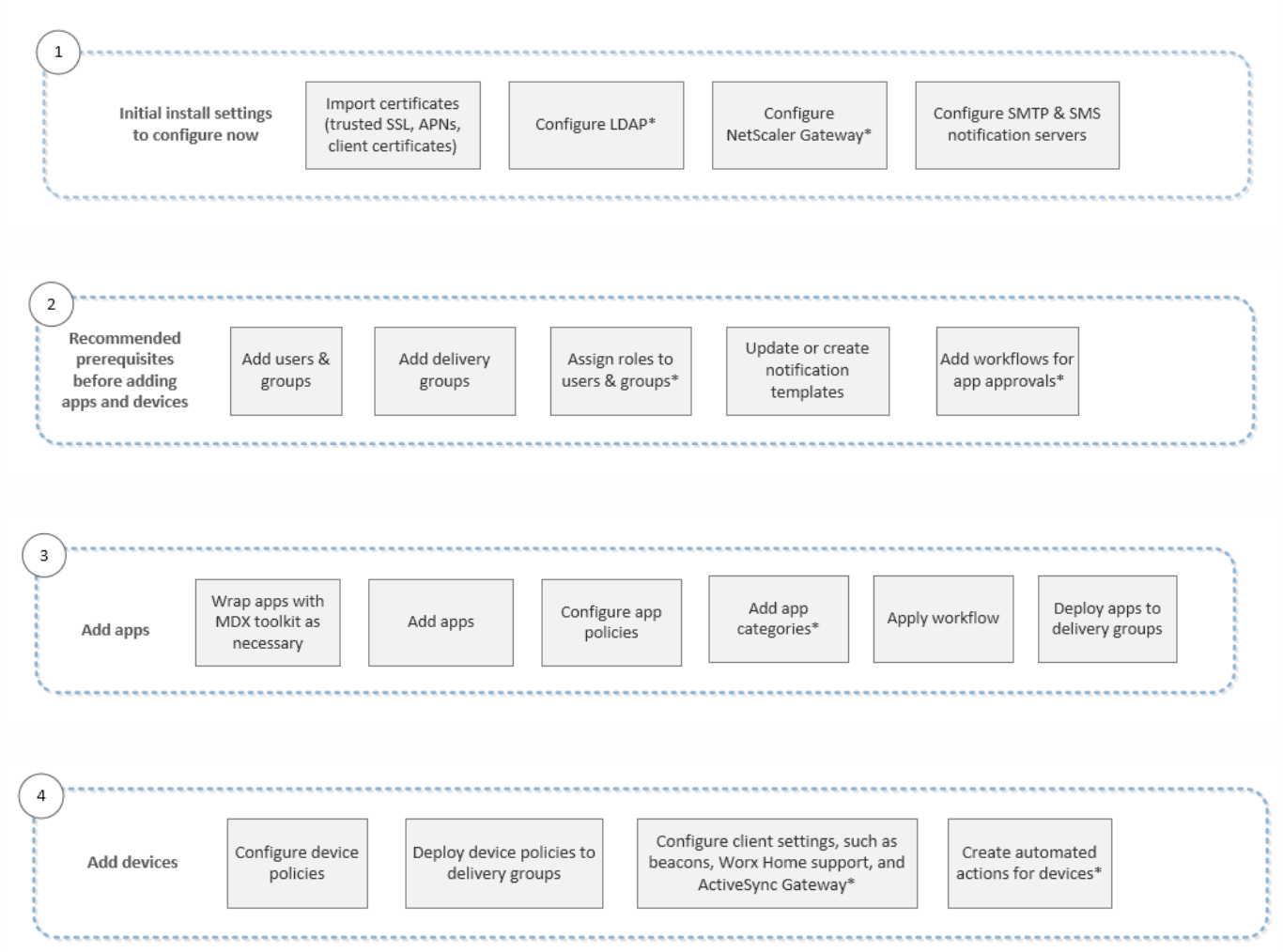
Die XenMobile-Konsole ist das zentrale Verwaltungstool in XenMobile 10, das die Komponenten App Controller und Device Manager aus XenMobile 9 und früheren Versionen vereint. In diesem Abschnitt wird vorausgesetzt, dass Sie XenMobile installiert haben und für die Arbeit mit der Konsole bereit sind. Für die Installation von XenMobile siehe Installieren von XenMobile.

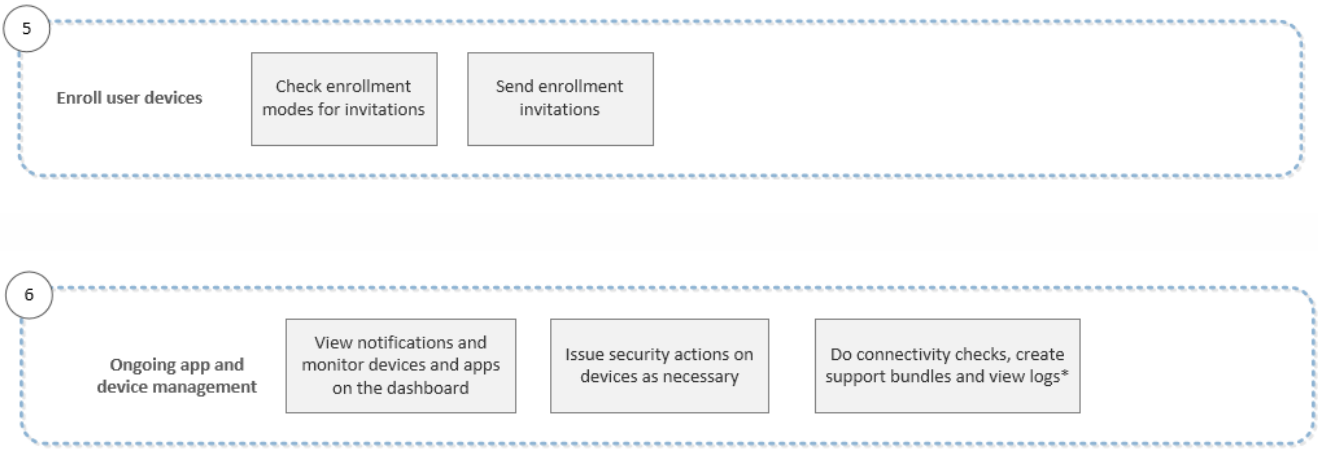
Die XenMobile-Konsole unterstützt die beiden neuesten Versionen von Firefox, Chrome und Internet Explorer.

Die folgende Abbildung zeigt die Reihenfolge der empfohlenen Workflows zur Vorbereitung der App- und Geräteverwaltung. Die Empfehlungen zu Beginn beziehen sich auf Ersteinstellungen, die Sie während der Installation möglicherweise übersprungen haben.

Tipp: Klicken Sie auf jede Zeile, um einen Abschnitt mit mehr Detailangaben und Links zu Verfahren zu öffnen.

Hinweis: Die mit einem Sternchen gekennzeichneten Elemente sind optional.



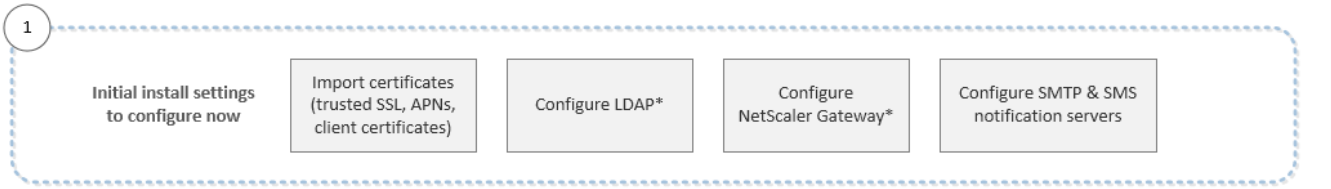


Workflow für erste Einstellungen

May 05, 2016

Wenn Sie XenMobile über die Befehlszeilenkonsole und anschließend in der XenMobile-Konsole konfiguriert haben, wird das Dashboard geöffnet. Da Sie die Bildschirme der Erstkonfiguration nicht wieder aufrufen können, wenn Sie einige Konfigurationsschritte bei der Installation ausgelassen haben, können Sie in der Konsole die folgenden Einstellungen konfigurieren. Bevor Sie Benutzer, Apps und Geräte hinzufügen, empfiehlt sich das Festlegen dieser Installationseinstellungen. Klicken Sie zunächst auf **Configure** > **Settings**. Den gesamten Workflow sehen Sie unter Erste Schritte mit der XenMobile-Konsole.

Hinweis: Die mit einem Sternchen gekennzeichneten Elemente sind optional.



Weitere Informationen zu jeder Einstellung und schrittweise Anleitungen finden Sie in den folgenden eDocs-Abschnitten:

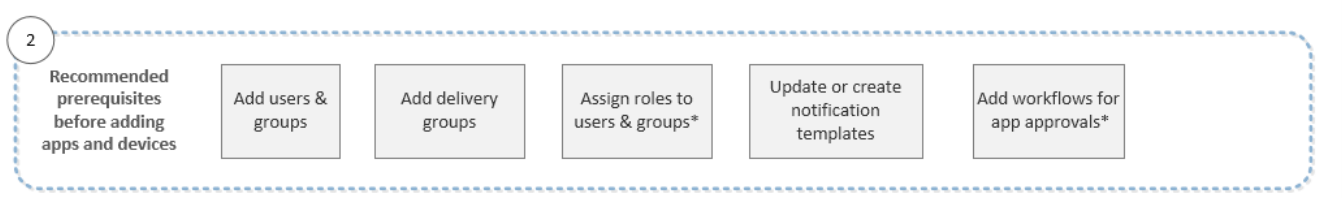
- Zertifikate in XenMobile
- Konfigurieren von LDAP
- NetScaler Gateway und XenMobile
- Benachrichtigungen in XenMobile

Workflow für Konsolenvoraussetzungen

May 05, 2016

Wenn Sie XenMobile über die Befehlszeilenkonsole und anschließend in der XenMobile-Konsole konfiguriert haben, wird das Dashboard geöffnet. Die Empfehlungen für eventuell zuvor ausgelassene Installationskonfigurationen finden Sie unter Workflow für erste Einstellungen. Den gesamten Workflow sehen Sie unter Erste Schritte mit der XenMobile-Konsole.

Der Workflow zeigt Voraussetzungen, deren Konfiguration vor dem Hinzufügen von Apps und Geräten empfohlen wird. Hinweis: Die mit einem Sternchen gekennzeichneten Elemente sind optional.



Weitere Informationen zu jeder Einstellung und schrittweise Anleitungen finden Sie in den folgenden eDocs-Abschnitten:

- Konfigurieren von Benutzerkonten, Rollen und Registrierungseinstellungen
- Verwalten von Bereitstellungsgruppen in XenMobile
- Erstellen und Aktualisieren benutzerdefinierter Rollen in XenMobile mit der rollenbasierten Zugriffssteuerung
- So erstellen oder aktualisieren Sie Benachrichtigungsvorlagen in XenMobile
- So konfigurieren Sie Registrierungsmodi und aktivieren das Selbsthilfeportal
- So erstellen und verwalten Sie Workflows

Workflow beim Hinzufügen von Apps

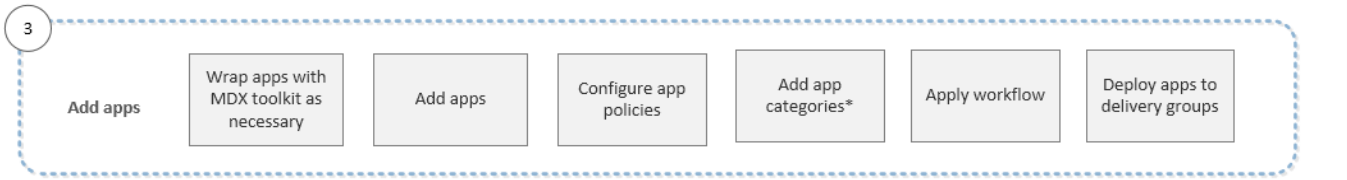
May 05, 2016

Wenn Sie XenMobile über die Befehlszeilenkonsole und anschließend in der XenMobile-Konsole konfiguriert haben, wird das Dashboard geöffnet. Die Empfehlungen für eventuell zuvor ausgelassene Installationskonfigurationen finden Sie unter Workflow für erste Einstellungen.

Sie können nun gemäß dem Workflow für Konsolenvoraussetzungen einige Voraussetzungen vor dem Hinzufügen von Apps und Geräten konfigurieren. Den gesamten Workflow sehen Sie unter Erste Schritte mit der XenMobile-Konsole.

Der Workflow zeigt die beim Hinzufügen von Apps in XenMobile empfohlene Reihenfolge.

Hinweis: Die mit einem Sternchen gekennzeichneten Elemente sind optional.



Weitere Informationen zu jeder Einstellung und schrittweise Anleitungen finden Sie in den folgenden eDocs-Abschnitten:

- Umschließen von Apps mit dem MDX Toolkit
- Hinzufügen von Apps in XenMobile
- MDX-Richtlinien für iOS, Android und Windows Phone 8.1
- So fügen Sie App-Kategorien hinzu
- So erstellen und verwalten Sie Workflows
- Verwalten von Bereitstellungsgruppen in XenMobile

Workflow beim Hinzufügen von Geräten

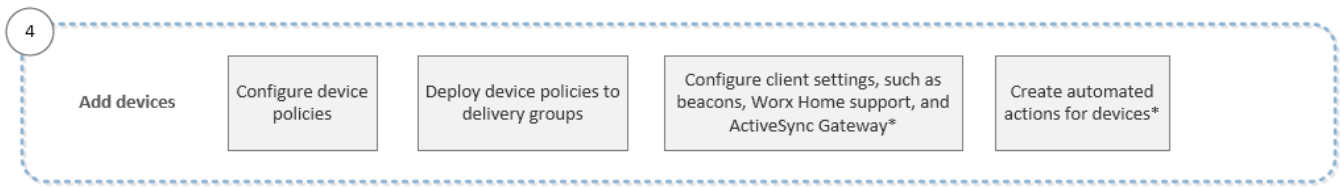
May 05, 2016

Wenn Sie XenMobile über die Befehlszeilenkonsole und anschließend in der XenMobile-Konsole konfiguriert haben, wird das Dashboard geöffnet. Die Empfehlungen für eventuell zuvor ausgelassene Installationskonfigurationen finden Sie unter Workflow für erste Einstellungen.

Sie können nun gemäß dem Workflow für Konsolenvoraussetzungen einige Voraussetzungen vor dem Hinzufügen von Apps und Geräten konfigurieren. Anschließend können Sie Apps gemäß dem Workflow beim Hinzufügen von Apps hinzufügen. Den gesamten Workflow sehen Sie unter Erste Schritte mit der XenMobile-Konsole.

Der Workflow zeigt die beim Hinzufügen und Registrieren von Geräten in XenMobile empfohlene Reihenfolge.

Hinweis: Die mit einem Sternchen gekennzeichneten Elemente sind optional.



Weitere Informationen zu jeder Einstellung und schrittweise Anleitungen finden Sie in den folgenden eDocs-Abschnitten:

- Hinzufügen von Geräten und Anzeigen von Gerätedetails in XenMobile
- XenMobile-Geräterichtlinien nach Plattform
- Verwalten von Bereitstellungsgruppen in XenMobile
- Konfigurieren der XenMobile-Clienteinstellungen
- Erstellen automatisierter Aktionen in XenMobile

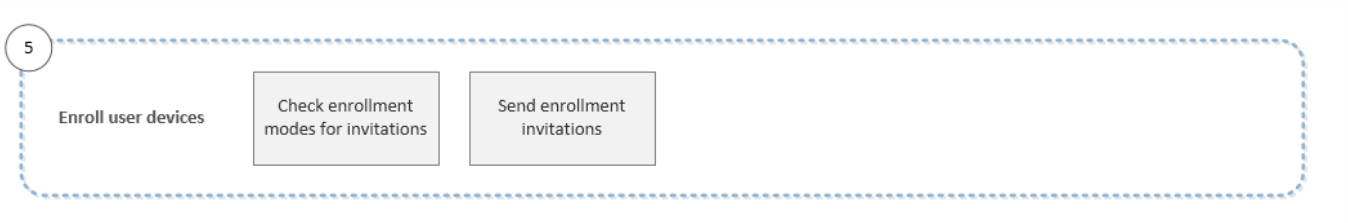
Workflow beim Registrieren von Benutzergeräten

May 05, 2016

Wenn Sie XenMobile über die Befehlszeilenkonsole und anschließend in der XenMobile-Konsole konfiguriert haben, wird das Dashboard geöffnet. Die Empfehlungen für eventuell zuvor ausgelassene Installationskonfigurationen finden Sie unter Workflow für erste Einstellungen.

Sie können nun gemäß dem Workflow für Konsolenvoraussetzungen einige Voraussetzungen vor dem Hinzufügen von Apps und Geräten konfigurieren. Anschließend können Sie gemäß dem Workflow beim Hinzufügen von Apps Apps hinzufügen und gemäß dem Workflow beim Hinzufügen von Geräten Geräte hinzufügen und registrieren. Den gesamten Workflow sehen Sie unter Erste Schritte mit der XenMobile-Konsole.

Der Workflow zeigt die beim Registrieren von Geräten in XenMobile empfohlene Reihenfolge.



Weitere Informationen zu jeder Einstellung und schrittweise Anleitungen finden Sie in den folgenden eDocs-Abschnitten:

- Konfigurieren von Benutzerkonten, Rollen und Registrierungseinstellungen
- So konfigurieren Sie Registrierungsmodi und aktivieren das Selbsthilfeportal

Workflow bei der Verwaltung von Apps und Geräten

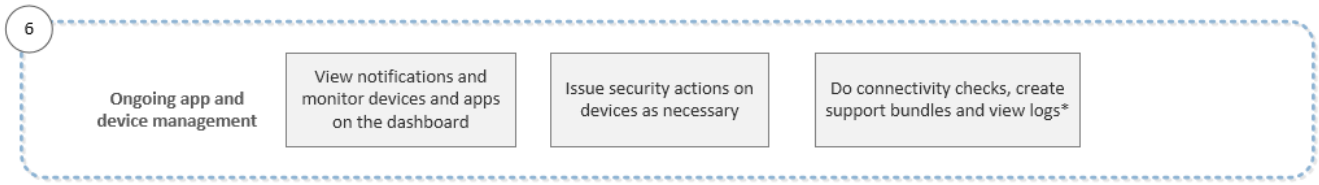
May 05, 2016

Wenn Sie XenMobile über die Befehlszeilenkonsole und anschließend in der XenMobile-Konsole konfiguriert haben, wird das Dashboard geöffnet. Die Empfehlungen für eventuell zuvor ausgelassene Installationskonfigurationen finden Sie unter Workflow für erste Einstellungen.

Sie können nun gemäß dem Workflow für Konsolenvoraussetzungen einige Voraussetzungen vor dem Hinzufügen von Apps und Geräten konfigurieren. Anschließend können Sie gemäß dem Workflow beim Hinzufügen von Apps Apps hinzufügen und gemäß dem Workflow beim Hinzufügen von Geräten Geräte hinzufügen und registrieren. Nach Abschluss der vier ersten Workflows folgen Sie den Workflow beim Registrieren von Benutzergeräten. Den gesamten Workflow sehen Sie unter Erste Schritte mit der XenMobile-Konsole.

Dieser sechste und letzte Workflow zeigt die empfohlenen Aktivitäten zur Verwaltung von Apps und Geräten, die Sie in der Konsole ausführen können.

Hinweis: Die mit einem Sternchen gekennzeichneten Elemente sind optional.



Informationen zu den Supportoptionen, die über das Schraubenschlüsselsymbol oben rechts in der Konsole aufgerufen werden, finden Sie unter Support und Wartung von XenMobile.

Filter und Tabellen in der XenMobile-Konsole

May 05, 2016

Filter und Tabellen gibt es in allen Bereichen der XenMobile-Konsole, auf den Registerkarten "Devices", "Enrollment", "Device Policies", "Apps", "Actions" und "Delivery Groups". Mit Filtern können Sie die Informationen in all diesen Bereichen auf die von Ihnen gesuchten einschränken. In Tabellen können Sie per Mausklick Optionen für die Ausführung von Aktionen an den Tabelleninformationen anzeigen.

So zeigen Sie Optionen in den Tabellen in der XenMobile-Konsole an

Sie können die Optionen zum Ausführen von Aktionen für Informationen in den Tabellen der Konsole auf verschiedene Weise anzeigen:

- Sie können das Kontrollkästchen neben einer Richtlinie auswählen, um das Menü der Optionen oberhalb der Richtlinienliste anzuzeigen.
- Sie können das Kontrollkästchen mehrerer Richtlinie auswählen, um diese Richtlinien in einem Schritt zu löschen.
- Sie können auf eine Richtlinie in der Liste klicken, um das Menü mit den Optionen rechts daneben anzuzeigen. Wenn Sie auf Show More klicken, wird eine Liste mit Details zur Konfiguration angezeigt.
- Sie können einen Richtliniennamen vollständig oder teilweise in das Feld Search eingeben, um die Anzahl der angezeigten Richtlinien zu beschränken.

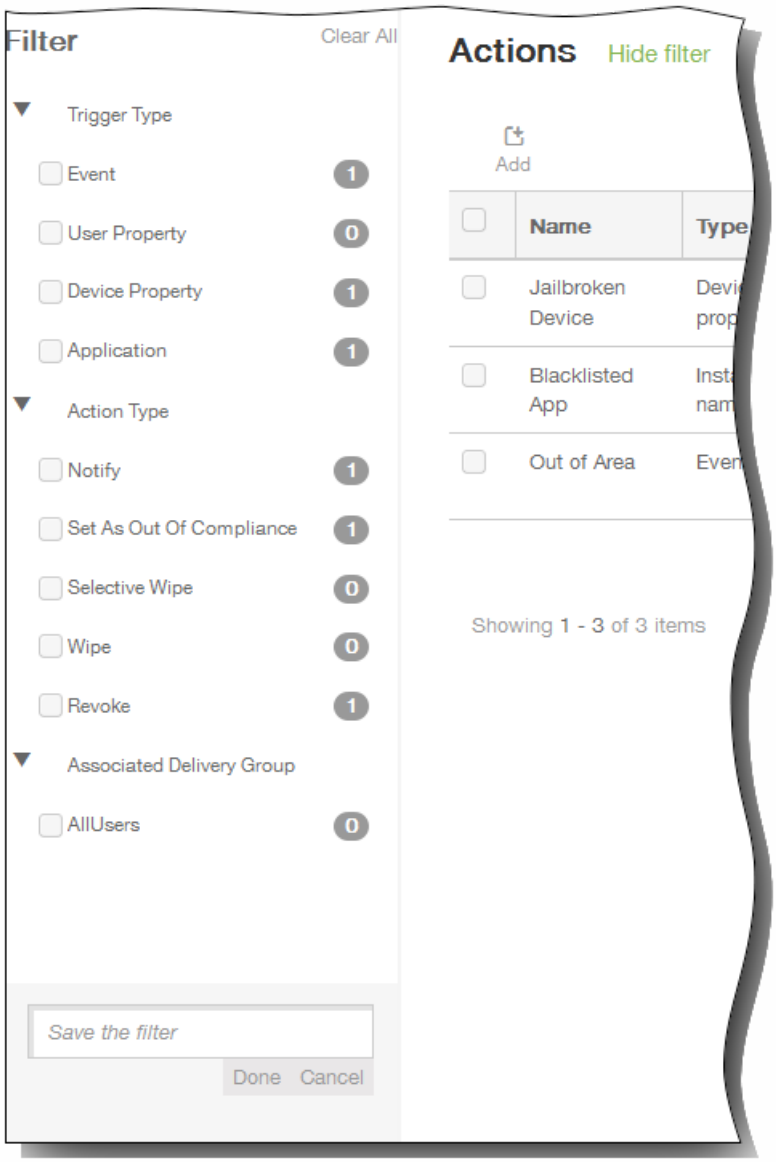
Die folgende Abbildung zeigt die Anzeige der Optionen im Bereich "Device Policies" der Konsole. Es werden nur 10 Objekte pro Seite aufgeführt. Klicken Sie auf die Dreiecke in der unteren rechten Ecke, um durch die Seiten zu blättern.

So filtern Sie Informationen in der XenMobile-Konsole

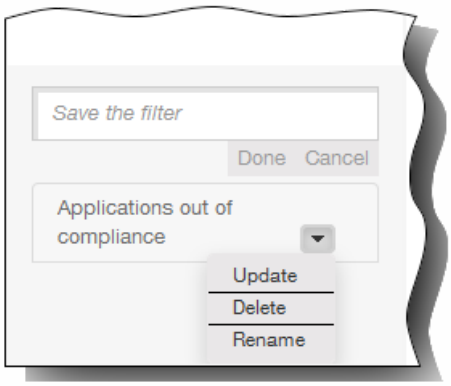
Wenn Sie einen bestimmten Teil der Informationen in einem Konsolenbereich wie "Devices", "Enrollment", "Device Policies", "Apps", "Actions" oder "Delivery Groups" anzeigen möchten, können Sie die Liste nach Ihren Kriterien filtern. Hier wird die Seite "Actions" als Beispiel verwendet, die Schritte zum Filtern sind jedoch in der gesamten Konsole gleich.

1. Klicken Sie auf der Seite Actions auf Show Filter.

   Der Bereich "Filter" wird angezeigt. Er zeigt die Kriterien, anhand derer Sie die Liste Actions filtern können. Die Zahlen rechts neben jedem Kriterium repräsentieren die Zahl der Aktionen, die dem Kriterium entsprechen.



2. Klicken Sie auf das Dreieck links neben einem Filter, um die Optionen für den Filter anzuzeigen.
3. Wählen Sie die gewünschten Filterkriterien aus. Die Liste Actions enthält nun nur die Aktionen, die den ausgewählten Kriterien entsprechen.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf Hide Filter, um die Arbeit mit der gefilterten Liste fortzusetzen.
   - Klicken Sie auf Clear All, um die vollständige Liste wiederherzustellen.
5. Zum Speichern der ausgewählten Kriterien in einem benutzerdefinierten Filter geben Sie im Feld Save the filter unten im Bereich Filter einen aussagekräftigen Namen ein und klicken Sie auf Done. Wenn Sie den Filter nicht speichern möchten, klicken Sie auf Cancel.



6. Nach dem Speichern des Filters können Sie ihn unten im Bereich Filter auswählen.
   Hinweis: Wenn Sie auf das Dreieck rechts neben dem Filternamen klicken, können Sie den Filter durch neue oder geänderte Kriterien aktualisieren, löschen oder umbenennen.

Benachrichtigungen

May 05, 2016

Sie können Benachrichtigungen in XenMobile zu folgenden Zwecken verwenden:

- Zur Kommunikation mit ausgewählten Benutzergruppen zu diversen Systemfunktionen. Sie können diese Benachrichtigungen auch an bestimmte Benutzer richten, z. B. alle Benutzer mit iOS-Geräten, Benutzer mit nicht richtlinientreuen Geräten, Benutzer mit Privatgeräten usw.
- Zur Registrierung von Benutzern und ihren Geräten.
- Zur automatischen Benachrichtigung von Benutzern (über automatisierte Aktionen), wenn bestimmte Bedingungen erfüllt sind, z. B. wenn ein Gerät aus der Unternehmensdomäne ausgeschlossen werden soll, weil es gegen eine Richtlinie verstößt, oder bei Jailbreak oder Rooting. Details über automatisierte Aktionen finden Sie unter Erstellen automatisierter Aktionen in XenMobile.

Zum Senden von Benachrichtigungen mit XenMobile müssen Sie ein Gateway und einen Benachrichtigungsserver konfigurieren. Sie können einen Benachrichtigungsserver in XenMobile konfigurieren, um Gatewayserver für Simple Mail Transfer Protocol (SMTP) und Short Message Service (SMS) einzurichten und den Versand von E-Mail- und Textnachrichten an die Benutzer zu ermöglichen. Sie können Benachrichtigungen über zwei Kanäle senden: SMTP oder SMS.

- SMTP ist ein verbindungsorientiertes textbasiertes Protokoll, bei dem ein E-Mail-Absender mit einem E-Mail-Empfänger unter Ausgabe von Befehlszeichenfolgen und Bereitstellung der erforderlichen Daten kommuniziert. Dies geschieht normalerweise über eine TCP-Verbindung (Transmission Control Protocol). SMTP-Sitzungen bestehen aus Befehlen von einem SMTP-Client (der Person, die die Nachricht sendet) und den entsprechenden Antworten vom SMTP-Server.
- SMS ist eine Dienstkomponente von Telefon-, Internet- oder mobilen Kommunikationssystemen für Textnachrichten. Sie verwendet standardisierte Kommunikationsprotokolle für den Austausch kurzer Textnachrichten zwischen Festnetz- oder Mobiltelefonen.

Sie können auch ein Netzbetreiber-SMS-Gateway in XenMobile einrichten, um Benachrichtigungen zu konfigurieren, die über das SMS-Gateway eines Netzbetreibers gesendet werden. Netzbetreiber nutzen SMS-Gateways für den Versand oder Empfang von Textnachrichten an bzw. von einem Telekommunikationsnetz. Standardisierte Kommunikationsprotokolle werden für den Austausch kurzer Textnachrichten zwischen Festnetz- oder Mobiltelefonen verwendet.

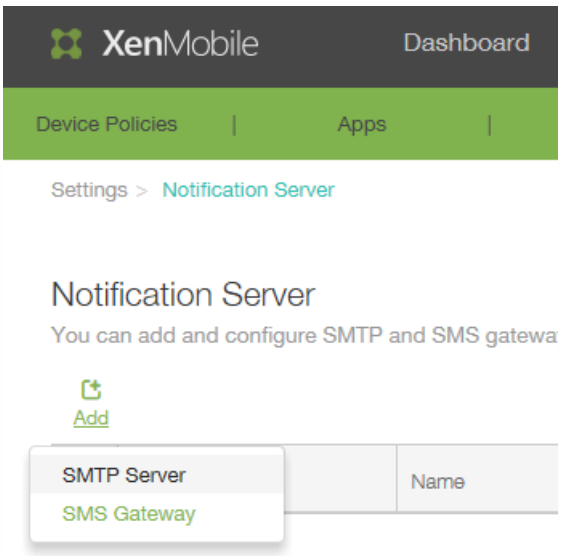
In diesem Abschnitt wird das Hinzufügen eines SMTP-Servers, eines SMS-Gateways und eines Netzbetreiber-SMS-Gateways beschrieben.

So konfigurieren Sie einen SMTP-Server und ein SMS-Gateway

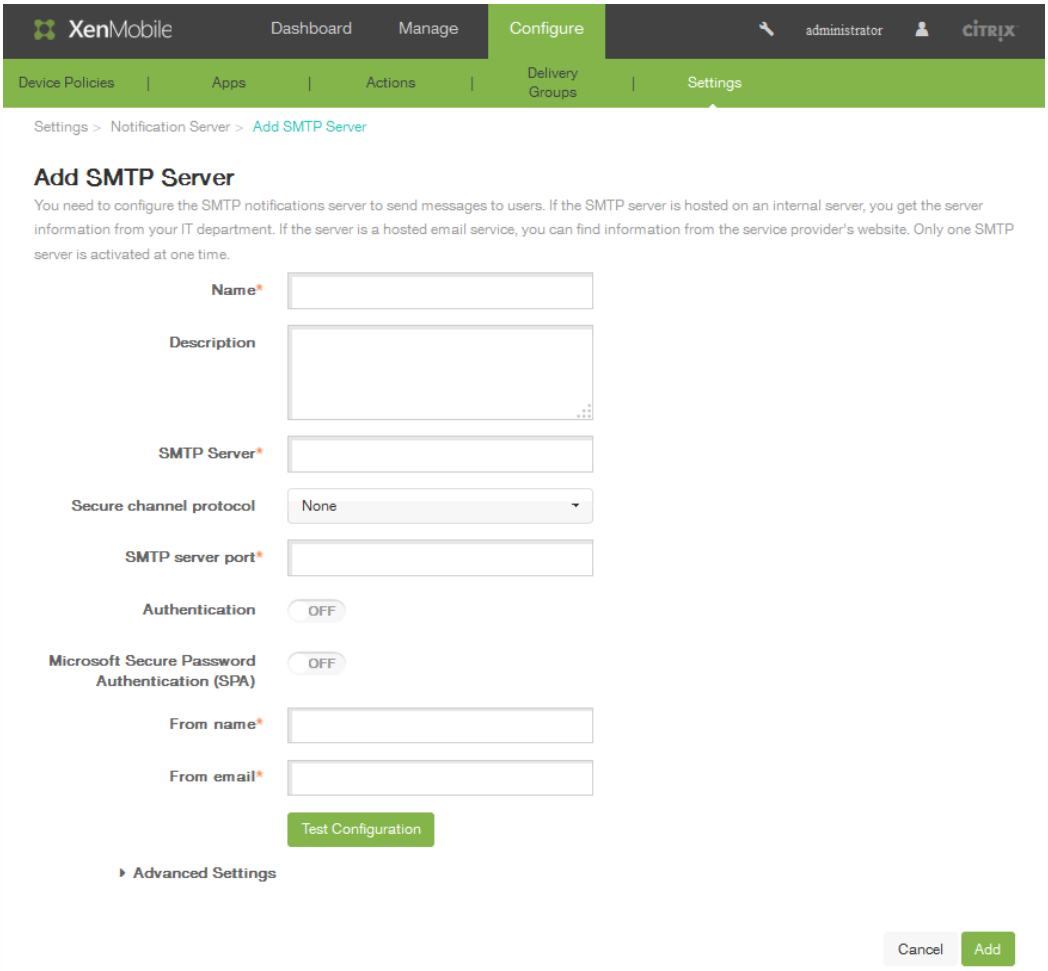
Voraussetzungen:

- Bringen Sie vor der Konfiguration des SMS-Gateways beim zuständigen Systemadministrator die Serverinformationen in Erfahrung. Wichtig ist, ob der SMS-Server auf einem internen Unternehmensserver gehostet wird oder Teil eines gehosteten E-Mail-Diensts ist. Im letzteren Fall benötigen Sie Informationen von der Website des jeweiligen Anbieters.
- Sie müssen den SMTP-Benachrichtigungsserver zum Senden von Nachrichten an Benutzer konfigurieren. Wenn der Server intern gehostet wird, bringen Sie die Konfigurationsinformationen beim Systemadministrator in Erfahrung. Gehört der Server zu einem gehosteten E-Mail-Dienst, suchen Sie die entsprechenden Konfigurationsinformationen auf der Website des Dienstanbieters.
- Es ist immer nur ein SMTP-Server und ein SMS-Server aktiv.
- Port 25 muss in XenMobile in der DMZ geöffnet sein und auf den SMTP-Server im internen Netzwerk zurückverweisen, damit Benachrichtigungen gesendet werden können.

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



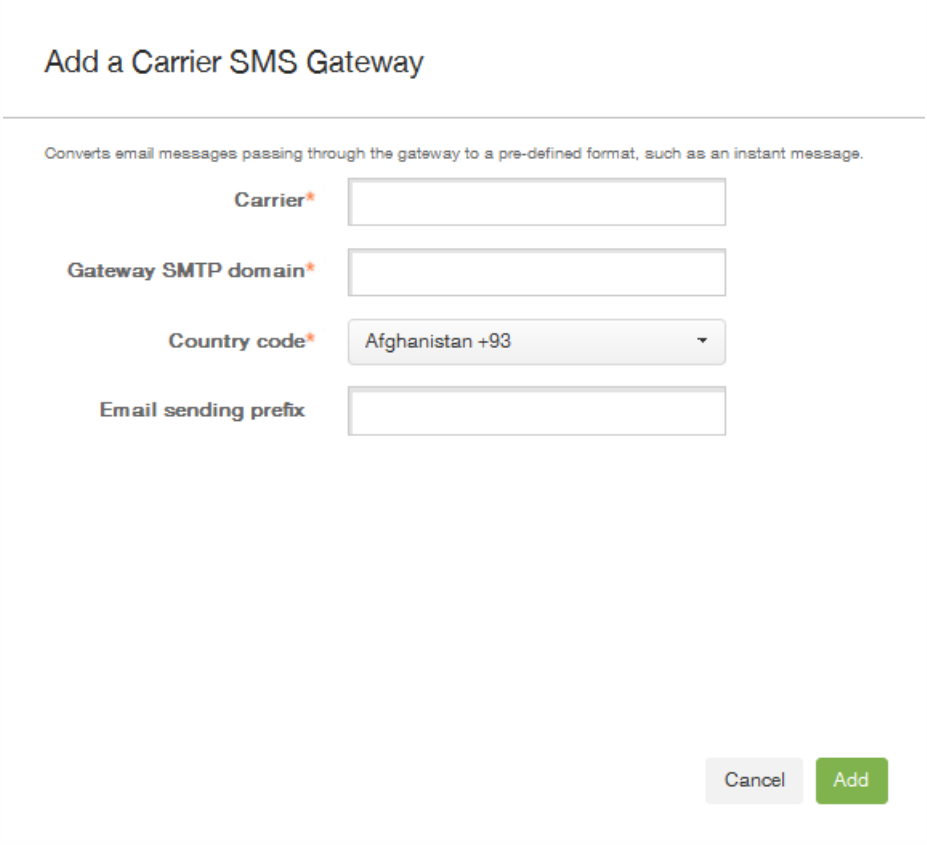
2. Klicken Sie auf Add, anschließend auf SMTP Server oder SMS Gateway und führen Sie je nach Auswahl die nachfolgenden Schritte aus.
   - Zum Hinzufügen eines SMTP-Servers führen Sie die Schritte 3 bis 6 aus.
   - Zum Hinzufügen eines SMS-Gateways führen Sie die Schritte 7 bis 9 aus.
3. Wenn Sie einen SMTP-Server hinzufügen, wird die Seite Add SMTP Server angezeigt.



4. Konfigurieren Sie die folgenden Einstellungen:
   - Name: Geben Sie den Namen des SMTP-Serverkontos ein.
   - Description: Geben Sie optional eine Beschreibung des Servers ein.
   - SMTP Server: Geben Sie den Hostnamen für den Server ein. Sie können einen vollqualifizierten Domänennamen (FQDN) oder eine IP-Adresse eingeben.
   - Secure channel protocol: Klicken Sie in der Liste auf den von dem Server verwendeten sichereren Kanal (sofern der Server für die Verwendung der sicheren Authentifizierung konfiguriert ist): SSL, TLS oder None. Standardmäßig ist für dieses Feld None festgelegt.
   - SMTP server port: Geben Sie den Port des SMTP-Servers ein. In der Standardeinstellung ist dies Port 25. Bei SMTP-Verbindungen, die SSL verwenden, ist der Port auf 465 festgelegt.
   - Authentication: Wählen Sie ON oder OFF. Standardmäßig ist dieses Feature deaktiviert.
   - Microsoft Secure Password Authentication (SPA): Wenn für den SMTP-Server SPA verwendet wird, klicken Sie auf ON. Standardmäßig ist dieses Feature deaktiviert.
   - From Name: Geben Sie den Namen ein, der in Benachrichtigungs-E-Mails von diesem Server im Absenderfeld angezeigt werden soll. Beispiel: Corporate IT.
   - From email: Geben Sie die E-Mail-Adresse ein, die verwendet werden soll, wenn eine E-Mail Empfänger auf eine Benachrichtigung vom SMTP-Server antwortet.
   - Test Configuration: Klicken Sie hier, um eine Test-E-Mail zu senden.
5. Erweitern Sie Advanced Settings und konfigurieren Sie folgende Einstellungen:
   - Number of SMTP retries: Geben Sie die Anzahl wiederholter Sendeversuche für fehlgeschlagene Nachrichten vom SMTP-Server ein. Standardeinstellung für dieses Feld ist 5.

- SMTP Timeout: Geben Sie die Dauer (in Sekunden) an, die beim Senden einer SMTP-Anforderung gewartet werden soll. Erhöhen Sie diesen Wert, wenn beim Senden von Nachrichten häufig Fehler aufgrund von Zeitüberschreitungen auftreten. Wenn Sie diesen Wert allerdings verringern, werden ggf. mehr Nachrichten aufgrund von Zeitüberschreitungen nicht gesendet. Standardeinstellung für dieses Feld ist 30 Sekunden.
- Maximum number of SMTP recipients: Geben Sie die maximale Anzahl Empfänger pro E-Mail-Nachricht vom SMTP-Server ein. Standardeinstellung für dieses Feld ist 100.

6. Nach dem Konfigurieren des SMTP-Servers klicken Sie auf **Add**.
7. Klicken Sie auf der Seite Notification Server zum Konfigurieren eines SMS-Gateways auf Add und dann auf SMS Gateway.
   Das Dialogfeld Add SMS Gateway wird angezeigt.



   Hinweis: XenMobile unterstützt für Textnachrichten nur Nexmo. Wenn Sie noch kein Konto für Nexmo Messaging haben, erstellen Sie eines auf der Nexmo-Website.
8. Konfigurieren Sie die folgenden Einstellungen:
   - Name: Geben Sie den Namen für die SMS-Gatewaykonfiguration ein.
   - Description: Geben Sie optional eine Beschreibung der Konfiguration ein.
   - Key: Geben Sie den numerischen Bezeichner ein, der vom Systemadministrator bereitgestellt wird, wenn das Konto aktiviert wird.
   - Secret: Geben Sie den vom Systemadministrator bereitgestellten Schlüssel ein, mit dem Sie im Fall eines Verlusts oder Diebstahls des Kennworts auf das Konto zugreifen können.
   - Virtual Phone Number: Dieses Feld wird beim Senden an nordamerikanische Telefonnummern (Vorwahl +1) verwendet. Sie müssen eine virtuelle Nexmo-Telefonnummer oder einen aussagekräftigen Namen eingeben. Sie können virtuelle Telefonnummern auf der Nexmo-Website erwerben.
   - HTTPS: Wählen Sie diese Option, wenn Sie für die Übermittlung von SMS-Anforderungen an Nexmo HTTPS verwenden möchten.
   - Country Code: Klicken Sie in der Liste auf die Standard-SMS-Ländervorwahl für Empfänger in Ihrem Unternehmen.

Dieses Feld beginnt immer mit +.

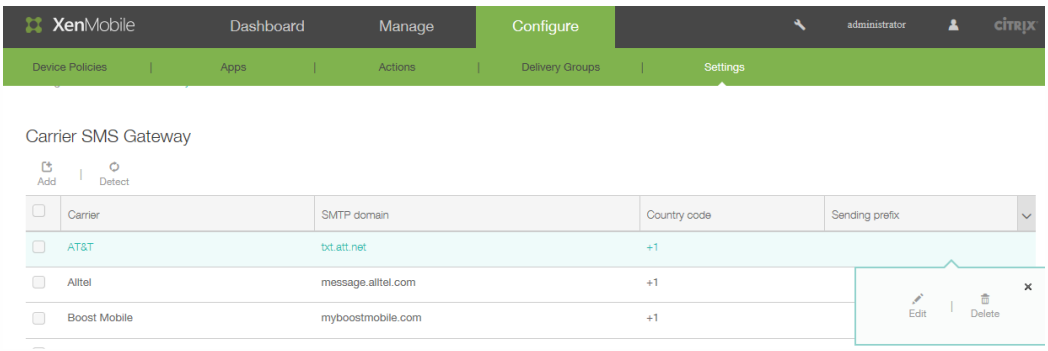
- Test Configuration: Hiermit können Sie eine Nachricht zum Testen der aktuellen Konfiguration senden. Verbindungsfehler werden erkannt und sofort angezeigt (z. B. Fehler bei der Authentifizierung oder virtuellen Telefonnummern). Die Übermittlung von Nachrichten dauert ungefähr so lange wie bei Mobiltelefonen.

9. Klicken Sie auf Add.

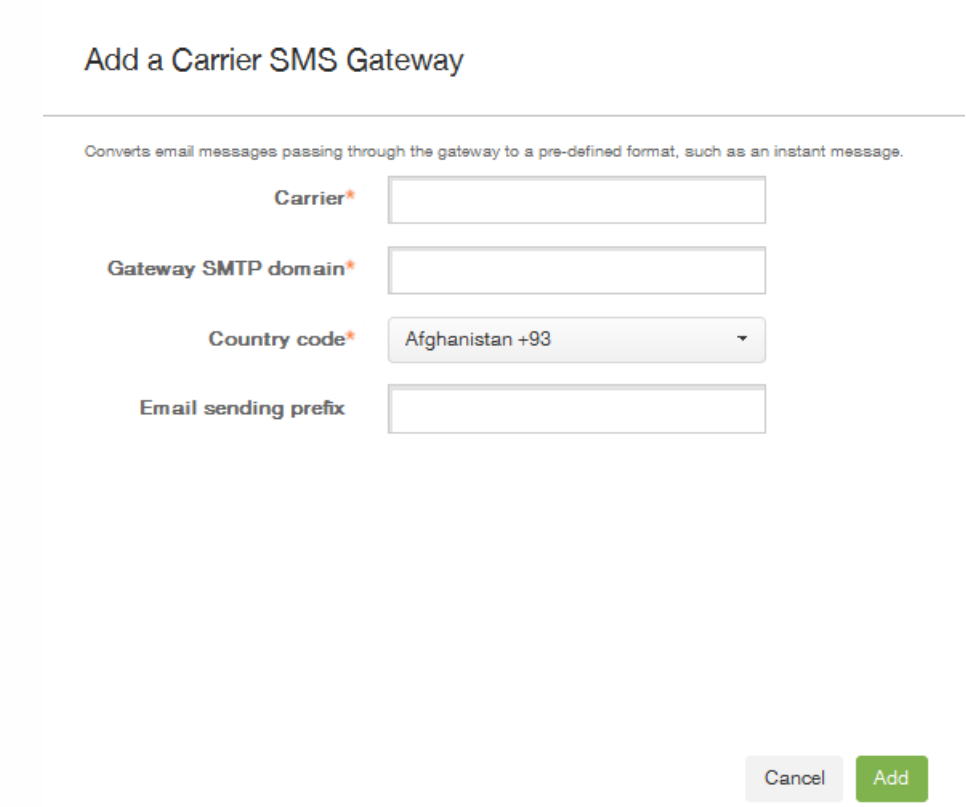
So fügen Sie ein Netzbetreiber-SMS-Gateway hinzu

Sie können ein Netzbetreiber-SMS-Gateway in XenMobile einrichten, um Benachrichtigungen zu konfigurieren, die über das SMS-Gateway eines Netzbetreibers gesendet werden. Netzbetreiber nutzen SMS-Gateways für den Versand oder Empfang von Textnachrichten an bzw. von einem Telekommunikationsnetz. Standardisierte Kommunikationsprotokolle werden für den Austausch kurzer Textnachrichten zwischen Festnetz- oder Mobiltelefonen verwendet.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > Carrier SMS Gateway. Die Seite Carrier SMS Gateway wird geöffnet.



2. Klicken Sie auf Add, um einen neuen Netzbetreiber hinzuzufügen. Klicken Sie auf Detect, um automatisch ein Gateway zu ermitteln. Das Dialogfeld Add a Carrier SMS Gateway wird angezeigt.



3. Geben Sie die folgenden Informationen ein: XenMobile unterstützt für Textnachrichten nur Nexmo. Wenn Sie noch kein Konto für Nexmo Messaging haben, erstellen Sie eines auf der Website.
   1. Carrier: Geben Sie den Namen des Netzbetreibers ein.
   2. Gateway SMTP domain: Geben Sie die dem SMTP-Gateway zugeordnete Domäne an.
   3. Country code: Klicken Sie in der Liste auf die Landeskennzahl des Netzbetreibers.
   4. Email sending prefix: Geben Sie optional ein Präfix für den E-Mail-Versand ein.

Zertifikate

Oct 13, 2016

Mit Zertifikaten erstellen Sie in XenMobile sichere Verbindungen und authentifizieren Benutzer.

Standardmäßig umfasst XenMobile ein selbstsigniertes SSL-Zertifikat (Secure Socket Layer), das während der Installation zum Sichern der Kommunikation mit dem Server generiert wird. Citrix empfiehlt, dass Sie das SSL-Zertifikat durch ein vertrauenswürdiges SSL-Zertifikat von einer allgemein bekannten Zertifizierungsstelle (ZS) ersetzen.

XenMobile verwendet zudem den eigenen PKI-Dienst bzw. ruft Zertifikate von der Zertifizierungsstelle (ZS) für Clientzertifikate ab. Alle Citrix Produkte unterstützen Platzhalter- und SAN-Zertifikate (Subject Alternative Name). Für die meisten Bereitstellungen genügen zwei Platzhalter- bzw. SAN-Zertifikate.

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. Schrittweise Anleitungen finden Sie unter Anfordern eines APNs-Zertifikats.

In der folgenden Tabelle werden Format und Typ des Zertifikats für jede XenMobile-Komponente aufgeführt:

XenMobile-Komponente	**Zertifikatformat**	**Erforderlicher Zertifikattyp**
NetScaler Gateway	PEM (BASE64) PFX (PKCS#12)	SSL, Stamm NetScaler Gateway konvertiert PFX automatisch in PEM.
XenMobile-Server	PEM oder PFX (PKCS#12)	SSL, SAML, APNs XenMobile generiert außerdem eine vollständige PKI während der Installation. XenMobile-Server unterstützt keine Zertifikate mit der Erweiterung .pem. Erstellen Sie aus einer PEM-Datei mit dem Befehl "openssl" eine PFX-Datei: openssl pkcs12 -export -out certificate.pfx -in certificate.pem
StoreFront	PFX (PKCS#12)	SSL, Stamm

XenMobile unterstützt SSL Listener- und Clientzertifikate einer Bitlänge von 4096, 2048 und 1024. Hinweis: 1024-Bit-Zertifikate lassen sich leicht manipulieren.

Für NetScaler Gateway und den XenMobile-Server empfiehlt Citrix das Abrufen von Serverzertifikaten von einer öffentlichen Zertifizierungsstelle, z. B. VeriSign, DigiCert oder Thawte. Sie können eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) mit dem NetScaler Gateway- oder dem XenMobile-Konfigurationsprogramm erstellen. Übermitteln Sie die CSR dann zum Signieren an die Zertifizierungsstelle. Wenn die Zertifizierungsstelle das signierte Zertifikat zurückgesendet hat, können Sie es unter NetScaler Gateway oder XenMobile installieren.

Konfigurieren von Clientzertifikaten für die Authentifizierung

NetScaler Gateway unterstützt die Verwendung von Clientzertifikaten für die Authentifizierung. Benutzer, die sich bei NetScaler Gateway anmelden, können auch anhand der Attribute des Clientzertifikats authentifiziert werden, das dem virtuellen Server präsentiert wird. Die Clientzertifikatauthentifizierung kann zusammen mit einem anderen Authentifizierungstyp (z. B. LDAP oder RADIUS) verwendet werden, um eine Zweifaktorauthentifizierung bereitzustellen.

Um Benutzer basierend auf Clientzertifikatattributen zu authentifizieren, sollte die Clientauthentifizierung auf dem virtuellen Server aktiviert sein und das Clientzertifikat angefordert werden. Sie müssen ein Stammzertifikat an den virtuellen Server von NetScaler Gateway binden.

Geräteauthentifizierung mit NetScaler Gateway wird nicht für Zertifikate unterstützt, die über eine eigenverwaltete Zertifizierungsstelle abgerufen wurden.

Wenn sich Benutzer bei NetScaler Gateway anmelden, wird der Benutzername nach der Authentifizierung aus dem angegebenen Feld des Zertifikats extrahiert. Üblicherweise ist es das Feld "Subject:CN". Wurde der Benutzername erfolgreich extrahiert, wird der Benutzer authentifiziert. Wenn der Benutzer kein gültiges Zertifikat während des SSL-Handshakes vorlegt oder wenn der Benutzernamen nicht extrahiert werden kann, schlägt die Authentifizierung fehl.

Sie können Benutzer anhand des Clientzertifikats authentifizieren, indem Sie für den Standardauthentifizierungstyp die Verwendung des Clientzertifikats angeben. Sie können auch eine Zertifikataktion erstellen, mit der Sie definieren, was während der Authentifizierung basierend auf einem Client-SSL-Zertifikat geschehen soll.

XenMobile PKI

Das Feature zur Integration der Public Key-Infrastruktur (PKI) von XenMobile ermöglicht die Verwaltung der Verteilung und des Lebenszyklus von Sicherheitszertifikaten auf den Geräten.

XenMobile erstellt während der Installation eine interne PKI für die Geräteauthentifizierung.

Zudem können externe PKIs für die Ausstellung von Gerätezertifikaten zur Verwendung in Konfigurationsrichtlinien oder für die Clientauthentifizierung bei NetScaler Gateway eingesetzt werden.

Hauptkomponente des PKI-Systems ist die PKI-Entität. Eine PKI-Entität modelliert eine Back-End-Komponente für PKI-Vorgänge. Diese Komponente ist Teil der Unternehmensinfrastruktur, z. B. einer Microsoft-, RSA-, Entrust-, Symantex- oder OpenTrust-PKI. Die PKI-Entität wickelt die Back-End-Zertifikatausstellung und -sperrung ab. Die PKI-Entität ist die autoritative Quelle für den Zertifikatstatus. Die XenMobile-Konfiguration enthält normalerweise eine PKI-Entität pro Back-End-PKI-Komponente.

Die zweite Komponente des PKI-Systems ist der Anmeldeinformationsanbieter. Ein Anmeldeinformationsanbieter ist eine bestimmte Konfiguration von Zertifikatausstellung und -lebenszyklus. Der Anmeldeinformationsanbieter steuert u. a. das Format des Zertifikats (Antragsteller, Schlüssel, Algorithmen) und ggf. die Bedingungen für die Verlängerung und Sperrung. Der Anmeldeinformationsanbieter delegiert Vorgänge an die PKI-Entitäten. Der Anmeldeinformationsanbieter steuert also, wann und mit welchen Daten PKI-Vorgänge durchgeführt werden, während PKI-Entitäten die Art und Weise der Durchführung solcher Vorgänge steuern. Die XenMobile-Konfiguration enthält normalerweise viele Anmeldeinformationsanbieter pro PKI-Entität.

XenMobile-Zertifikatverwaltung

Es empfiehlt sich, die in der XenMobile-Bereitstellung verwendeten Zertifikate, insbesondere die Ablaufdaten und Kennwörter zu überwachen. In diesem Abschnitt finden Sie Tipps, um Ihnen die Zertifikatverwaltung in XenMobile zu

erleichtern.

Ihre Umgebung enthält möglicherweise einige oder alle der folgenden Zertifikate:

XenMobile-Server
SSL-Zertifikat für MDM FQDN
SAML-Zertifikat (für ShareFile)
Stamm- und Zwischenzertifikate für die zuvor genannten Zertifikate und andere interne Ressourcen (StoreFront, Proxy usw.)
APNs-Zertifikat für iOS-Geräteverwaltung
Internes APNs-Zertifikat für Benachrichtigungen von XMS an Worx Home
PKI-Benutzerzertifikat für die Verbindung mit der PKI

MDX Toolkit
Apple Entwicklerzertifikat
Apple Provisioningprofil (pro Anwendung)
Apple APNs-Zertifikat (für WorxMail)
Android-Schlüsselspeicherdatei
Windows Phone – Symantec-Zertifikat

NetScaler
SSL-Zertifikat für MDM FQDN
SSL-Zertifikat für Gateway FQDN
SSL-Zertifikat für ShareFile SZC FQDN
SSL-Zertifikat für Exchange-Lastausgleich (bei konfiguriertem Offload)
SSL-Zertifikat für StoreFront-Lastausgleich
Zertifikate der Stamm- und Zwischenzertifizierungsstellen für die zuvor aufgeführten Zertifikate

Ablaufrichtlinie für Zertifikate in XenMobile

Wenn ein Zertifikat abläuft, wird das Zertifikat ungültig und Sie können in Ihrer Umgebung keine sicheren Transaktionen mehr ausführen und nicht mehr auf XenMobile-Ressourcen zugreifen.

> **Hinweis**
>
> Die Zertifizierungsstelle fordert Sie auf, das SSL-Zertifikat zu erneuern, bevor es abläuft.

APNs-Zertifikat für WorxMail

Die Zertifikate für den Apple Dienst für Push-Benachrichtigungen (APNs) laufen jährlich ab, daher sollten Sie ein neues APNs-SSL-Zertifikat erstellen und im Citrix Portal aktualisieren, bevor das Zertifikat abläuft. Wenn das Zertifikat abläuft, treten Inkonsistenzen bei den WorxMail-Pushbenachrichtigungen für Benutzer auf. Sie können zudem keine Pushbenachrichtigungen für Ihre Apps senden.

APNs-Zertifikat für iOS-Geräteverwaltung

Zum Registrieren und Verwalten von iOS-Geräten mit XenMobile müssen Sie ein APNs-Zertifikat von Apple erstellen und einrichten. Wenn das Zertifikat abläuft, können Benutzer sich nicht bei XenMobile registrieren und Sie können die iOS-

Geräte der Benutzer nicht verwalten. Einzelheiten finden Sie unter Anfordern eines APNs-Zertifikats.

Sie können den Status und das Ablaufdatum des APNs-Zertifikats anzeigen, indem Sie sich am Apple Push Certificates Portal anmelden. Melden Sie sich als der Benutzer an, der das Zertifikat erstellt hat.

Zudem erhalten Sie 30 und 10 Tage vor dem Ablaufdatum eine E-Mail-Benachrichtigung von Apple mit folgenden Informationen:

"The following Apple Push Notification Service certificate, created for AppleID CustomersID will expire on Date. Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

Please contact your vendor to generate a new request (a signed CSR), then visit https://identity.apple.com/pushcert to renew your Apple Push Notification Service certificate.

Thank You,

Apple Push Notification Service"

MDX Toolkit (iOS-Verteilungszertifikat)

Abgesehen von Apps aus dem Apple App Store müssen alle Apps, die auf einem physischen iOS-Gerät ausgeführt werden, mit einem Provisioningprofil und einem entsprechenden Verteilungszertifikat signiert sein.

Ein vorhandenes iOS Developer for Enterprise-Zertifikat oder Provisioningprofil ist eventuell nicht mit 9 kompatibel. Weitere Informationen finden Sie unter "Umschließen von Worx-Apps für iOS 9".

Mit den folgenden Schritten stellen Sie sicher, dass Sie ein gültiges iOS-Verteilungszertifikat haben:

1. Erstellen Sie über das Apple Enterprise Developer-Portal eine explizite App-ID für jede App, die Sie mit dem MDX Toolkit umschließen möchten. Folgendes ist ein Beispiel für eine zulässige App-ID: com.Firmenname.Produktname.
2. Wählen Sie im Apple Enterprise Developer-Portal **Provisioning Profiles** > **Distribution** und erstellen Sie ein Provisioningprofil zur hausinternen Verwendung. Wiederholen Sie diesen Schritt für jede zuvor erstellte App-ID.
3. Laden Sie alle Provisioningprofile herunter. Weitere Informationen finden Sie unter Umschließen von mobilen iOS-Apps.

Bestätigen Sie mit den folgenden Schritten, dass alle XenMobile-Serverzertifikate gültig sind:

1. Klicken Sie in der XenMobile-Konsole auf **Einstellungen** und dann auf **Zertifikate**.
2. Stellen Sie sicher, dass alle Zertifikate, einschließlich APNs-, SSL Listener-, Root- und Zwischenzertifikate gültig sind.

Android-Schlüsselspeicher

Der Schlüsselspeicher ist eine Datei mit den Zertifikaten zum Signieren der Android-App. Wenn die Gültigkeitsdauer Ihres Schlüssels abläuft, können Benutzer nicht länger problemlose Upgrades auf neue Versionen der App durchführen.

Enterprise-Zertifikat von Symantec für Windows Phones

Symantec ist der exklusive Anbieter von Codesignaturzertifikaten für den Microsoft App Hub-Dienst. Entwickler und Herausgeber von Software registrieren sich bei der App Hub, um Anwendungen für Windows Phone und Xbox 360 zum Download im Windows Marketplace bereitzustellen. Weitere Informationen finden Sie unter Symantec Code Signing Certificates for Windows Phone in der Dokumentation von Symantec.

Wenn das Zertifikat abläuft, können sich Windows Phone-Benutzer nicht registrieren, keine vom Unternehmen

veröffentlichten und signierten Apps installieren und keine Unternehmensapps öffnen, die auf dem Telefon installiert sind.

NetScaler

Informationen zum Handhaben des Zertifikatablaufs für NetScaler finden Sie unter How to handle certificate expiry on NetScaler im Citrix Support Knowledge Center.

Wenn ein NetScaler-Zertifikat abläuft, können Benutzer sich nicht registrieren, nicht auf den Worx Store zugreifen, beim Verwenden von WorxMail können sie keine Verbindung mit Exchange Server herstellen und sie können keine HDX-Apps enumerieren und öffnen (abhängig vom abgelaufenen Zertifikat).

Mit dem Expiry Monitor und Command Center können Sie Ihre NetScaler-Zertifikate überwachen und Sie werden vom Ablaufen eines Zertifikats benachrichtigt. Mit diesen beiden Tools können Sie folgende NetScaler-Zertifikate überwachen:

SSL-Zertifikat für MDM FQDN
SSL-Zertifikat für Gateway FQDN
SSL-Zertifikat für ShareFile SZC FQDN
SSL-Zertifikat für Exchange-Lastausgleich (bei konfiguriertem Offload)
SSL-Zertifikat für StoreFront-Lastausgleich
Zertifikate der Stamm- und Zwischenzertifizierungsstellen für die zuvor aufgeführten Zertifikate

Hochladen von Zertifikaten in XenMobile

May 05, 2016

Zertifikate werden funktional vom XenMobile-Server verwendet. Zertifikate werden in XenMobile über den Bereich Certificates der XenMobile-Konsole hochgeladen. Zu den Zertifikaten gehören Zertifizierungsstellenzertifikate (CA-Zertifikate), Registrierungsstellenzertifikate (RA-Zertifikate) und Zertifikate für die Clientauthentifizierung bei anderen Komponenten der Infrastruktur. Außerdem können Sie den Bereich "Certificates" als Speicherbereich für Zertifikate verwenden, die Sie Geräten bereitstellen möchten. Dies gilt insbesondere für Zertifizierungsstellen, die zur Herstellung einer Vertrauensbeziehung auf dem Gerät verwendet werden.
Jedes hochgeladene Zertifikat erhält einen Eintrag in der Tabelle der Zertifikate mit einer Zusammenfassung seines Inhalts. Wenn Sie Komponenten zur PKI-Integration konfigurieren, die ein Zertifikat erfordern, werden Sie aufgefordert, aus der Liste der Serverzertifikate eine Auswahl zu treffen, die die kontextabhängigen Kriterien erfüllt. Beispiel: Sie konfigurieren die Integration von XenMobile in Ihrer Microsoft-Zertifizierungsstelle. Die Verbindung mit der Microsoft-Zertifizierungsstelle erfordert eine Authentifizierung mit einem Clientzertifikat.

Anforderungen an private Schlüssel

XenMobile kann den privaten Schlüssel für ein bestimmtes Zertifikat haben oder auch nicht. Analog erfordert XenMobile einen privaten Schlüssel für hochgeladene Zertifikate oder auch nicht.

Hochladen von Zertifikaten in die Konsole

Sie können das CA-Zertifikat ohne privaten Schlüssel hochladen, das die Zertifizierungsstelle zum Signieren von Anforderungen verwenden soll, und ein SSL-Clientzertifikat mit privatem Schlüssel für die Clientauthentifizierung. Wenn Sie die Entität der Microsoft-Zertifizierungsstelle konfigurieren, müssen Sie das Zertifizierungsstellenzertifikat angeben. Dieses können Sie dann aus der Liste mit allen Serverzertifikaten, die CA-Zertifikate sind, auswählen. Analog können Sie bei der Konfiguration der Clientauthentifizierung aus einer Liste mit allen Serverzertifikaten auswählen, für die XenMobile den privaten Schlüssel hat.

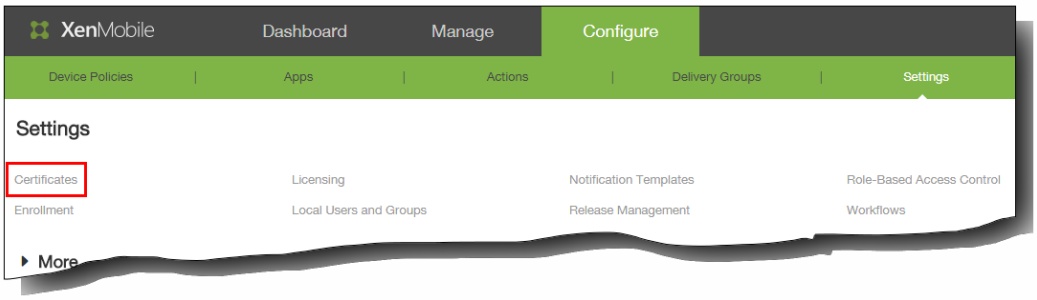
XenMobile unterstützt die folgenden Eingabeformate für Zertifikate:

- PEM- oder DER-codierte Zertifikatdateien
- PEM- oder DER-codierte Zertifikatdateien mit zugehöriger PEM- oder DER-codierter privater Schlüsseldatei
- PKCS#12-Schlüsselspeicher (P12, unter Windows auch PFX)

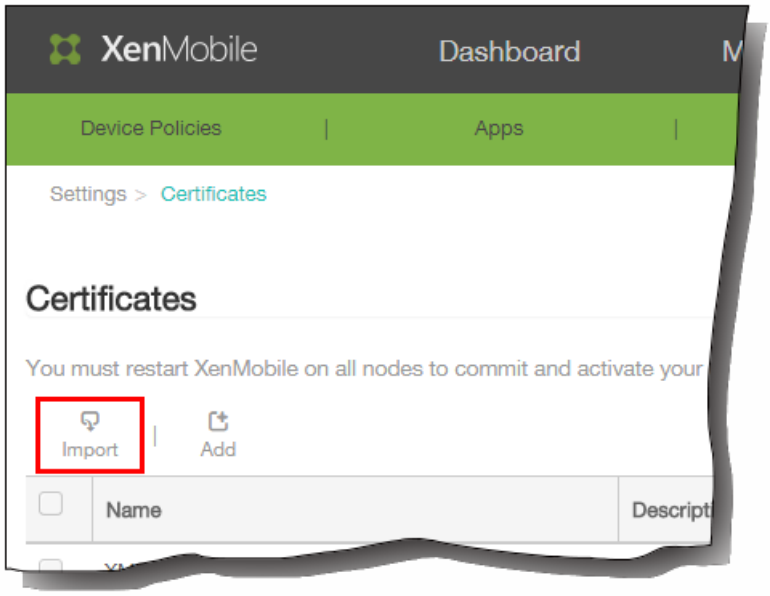
Importieren eines Schlüsselspeichers

Schlüsselspeicher können mehrere Einträge enthalten. Beim Laden aus einem Schlüsselspeicher werden Sie aufgefordert, das Alias des gewünschten Eintrags anzugeben. Wenn Sie kein Alias angeben, wird der erste Eintrag aus dem Speicher geladen. Da PKCS#12-Dateien normalerweise nur einen Eintrag enthalten, wird das Aliasfeld nicht angezeigt, wenn Sie PKCS#12 als Schlüsselspeichertyp auswählen.

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

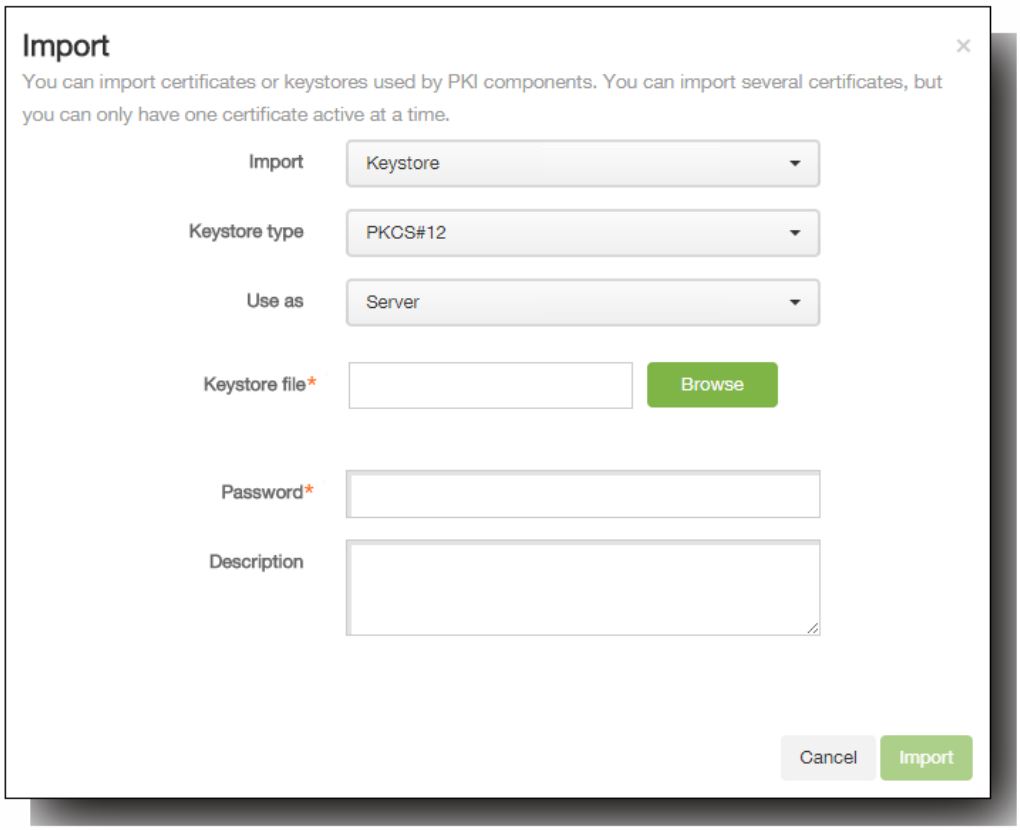


2. Klicken Sie auf der Seite Certificates auf Import.



Das Dialogfeld Import wird angezeigt.

3. Klicken Sie im Dialogfeld Import für Import auf Keystore.



Das Dialogfeld Import ändert sich und enthält nun die verfügbaren Schlüsselspeicheroptionen (Beispiel siehe Abbildung oben).

4. Klicken Sie für Keystore type auf PKCS#12.
5. Wählen Sie unter Use as aus, wie Sie den Schlüsselspeicher verwenden möchten. Es gibt folgende Optionen:
   - **Server**: Serverzertifikate sind Zertifikate, die funktional vom XenMobile-Server verwendet werden und in die XenMobile-Konsole hochgeladen werden. Sie umfassen CA-Zertifikate, RA-Zertifikate und Zertifikate für die Clientauthentifizierung bei anderen Komponenten der Infrastruktur. Außerdem können Sie Serverzertifikate als Speicher für Zertifikate verwenden, die Sie Geräten bereitstellen möchten. Dies gilt insbesondere für Zertifizierungsstellen, die zur Herstellung einer Vertrauensbeziehung auf dem Gerät verwendet werden.
   - **SAML**: Mit der SAML-Zertifizierung (Security Assertion Markup Language) können Sie Single Sign-On (SSO) auf Servern, Websites und für Apps bereitstellen.
   - **APNs**: APNs-Zertifikate (Apple Dienst für Pushbenachrichtigungen) ermöglichen die Mobilgeräteverwaltung über das Apple Push-Netzwerk.
   - **SSL Listener**: Der Secure Sockets Layer-Listener benachrichtigt XenMobile über SSL-Kryptografieaktivitäten.
6. Navigieren Sie zu dem Schlüsselspeicher, den Sie importieren möchten.
7. Geben Sie unter Password das Kennwort für das Zertifikat ein.
8. Geben Sie optional eine Beschreibung für den Schlüsselspeicher ein, anhand derer Sie diesen von anderen Schlüsselspeichern unterscheiden können.
9. Klicken Sie auf Import. Der Schlüsselspeicher wird der Zertifikattabelle hinzugefügt.

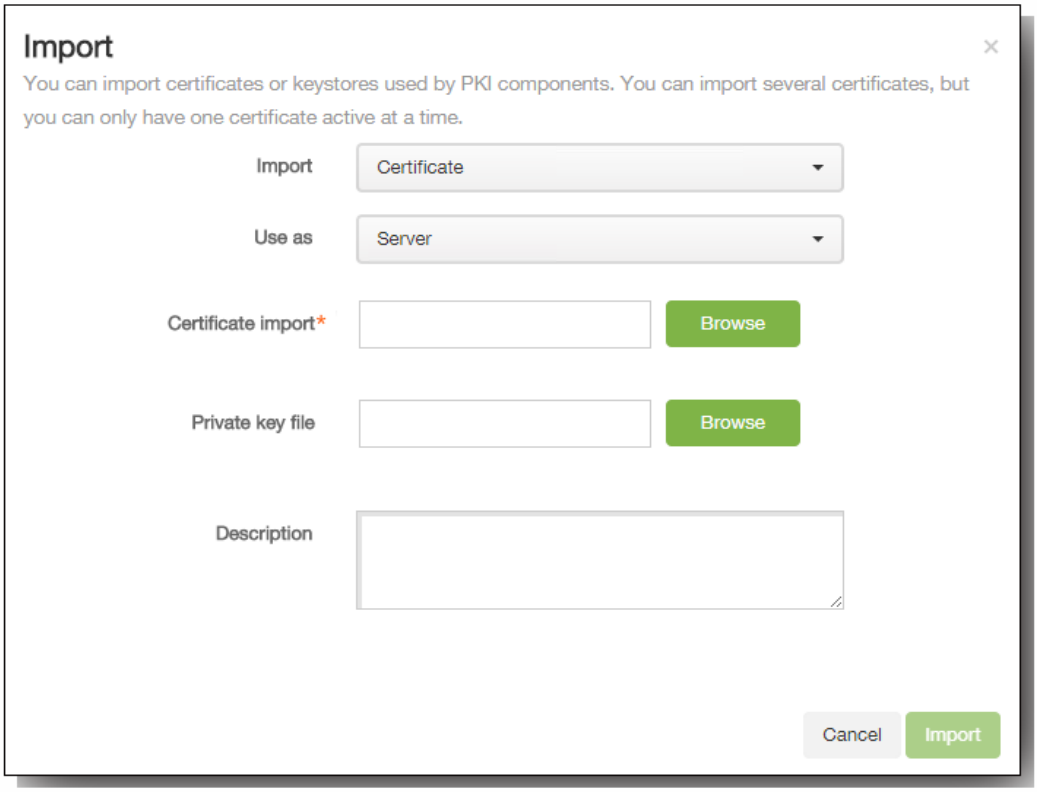
So importieren Sie ein Zertifikat

Beim Importieren eines Zertifikats aus einer Datei oder einem Schlüsselspeichereintrag versucht XenMobile die Erstellung einer Zertifikatkette und importiert alle Zertifikate in der Kette (wobei für jedes ein Serverzertifikateintrag erstellt wird). Dies

funktioniert nur, wenn die Zertifikate in der Datei oder dem Schlüsselspeichereintrag tatsächlich eine Kette bilden, z. B. wenn jedes folgende Zertifikat in der Kette Aussteller des vorherigen Zertifikats ist.

Zum Zweck der Heuristik können Sie optional eine Beschreibung für die importierten Zertifikate eingeben. Die Beschreibung wird nur dem ersten Zertifikat in der Kette angefügt. Sie können die Beschreibung der verbleibenden Zertifikate später aktualisieren.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Certificates.
2. Klicken Sie auf der Seite Certificates auf Import. Das Dialogfeld Import wird angezeigt.
3. Aktivieren Sie im Dialogfeld Import unter Import die Option Certificate, sofern sie noch nicht aktiviert ist.



Das Dialogfeld Import ändert sich und enthält nun die verfügbaren Zertifikatoptionen.

4. Wählen Sie unter Use as aus, wie Sie den Schlüsselspeicher verwenden möchten. Es gibt folgende Optionen:
   - **Server**: Serverzertifikate sind Zertifikate, die funktional vom XenMobile-Server verwendet werden und in die XenMobile-Konsole hochgeladen werden. Sie umfassen CA-Zertifikate, RA-Zertifikate und Zertifikate für die Clientauthentifizierung bei anderen Komponenten der Infrastruktur. Außerdem können Sie Serverzertifikate als Speicher für Zertifikate verwenden, die Sie Geräten bereitstellen möchten. Dies gilt insbesondere für Zertifizierungsstellen, die zur Herstellung einer Vertrauensbeziehung auf dem Gerät verwendet werden.
   - **SAML**: Mit der SAML-Zertifizierung (Security Assertion Markup Language) können Sie Single Sign-On (SSO) auf Servern, Websites und für Apps bereitstellen.
   - **SSL Listener**: Der Secure Sockets Layer-Listener benachrichtigt XenMobile über SSL-Kryptografieaktivitäten.
5. Navigieren Sie zu dem Zertifikat, das Sie importieren möchten.
6. Navigieren Sie optional zu einer Datei eines privaten Schlüssels für das Zertifikat. Der private Schlüssel wird für die Ver- und Entschlüsselung im Zusammengang mit dem Zertifikat verwendet.
7. Geben Sie optional eine Beschreibung für das Zertifikat ein, anhand derer Sie dieses von anderen Zertifikaten

unterscheiden können.

8. Klicken Sie auf Import. Das Zertifikat wird der Zertifikattabelle hinzugefügt.

Aktualisieren eines Zertifikats

In XenMobile darf nur jeweils ein Zertifikat pro öffentlichem Schlüssel im System vorhanden sein. Wenn Sie versuchen, ein Zertifikat für ein Schlüsselpaar zu importieren, das bereits ein importiertes Zertifikat besitzt, erhalten Sie die Option, den vorhandenen Eintrag zu ersetzen oder zu löschen.

Als bestes Verfahren zur Aktualisierung der Zertifikate klicken Sie in der XenMobile-Konsole auf Configure > Settings > Certificates und importieren Sie im Dialogfeld Import das neue Zertifikat. Wenn Sie ein Serverzertifikat aktualisieren, wechseln Komponenten, die das vorherige Zertifikat verwendet haben, automatisch zu dem neuen. Gleichermaßen wird das Serverzertifikat auf Geräten, auf denen es bereitgestellt ist, bei der nächsten Bereitstellung automatisch aktualisiert.

PKI-Entitäten

May 05, 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.

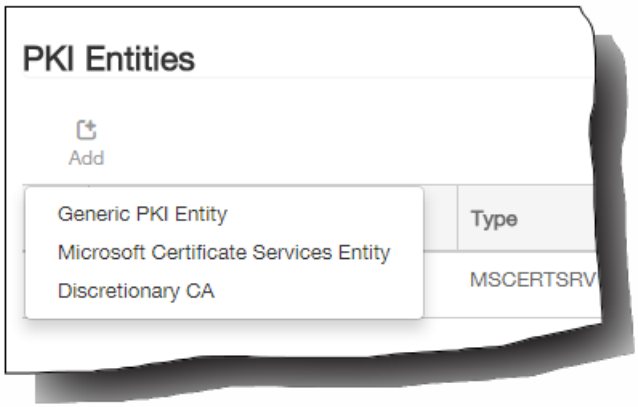
Der GPKI-Adapter veröffentlicht als SOAP-Webdienst-Endpunkt eine selbstbeschreibende WSDL-Definition (Web Services Description Language). Die Erstellung einer GPKI-PKI-Entität besteht in der Bereitstellung dieser WSDL-Definition für XenMobile über eine URL oder durch Hochladen der Datei selbst.

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

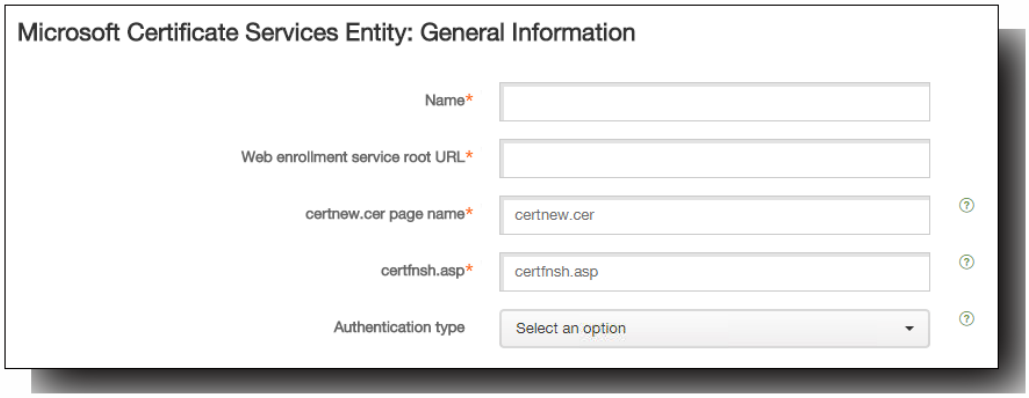
XenMobile interagiert mit Microsoft Zertifikatdiensten über seine Schnittstelle zur Webregistrierung. XenMobile unterstützt nur die Ausstellung neuer Zertifikate über diese Schnittstelle (entspricht der sign-Funktion von GPKI).

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.

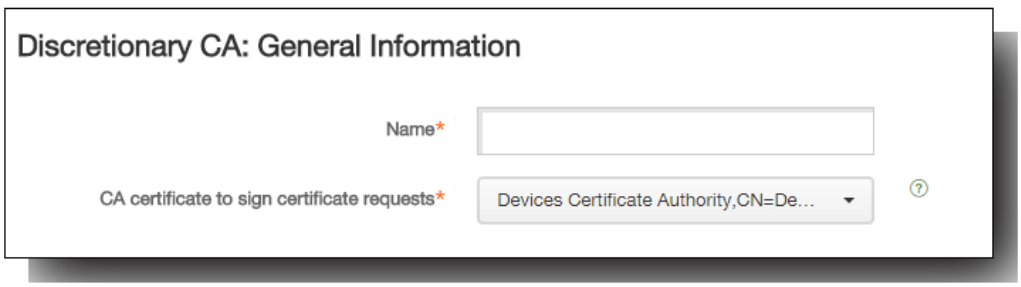
Der OCSP-Responder-Dienst von XenMobile unterstützt einfache OCSP-Antworten und folgende Hashalgorithmen in Anforderungen:

- 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

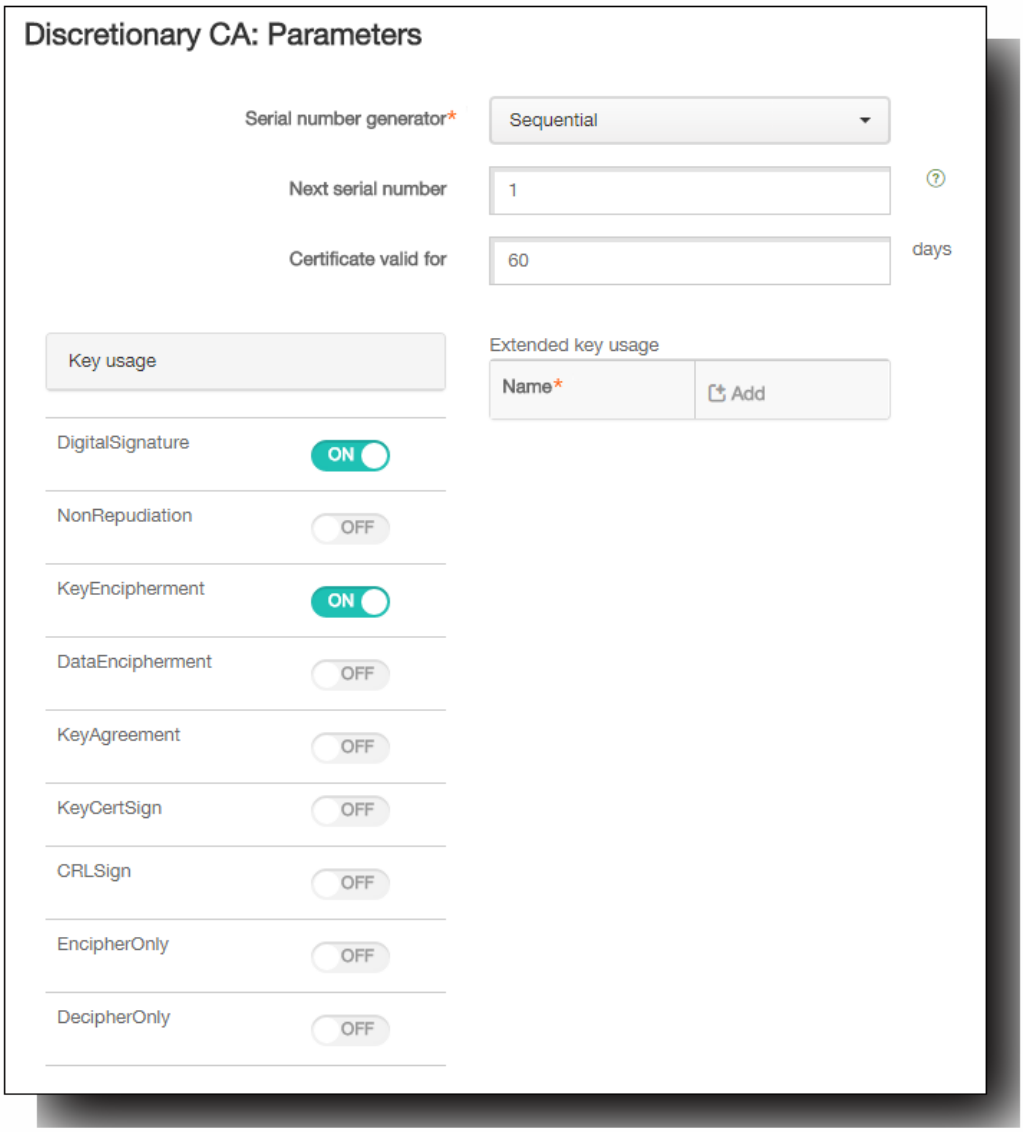
1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > PKI Entities.
2. Klicken Sie auf der Seite PKI Entities auf Add.
   Eine Liste mit den Typen der PKI-Entitäten, die Sie hinzufügen können, wird angezeigt.
3. Klicken Sie auf Discretionary CA.
   Die Seite Discretionary CA: General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

May 05, 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

Kontext	SCEP unterstützt	SCEP erforderlich

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.

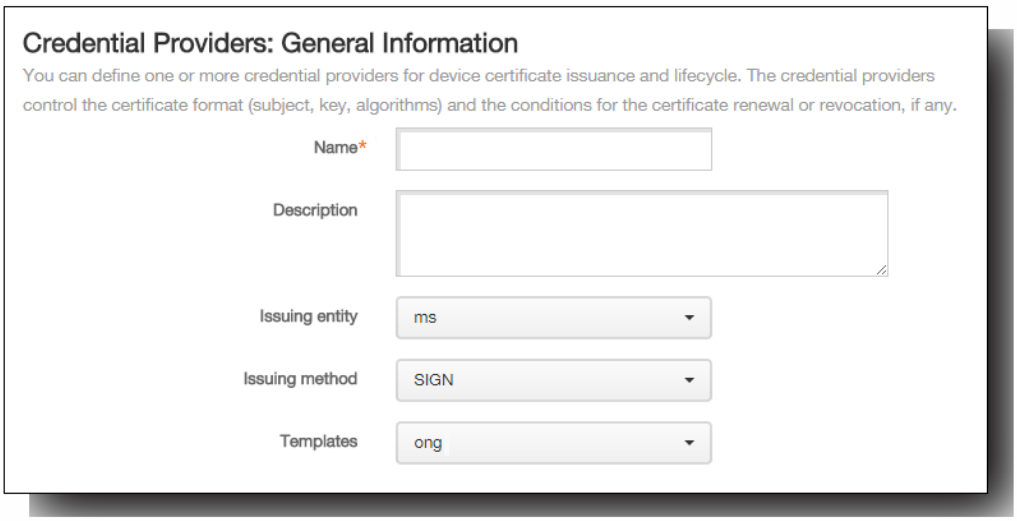
In XenMobile wird vor Sperrung des vorhandenen Zertifikats versucht, das neue Zertifikat abzurufen, um eine Dienstunterbrechung zu vermeiden, wenn die Ausstellung fehlschlägt. Wenn die verteilte (SCEP-unterstützte) Bereitstellung verwendet wird, erfolgt die Sperrung zudem erst, wenn das Zertifikat erfolgreich 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.

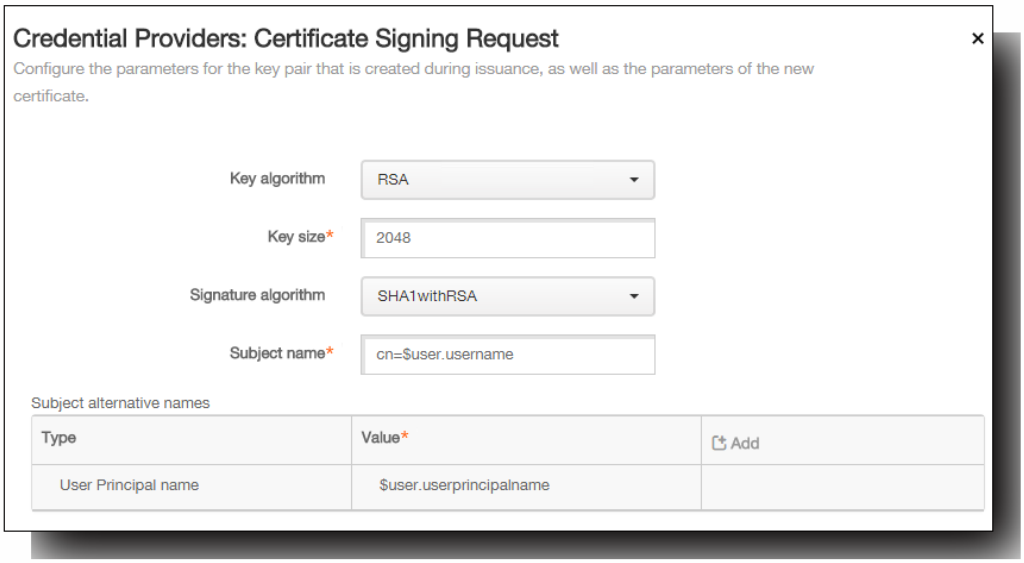
So erstellen Sie einen Anmeldeinformationsanbieter

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.

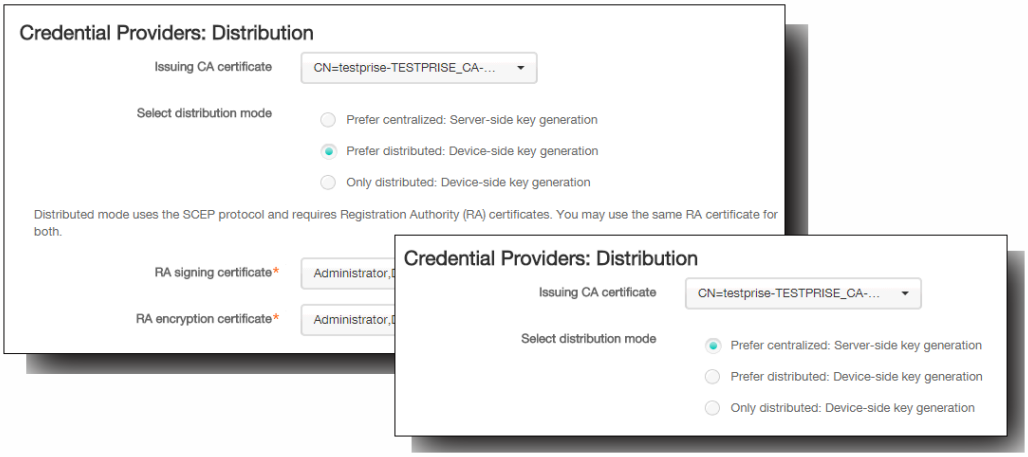


4. Führen Sie auf der Seite Credential Providers: Certificate Signing Request folgende Schritte aus:

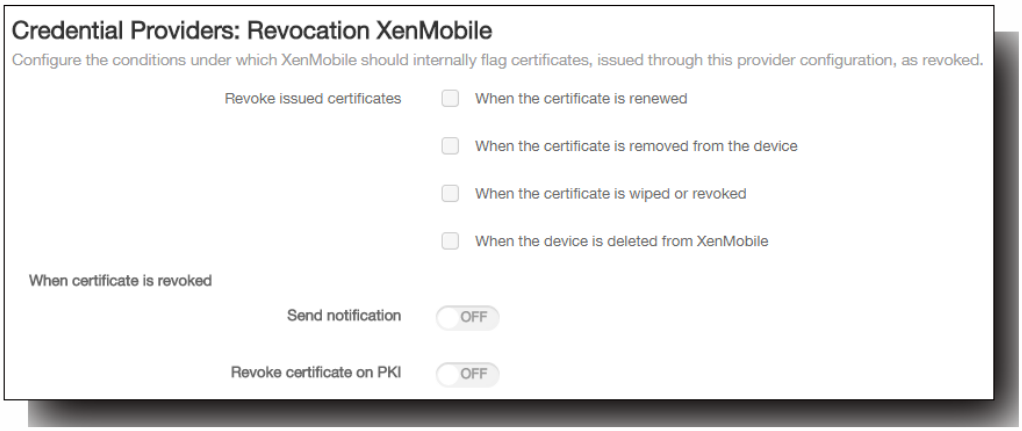
1. Key algorithm: Klicken Sie auf den Schlüsselalgorithmus für das neue Schlüsselpaar. Verfügbare Werte sind RSA, DSA und ECDSA.
2. Key size: Geben Sie Länge des Schlüsselpaars in Bits ein. Dies ist ein Pflichtfeld.
   Hinweis: Welche Werte zulässig sind, hängt von der Art des Schlüssels ab. Die maximale 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.

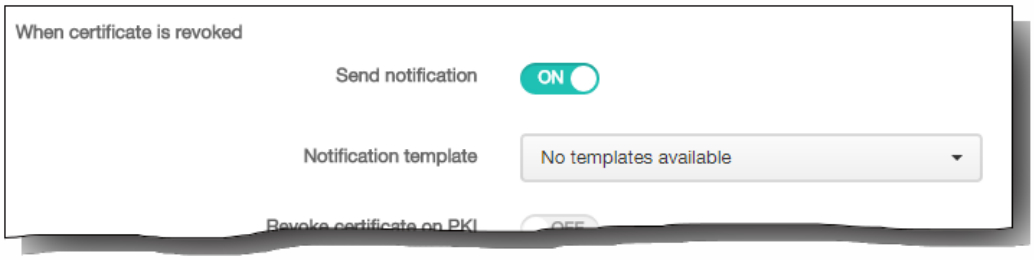
      Bei Auswahl von Prefer distributed: Device-side key generation oder Only distributed: Device-side key generation müssen Sie zusätzlich ein RA-Signaturzertifikat und ein RA-Verschlüsselungszertifikat auswählen. Es werden neue Felder für diese Zertifikate eingeblendet.



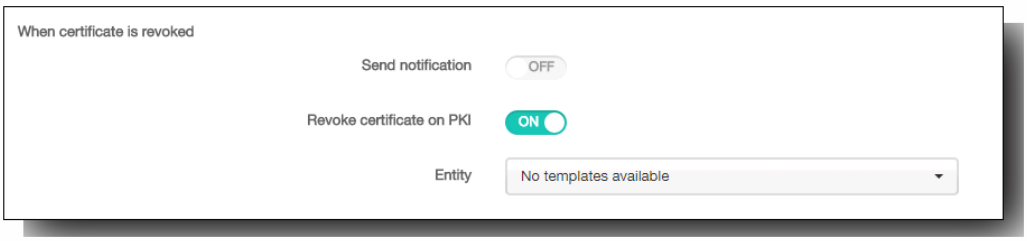
3. Wenn Sie Prefer distributed: Device-side key generation oder Only distributed: Device-side key generation ausgewählt haben, klicken Sie auf das gewünschte RA-Signaturzertifikat und das RA-Verschlüsselungszertifikat. Das gleiche Zertifikat kann für beides verwendet werden.
4. Klicken Sie auf Next.
   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.



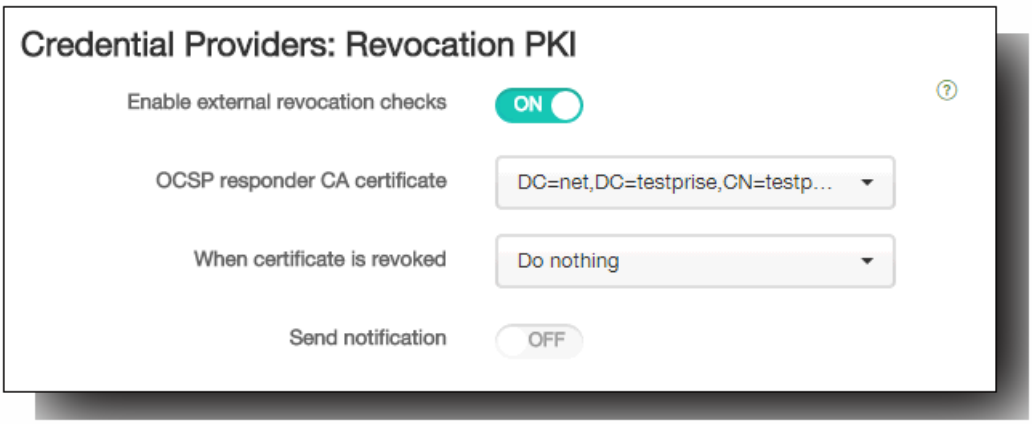
6. Führen Sie auf der Seite Credential Providers: Revocation XenMobile folgende Schritte aus:
   1. Wählen Sie für Revoke issued certificates aus, wann Zertifikate gesperrt werden sollen.
   2. Wenn XenMobile eine Benachrichtigung bei Sperrung des Zertifikats senden soll, legen Sie für Send notification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

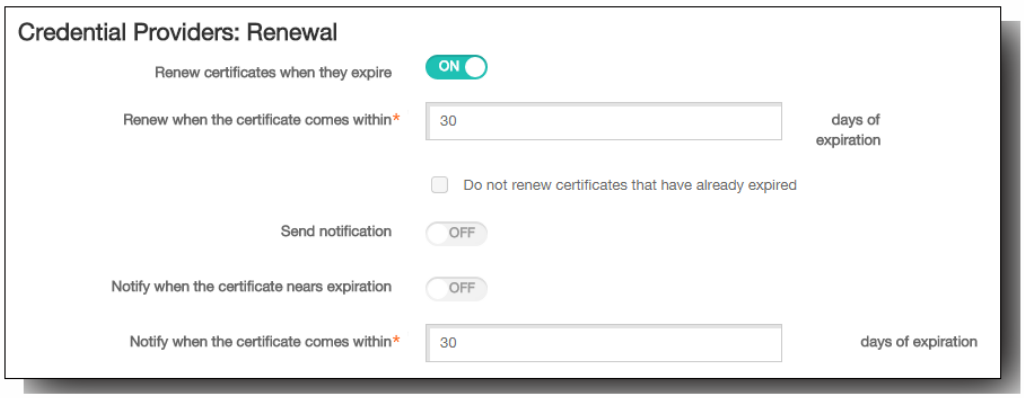


7. Führen Sie auf der Seite Credential Providers: Revocation PKI folgende Schritte aus, wenn Sie Zertifikate über die PKI sperren möchten:
   1. Ändern Sie die Einstellung für Enable external revocation checks in On.
      Zusätzliche Felder für die Sperrung werden angezeigt.
   2. Klicken Sie in der 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 Speichern.
   Der neue Anbieter wird der Tabelle der Anmeldeinformationsanbieter hinzugefügt.

May 05, 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 Sie einen Computer mit Windows Server 2012 R2 oder Windows Server 2008 R2 und Microsoft Internetinformationsdienste (IIS) oder einen Mac-Computer zum Generieren einer Zertifikatsignieranforderung (Certificate Signing Request, CSR).
- Die CSR muss von Citrix signiert werden.
- Fordern Sie ein APNs-Zertifikat bei Apple an.
- 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.

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.

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**.

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.

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.

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.

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.

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 bei 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 **Aktualisieren**.

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.

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.

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 bei der XenMobile-Konsole als Administrator an.
2. Klicken Sie auf **Konfigurieren** > **Einstellungen** > **Zertifikate**.
3. Klicken Sie auf der Seite **Zertifikate** auf **Importieren**. Das Dialogfeld **Importieren** wird angezeigt.
4. Navigieren Sie zu der P12-Datei auf Ihrem Computer.
5. Geben Sie ein Kennwort ein und klicken Sie auf **Importieren**.

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

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 **Konfigurieren** > **Einstellungen** > **Zertifikate**. Ist das Zertifikat abgelaufen, müssen Sie es nicht widerrufen.

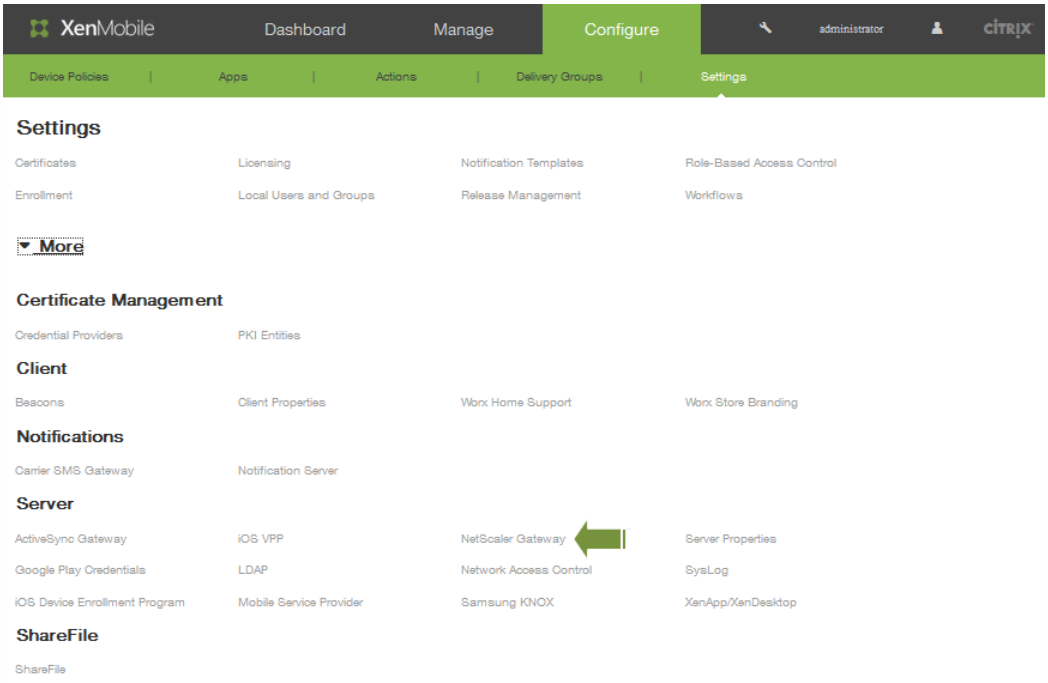
1. Generieren Sie eine Zertifikatsignieranforderung mit Microsoft Internetinformationsdienste (IIS).
2. Laden Sie die neue CSR auf die XenMobile APNs CSR Signing-Website hoch und klicken Sie dann auf **Sign**.
3. Senden Sie die signierte Zertifikatsignieranforderung im Apple Push Certificate Portal an 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 **Konfigurieren** > **Einstellungen** > **Zertifikate** klicken.
7. Importieren Sie das neue Zertifikat im Dialogfeld **Importieren**.

May 05, 2016

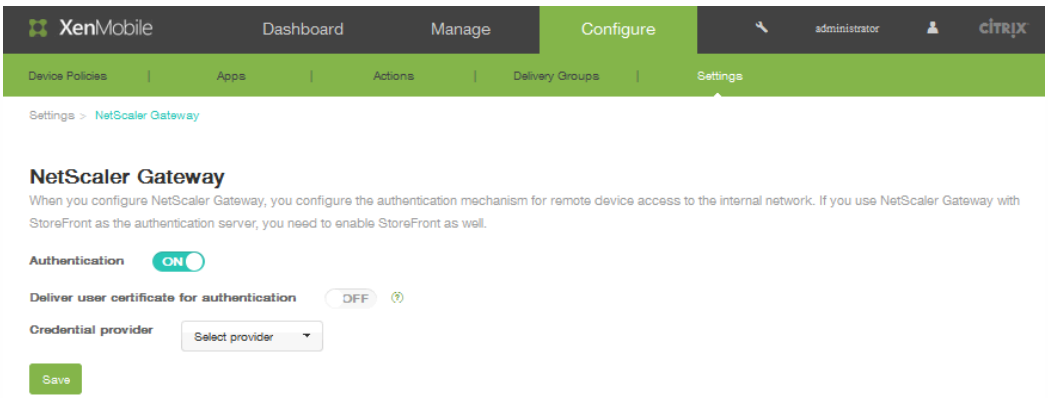
Bei der Konfiguration von NetScaler Gateway mit XenMobile erstellen Sie die Authentifizierungsmethode für den Remote-Gerätezugriff auf das interne Netzwerk. Mit dieser Funktionalität können Apps auf einem Mobilgerät auf Unternehmensserver im Intranet zugreifen, indem ein Micro VPN von den Apps zu NetScaler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

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



2. Legen Sie für Authentication die Einstellung ON fest.

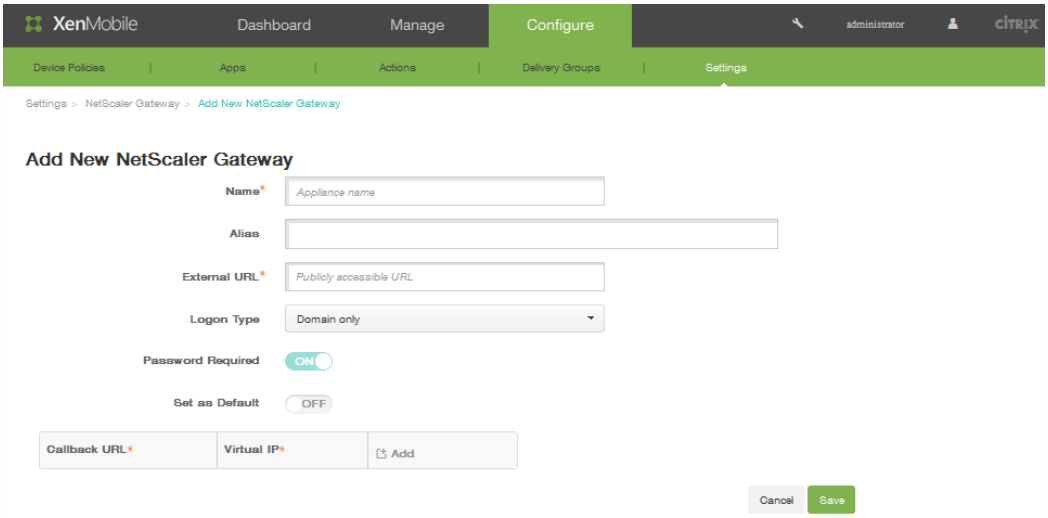


3. Wenn Sie möchten, dass XenMobile das Authentifizierungszertifikat mit Worx Home gemeinsam verwendet, sodass

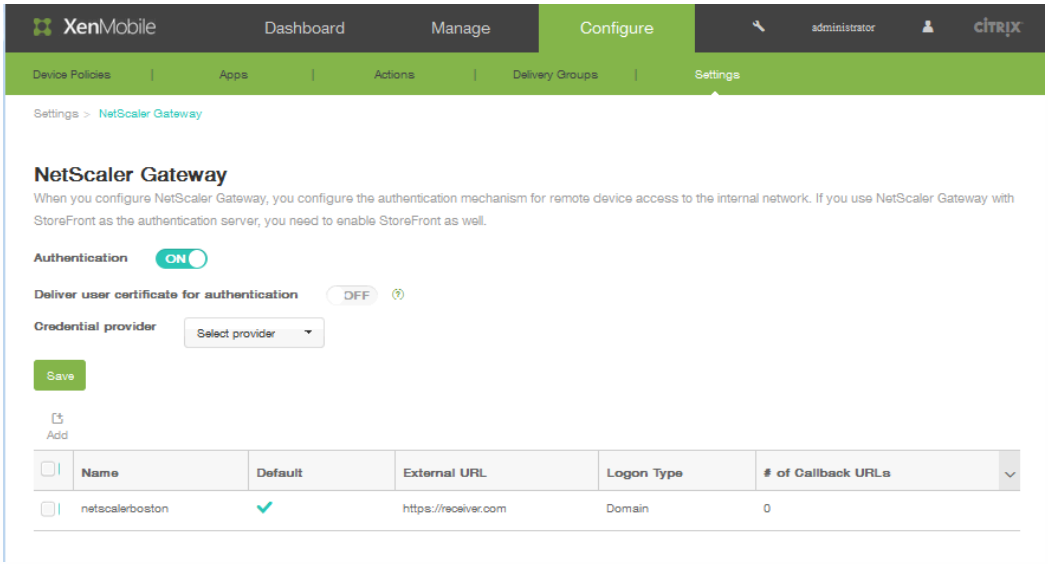
NetScaler Gateway die Clientzertifikatauthentifizierung abwickelt, wählen Sie für Deliver user certificate for authentication die Einstellung ON.

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

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.

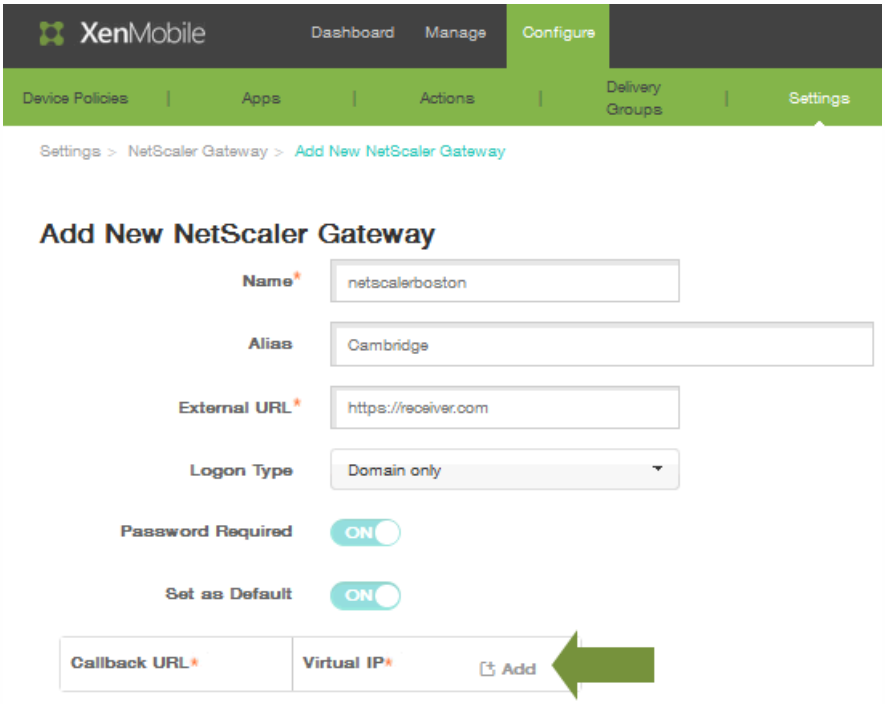


3. Geben Sie unter Name einen Namen für die NetScaler Gateway-Instanz ein.
4. Geben Sie optional unter Alias ein Alias ein.
5. Geben Sie unter External URL die öffentlich zugängliche URL für NetScaler Gateway ein. Beispiel: https://receiver.com.
6. Klicken Sie in der Liste Logon Type auf einen Anmeldetyp. 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. Bei mehreren Domänen funktioniert **Domain only** nicht, verwenden Sie daher **Certificate and domain**. 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 **Speichern**. 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.

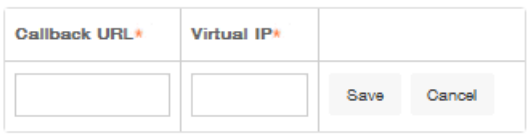


Nach dem Hinzufügen der NetScaler Gateway-Instanz können Sie eine Callback-URL hinzufügen und eine virtuelle IP-Adresse für das NetScaler Gateway VPN angeben. **Hinweis**: Dies ist optional, kann aber für zusätzliche Sicherheit konfiguriert werden, insbesondere dann, wenn der XenMobile-Server in der 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. 4. Geben Sie die virtuelle IP-Adresse für NetScaler Gateway ein und klicken Sie auf **Speichern**.

May 05, 2016

Sie können in XenMobile eine Verbindung mit einem oder mehreren LDAP-kompatiblen Verzeichnissen, z. B. Active Directory, herstellen. 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.

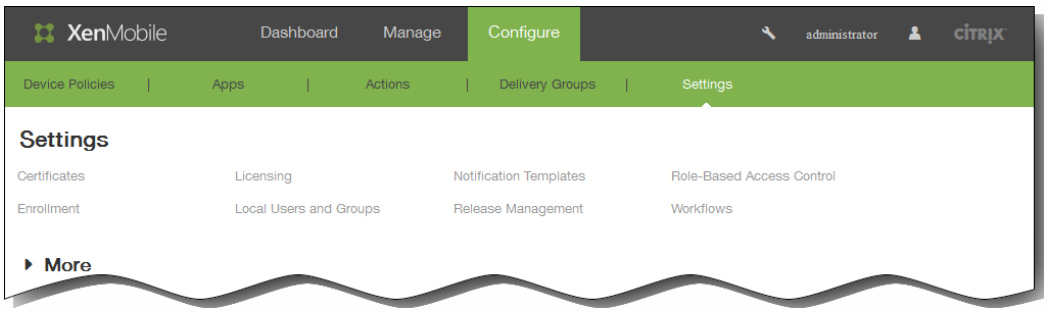
3. Konfigurieren Sie die folgenden Einstellungen:
   - Directory type: Klicken Sie auf den verwendeten Verzeichnistyp. Standardmäßig ist Microsoft Active Directory ausgewählt.
   - Primary server: Geben Sie den für LDAP verwendeten primären Server an. Sie können die IP-Adresse oder den vollqualifizierten 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 Speichern.

May 05, 2016

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



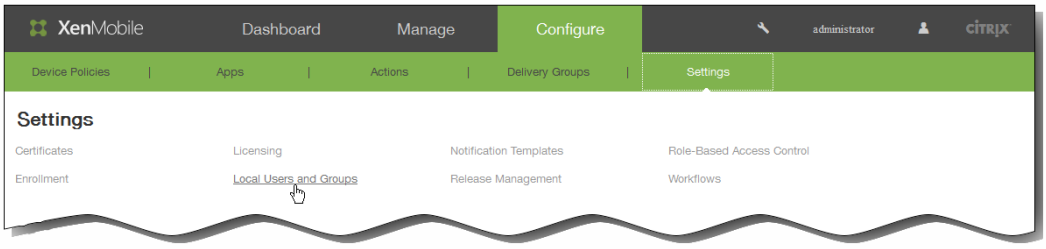
Auf der Seite Settings können Sie folgende Einstellungen ändern:

- 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

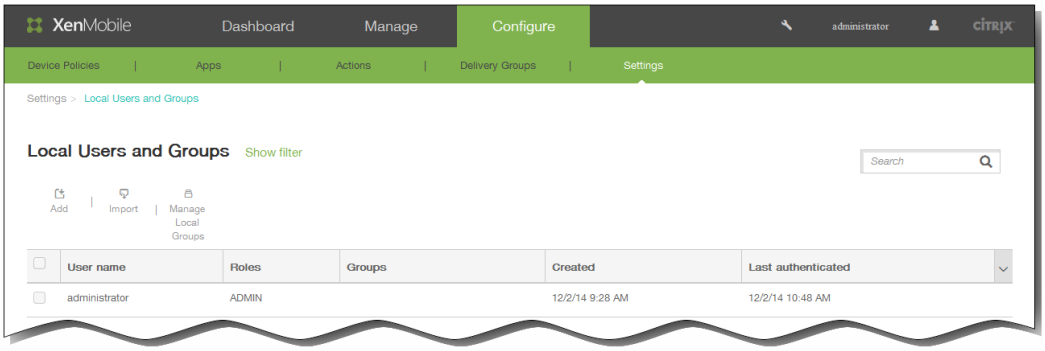
May 05, 2016

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.

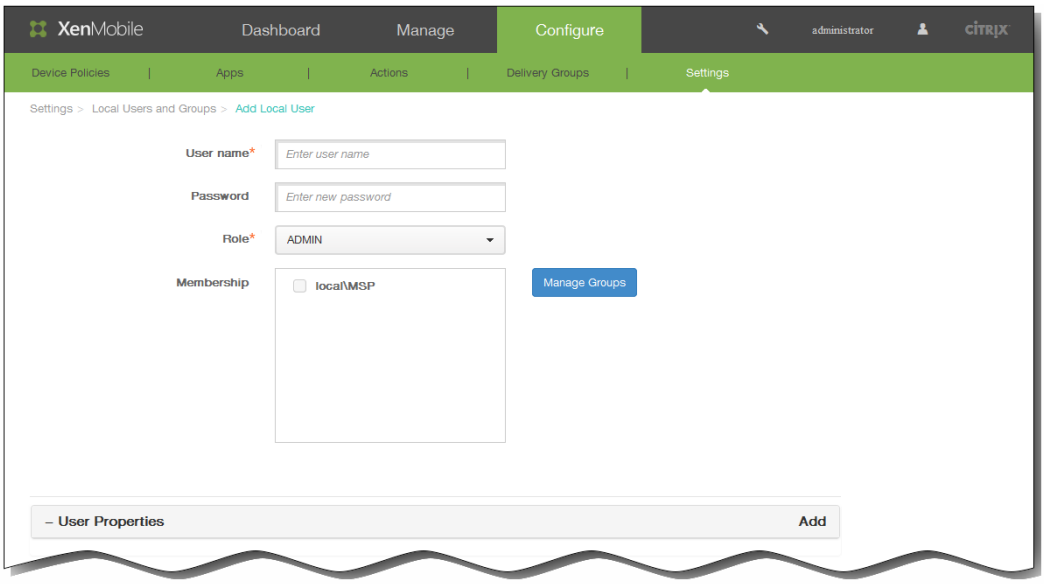


Die Seite Local Users and Groups wird angezeigt.

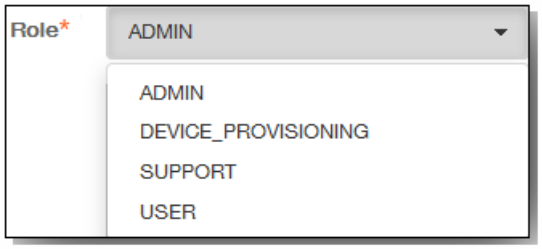


Mit diesem Verfahren werden XenMobile Benutzer einzeln hinzugefügt. Zum Hinzufügen mehrerer Benutzer siehe So importieren Sie Benutzerkonten über eine CSV-Provisioningdatei.

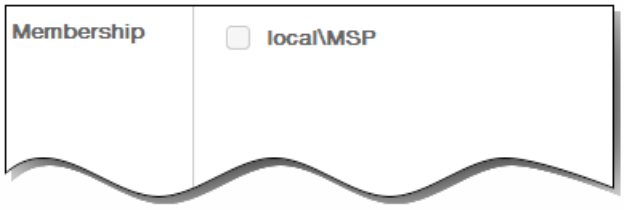
1. Klicken Sie auf der Seite Local Users and Groups auf Add. Die Seite Add Local User wird angezeigt.



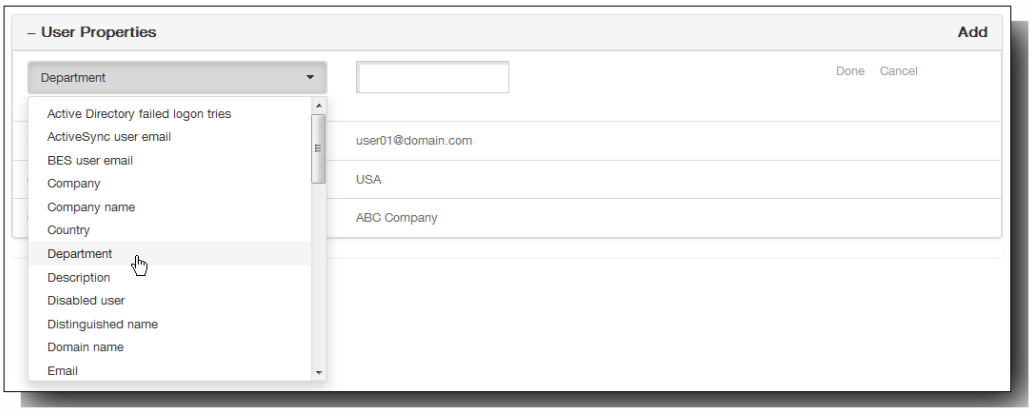
2. Geben Sie zum Hinzufügen des lokalen Benutzers die folgenden Informationen ein:
   1. User name: Geben Sie den Benutzernamen ein. Dies ist ein Pflichtfeld.
   2. Password: Geben Sie ein optionales Benutzerkennwort ein.
   3. Role: Klicken Sie in der Liste Role auf die Rolle des Benutzers. Weitere 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.

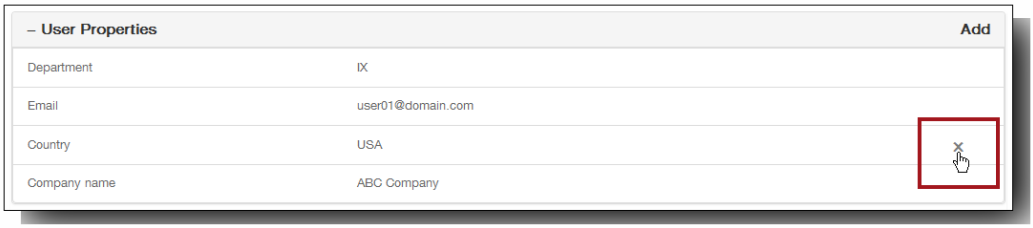


3. Wenn Sie (optional) Eigenschaften hinzufügen möchten, führen Sie die folgenden Schritte aus:
   1. Klicken Sie neben User Properties auf Add.
   2. Klicken Sie in der Liste User Properties auf eine Eigenschaft.
   3. Geben Sie das zugehörige Attribut in das Feld neben der Liste ein.



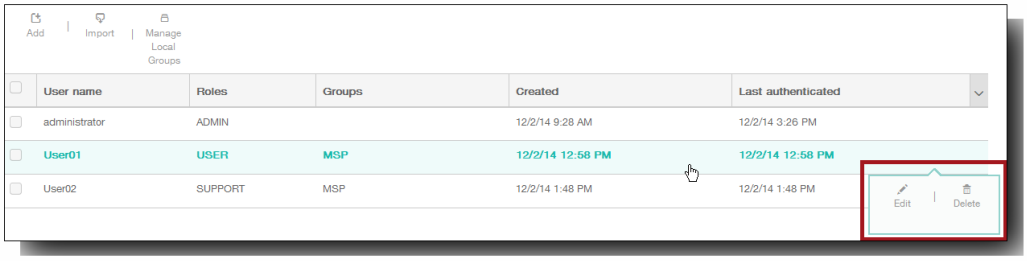
4. Klicken Sie auf Done, um die Eigenschaft zu speichern, oder auf Cancel, um den Vorgang abzubrechen.
5. Wiederholen Sie die Schritte b und c für jede Eigenschaft, die Sie hinzufügen möchten.

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.

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

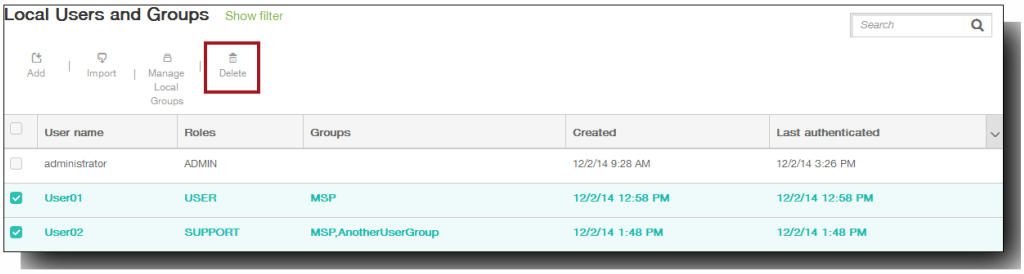


   Die Seite Edit Local User wird angezeigt.
2. Ändern Sie nach Bedarf die folgenden Informationen:
   1. User name: Geben Sie den Benutzernamen ein. Dies ist ein Pflichtfeld.

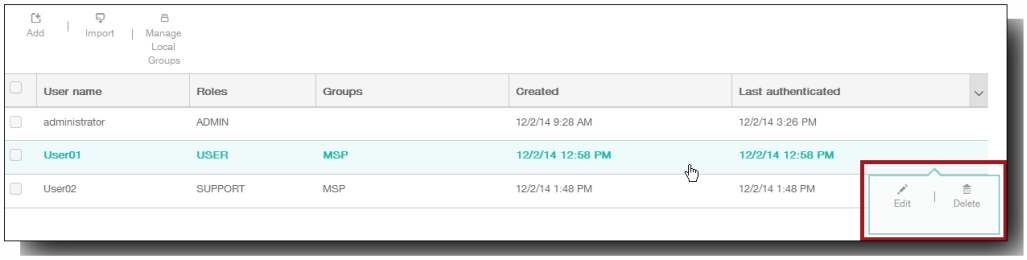
2. Password: Geben Sie ein optionales Benutzerkennwort ein.
3. Role: Klicken Sie in der Liste Role auf die Rolle des Benutzers.
4. Membership: Klicken Sie in der Liste Membership auf die Gruppen, zu denen der Benutzer gehören soll.
5. User properties: Fügen Sie neue Benutzereigenschaften hinzu oder bearbeiten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

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

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.

May 05, 2016

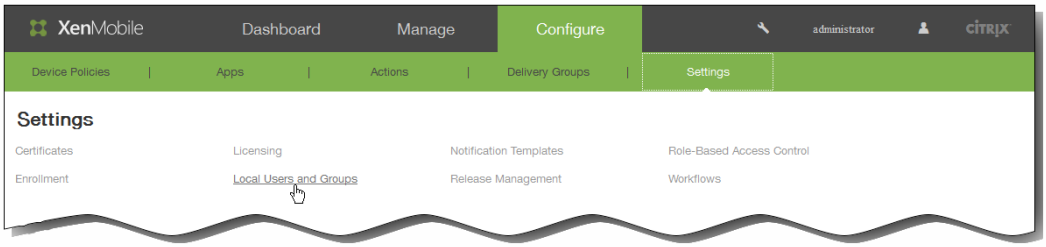
Sie können Benutzerkonten und Eigenschaften aus einer CSV-Datei, einer so genannten Provisioningdatei importieren, die Sie manuell erstellen können. Informationen zur Formatierung von Provisioningdateien finden Sie unter Provisioningdateiformate.

Hinweis:

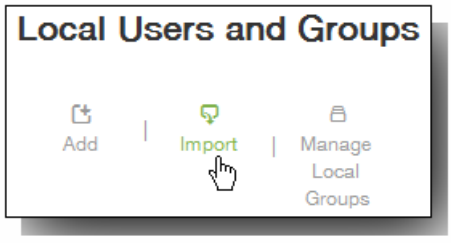
- Wenn Sie Benutzer aus einem LDAP-Verzeichnis importieren, verwenden Sie den Domänennamen zusammen mit dem Benutzernamen in der Importdatei. Beispiel: username@domain.com. Diese Syntax vermeidet zusätzliche Nachschlagevorgänge, die den Import verlangsamen.
- Beim Import von Benutzerkonten in das interne 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.

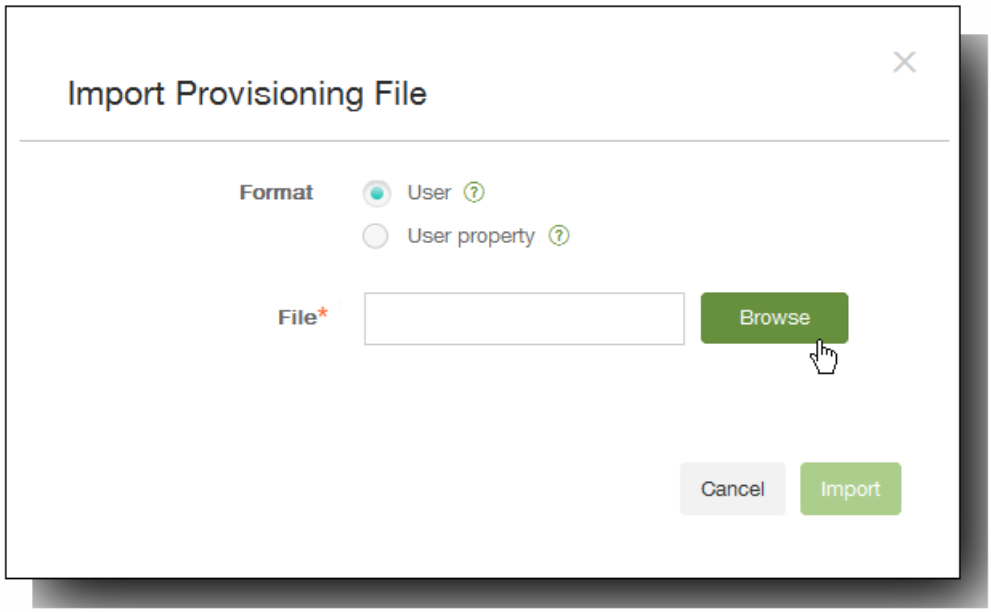
1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Local Users and Groups.



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.

May 05, 2016

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.

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

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

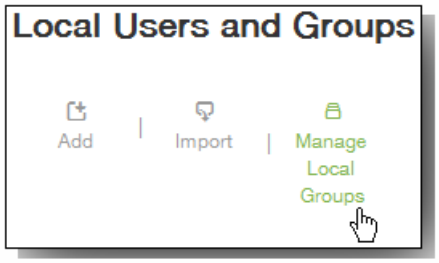
Der Eintrag: `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value`Bedeutet:

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

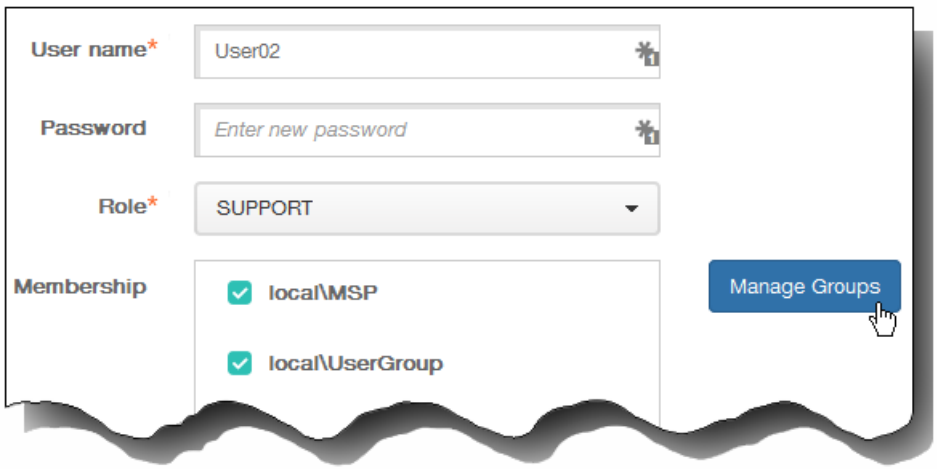
May 05, 2016

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.

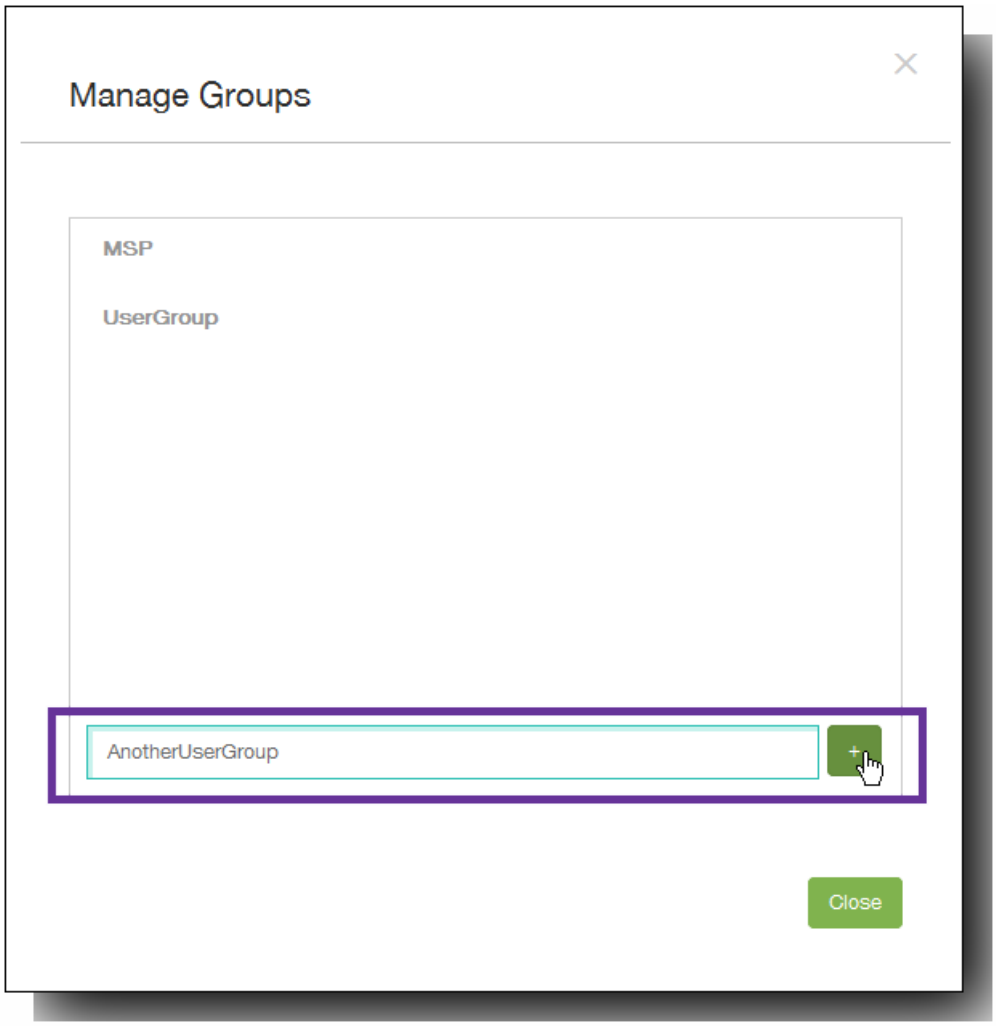
1. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf der Seite Local Users and Groups auf Manage Local Groups.



   - 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 (+).



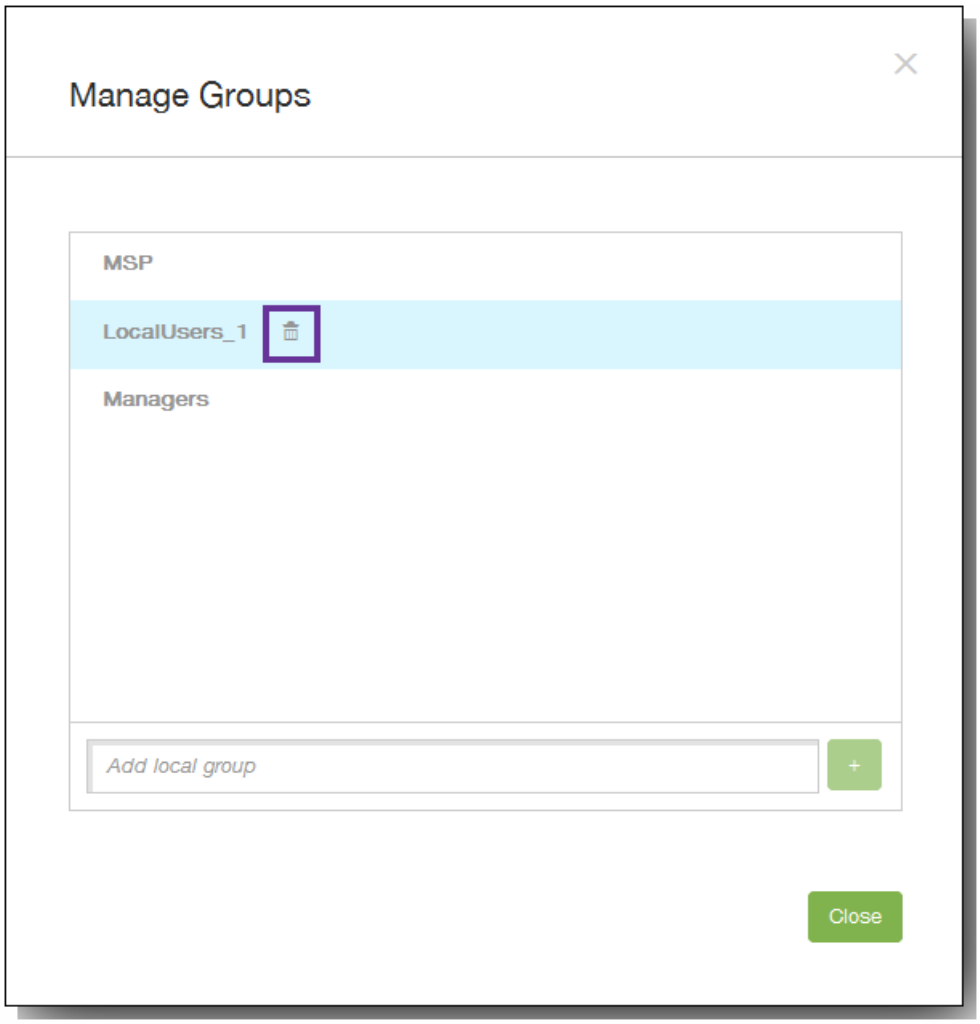
Die Benutzergruppe wird der Liste hinzugefügt.

3. Klicken Sie auf Close.

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.

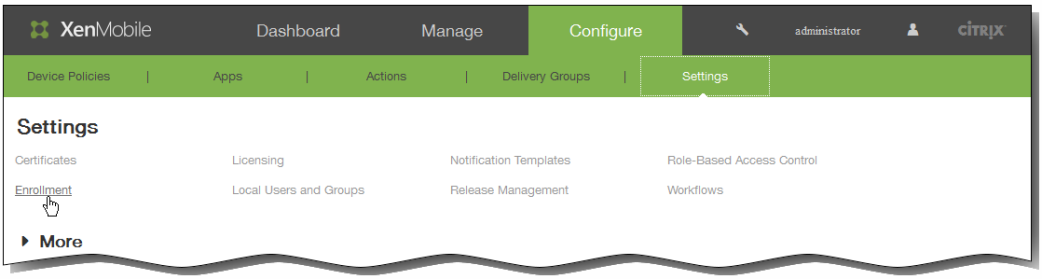
May 05, 2016

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.

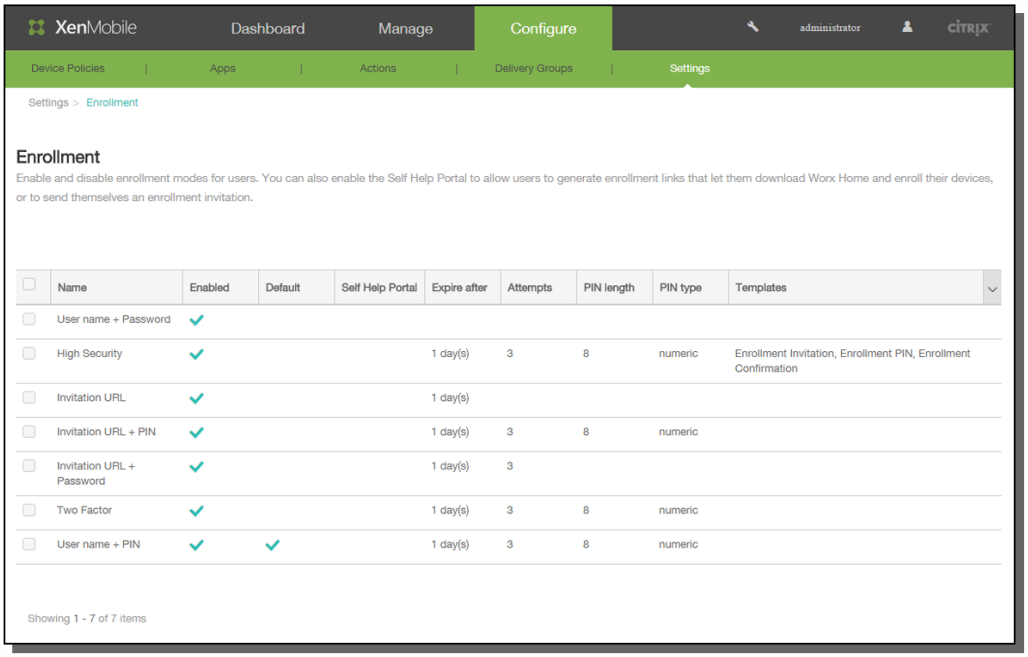
Zum Konfigurieren von Registrierungsmodi verwenden Sie in der XenMobile-Konsole die Seite Settings > Enrollment. Zum Senden von Registrierungseinladungen verwenden Sie in der XenMobile-Konsole die Seite Manage > Enrollment (siehe Registrieren von Benutzern und Geräten in XenMobile).

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.

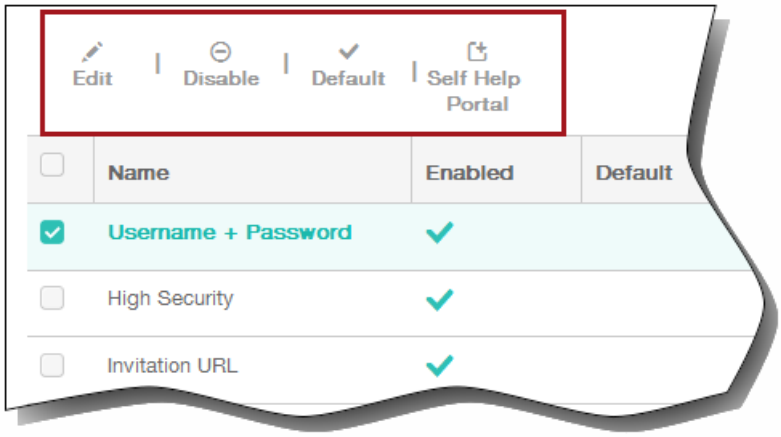
1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Enrollment.

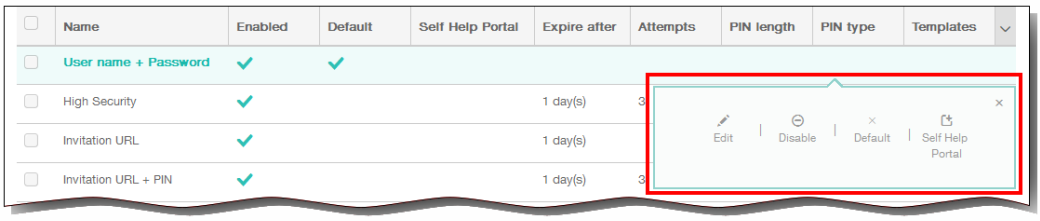


Die Seite Enrollment wird angezeigt. Sie enthält eine Tabelle aller verfügbaren Registrierungsmodi.



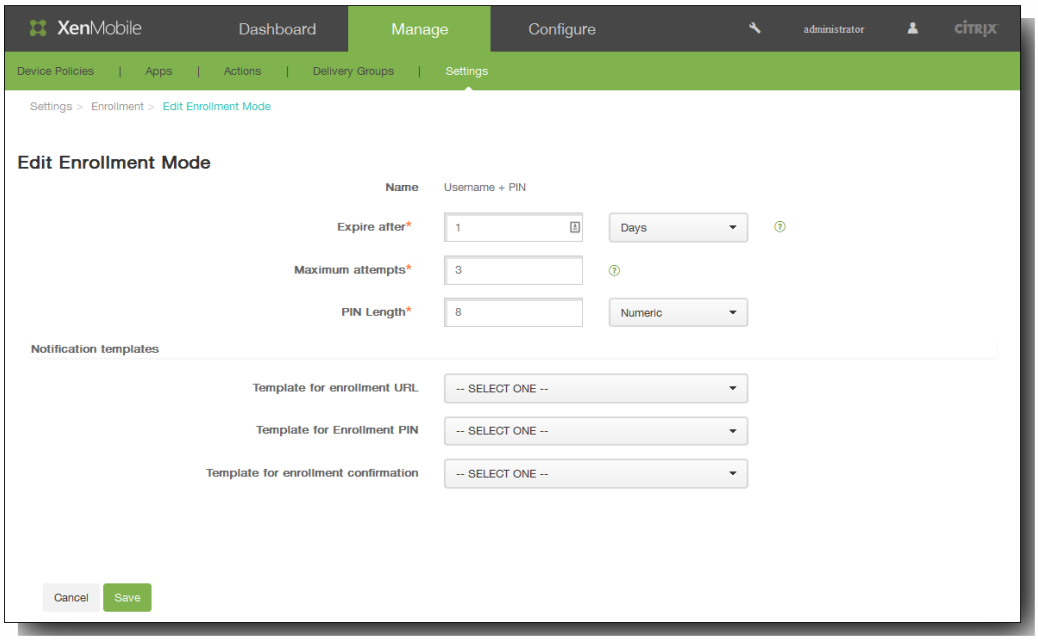
2. Wählen Sie einen Registrierungsmodus in der Liste zur Bearbeitung aus und legen Sie diesen als Standard fest, löschen Sie ihn oder erteilen Sie Benutzern Zugriff darauf über das Selbsthilfeportal.
   Hinweis: Wenn Sie das Kontrollkästchen neben einem Registrierungsmodus auswählen, wird das Menü mit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



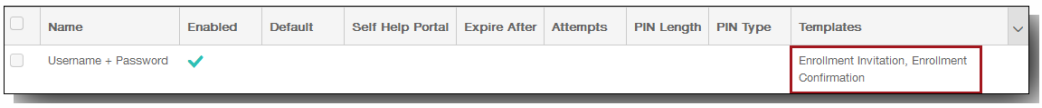


1. Wählen Sie in der Liste Enrollment einen Registrierungsmodus aus und klicken Sie dann auf Edit. Abhängig vom

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.

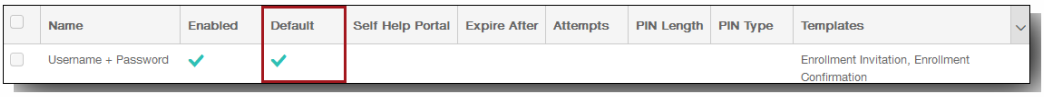


Wenn Sie einen Registrierungsmodus als Standard festlegen, wird er für alle Geräteregistrierungsanfragen verwendet, wenn

kein anderer Registrierungsmodus ausgewählt wird. Wenn kein Registrierungsmodus als Standard festgelegt wird, muss für jede Geräteregistrierung eine eigene Registrierungsanforderung erstellt werden.

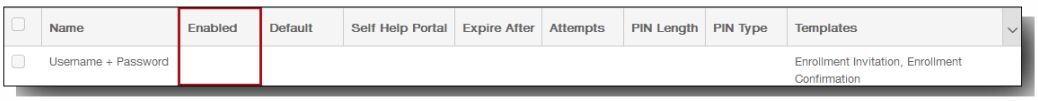
Hinweis: Nur Username + Passwords, Two Factor oder Username + PIN können als Standardregistrierungsmodus festgelegt werden.

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.



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.

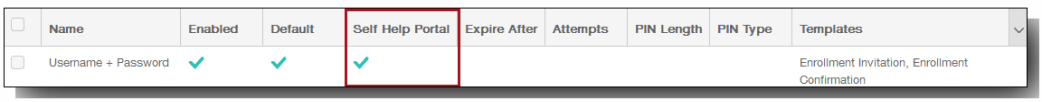


Durch Aktivieren eines Registrierungsmodus auf dem Selbsthilfeportal können Benutzer ihre Geräte in XenMobile selbst registrieren.

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.



May 05, 2016

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.
- **Provisioning**: wird von den Administratoren für die Bereitstellung aller Windows Mobile-/CE-Geräte als eine Gruppe mit dem Device Provisioning-Tool verwendet.
- **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.

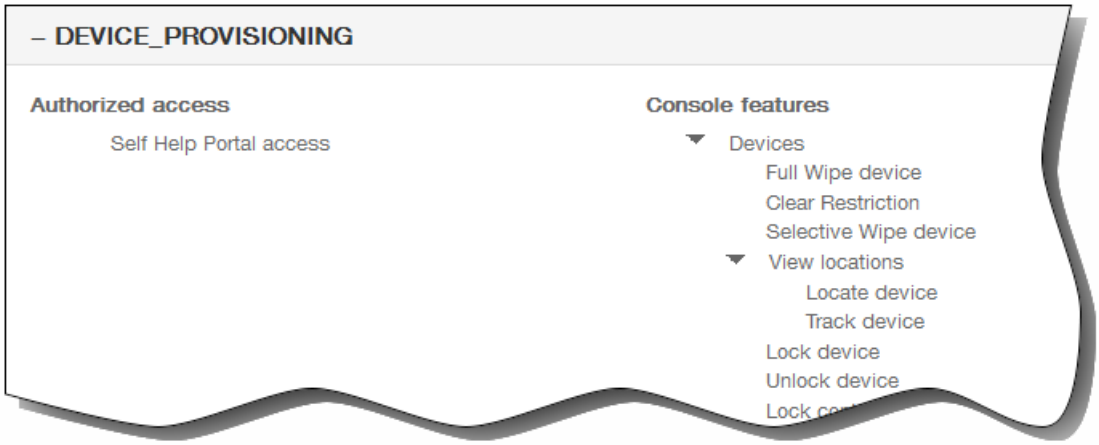
Rollen können lokalen Benutzern (auf Benutzerebene) oder Active Directory-Gruppen (alle Benutzer in der Gruppe haben dieselben Berechtigungen) zugewiesen werden. Gehört ein Benutzer mehreren Active Directory-Gruppen an, werden alle entsprechenden Berechtigungen zu einem für diesen Benutzer spezifischen 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

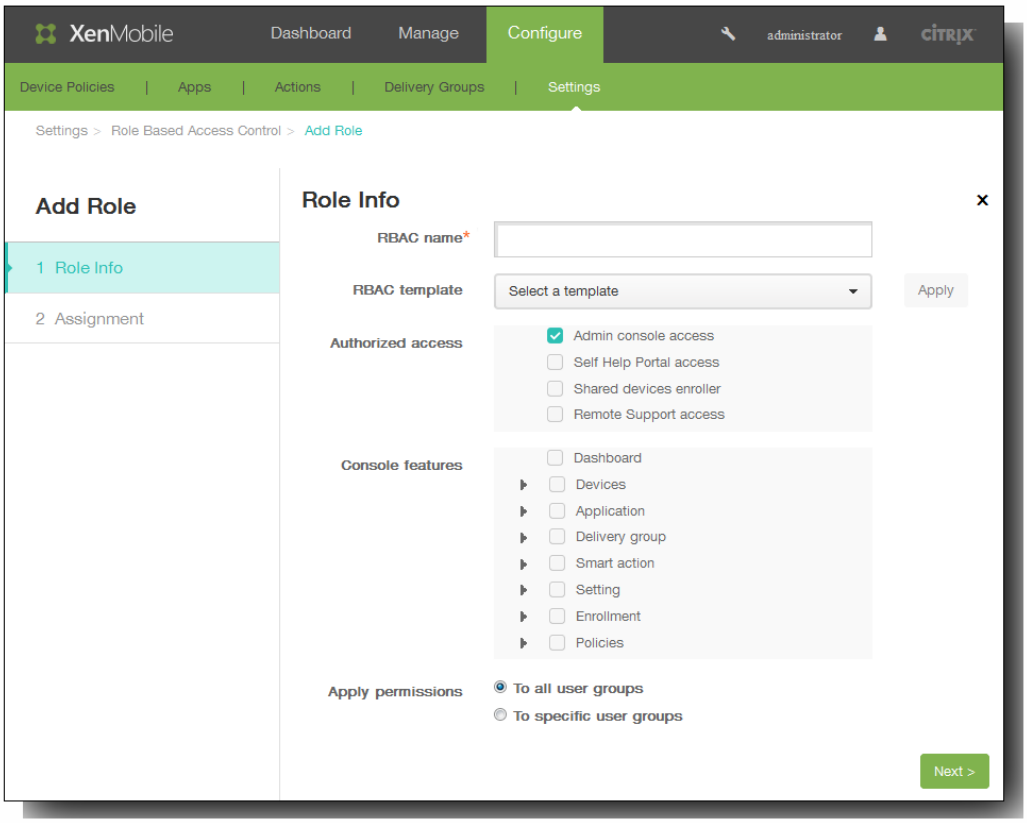
1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Role-Based Access Control.

   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).



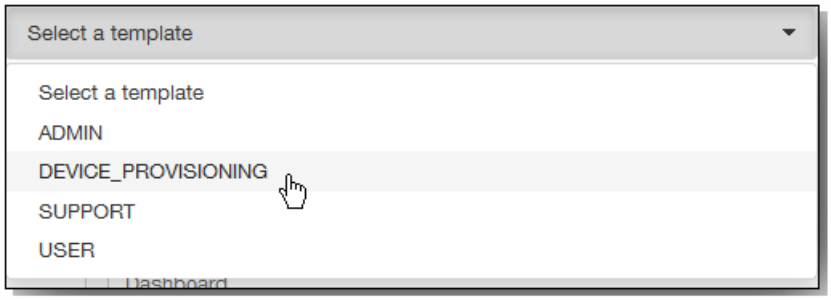
2. Klicken Sie auf Add, um eine neue Benutzerrolle hinzuzufügen, klicken Sie auf das Stiftsymbol rechts neben einer vorhandenen Rolle, um diese zu bearbeiten, oder klicken Sie auf das Papierkorbsymbol rechts neben einer von Ihnen hinzugefügten Rolle, um sie zu löschen. Sie können die Standardbenutzerrollen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



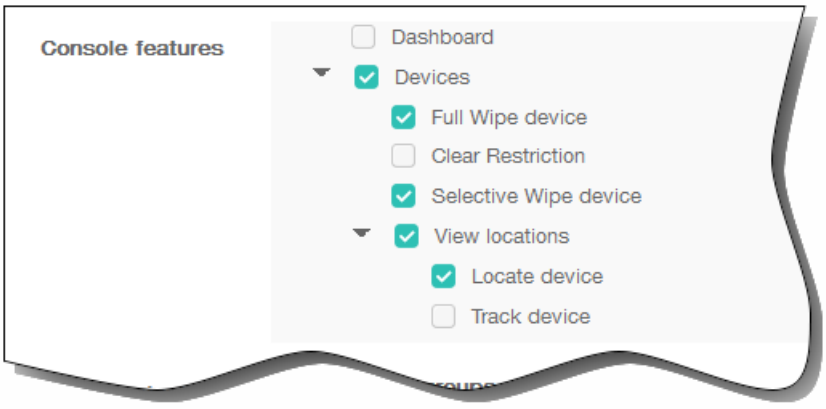
   - Wenn Sie auf das Papierkorbsymbol klicken, wird ein Bestätigungsdialogfeld angezeigt. Klicken Sie auf Delete, um die ausgewählte Rolle zu entfernen.
3. Geben Sie die folgenden Informationen zum Erstellen einer neuen Benutzerrolle bzw. zum Bearbeiten einer vorhandenen Benutzerrolle ein:
   1. RBAC name: Geben Sie einen aussagekräftigen Namen für die neue Benutzerrolle ein. Sie können den Namen

vorhandener Rollen nicht ändern.

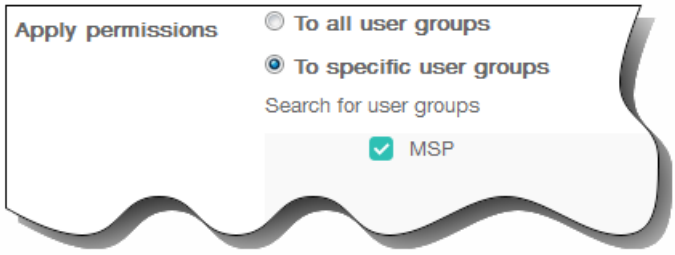
2. RBAC template: Klicken Sie auf eine Vorlage als Ausgangspunkt für eine neue Rolle oder auf eine neue Vorlage für eine vorhandene Rolle.
   Hinweis: RBAC-Vorlagen sind die Standardbenutzerrollen sowie alle Rollen, die Sie selbst definiert haben. Sie definieren Sie den Zugriff auf Systemfunktionen für 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.

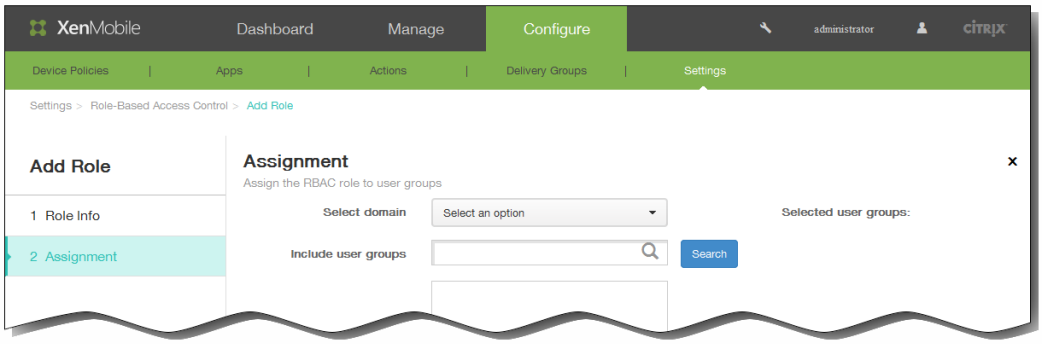


3. Apply permissions: Wählen Sie die Gruppen aus, denen Sie die ausgewählten Berechtigungen erteilen möchten.

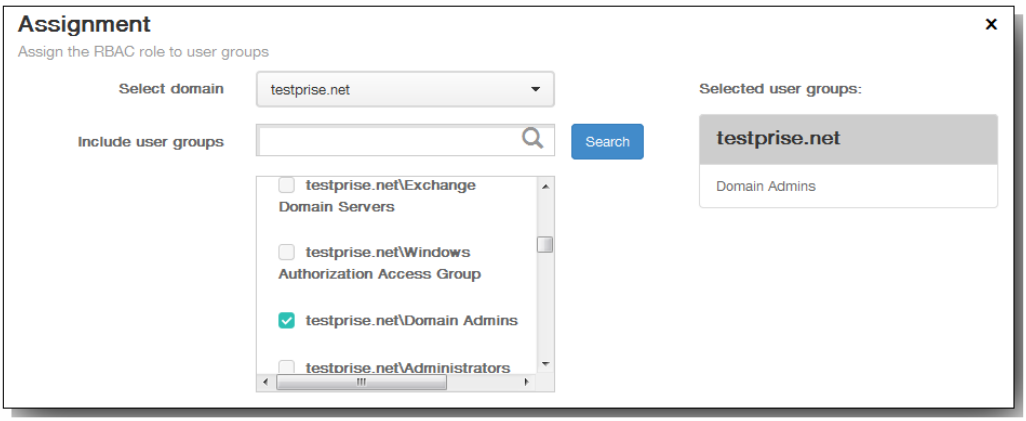


Wenn Sie auf To specific user groups klicken, wird eine Liste mit Gruppen angezeigt, in der Sie eine oder mehrere Gruppen auswählen können.

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 diese in der Liste der ausgewählten Gruppen rechts neben dem Suchfeld 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.

Oct 13, 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.

Um Autodiscovery zu aktivieren, greifen Sie auf das Autodiscovery-Dienstportal unter https://xenmobiletools.citrix.com zu. Weitere Informationen über das Autodiscovery-Dienstportal finden Sie unter XenMobile Autodiscovery-Dienst.

In einigen Fällen ist zur Autodiscovery-Aktivierung eine Anfrage beim Citrix Support erforderlich. Folgen Sie hierfür den Anweisungen unten, um dem Support 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:

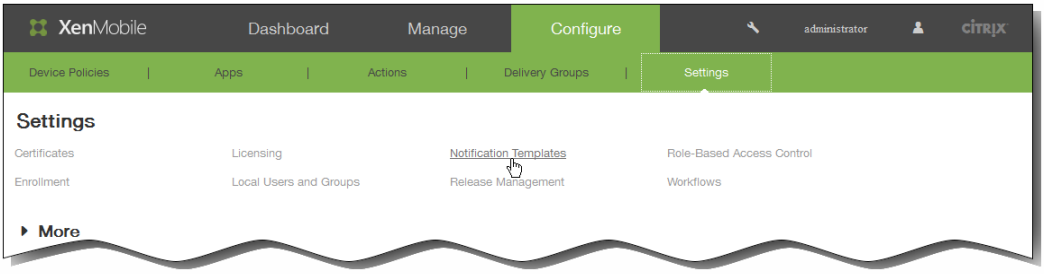
- SubjectDN mit einem CN, der die primäre Domäne für das Zertifikat angibt (z. B. enterpriseenrollment.mycompany1.com)
- SANs der restlichen Domänen (z. B. enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com usw.)

May 05, 2016

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.

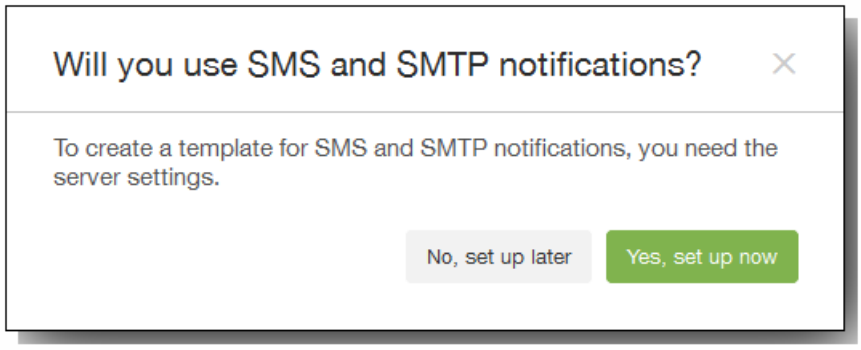
1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > Notification Templates.



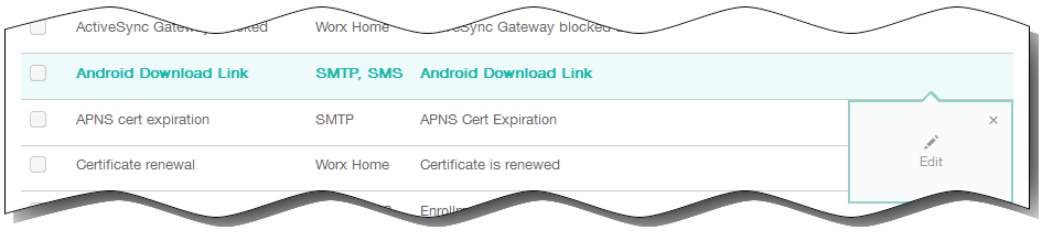
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf Add, um eine neue Benachrichtigungsvorlage hinzuzufügen. Wenn kein SMS-Gateway oder SMTP-Server eingerichtet wurde, wird eine Meldung bezüglich der Verwendung von SMS- und SMTP-Benachrichtigungen angezeigt. Sie können wählen, ob Sie 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.

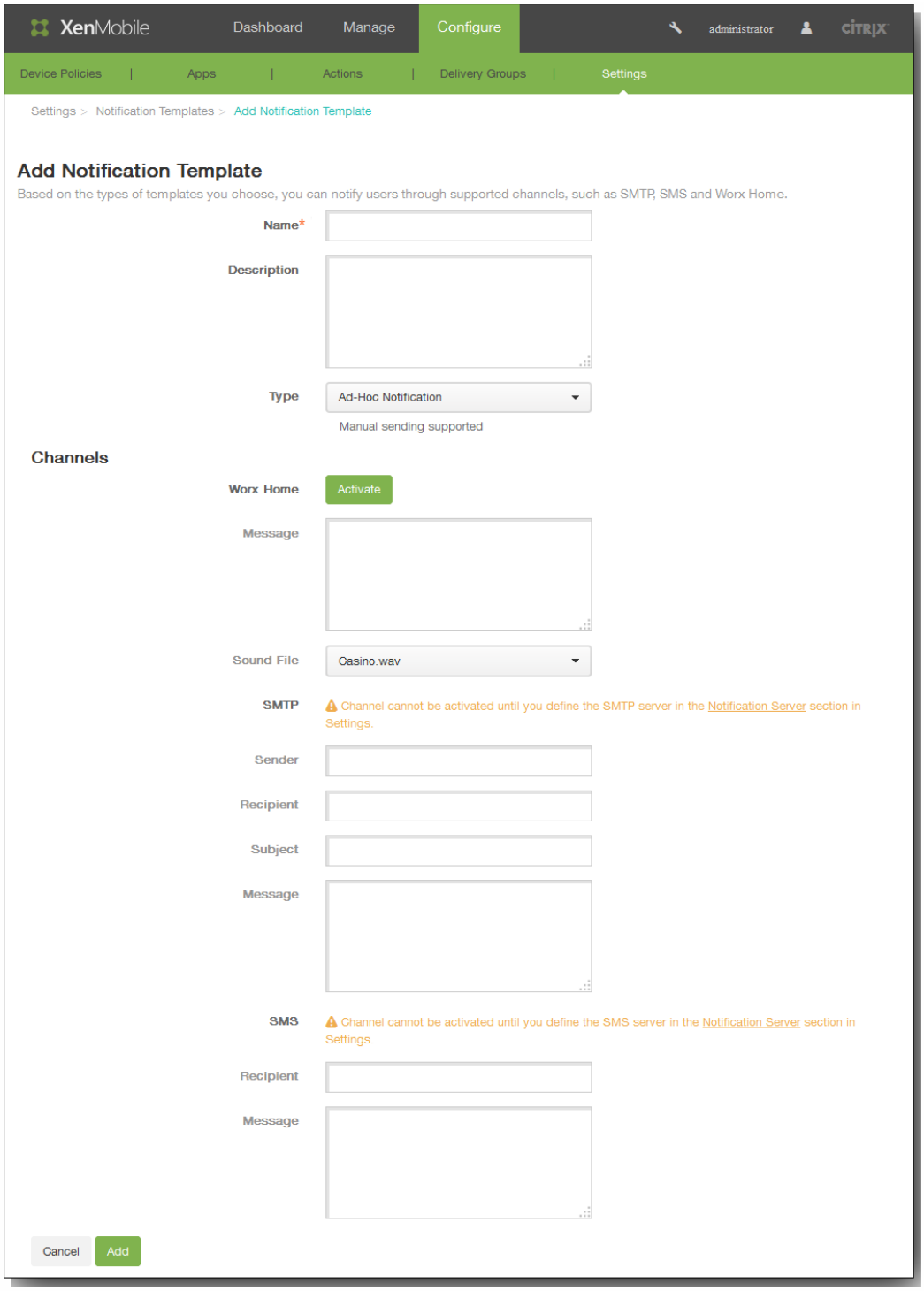
     Wichtig: Wenn Sie entscheiden, die SMS- oder SMTP-Server-Einstellungen später einzurichten, können Sie diese Kanäle beim Hinzufügen oder Bearbeiten einer Benachrichtigungsvorlage nicht aktivieren, d. h. die Kanäle sind nicht zum Senden von Benutzerbenachrichtigungen verfügbar.



- 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.

May 05, 2016

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 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.

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.

Sie können Bereitstellungsgruppen in XenMobile hinzufügen, bearbeiten, deaktivieren, aktivieren, bereitstellen und löschen und dadurch die Bereitstellung von Richtlinien, Apps und Aktionen verwalten. Jede dieser Aktionen wird in den folgenden Abschnitten detailliert beschrieben.

- So fügen Sie eine Bereitstellungsgruppe hinzu
- So bearbeiten Sie eine Bereitstellungsgruppe
- So aktivieren oder deaktivieren Sie die Bereitstellungsgruppe "AllUsers"
- So stellen Sie Bereitstellungsgruppen bereit
- So löschen Sie Bereitstellungsgruppen

Zur Verwaltung der Bereitstellungsgruppen öffnen Sie zunächst die Seite Delivery Groups:

1. Klicken Sie in der XenMobile-Konsole auf Configure > Delivery Groups.

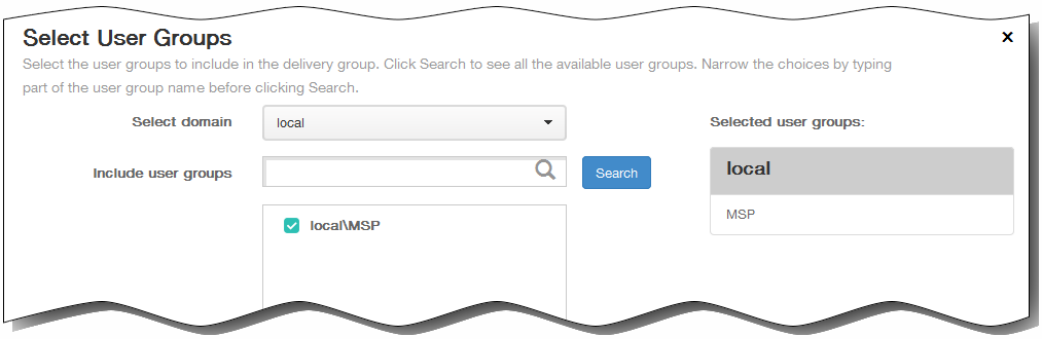
   Die Seite Delivery Groups wird angezeigt. Für Informationen zu den einzelnen Aktionen konsultieren Sie den relevanten eDocs-Abschnitt.

1. Klicken Sie auf der Seite Delivery Groups auf Add. Die Seite Delivery Group Information wird angezeigt.

2. Geben Sie im Bereich Delivery Group Information die folgenden Informationen ein:
   1. Name: Geben Sie einen aussagekräftigen Namen für die Bereitstellungsgruppe ein.

2. Description: Geben Sie optional eine Beschreibung der Bereitstellungsgruppe ein.
3. Klicken Sie auf Next. Die Seite Delivery Group User wird angezeigt.

4. Geben Sie im Bereich Select User Groups die folgenden Informationen ein:
   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.

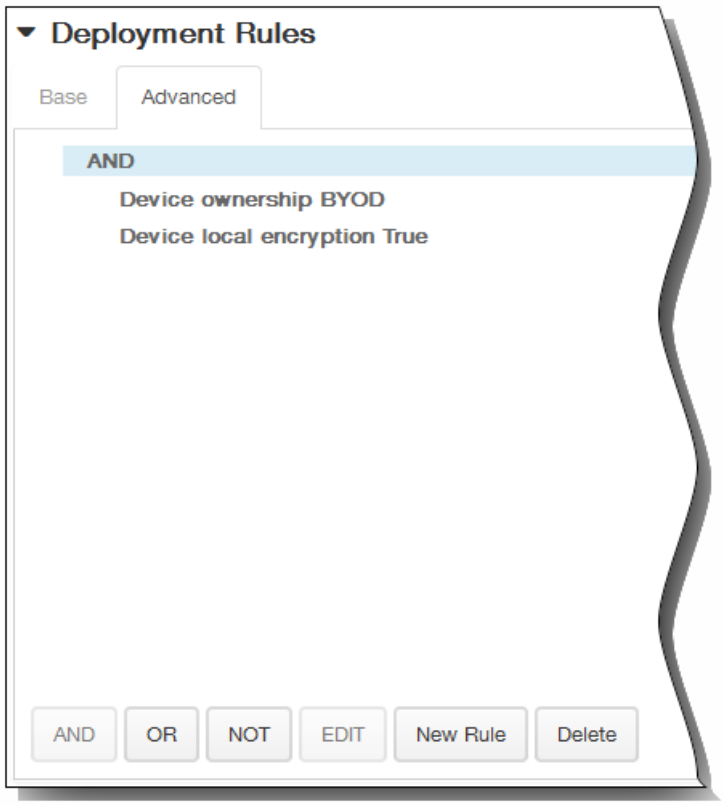


   Zum Entfernen einer Benutzergruppe aus der Liste Selected user groups führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf Search, um eine Liste aller Benutzergruppen in der ausgewählten Domäne anzuzeigen.
   - Geben Sie den Gruppennamen vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf Search, um die Liste der Benutzergruppen einzuschränken.

   Die Namen der 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.

   4. Or/And: Wählen Sie aus, ob Benutzer für die bereitzustellende Ressource 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, denen jedoch dennoch eine Verbindung mit XenMobile gestattet wurde.
5. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

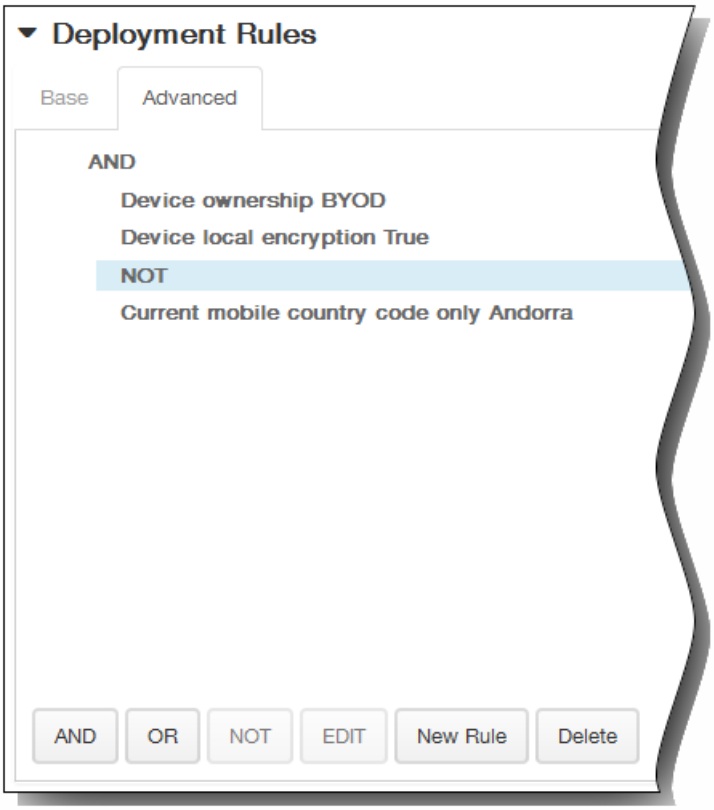
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



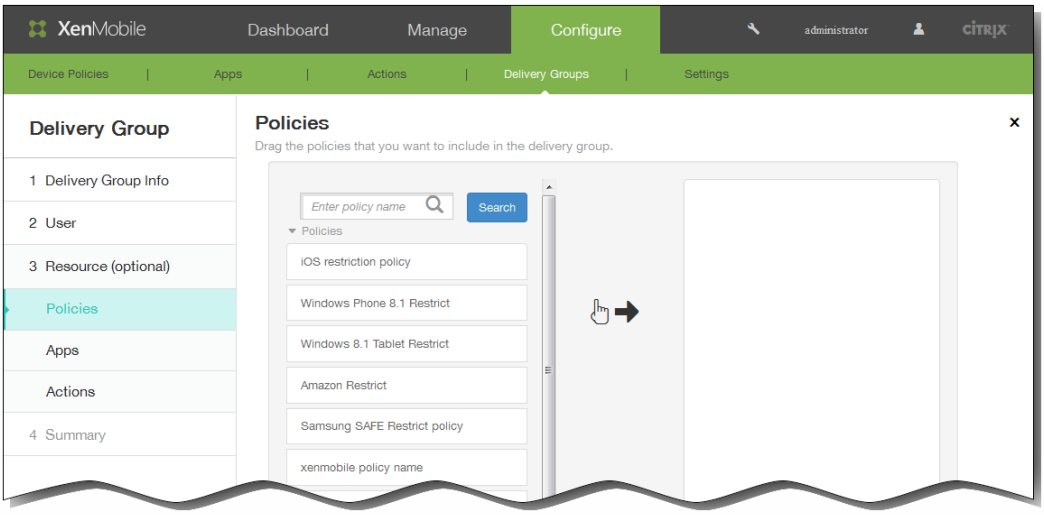
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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.

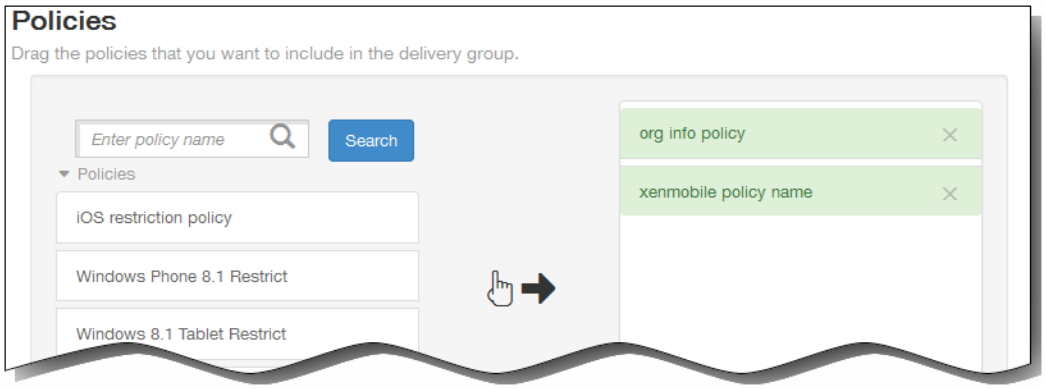
3. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten.
   In diesem Beispiel wurde für "Device ownership" "BYOD", für "Device local encryption" und "Passcode compliant" "True" eingestellt und "Current mobile country code" auf Andorra eingeschränkt.



6. Klicken Sie auf Next. Die Seite Delivery Group Resources wird angezeigt. Hier können Sie für die Bereitstellungsgruppe optional Richtlinien, Apps oder Aktionen hinzufügen. Zum Überspringen dieses Schritts klicken Sie unter Delivery Group auf Summary, um eine Zusammenfassung der Bereitstellungsgruppenkonfiguration anzuzeigen, oder führen Sie einen der folgenden Schritte aus:
   Hinweis: Zum Überspringen einer Ressource klicken Sie unter Resources (optional) auf die Ressource, die Sie hinzufügen möchten, und folgen Sie den Schritten für diese Ressource.
   So fügen Sie Richtlinien hinzu



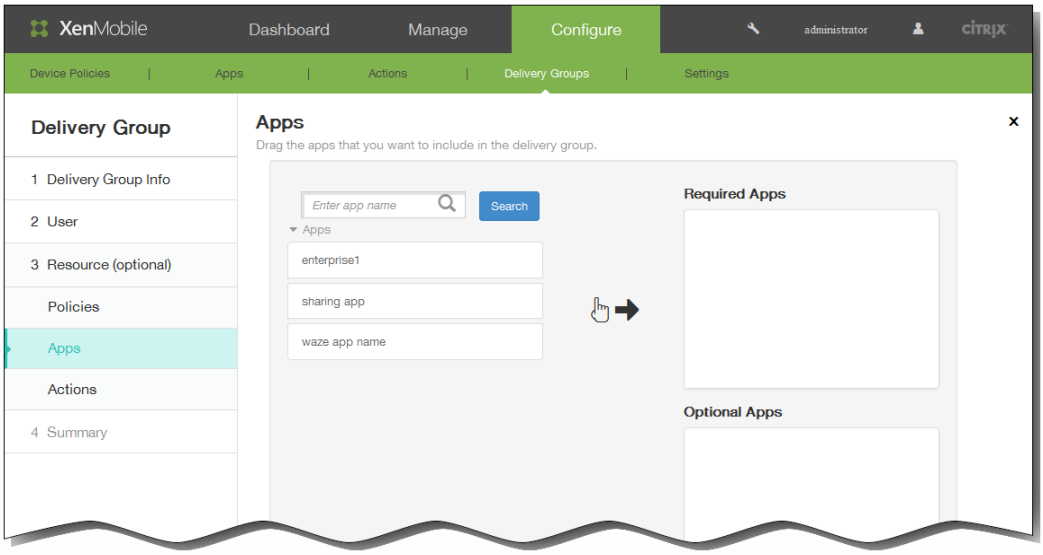
1. Navigieren Sie in der Liste der verfügbaren Richtlinien zu der gewünschten Richtlinie oder geben Sie zum Einschränken der Richtlinienliste in das Suchfeld einen Richtlinienamen vollständig oder teilweise ein und klicken Sie dann auf Search.
2. Klicken Sie auf eine Richtlinie und ziehen Sie sie in das Feld auf der rechten Seite.
3. Wiederholen Sie die Schritte a und b zum Hinzufügen weiterer Richtlinien.



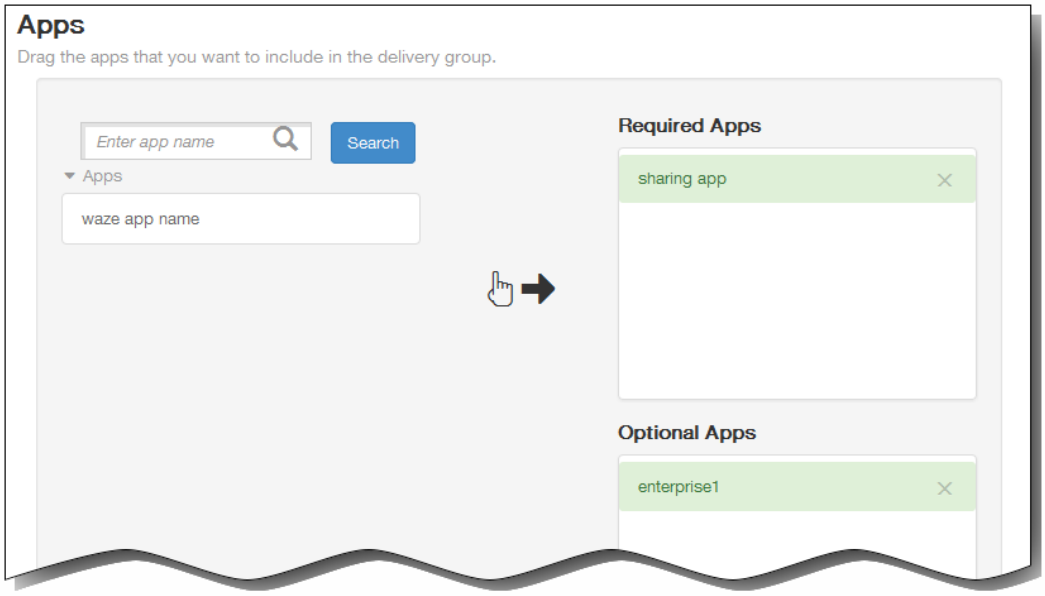
Zum Entfernen einer Richtlinienressource klicken Sie auf das X neben deren Namen.

4. Klicken Sie auf Next, um die Seite Apps aufzurufen. Wenn Sie keine weiteren Ressourcen hinzufügen, klicken Sie unter Delivery Group auf Summary. Es wird die Seite Apps bzw. Summary angezeigt.

So fügen Sie Apps hinzu



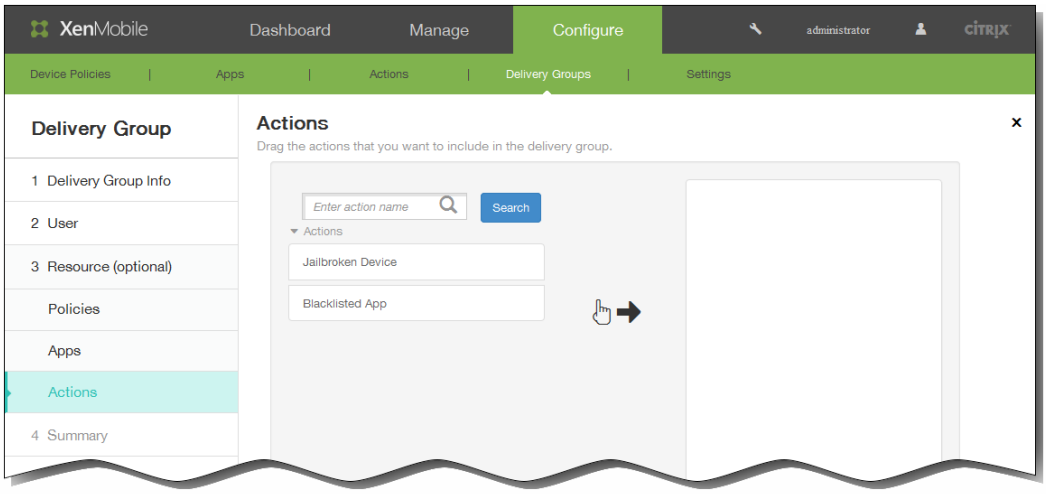
1. Navigieren Sie in der Liste der verfügbaren Apps zu der gewünschten App oder geben Sie zum Einschränken der App-Liste in das Suchfeld einen App-Namen vollständig oder teilweise ein und klicken Sie dann auf Search.
2. Klicken Sie auf eine App und ziehen Sie sie entweder in das Feld Required Apps oder in das Feld Optional Apps.
3. Wiederholen Sie die Schritte a und b zum Hinzufügen weiterer Apps.



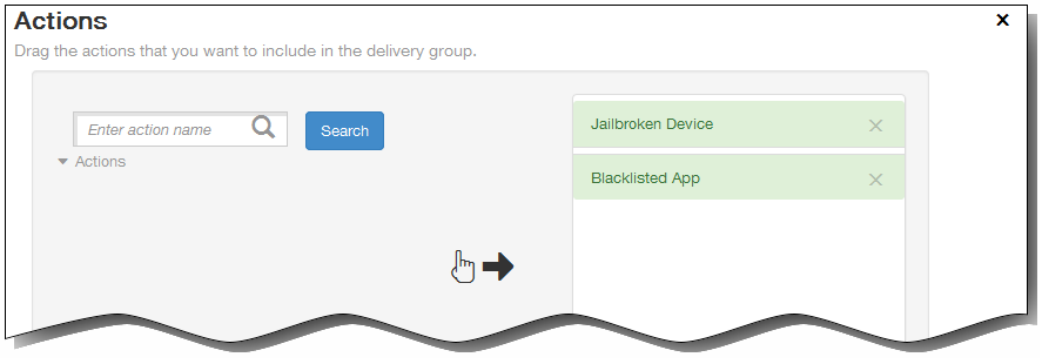
Zum Entfernen einer App-Ressource klicken Sie auf das X neben deren Namen.

4. Klicken Sie auf Next, um die Seite Actions aufzurufen. Wenn Sie keine weiteren Ressourcen hinzufügen, klicken Sie unter Delivery Group auf Summary. Es wird die Seite Actions bzw. Summary angezeigt.

So fügen Sie Aktionen hinzu

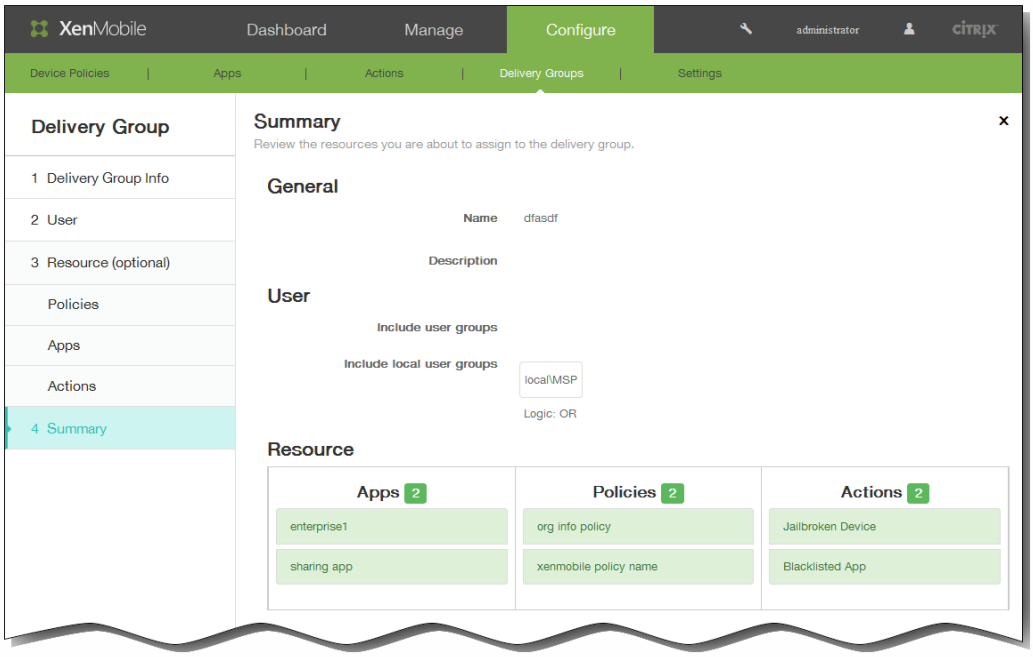


1. Navigieren Sie in der Liste der verfügbaren Aktionen zu der gewünschten Aktion oder geben Sie zum Einschränken der Liste der Aktionen in das Suchfeld einen Aktionsnamen vollständig oder teilweise ein und klicken Sie dann auf Search.
2. Klicken Sie auf eine Aktion und ziehen Sie sie in das Feld auf der rechten Seite.
3. Wiederholen Sie die Schritte a und b zum Hinzufügen weiterer Aktionen.



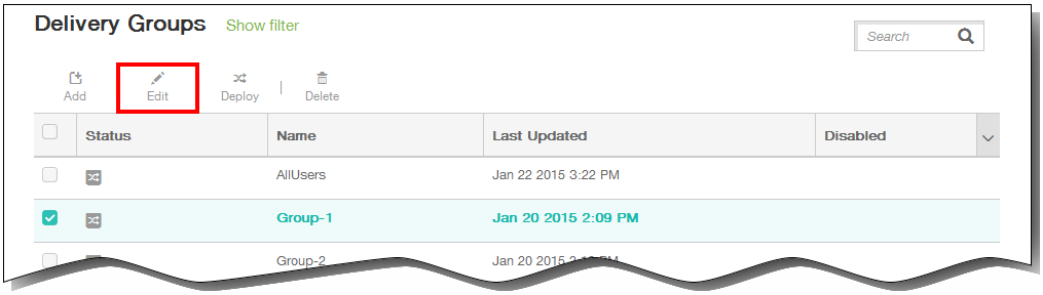
Zum Entfernen einer Aktionsressource klicken Sie auf das X neben deren Namen.

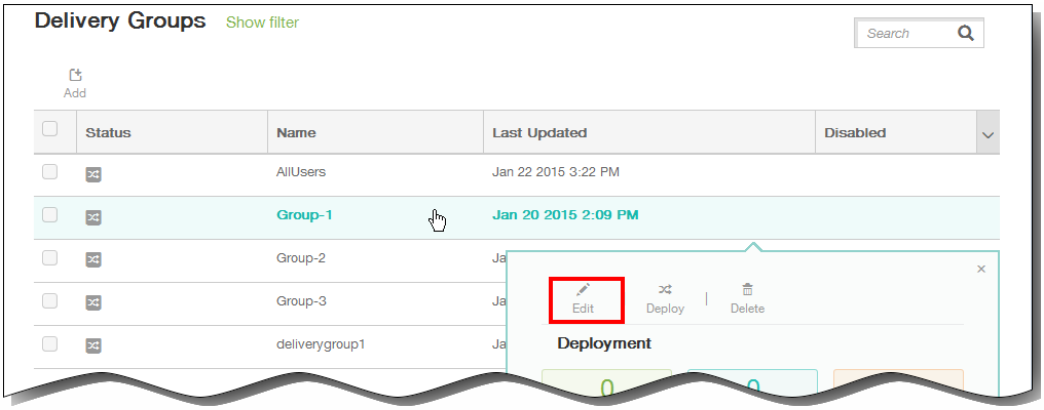
4. Klicken Sie auf Next. Die Zusammenfassungsseite wird angezeigt.



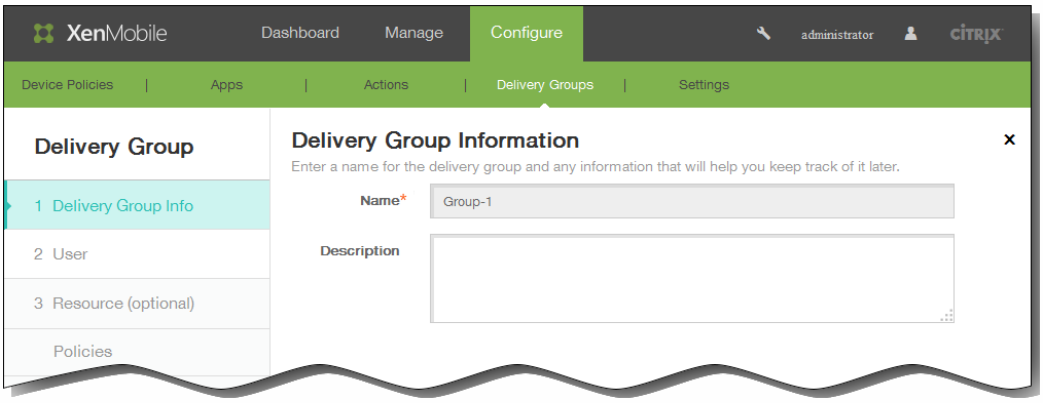
7. Überprüfen Sie auf der Seite Summary die Optionen, die Sie für die Bereitstellung konfiguriert haben. Klicken Sie auf Back, um auf vorherige Seiten aufzurufen, wenn Sie Änderungen vornehmen müssen.
8. Klicken Sie auf Save, um die Bereitstellungsgruppe zu speichern.

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.



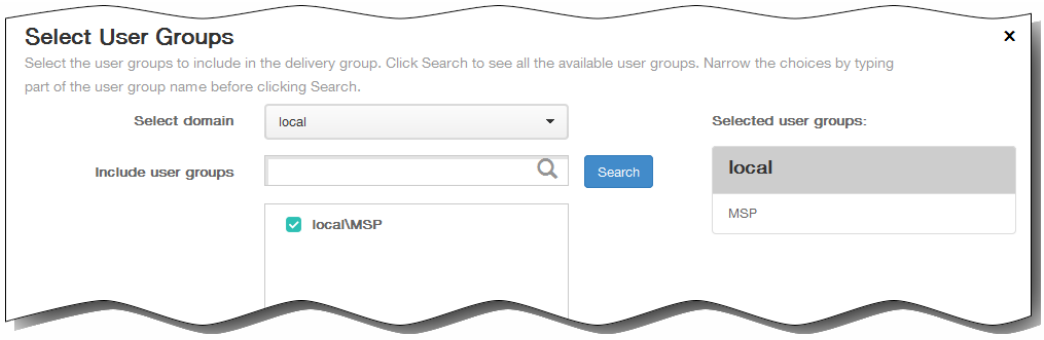


Die Seite Delivery Group Information wird zur Bearbeitung angezeigt.



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.

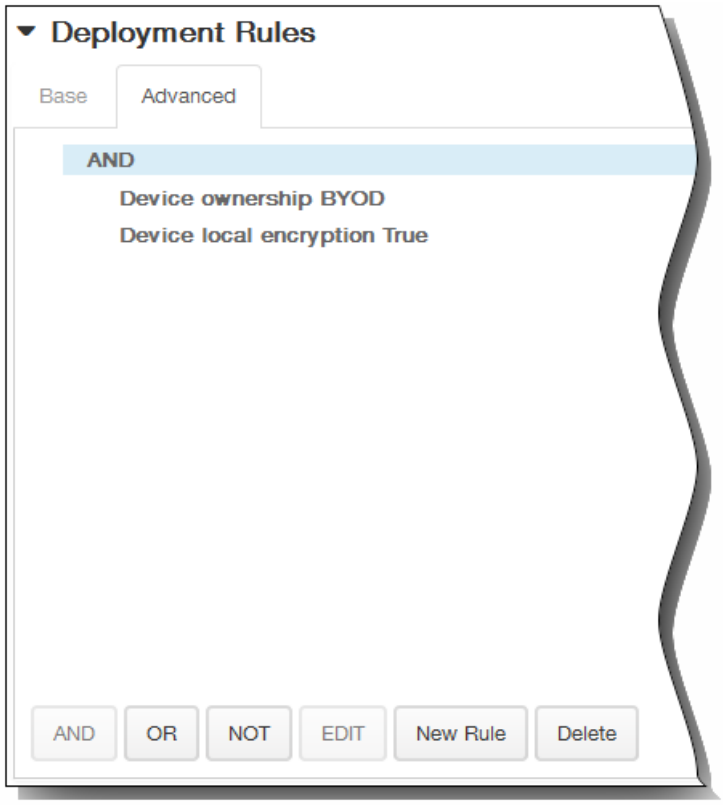


Hinweis: Zum Entfernen von Benutzergruppen klicken Sie auf Search und deaktivieren Sie in der Liste der Benutzergruppen die Kontrollkästchen der Gruppen, die Sie entfernen möchten. Sie können den Gruppennamen vollständig oder teilweise in das Suchfeld eingeben und auf Search klicken, um die Liste der 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.

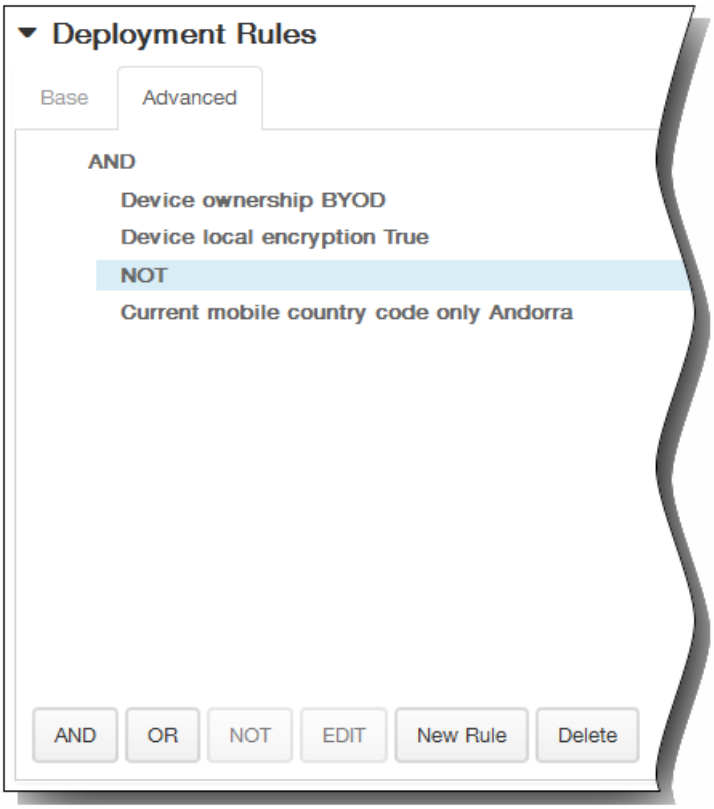
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.

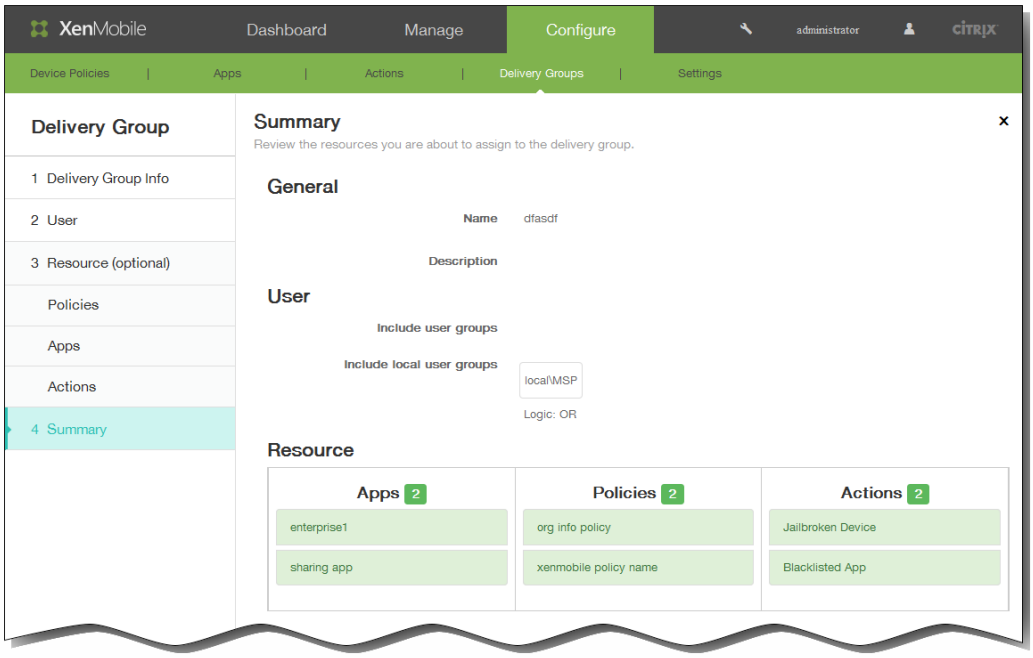
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf 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.

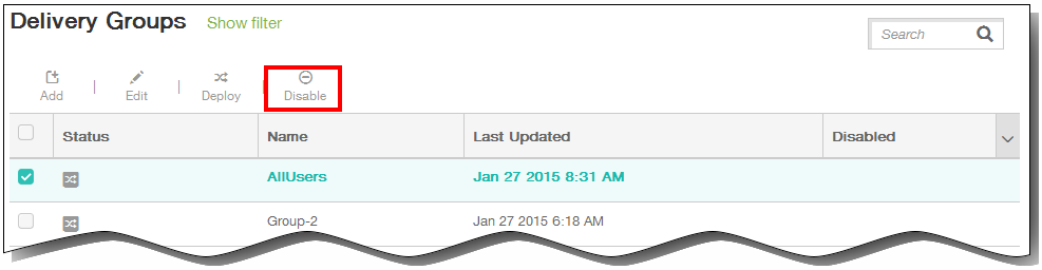
   Es wird die nächste Seite für die Ressource bzw. die Seite Summary angezeigt.

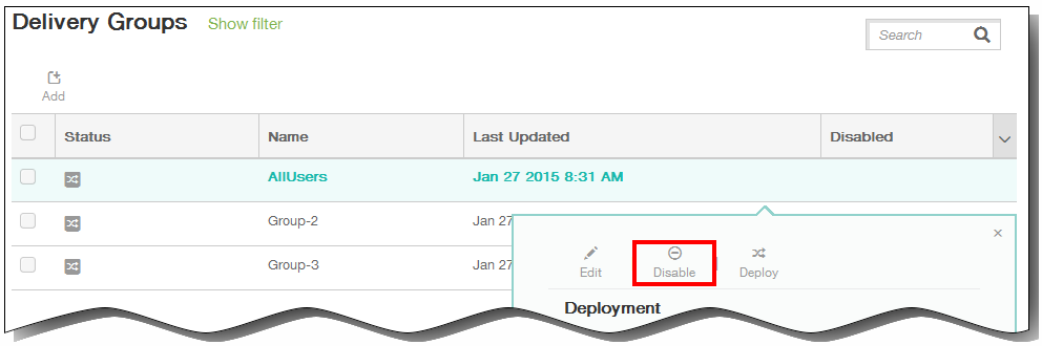


8. Überprüfen Sie auf der Seite Summary Ihre Änderungen. Klicken Sie auf Back, um auf vorherige Seiten aufzurufen, wenn Sie Änderungen vornehmen müssen.
9. Klicken Sie auf Save, um die Änderungen zu speichern.

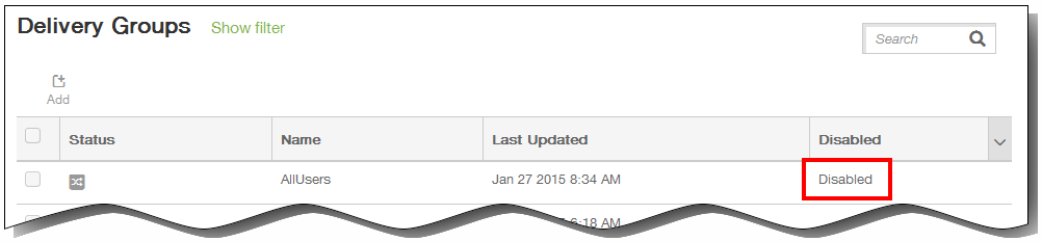
Hinweis: "AllUsers" ist die einzige Bereitstellungsgruppe, die Sie aktivieren oder deaktivieren können.

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.

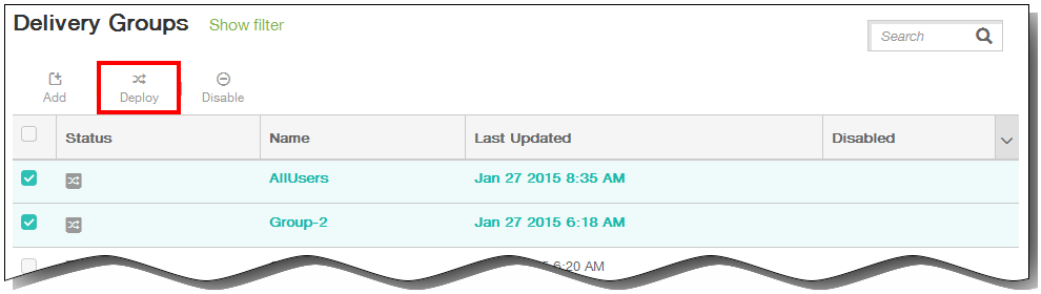


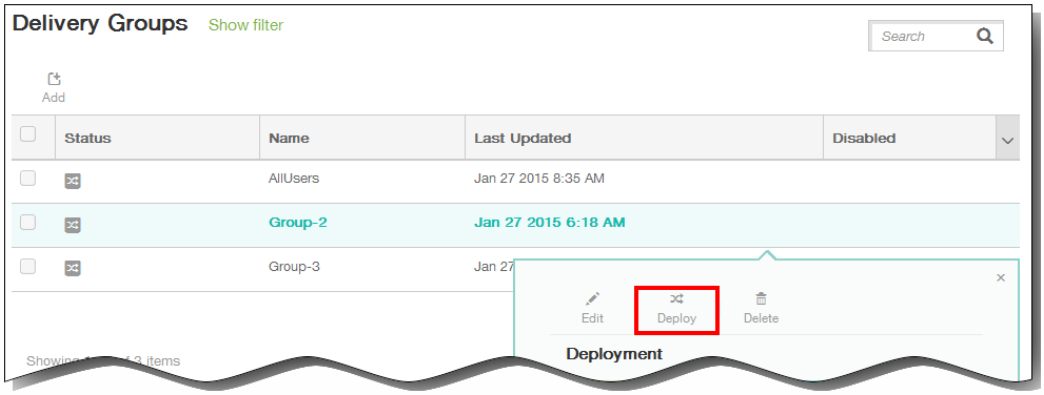
- Klicken Sie auf Enable, um die Bereitstellungsgruppe "AllUsers" zu aktivieren. Dieser Befehl ist nur verfügbar, wenn AllUsers deaktiviert ist.
  Disabled wird unter der gleichnamigen Spaltenüberschrift in der Tabelle ausgeblendet.

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.

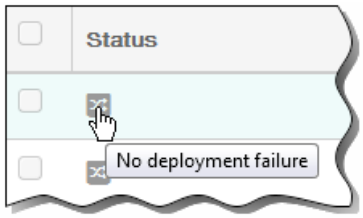
Hinweis: Damit aktualisierte Apps in der Liste der verfügbaren Updates im Worx Store auf Android-Geräten angezeigt werden, müssen Sie auf den Geräten eine App-Bestandsrichtlinie bereitstellen.

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.

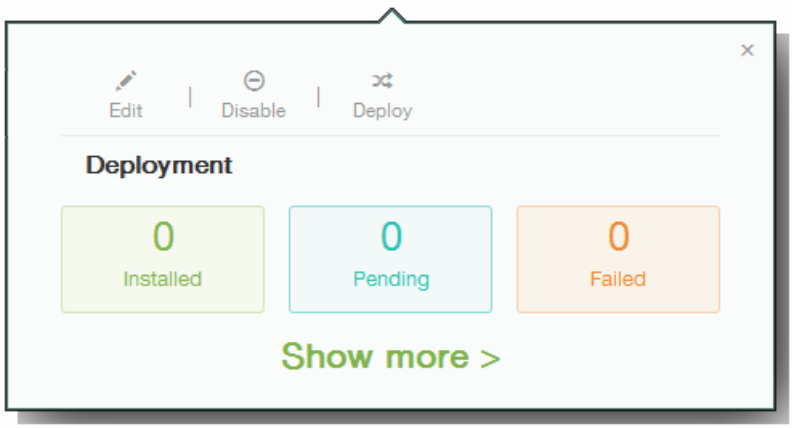




   Das Dialogfeld Deploy Devices wird geöffnet.
3. Vergewissern Sie sich, dass die Gruppen, für die Sie Apps, Richtlinien und Aktionen bereitstellen möchten, aufgelistet sind, und klicken Sie dann auf Deploy. Die Bereitstellung von Apps, Richtlinien und Aktionen für die ausgewählten Gruppen erfolgt basierend 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.

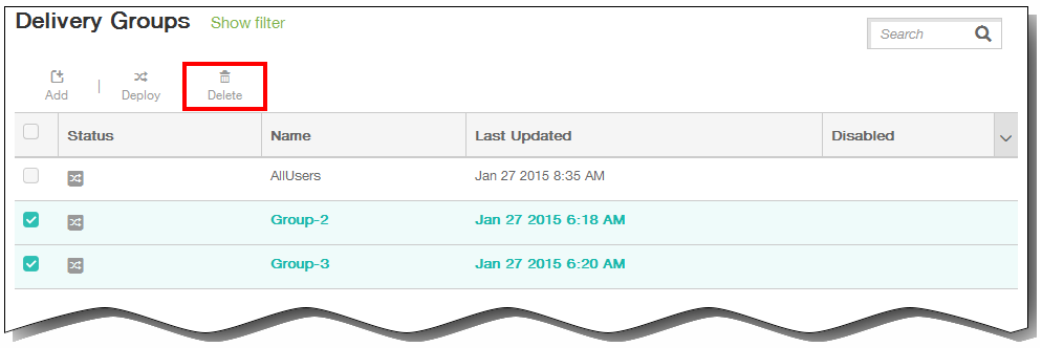


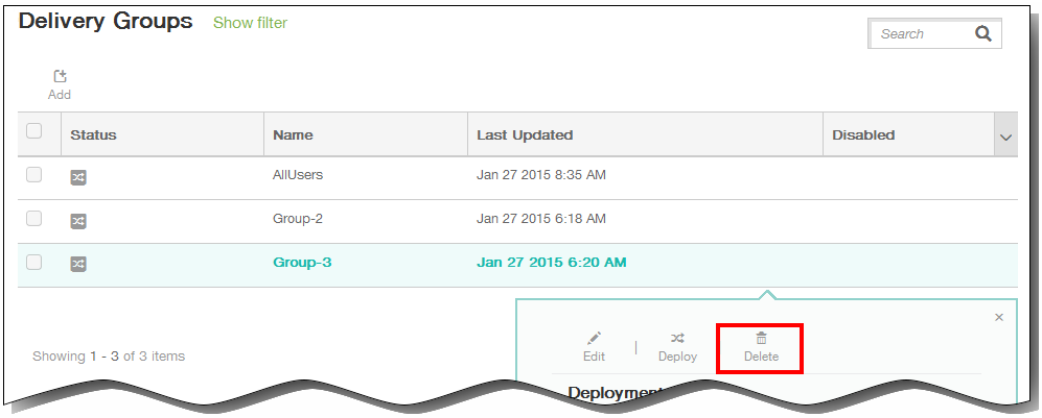
- Klicken Sie auf der Zeile mit der Bereitstellungsgruppe, um eine Überlagerung einzublenden, in der der Status "Installed", "Pending" oder "Failed" angezeigt wird.



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.

May 05, 2016

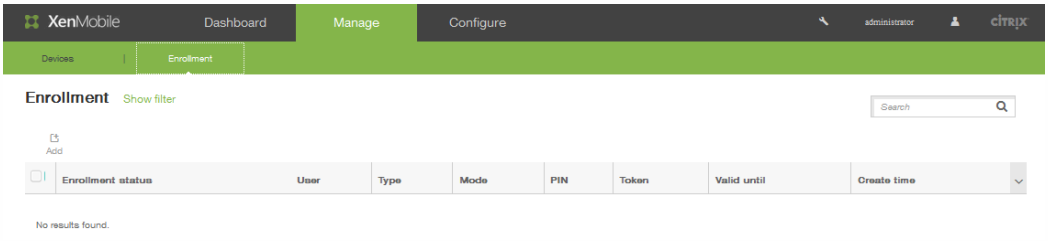
Für die sichere Remote-Verwaltung von Benutzergeräten müssen diese bei XenMobile registriert werden. Die XenMobile-Clientsoftware wird auf dem Benutzergerät installiert, die Identität des Benutzers wird authentifiziert und anschließend werden XenMobile und das Profil des Benutzers installiert. Nachdem 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**:



May 05, 2016

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. Geben Sie im Bildschirm Worx-PIN erstellen eine PIN aus sechs beliebigen Zahlen ein.
8. Geben Sie die PIN erneut ein.

Sie werden nun mit dem Android-Gerät registriert. Tippen Sie auf den Worx Store, um auf den App-Store Ihres Unternehmens sowie Worx-aktivierte Apps (WorxMail, WorxWeb, ShareFile usw.) zuzugreifen.

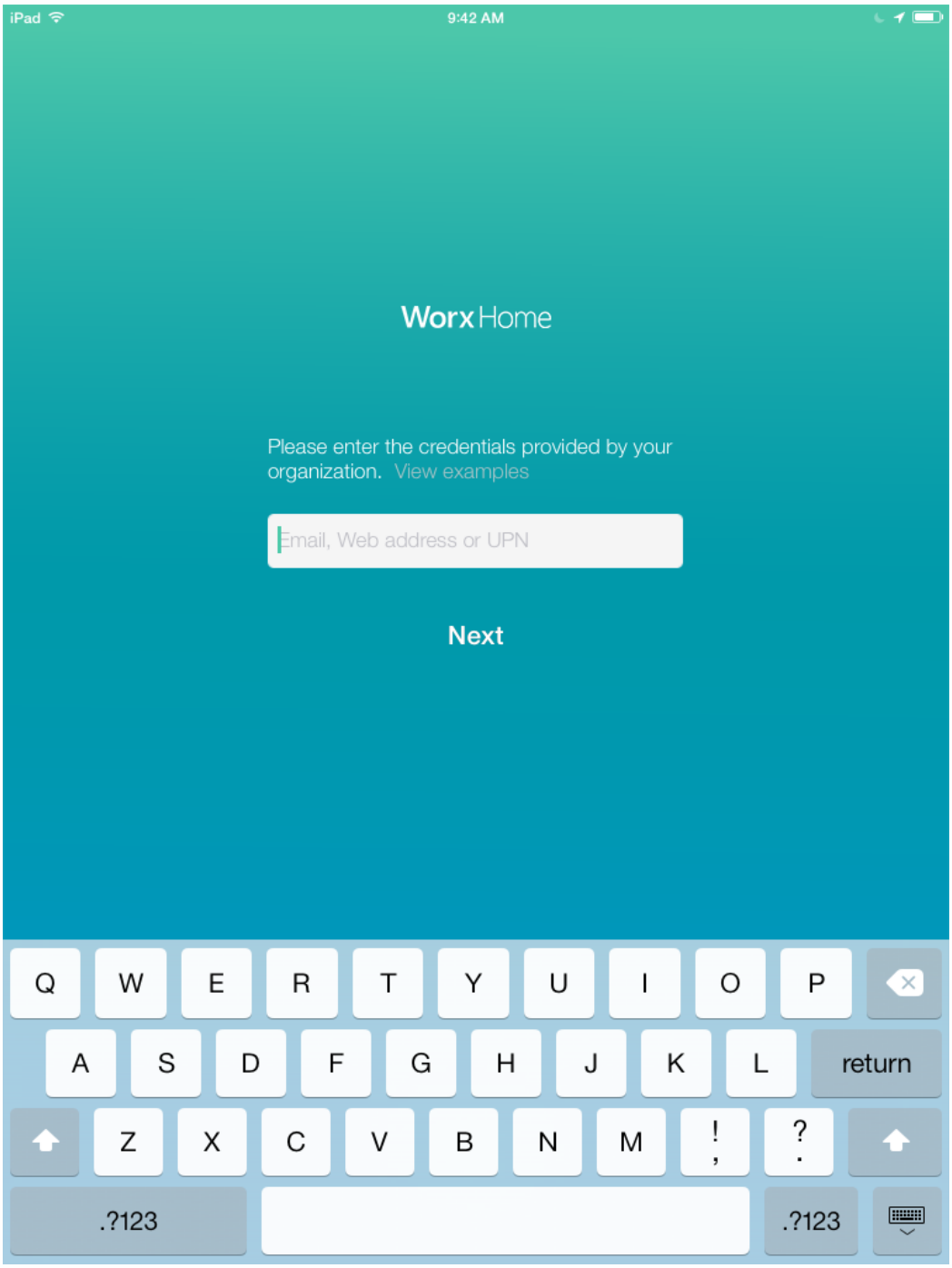
Aktualisiert: 2015-02-12

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.

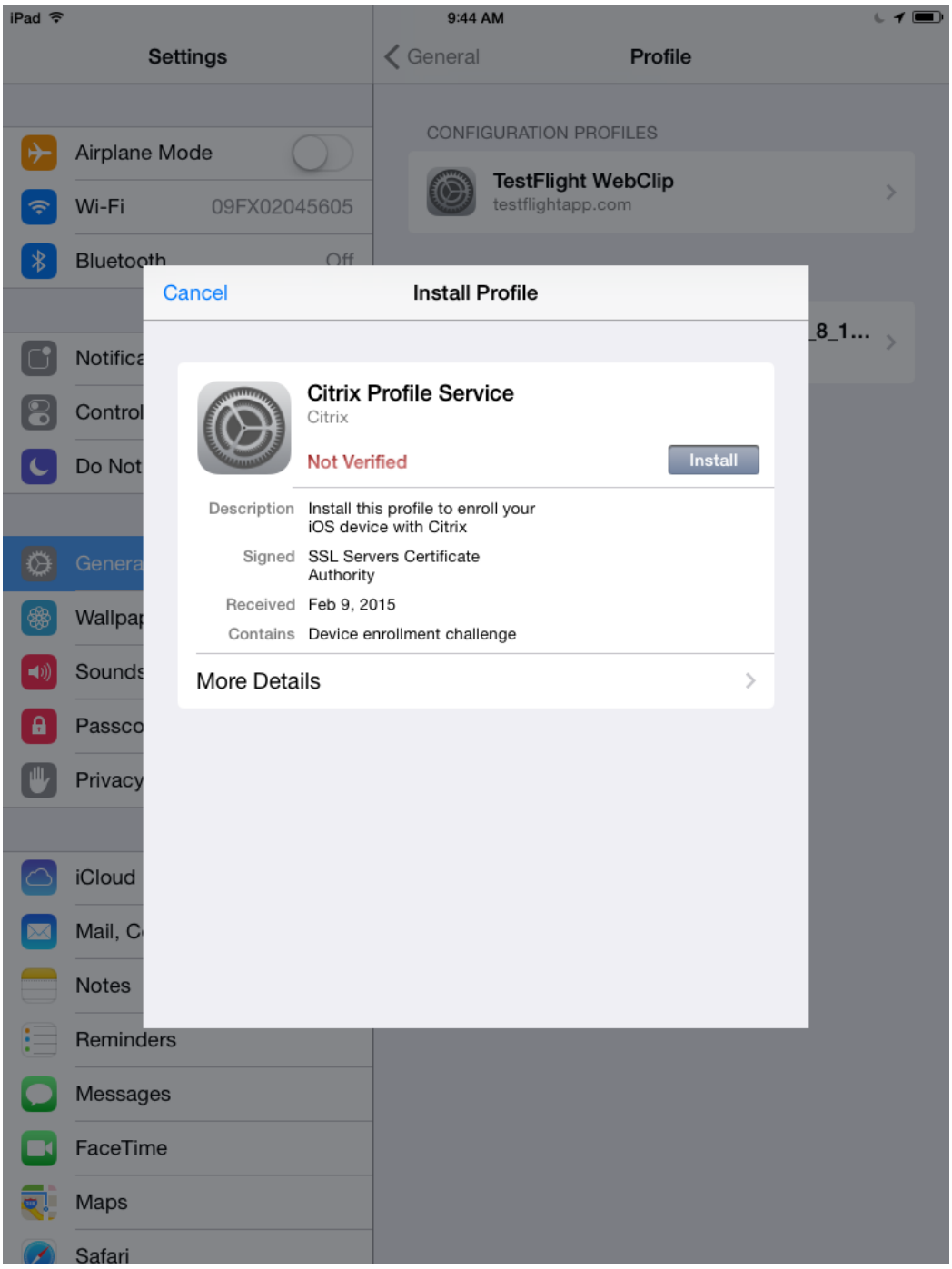
1. Tippen Sie auf die Worx Home-App.
2. Tippen Sie auf das Einstellungssymbol oben links im App-Fenster.
3. Tippen Sie auf Re-Enroll. Eine Meldung wird zur Bestätigung, dass Sie das Gerät erneut registrieren möchten, angezeigt.
4. Tippen Sie auf OK. Die Registrierung des Geräts wird aufgehoben.
5. Folgen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

May 05, 2016

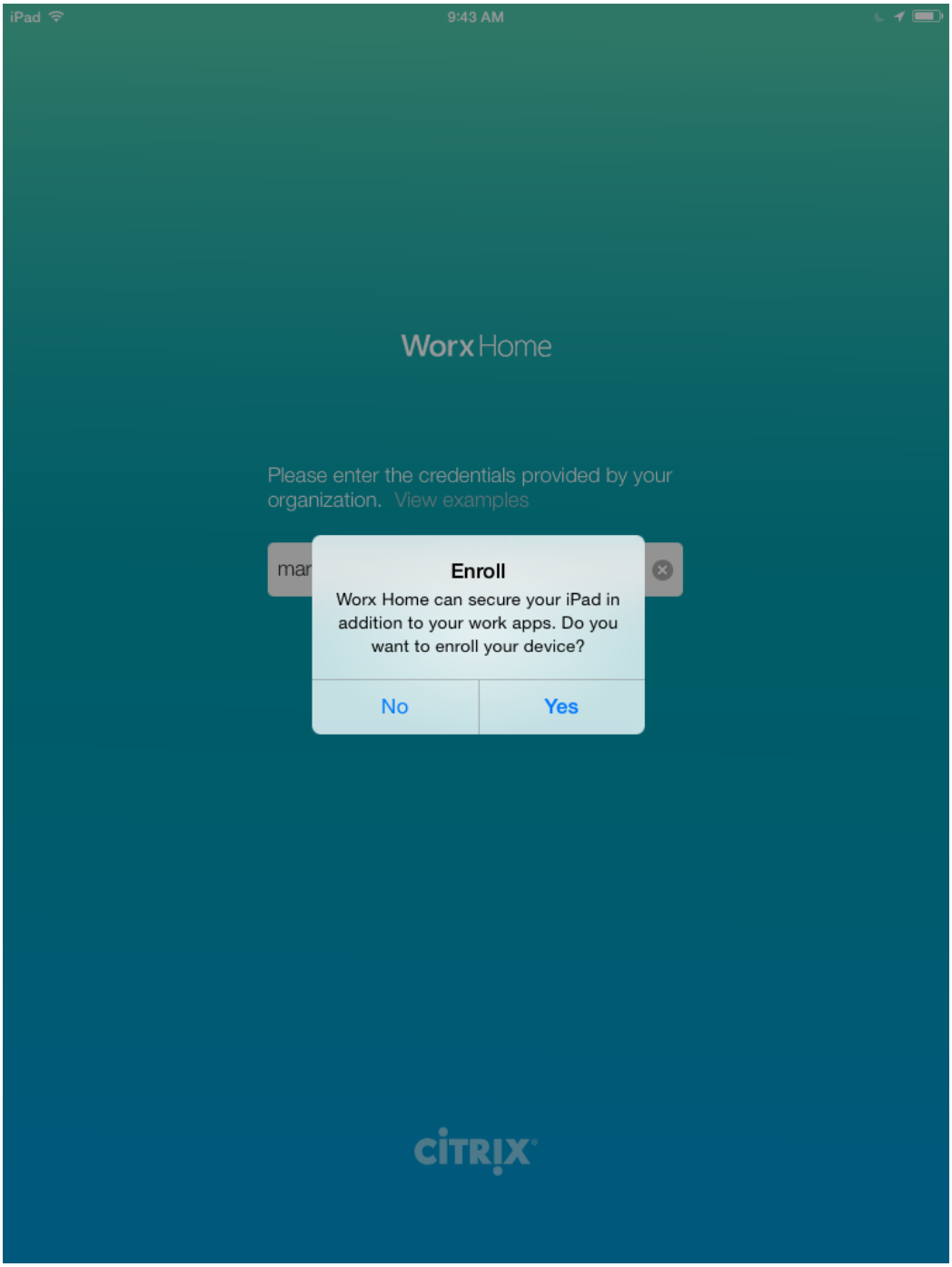
1. Laden Sie die Worx Home-App aus dem Apple iTunes-App Store auf das Gerät herunter und installieren Sie sie auf dem Gerät.
2. Tippen Sie auf dem Homebildschirm des iOS-Geräts auf die Worx Home-App.
3. Wenn die Worx Home-App sich öffnet, geben Sie Ihre geschäftlichen Anmeldeinformationen ein, z. B. 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.

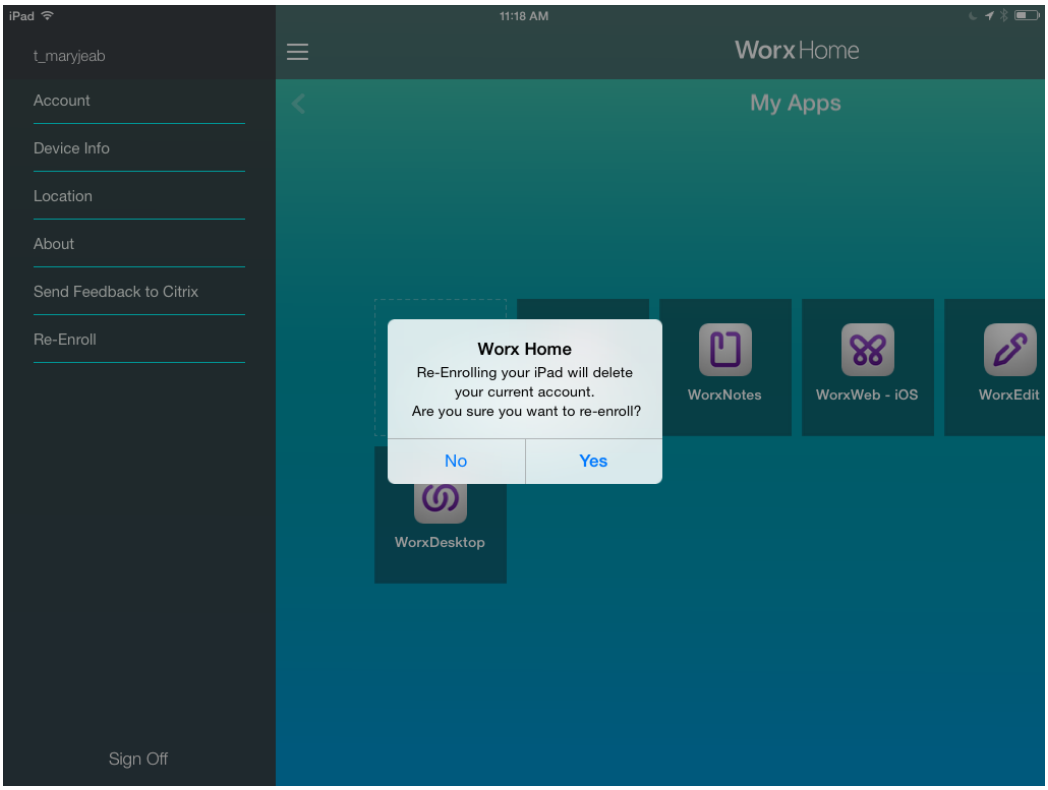


11. Je nach XenMobile-Konfiguration müssen Sie möglicherweise eine Worx-PIN zur Anmeldung bei Worx Home und anderen Worx-aktivierten Apps (WorxMail, WorxWeb, ShareFile usw.) einrichten. Sie müssen die Worx-PIN zweimal eingeben. Worx Home wird geöffnet. Sie können nun auf den Worx Store zugreifen und 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.

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.

May 05, 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.

> Damit Windows-Geräte sich registrieren können, muss das SSL-Listenerzertifikat ein öffentliches Zertifikat sein. Bei einem selbstsignierten SSL-Zertifikat schlägt die Registrierung fehl.

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.

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 Serveradresse eingeben 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.

Aktualisiert: 2015-02-11

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.

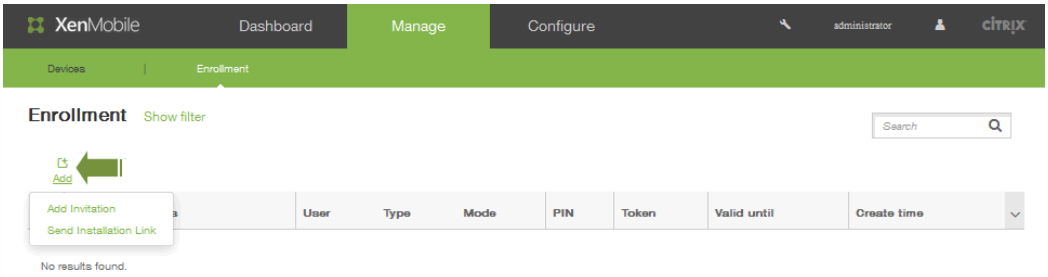
May 05, 2016

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.

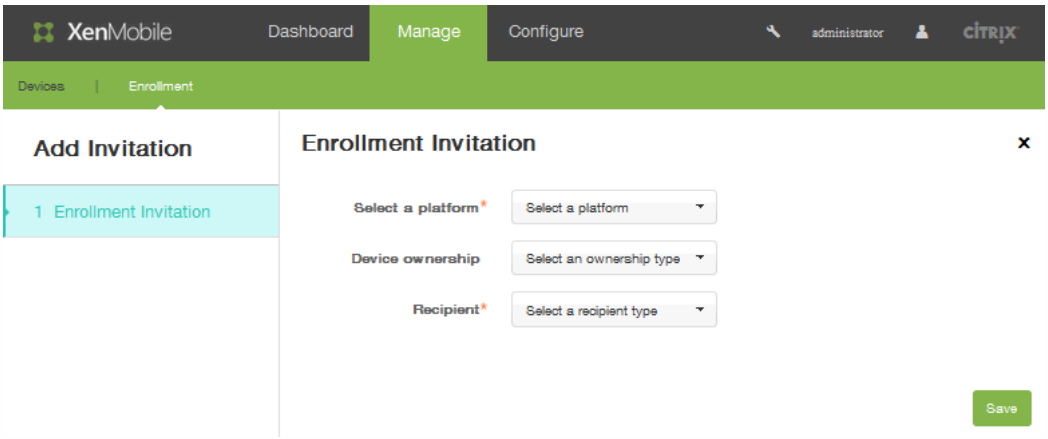
May 05, 2016

In der XenMobile-Konsole können Sie Registrierungseinladungen an Benutzer mit iOS- und Android-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.

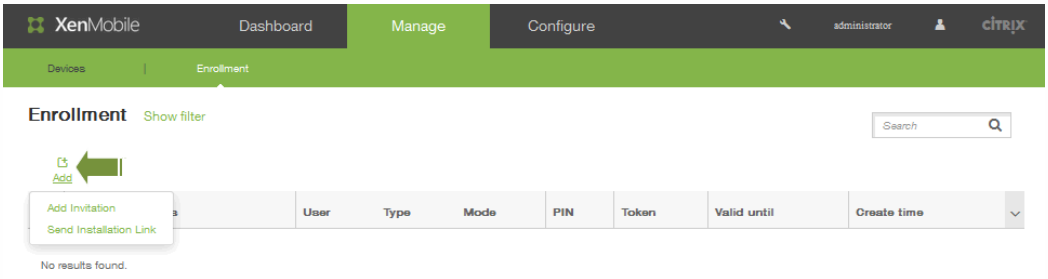


3. Klicken Sie auf Add Invitation. Die Seite Enrollment Invitation wird angezeigt.

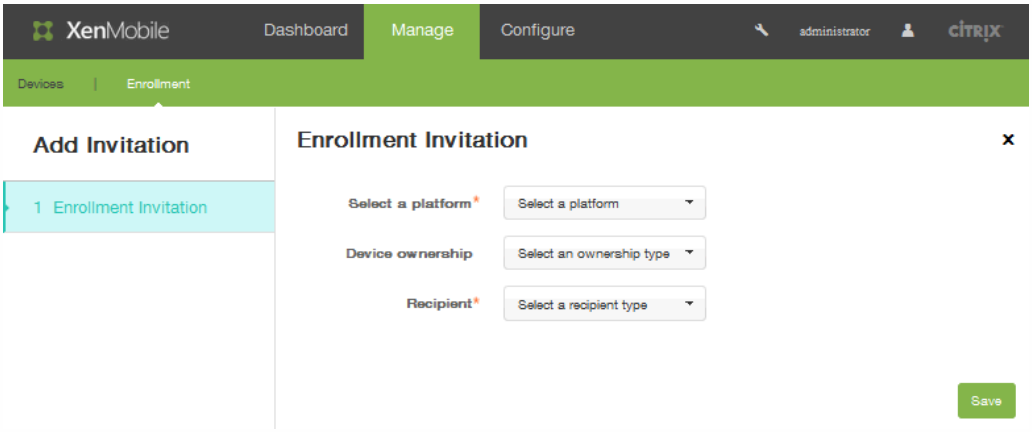


4. Klicken Sie in der Liste Select a platform auf iOS oder Android.
5. Klicken Sie in der Liste Device ownership auf Corporate oder Employee.
6. Klicken Sie in der Liste Recipient auf User oder Group. Wenn Sie als Empfänger "User" auswählen, werden weitere Konfigurationsoptionen eingeblendet. Folgen Sie den Schritten im entsprechenden Abschnitt zum Festlegen der Einladungseinstellungen nach Empfängertyp:

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.

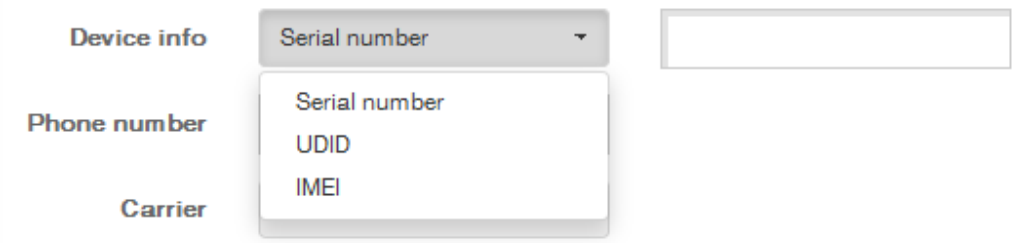


3. Klicken Sie auf Add Invitation. Die Seite Enrollment Invitation wird angezeigt.



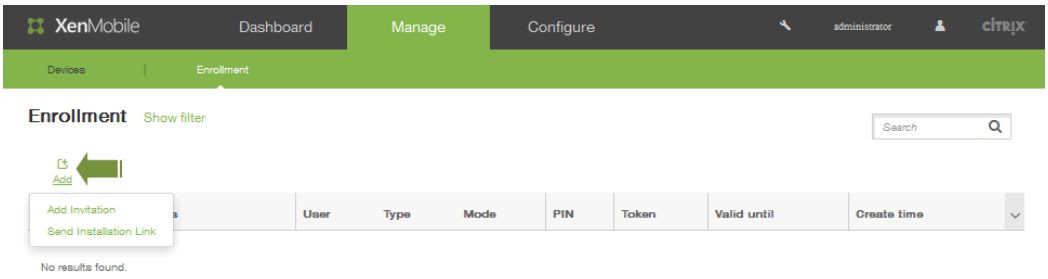
4. Klicken Sie in der Liste Select a platform auf iOS oder Android.
5. Klicken Sie in der Liste Device ownership auf Corporate oder Employee.
6. Klicken Sie in der Liste Recipient auf User. Auf der Benutzeroberfläche werden nun die Konfigurationsoptionen für die Benutzerregistrierung angezeigt:

7. Geben Sie in das Feld Username einen Benutzernamen ein. 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. Je nachdem, welche Option Sie auswählen, wird ein Feld eingeblendet, in dem Sie den entsprechenden Wert für das Gerät eingeben können:

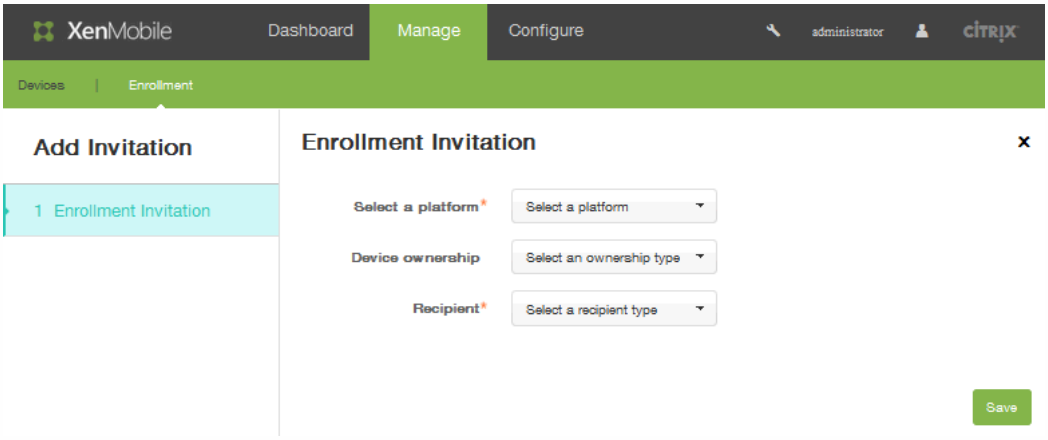


9. Geben Sie für Phone number optional eine Telefonnummer für den Benutzer ein.
10. Wählen Sie in der Liste Carrier den Netzbetreiber aus, der der Telefonnummer zugeordnet werden soll.
11. Wählen Sie in der Liste Enrollment mode die Option User name + Password (the default), High Security, Invitation 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. Klicken Sie für Send invitation auf ON.
16. Klicken Sie auf Speichern.

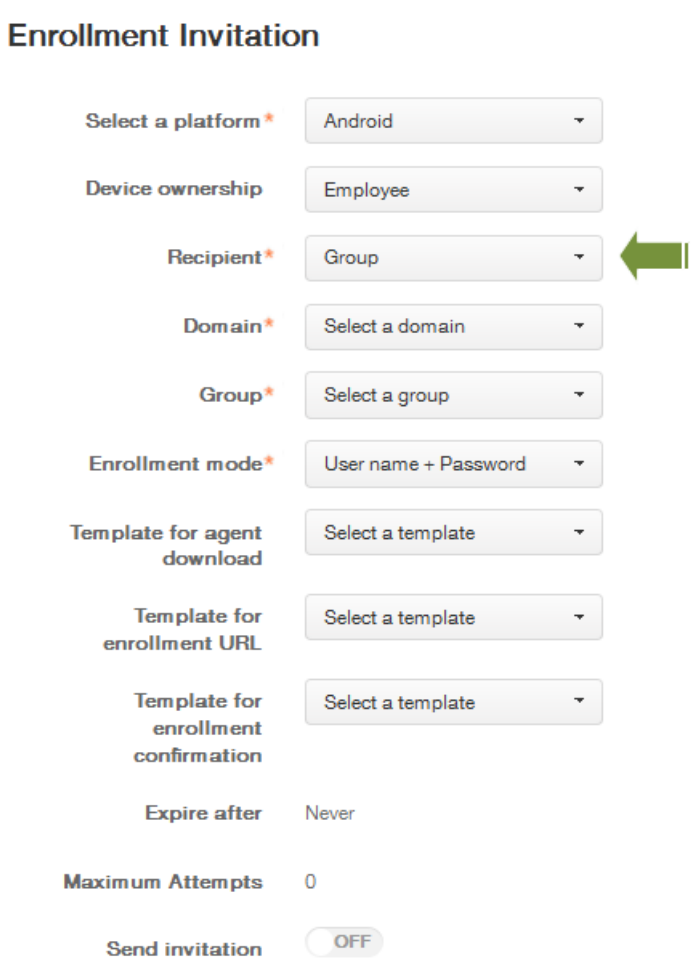
1. Klicken Sie in der XenMobile-Konsole auf Manage > Enrollment.
2. Klicken Sie auf der Seite Enrollment auf Add. Ein Menü wird eingeblendet, in dem Sie die Option zum Hinzufügen einer Einladung oder zum Senden eines Installationslinks auswählen können.



3. Klicken Sie auf Add Invitation. Die Seite Enrollment Invitation wird angezeigt.



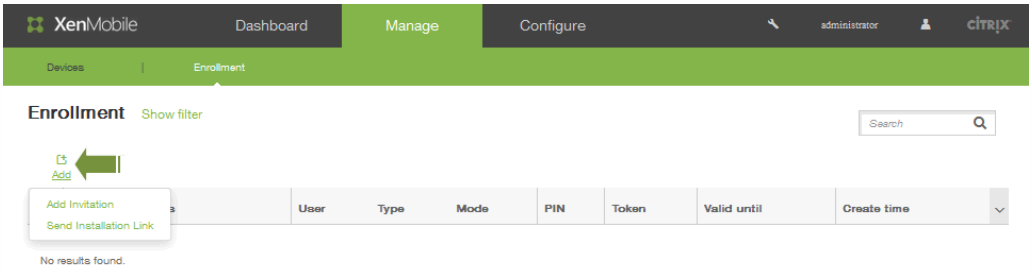
4. Wählen Sie in der Liste Select a platform die Option iOS oder Android aus.
5. Wählen Sie in der Liste Device ownership die Option Corporate oder Employee aus.
6. Wählen Sie in der Liste Recipient die Option Group aus. Auf der Benutzeroberfläche werden nun die Konfigurationsoptionen für die Gruppenregistrierung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



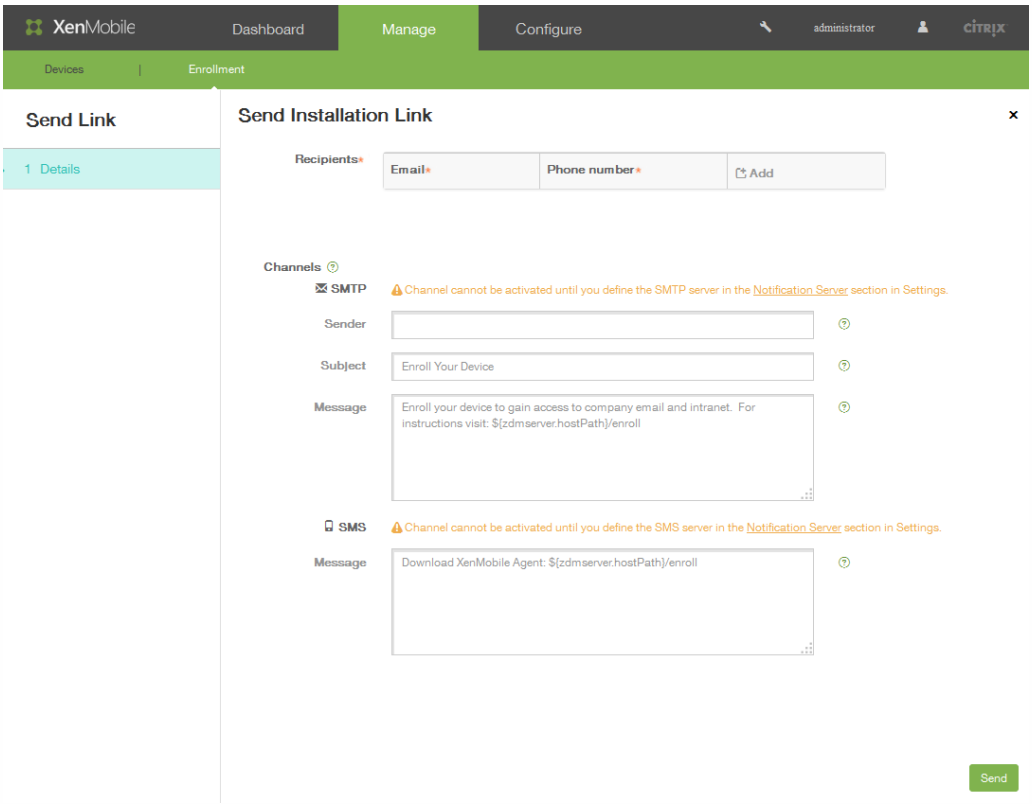
7. Wählen Sie für Domain die Domäne aus, in der die Empfängergruppe residiert.
8. Wählen Sie für Group die Gruppe aus, der Sie eine Registrierungsbenachrichtigung senden möchten.
9. Wählen Sie für Enrollment mode die Option User name + Password (Standardeinstellung), High Security, Invitation URL + PIN, Invitation URL + Password, Two Factor oder User name + PIN aus.
10. 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.
11. Wählen Sie für Template for enrollment URL die Option Enrollment Invitation aus.
12. 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.
13. Klicken Sie in Send invitation auf ON, um die Registrierungseinladung an die ausgewählte Gruppe zu senden.
14. Klicken Sie auf Speichern.

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.

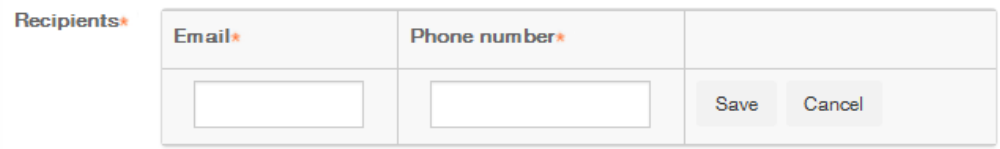
1. Klicken Sie in der XenMobile-Konsole auf Manage > Enrollment.
2. Klicken Sie auf der Seite Enrollment auf Add. Ein Menü wird eingeblendet, in dem Sie die Option zum Hinzufügen einer Einladung oder zum Senden eines Installationslinks auswählen können.



3. Klicken Sie auf Send Installation Link. Auf der Benutzeroberfläche werden die Optionen für Send Installation Link angezeigt.



4. Klicken Sie auf für Recipient auf Add, um einen Empfänger für den Registrierungslink anzugeben. Das Feld Recipient wird erweitert, damit Sie eine E-Mail-Adresse und Telefonnummer eingeben können.



5. Geben Sie im Feld Email die E-Mail-Adresse und im Feld Phone number die Telefonnummer des Empfängers des Installationslinks ein. Die Felder sind obligatorisch.
6. Wählen Sie unter Channelsden Kanal zum Senden des Installationslinks aus. Benachrichtigungen werden über SMTP oder SMS gesendet. **Hinweis**: SMTP oder SMS kann nur aktiviert werden, wenn die Servereinstellungen unter Configure > Settings > Notification Server konfiguriert wurden. Weitere Informationen finden Sie unter Benachrichtigungen in XenMobile.

7. 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.
8. Für SMTP-Benachrichtigungen geben Sie optional den Betreff unter Subject ein. Beispiel: "Registrieren Sie Ihr Gerät".
9. Geben Sie unter Message den Inhalt der Nachricht an den Empfänger ein. Beispiel: "Registrieren Sie Ihr Gerät für den Zugriff auf Unternehmens-E-Mail und -Intranet".
10. 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.
11. Klicken Sie auf Senden.

> 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.

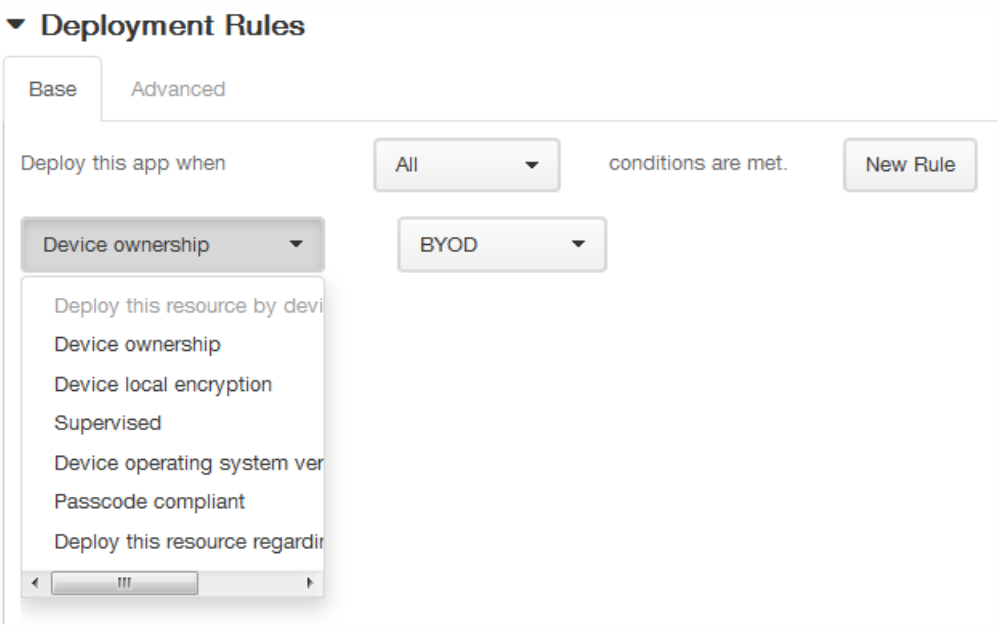
Oct 13, 2016

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.

Sie können eine beliebige Anzahl Parameter zur Steuerung der Paketbereitstellung festlegen.

Beispielsweise kann die Paketbereitstellung basierend auf einer bestimmten Betriebssystemversion, Hardwareplattform oder einer anderen Parameterkombination erfolgen. Der Assistent bietet 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 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.

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.

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: Die Standardeinstellung ist **EIN**. Wenn Sie eine Bereitstellung verhindern möchten, ändern Sie die Einstellung in **AUS**.

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.

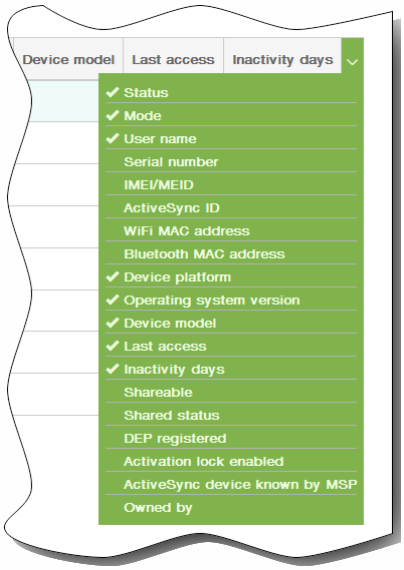
Hinzufügen von Geräten und Anzeigen von Gerätedetails

May 05, 2016

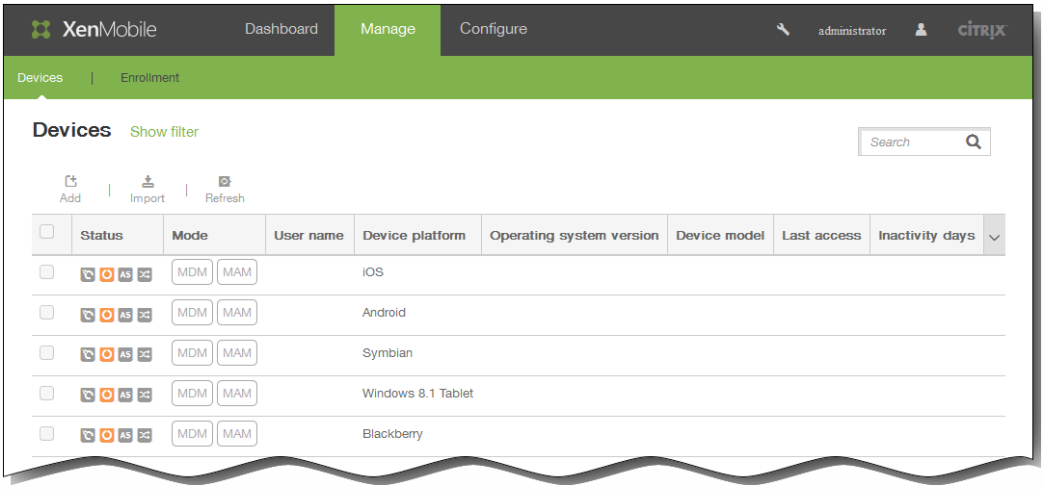
In der Repositorydatenbank auf dem XenMobile-Konsolenserver wird eine Liste der Mobilgeräte gespeichert. Jedes Mobilgerät ist durch eine eindeutige Seriennummer und/oder eine IMEI (International Mobile Station Equipment Identity) bzw. einen MEID (Mobile Equipment Identifier) gekennzeichnet. Sie können 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.

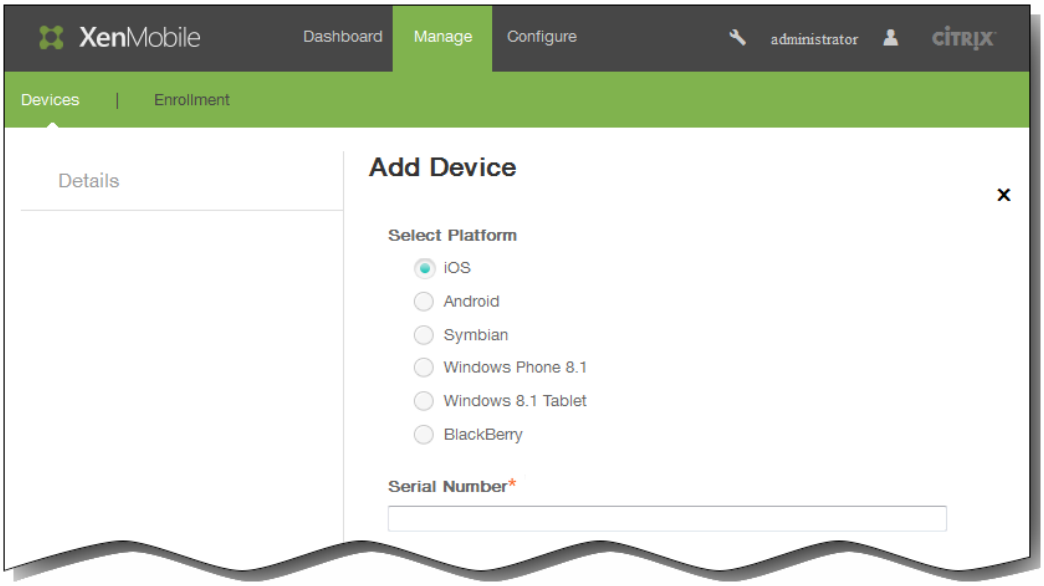
Hinweis: Die oben genannten Tabellenspalten sind die Standardspalten. Sie können die Tabelle anpassen, indem Sie auf den Pfeil nach unten in der letzten Spaltenüberschrift klicken und dann die Spaltenüberschriften aktivieren, die angezeigt werden sollen, bzw. diejenigen, die nicht angezeigt werden sollen,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



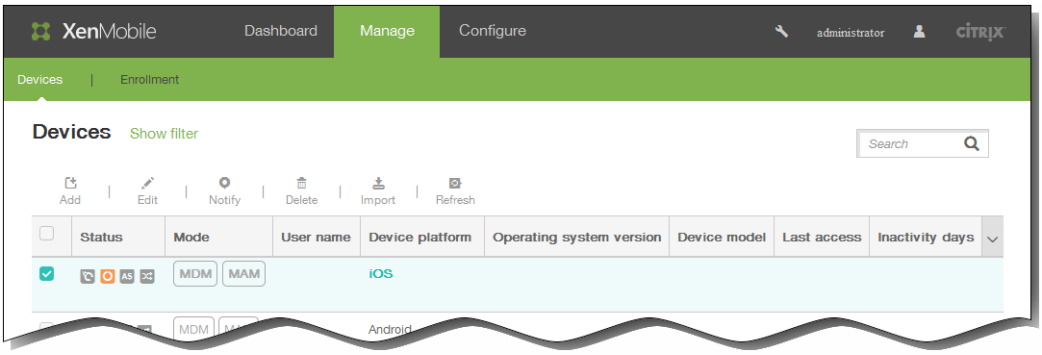
Sie können ein neues Gerät manuell durch Klicken auf Add oder per Import einer Provisioningdatei durch Klicken auf Import hinzufügen. Zum Aktualisieren der Tabelle klicken Sie auf Refresh.



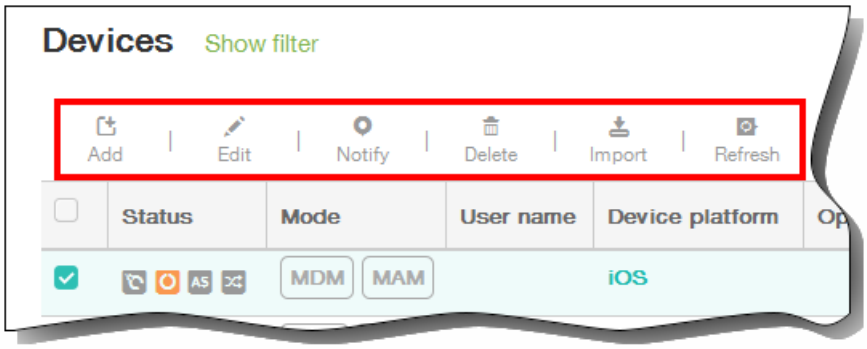
1. Klicken Sie in der XenMobile-Konsole auf ManageDevices und dann auf Add. Die Seite Add Device wird angezeigt.

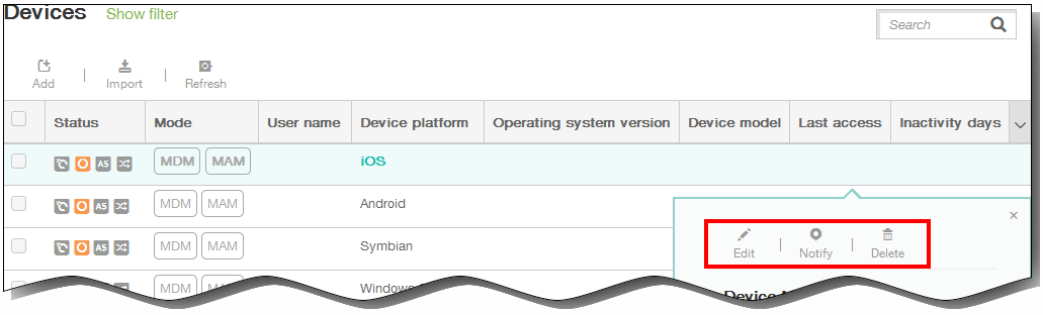


2. Klicken Sie unter Select platform auf iOS, Android, Symbian, Windows Phone 8.1, Windows 8.1 Tablet oder BlackBerry.
3. Geben Sie die folgenden Informationen ein:
   1. iOS: Geben Sie unter Serial Number die Seriennummer ein.
   2. Android: Geben Sie unter Serial Number die Seriennummer und die IMEI/MEID ein.
   3. Symbian: Geben Sie die IMEI/MEID ein.
   4. Windows Phone 8.1: Geben Sie unter Serial Number die Seriennummer und die IMEI/MEID ein.
   5. Windows 8.1 Tablet: Geben Sie unter Serial Number die Seriennummer und die IMEI/MEID ein.
   6. BlackBerry: Geben Sie unter Serial Number die Seriennummer und 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.

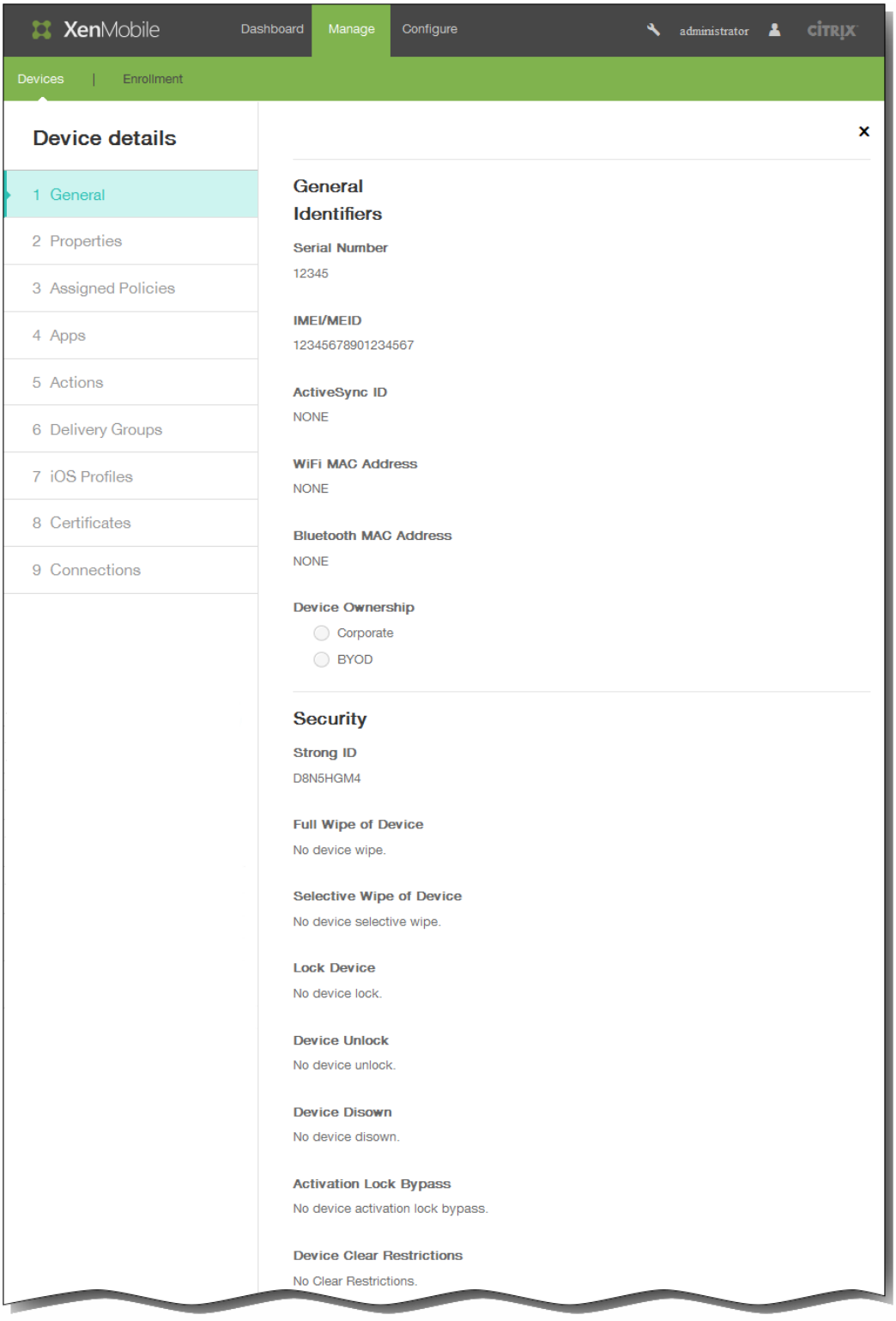


Hinweis: Wenn Sie das Kontrollkästchen neben einem Gerät auswählen, wird das Menü mit den Optionen oberhalb der Geräteliste eingeblendet. Wenn Sie auf eine andere Stelle im Eintrag klicken, wird es rechts neben dem Eintrag eingeblendet.

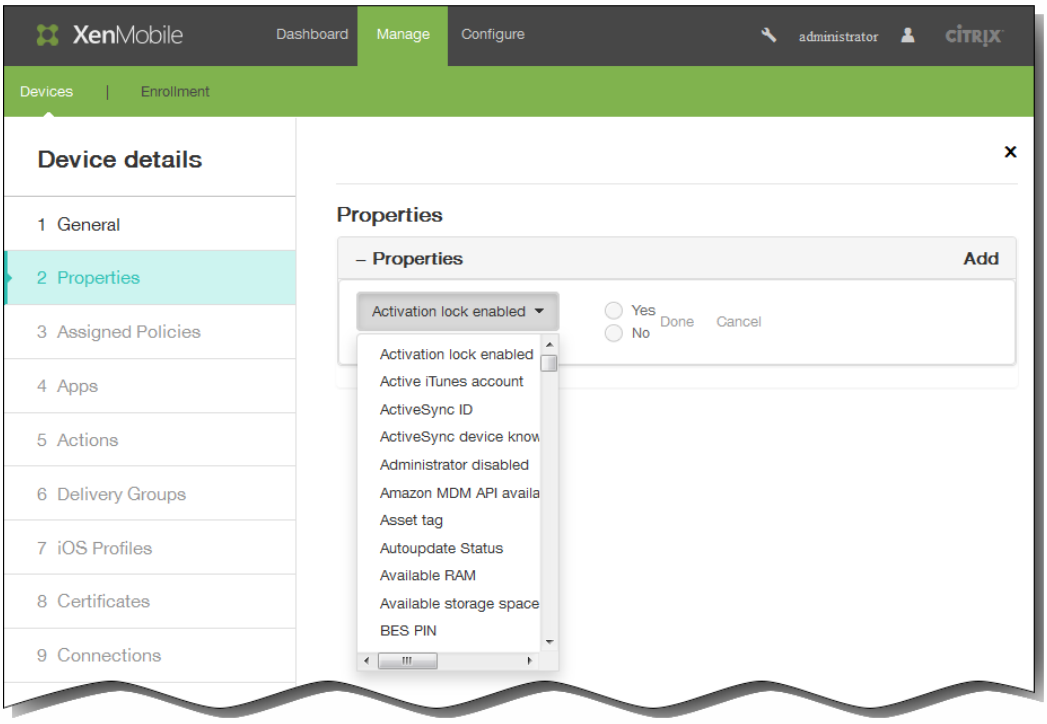




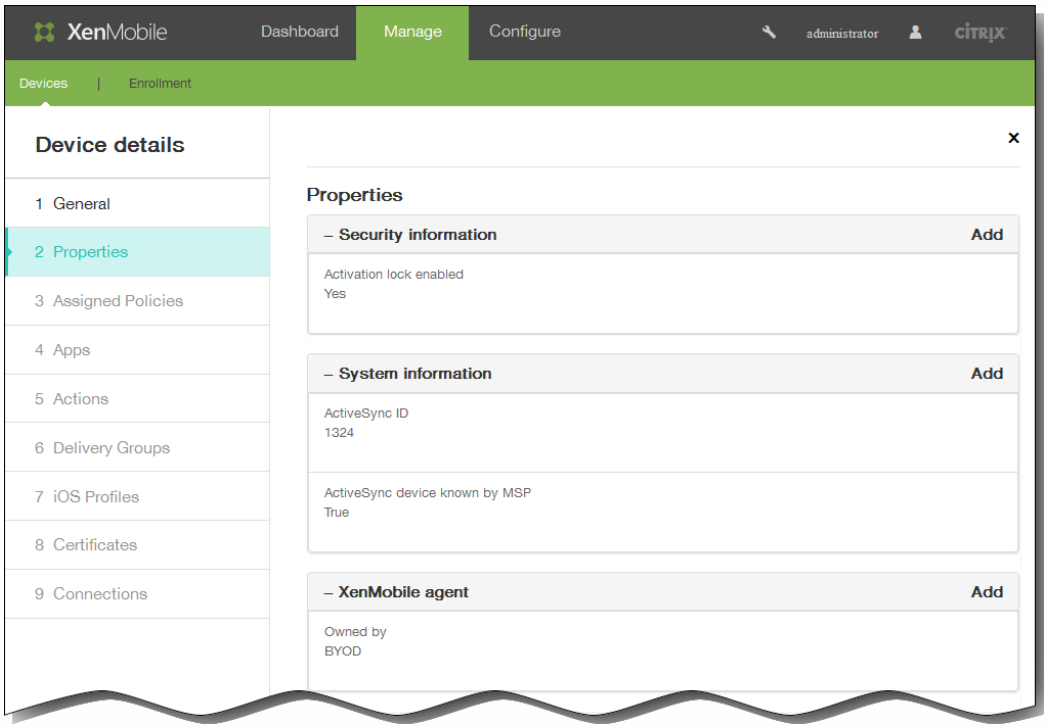
6. Prüfen Sie unter General Identifiers die angezeigten Informationen (welche Parameter angezeigt werden, hängt vom Plattformtyp ab): Seriennummer, IMEI/MEID, ActiveSync-ID, WiFi-MAC-Adresse, Bluetooth-MAC-Adresse, Geräteeigentümer: Corporate oder BYOD.



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. In der Abbildung oben ist beispielsweise die Eigenschaft Activation lock enabled ausgewählt, deren Wert Sie auf Yes oder No festlegen können.
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.



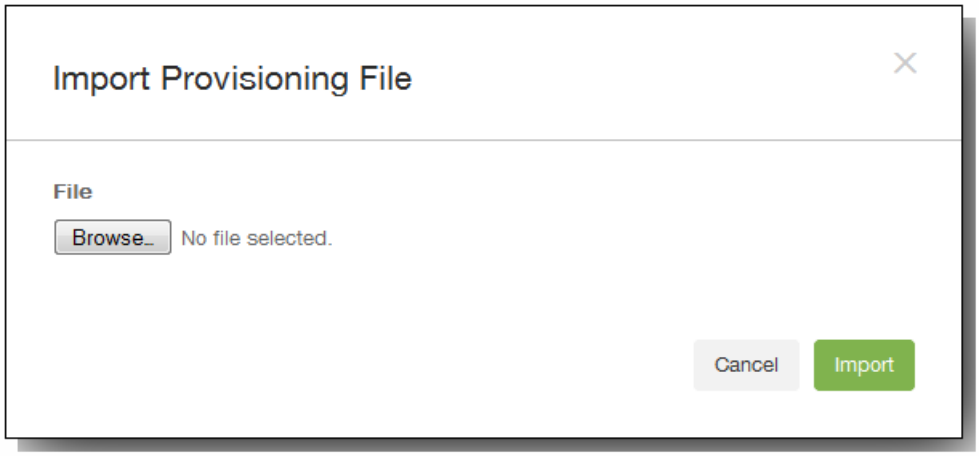
Der Bereich **Assigned Policies** und die nachfolgenden Bereiche enthalten zusammengefasste Informationen zu dem Gerät.

- 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 Speichern.

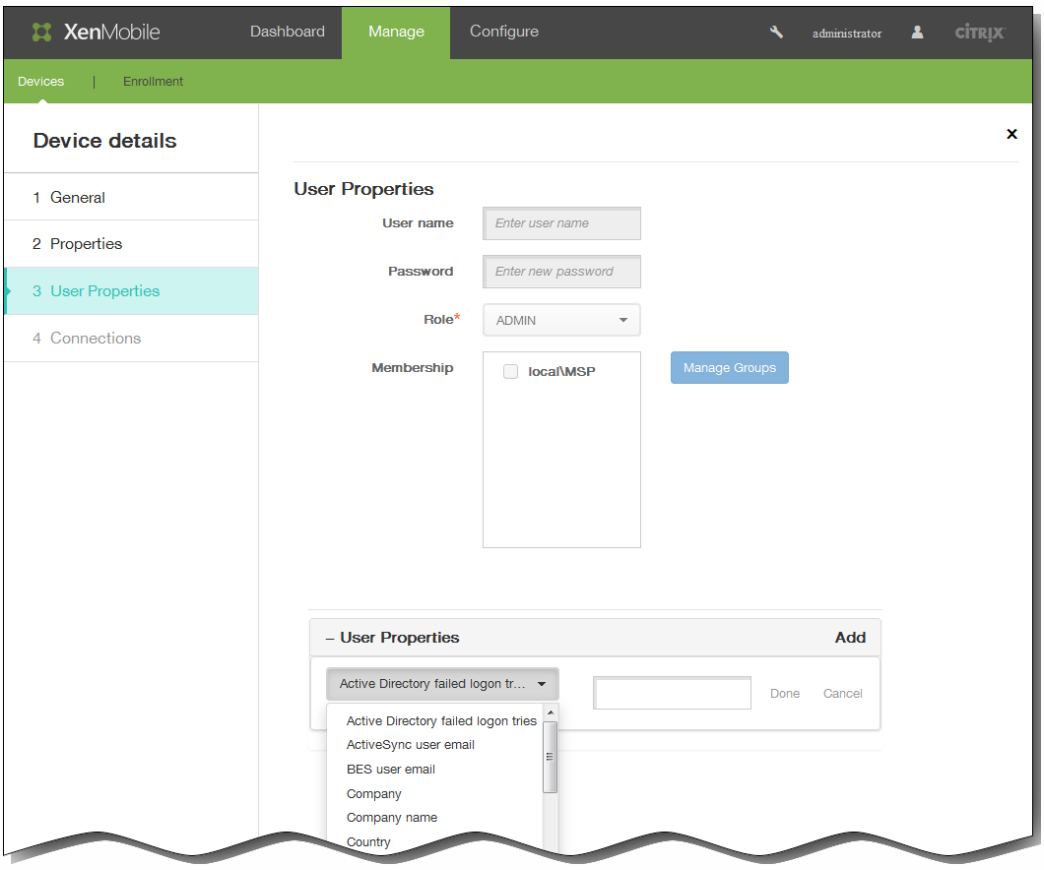
Sie können die Datei eines Mobilfunkanbieters oder Geräteherstellers oder Ihre eigene Provisioningdatei importieren. Siehe Geräte-Provisioningdateiformate.

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.

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.

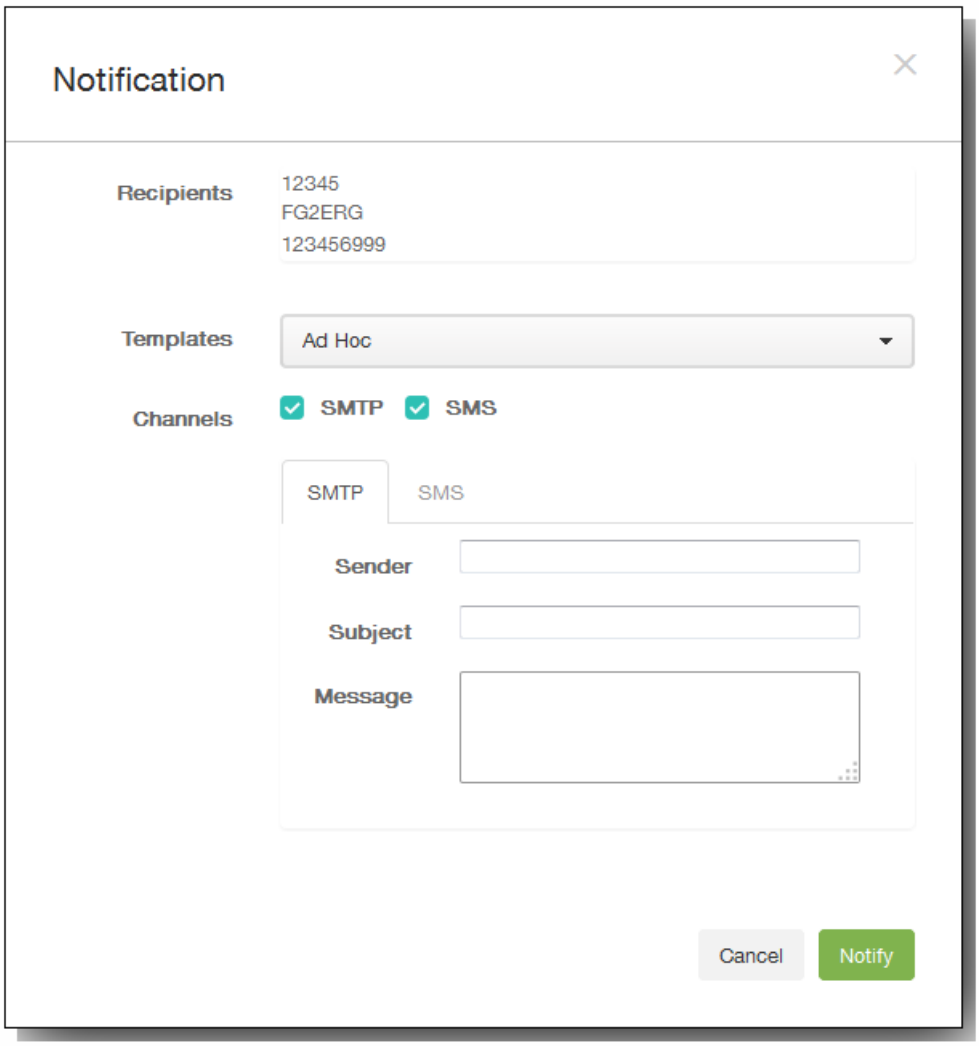
- Um eine Benutzereigenschaft hinzuzufügen, klicken Sie auf Add.
  - Klicken Sie in der Liste auf die gewünschte Eigenschaft, geben Sie den Wert ein und klicken Sie auf Done oder auf Cancel. Wiederholen Sie diese Schritte für jede Eigenschaft, die Sie hinzufügen möchten.
- Zum Bearbeiten klicken Sie 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.

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.

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.

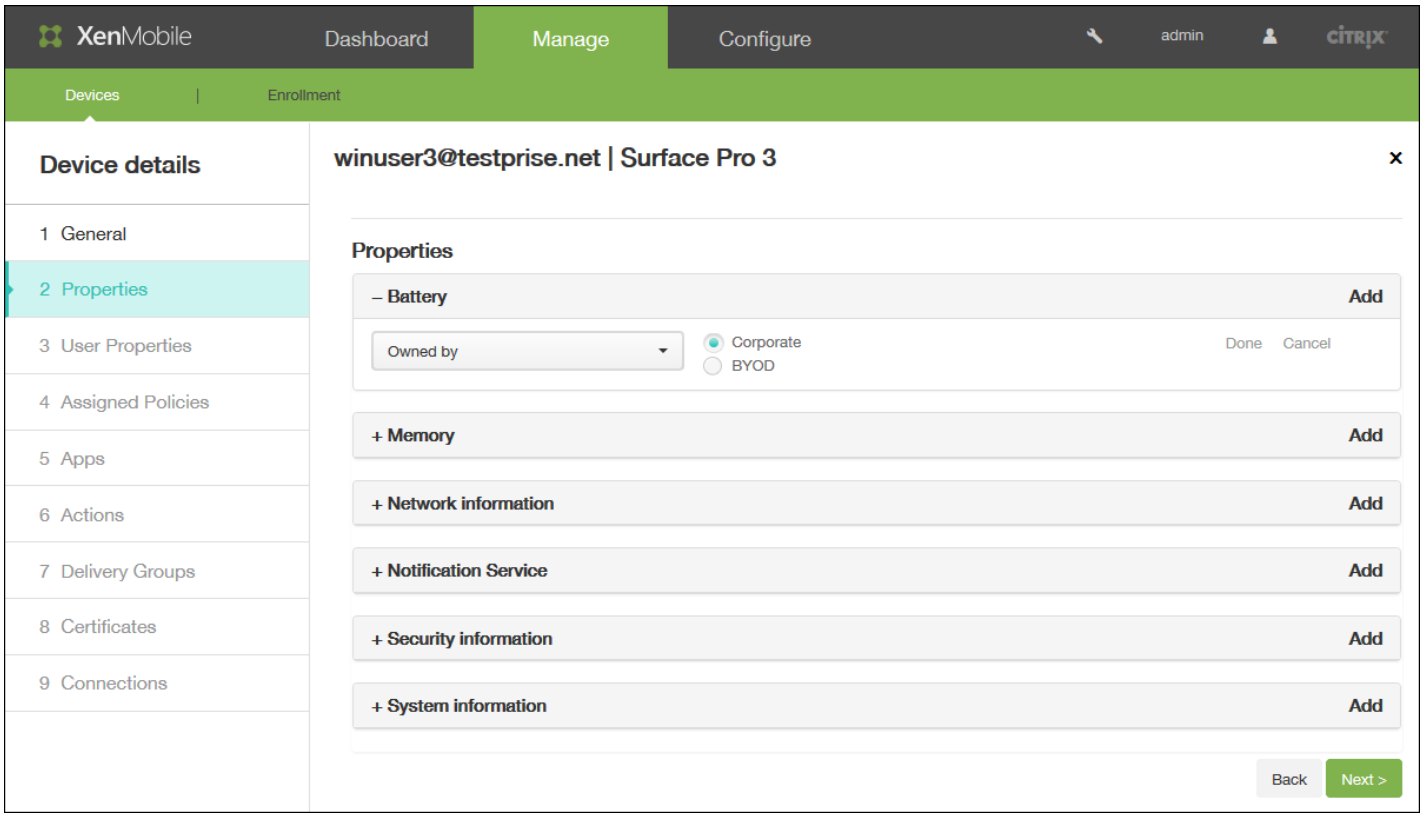
Manuelles Kennzeichnen von Benutzergeräten

May 05, 2016

Es gibt drei Möglichkeiten, Geräte in XenMobile manuell zu kennzeichnen:

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

Sie können das Gerät als Unternehmens- oder Privatgerät kennzeichnen. Bei der Registrierung eines Geräts über das Selbsthilfeportal können Sie es ebenfalls als Unternehmens- oder Privatgerät kennzeichnen. Wie in der folgenden Abbildung dargestellt können Sie das Gerät auch manuell kennzeichnen, indem Sie dem Gerät eine Eigenschaft hinzufügen. Öffnen Sie dazu in der XenMobile-Konsole die Registerkarte **Devices**, fügen Sie die Eigenschaft **Owned by** hinzu und wählen Sie **Corporate** oder **BYOD** (Privat).



Geräte-Provisioningdateiformate

May 05, 2016

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.

Die folgenden Zeilen beschreiben ein Gerät in einer Geräteprovisioningdatei.

1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyN;propertyV$*&&éééétest

3050BF3F517301081610065510590393;35244201625379903;iOS;test;

4050BF3F517301081610065510590393;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;

Der erste Eintrag bedeutet Folgendes:

- Seriennummer: 1050BF3F517301081610065510590391
- IMEI: 15244201625379901
- Betriebssystemfamilie: WINDOWS
- Eigenschaftsname: propertyN
- Eigenschaftswert: propertyV\;test\;1\;2;prop 2

Makros in XenMobile

May 05, 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.

Folgende Benutzermakros sind immer verfügbar:

- Anmeldename (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.

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

May 05, 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.

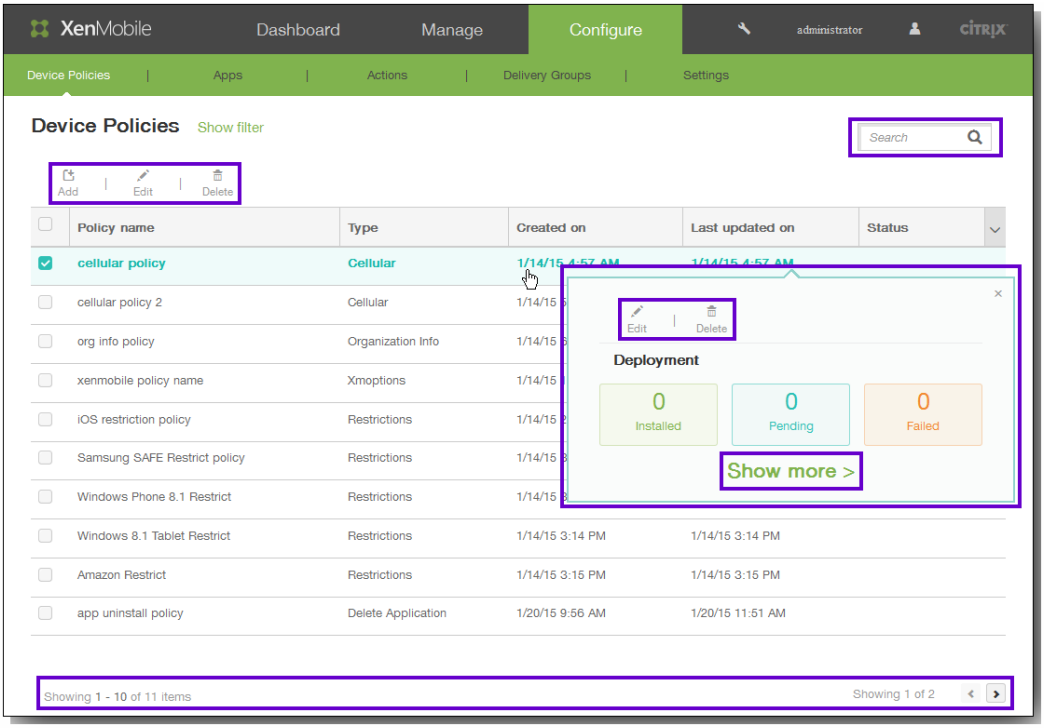
Das Erstellen einer Geräterichtlinie besteht im Wesentlichen aus folgenden Schritten:

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)

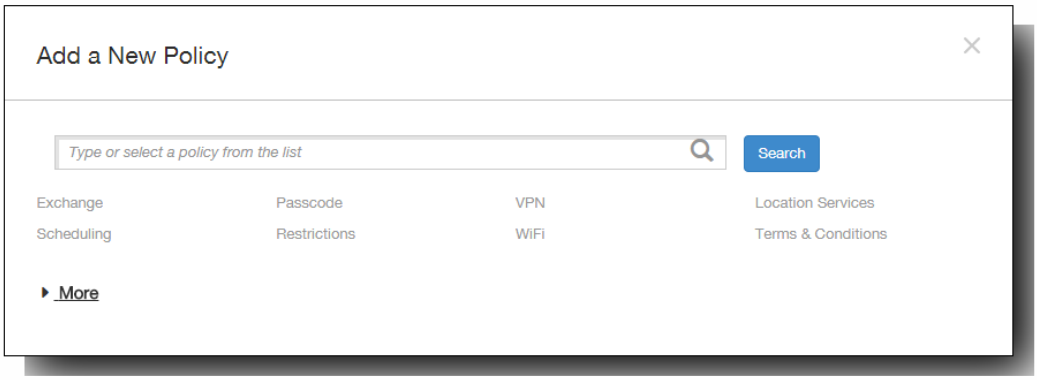
Die Arbeit mit Geräterichtlinien erfolgt in der XenMobile-Konsole auf der Seite Device Policies. Zum Aufrufen der Seite Device Policies klicken Sie auf Configure > Device Policies. Auf dieser Seite können Sie neue Richtlinien hinzufügen, den Status vorhandener Richtlinien prüfen und Richtlinien bearbeiten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

Die Seite Device Policies enthält eine Tabelle aller aktuellen Richtlinien.

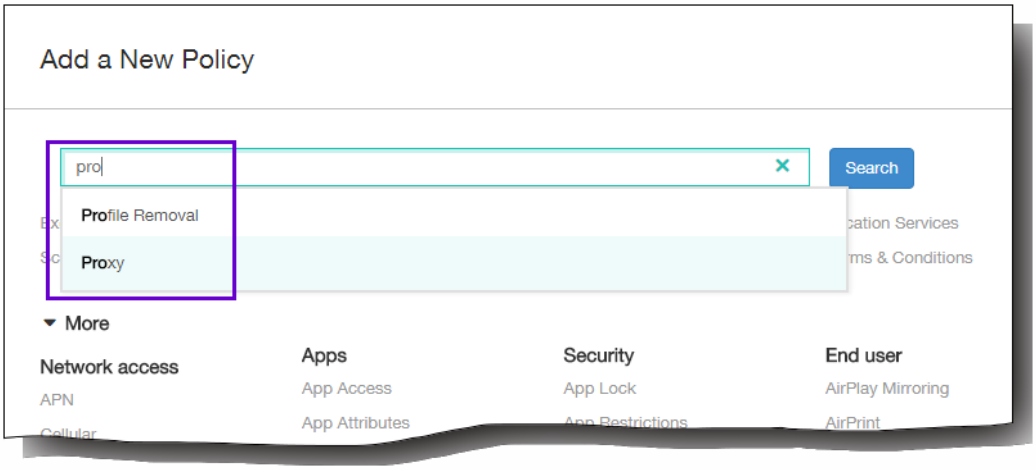
Zum Bearbeiten oder Löschen einer Richtlinie auf der Seite Device Policies können Sie das Kontrollkästchen neben der Richtlinie auswählen, um das Menü mit den Optionen oberhalb der Liste einzublenden, oder auf eine Richtlinie in der Liste klicken, um das Menü rechts neben dem Eintrag einzublenden. Wenn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



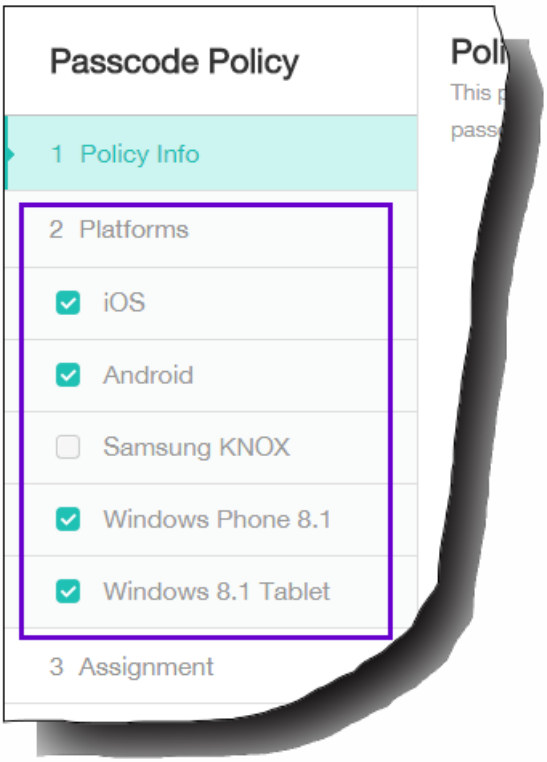
1. Klicken Sie auf der Seite Device Policies auf Add.
   Das Dialogfeld Add a New Policy wird angezeigt. Mit More können Sie weitere Richtlinien einblenden.



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.

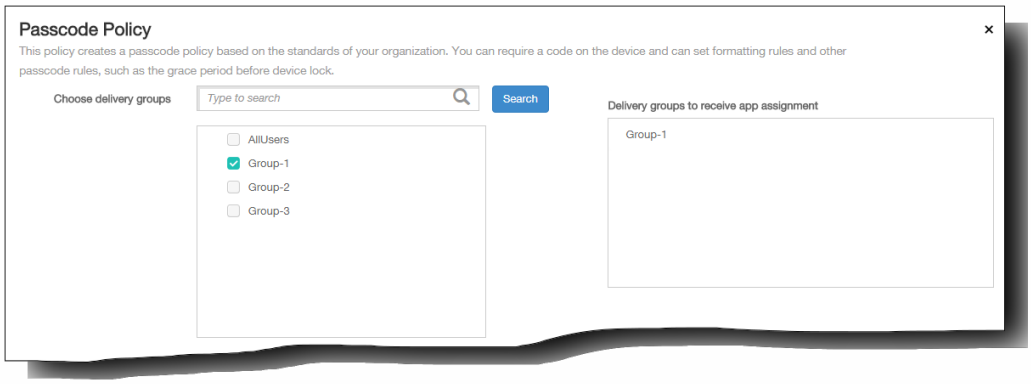


3. Wählen Sie die Plattformen aus, die Sie in die Richtlinie einschließen möchten. Die Seiten zur Konfiguration für die ausgewählten Plattformen werden in Schritt 5 angezeigt.
   Hinweis: Nur die von der Richtlinie unterstützten Plattformen werden aufgelistet.



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.

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

May 05, 2016

Die folgende Tabelle zeigt die Geräterichtlinien, die Sie in XenMobile 10.0 für Amazon-, iOS-, Android-, Samsung SAFE-, Samsung KNOX-, Symbian-, Windows Phone 8.1- und Windows 8.1 Tablet-Geräte konfigurieren können. 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	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1-Tablet
Allgemeines								
Exchange		X	X	X	X		X	
Planung			X			X		
Passcode		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	X	X
Network access								
APN		X	X		X			
Mobilfunk			X					
Persönlicher Hotspot		X						
Proxy		X						

Gerätericht linie	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1-Tablet
Remote Support					X			
Roaming		X						
Samsung-Firewall				X				
Tunnel			X					

	Amazon	iOS	Android	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						
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
Einschränkungen für App-Deinstallation	X			X				
Dateien			X					
Samsung-Browser				X	X			

Geräterichtlinie	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1-Tablet
Sideloading-Schlüssel								X
Signaturzertifikat								X
Webclip		X	X					X
Worx Store		X	X					X
	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1-Tablet
Security								
App-Sperre		X	X					
App-Einschränkungen					X			
Kontakte (CardDAV)		X						
Anmeldeinformationen		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		

Geräterichtlinie XenMobile-Deinstallation	Amazon	iOS	Android X	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1-Tablet
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						

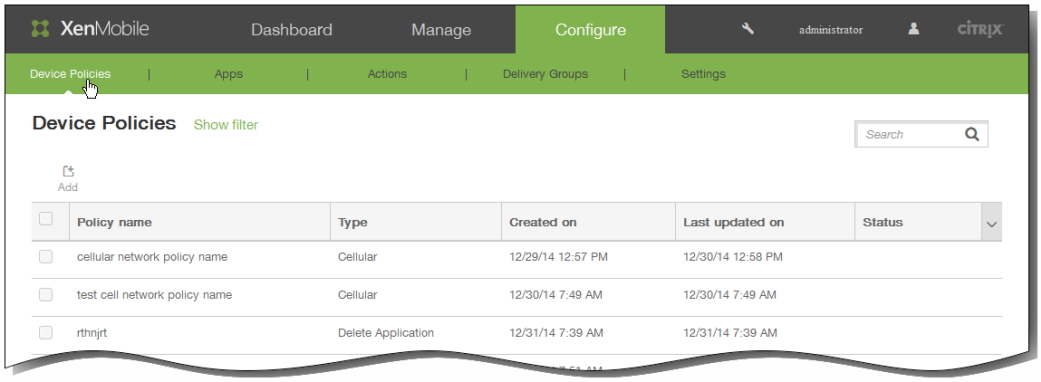
So fügen Sie eine App-Zugriffsrichtlinie für Geräte hinzu

May 05, 2016

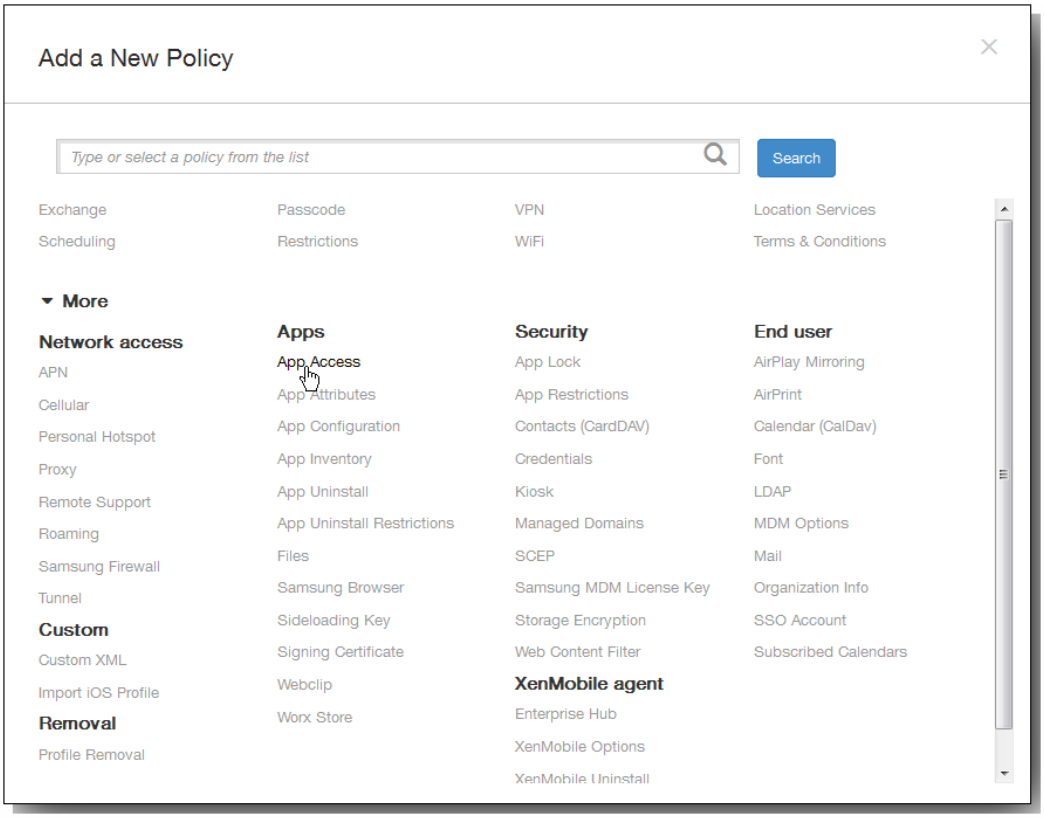
Über eine App-Zugriffsrichtlinie für Geräte können Sie in XenMobile eine Liste der Apps definieren, die auf Geräten installiert werden müssen, nach Wahl installiert werden können oder nicht installiert werden dürfen. Sie können dann eine automatisierte Aktion erstellen, mit der die Reaktion auf die Richtlinientreue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

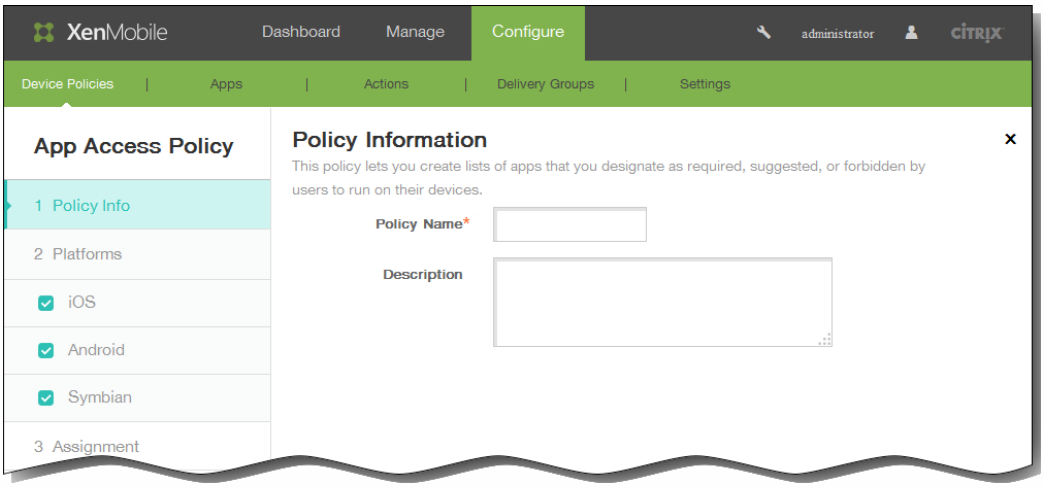
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies.



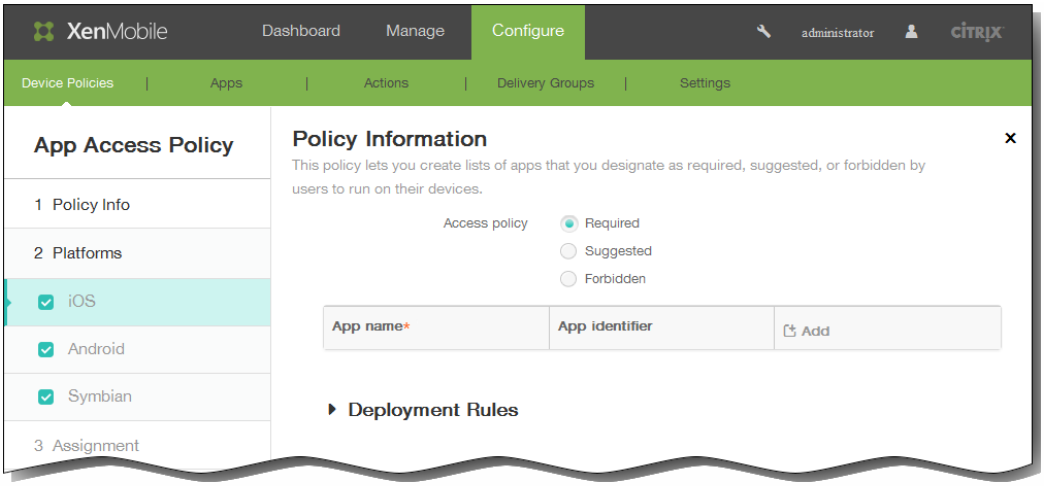
2. Klicken Sie auf Add. Das Dialogfeld Add a New Policy wird angezeigt.



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.

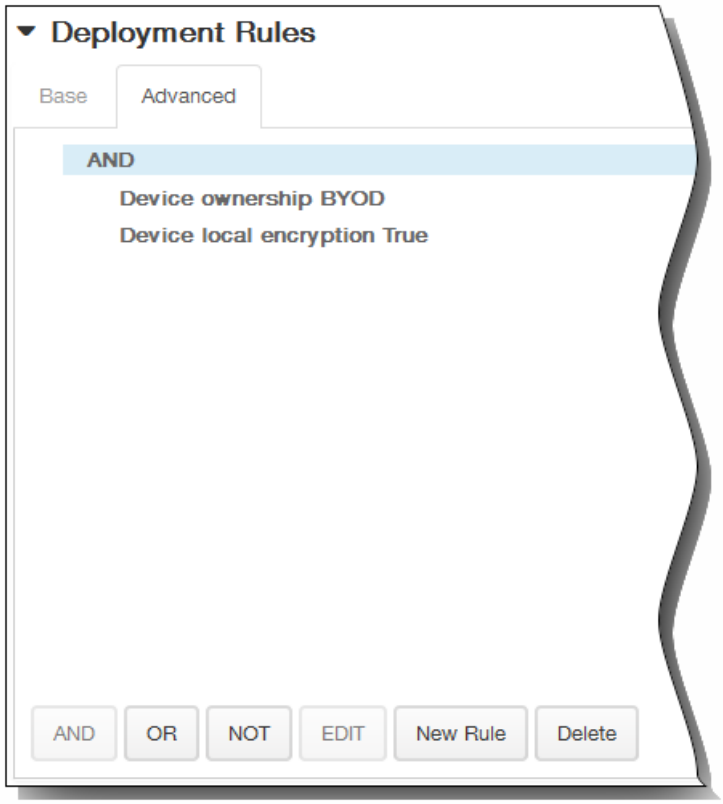
      Zum Bearbeiten einer App zeigen Sie auf deren Zeile und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf Save, um die Änderungen zu speichern oder auf Cancel, um den Vorgang abzubrechen.

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.

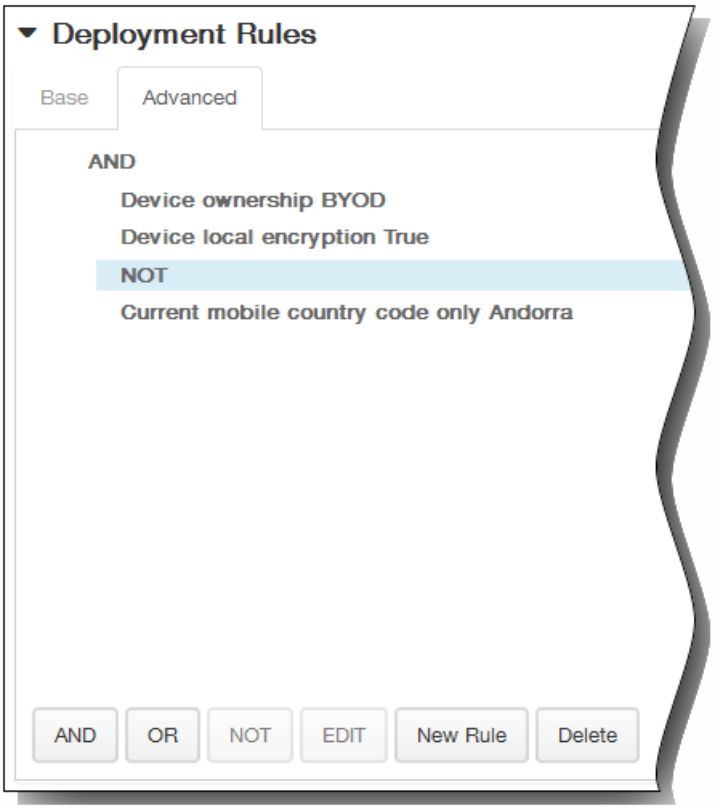
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



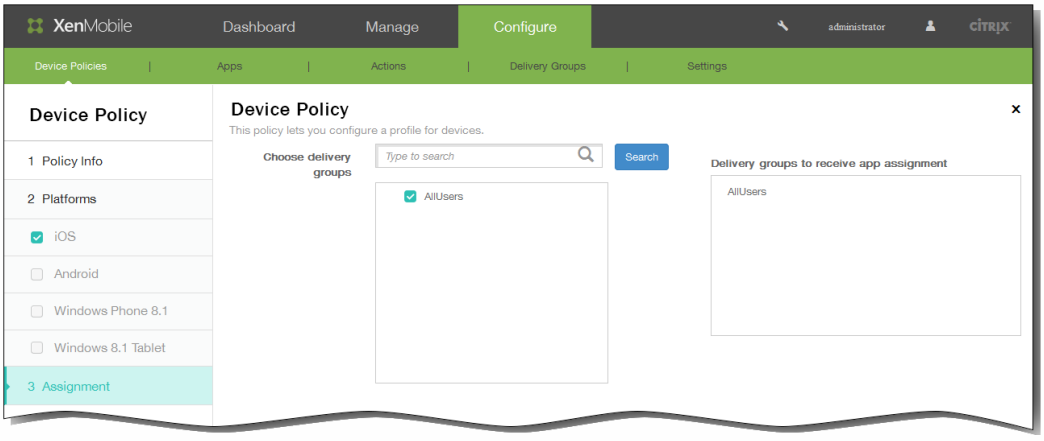
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



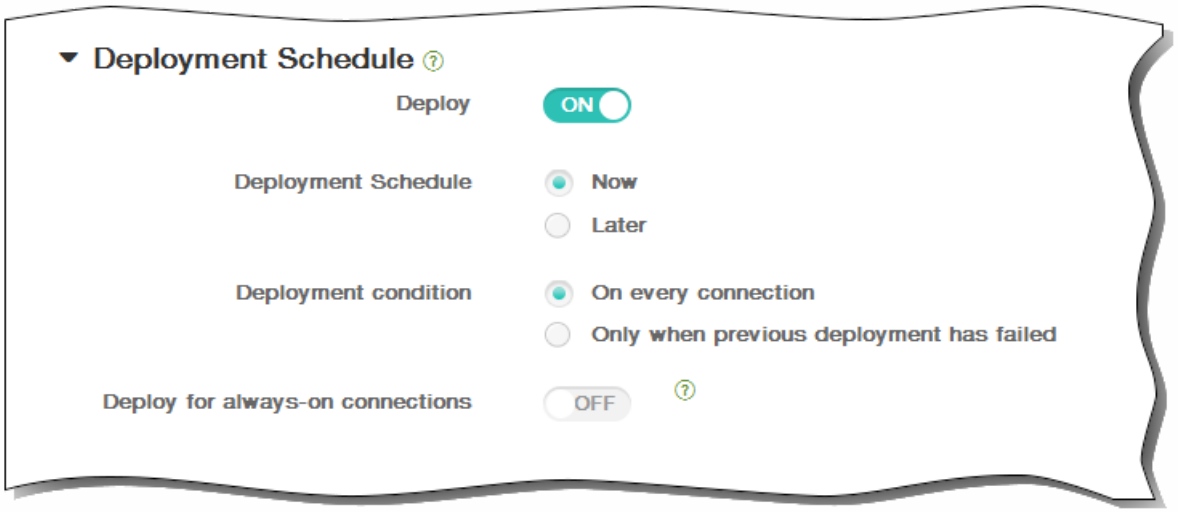
8. Klicken Sie auf Next. Der Seite für die nächste Plattform bzw. die Seite Assignment wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten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

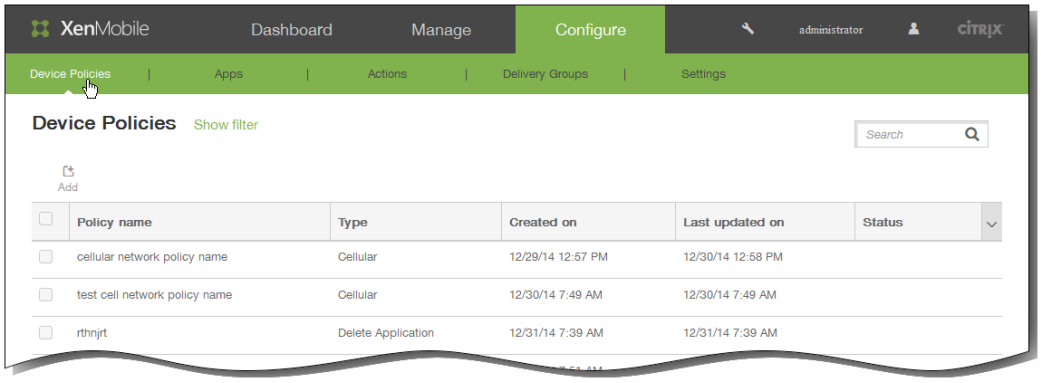
So fügen Sie eine App-Bestandsrichtlinie für Geräte hinzu

May 05, 2016

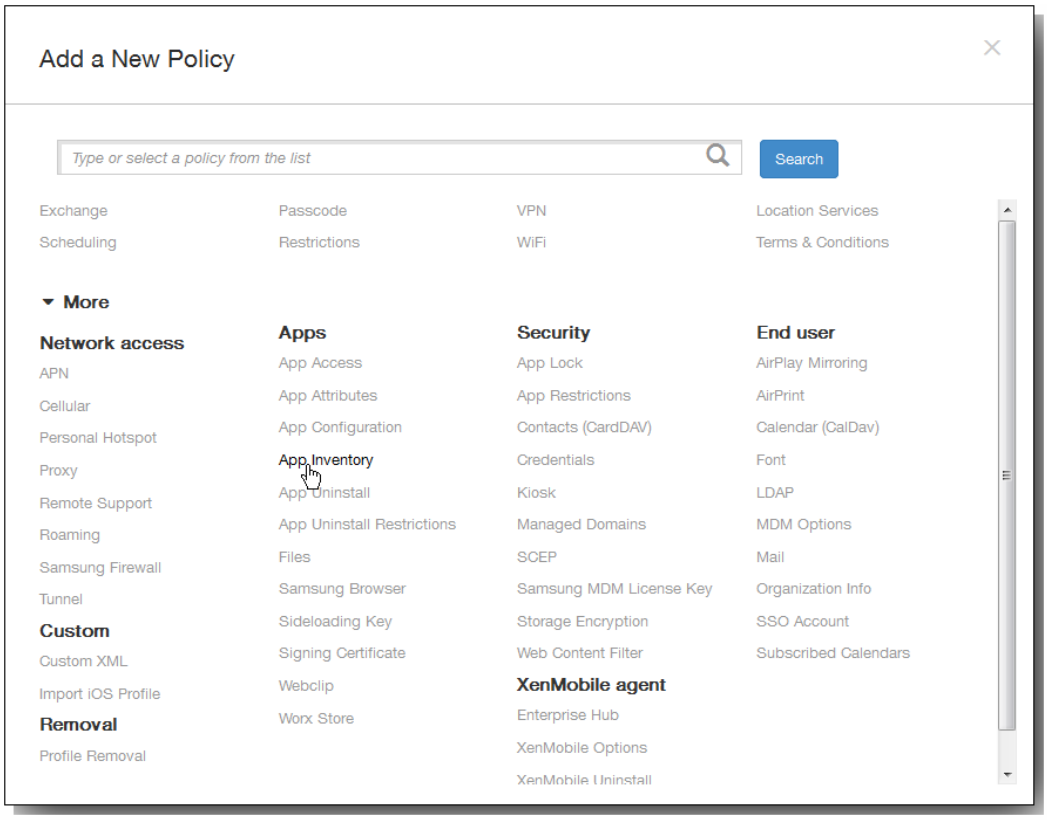
Mit einer App-Bestandsrichtlinie können Sie in XenMobile einen Bestand der Apps auf verwalteten Geräten sammeln und dann mit allen auf diesen Geräten bereitgestellten App-Zugriffsrichtlinien vergleichen. Auf diese Weise können Sie Apps erkennen, die in einer App-Sperrliste (d. h. in einer App-Zugriffsrichtlinie 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.

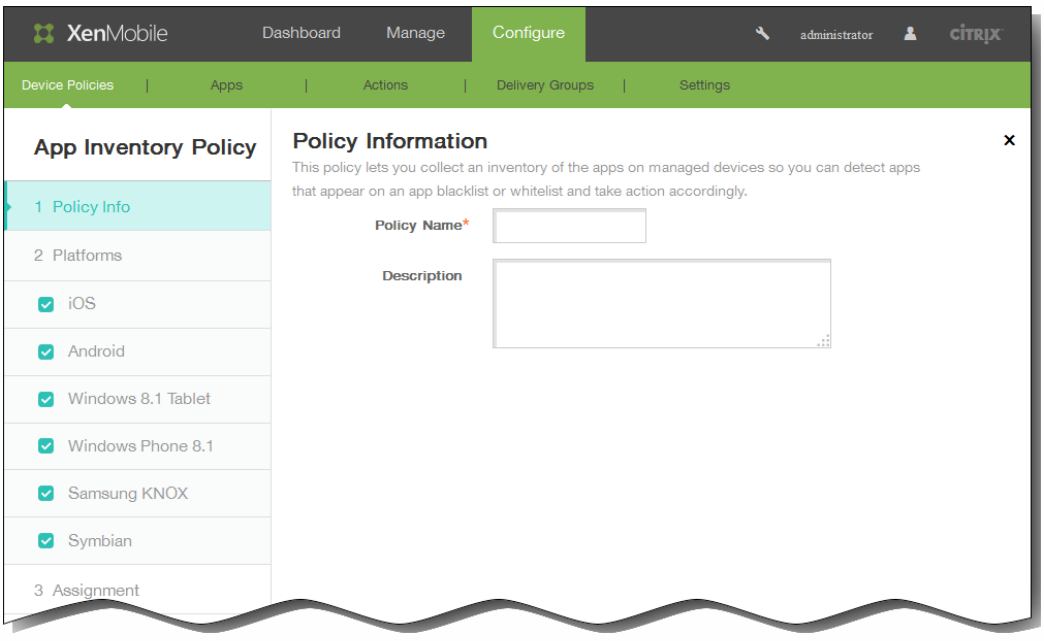
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



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

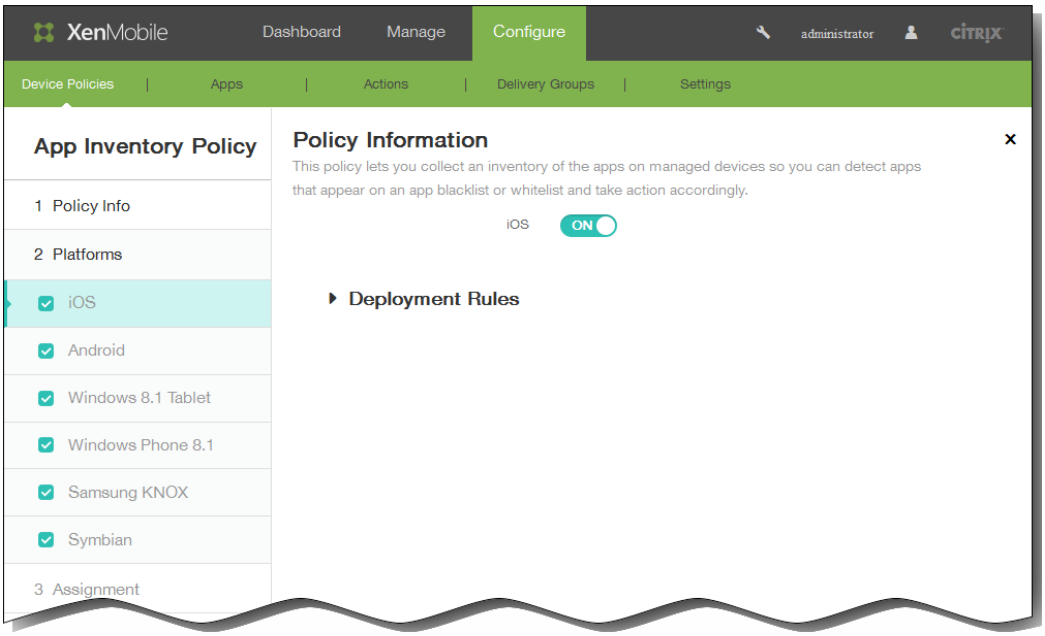


3. Klicken Sie auf More > App Inventory. Die Seite App Inventory Policy wird angezeigt.



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.

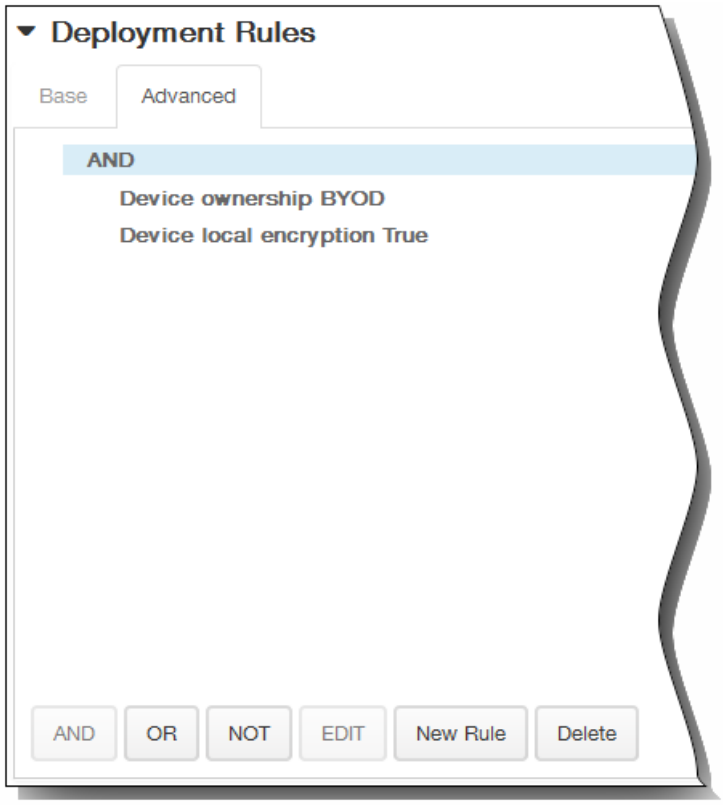
Hinweis: Auf der Seite Policy Platforms sind alle Plattformen ausgewählt, der Konfigurationsbereich für die iOS-Plattform wird als erstes angezeigt.



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.

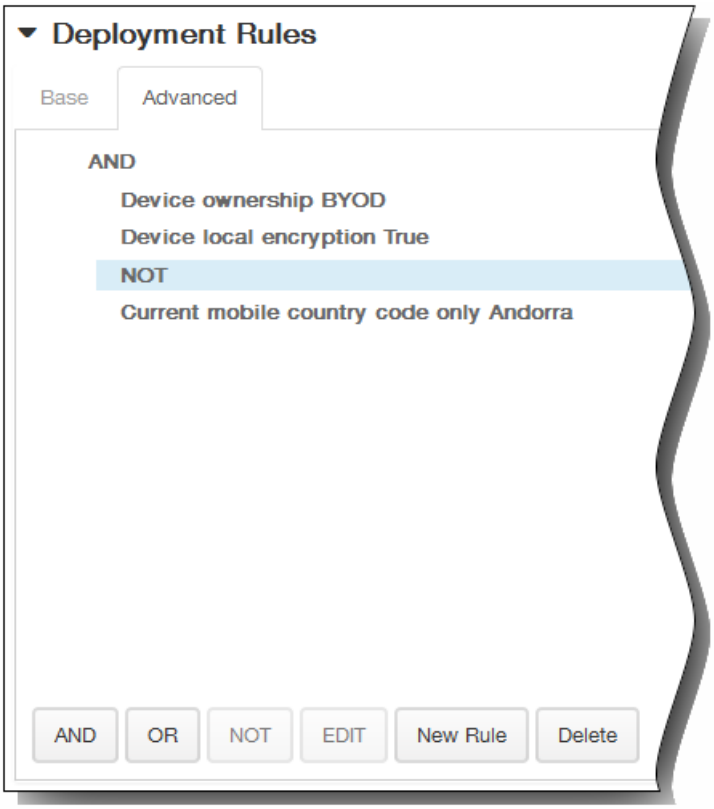
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen 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.



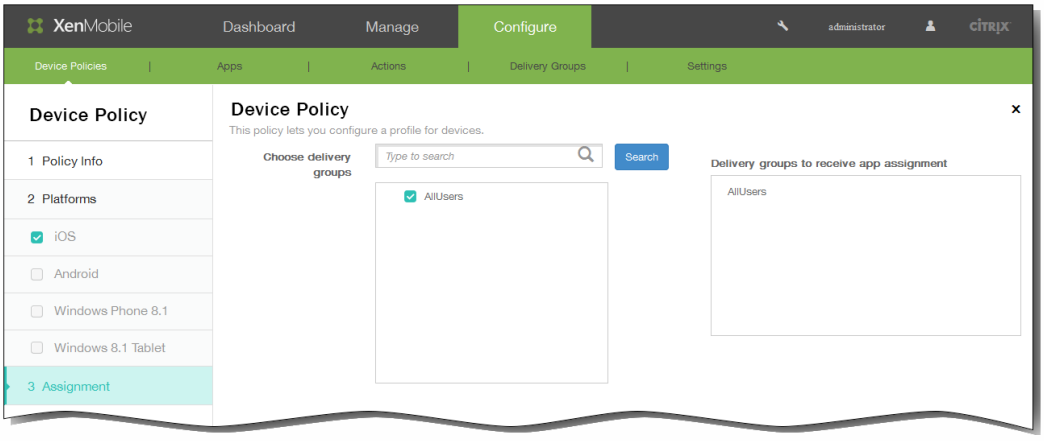
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



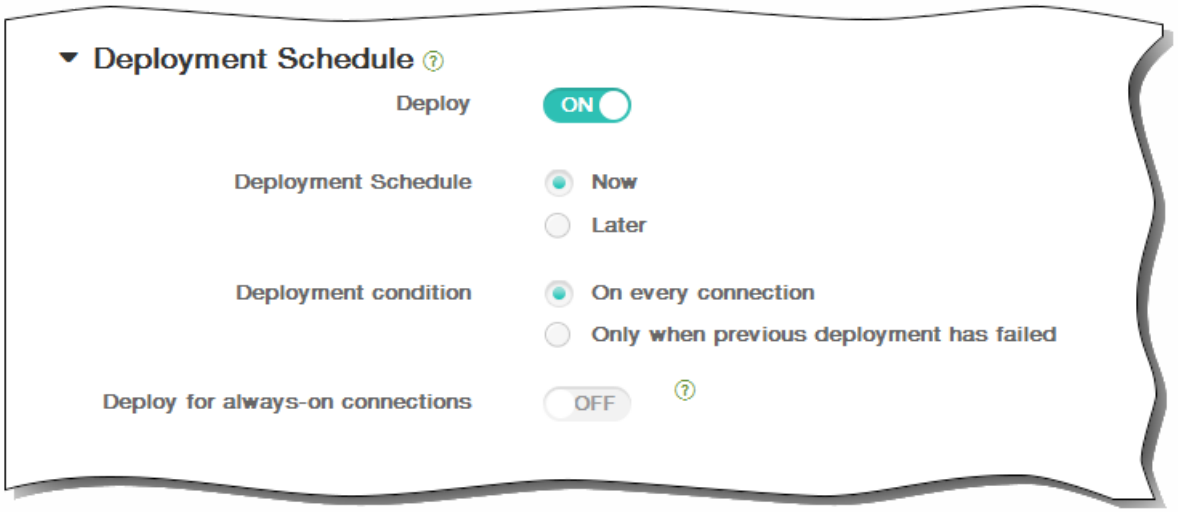
8. Klicken Sie auf Next. Der Seite für die nächste Plattform bzw. die Seite Assignment wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten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

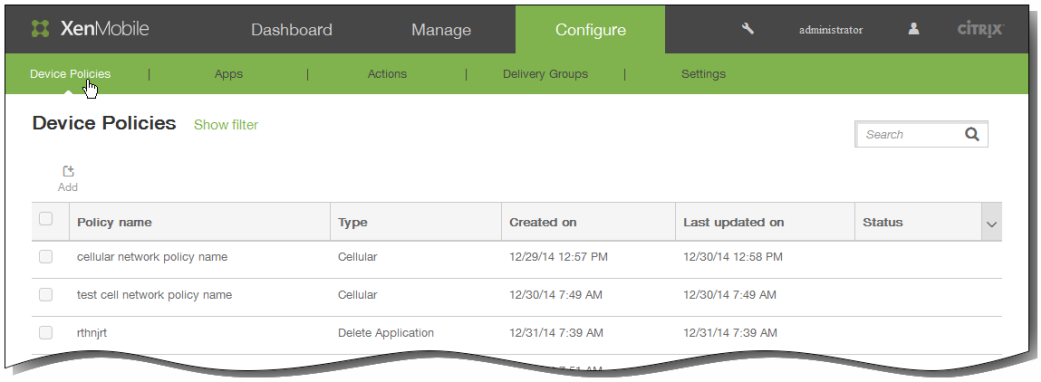
So fügen Sie eine App-Tunnelrichtlinie für Android-Geräte hinzu

May 05, 2016

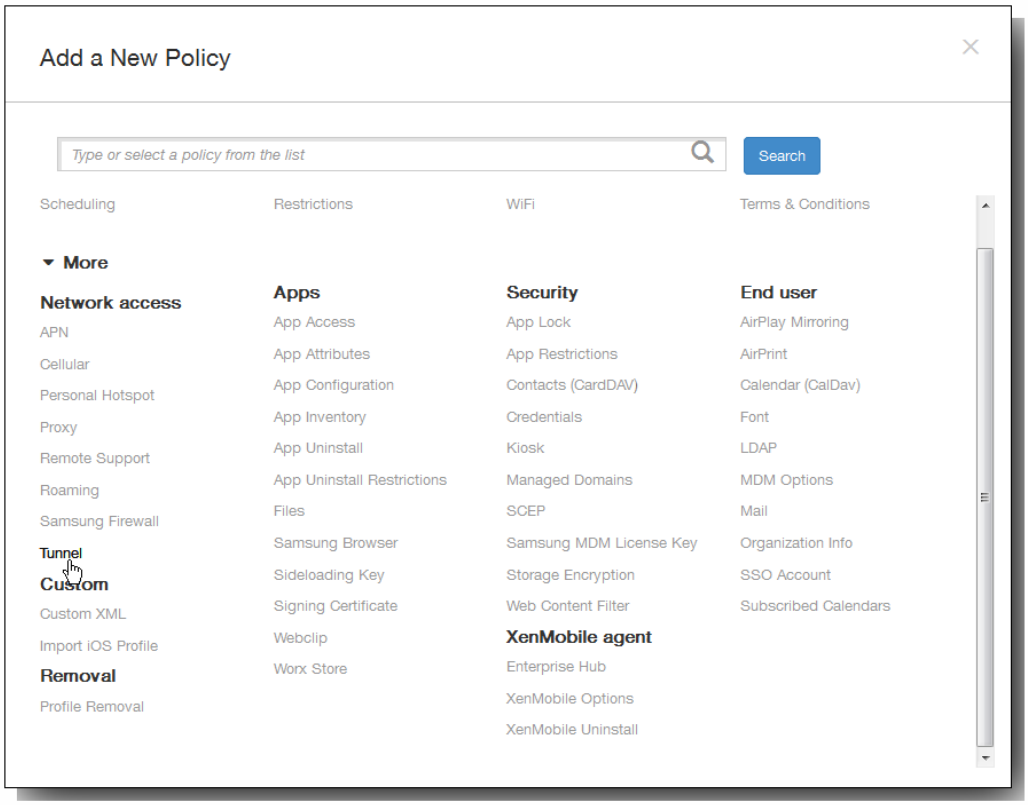
App-Tunnel verbessern die Dienstkontinuität und die Zuverlässigkeit bei der Datenübertragung für mobile Apps. Mit App-Tunneln werden Proxyparameter zwischen der Clientkomponente beliebiger Mobilgeräte-Apps und der App-Serverkomponente definiert. Sie können App-Tunnel auch für den Remotesupport auf Geräten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

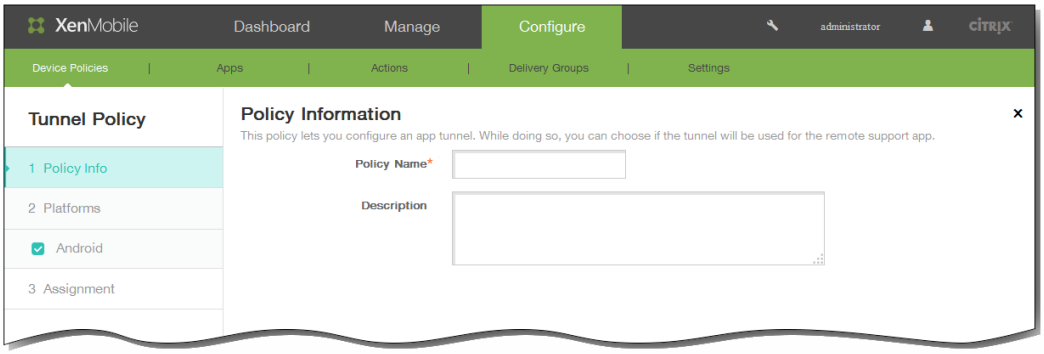
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



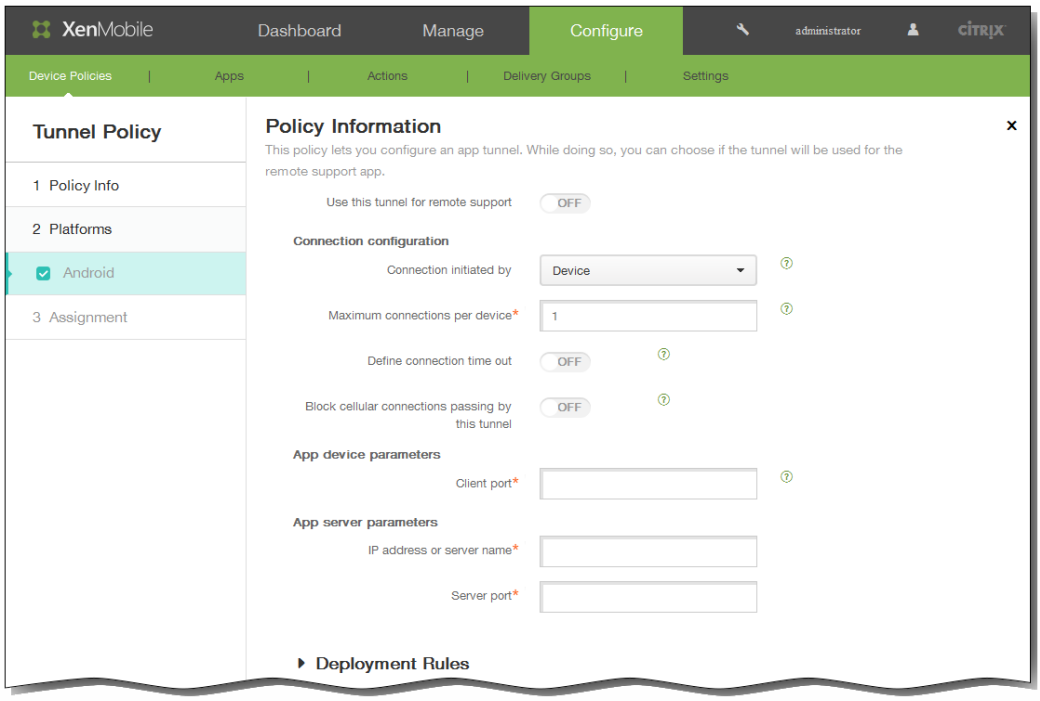
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



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.

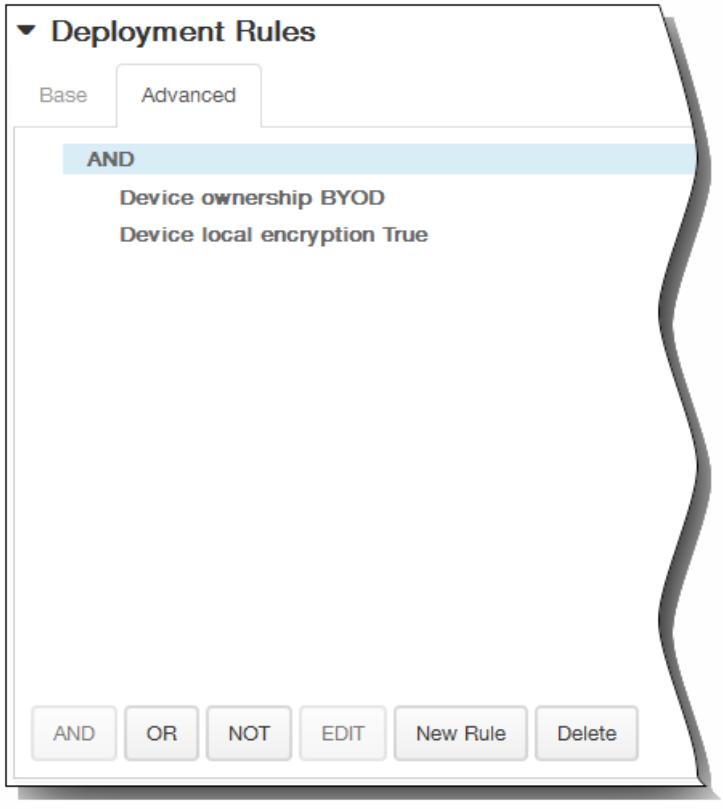


6. Geben Sie in Use this tunnel for remote support an, ob der Tunnel für Remotesupport verwendet werden soll.
   Hinweis: Die Konfigurationsschritte unterscheiden sich je nachdem, ob Sie hier Remotesupport auswählen.
   Wenn Sie Remotesupport **nicht auswählen**, führen Sie folgende Schritte aus:
   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.

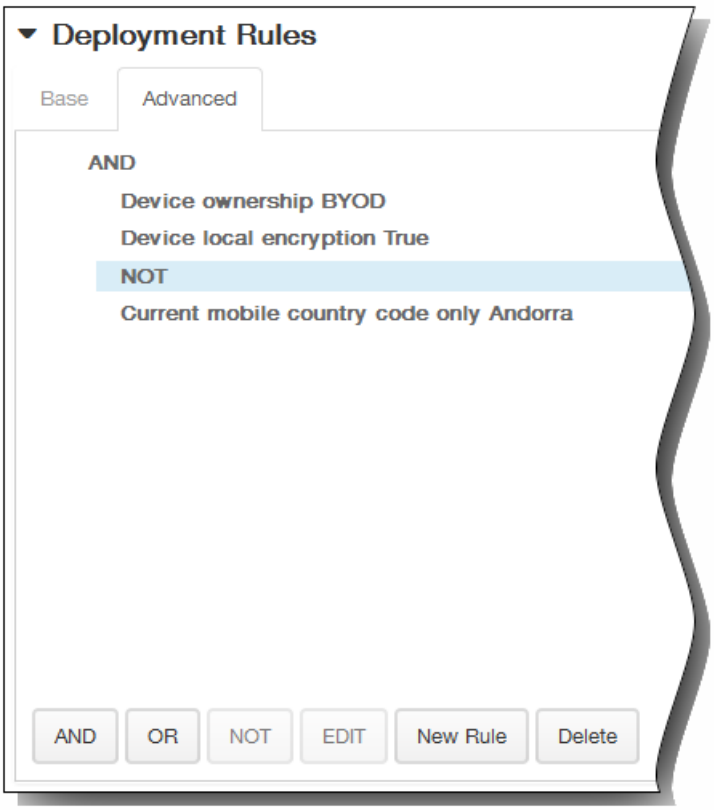
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



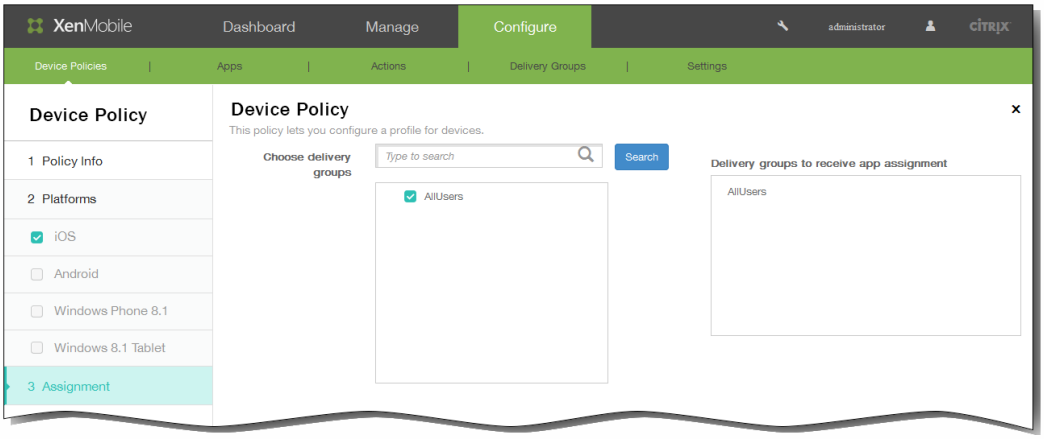
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.

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.

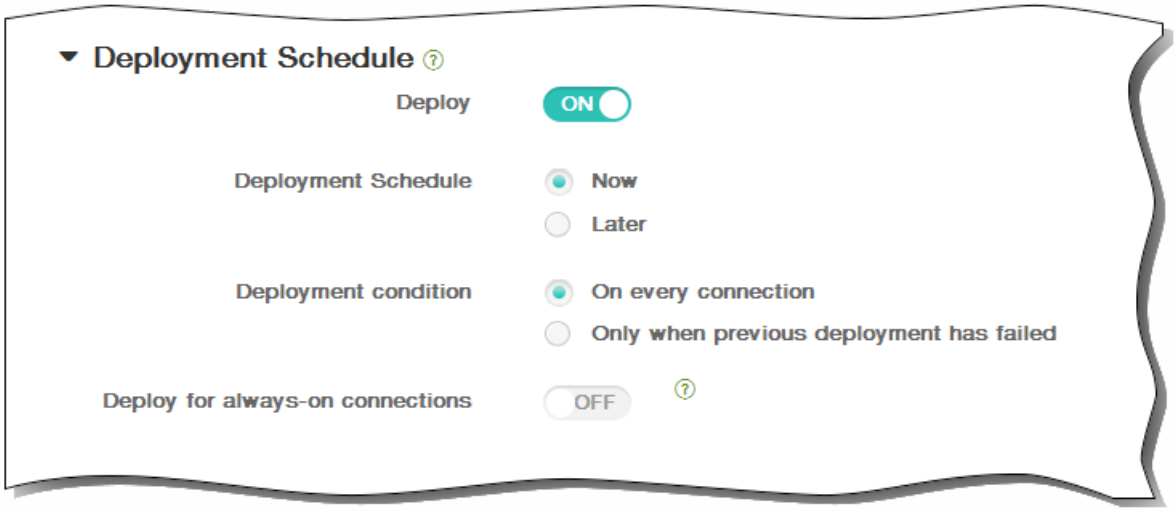


8. Klicken Sie auf Next. Die Seite Tunnel Policy zum Zuweisen der Tunnelrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten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

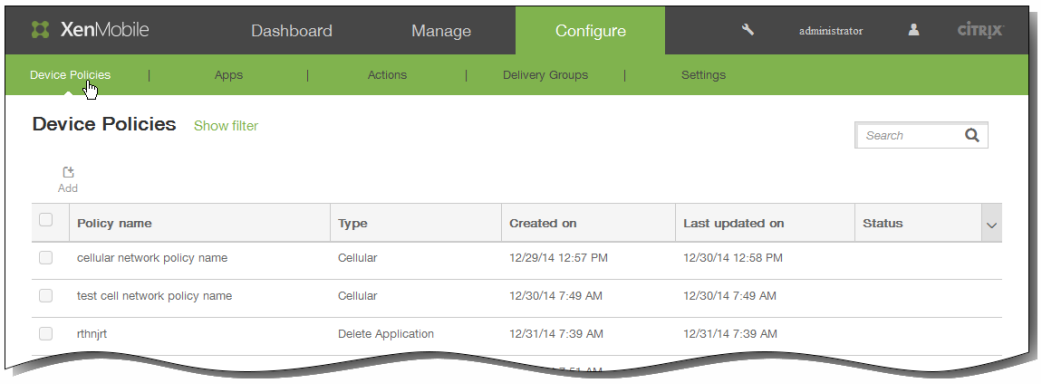
May 05, 2016

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:

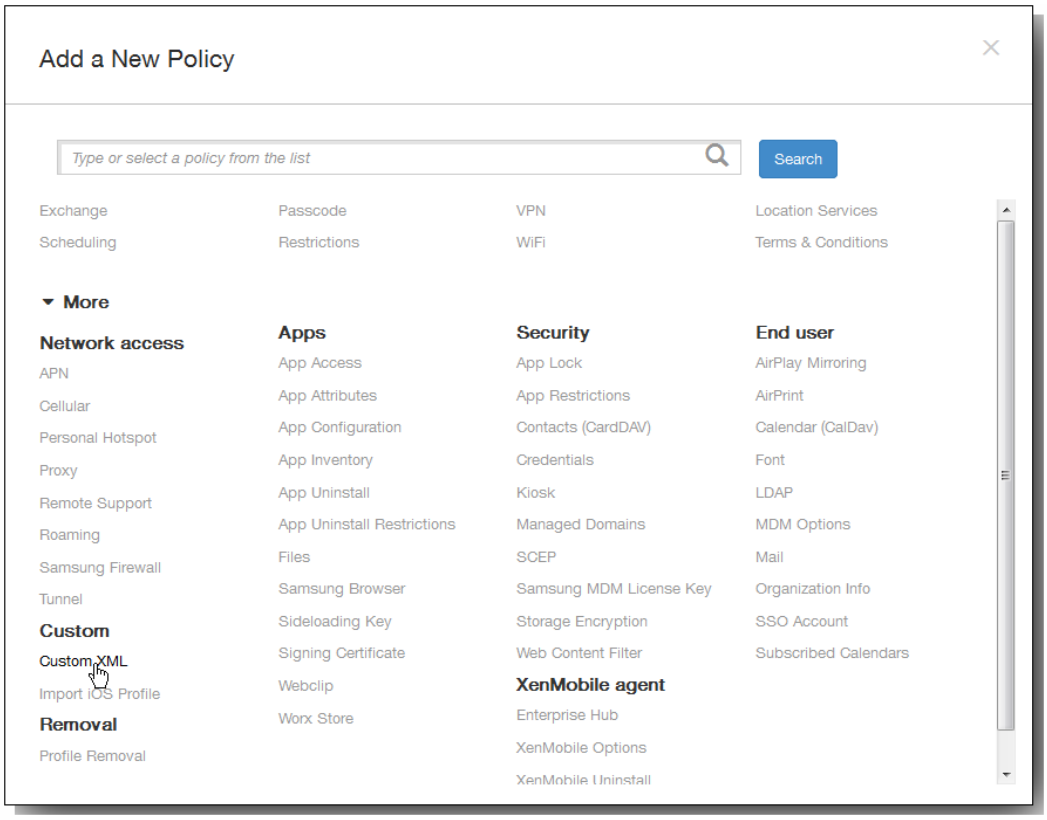
- Provisioning, d. h. Konfiguration des Geräts und Aktivieren bzw. Deaktivieren von Features
- Gerätekonfiguration, einschließlich des Zulassens der Änderung von Einstellungen und Geräteparametern durch die Benutzer
- Softwareupgrades, d. h. Bereitstellung neuer Software oder von Fehlerbehebungen für 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.

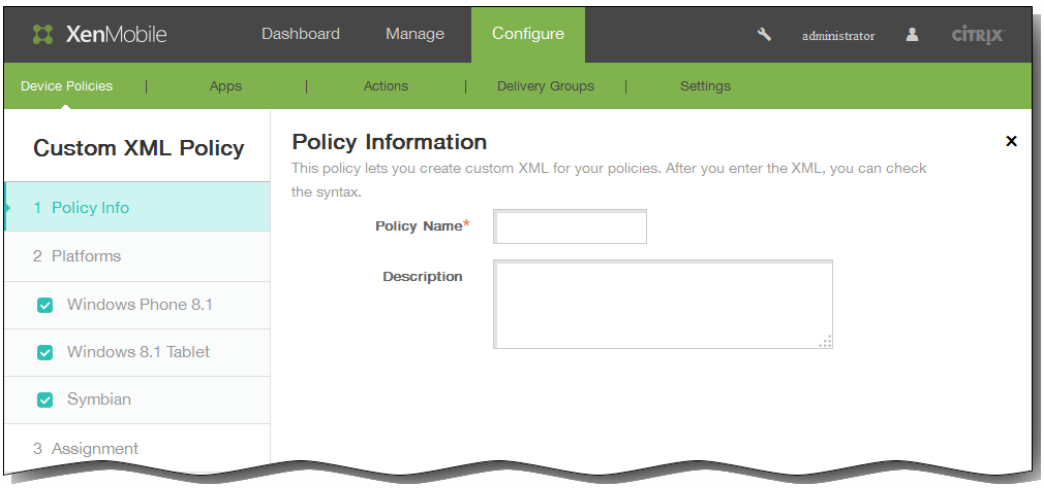
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



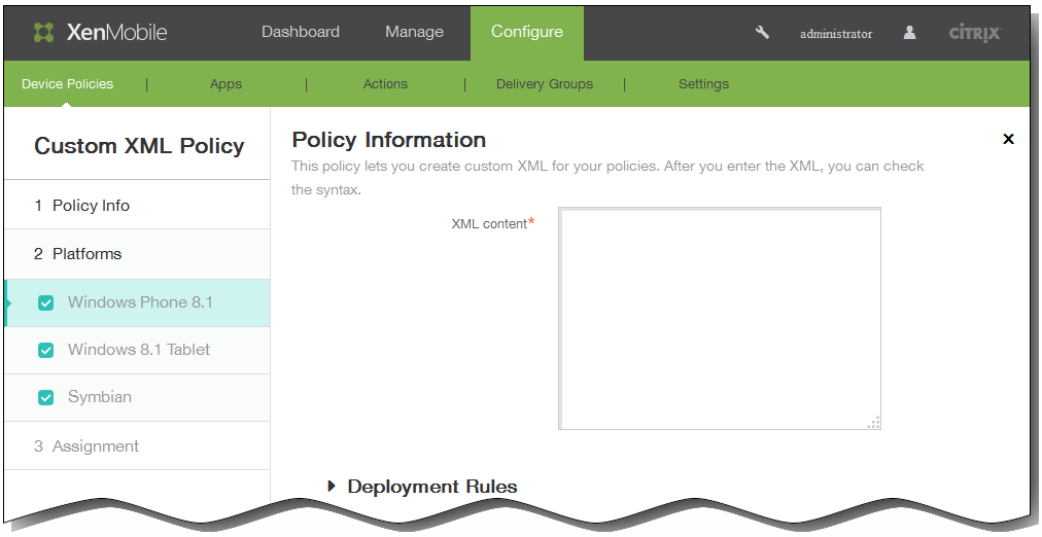
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add New Policy wird angezeigt.



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

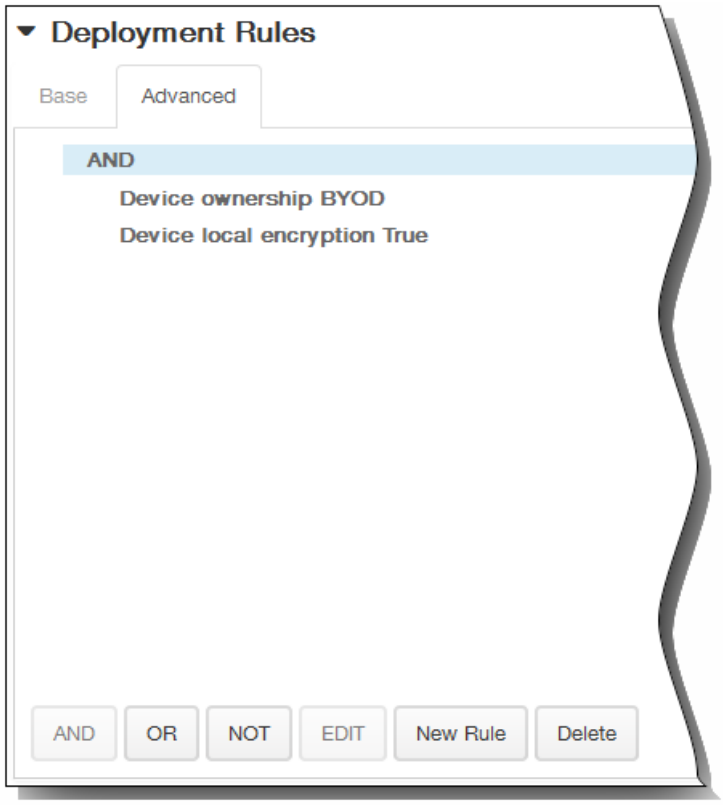


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Policy Platforms wird angezeigt.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

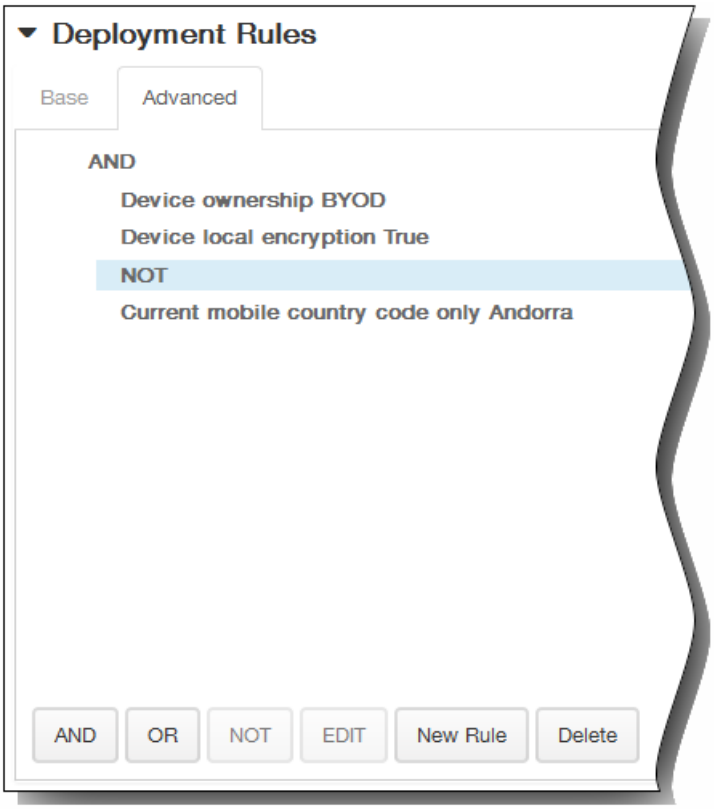
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen 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.

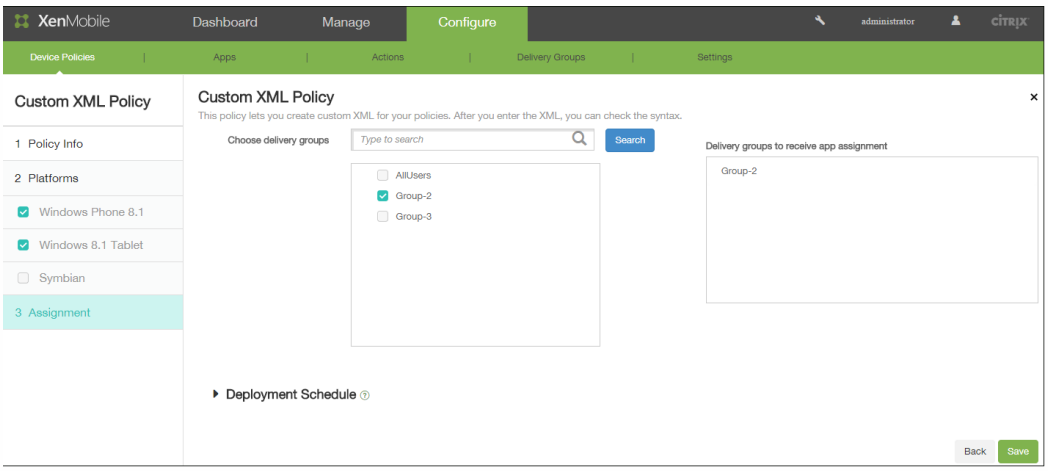
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf 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.

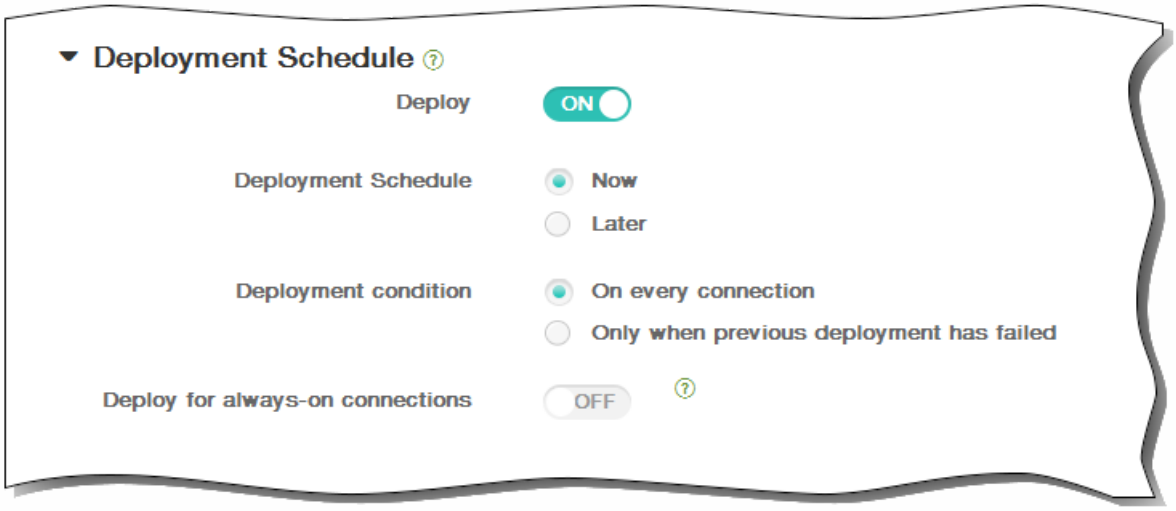


11. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert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



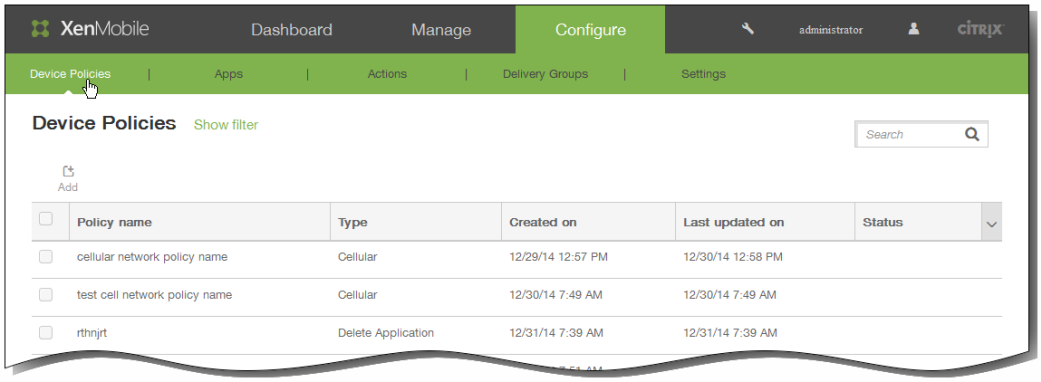
12. Klicken Sie auf Save, um die Richtlinie zu speichern.

App-Deinstallationsrichtlinien für Geräte

May 05, 2016

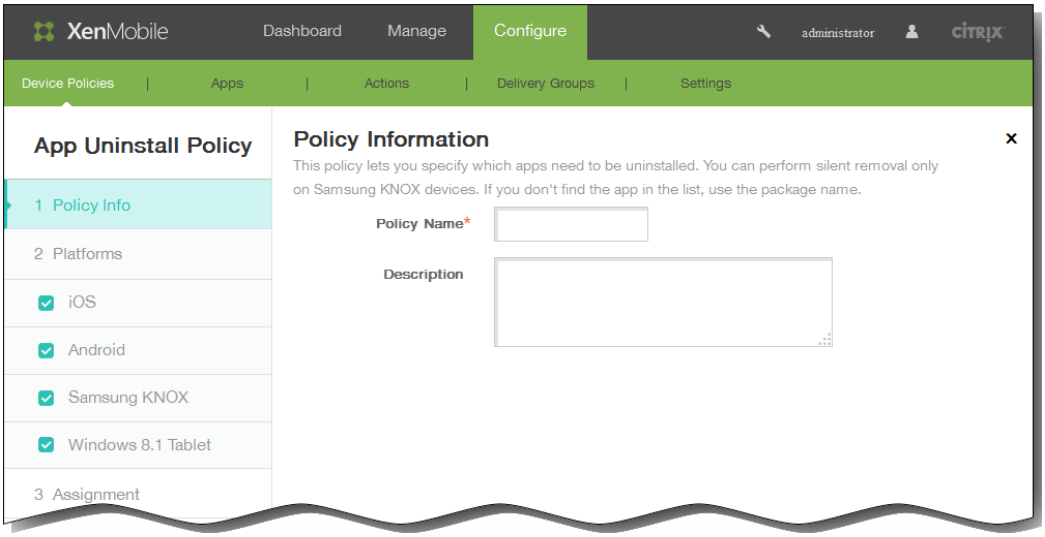
Sie können App-Deinstallationsrichtlinien für iOS-, Android- sowie Samsung KNOX-Geräte und für Windows 8.1-Tablets erstellen. Mit einer App-Deinstallationsrichtlinie können Sie Apps von Benutzergeräten entfernen. Grund für die Notwendigkeit des Entfernens von Apps kann sein, dass Sie für diese keinen 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.

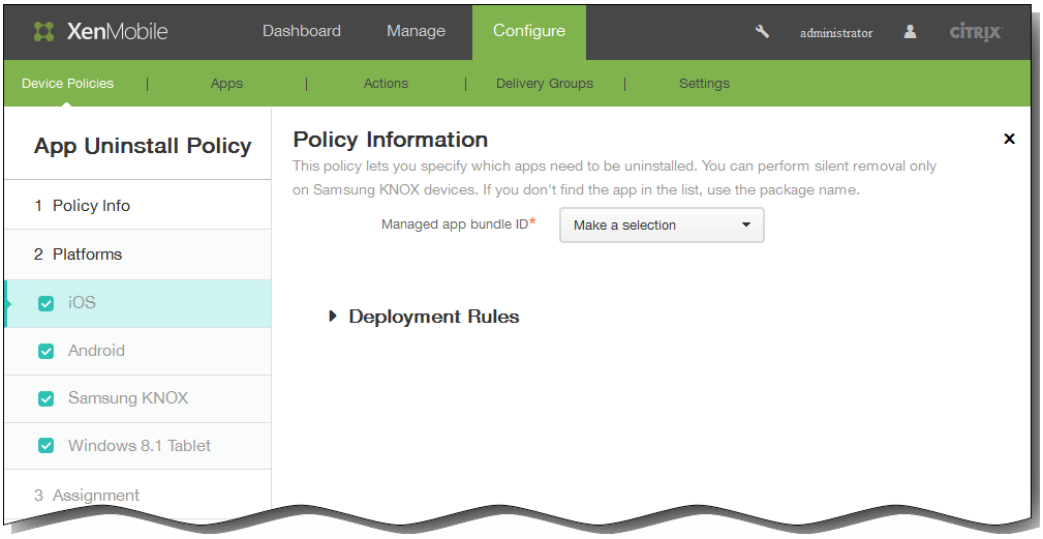


2. Klicken Sie im Dialogfeld Add a New Policy auf More und dann unter Apps auf App Uninstall.

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.

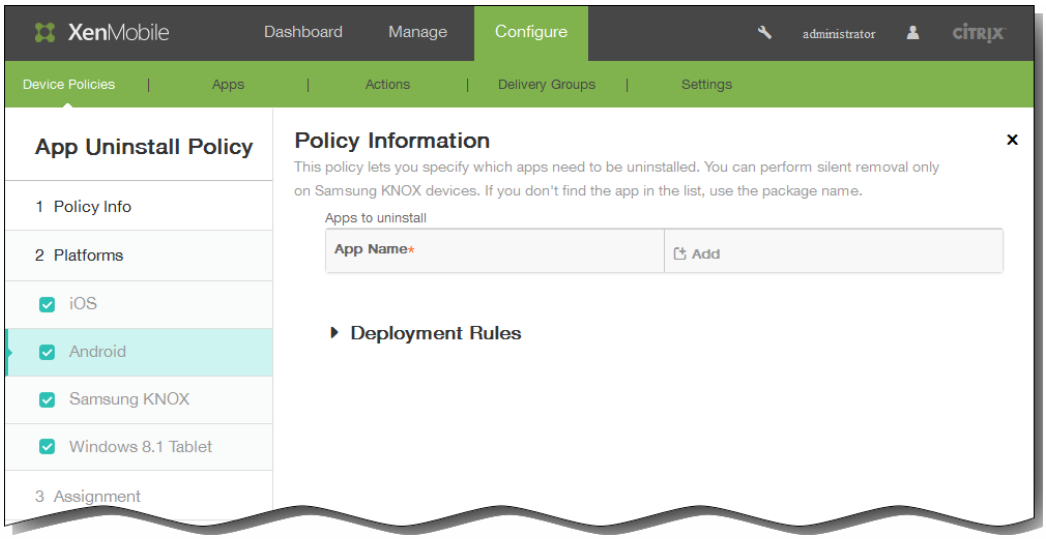


4. Auf der Seite Policy Platforms sind alle Plattformen ausgewählt, der Konfigurationsbereich für die iOS-Plattform wird als erstes angezeigt. Wählen Sie unter Platforms die gewünschten Plattformen aus und deaktivieren Sie die nicht gewünschten.



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. Wenn Sie Android, Samsung KNOX oder Windows 8.1 Tablet ausgewählt haben, führen Sie folgende Schritte aus:



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

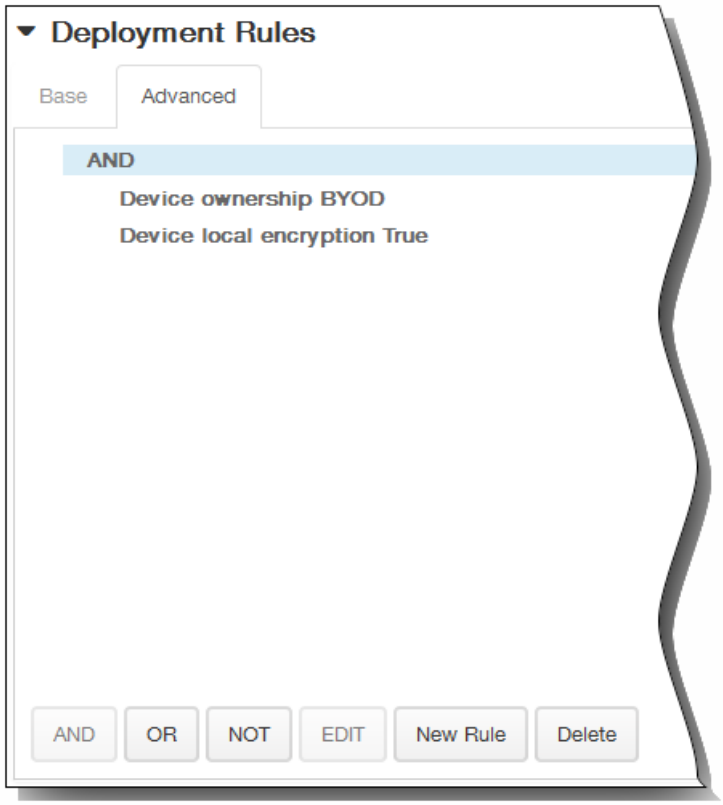
1. App name: Klicken Sie in der Liste auf eine vorhandene App oder klicken Sie auf Add, um einen neuen App-Namen einzugeben.
   Hinweis: Wenn keine Apps für diese Plattform konfiguriert sind, ist die Liste leer und Sie müssen neue Apps hinzufügen.
2. Klicken Sie auf Add, um die App hinzuzufügen, oder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

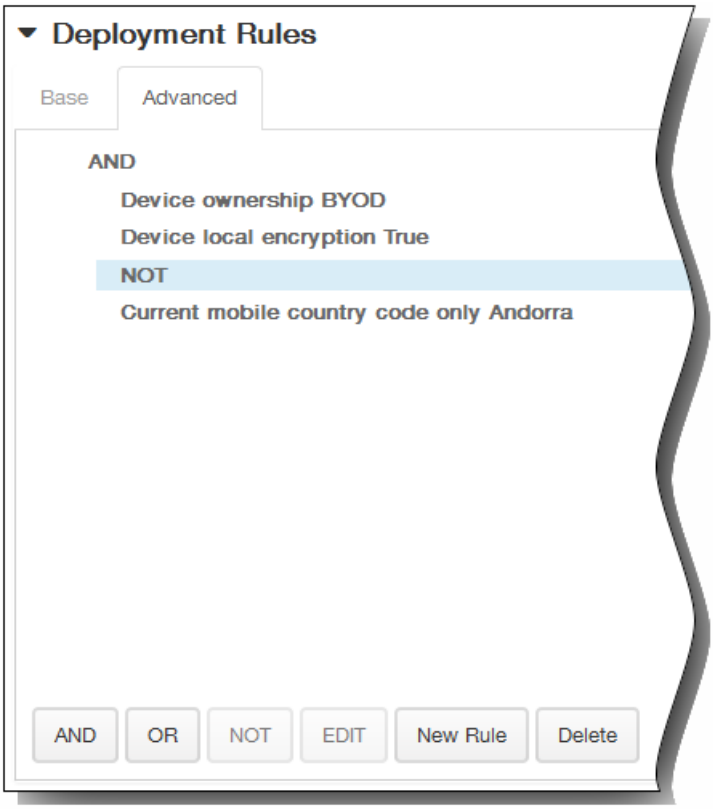
2. Klicken Sie auf die Registerkarte Advanced, um die Regeln mit booleschen Optionen zu kombinieren.



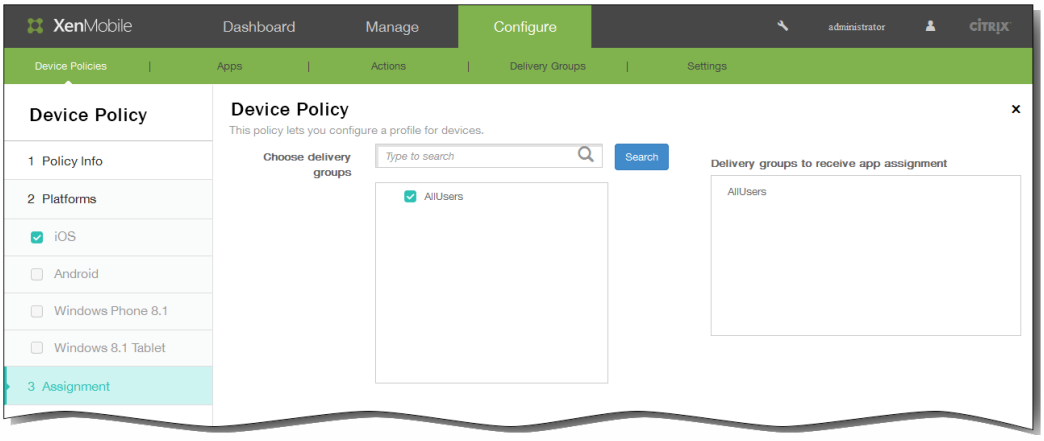
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



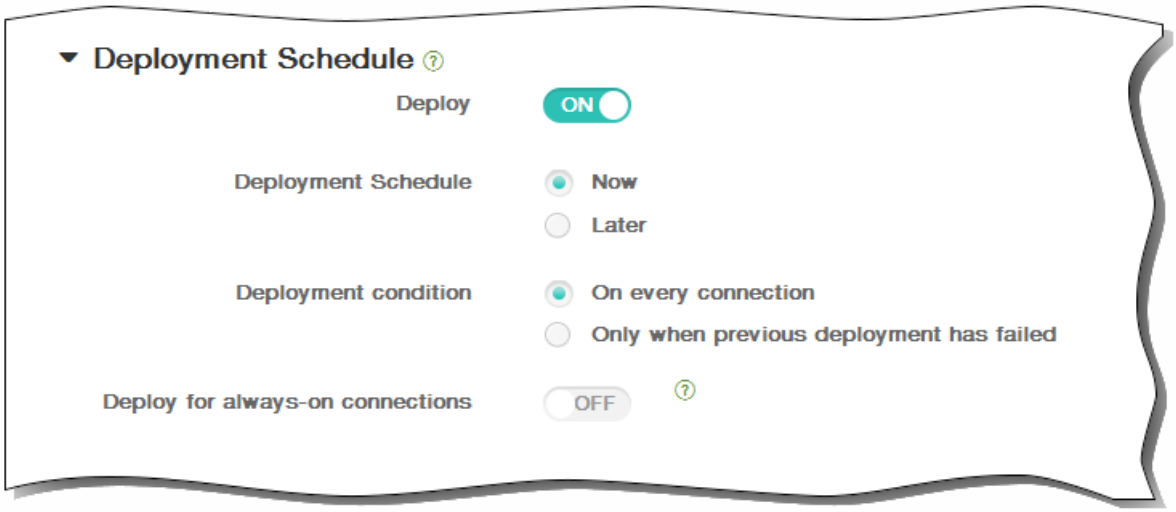
7. Klicken Sie auf Next. Die Seite Assignment für die Deinstallationsrichtlinie wird angezeigt.
8. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten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



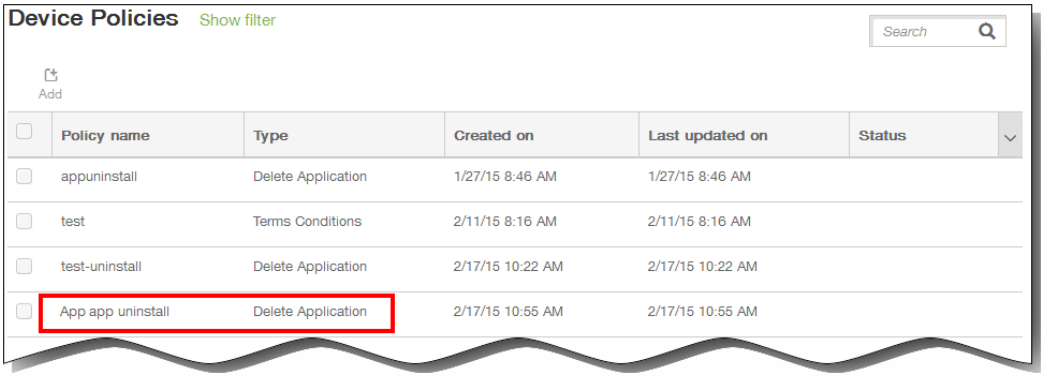
9. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
   1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert 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. Die Spalte Type auf der Seite Device Policies enthält die Richtlinie, die Sie als Deinstallationsrichtlinie hinzugefügt haben.

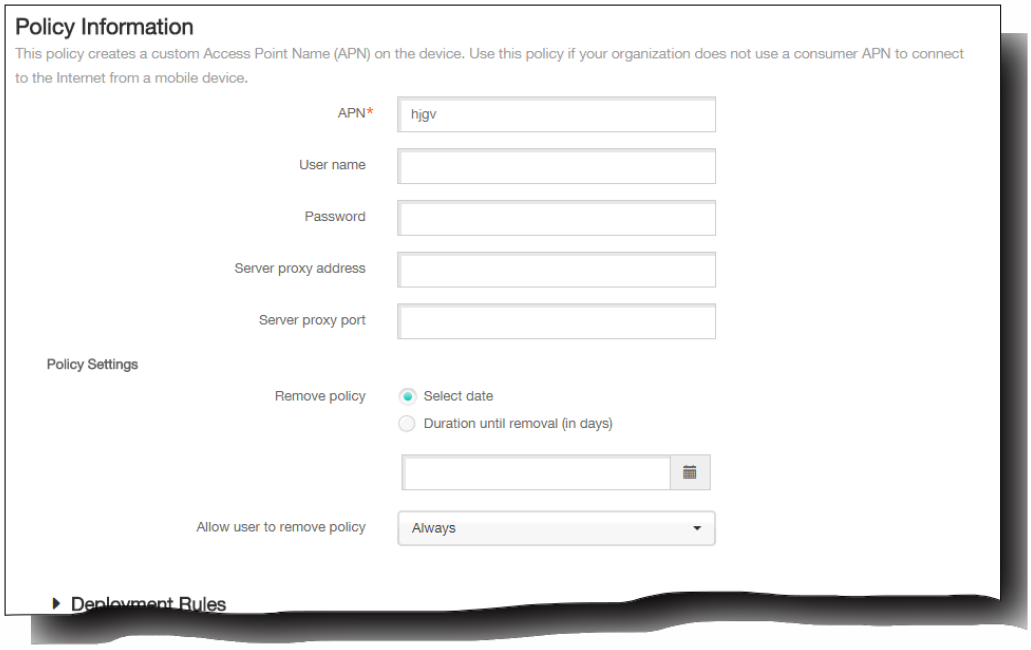


So fügen Sie eine APN-Richtlinie hinzu

May 05, 2016

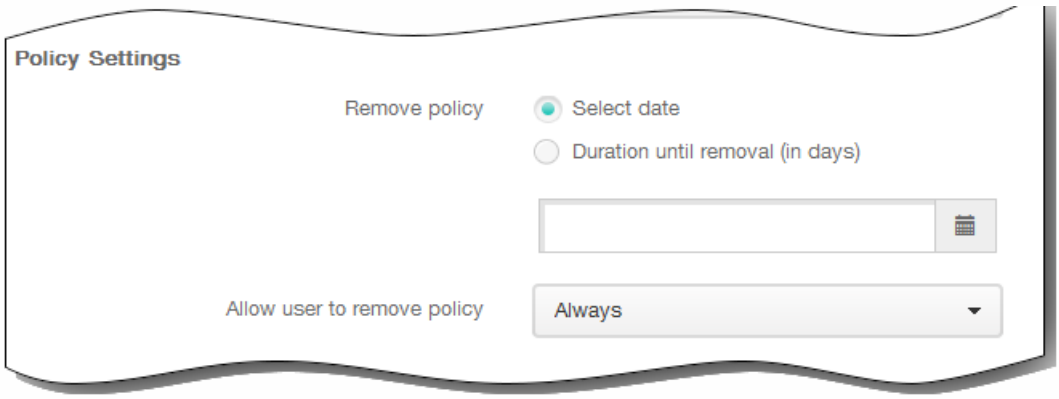
Mit dieser Richtlinie können Sie einen benutzerdefinierten Zugriffspunktnamen (APN) auf einem iOS-, Android- oder Samsung KNOX-Gerät konfigurieren. Eine APN-Richtlinie definiert die Einstellungen für die Verbindung zwischen den Geräten und dem General Packet Radio Service (GPRS) eines Netzbetreibers. Diese Einstellung ist bei den meisten neueren Telefonen bereits definiert.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies > Add.
2. Klicken Sie auf der Seite Add a New Policy auf More und dann unter Network access auf APN.
3. Wählen Sie die Plattformen aus, die Sie in die Richtlinie einschließen möchten. Die Seiten zur Konfiguration für die ausgewählte Plattform werden in Schritt 5 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 erste Plattforminformationsseite wird angezeigt.
6. Wenn Sie die iOS-Plattform ausgewählt haben, führen Sie auf der iOS- Plattforminformationsseite die folgenden Schritte aus:



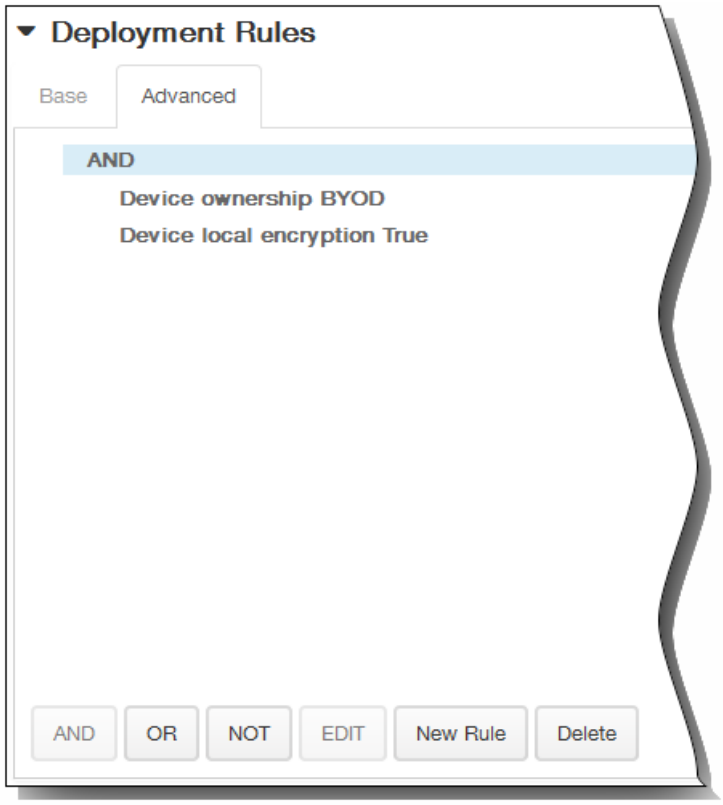
   1. APN: Geben Sie den Namen des Zugriffspunkts ein.
   2. User name: Diese Zeichenfolge repräsentiert den Benutzernamen für diesen APN. Fehlt der Benutzername, fordert das Gerät die Zeichenfolge während der Profilinstallation an.
   3. Password: das Kennwort für den Benutzer für den APN. Für höhere Sicherheit ist das Kennwort codiert. Fehlt es, fordert das Gerät die Zeichenfolge während der Profilinstallation an.
   4. Server proxy address: IP-Adresse oder URL des APN-Proxy
   5. Server proxy port: Portnummer des APN-Proxys
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.

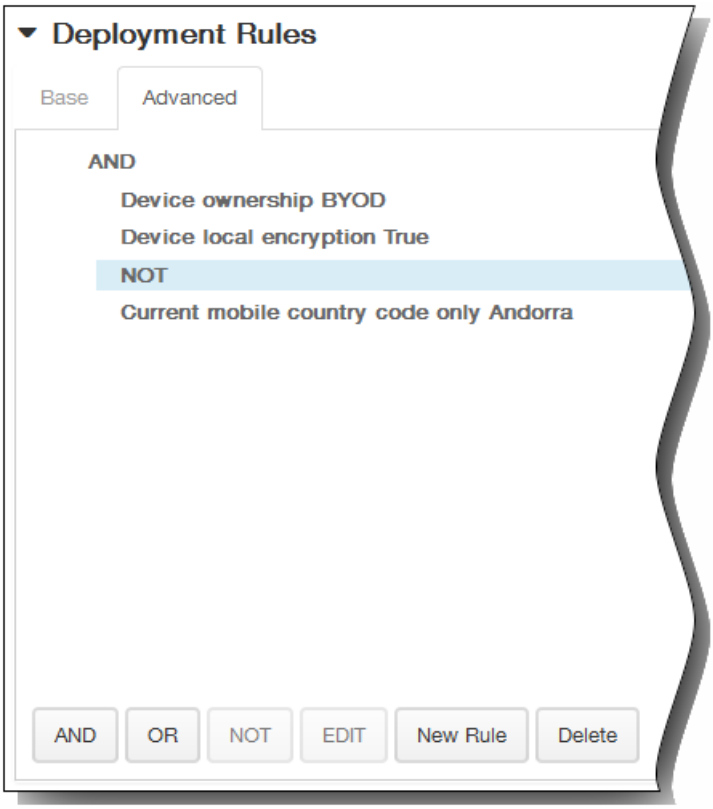
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen 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.



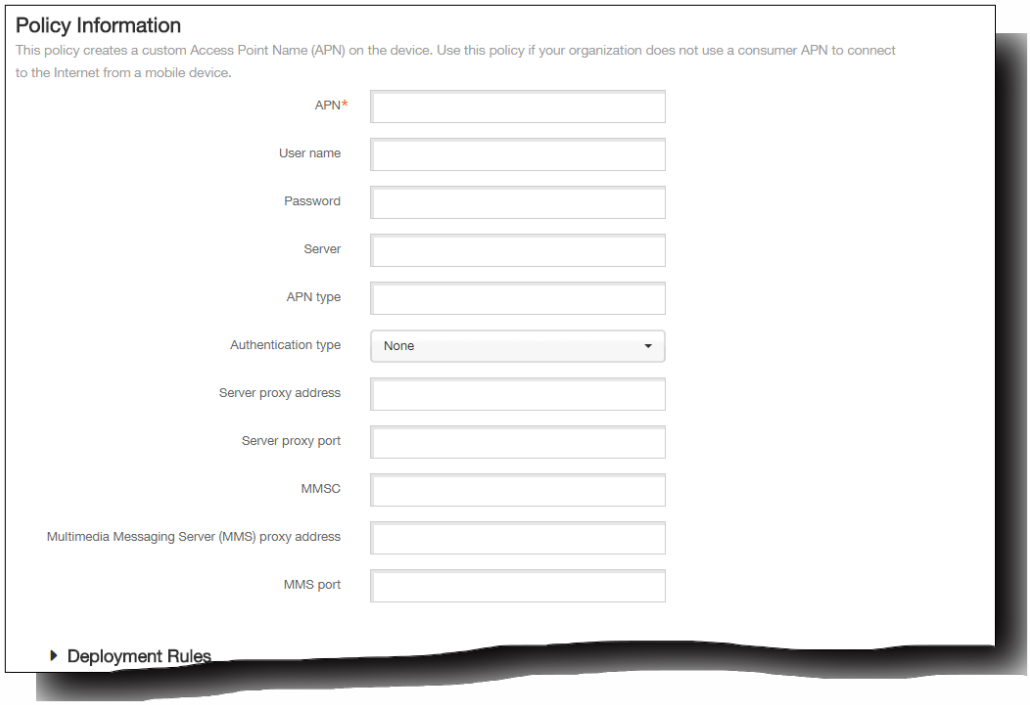
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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. Wenn Sie die Android- oder Samsung KNOX-Plattform ausgewählt haben, führen Sie auf der Plattforminformationsseite die folgenden Schritte aus:

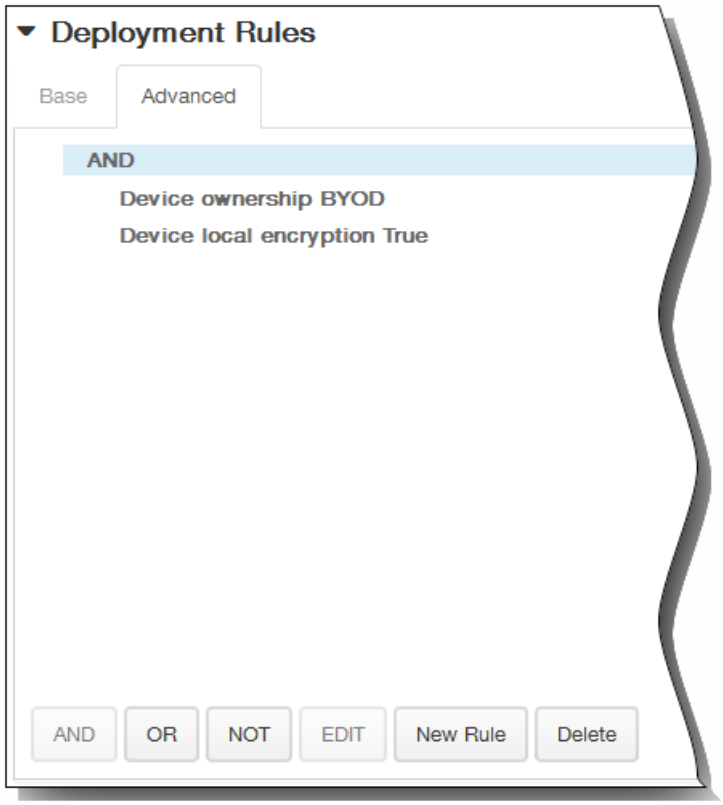


1. APN: Geben Sie den Namen des Zugriffspunkts ein.

2. User name: Diese Zeichenfolge repräsentiert den Benutzernamen für diesen APN. Fehlt der Benutzername, fordert das Gerät die Zeichenfolge während der Profilinstallation an.
3. 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.
4. 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.
5. 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.
6. Authentication type: entweder PAP, CHAP oder PAP or CHAP. Standardwert ist None.
7. Server proxy address: IP-Adresse oder URL des APN-Proxy
8. Server proxy port: Portnummer des APN-Proxys
9. MMSC: 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).
10. Multimedia Messaging Server (MMS) proxy address: HTTP-Proxyserver für MMS.
11. MMS port: Port des MMS-Proxyservers.

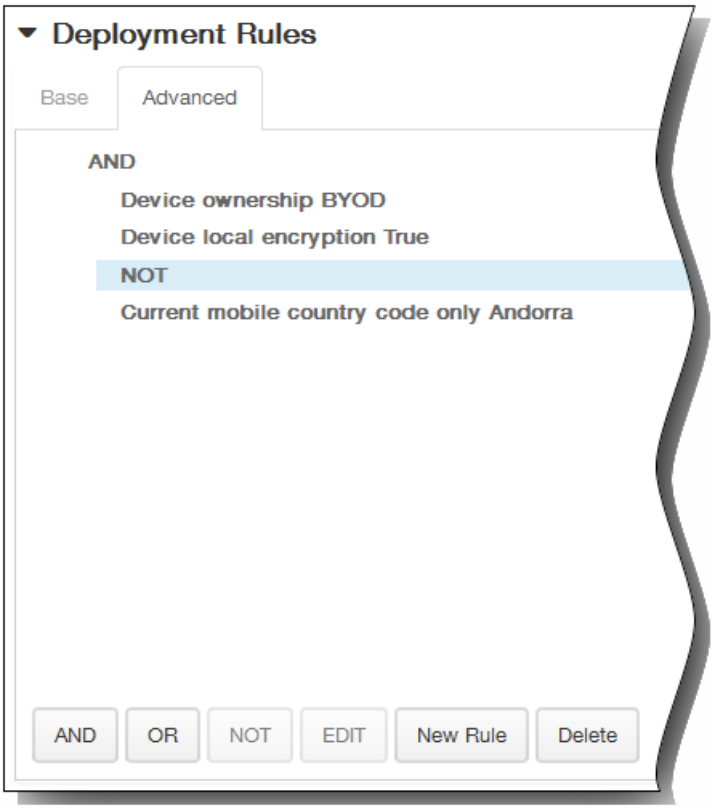
13. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

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.

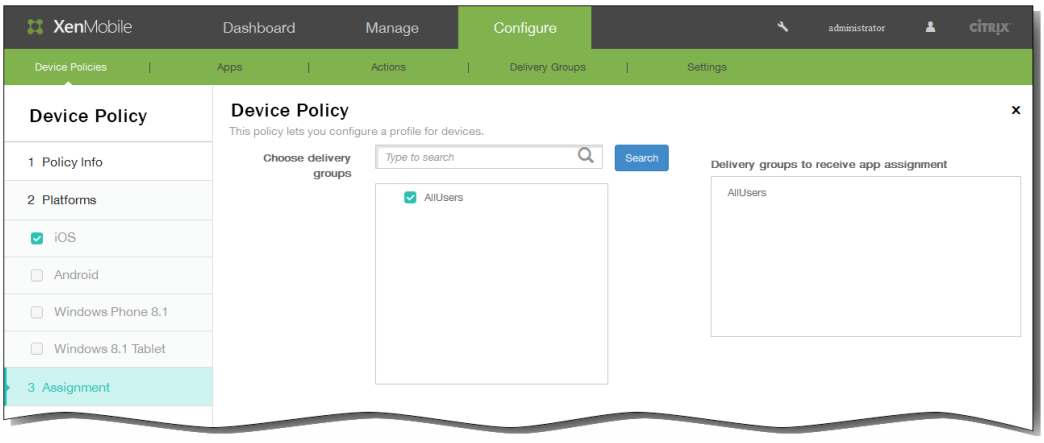


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



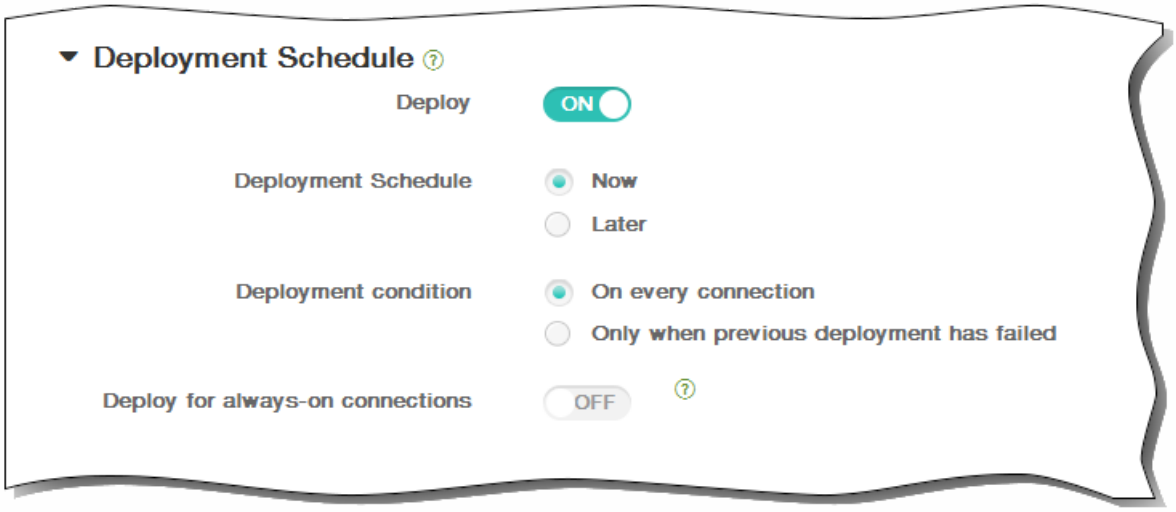
14. Wenn Sie sowohl Android als auch Samsung KNOX ausgewählt haben, wiederholen Sie Schritt 8 zum Ausfüllen der Informationsseite für die Samsung KNOX-Plattform und klicken Sie dann auf Next. Die Seite Assignment für die APN-Richtlinie wird angezeigt.
15. Machen Sie neben Choose delivery groups eine 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.



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.



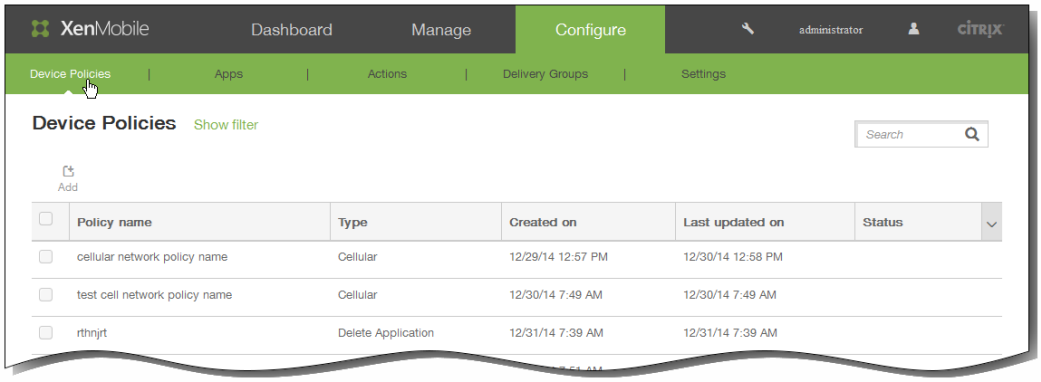
17. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Mobilfunkrichtlinie für iOS-Geräte hinzu

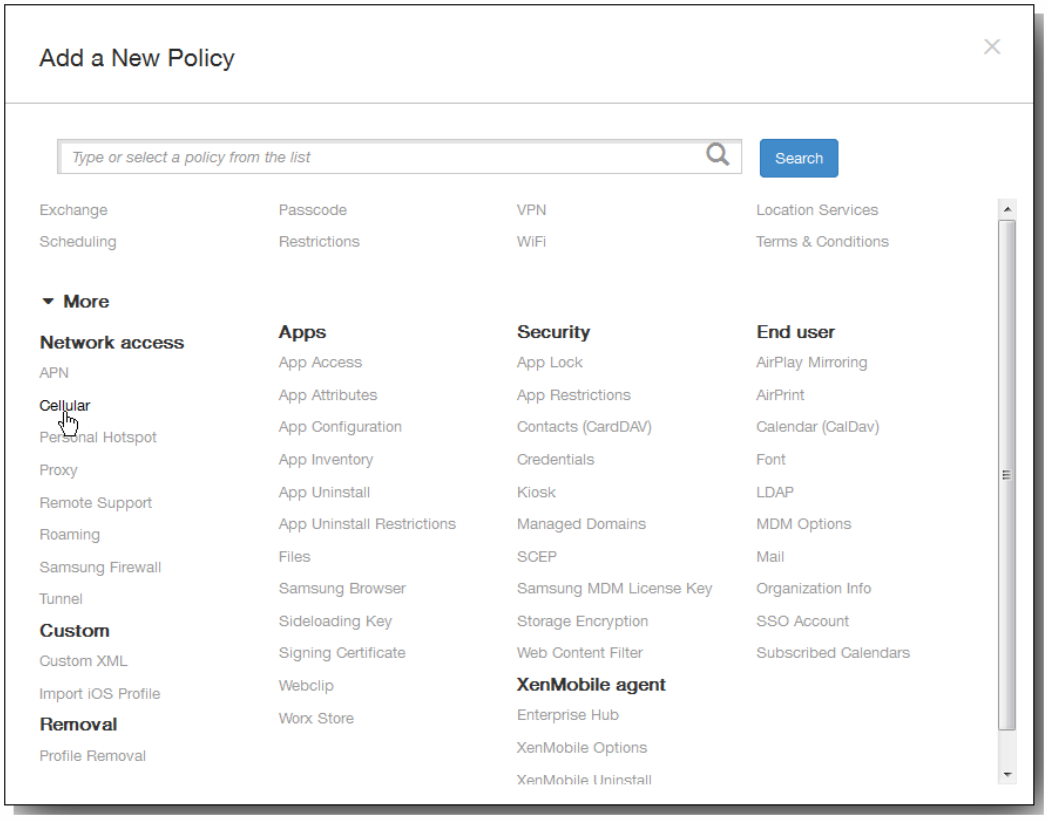
May 05, 2016

Mit dieser Richtlinie können Sie Einstellungen für das Mobilfunknetz auf iOS-Geräten konfigurieren.

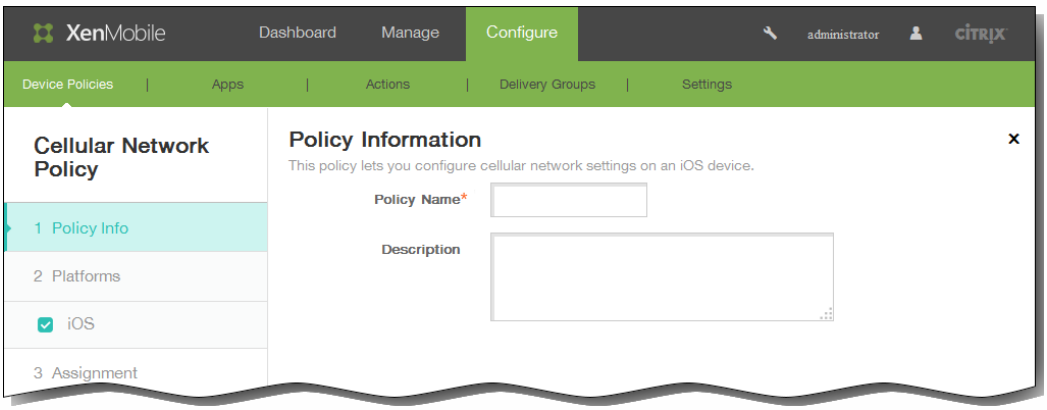
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies.



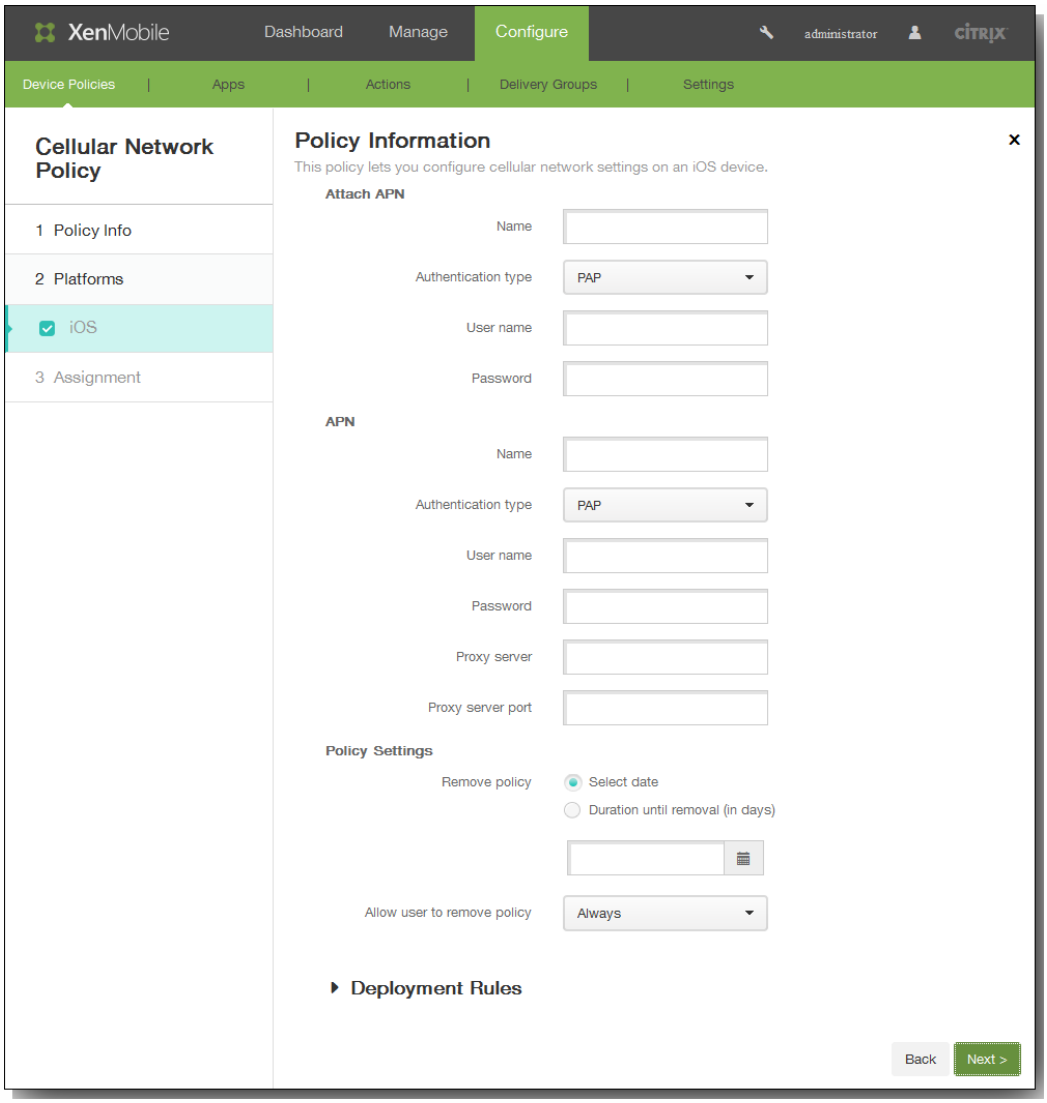
2. Klicken Sie auf Add.
   Die Seite Add a New Policy wird angezeigt.



3. Klicken Sie auf der Seite Add a New Policy auf More und dann unter Network Access auf Cellular. Die Seite Cellular Network Policy wird angezeigt.



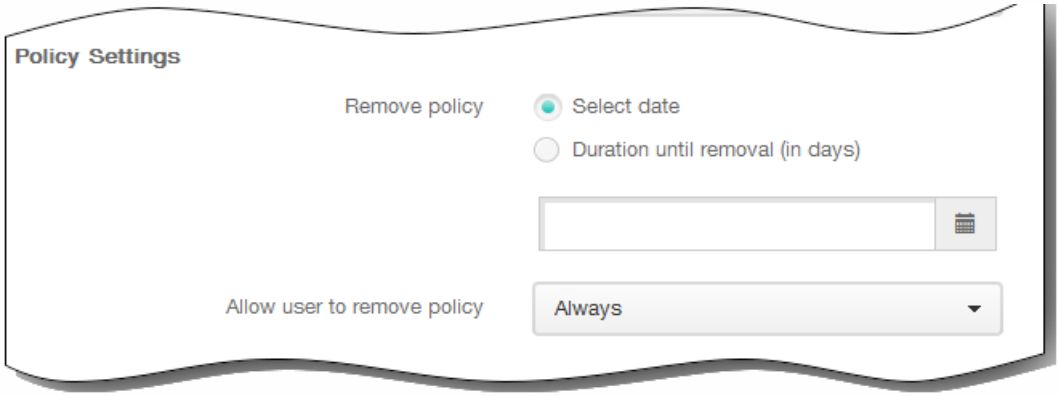
4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite iOS Platform information wird angezeigt.



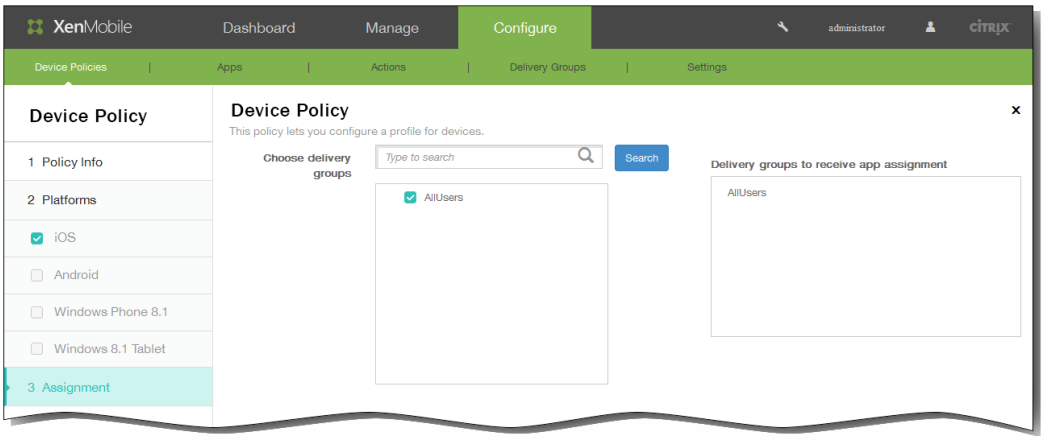
6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein: Führen Sie unter **Attach APN** folgende Schritte aus:
   1. Name: Geben Sie einen Namen für die Konfiguration ein.
   2. Authentication type: Klicken Sie in der Liste auf das Challenge Handshake Authentication-Protokoll (CHAP) oder das Password Authentication-Protokoll (PAP). Die Standardeinstellung ist PAP.
   3. User name: Geben Sie einen Benutzernamen für die Authentifizierung ein.
   4. Password: Geben Sie ein Kennwort für die Authentifizierung ein.

   Führen Sie unter **APN** folgende Schritte aus:
   1. Name: Geben Sie einen Namen für die APN-Konfiguration ein.
   2. Authentication type: Klicken Sie in der Liste auf CHAP oder PAP. Die Standardeinstellung ist PAP.
   3. User name: Geben Sie einen Benutzernamen für die Authentifizierung ein.
   4. Password: Geben Sie ein Kennwort für die Authentifizierung ein.
   5. Proxy server: Geben Sie die Netzwerkadresse des Proxyservers ein.
   6. Proxy server port: Geben Sie den Port des Proxyservers ein.
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.

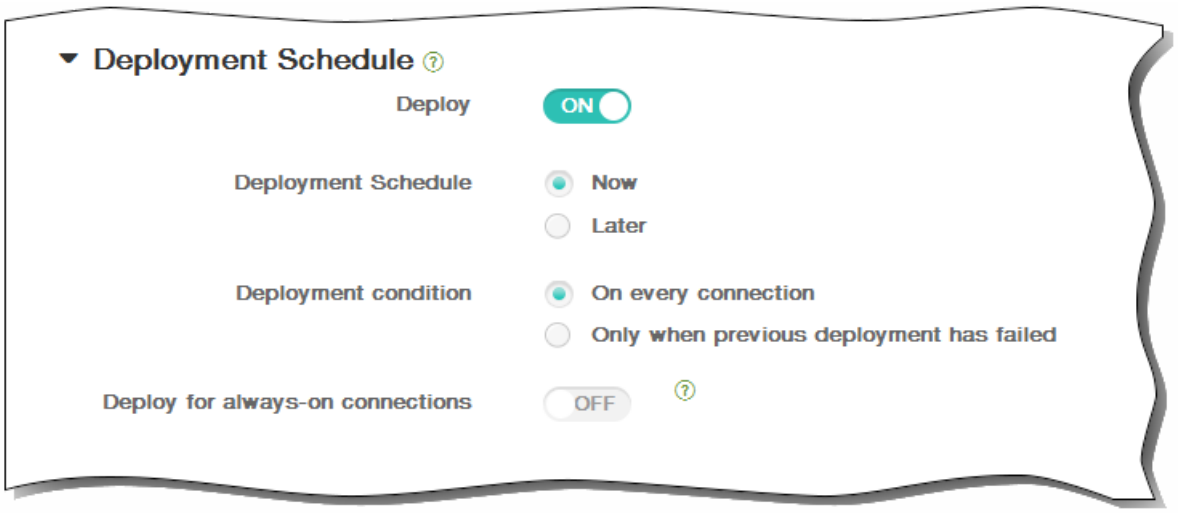


11. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



12. 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.



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

So fügen Sie eine Enterprise Hub-Richtlinie für Windows Phone 8.1-Geräte hinzu

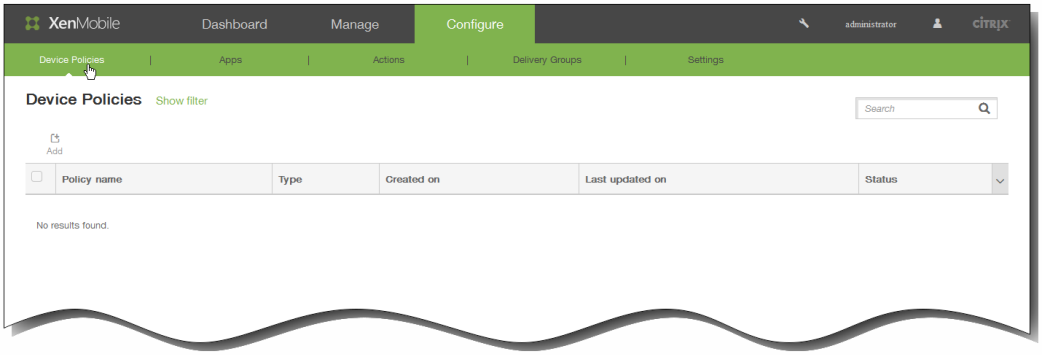
May 05, 2016

Mit einer Enterprise Hub-Geräterichtlinie für Windows Phone 8.1 können Sie Apps über den Enterprise Hub Company-Store an Geräte verteilen.

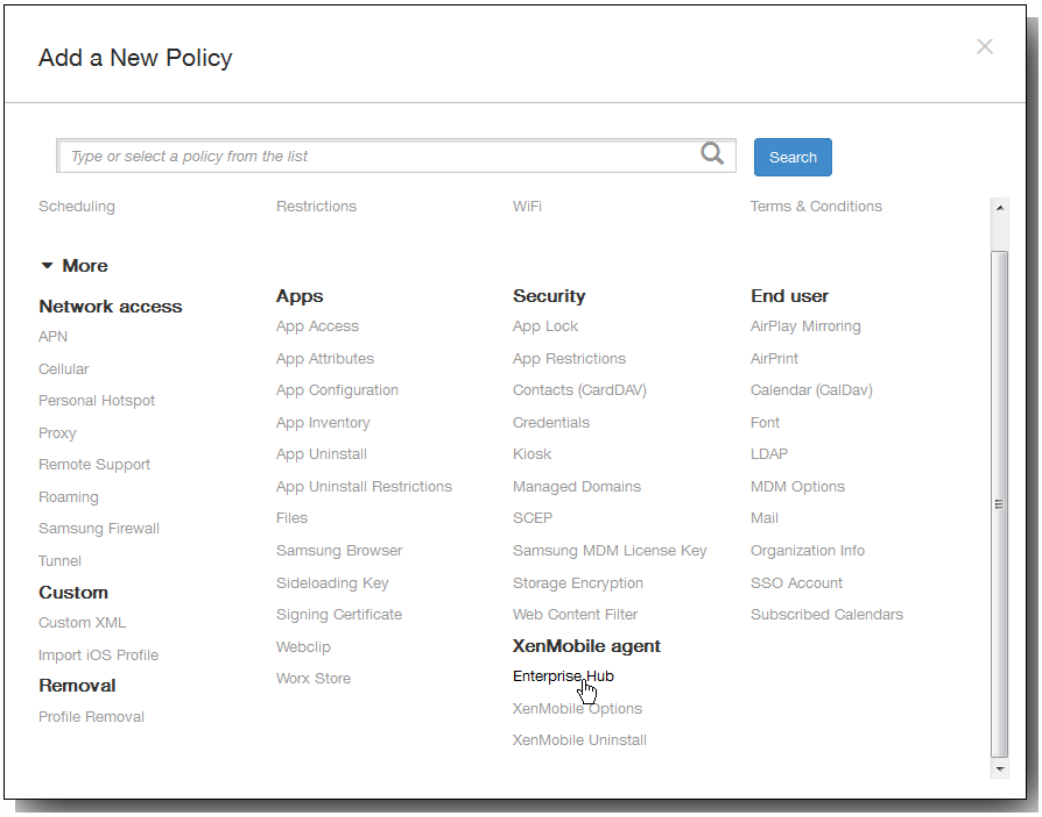
Zum Erstellen der Richtlinie benötigen Sie Folgendes:

- Ein AET-Signaturzertifikat (.aetx) von Symantec
- Die mit dem Microsoft App-Signierungstool (XapSignTool.exe) signierte Citrix Company Hub-App

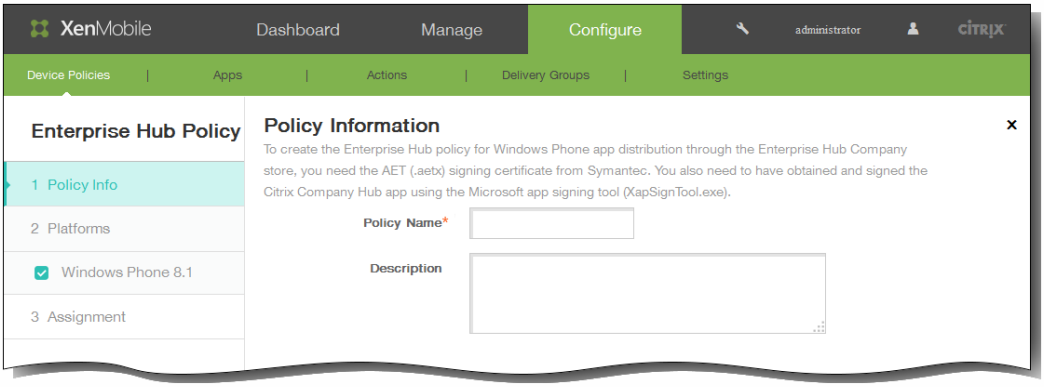
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



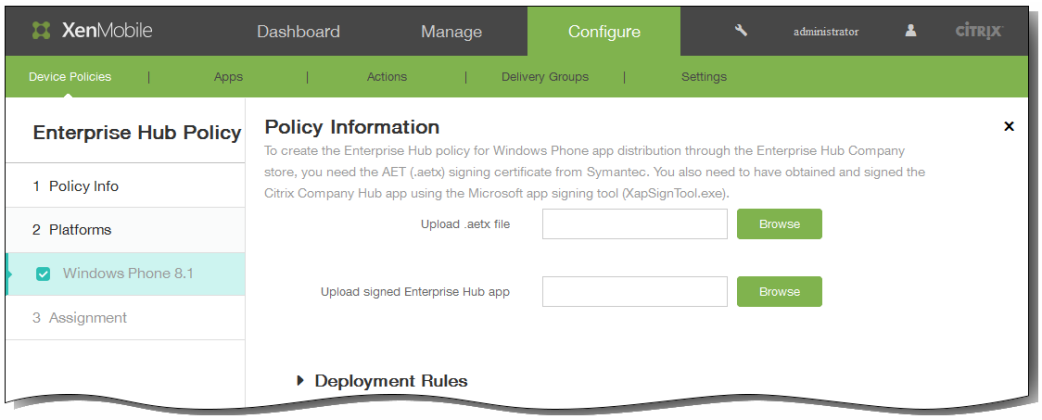
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter XenMobile agent auf Enterprise Hub. Die Seite Enterprise Hub Policy wird angezeigt.

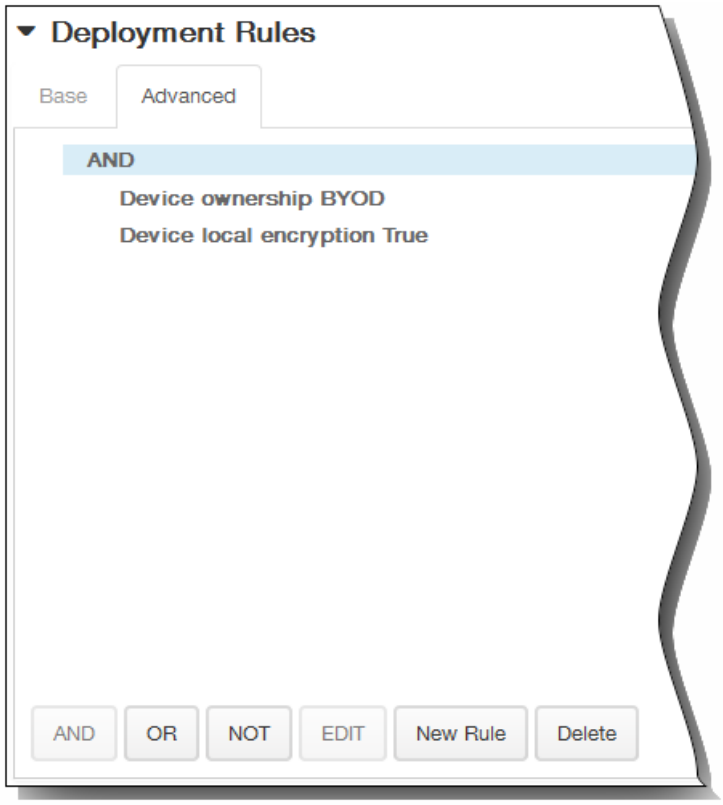


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung für die Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Windows Phone 8.1 wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:
   1. Upload .aetx file: Navigieren Sie zum Speicherort der AETX-Datei und wählen Sie die Datei aus.
   2. Upload signed Enterprise Hub app: Navigieren Sie zu dem Speicherort der Enterprise Hub-App und wählen Sie diese aus.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

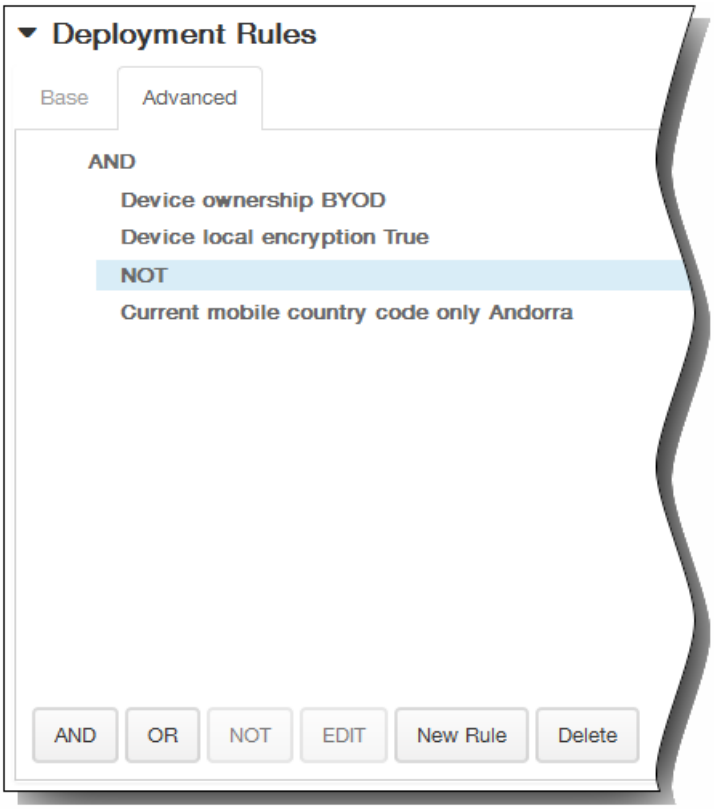
   1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
      1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
      2. Klicken Sie auf New Rule, um Bedingungen 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.



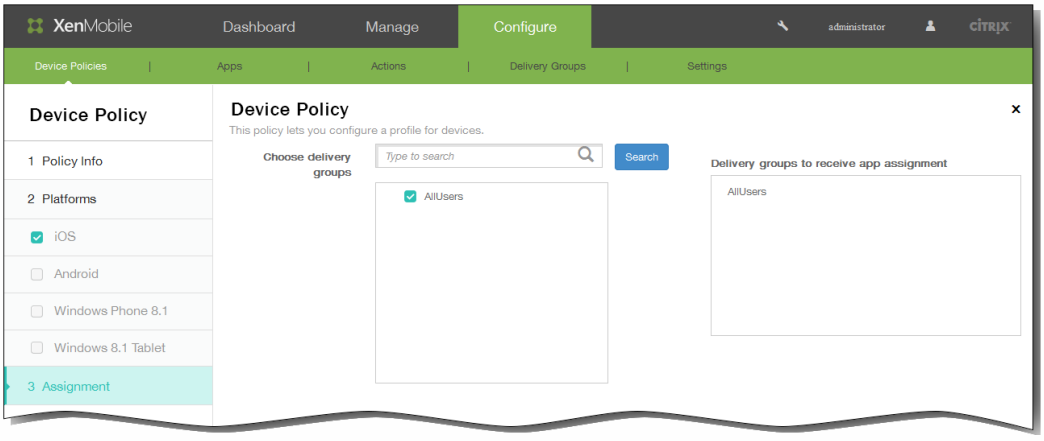
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



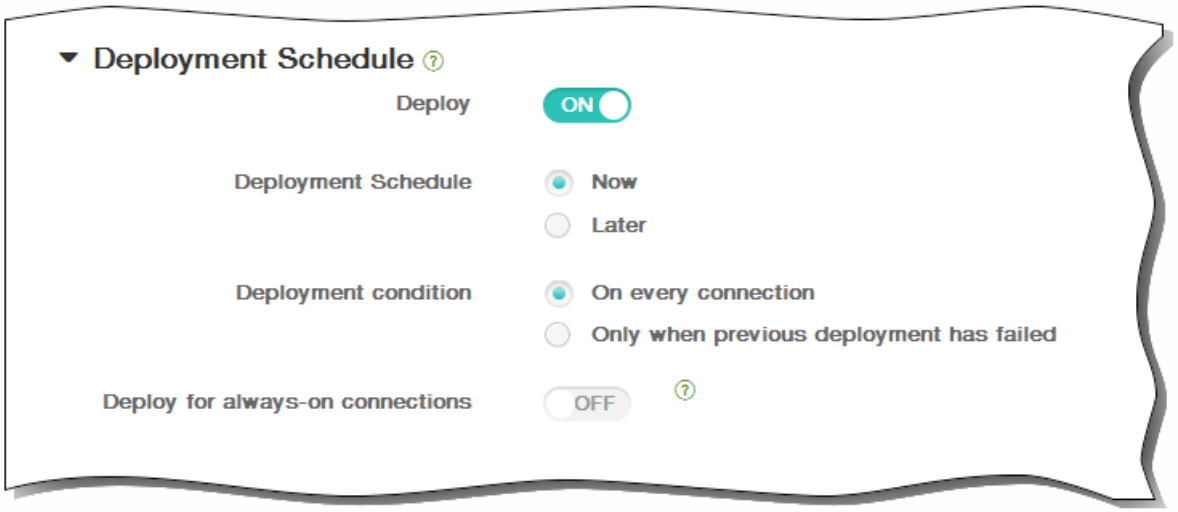
8. Klicken Sie auf Next. Die Seite Assignment für die Enterprise Hub-Richtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.

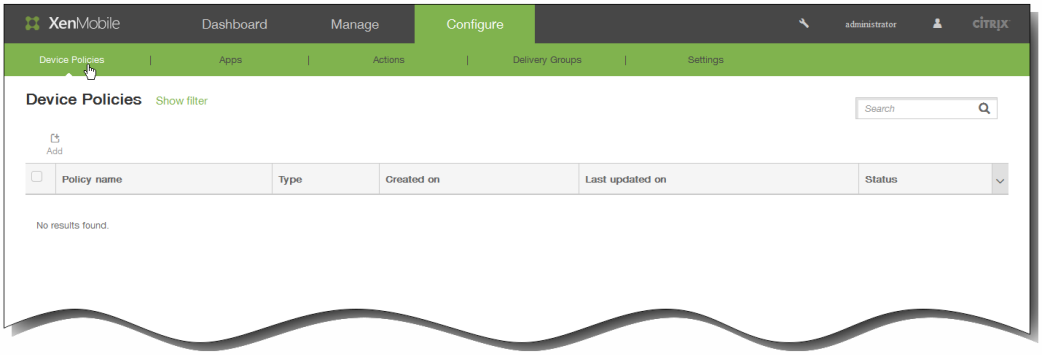
Microsoft Exchange ActiveSync-Geräterichtlinien

May 05, 2016

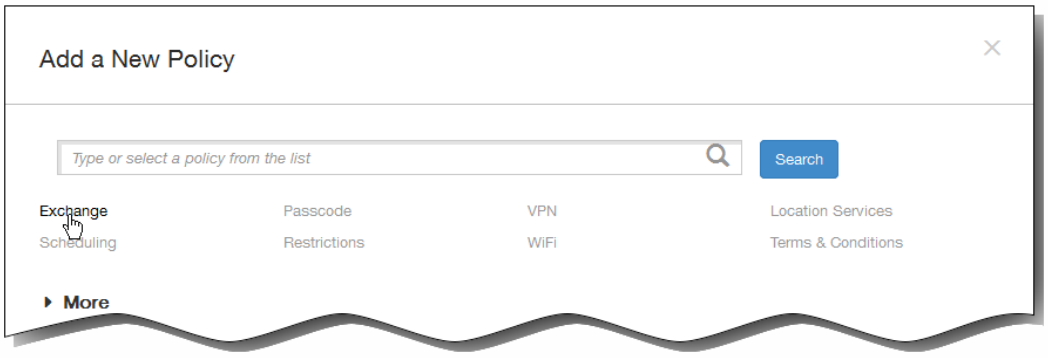
Mit der Exchange ActiveSync-Geräterichtlinie können sie einen E-Mail-Client auf den Geräten der Benutzer konfigurieren, über den diese auf ihre mit Exchange gehostete Unternehmens-E-Mail zugreifen können. Sie können Richtlinien für iOS, Android HTC, Android TouchDown, Samsung SAFE, Samsung KNOX und Windows Phone 8.1 erstellen. Jede Plattform erfordert andere Werte. Diese werden in den folgenden Abschnitten detailliert beschrieben:

Zum Erstellen dieser Richtlinie benötigen Sie den Hostnamen oder die IP-Adresse des Exchange Server-Computers.

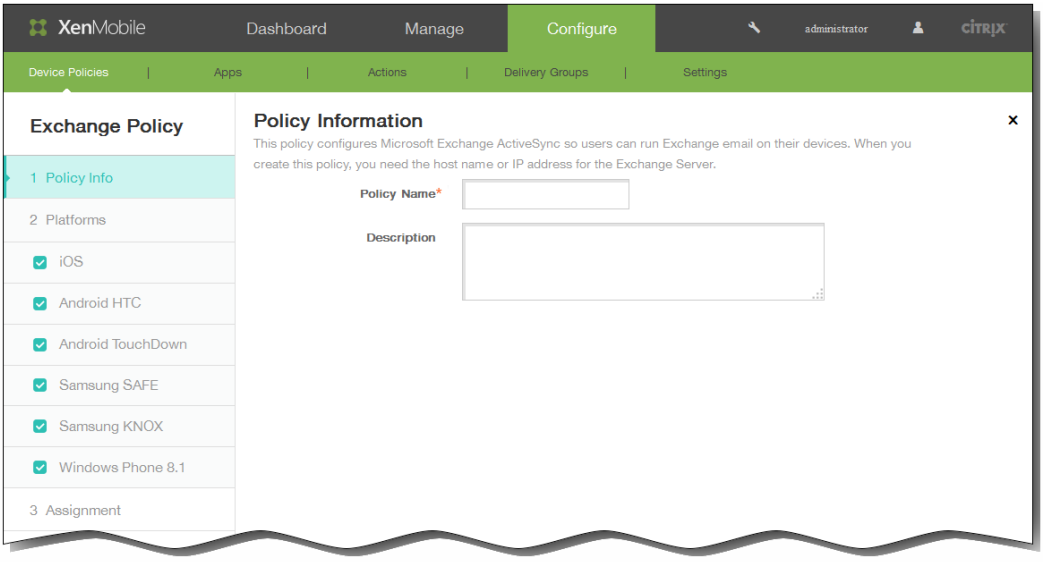
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



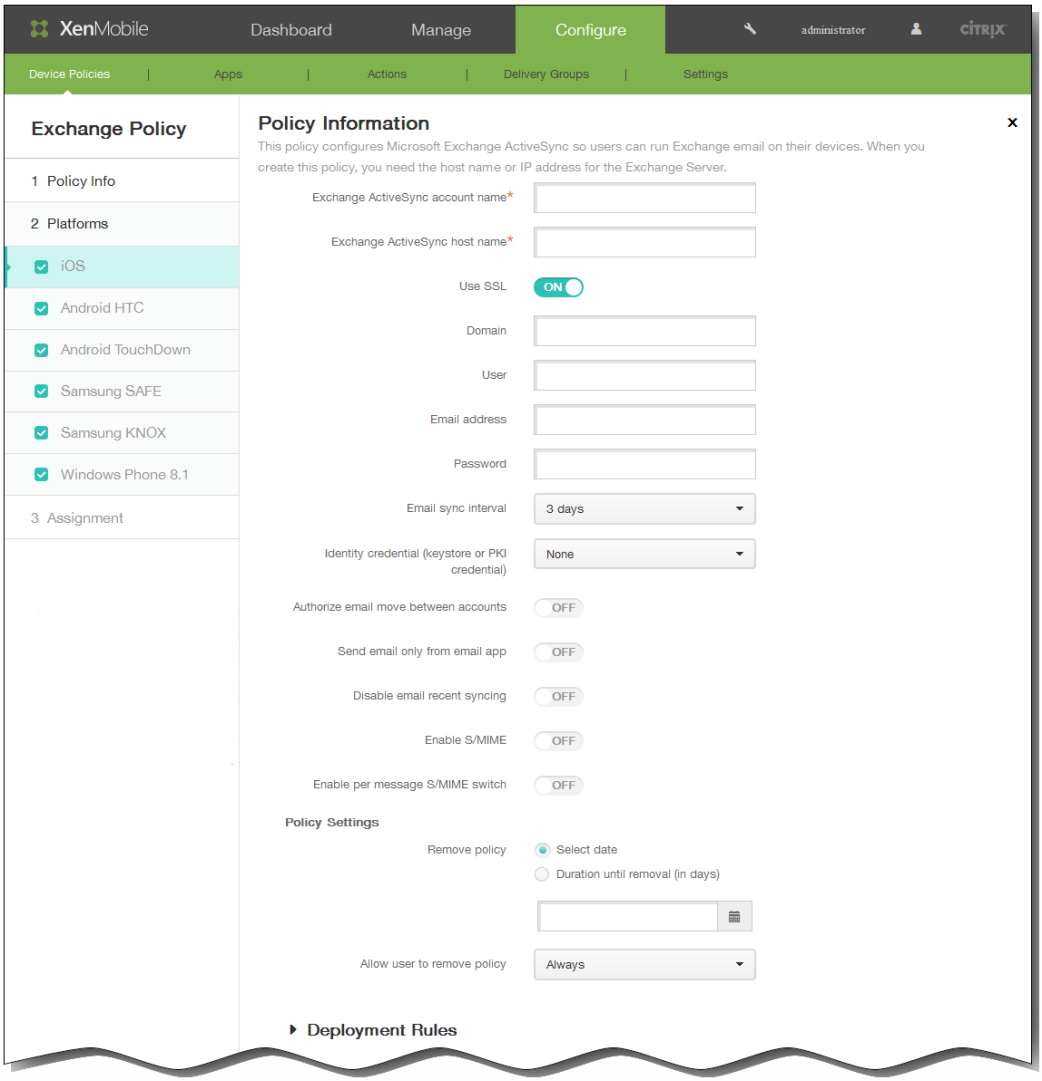
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add New Policy wird angezeigt.



3. Klicken Sie auf Exchange. Die Seite Exchange 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 iOS-Plattform wird als erstes angezeigt.



6. Wählen Sie unter Platforms die gewünschten Plattformen aus.
   - Bei Auswahl von iOS konfigurieren Sie die folgenden Einstellungen:

     Configuration display name: Geben Sie den Namen für die Richtlinie ein, wie er auf den Geräten der Benutzer angezeigt werden soll.

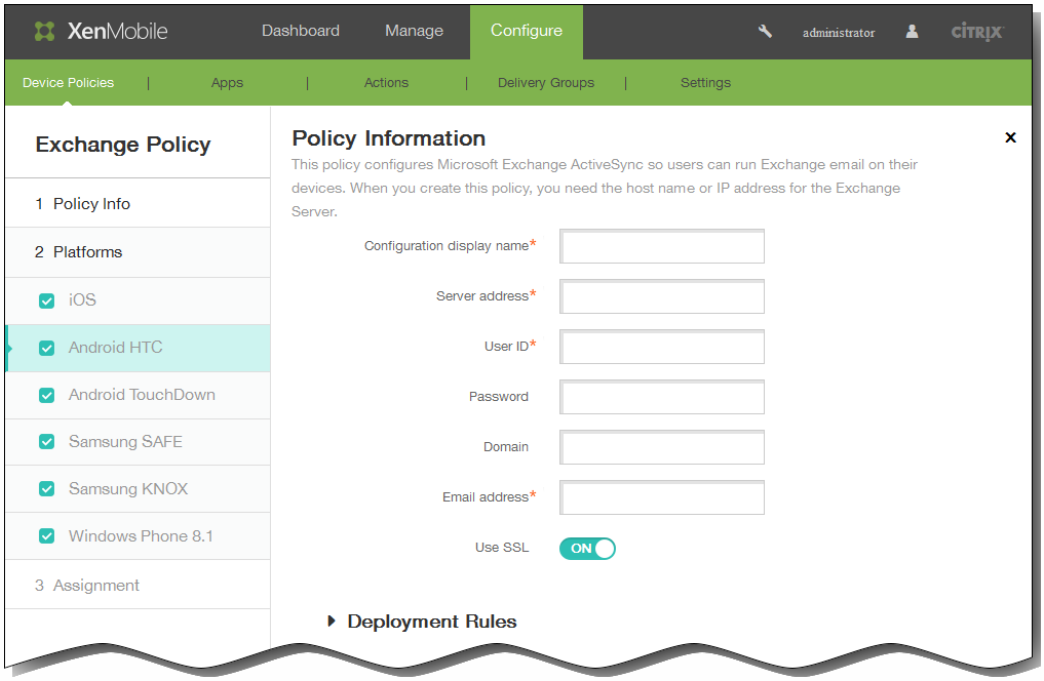
     Server address: Geben Sie den Hostnamen oder die IP-Adresse des Exchange-Servers ein.

     User ID: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein.
     Hinweis: Sie können in diesem Feld das Systemmakro ${user.username} verwenden, um die Benutzernamen automatisch ermitteln zu lassen.
     Password: Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.

     Domain: Geben Sie die Domäne ein, in der der Exchange-Server residiert.
     Hinweis: Sie können in diesem Feld das Systemmakro ${user.domainname} verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
     Email address: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein.
     Hinweis: Sie können in diesem Feld das Systemmakro ${user.mail}verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
     Use SSL: Wählen Sie aus, ob Verbindungen zwischen Benutzergeräten und dem Exchange-Server geschützt werden

sollen. Der Standardwert ist Ein.

- Bei Auswahl von Android HTC konfigurieren Sie die folgenden Einstellungen:



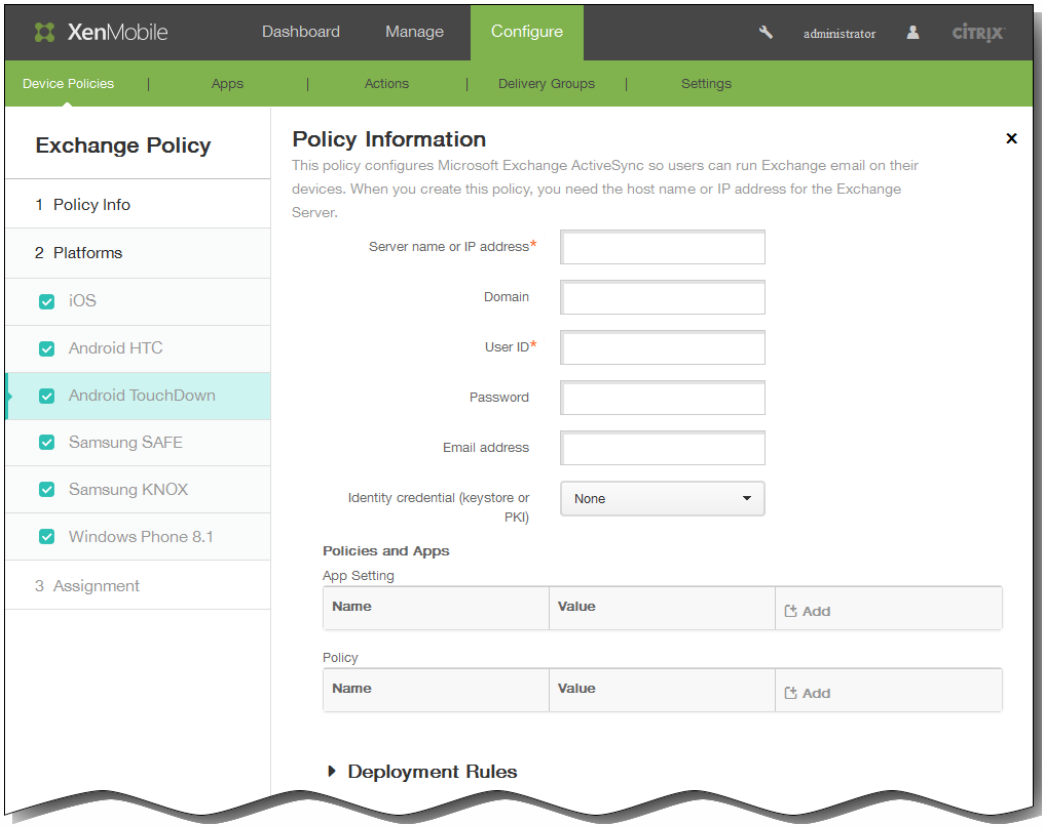
Configuration display name: Geben Sie den Namen für die Richtlinie ein, wie er auf den Geräten der Benutzer angezeigt werden soll.

Server address: Geben Sie den Hostnamen oder die IP-Adresse des Exchange-Servers ein.

User ID: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.username} verwenden, um die Benutzernamen automatisch ermitteln zu lassen.
Password: Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.

Domain: Geben Sie die Domäne ein, in der der Exchange-Server residiert.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.domainname} verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
Email address: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.mail}verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
Use SSL: Wählen Sie aus, ob Verbindungen zwischen Benutzergeräten und dem Exchange-Server geschützt werden sollen. Der Standardwert ist Ein.

- Bei Auswahl von Android TouchDown konfigurieren Sie die folgenden Einstellungen:



Server name or IP address: Geben Sie den Hostnamen oder die IP-Adresse des Exchange-Servers ein.

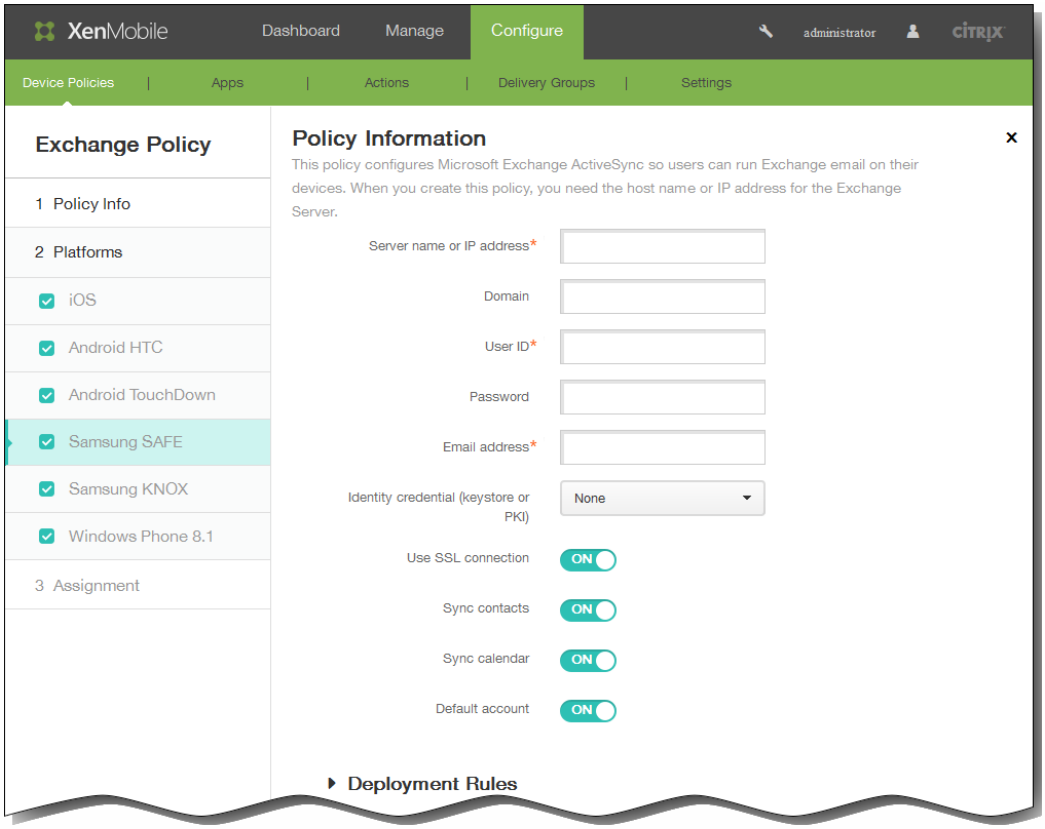
Domain: Geben Sie die Domäne ein, in der der Exchange-Server residiert.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.domainname} verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
User ID: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.username} verwenden, um die Benutzernamen automatisch ermitteln zu lassen.
Password: Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.

Email address: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.mail}verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
Identity credential (keystore or PKI): Klicken Sie in dieser Liste optional auf Identitätsanmeldeinformationen, sofern Sie einen Identitätsanbieter für XenMobile konfiguriert haben. Diese Angabe ist nur erforderlich, wenn Exchange eine Clientzertifikatauthentifizierung erfordert.

App Setting: Fügen Sie optional TouchDown-App-Einstellungen für die Richtlinie hinzu.

Policy: Fügen Sie optional TouchDown-Richtlinien für die Richtlinie hinzu.

- Bei Auswahl von Samsung SAFE oder Samsung KNOX konfigurieren Sie die folgenden Einstellungen:



Server name or IP address: Geben Sie den Hostnamen oder die IP-Adresse des Exchange-Servers ein.

Domain: Geben Sie die Domäne ein, in der der Exchange-Server residiert.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.domainname} verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
User ID: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.username} verwenden, um die Benutzernamen automatisch ermitteln zu lassen.
Password: Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.

Email address: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.mail}verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
Identity credential (keystore or PKI): Klicken Sie in dieser Liste optional auf Identitätsanmeldeinformationen, sofern Sie einen Identitätsanbieter für XenMobile konfiguriert haben. Diese Angabe ist nur erforderlich, wenn Exchange eine Clientzertifikatauthentifizierung erfordert.

Use SSL connection: Wählen Sie aus, ob Verbindungen zwischen Benutzergeräten und dem Exchange-Server geschützt werden sollen. Der Standardwert ist On.

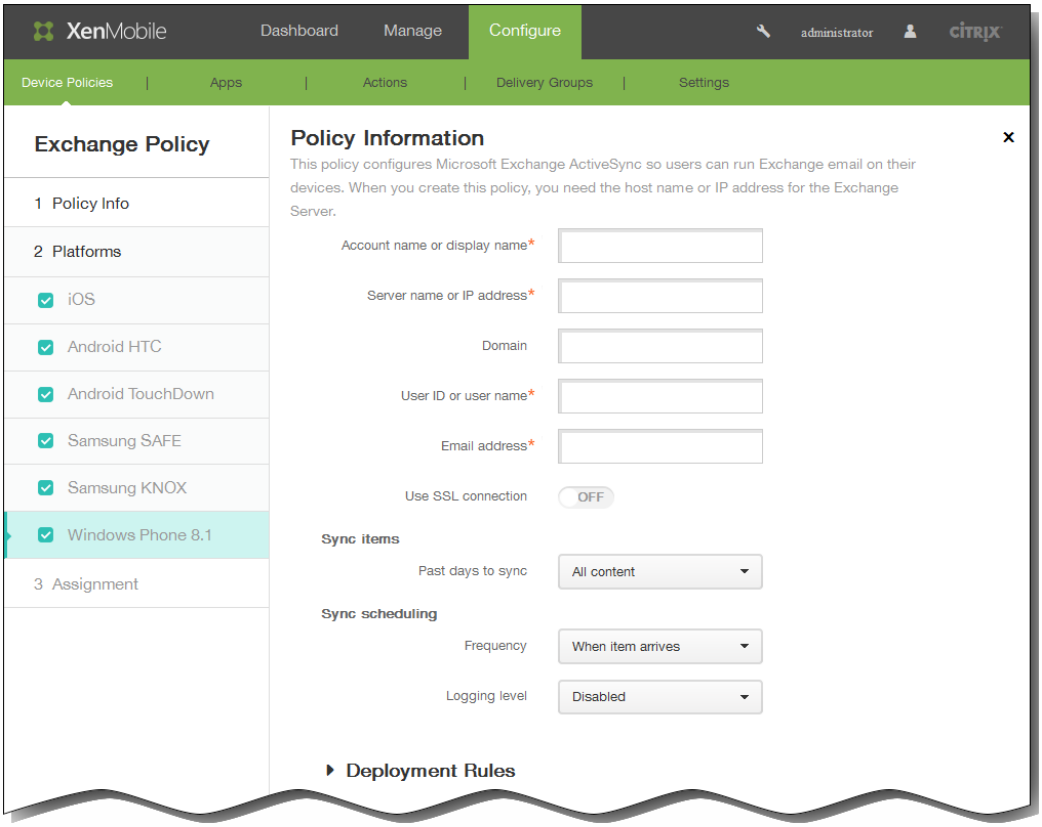
Synchronize contacts: Wählen Sie aus, ob die Synchronisierung von Kontakten zwischen den Benutzergeräten und dem Exchange Server ermöglicht werden soll. Der Standardwert ist On.

Synchronize calendar: Wählen Sie aus, ob die Synchronisierung des Kalenders zwischen den Benutzergeräten und dem Exchange Server ermöglicht werden soll. Der Standardwert ist On.

Default account: Wählen Sie aus, ob das Exchange-Konto der Benutzer standardmäßig für das Senden von E-Mail von ihren Geräten verwendet werden soll. Der Standardwert ist On.

- Bei Auswahl von Windows Phone 8.1 konfigurieren Sie die folgenden Einstellungen:

  Hinweis: Über diese Richtlinie können Sie nicht das Benutzerkennwort festlegen. Die Benutzer müssen diesen Parameter auf ihrem Gerät festlegen, nachdem Sie die Richtlinie per Push bereitgestellt haben.



Account name or display name: Geben Sie den Exchange ActiveSync-Kontonamen ein.

Server name or IP address: Geben Sie den Hostnamen oder die IP-Adresse des Exchange-Servers ein.

Domain: Geben Sie die Domäne ein, in der der Exchange-Server residiert.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.domainname} verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
User ID or user name: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.username} verwenden, um die Benutzernamen automatisch ermitteln zu lassen.
Email address: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein.
Hinweis: Sie können in diesem Feld das Systemmakro ${user.mail}verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
Use SSL connection: Wählen Sie aus, ob Verbindungen zwischen Benutzergeräten und dem Exchange-Server geschützt werden sollen. Der Standardwert ist Off.

Past days to sync: Wählen Sie in der Liste aus, wie viele Tage die Synchronisierung zwischen Gerät und dem Exchange-

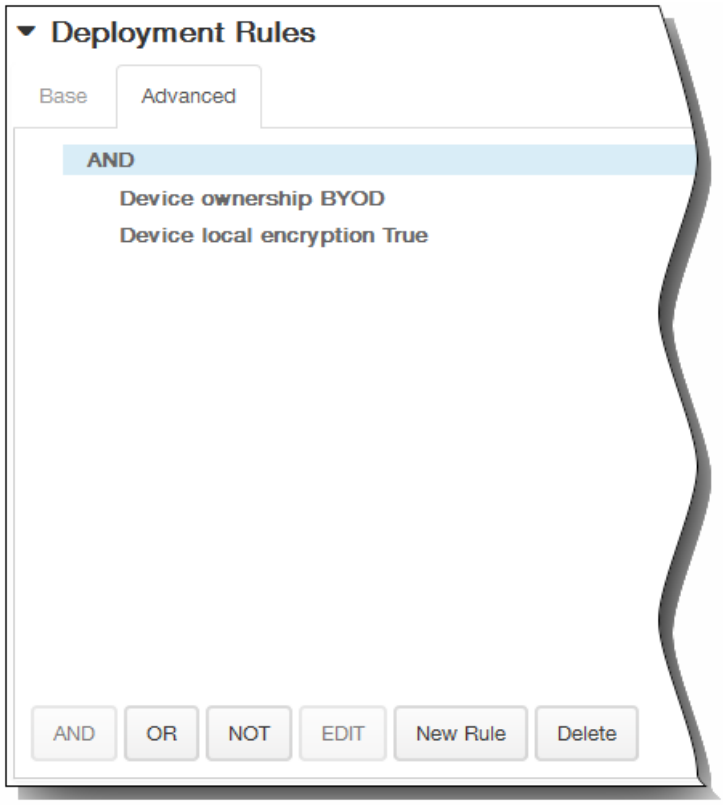
Server in die Vergangenheit reichen soll.

Frequency: Wählen Sie in der Liste den Zeitplan für die Synchronisierung von Daten, die vom Exchange-Server auf Geräte gesendet werden, aus.

Logging level: Klicken Sie in der Liste auf Disabled, Basic oder Advanced, um festzulegen, wie detailliert Exchange-Aktivitäten protokolliert werden sollen.

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

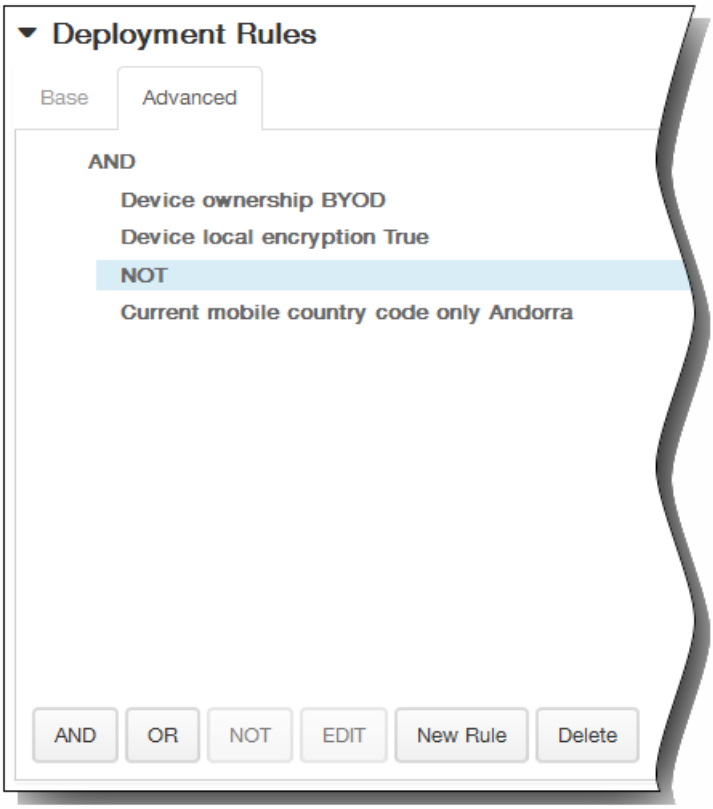
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie noch einmal 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.



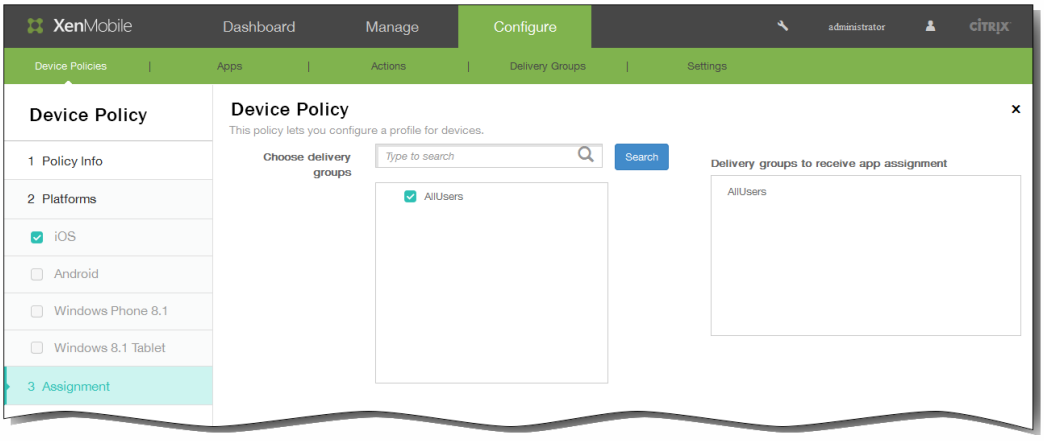
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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 noch einmal 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.



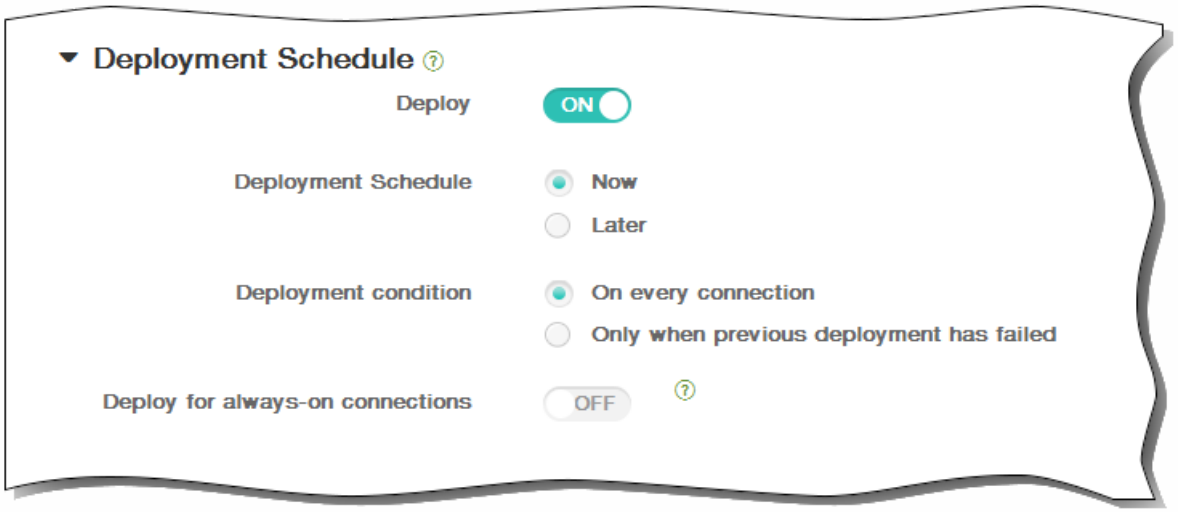
8. Klicken Sie auf Next. Die Seite Assignment für die Exchange-Richtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen 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 Speichern.

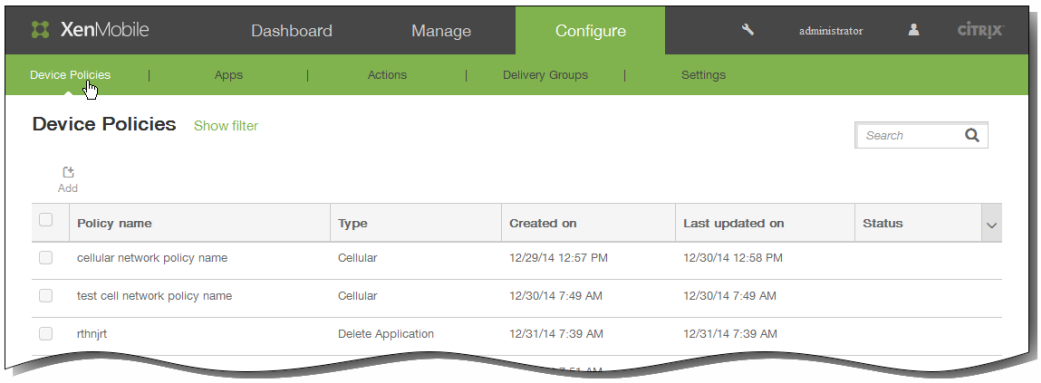
Standortrichtlinien für Geräte

May 05, 2016

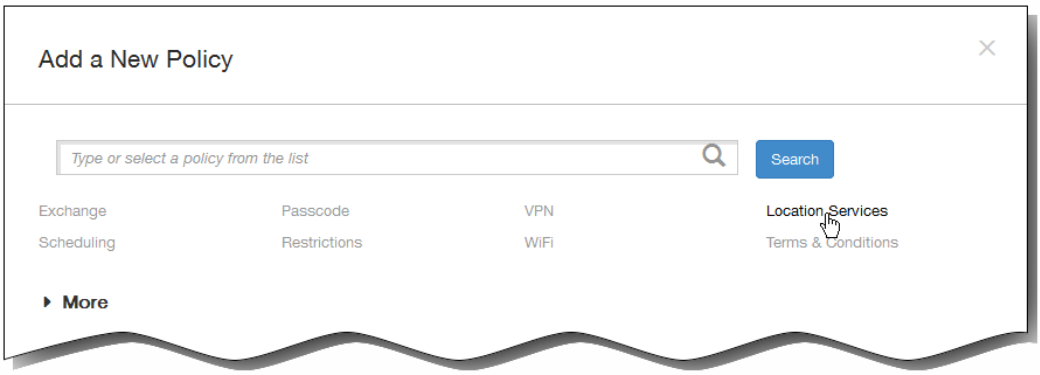
Mit einer Standortrichtlinie legen Sie in XenMobile geografische Grenzen fest und verfolgen den Standort und die Bewegung der Geräte der Benutzer. Wenn ein Benutzer den festgelegten Bereich ("Geofence") verlässt, kann XenMobile eine selektive oder vollständige Löschung der Daten auf seinem Gerät durchführen. Diese kann sofort erfolgen oder nach einem spezifischen Zeitraum, der es dem Benutzer gestattet, in den zulässigen Bereich zurückzukehren.

Sie können Standortrichtlinien für iOS und Android erstellen. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Abschnitt beschrieben.

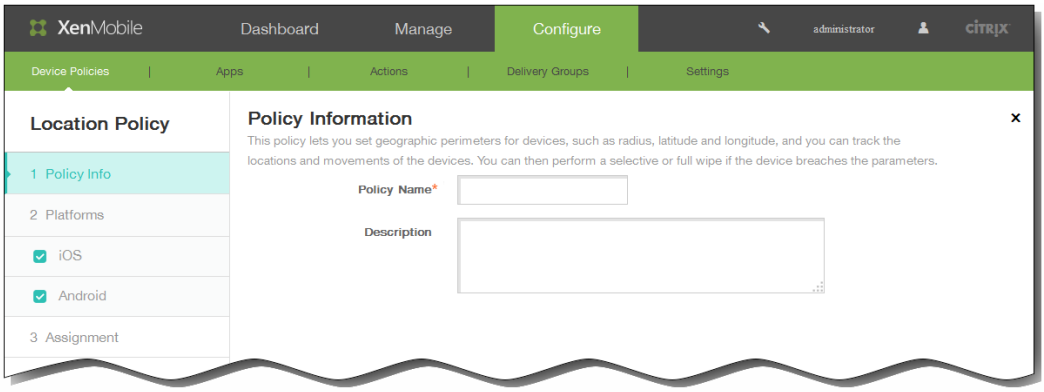
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



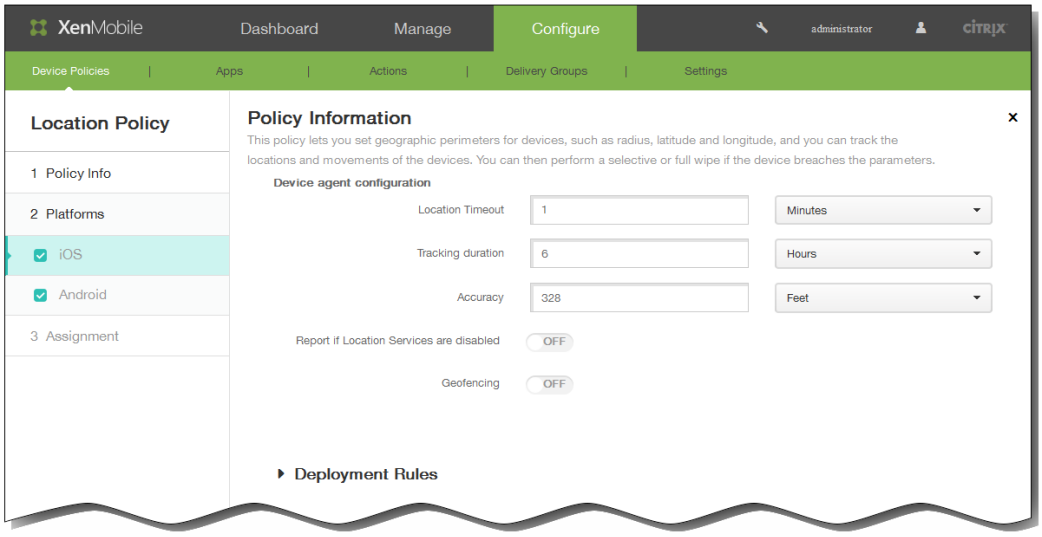
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add New Policy wird angezeigt.



3. Klicken Sie auf Location Services. Die Seite Location 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 iOS-Plattform wird als erstes angezeigt.



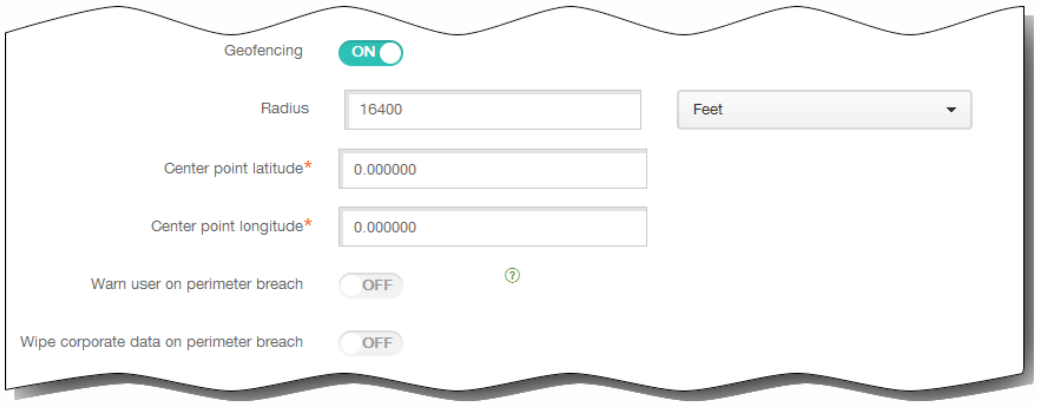
6. Wählen Sie unter Platforms die gewünschten Plattformen aus.
   - Bei Auswahl von iOS konfigurieren Sie die folgenden Einstellungen:
     Location timeout: Geben Sie eine Ziffer ein und klicken Sie in der Liste auf Seconds oder Minutes, um festzulegen, wie häufig XenMobile den Gerätestandort abrufen soll. Gültige Werte sind 60-900 Sekunden oder 1-15 Minuten. Der Standardwert ist 1 Minute.

     Tracking duration: Geben Sie eine Ziffer ein und klicken Sie in der Liste auf Hours oder Minutes, um festzulegen, wie lange XenMobile das Gerät verfolgen soll. Gültige Werte sind 1-6 Stunden oder 10-360 Minuten. Der Standardwert ist 6 Stunden.

     Accuracy: Geben Sie eine Ziffer ein und klicken Sie in der Liste auf Meters, Feet oder Yards, um festzulegen, wie nahe am Gerät XenMobile das Gerät verfolgen soll. Gültige Werte sind 10-5000 Yard/Meter oder 30-15000 Fuß. Der Standardwert ist 328 Fuß.

Report if Location Services are disabled: Wählen Sie, ob das Gerät einen Bericht an XenMobile senden soll, wenn GPS deaktiviert ist. Der Standardwert ist OFF.

Geofencing: Wählen Sie diese Option, um die folgenden Einstellungen zu konfigurieren:



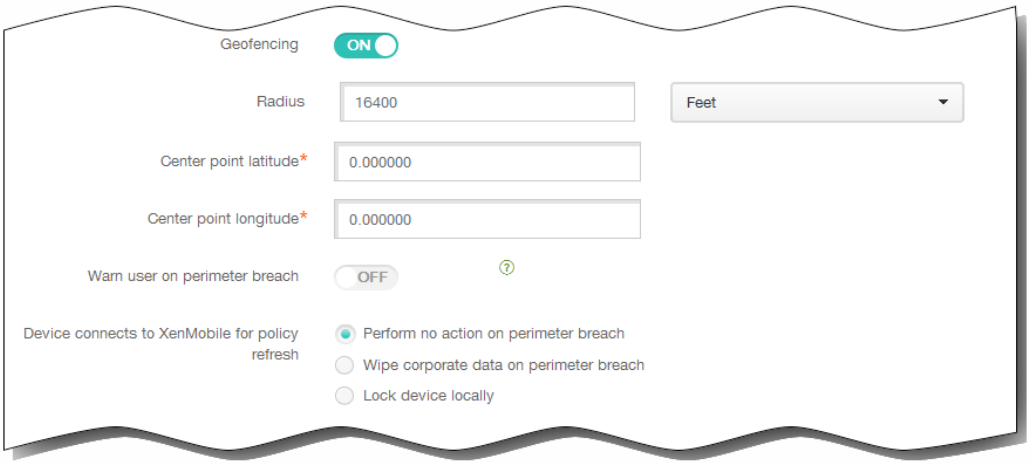
- Radius: Geben Sie zur Messung des Radius eine Ziffer ein und klicken Sie in Liste auf die Einheit. Der Standardwert ist 16.400 Fuß.
  Gültige Werte für den Radius:
  - 164-164000 Fuß
  - 1-50 Kilometer
  - 50-50000 Meter
  - 54-54680 Yard
  - 1-31 Meilen
- Center point latitude: Geben Sie einen Wert (z. B. 37.787454) zum Festlegen des Breitengrads des Geofence-Mittelpunkts ein.
- Center point longitude: Geben Sie einen Wert (z. B. 122.402952) zum Festlegen des Längengrads des Geofence-Mittelpunkts ein.
- Warn user on perimeter breach: Wählen Sie aus, ob eine Warnmeldung angezeigt werden soll, wenn Benutzer den vorgegebenen Bereich verlassen. Der Standardwert ist OFF. Zum Anzeigen der Warnmeldung ist keine Verbindung mit XenMobile erforderlich.
- Wipe corporate data on perimeter breach: Wählen Sie aus, ob auf den Geräten bei Verlassen des Bereichs eine Datenlöschung erfolgen soll. Der Standardwert ist OFF.
  Wenn Sie diese Option aktivieren, wird das Feld Delay on local wipe angezeigt.

  Geben Sie eine Ziffer ein und klicken Sie in der Liste auf Seconds oder Minutes, um die Dauer der Verzögerung bis zum Löschen der Unternehmensdaten von den Geräten festzulegen. Dadurch haben Benutzer die Möglichkeit, in den zulässigen Bereich zurückzukehren, bevor XenMobile eine selektive Datenlöschung auf ihrem Gerät durchführt. Der Standardwert ist 0 Sekunden.

- Bei Auswahl von Android konfigurieren Sie die folgenden Einstellungen:
  Poll interval: Geben Sie eine Ziffer ein und klicken Sie in der Liste auf Minutes, Hours oder Days, um festzulegen, wie häufig XenMobile den Gerätestandort abrufen soll. Gültige Werte sind 1-1440 Minuten, 1-24 Stunden oder eine beliebige Anzahl an Tagen. Der Standardwert ist 10 Minuten.
  Hinweis: Wenn dieser Wert auf weniger als 10 Minuten festgelegt wird, kann dies die Akkulaufzeit des Geräts

nachteilig beeinflussen.
Report if Location Services are disabled: Wählen Sie, ob das Gerät einen Bericht an XenMobile senden soll, wenn GPS deaktiviert ist. Der Standardwert ist OFF.

Geofencing: Wählen Sie diese Option, um die folgenden Einstellungen zu konfigurieren:



- Radius: Geben Sie zur Messung des Radius eine Ziffer ein und klicken Sie in Liste auf die Einheit. Der Standardwert ist 16.400 Fuß.
  Gültige Werte für den Radius:
  - 164-164000 Fuß
  - 1-50 Kilometer
  - 50-50000 Meter
  - 54-54680 Yard
  - 1-31 Meilen
- Center point latitude: Geben Sie einen Wert (z. B. 37.787454) zum Festlegen des Breitengrads des Geofence-Mittelpunkts ein.
- Center point longitude: Geben Sie einen Wert (z. B. 122.402952) zum Festlegen des Längengrads des Geofence-Mittelpunkts ein.
- Warn user on perimeter breach: Wählen Sie aus, ob eine Warnmeldung angezeigt werden soll, wenn Benutzer den vorgegebenen Bereich verlassen. Der Standardwert ist OFF. Zum Anzeigen der Warnmeldung ist keine Verbindung mit XenMobile erforderlich.
- Device connects to XenMobile for policy refresh: Wählen Sie eine der folgenden Aktionen aus, die durchgeführt werden soll, wenn Benutzer den Bereich verlassen:
  - Perform no action on perimeter breach: keine Aktion. Dies ist die Standardeinstellung.
  - Wipe corporate data on perimeter breach: Unternehmensdaten werden nach einem festgelegten Zeitraum gelöscht.
    Wenn Sie diese Option aktivieren, wird das Feld Delay on local wipe angezeigt.

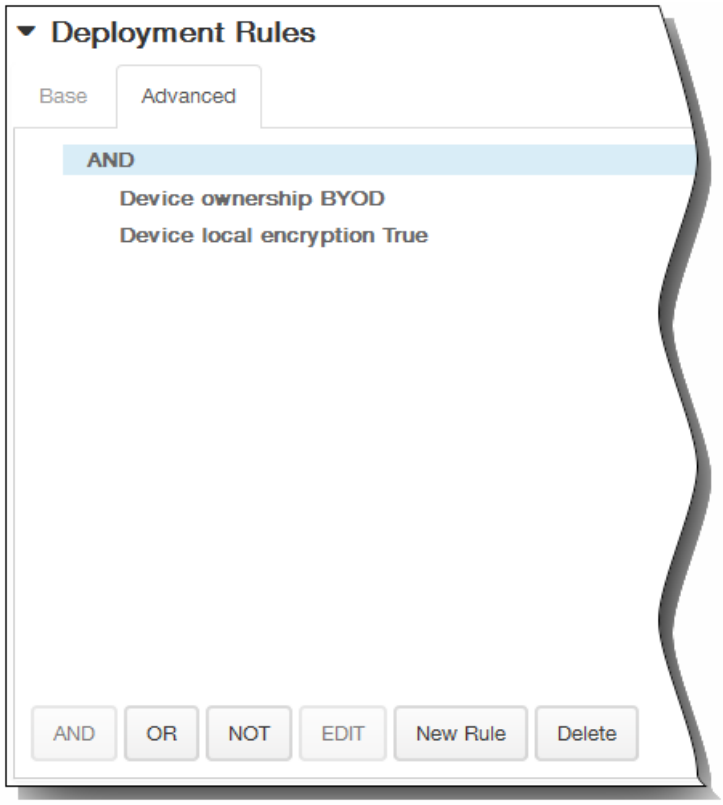
    Geben Sie eine Ziffer ein und klicken Sie in der Liste auf Seconds oder Minutes, um die Dauer der Verzögerung bis zum Löschen der Unternehmensdaten von den Geräten festzulegen. Dadurch haben Benutzer die Möglichkeit, in den zulässigen Bereich zurückzukehren, bevor XenMobile eine selektive Datenlöschung auf ihrem Gerät durchführt. Der Standardwert ist 0 Sekunden.

- Delay on lock: Sperrt die Geräte nach einem festgelegten Zeitraum.
  Wenn Sie diese Option aktivieren, wird das Feld Delay on lock angezeigt.

  Geben Sie eine Ziffer ein und klicken Sie in der Liste auf Seconds oder Minutes, um die Dauer der Verzögerung bis zum Sperren der Geräte festzulegen. Dadurch haben Benutzer die Möglichkeit, in den zulässigen Bereich zurückzukehren, bevor XenMobile die Geräte sperrt. Der Standardwert ist 0 Sekunden.

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

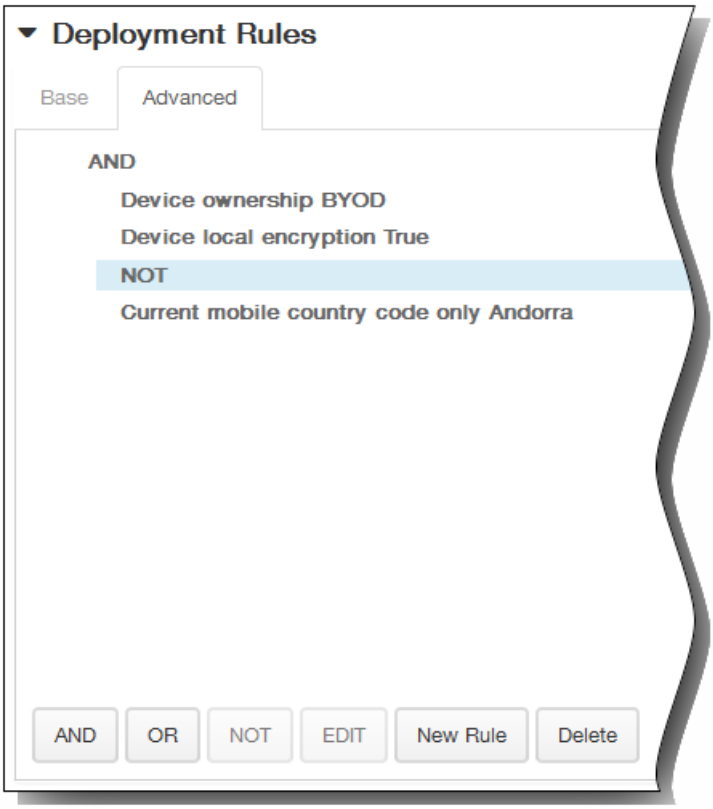
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
   3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
   4. Klicken Sie noch einmal 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.



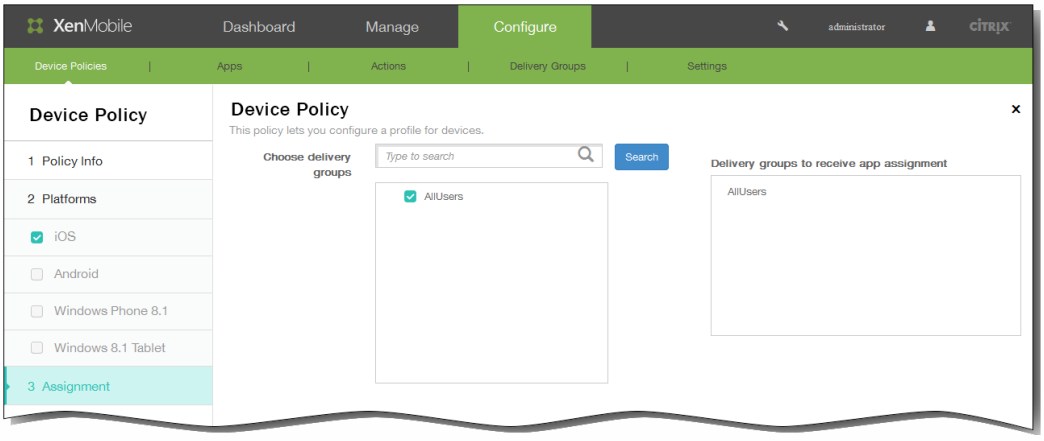
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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 noch einmal 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.



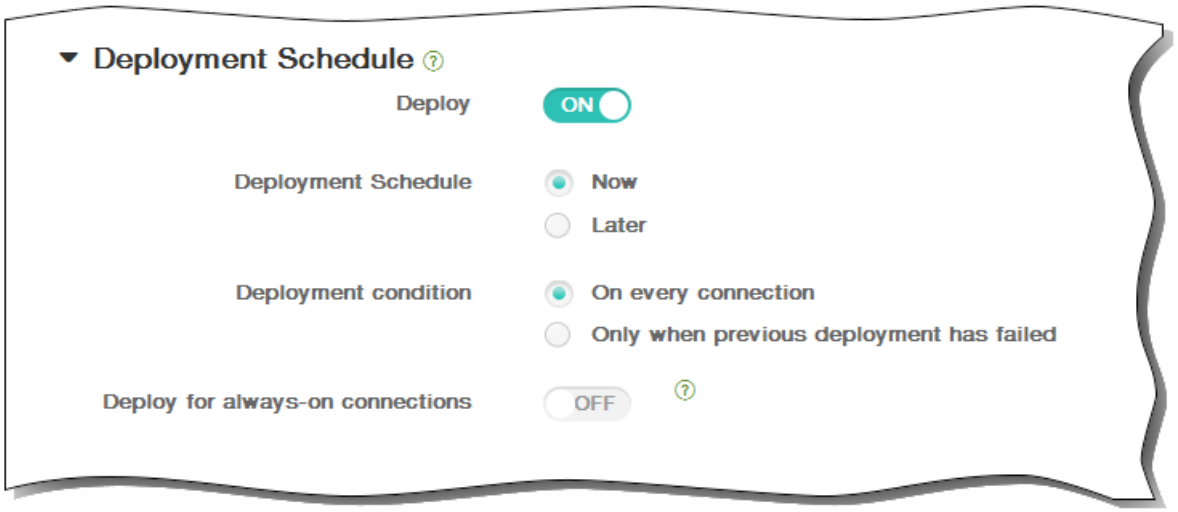
8. Klicken Sie auf Next. Die Seite Location Policy für die Standortrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.



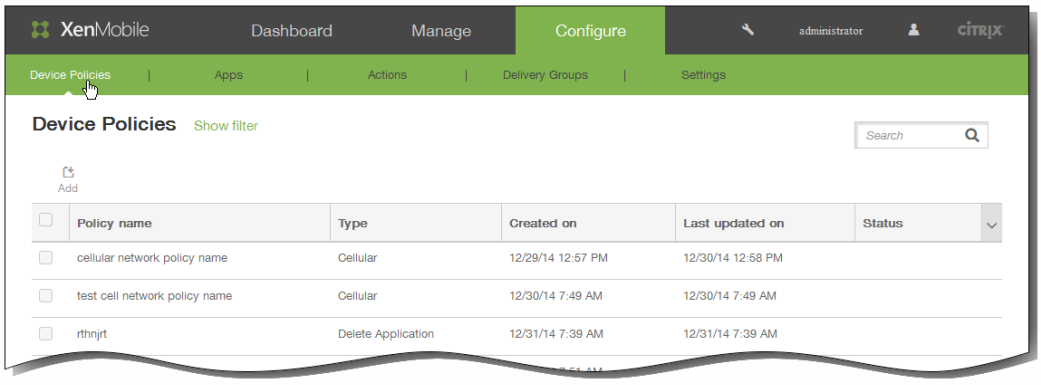
11. Klicken Sie auf Save, um die Richtlinie zu speichern.

Verbindungszeitplanrichtlinien für Geräte

May 05, 2016

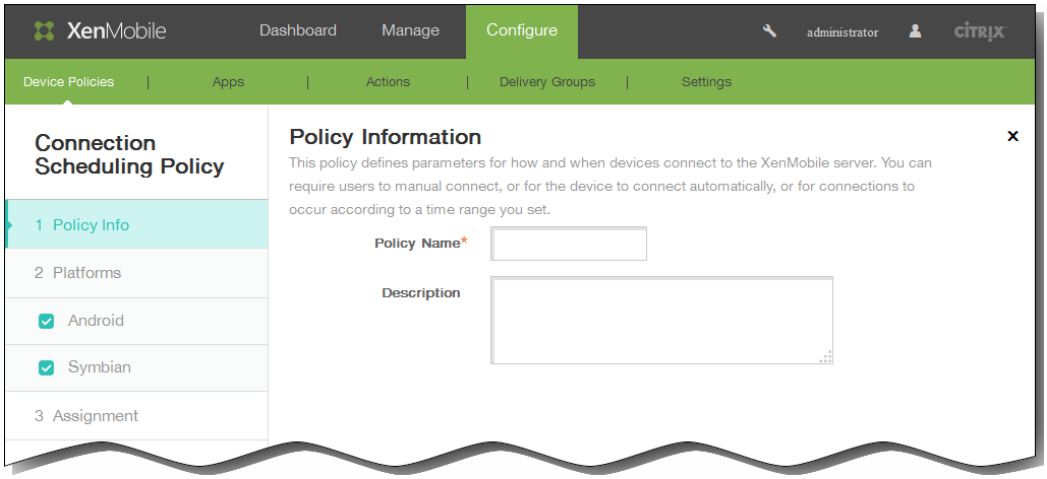
Sie erstellen Verbindungszeitplanrichtlinien, um zu vorzugeben, wie und wann Android- und Symbian-Geräte eine Verbindung mit XenMobile herstellen sollen. Sie können festlegen, dass Benutzer eine Verbindung manuell herstellen, dass die Geräte permanent verbunden bleiben oder dass die Geräte in einem festgelegten Zeitrahmen eine Verbindung herstellen.

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 Scheduling. Die Seite Connection Scheduling 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 Android-Plattform wird als erstes angezeigt.
6. Wählen Sie unter Platforms die gewünschten Plattformen aus.
7. Konfigurieren Sie für jede ausgewählte Plattform die folgenden Einstellungen: Require devices to connect: Klicken Sie auf die Option, die Sie für diesen Zeitplan festlegen möchten.
   - Always: Die Verbindung bleibt jederzeit bestehen. XenMobile auf dem Benutzergerät versucht nach einer Netzwerkverbindungsunterbrechung eine Wiederherstellung der Verbindung mit dem XenMobile-Server und überwacht die Verbindung durch regelmäßige Übertragung von Steuerpaketen.
     Diese Option wird nicht empfohlen, da sie viel Akkuleistung erfordert und viel Netzwerkdatenverkehr generiert.
   - Never: Die Verbindung muss manuell hergestellt werden. Die Benutzer müssen die Verbindung mit XenMobile auf ihrem Gerät herstellen.
   - Every: Die Verbindung wird in dem hier ausgewählten Intervall hergestellt. Die Geräte stellen nach dem hier in Minuten definierten Intervall automatisch eine Verbindung her.
     Wenn Sie diese Option auswählen, wird das Feld Connect every N minutes eingeblendet, in dem Sie die Zeitdauer (in Minuten) eingeben müssen, nach der Geräte eine Verbindung wiederherstellen. Der Standardwert ist 20.
   - Define schedule: XenMobile auf dem Benutzergerät versucht nach einer Netzwerkverbindungsunterbrechung eine Wiederherstellung der Verbindung mit dem XenMobile-Server und überwacht die Verbindung durch regelmäßige Übertragung von Steuerpaketen innerhalb des von Ihnen definierten Zeitrahmens. Im folgenden Abschnitt wird beschrieben, wie Sie einen Verbindungszeitrahmen definieren.

     So definieren Sie einen Verbindungszeitrahmen

     Wenn Sie die folgenden Optionen aktivieren, wird eine Zeitachse angezeigt, mit der Sie den gewünschten Zeitrahmen definieren können. Sie können jeweils eine oder beide Optionen für eine bleibende Verbindung zu einer spezifischen Zeit oder zum Erzwingen einer Verbindung innerhalb bestimmter Zeitrahmen aktivieren. Jedes Quadrat der Zeitachse repräsentiert 30 Minuten. Wenn Sie beispielsweise eine Verbindung zwischen 8:00 und 9:00 Uhr an jedem Werktag wünschen, klicken Sie für jeden Werktag auf die beiden Quadrate zwischen 8:00 und 9:00 Uhr.

     Beispiel: Die beiden Zeitachsen in der folgenden Abbildung definieren die Erfordernis einer bleibenden Verbindung

zwischen 8:00 und 9:00 Uhr an allen Werktagen und zwischen 12:00 Samstag und 1:00 Uhr Sonntag sowie mindestens eine Verbindung an allen Werktagen zwischen 5:00 und 8:00 Uhr oder zwischen 10:00 und 23:00 Uhr.

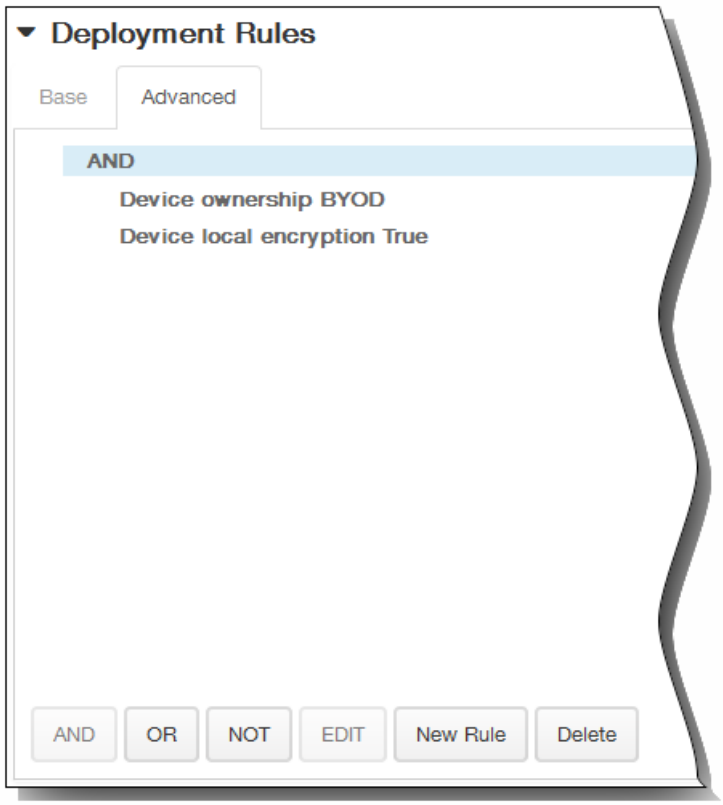
Maintain permanent connection during these hours: Die Geräte der Benutzer müssen während der definierten Zeiten verbunden sein.

Require a connection within each of these ranges: Die Geräte der Benutzer müssen während der definierten Zeiten mindestens einmal verbunden sein.

Use local device time rather than UTC: Der Zeitrahmen soll auf die lokale Zeit des Geräts synchronisiert werden, anstelle die koordinierte Weltzeit (UTC) zu verwenden.

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

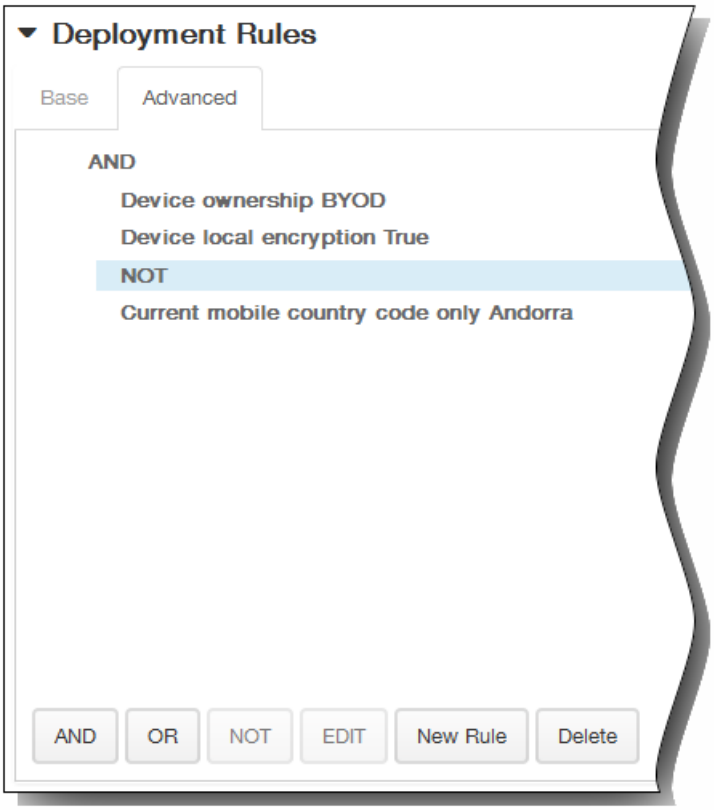
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
   3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
   4. Klicken Sie noch einmal 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.



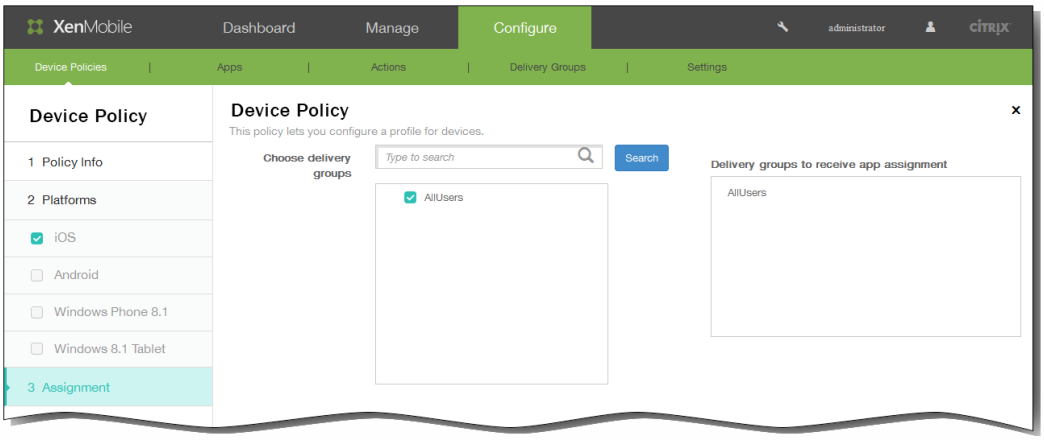
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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 noch einmal 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.



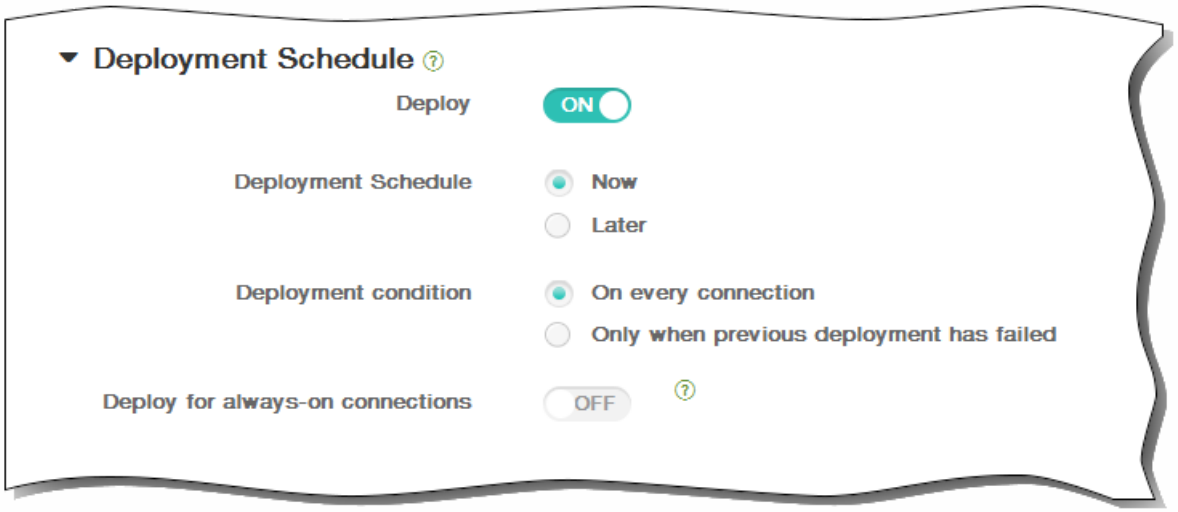
9. Klicken Sie auf Next. Die Seite Assignment für die Verbindungszeitplanrichtlinie wird angezeigt.
10. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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. 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.



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

So fügen Sie eine AirPlay-Spiegelungsrichtlinie für iOS-Geräte hinzu

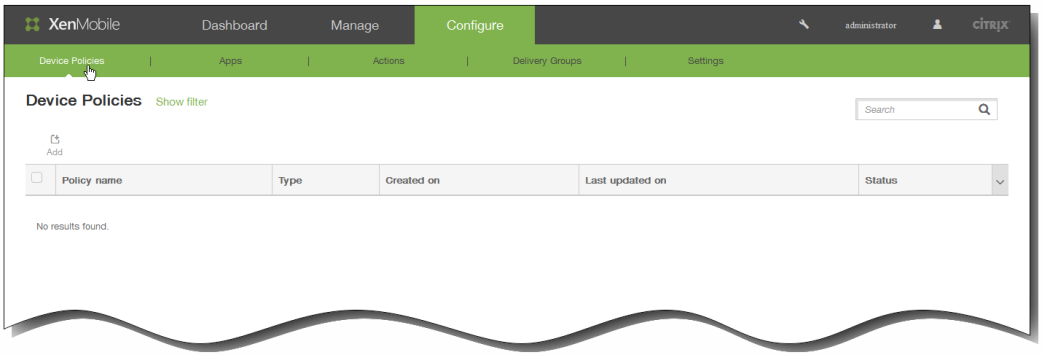
May 05, 2016

Mit dem Apple AirPlay-Feature kann Inhalt drahtlos von einem iOS-Gerät über Apple TV auf einen Fernseher gestreamt oder die Anzeige auf dem Gerät auf einem Fernseher oder einem Mac-Computer gespiegelt werden.

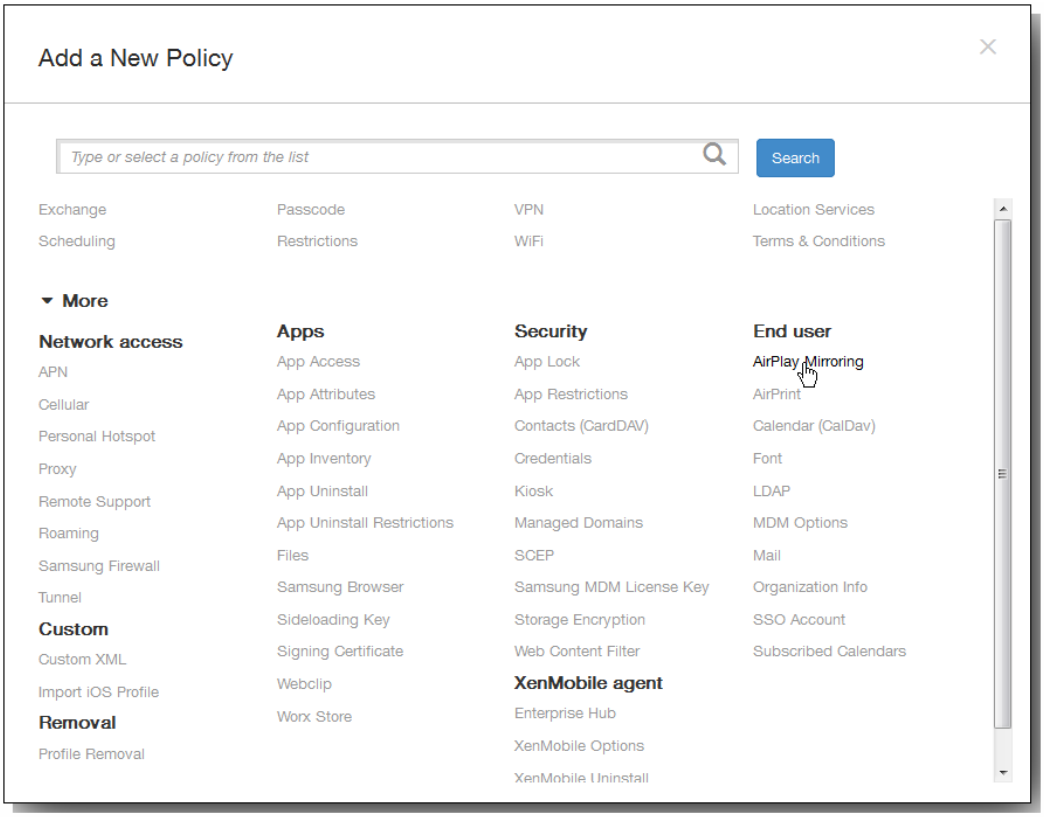
Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen spezifischer AirPlay-Geräte (z. B. Apple TV oder einen anderen Mac-Computer) einrichten und iOS-Geräten hinzufügen. Zudem können Sie Geräte zu einer Positivliste überwachter Geräte hinzufügen, sodass Benutzer nur die AirPlay-Geräte auf der Positivliste verwenden können. 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.

Hinweis: Sammeln Sie zunächst die Kennungen und Kennwörter aller Geräte, die Sie hinzufügen möchten.

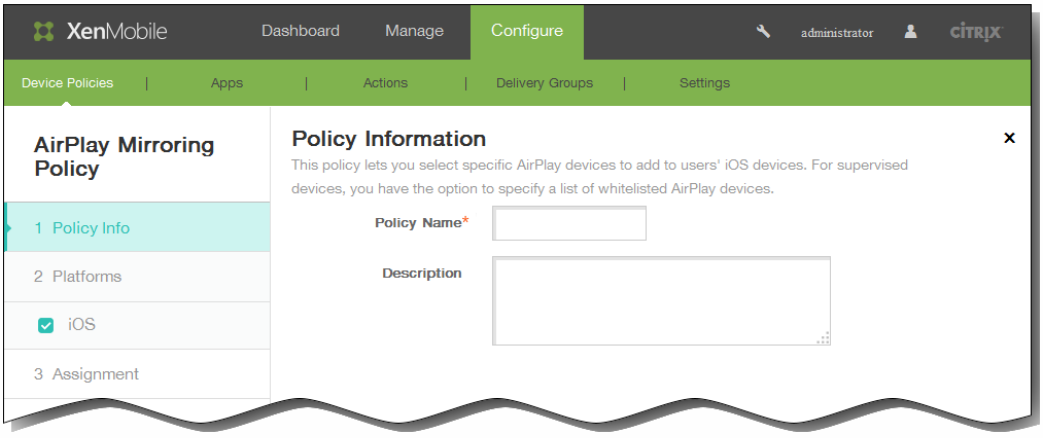
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



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 End user auf AirPlay Mirroring. Die Seite AirPlay Mirroring 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.

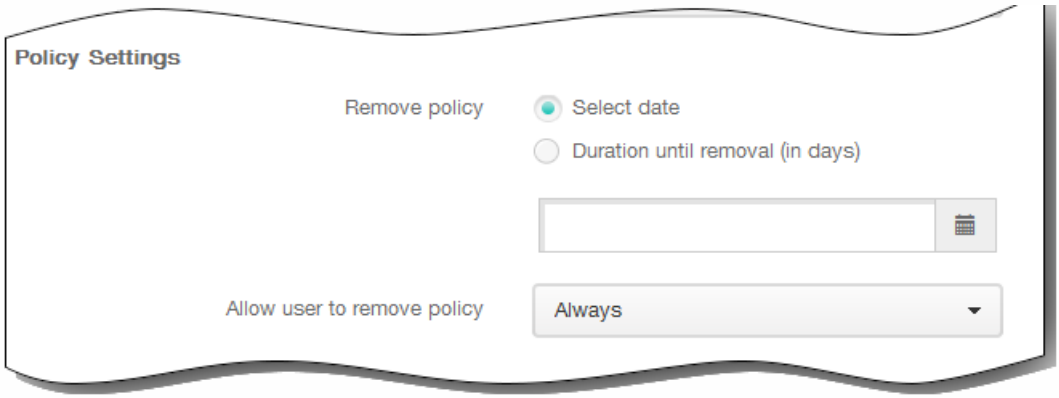
6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:

1. AirPlay Password: Klicken Sie auf Add und führen Sie folgende Schritte aus:
    1. Device ID: Geben Sie die Gerätekennung im Format xx:xx:xx:xx:xx:xx ein. Bei diesem Feld wird nicht zwischen Groß- und Kleinschreibung unterschieden.
    2. Password: Geben Sie optional ein Kennwort für das Gerät ein.
    3. Klicken Sie auf Add, um das Gerät hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
    4. Wiederholen Sie die Schritte i bis iii für jedes Gerät, das Sie hinzufügen möchten.
2. Whitelist ID: Klicken Sie auf Add und führen Sie folgende Schritte aus, um überwachte Geräte auf die Kennungen in der Positivliste zu beschränken:
   Hinweis: Diese Liste wird bei unbetreuten Geräten ignoriert.
    1. Device ID: Verwenden Sie für die Geräte-ID das xx:xx:xx:xx:xx:xx -Format Bei diesem Feld wird nicht zwischen Groß- und Kleinschreibung unterschieden.
    2. Klicken Sie auf Add, um das Gerät hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
    3. Wiederholen Sie die Schritte i und ii für jedes Gerät, das Sie der Positivliste hinzufügen möchten.

   Hinweis: Zum Löschen eines vorhandenen Geräts 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.

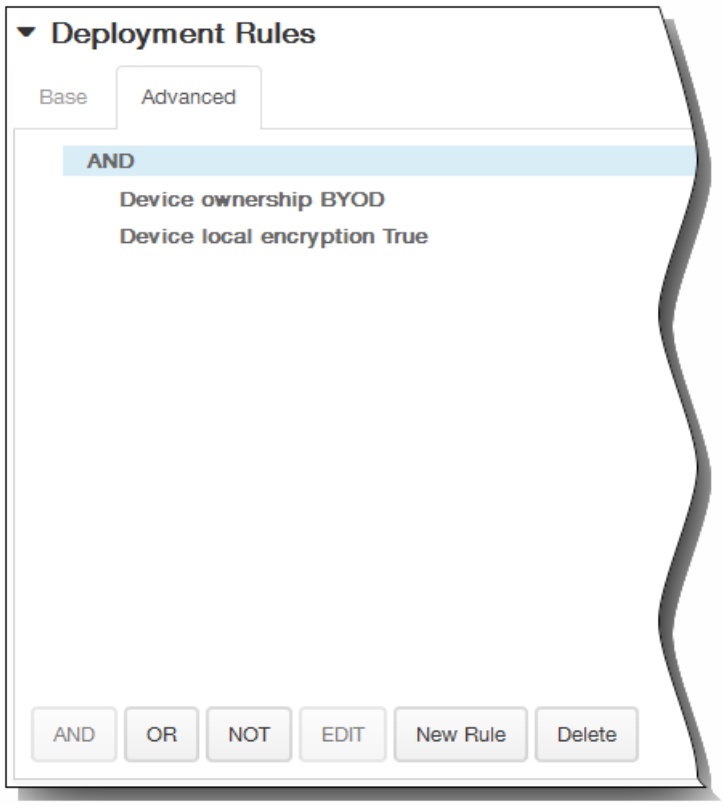
   Zum Bearbeiten eines Geräts zeigen Sie auf dessen Zeile und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf Save, um die Änderungen zu speichern oder auf Cancel, um den Vorgang abzubrechen.

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.

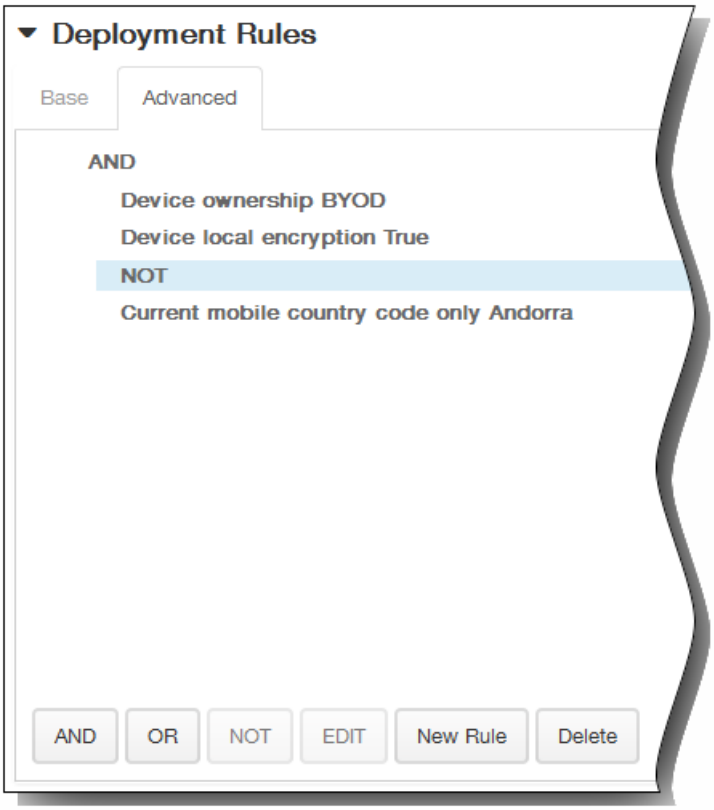
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



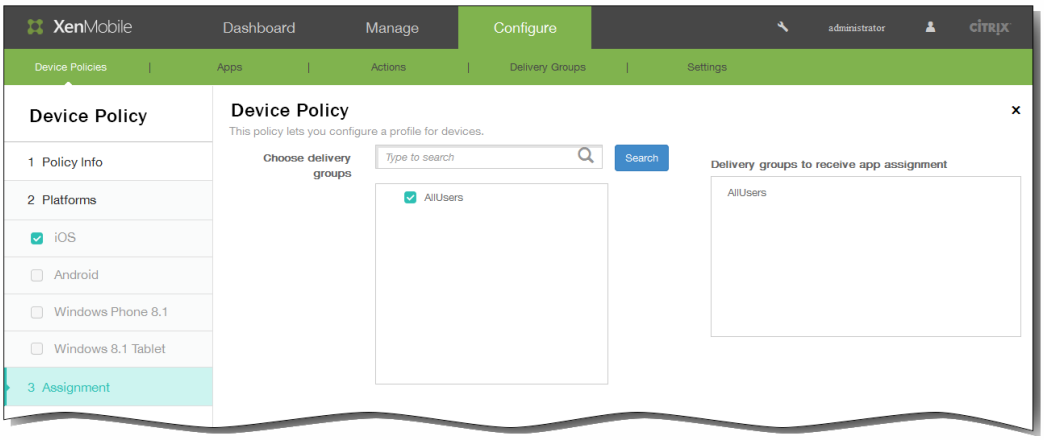
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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.



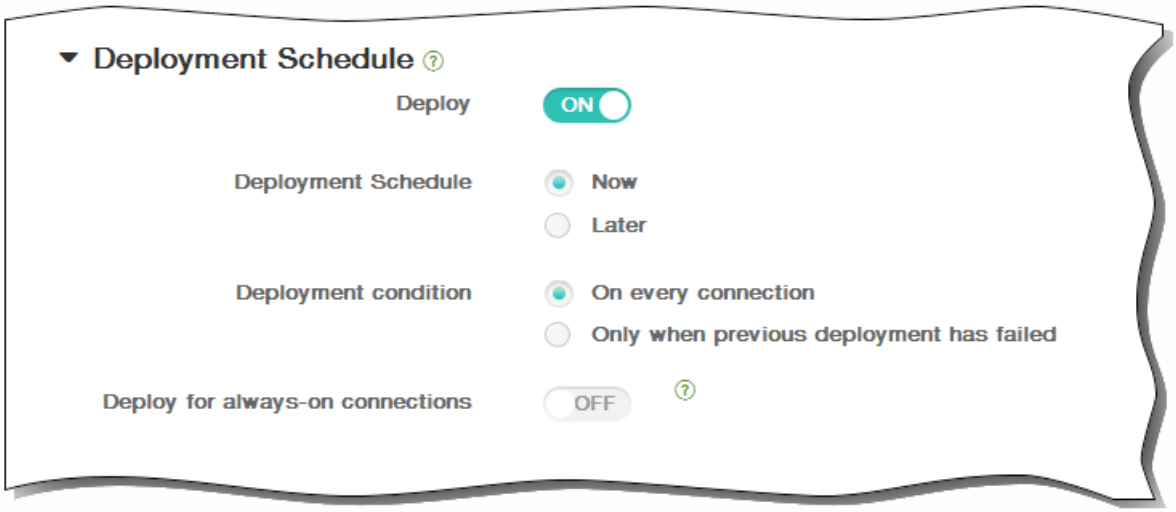
12. Klicken Sie auf Next. Die Seite Assignment für die AirPlay-Spiegelungsrichtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.

So fügen Sie eine AirPrint-Geräterichtlinie für iOS hinzu

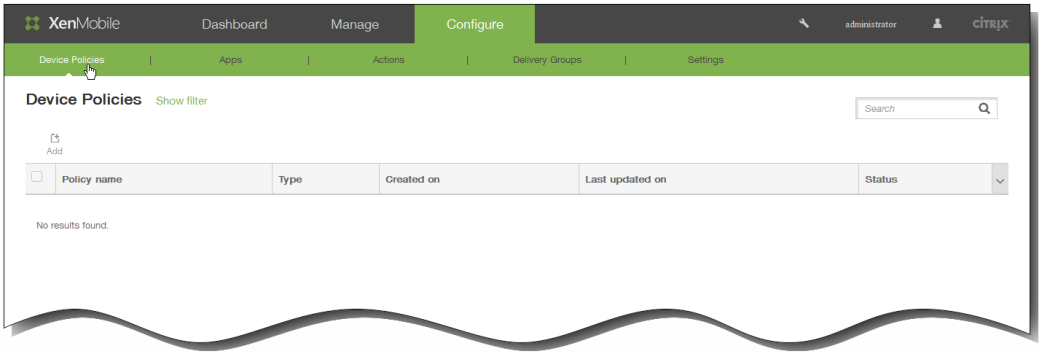
May 05, 2016

Sie können in XenMobile eine Geräterichtlinie einrichten, mit der AirPrint-Drucker der AirPrint-Druckerliste auf iOS-Geräten hinzugefügt wird. Diese Richtlinie erleichtert die Pflege von Umgebungen, bei denen Drucker und Geräte in verschiedenen Subnetzen sind.

Hinweis:

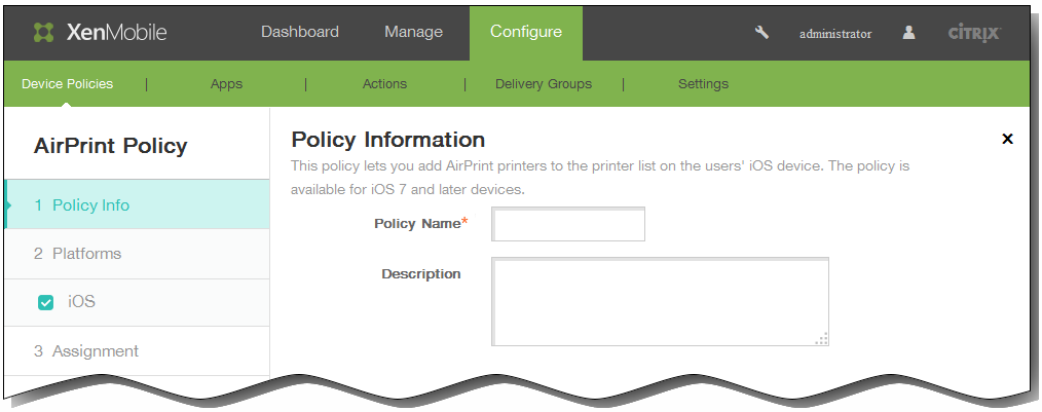
- Die Richtlinie gilt für iOS 7.0 und höher.
- Stellen Sie sicher, dass Sie die IP-Adresse und den Ressourcenpfad für jeden Drucker haben.

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.

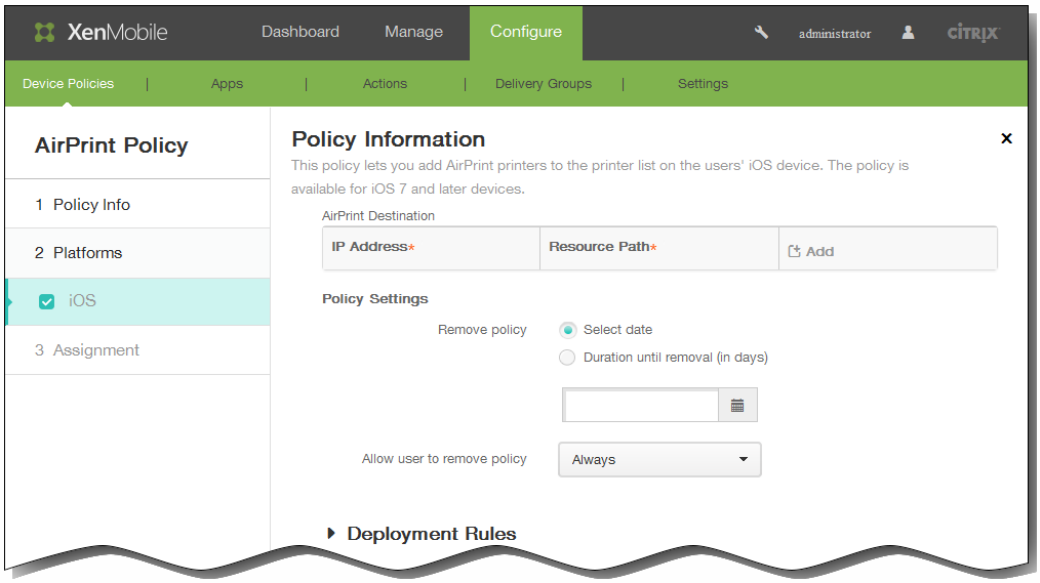
3. Klicken Sie auf More und dann unter End user auf AirPrint. Die Seite AirPrint Policy wird angezeigt.



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.

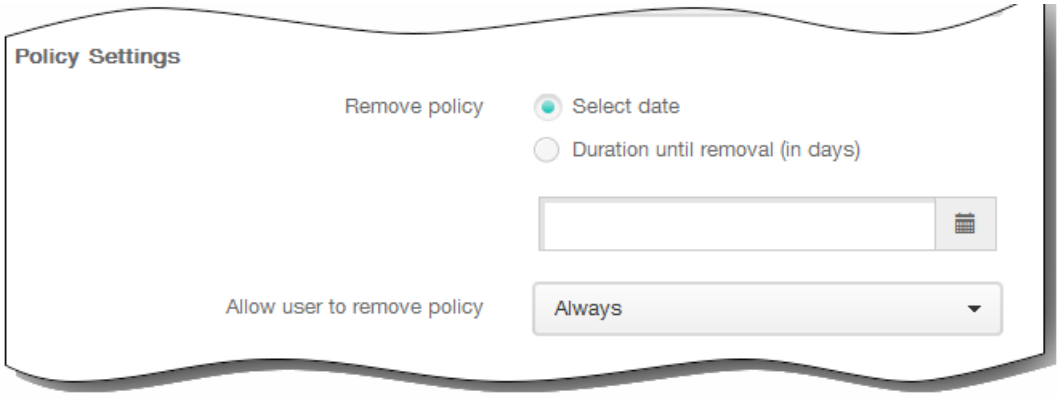


6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:
   1. AirPrint Destination: Klicken Sie auf Add und führen Sie folgende Schritte aus:
      1. IP Address: Geben Sie die IP-Adresse des AirPrint-Druckers ein.
      2. Resource Path: Geben Sie den Ressourcenpfad des Druckers ein. Dieser entspricht dem Parameter des _ipps.tcp Bonjour-Datensatzes. Beispiel: printers/Canon_MG5300_series oder printers/Xerox_Phaser_7600.
      3. Klicken Sie auf Add, um den Drucker hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
      4. Wiederholen Sie die Schritte i bis iii für jedes Gerät, das Sie hinzufügen möchten.

      Hinweis: Zum Löschen eines vorhandenen Druckers 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.

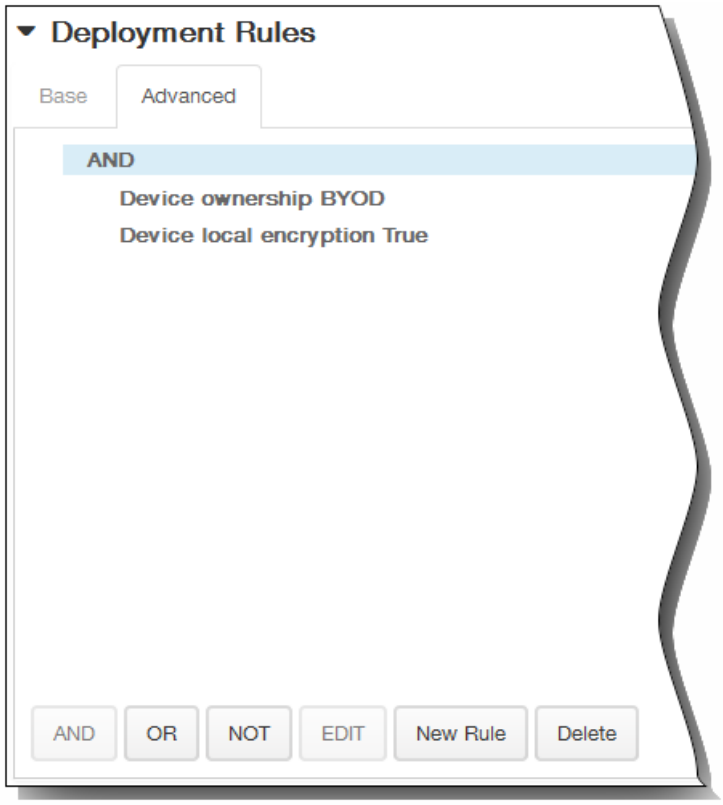
      Zum Bearbeiten eines Druckers zeigen Sie auf dessen Zeile und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf Save, um die Änderungen zu speichern oder auf Cancel, um den Vorgang abzubrechen.

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.

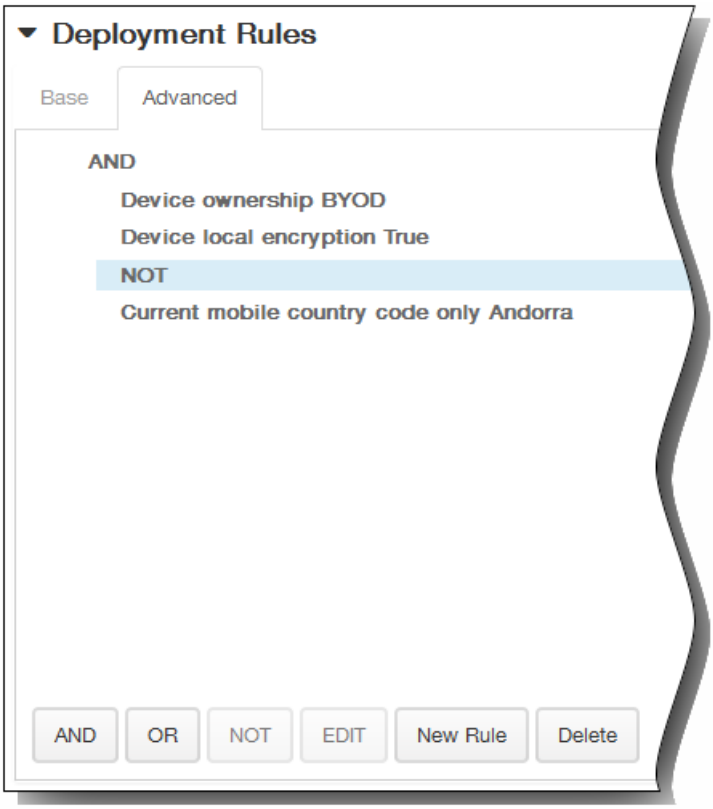
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen 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.



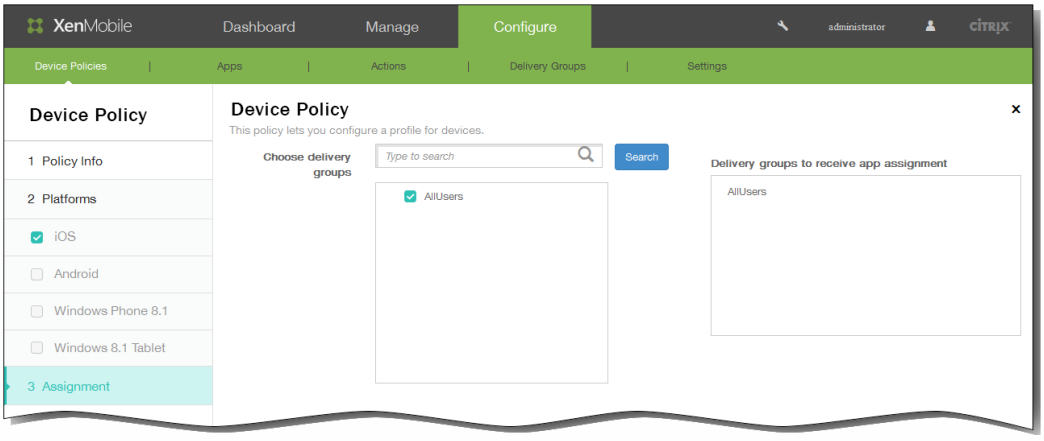
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



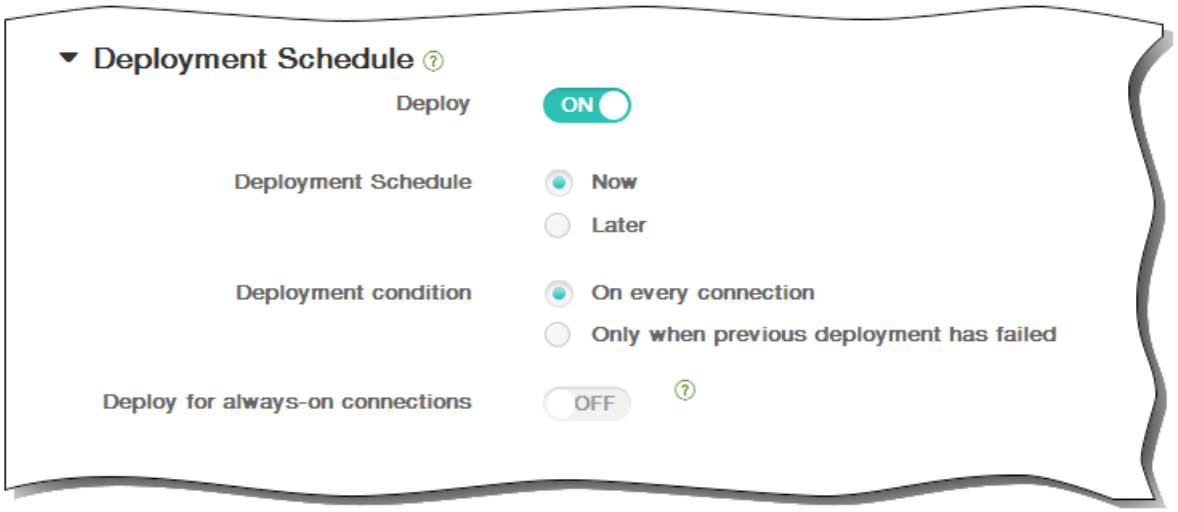
12. Klicken Sie auf Next. Die Seite Assignment für die AirPrint-Richtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.



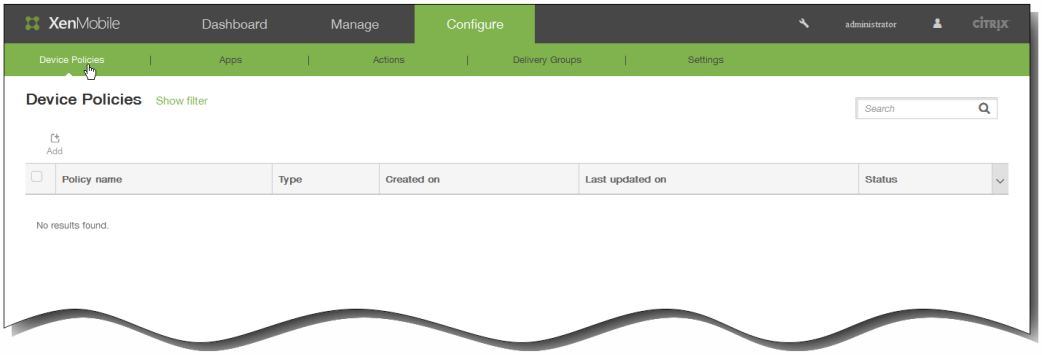
15. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Kalenderrichtlinie (CalDAV) für iOS-Geräte hinzu

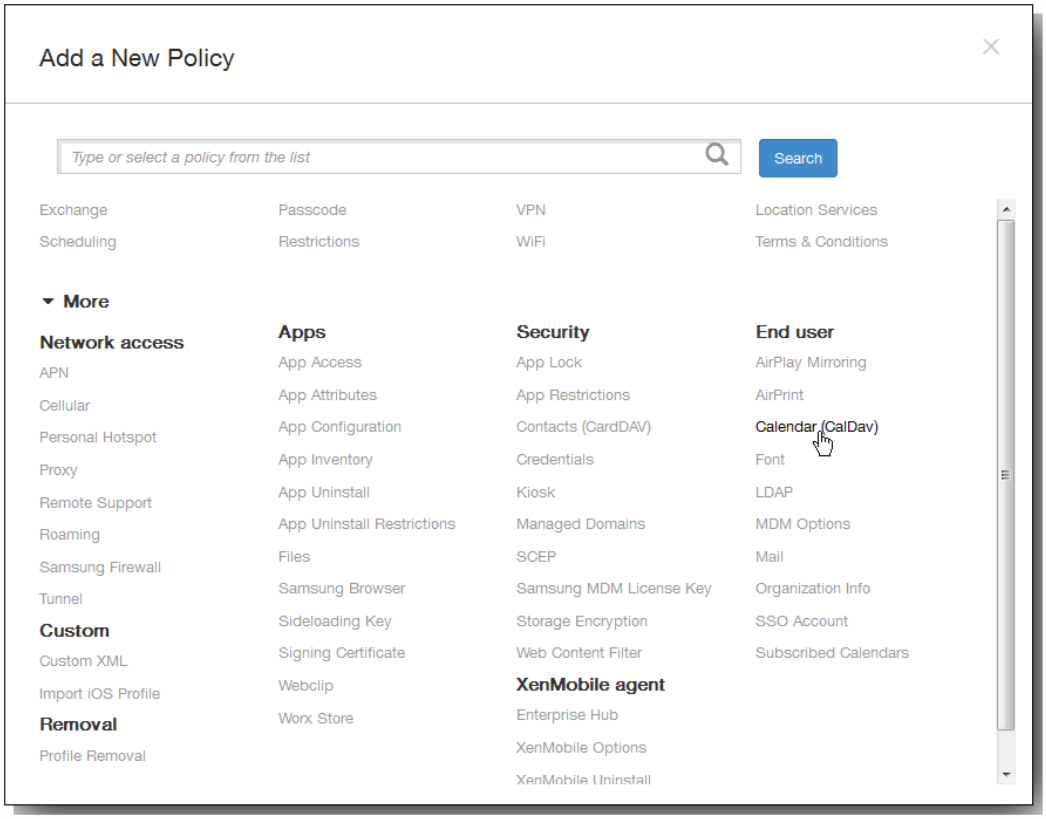
May 05, 2016

Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen eines iOS-Kalenderkontos (CalDAV) zu iOS-Geräten einrichten, damit die Benutzer Kalendereinträge mit einem beliebigen Server, der CalDAV unterstützt, synchronisieren können.

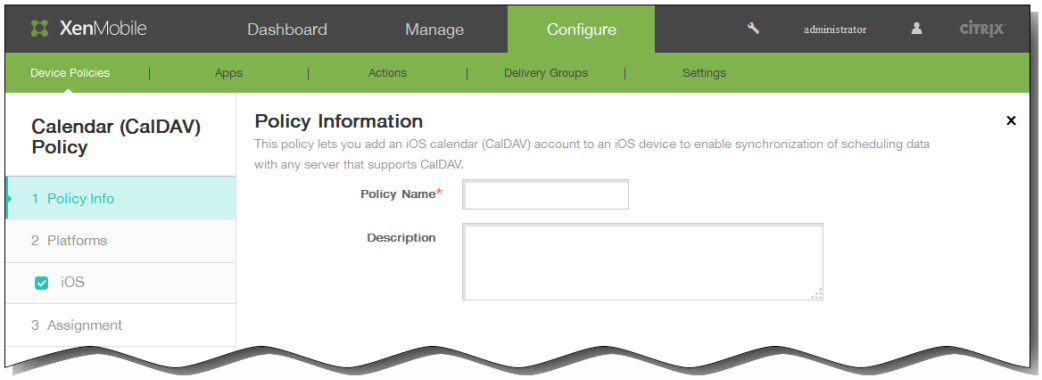
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



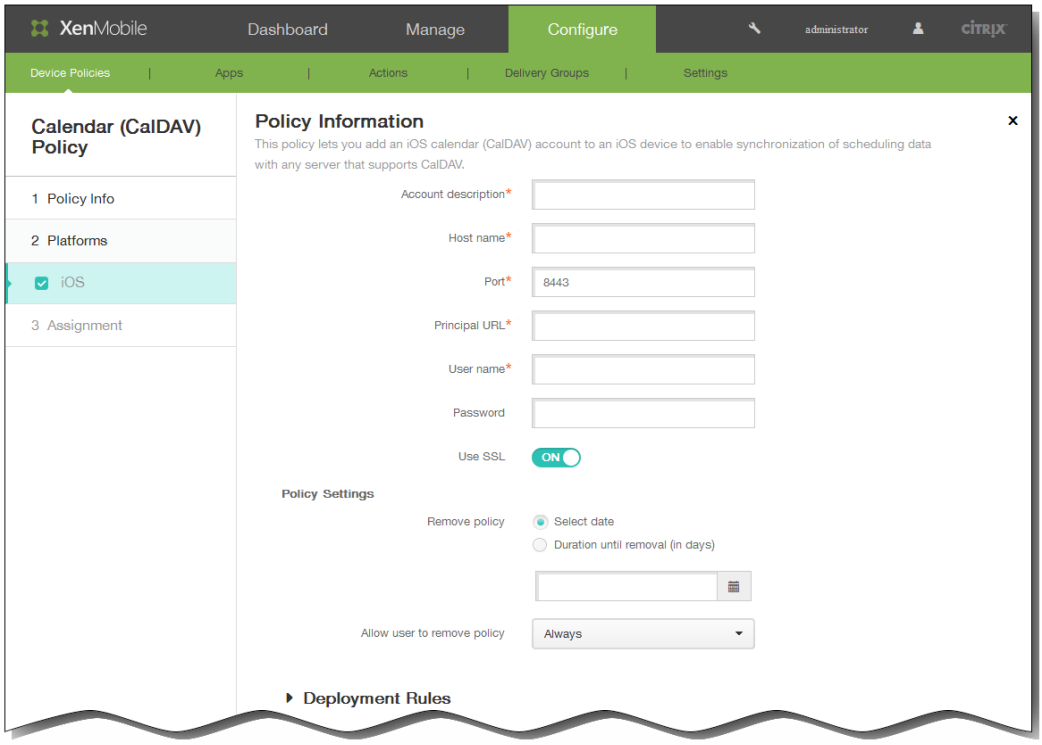
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter End user auf Calendar (CalDAV). Die Seite Calendar (CalDAV) Policy wird angezeigt.



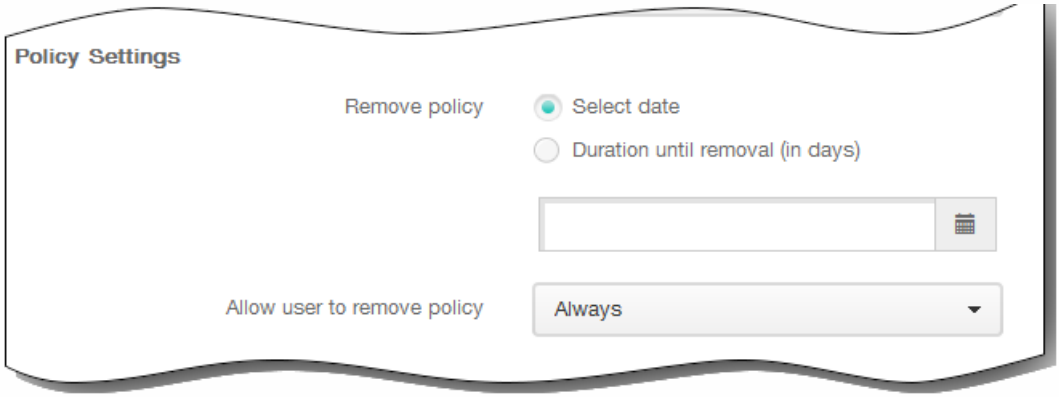
4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite iOS Platform Information wird angezeigt.



6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:
   1. Account description: Geben Sie ein Kontobeschreibung ein. Diese Angabe ist erforderlich.
   2. Host name: Geben Sie die Adresse des CalDAV-Servers ein. Diese Angabe ist erforderlich.
   3. Port: Geben Sie den Port für die Verbindung mit dem CalDAV-Server ein. Diese Angabe ist erforderlich. Der Standardwert ist 8443.
   4. Principal URL: Geben Sie die Basis-URL des Kalenders des Benutzers ein.
   5. User name: Geben Sie den Anmeldenamen des Benutzers ein. Diese Angabe ist erforderlich.

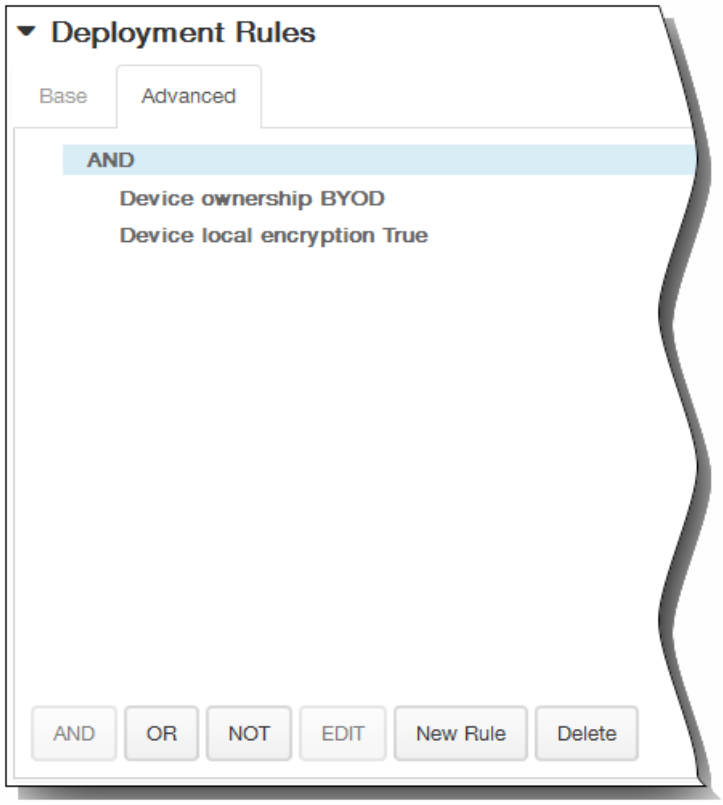
6. Password: Geben Sie ein optionales Benutzerkennwort ein.
7. Use SSL: Wählen Sie aus, ob für die Verbindung mit dem CalDAV-Server Secure Socket Layer verwendet werden soll. Der Standardwert ist On.

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.



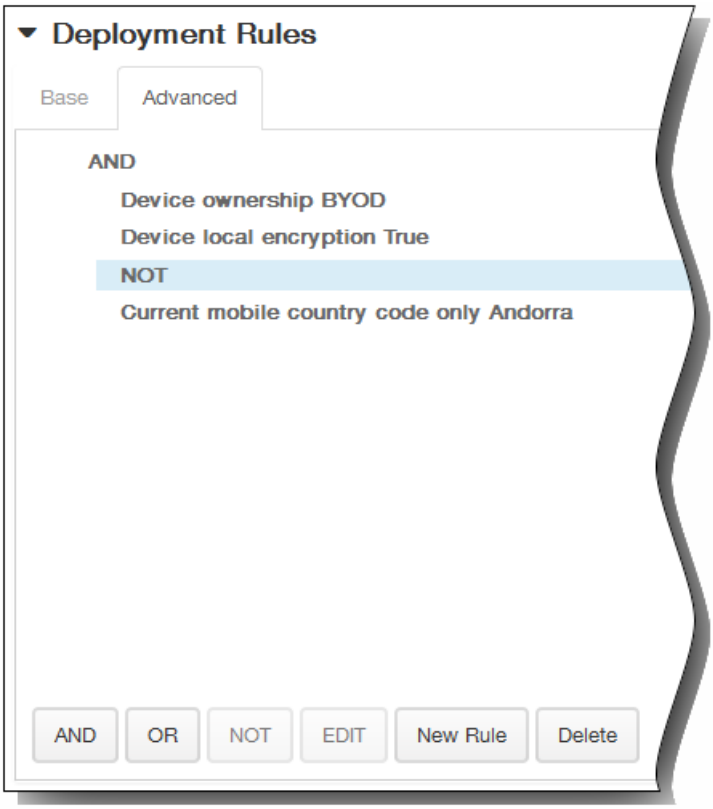
11. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

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.

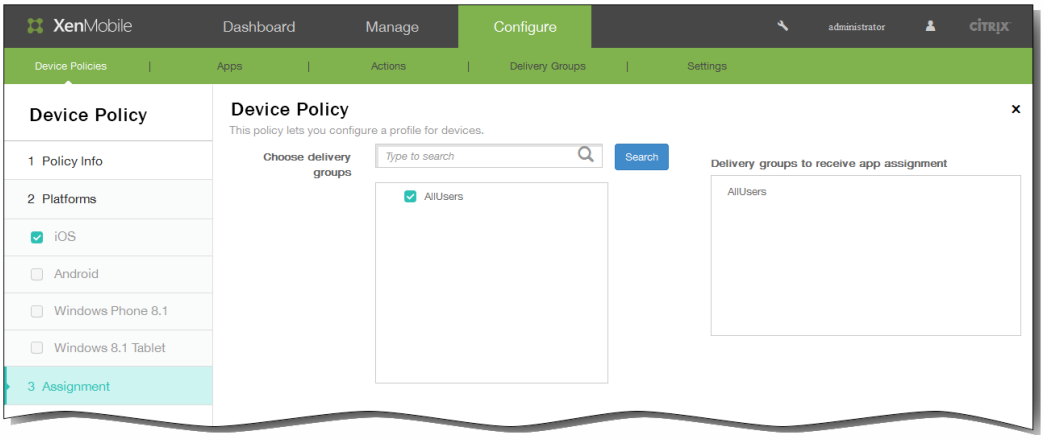


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



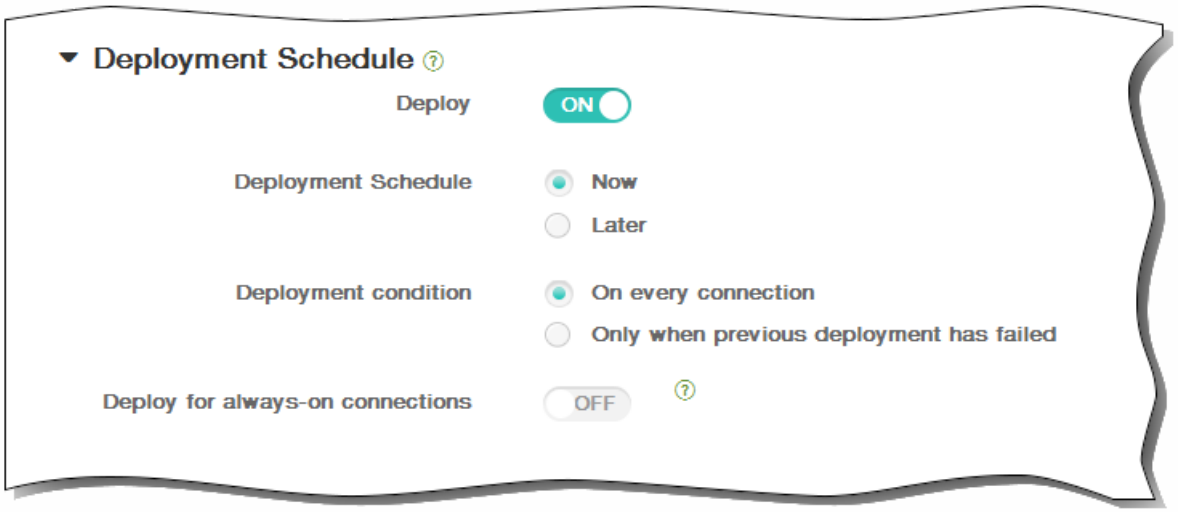
12. Klicken Sie auf Next. Die Seite Calendar (CalDAV) Policy für die Kalenderrichtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese 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.



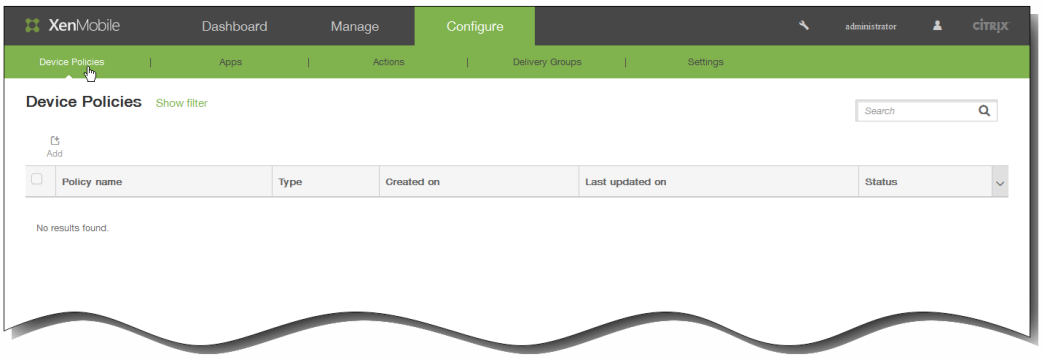
15. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Kontakterichtlinie (CardDAV) für iOS-Geräte hinzu

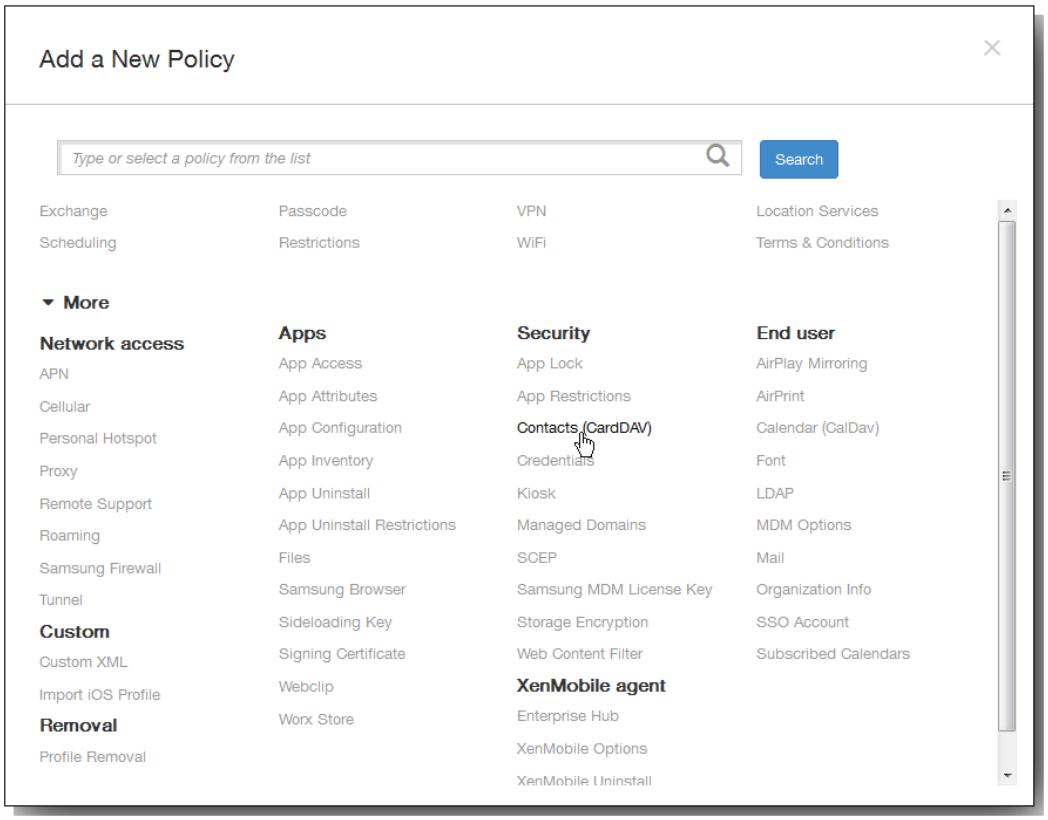
May 05, 2016

Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen eines iOS-Kontaktekontos (CardDAV) zu iOS-Geräten einrichten, damit die Benutzer Kontaktdaten mit einem beliebigen Server, der CardDAV unterstützt, synchronisieren können.

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

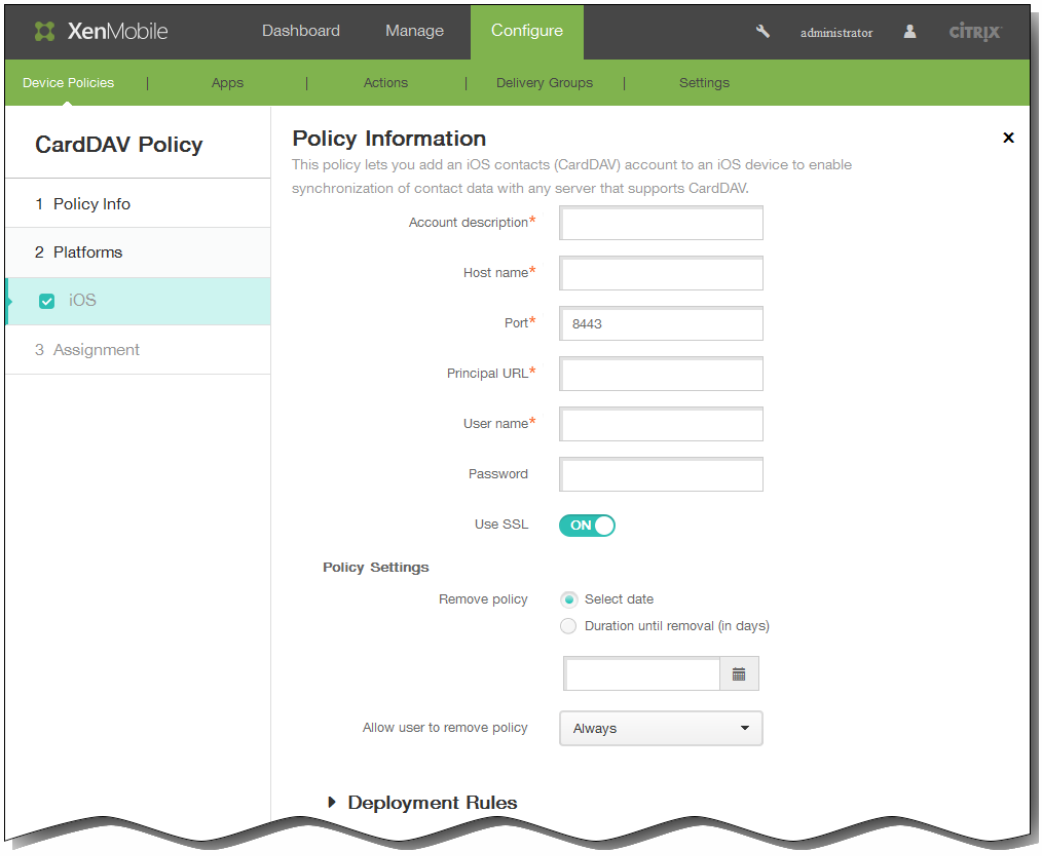


2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



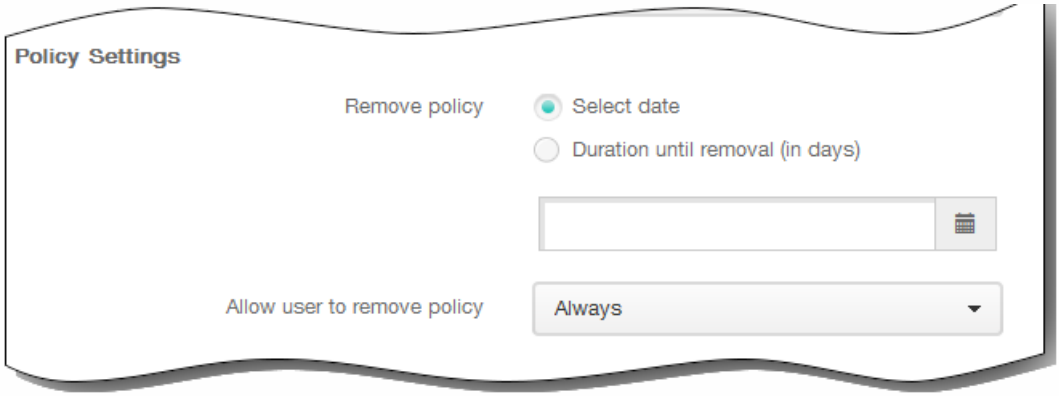
3. Klicken Sie auf More und dann unter Security auf Contacts CardDAV. Die Seite CardDAV Policy wird angezeigt.

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.



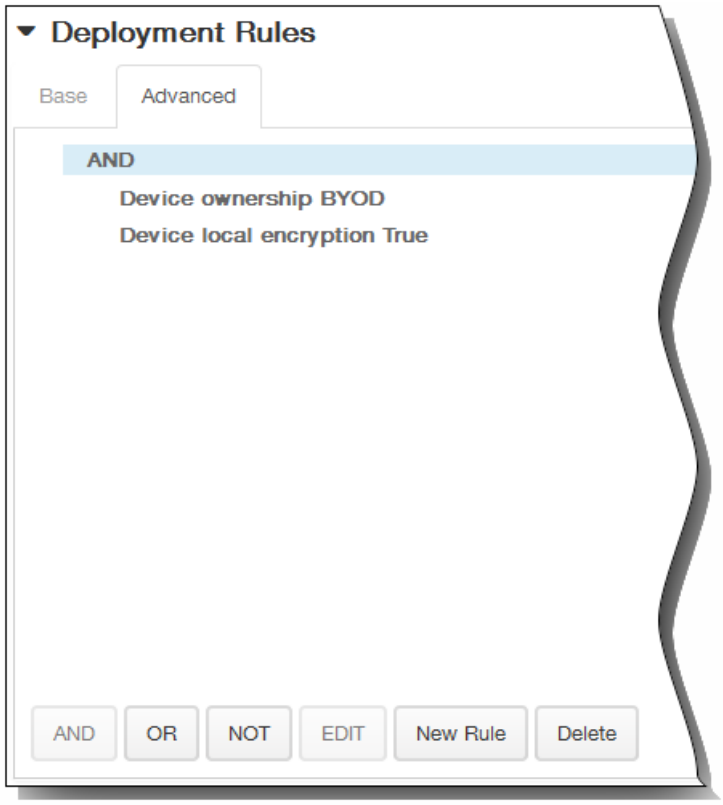
6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:
   1. Account description: Geben Sie eine Kontobeschreibung ein. Diese Angabe ist erforderlich.
   2. Host name: Geben Sie die Adresse des CardDAV-Servers ein. Diese Angabe ist erforderlich.
   3. Port: Geben Sie den Port für die Verbindung mit dem CardDAV-Server ein. Diese Angabe ist erforderlich. Der Standardwert ist 8443.
   4. Principal URL: Geben Sie die Basis-URL des Kalenders des Benutzers ein.
   5. User name: Geben Sie den Anmeldenamen des Benutzers ein. Diese Angabe ist erforderlich.
   6. Password: Geben Sie ein optionales Benutzerkennwort ein.
   7. Use SSL: Wählen Sie aus, ob für die Verbindung mit dem CardDAV-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist ON.
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.

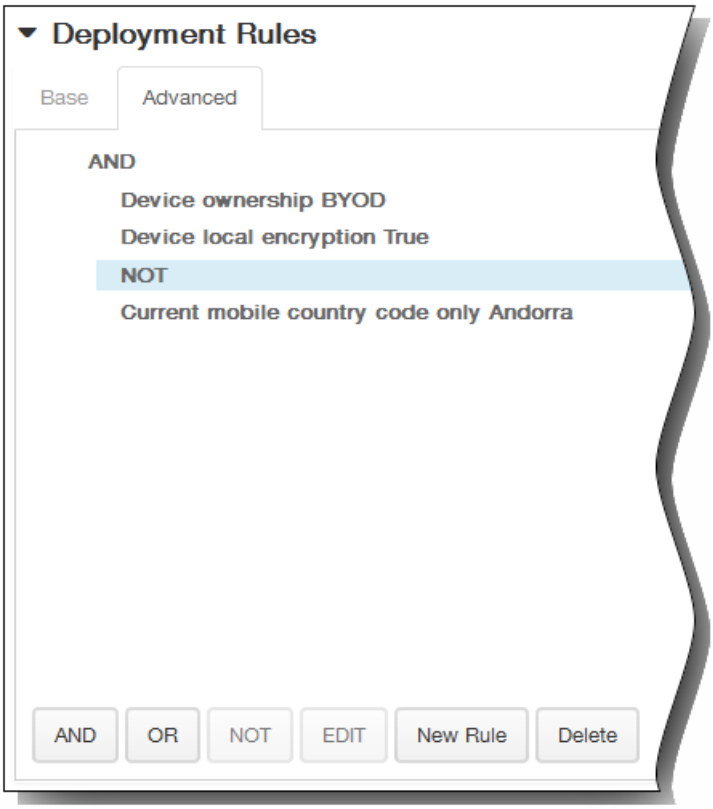
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie noch einmal 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.



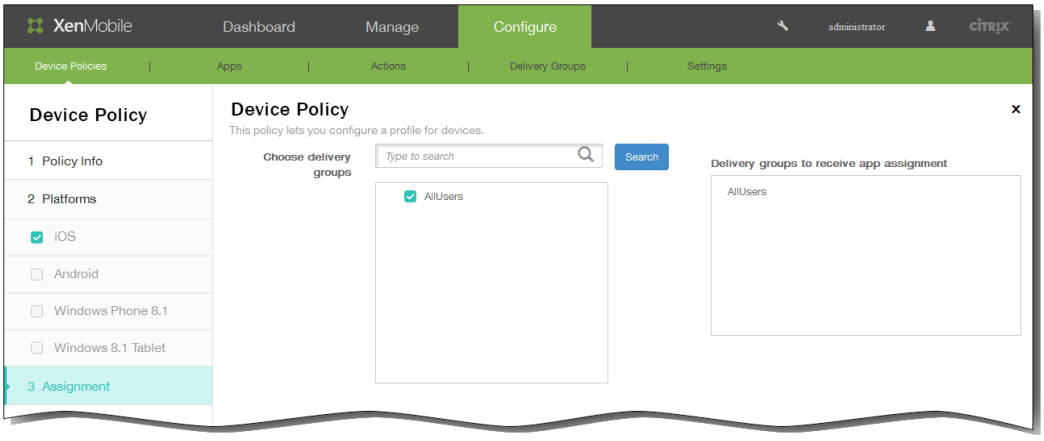
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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 noch einmal 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.



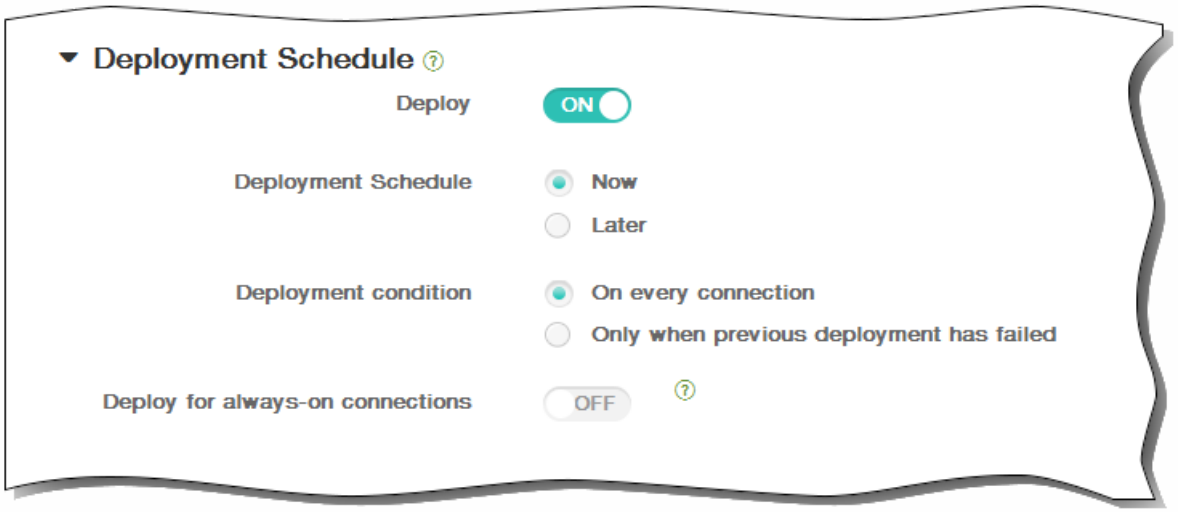
12. Klicken Sie auf Next. Die Seite Assignment für die CardDAV-Richtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.

Anmeldeinformationsrichtlinien für Geräte

May 05, 2016

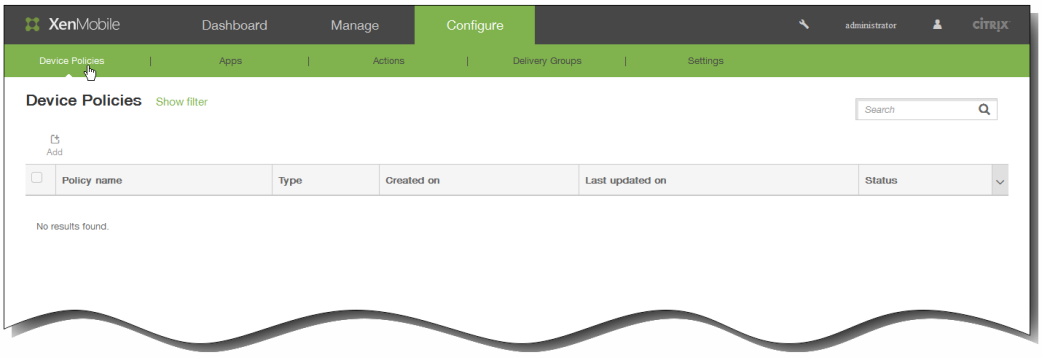
Sie können in XenMobile Anmeldeinformationsrichtlinien erstellen, um eine in die Public Key-Infrastruktur in XenMobile (z. B. PKI-Entität, Schlüsselspeicher, Anmeldeinformationsanbieter oder Serverzertifikat) integrierte Authentifizierung zu ermöglichen. Weitere Informationen über Anmeldeinformationen finden Sie unter Zertifikate in XenMobile.

Sie können Anmeldeinformationsrichtlinien für iOS- und Android-Geräte und für Windows 8.1-Tablets erstellen. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Abschnitt beschrieben.

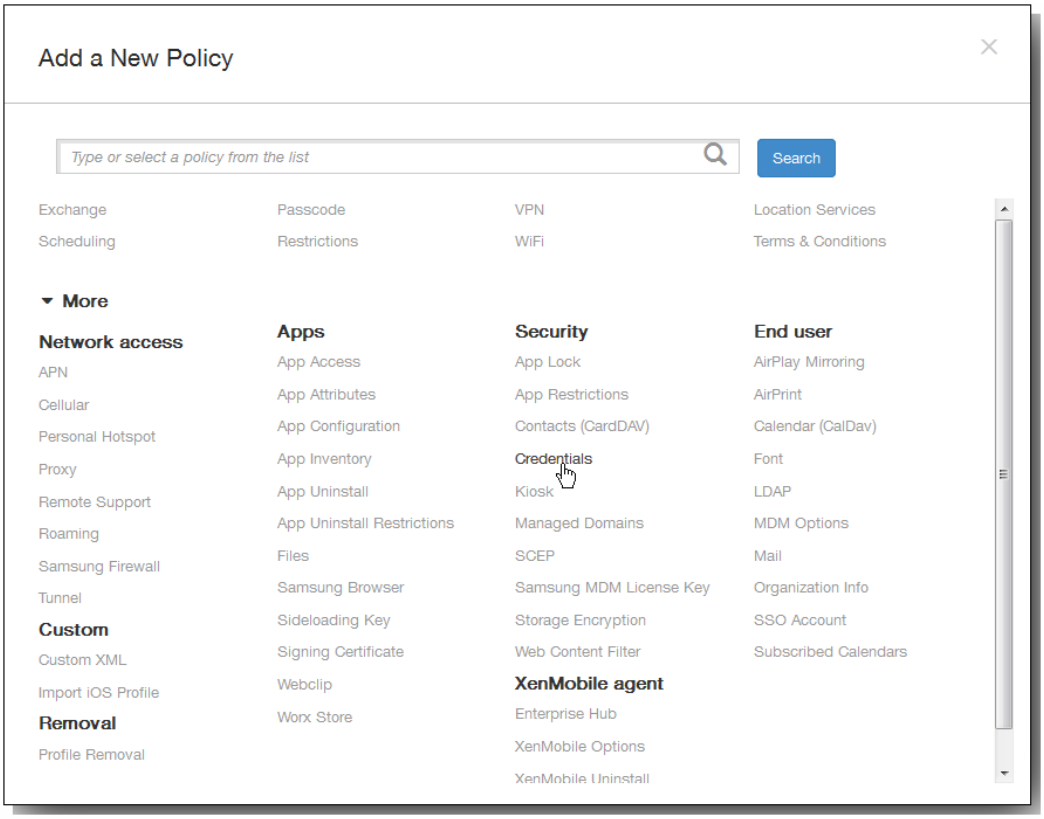
Sie benötigen zum Erstellen der Richtlinie die folgenden Informationen:

- Anmeldeinformationen für jede Plattform sowie jegliche Zertifikate und Kennwörter.

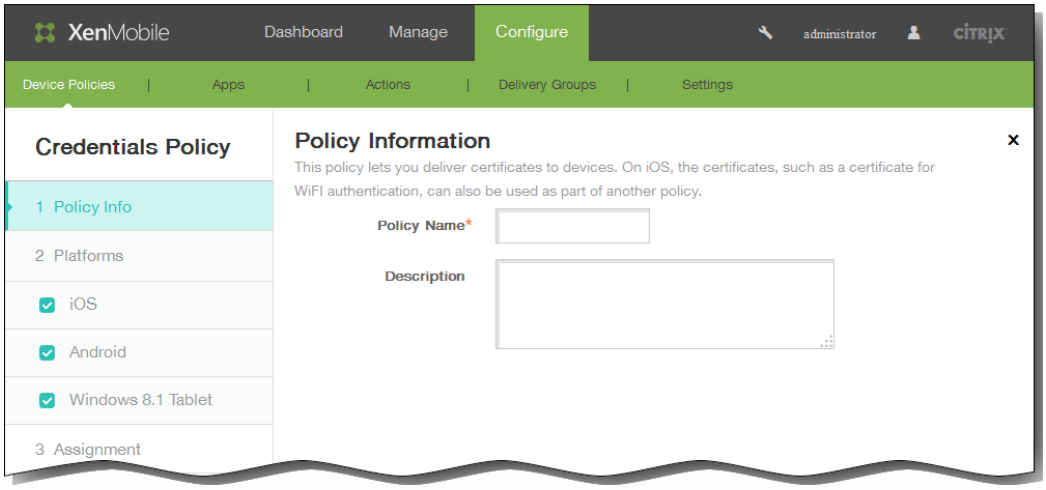
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



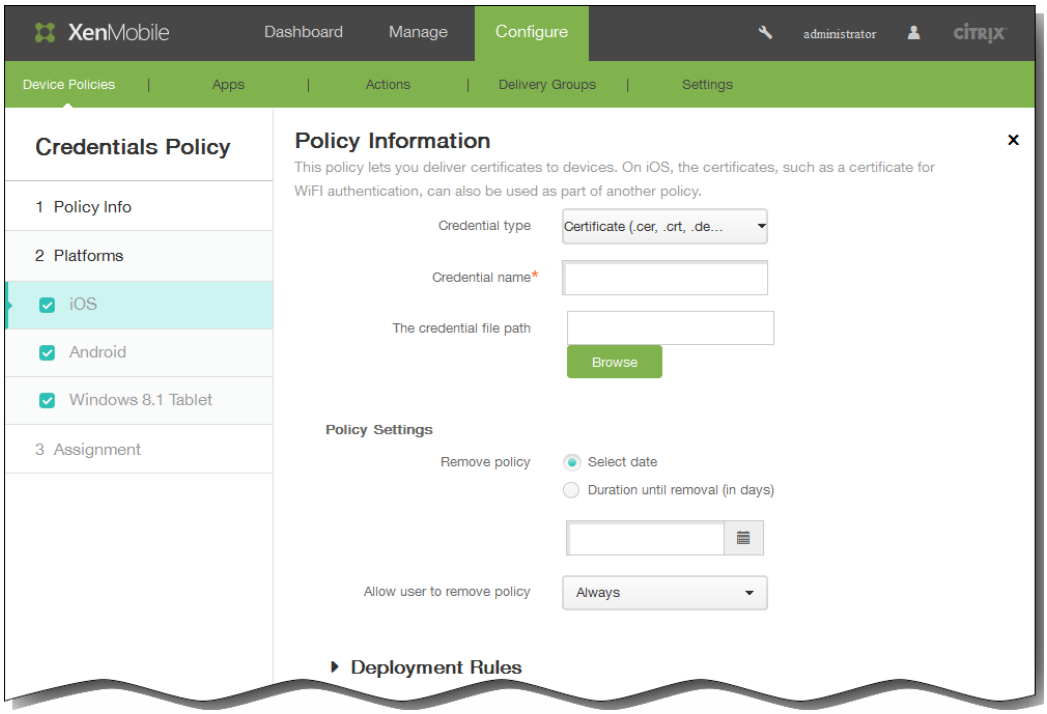
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add New Policy wird angezeigt.



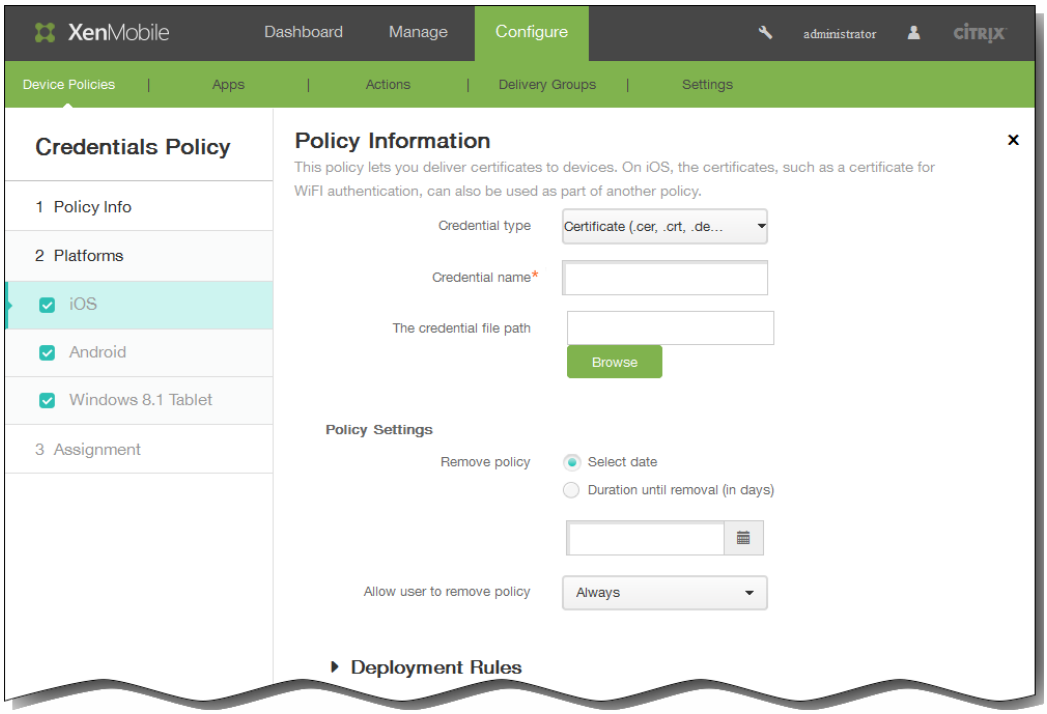
3. Klicken Sie auf More und dann unter Security auf Credentials. Die Seite Credentials Policy wird angezeigt.



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 iOS-Plattform wird als erstes angezeigt.



6. Wählen Sie unter Platforms die gewünschten Plattformen aus.
   - Bei Auswahl von iOS konfigurieren Sie die folgenden Einstellungen:



Credential type: Klicken Sie in der Liste auf den Typ der Anmeldeinformationen, die für die Richtlinie verwendet werden soll.

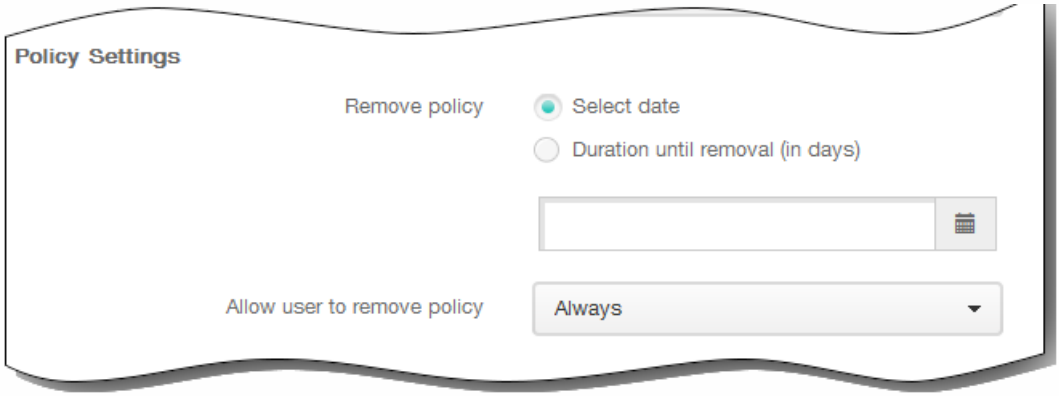
Geben Sie für die ausgewählten Anmeldeinformationen die folgenden Informationen ein:

- Zertifikat

- Credential Name: Geben Sie einen Namen für die Anmeldeinformationen ein.
- The credential file path: Klicken Sie auf Browse und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.

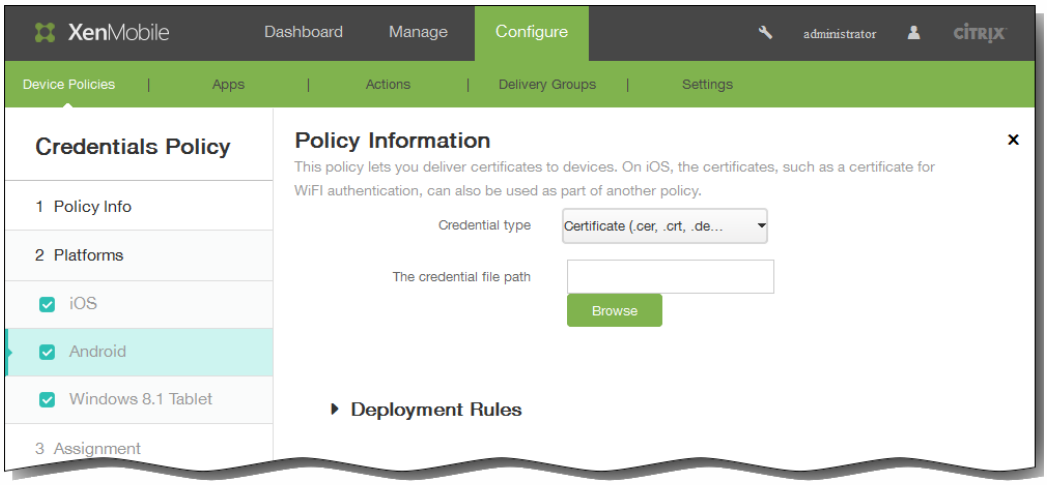
- **Schlüsselspeicher**
  - Credential Name: Geben Sie einen Namen für die Anmeldeinformationen ein.
  - The credential file path: Klicken Sie auf Browse und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
  - Password: Geben Sie das Schlüsselspeicherkennwort für die Anmeldeinformationen ein.
- **Serverzertifikat**
  - Server certificate: Klicken Sie in der Liste auf das Zertifikat, das verwendet werden soll.
- **Anmeldeinformationsanbieter**
  - Credential Provider: Klicken Sie in der Liste auf den Namen des Anmeldeinformationsanbieters.

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.

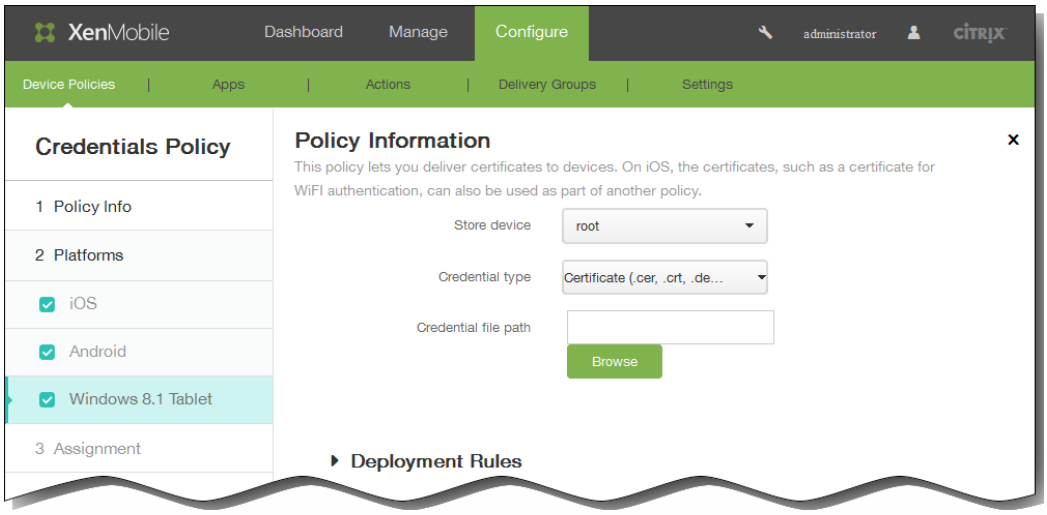
- Bei Auswahl von Android konfigurieren Sie die folgenden Einstellungen:



Credential type: Klicken Sie in der Liste auf den Typ der Anmeldeinformationen, die für die Richtlinie verwendet werden soll.

Geben Sie für die ausgewählten Anmeldeinformationen die folgenden Informationen ein:

- **Zertifikat**
  - Credential Name: Geben Sie einen Namen für die Anmeldeinformationen ein.
  - The credential file path: Klicken Sie auf Browse und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
- **Schlüsselspeicher**
  - Credential Name: Geben Sie einen Namen für die Anmeldeinformationen ein.
  - The credential file path: Klicken Sie auf Browse und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
  - Password: Geben Sie das Schlüsselspeicherkennwort für die Anmeldeinformationen ein.
- **Serverzertifikat**
  - Server certificate: Klicken Sie in der Liste auf das Zertifikat, das verwendet werden soll.
- **Anmeldeinformationsanbieter**
  - Credential Provider: Klicken Sie in der Liste auf den Namen des Anmeldeinformationsanbieters.
- Bei Auswahl von Windows 8.1 Tablet konfigurieren Sie die folgenden Einstellungen:



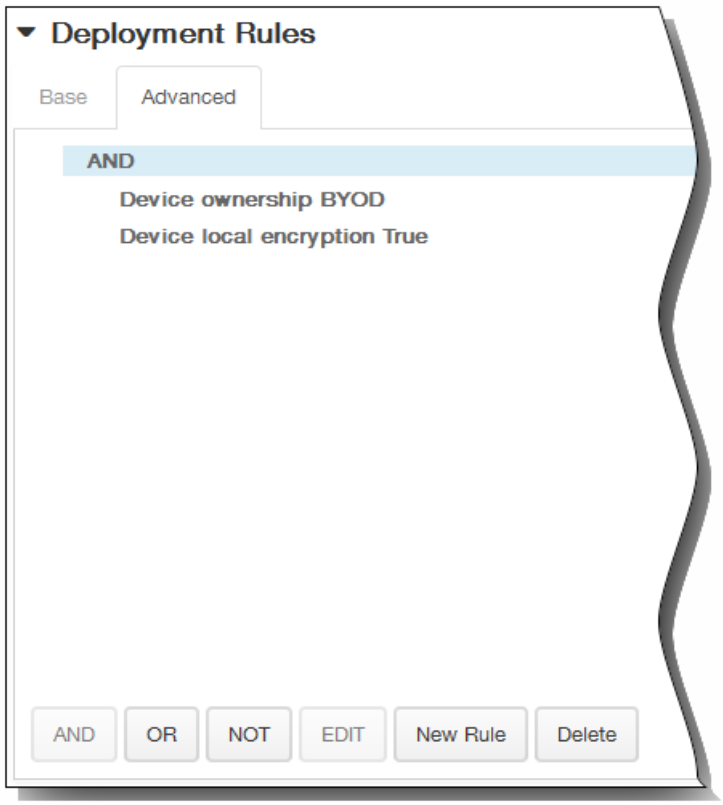
Store device: Klicken Sie in der Liste auf root, My oder CA, um den Speicherort des Zertifikatspeichers für die Anmeldeinformationen anzugeben. Bei Auswahl von My wird das Zertifikat in den Zertifikatspeichern der Benutzer gespeichert.

Credential type: Für Windows 8.1-Tablets steht nur der Typ "Certificate" zur Verfügung.

The credential file path: Klicken Sie auf Browse und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.

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

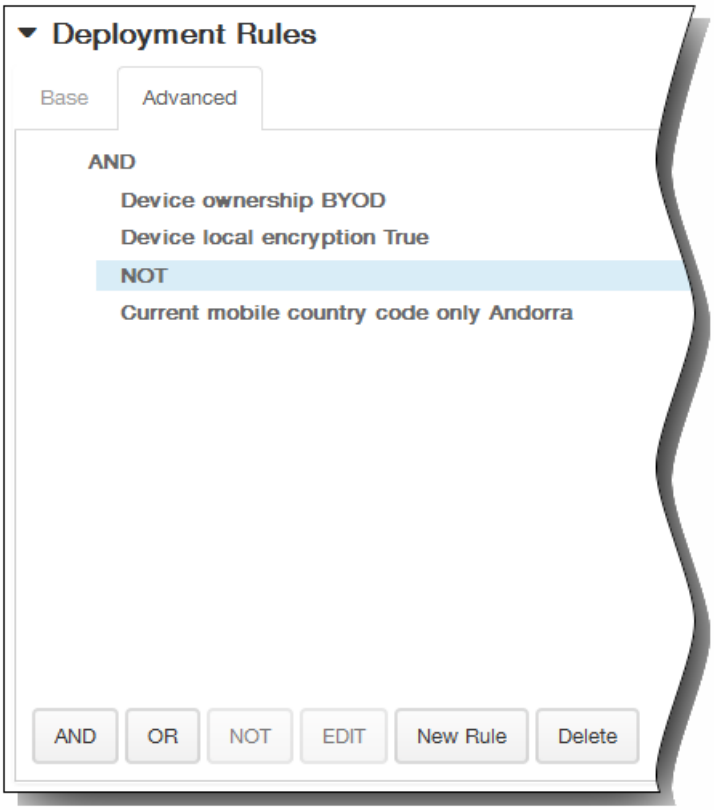
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



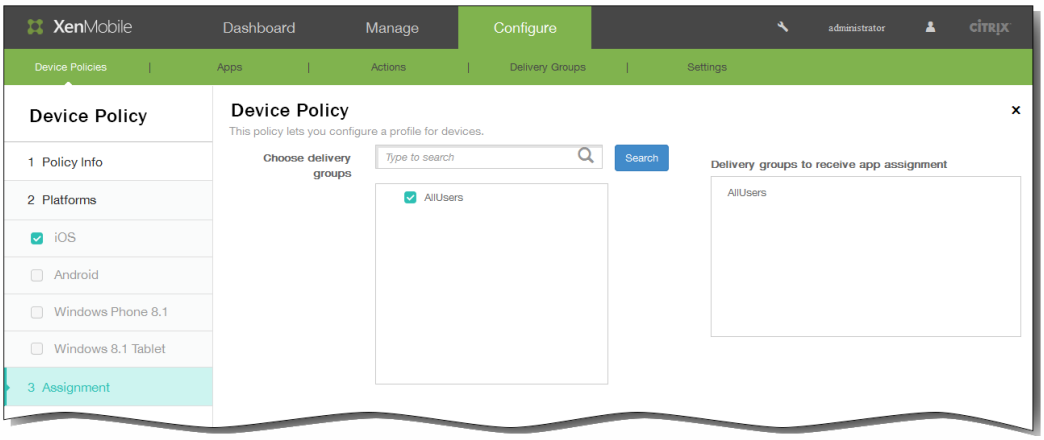
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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.



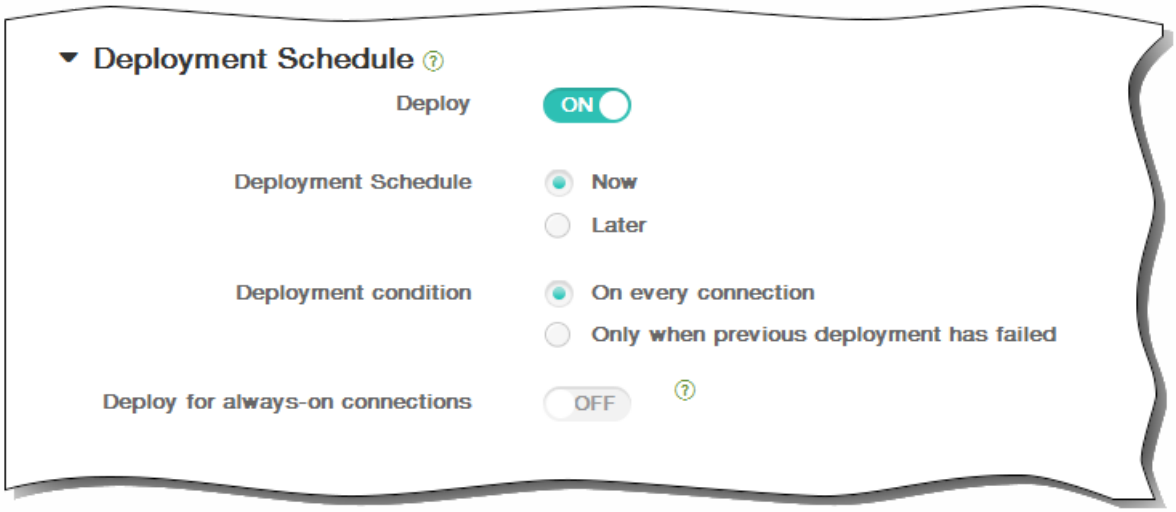
8. Klicken Sie auf Next. Die Seite Assignment für die Anmeldeinformationsrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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 Kioskrichtlinie für Samsung SAFE-Geräte hinzu

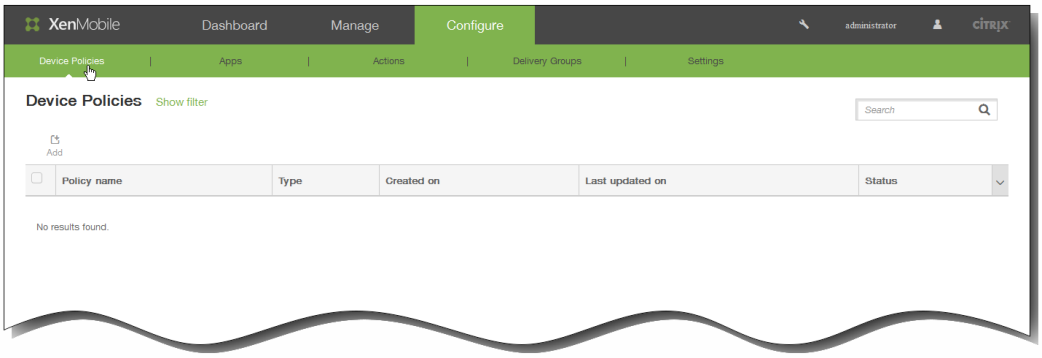
May 05, 2016

Mit einer Kioskrichtlinie können Sie in XenMobile festlegen, dass nur bestimmte Apps auf Samsung SAFE-Geräten verwendet werden können. Diese Richtlinie ist für Unternehmensgeräte nützlich, die nur für bestimmte App-Typen oder -Klassen vorgesehen sind. Mit der Richtlinie können Sie auch benutzerdefinierte Bilder für Home- und Sperrbildschirm auswählen, die angezeigt werden, wenn sich ein Gerät im Kioskmodus befindet.

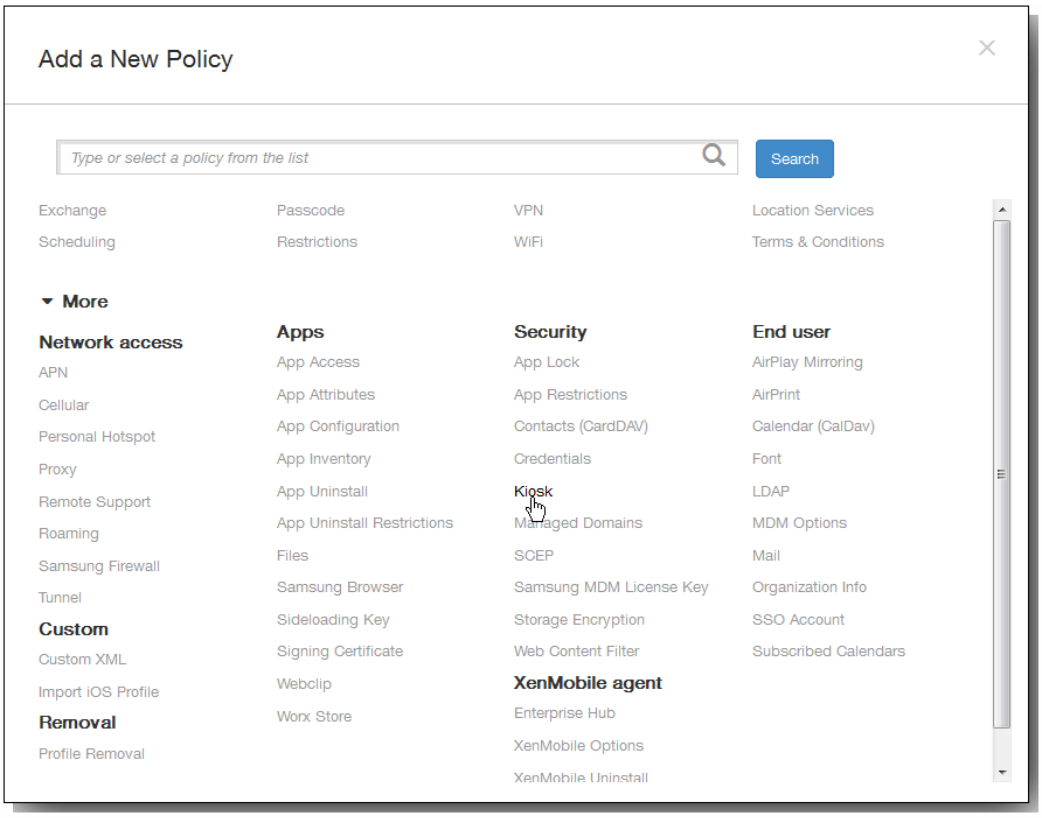
Hinweis:

- Alle Apps, die Sie für den Kioskmodus festlegen, müssen bereits auf den Benutzergeräten installiert sein.
- Einige Optionen gelten nur für Samsung Mobile Device Management API 4.0 und höher.

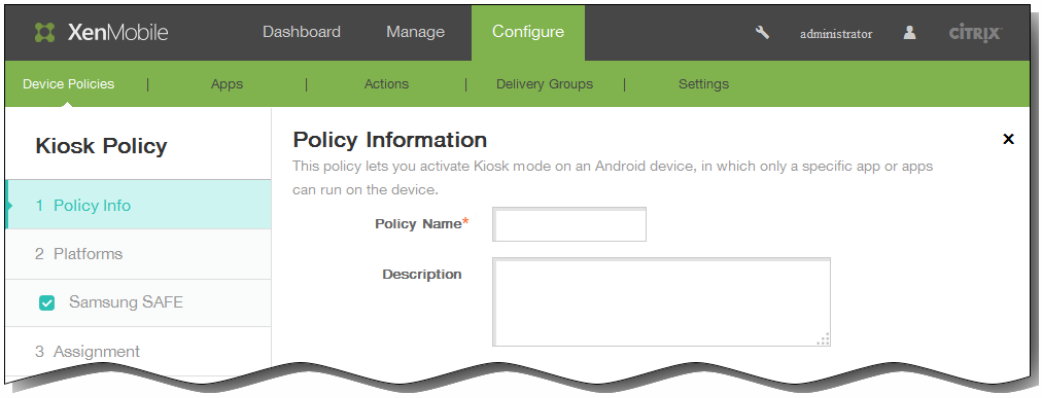
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



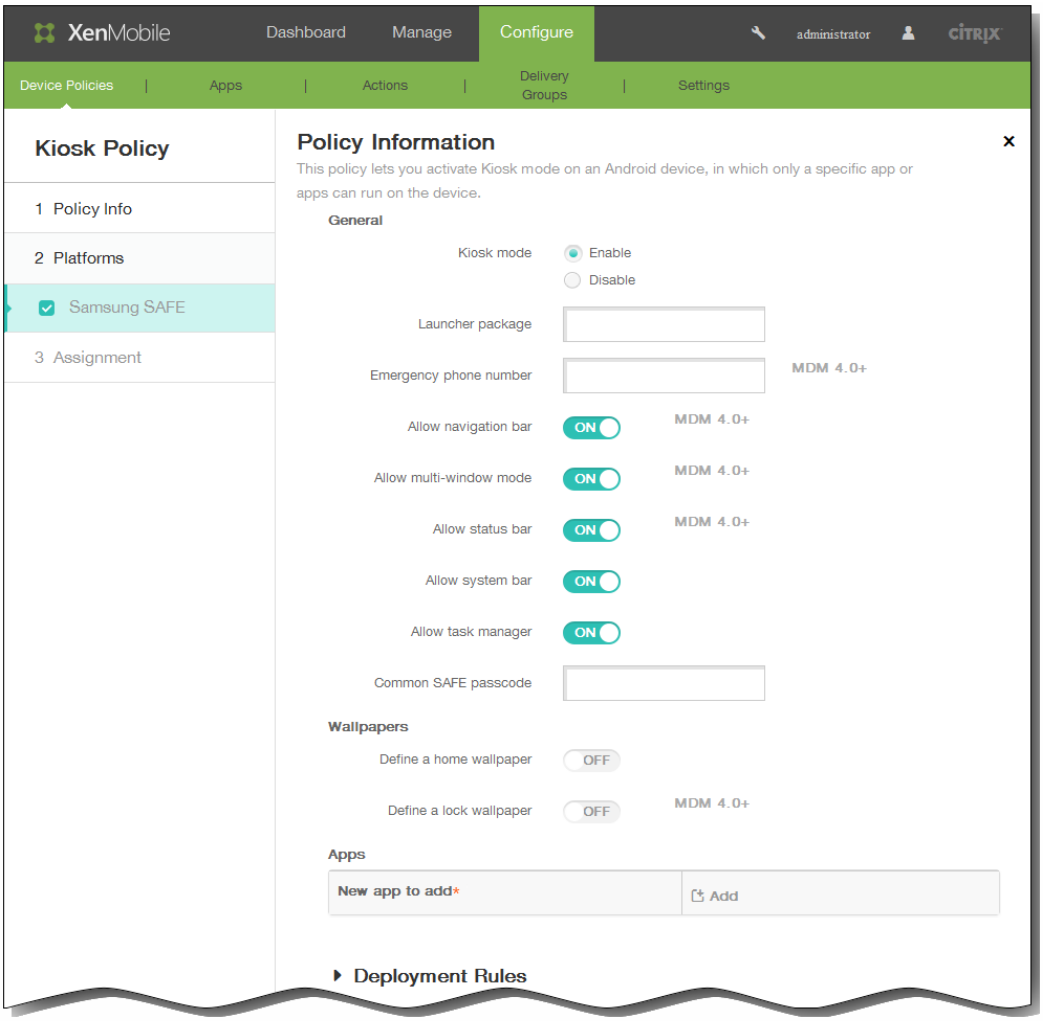
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter Security auf Kiosk. Die Seite Kiosk Policy wird angezeigt.



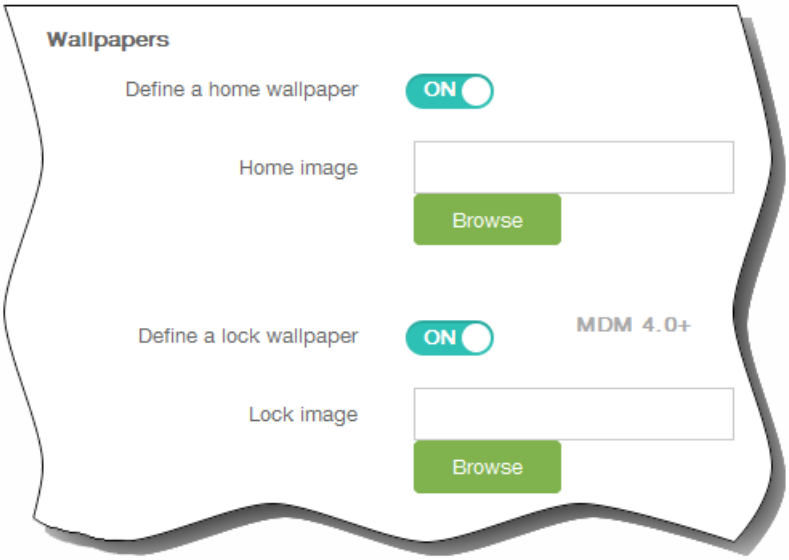
4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Samsung SAFE Platform wird angezeigt.



6. Geben Sie auf der Seite Samsung SAFE Platform die folgenden Informationen ein:
    1. Kiosk mode: Klicken Sie auf Enable oder Disable. Der Standardwert ist Enable. Wenn Sie auf Disable klicken, werden die nachfolgend aufgeführten Optionen ausgeblendet.
    2. Launcher package: Citrix empfiehlt, dieses Feld leer zu lassen, es sei denn, Sie haben einen internen Launcher entwickelt, mit dem Benutzer Kiosk-Apps öffnen können. Bei Verwendung eines internen Launchers geben Sie den vollständigen Namen des Launcher-Anwendungspakets ein.
    3. Emergency phone number: Geben Sie optional eine Telefonnummer ein. Über diese Nummer kann der etwaige Finder eines verlorenen Geräts sich an Ihr Unternehmen wenden. Gilt nur für Samsung Mobile Device Management API 4.0 und höher.
    4. Allow navigation bar: Wählen Sie aus, ob Benutzer im Kioskmodus die Navigationsleiste anzeigen und verwenden können sollen. Gilt nur für MDM 4.0 und höher.
    5. Allow multi-window mode: Wählen Sie aus, ob Benutzer im Kioskmodus mehrere Fenster verwenden können sollen. Gilt nur für MDM 4.0 und höher.
    6. Allow status bar: Wählen Sie aus, ob Benutzer im Kioskmodus die Statusleiste anzeigen können sollen. Gilt nur für MDM 4.0 und höher.
    7. Allow system bar: Wählen Sie aus, ob Benutzer im Kioskmodus die Systemleiste anzeigen können sollen.
    8. Allow task manager: Wählen Sie aus, ob Benutzer im Kioskmodus den Task-Manager anzeigen und verwenden können sollen.
    9. Common SAFE passcode: Wenn Sie eine allgemeine Passcoderichtlinie für alle Samsung SAFE Geräte festgelegt haben,

geben Sie den optionalen Passcode in dieses Feld ein.

10. Define a home wallpaper: Wählen Sie aus, ob für den Homebildschirm im Kioskmodus ein benutzerdefiniertes Bild verwendet werden soll. Der Standardwert ist OFF.
11. Define a lock wallpaper: Wählen Sie aus, ob für den Sperrbildschirm im Kioskmodus ein benutzerdefiniertes Bild verwendet werden soll. Der Standardwert ist OFF. Gilt nur für MDM 4.0 und höher. Wenn Sie eine der beiden Optionen aktivieren, wird ein Feld zur Auswahl des benutzerdefinierten Bilds angezeigt. Klicken Sie auf Browse und navigieren Sie zu dem Bild.



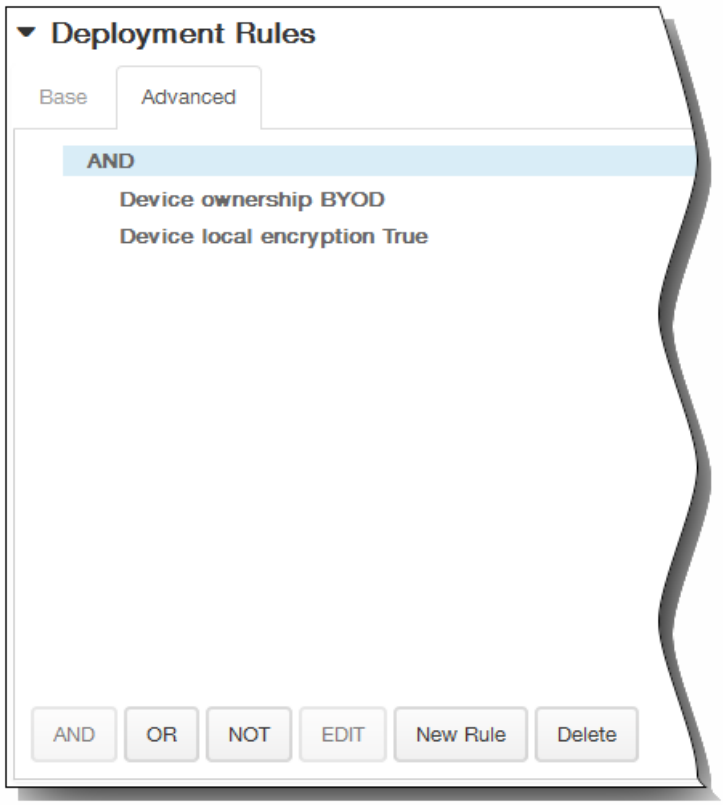
12. Apps: Klicken Sie auf Add und führen Sie die folgenden Schritte aus:
    1. New app to add: Geben Sie den vollständigen Namen der App ein. Beispiel: Bei Eingabe von "com.android.calendar" können Benutzer die Android-Kalender-App verwenden.
    2. Klicken Sie auf Add, um die App hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
    3. Wiederholen Sie die Schritte i und ii für jede App, die Sie 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.

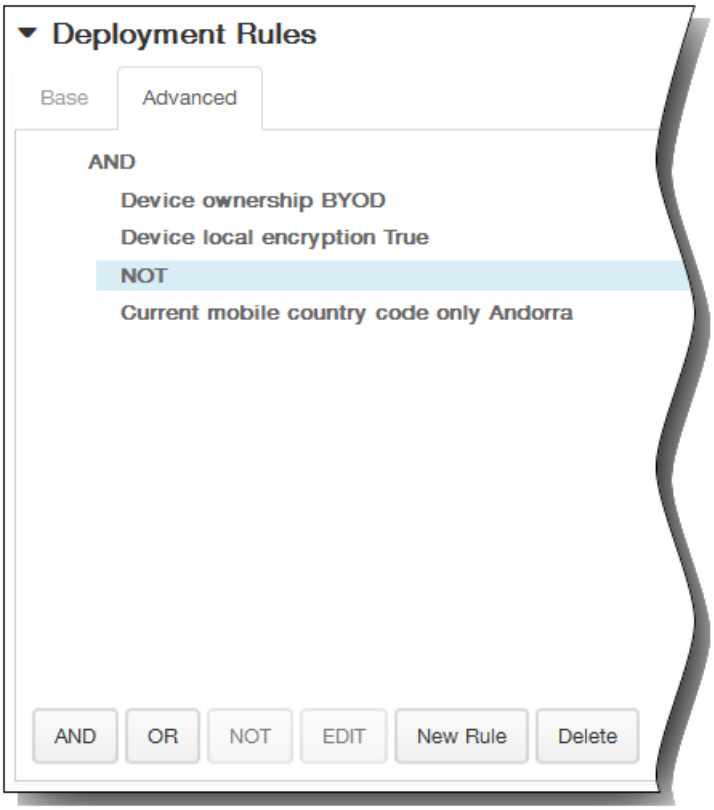
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



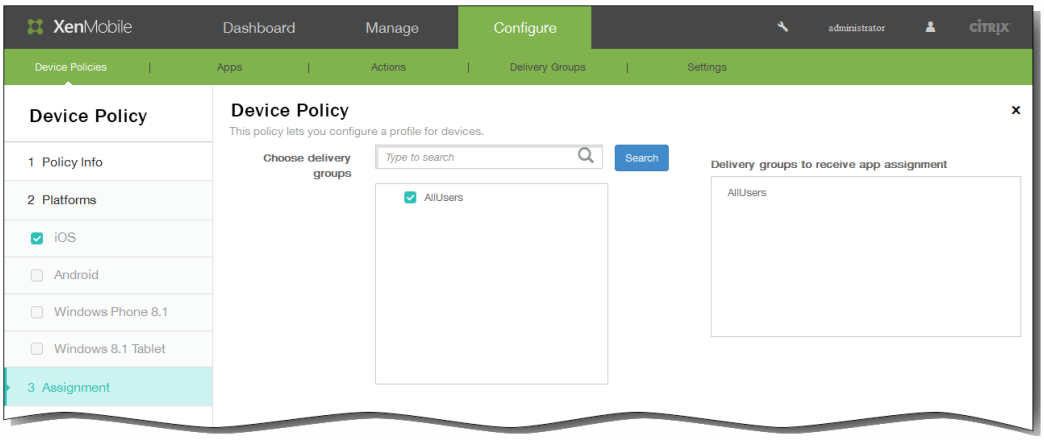
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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 noch einmal 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.



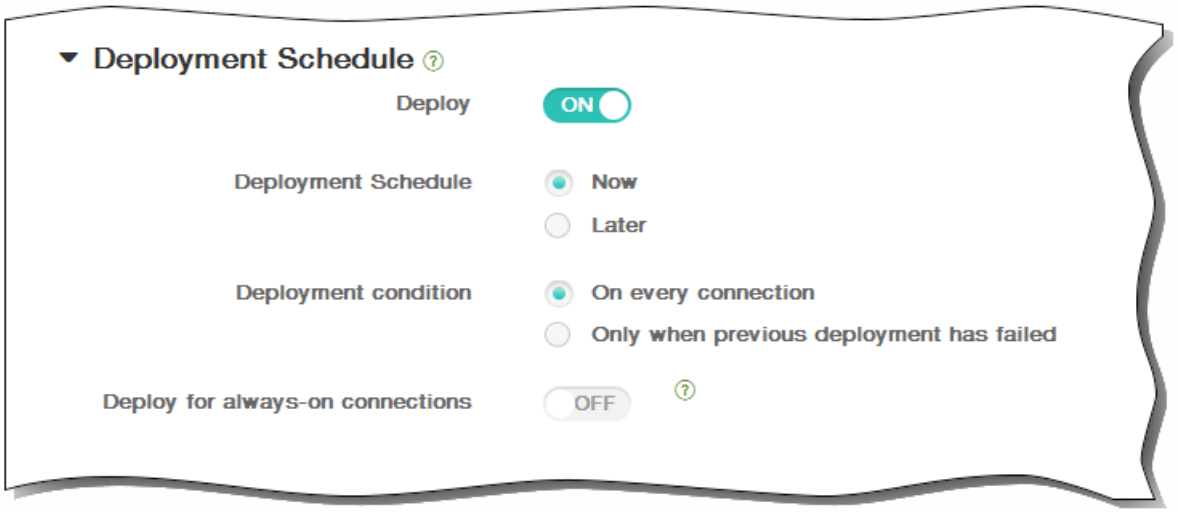
8. Klicken Sie auf Next. Die Seite Assignment für die Kioskrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen 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.

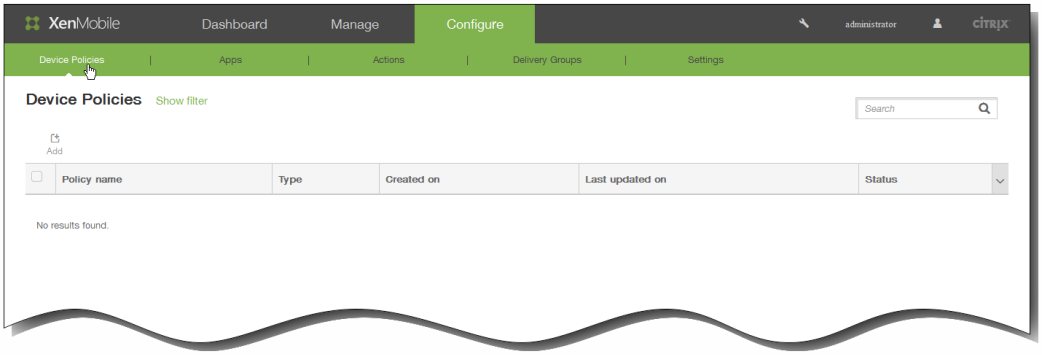
So fügen Sie eine Schriftartrichtlinie für iOS-Geräte hinzu

May 05, 2016

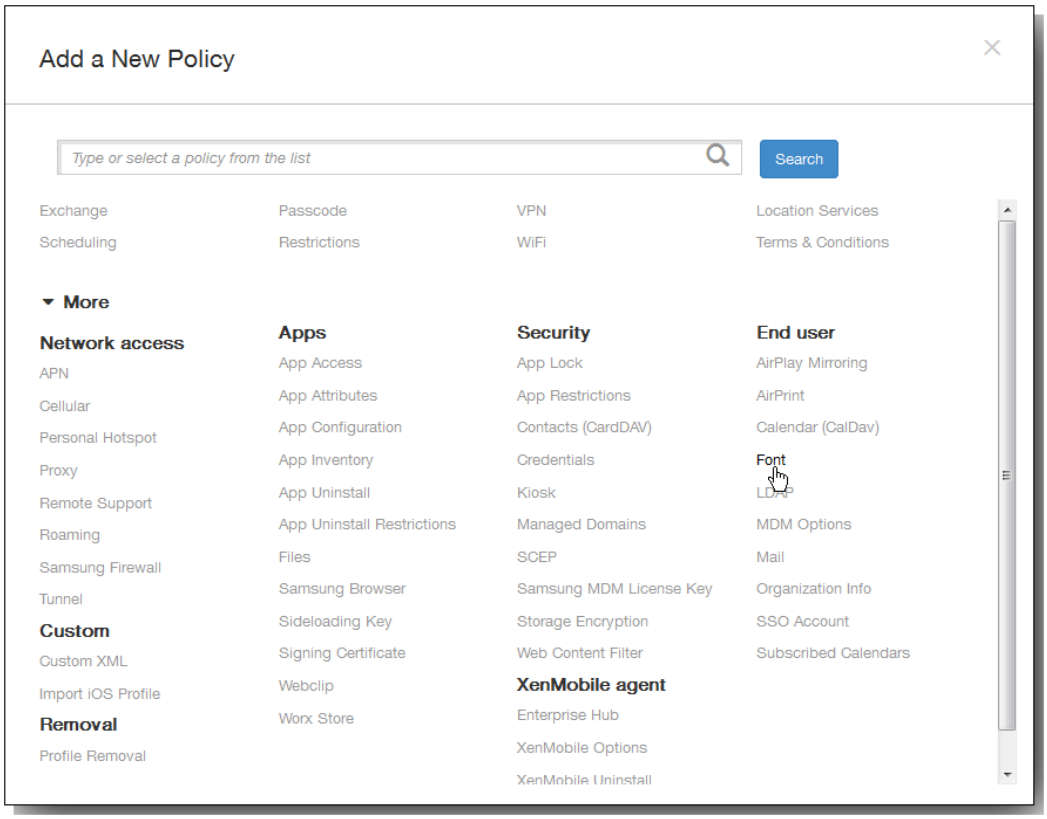
Sie können in XenMobile eine Geräterichtlinie einrichten, mit der zusätzliche Schriftarten auf iOS-Geräten hinzugefügt werden. Schriftarten müssen im Format TrueType (.ttf) oder OpenType (.oft) vorliegen. Schriftsammlungen (.ttc oder .otc) werden nicht unterstützt.

Hinweis: Die Richtlinie gilt nur für iOS 7.0 und höher.

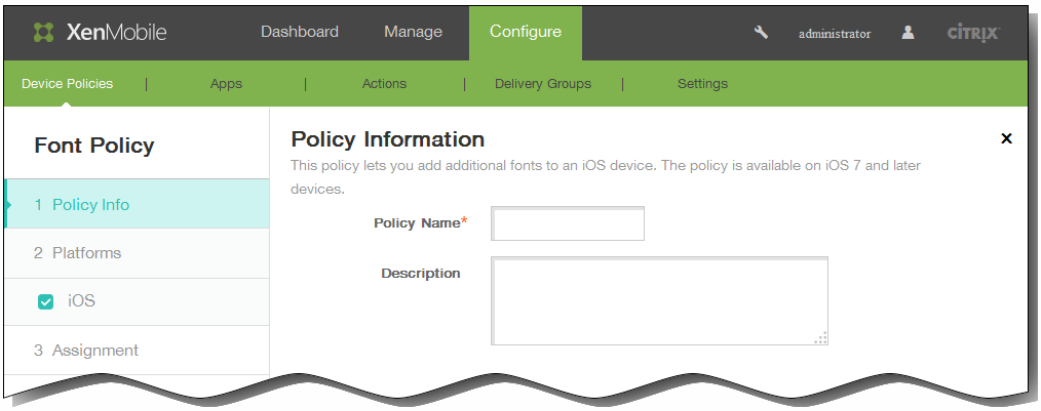
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



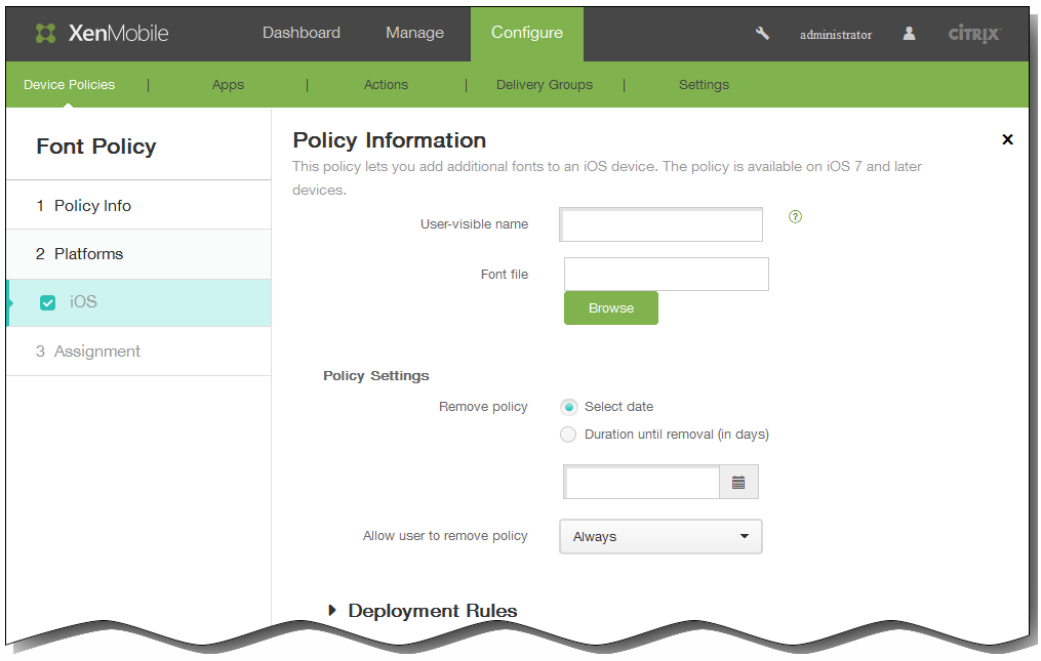
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter End user auf Font. Die Seite Font Policy wird angezeigt.

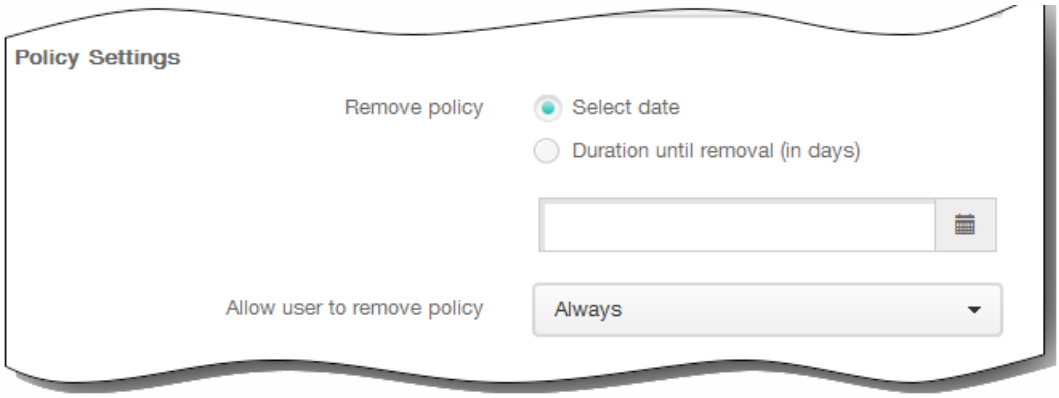


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite iOS Platform Information wird angezeigt.



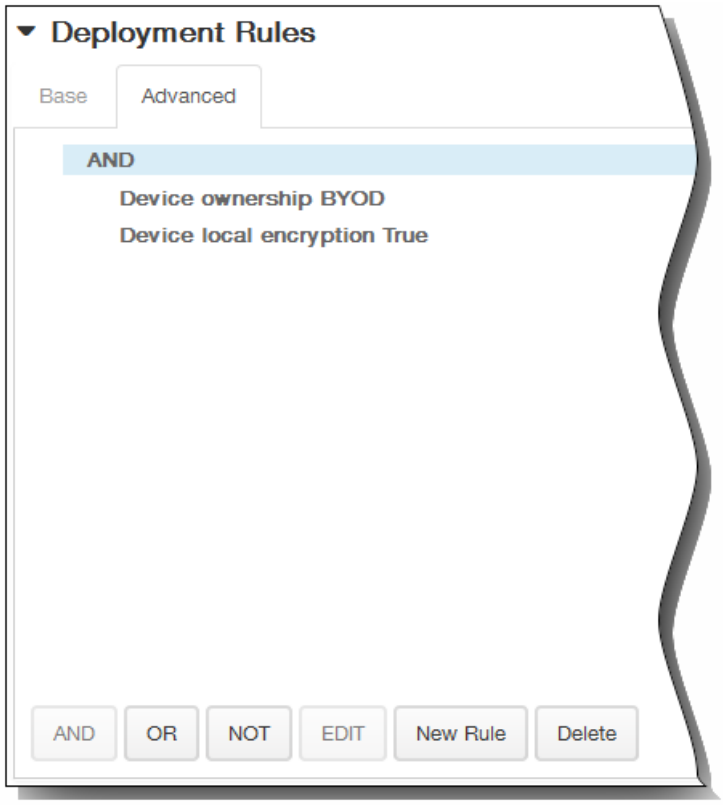
6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:
   1. User-visible name: Geben Sie den Namen so ein, wie er in der Liste der Schriftarten auf den Geräten angezeigt werden soll.
   2. Font file: Wählen Sie die Schriftartdatei aus, die auf den Geräten der Benutzer hinzugefügt werden soll, indem Sie auf Browse klicken und zum Speicherort der Datei navigieren.
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.

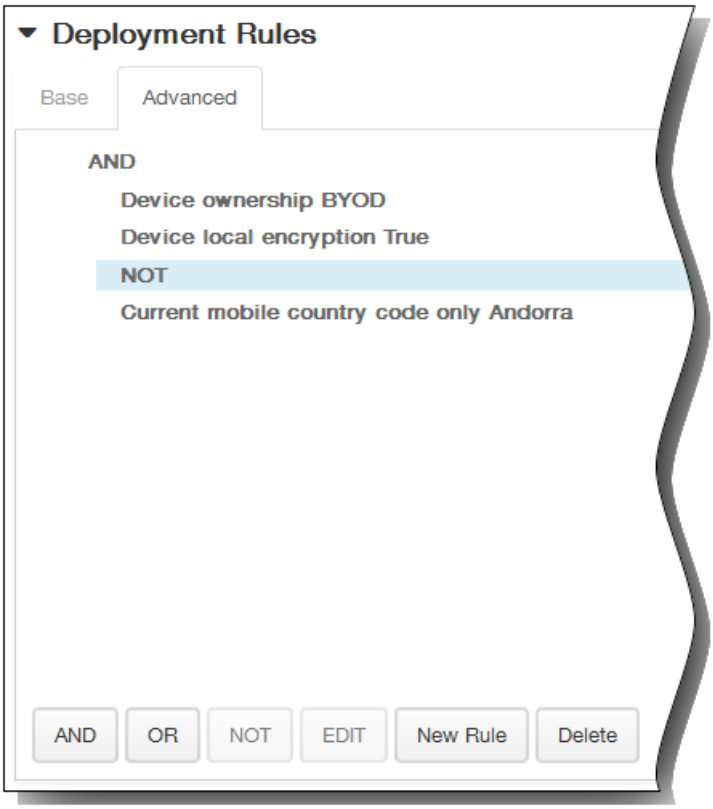
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen 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.



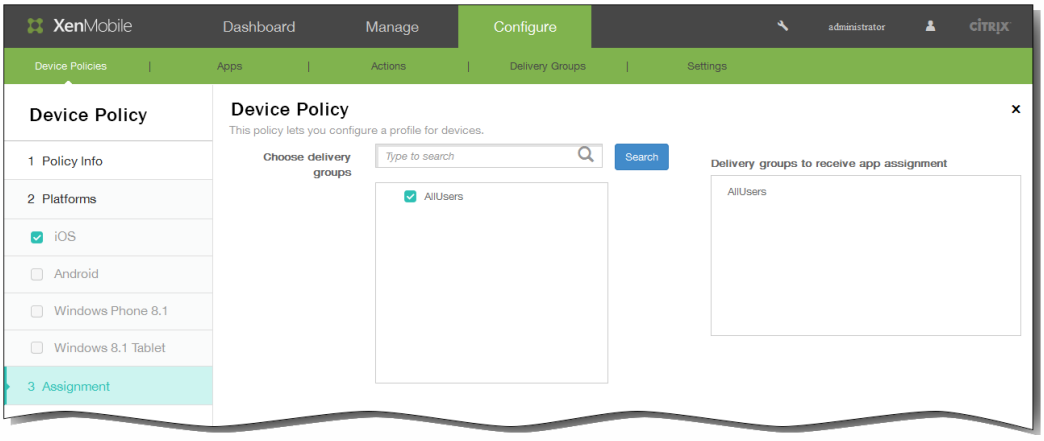
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



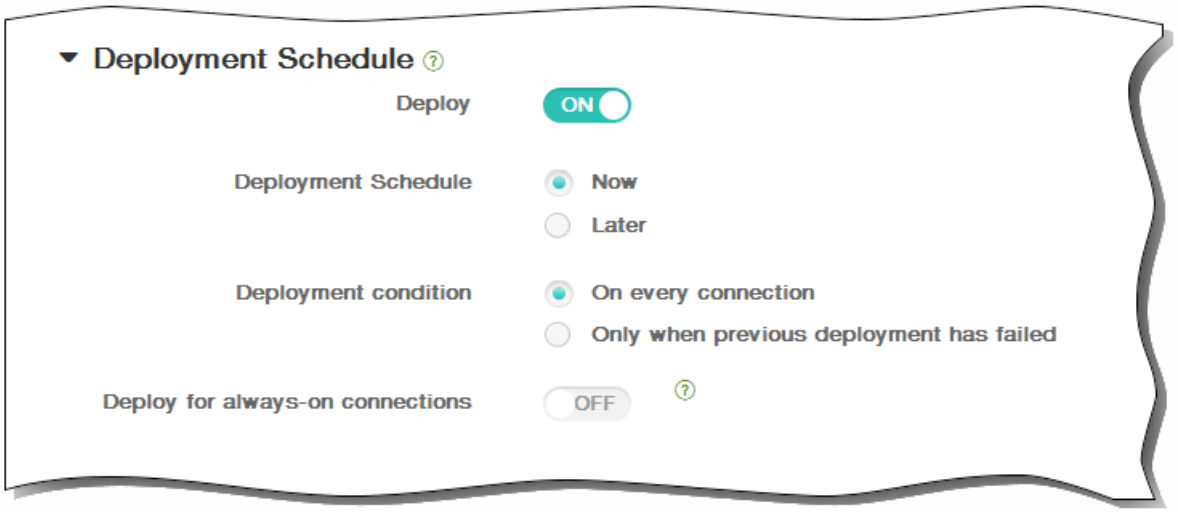
12. Klicken Sie auf Next. Die Seite Assignment für die Schriftartrichtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.



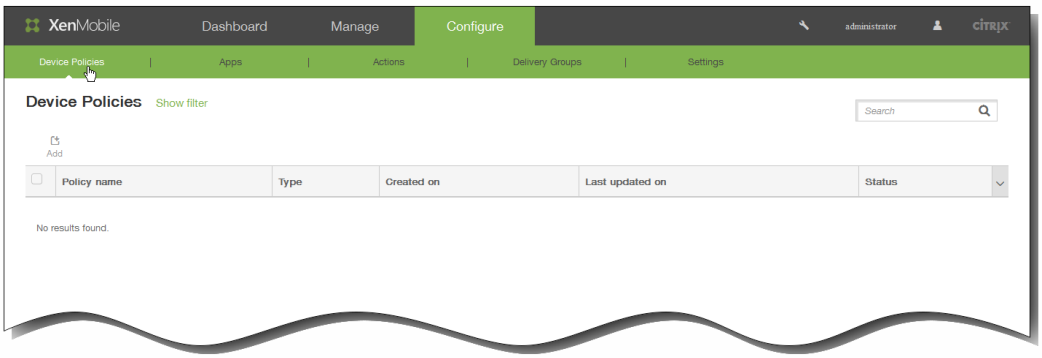
15. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Richtlinie für Unternehmensinformationen für iOS-Geräte hinzu

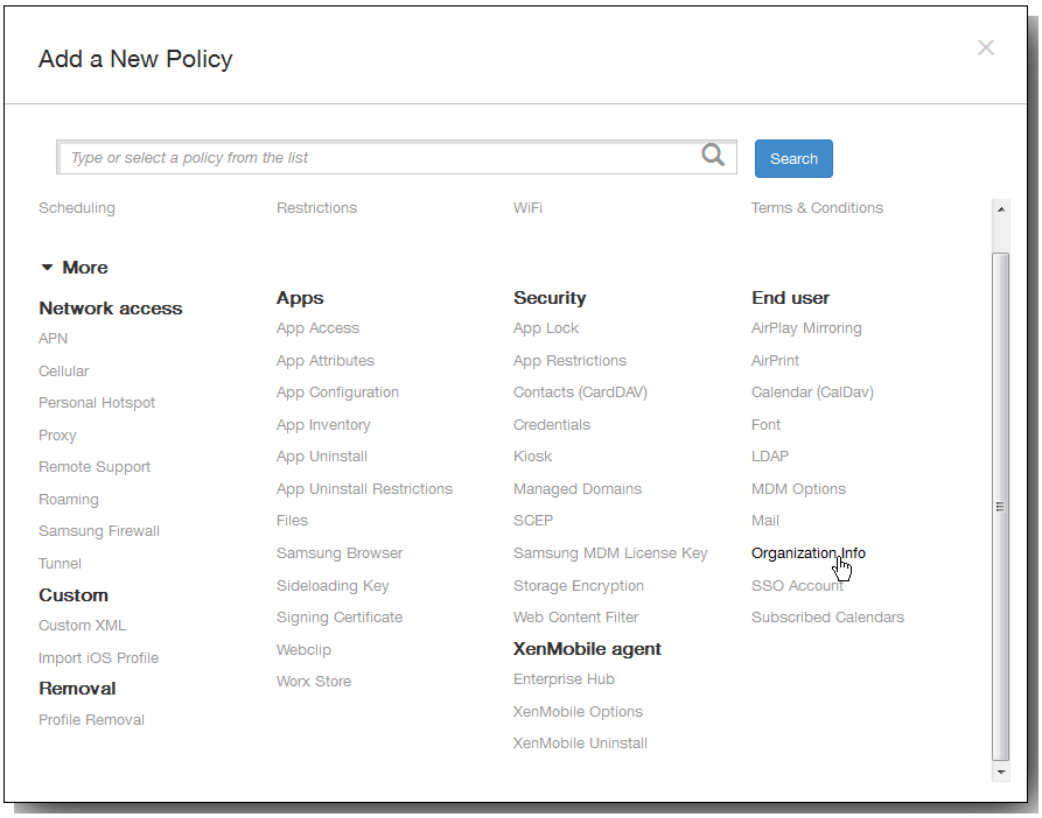
May 05, 2016

Sie können in XenMobile eine Richtlinie hinzufügen, um Ihre Unternehmensinformationen für Warnmeldungen anzugeben, die von XenMobile an iOS-Geräte gesendet werden. Die Richtlinie ist für iOS 7 und höher verfügbar.

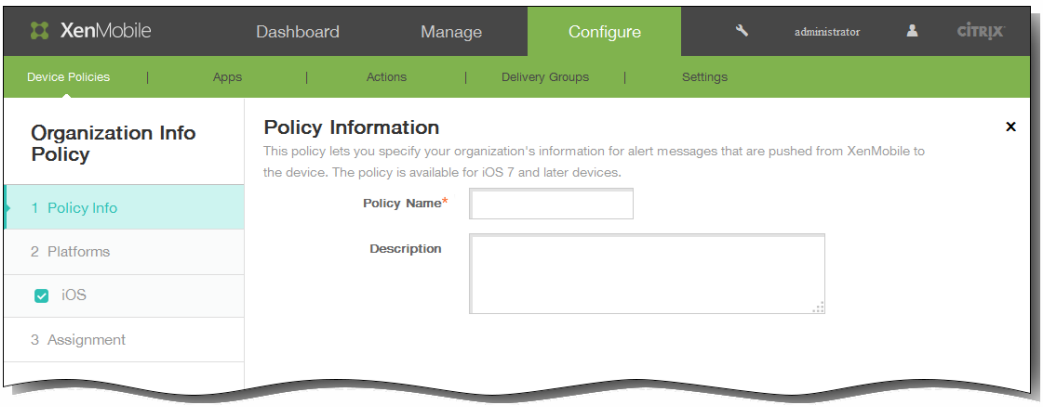
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



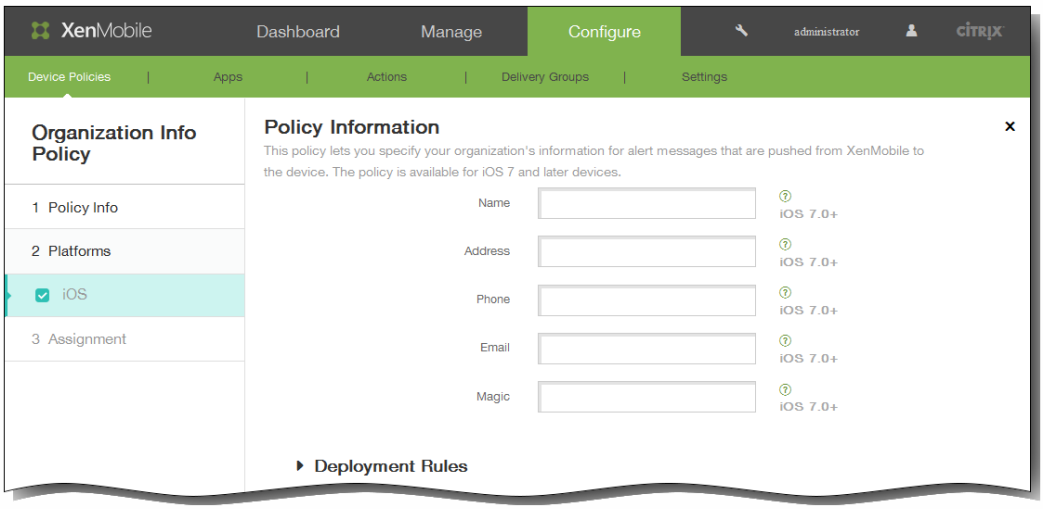
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter End user auf Organization info. Die Seite Organization Info Policy wird angezeigt.

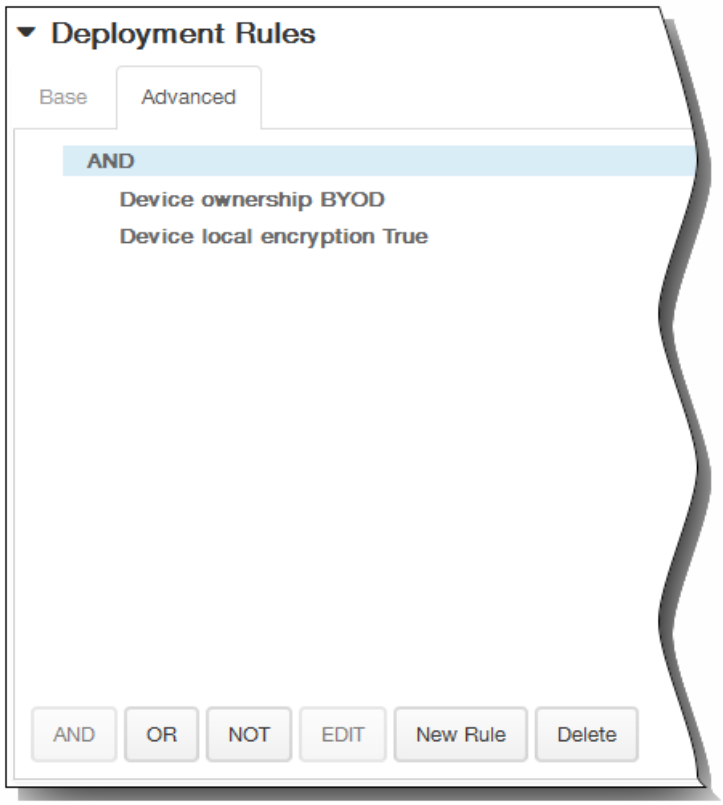


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung für die Richtlinie ein.
5. Klicken Sie auf Next. Die Seite iOS Platform Information wird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



6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:
   1. Name: Geben Sie den Namen des Unternehmens ein, das XenMobile ausführt.
   2. Address: Geben Sie die Adresse des Unternehmens ein.
   3. Phone: Geben Sie die Supporttelefonnummer des Unternehmens ein.
   4. Email: Geben Sie die Support-E-Mail-Adresse des Unternehmens ein.
   5. Magic: Geben Sie ein oder mehrere Stichwörter zur Beschreibung der vom Unternehmen verwalteten Dienste ein.
7. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

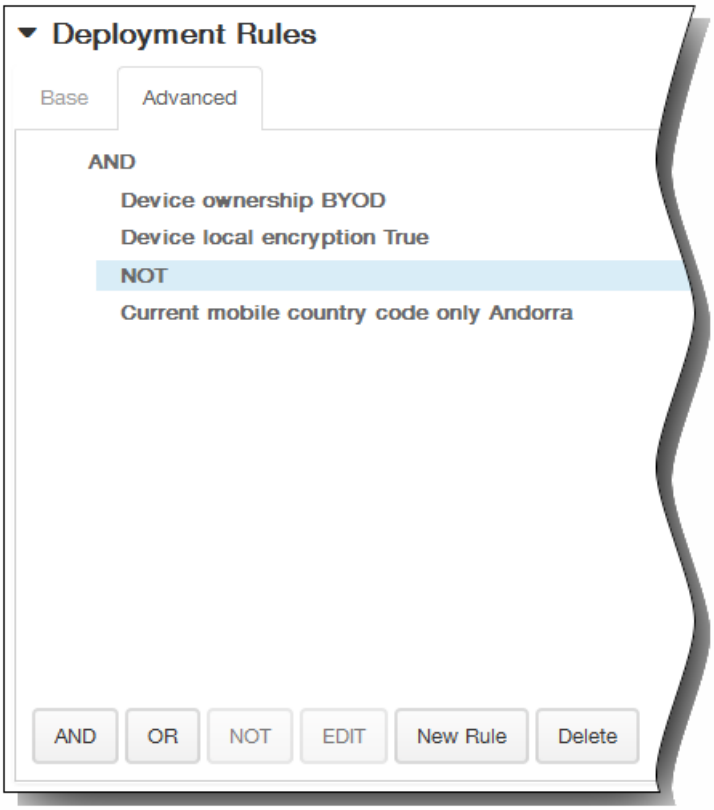
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



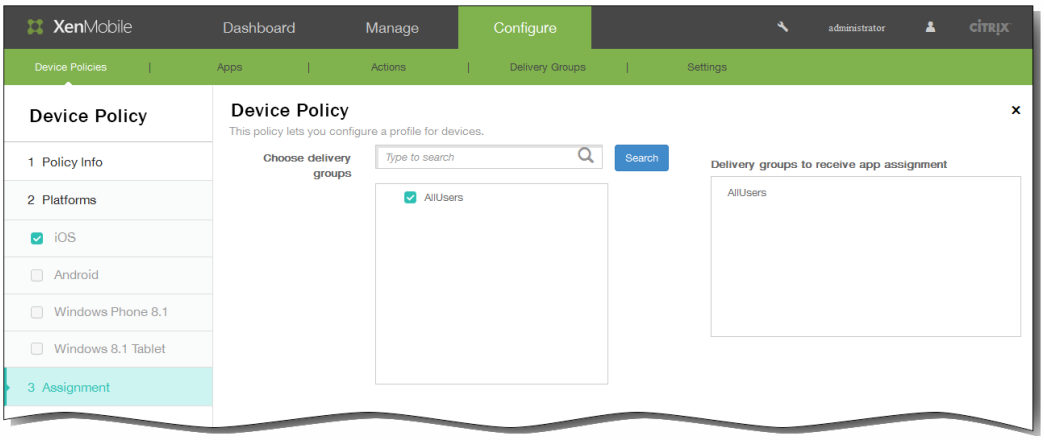
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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.



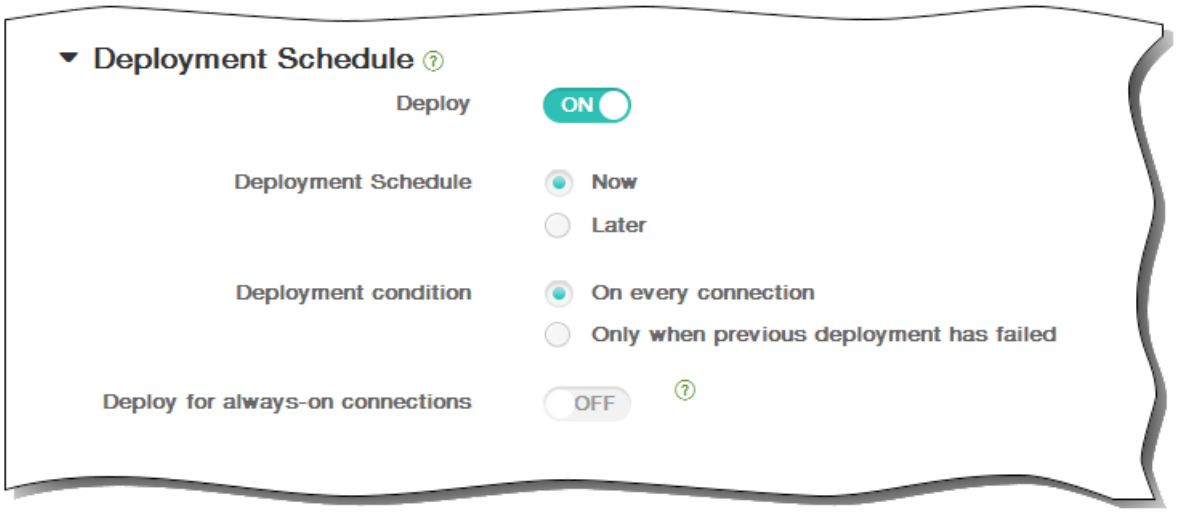
8. Klicken Sie auf Next. Die Seite Assignment für die Richtlinie für Unternehmensinformationen wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. 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.

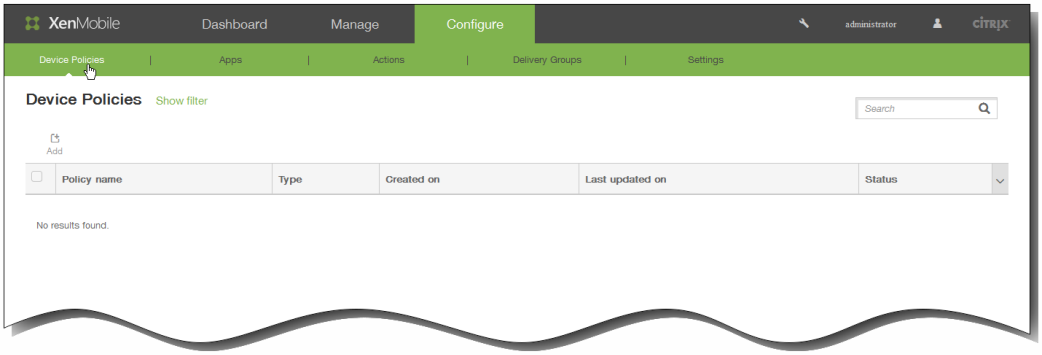
So fügen Sie eine LDAP-Richtlinie für iOS-Geräte hinzu

May 05, 2016

Sie erstellen eine LDAP-Richtlinie für iOS-Geräte in XenMobile, um Informationen zu dem zu verwendenden LDAP-Server und erforderliche Kontoinformationen anzugeben. Die Richtlinie umfasst auch eine Reihe von LDAP-Suchrichtlinien für Abfragen beim LDAP-Server.

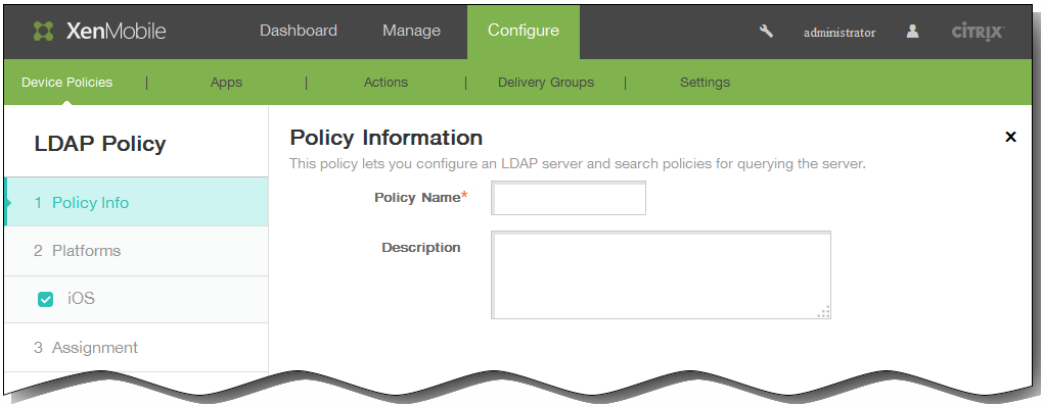
Zum Konfigurieren der Richtlinie benötigen Sie den LDAP-Hostnamen.

1. Klicken Sie in der XenMobile-Konsole auf ConfigureDevice 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 End user auf LDAP. Die Seite LDAP Policy wird angezeigt.

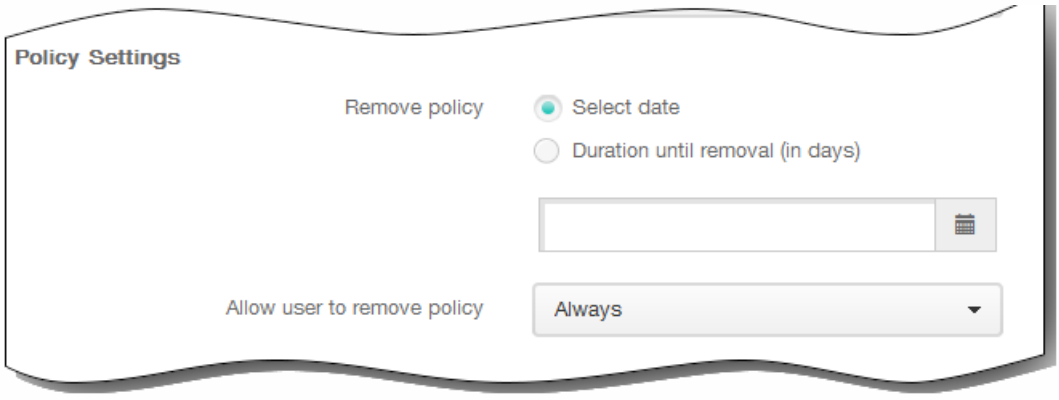


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite iOS Platform wird angezeigt.

6. Geben Sie auf der Seite iOS Platform die folgenden Informationen ein:
    1. Account description: Geben Sie ein optionale Kontobeschreibung ein.
    2. Account user name: Geben Sie einen optionalen Benutzernamen ein.
    3. Account password: Geben Sie ein optionales Kennwort ein. Verwenden Sie dieses nur bei verschlüsselten Profilen.
    4. LDAP host name: Geben Sie den Hostnamen des LDAP-Servers ein. Diese Angabe ist erforderlich.
    5. Use SSL: Wählen Sie aus, ob für die Verbindung mit dem LDAP-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist ON.
    6. Search Settings: Klicken Sie auf Add und führen Sie folgende Schritte aus:
       Hinweis: Sie können beliebig viele Sucheinstellungen eingeben, es ist jedoch mindestens eine erforderlich, damit das Konto einen Nutzen hat.
        1. Description: Geben Sie eine Beschreibung der Sucheinstellung ein. Diese Angabe ist erforderlich.
        2. Scope: Klicken Sie in der Liste auf Base, One level oder Subtree, um die Tiefe der Suche in der LDAP-Struktur anzugeben. Der Standardwert ist Base.
            - Base durchsucht den unter Search base angegebenen Knoten.
            - One level durchsucht den unter Base angegebenen Knoten und eine Ebene darunter.
            - Subtree durchsucht den unter Base angegebenen Knoten und alle Ebenen darunter.
        3. Search base: Geben Sie den Pfad des Knotens ein, an dem die Suche beginnen soll. Beispiel: `ou=people` oder `0=example corp`. Diese Angabe ist erforderlich.
        4. Klicken Sie auf Add, um die Sucheinstellung hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
        5. Wiederholen Sie die Schritte i bis iv für jede Sucheinstellung, die Sie hinzufügen möchten.

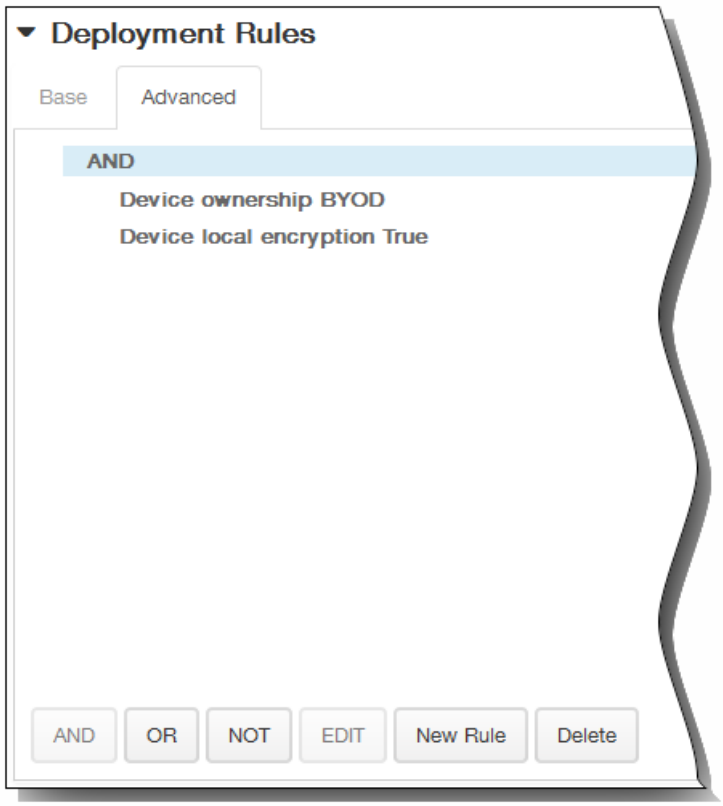
       Hinweis: Zum Löschen einer vorhandenen Sucheinstellung zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf Delete zum Löschen des Eintrags oder auf Edit, um ihn beizubehalten.

       Zum Bearbeiten einer Sucheinstellung 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. 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.

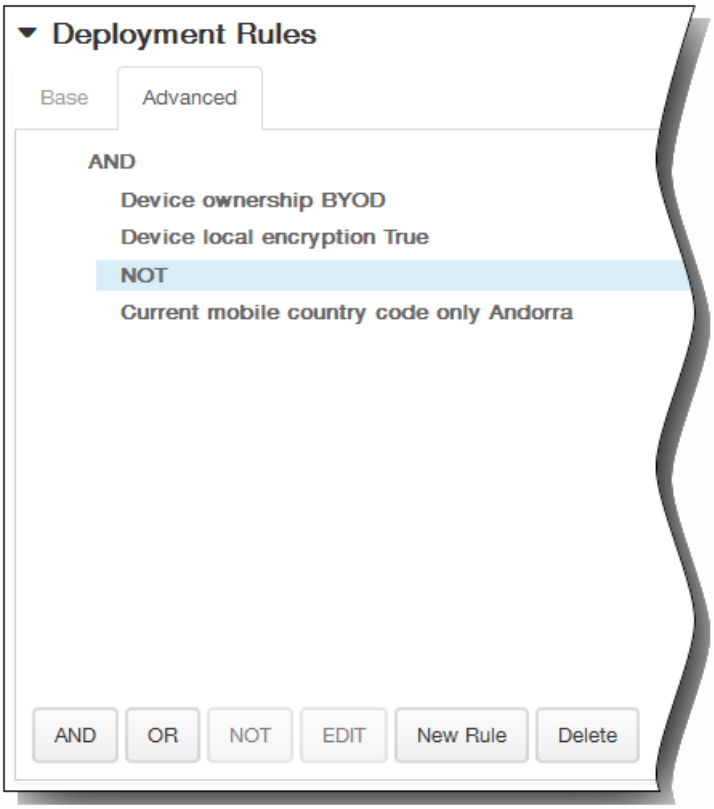
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



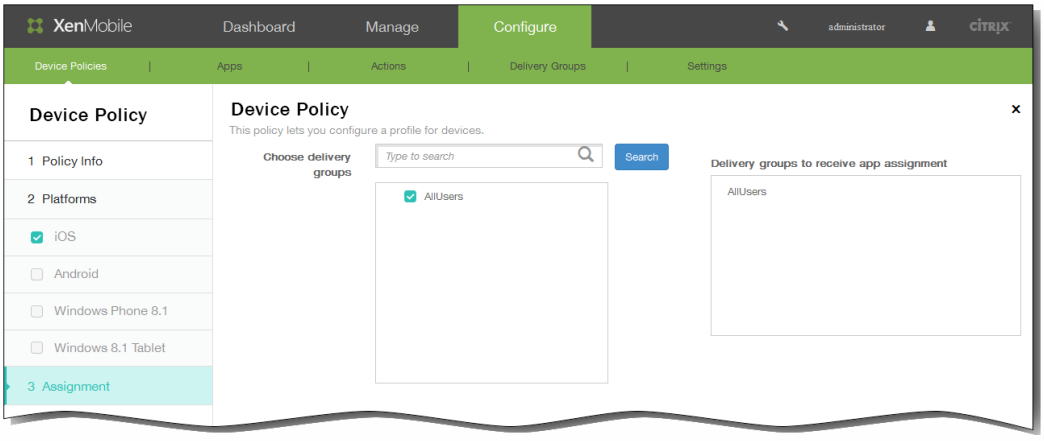
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.

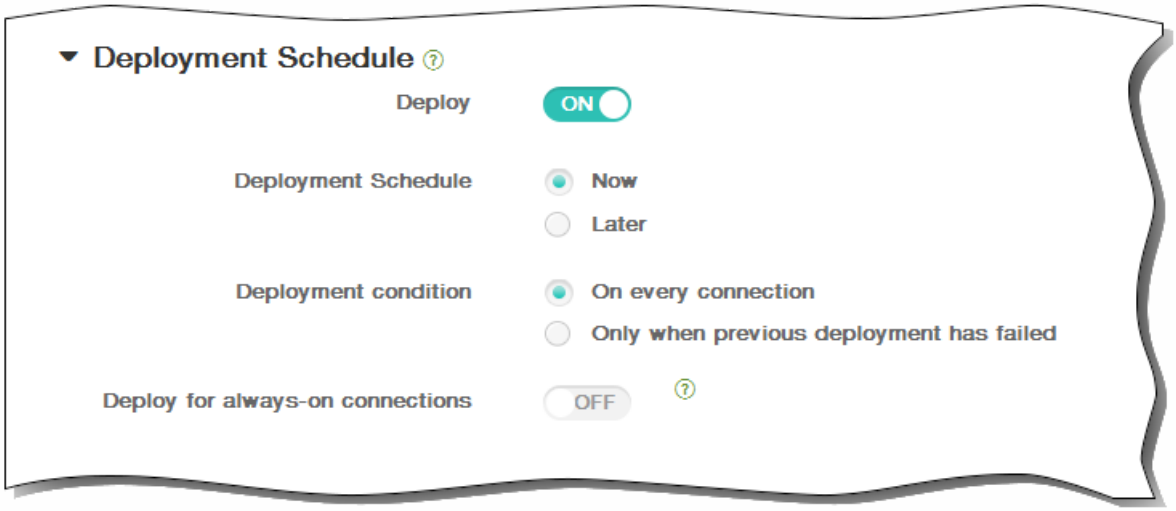


12. Klicken Sie auf Next. Die Seite Assignment für die LDAP-Richtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen 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.

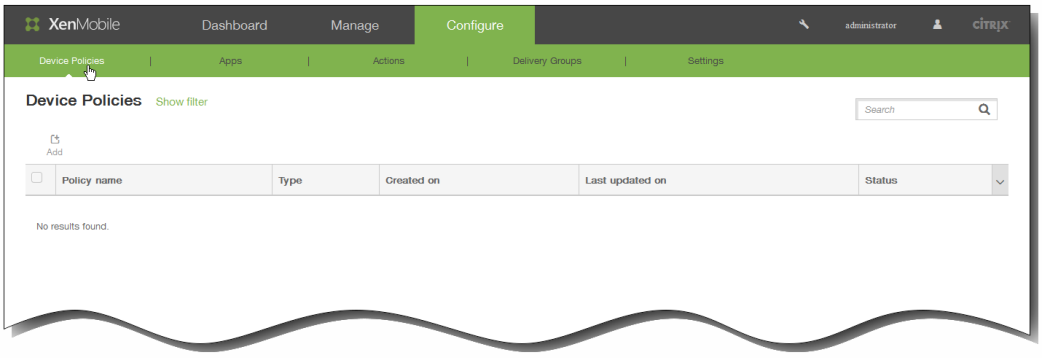
So fügen Sie eine Single Sign-On-Kontorichtlinie für iOS-Geräte hinzu

May 05, 2016

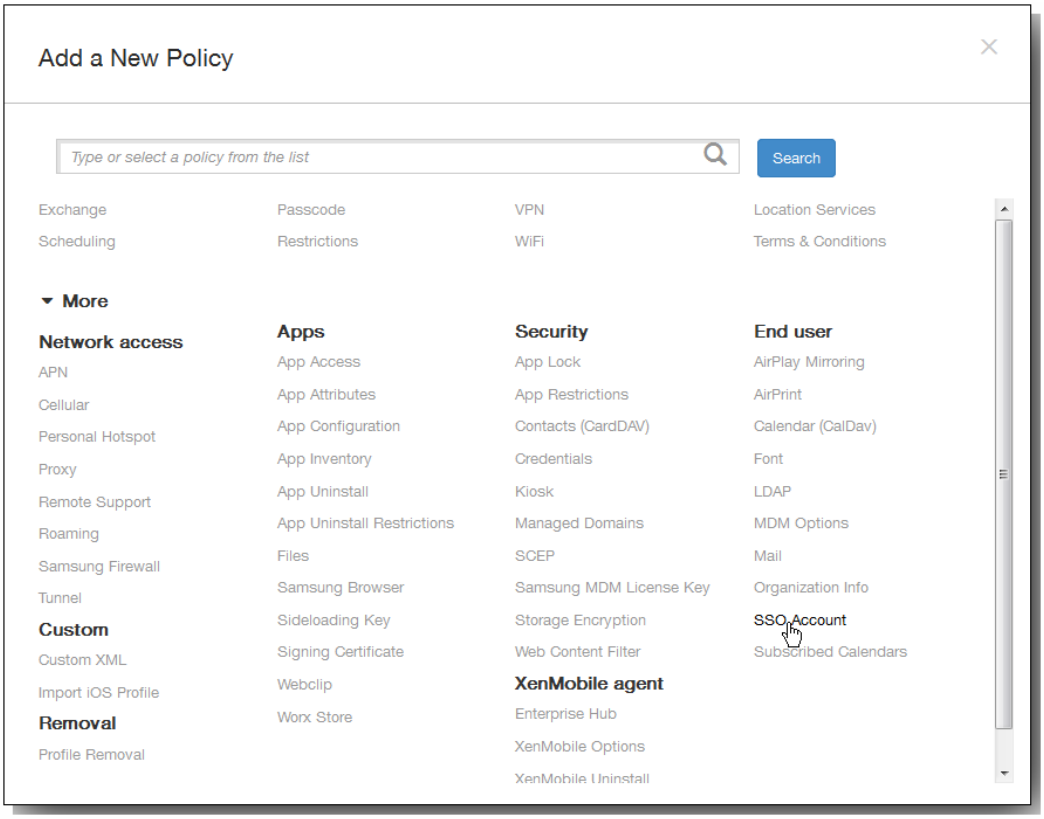
Sie erstellen Single Sign-On-Konten (SSO) in XenMobile, damit Benutzer nach einmaliger Anmeldung auf XenMobile und interne Unternehmensressourcen von unterschiedlichen Apps aus zugreifen können. Sie müssen keine Anmeldeinformationen auf dem Gerät speichern. Die Unternehmensanmeldeinformationen des SSO-Kontos werden für alle Apps verwendet, einschließlich derer aus dem App-Store. Diese Richtlinie ist für Kerberos-Authentifizierungs-Back-Ends ausgelegt.

Hinweis: Die Richtlinie gilt nur für iOS 7.0 und höher.

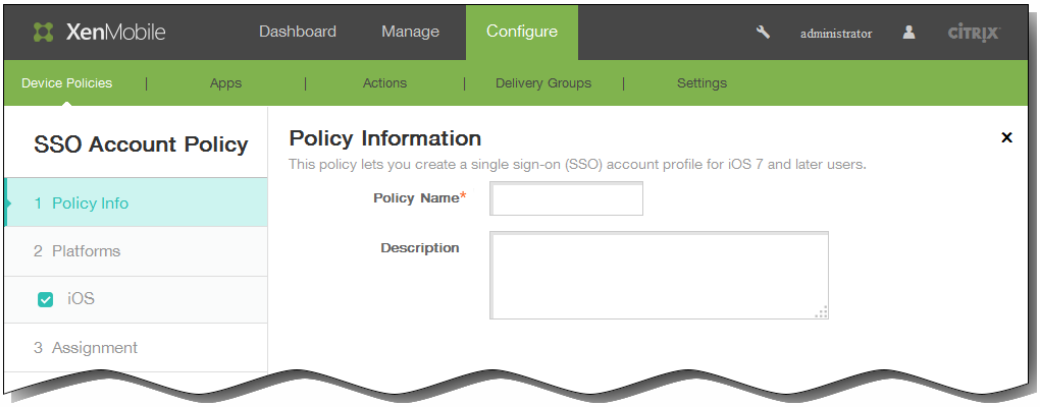
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



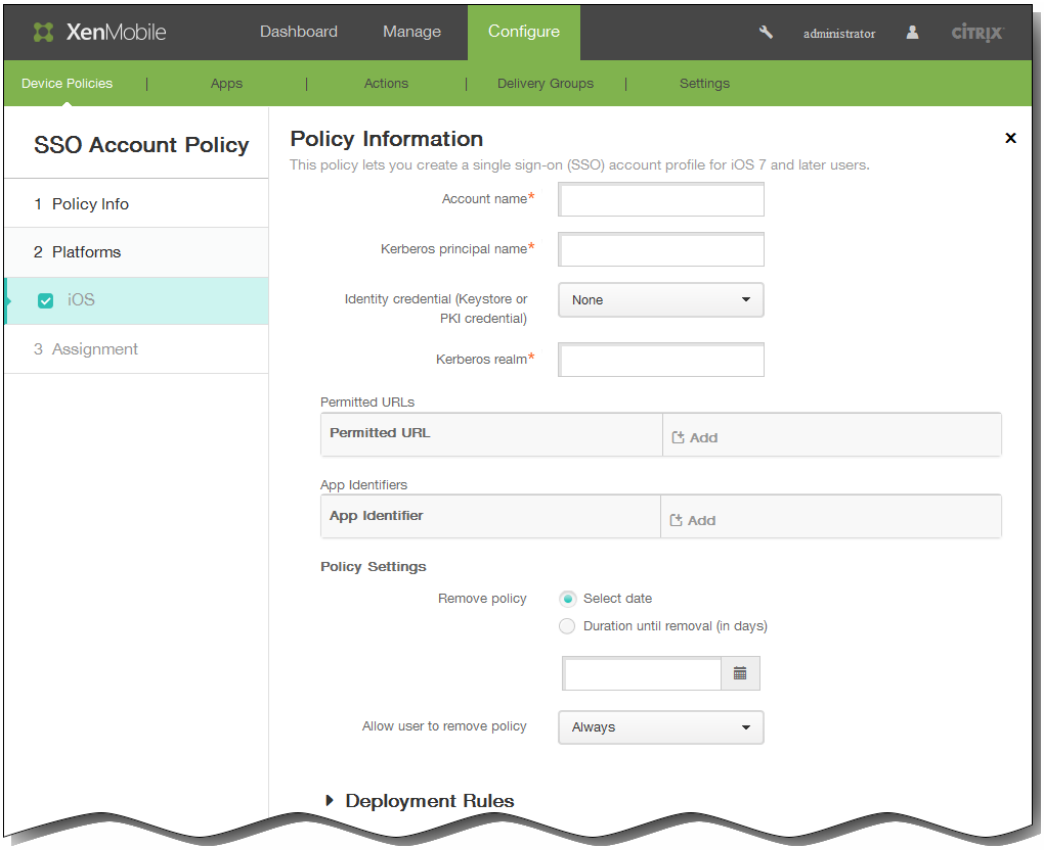
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter End user auf SSO Account. Die Seite SSO Account Policy wird angezeigt.



4. Geben Sie im Bereich SSO Account 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.
5. Klicken Sie auf Next. Die Seite iOS Platform wird angezeigt.



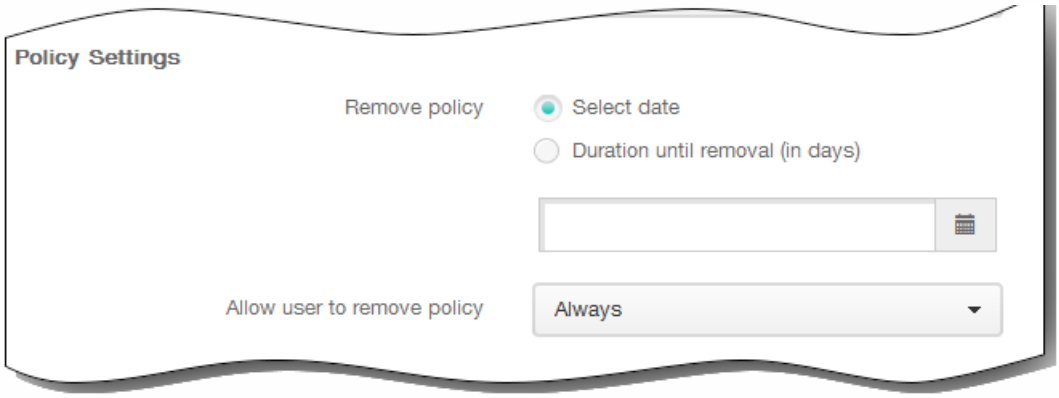
6. Geben Sie auf der Seite iOS Platform die folgenden Informationen ein:
    1. Account name: Geben Sie den Kerberos-SSO-Kontonamen ein, der auf dem Benutzergerät angezeigt wird. Diese Angabe ist erforderlich.
    2. Kerberos principal name: Geben Sie den Kerberos-Prinzipalnamen ein. Diese Angabe ist erforderlich.
    3. Identity credential (Keystore or PKI credential): Klicken Sie in der Liste auf optionale Anmeldeinformationen zum Verlängern der Kerberos-Anmeldeinformationen ohne Benutzereingriff.
    4. Kerberos realm: Geben Sie den Kerberos-Bereich für die Richtlinie ein. Dies ist normalerweise der Domänenname in Großbuchstaben (z. B. EXAMPLE.COM). Diese Angabe ist erforderlich.
    5. Permitted URLs: Klicken Sie auf Add und führen Sie folgende Schritte aus:
        1. Permitted URL: Geben Sie eine URL ein, für die SSO erforderlich sein soll, wenn ein Benutzer auf sie von einem iOS-Gerät aus zugreift.
           Wenn ein Benutzer beispielsweise zu einer Website navigiert und von dieser eine Kerberos-Aufforderung ausgegeben wird, erfolgt kein SSO-Versuch durch Angabe des möglicherweise auf dem Gerät bei einer vorherigen Anmeldung von Kerberos zwischengespeicherten Kerberos-Tokens, wenn die Website nicht in der URL-Liste ist. Die Zuordnung im Hostteil der URL muss exakt sein. Beispiel: http://shopping.apple.com ist zulässig, nicht aber http://*.apple.com. Wenn Kerberos nicht basierend auf Hostzuordnung aktiviert wird, erfolgt für die URL zudem weiterhin ein standardmäßiger HTTP-Aufruf. Dies kann fast alles sein, einschließlich einer Standard-Kennwortanforderung oder eines HTTP-Fehlers, wenn die URL nur für SSO mit Kerberos konfiguriert ist.
        2. Klicken Sie auf Add, um die URL hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
        3. Wiederholen Sie die Schritte i und ii für jede URL, die Sie hinzufügen möchten.
    6. App Identifiers: Klicken Sie auf Add und führen Sie die folgenden Schritte aus:
        1. App Identifier: Geben Sie eine App-ID für eine App ein, bei der die Verwendung der Anmeldung zulässig sein soll. Hinweis: Wenn Sie keine App-ID angeben, gilt die Anmeldung für **alle** App-IDs.

2. Klicken Sie auf Add, um die App-ID hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
3. Wiederholen Sie die Schritte i und ii für jede App-ID, die Sie hinzufügen möchten.

Hinweis: Zum Löschen vorhandener URLs oder App-IDs 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.

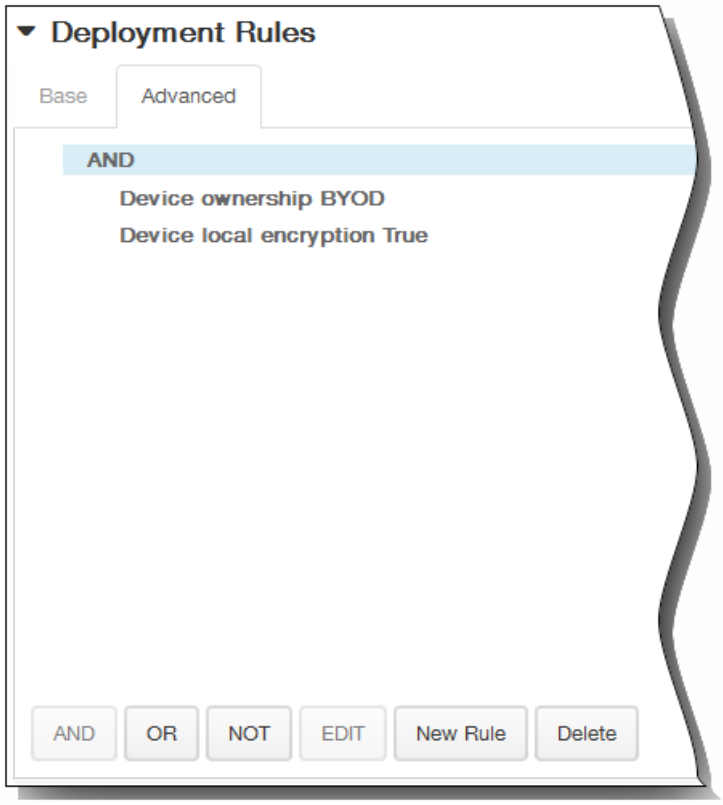
Zum Bearbeiten vorhandener URLs oder App-IDs zeigen Sie auf deren Zeile und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf Save, um die Änderungen zu speichern oder auf Cancel, um den Vorgang abzubrechen.

7. 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.



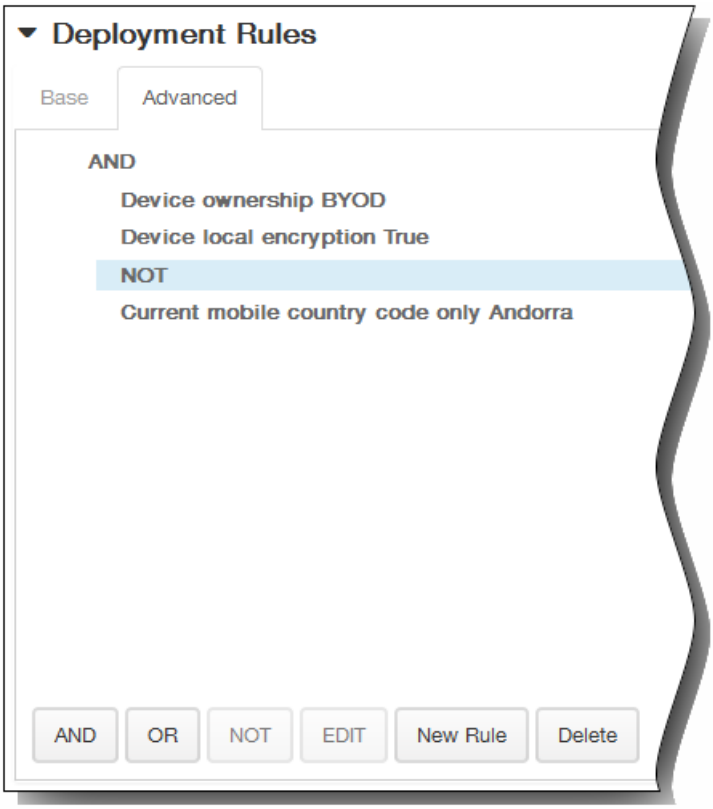
11. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

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.

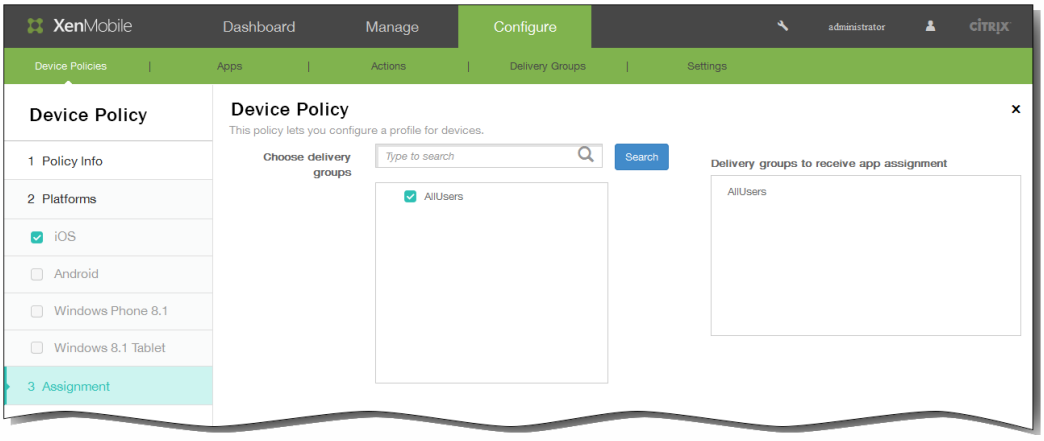


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



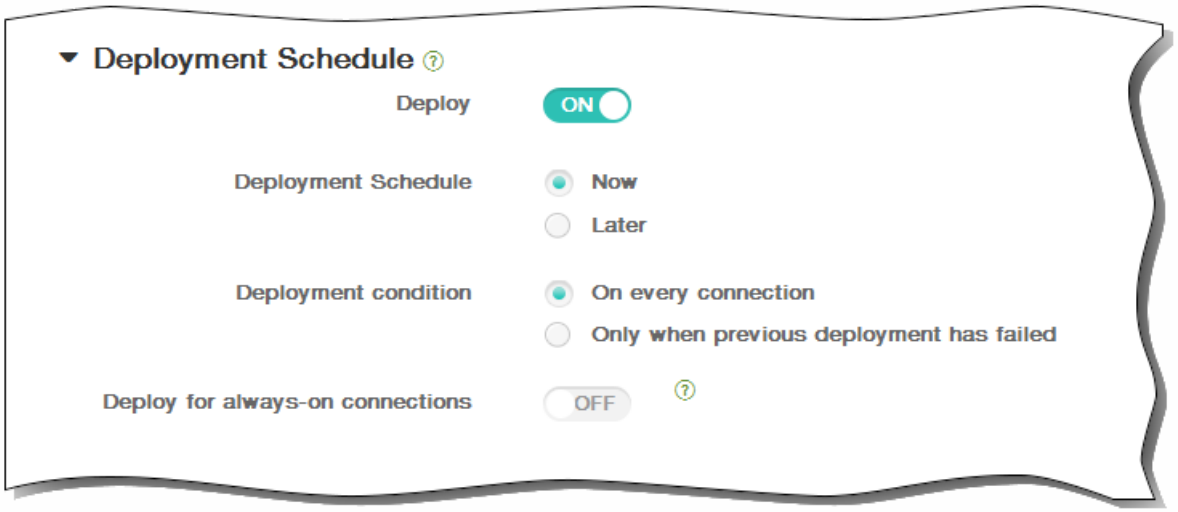
12. Klicken Sie auf Next. Die Seite Assignment für die SSO-Kontorichtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.

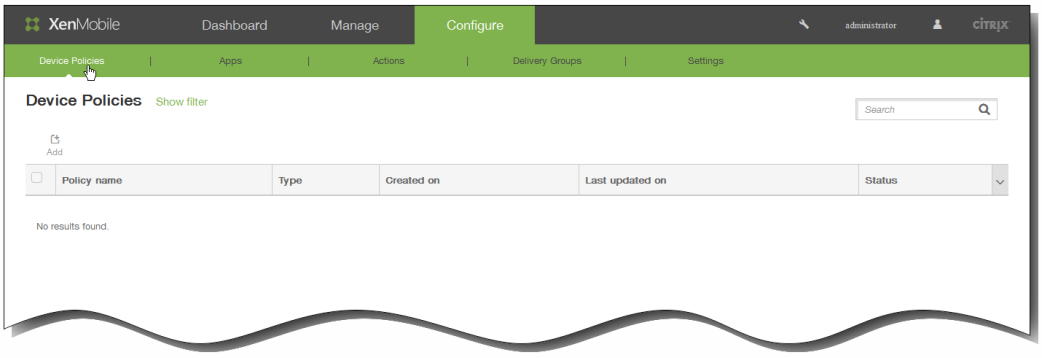
So fügen Sie eine Richtlinie für abonnierte Kalender für iOS-Geräte hinzu

May 05, 2016

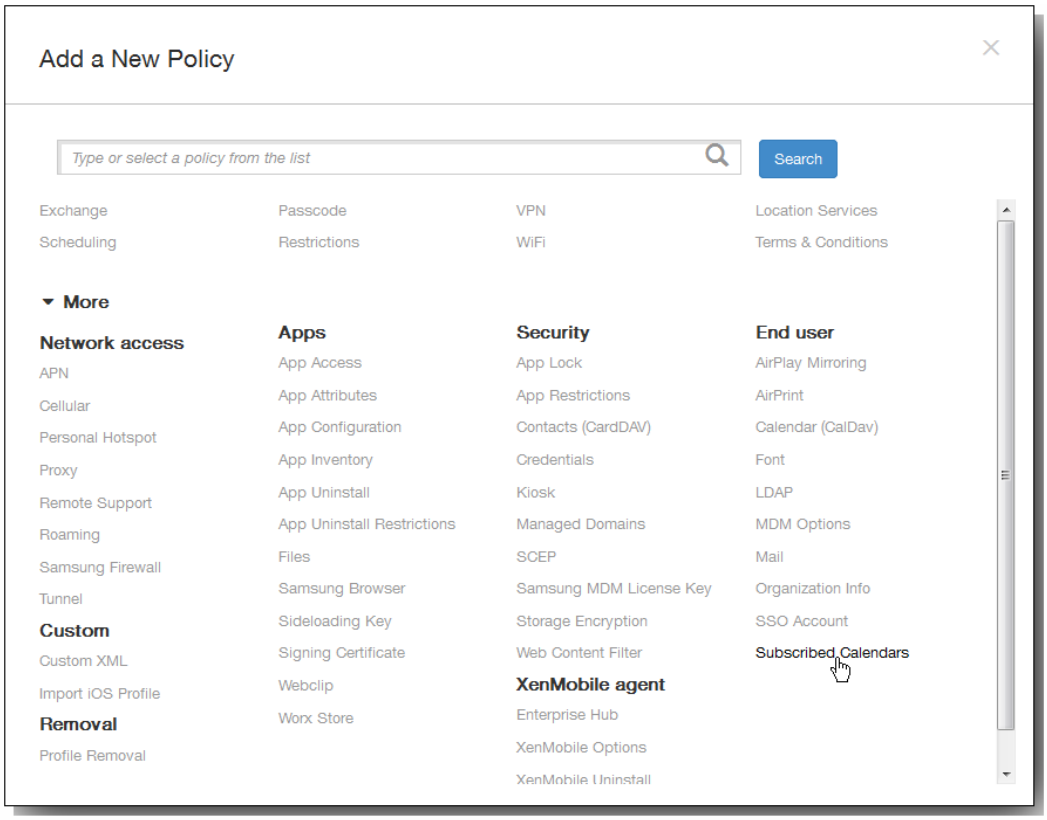
Sie können in XenMobile eine Richtlinie einrichten, mit der ein abonnierter Kalender der Liste der Kalender auf iOS-Geräten hinzugefügt wird. Die Liste der öffentlichen Kalender, die zum Abonnieren verfügbar sind, finden Sie unter www.apple.com/downloads/macosx/calendars.

Hinweis: Sie müssen einen Kalender zunächst abonnieren, bevor Sie ihn der Liste der abonnierten Kalender auf den Geräten der Benutzer hinzufügen können.

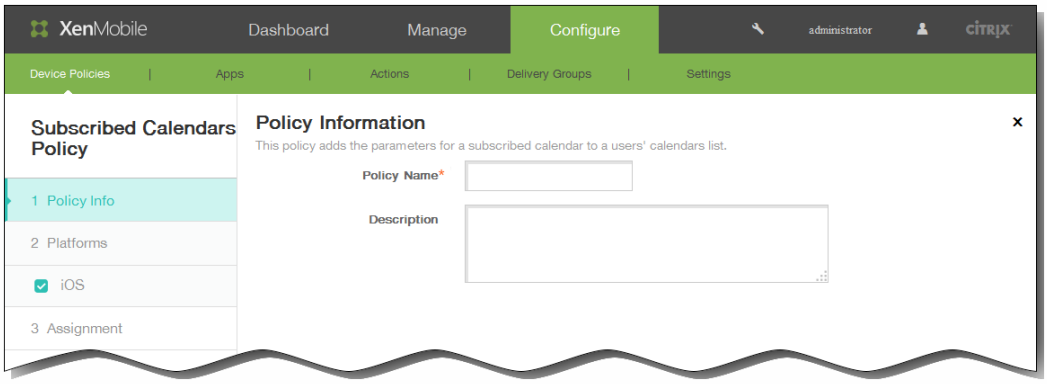
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



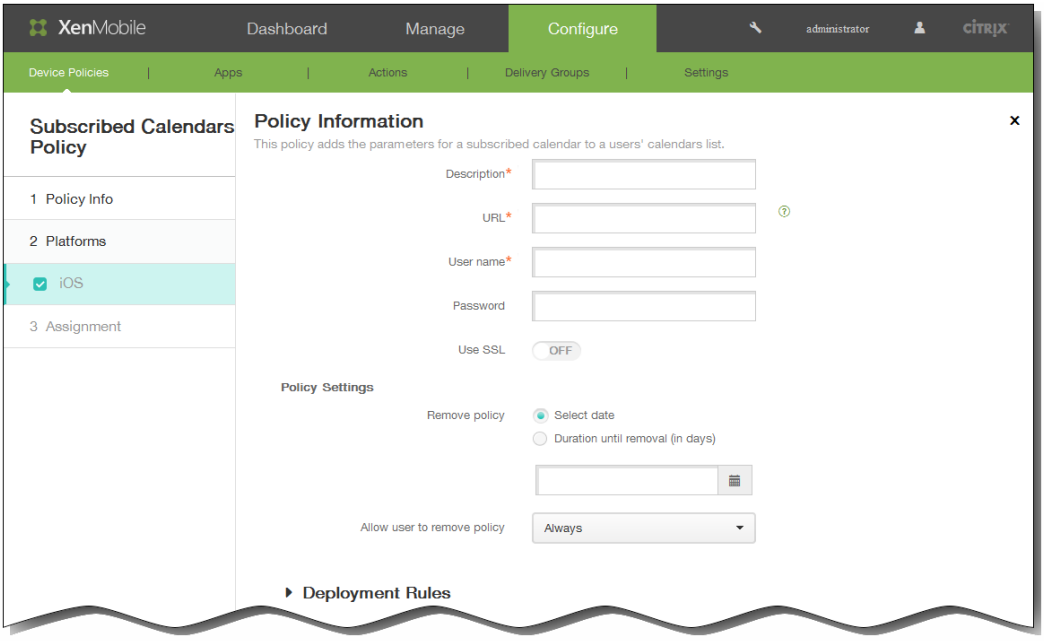
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



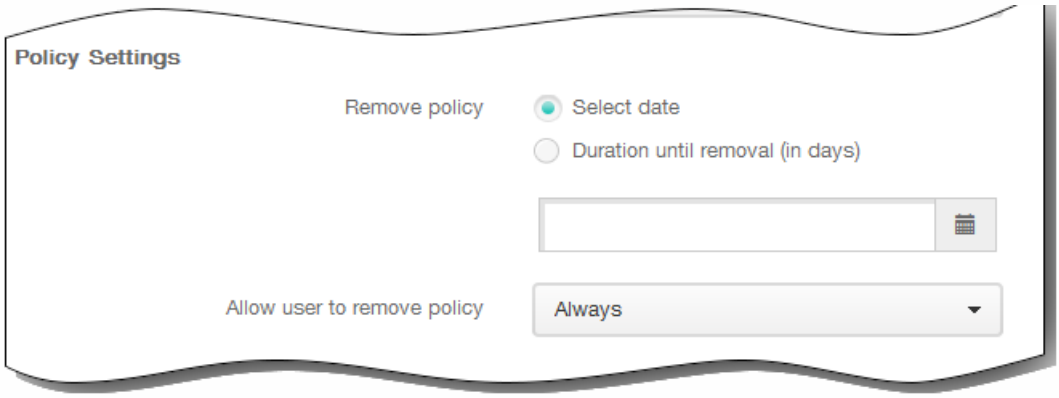
3. Klicken Sie auf More und dann unter End user auf Subscribed Calendars. Die Seite Subscribed Calendars Policy wird angezeigt.



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.

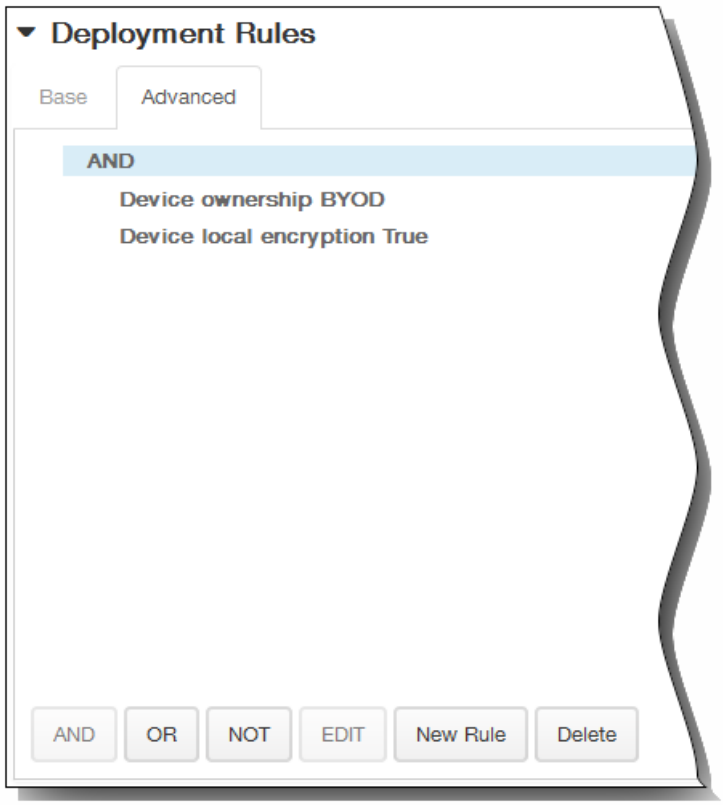


6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:
   1. Description: Geben Sie eine Beschreibung des Kalenders ein. Diese Angabe ist erforderlich.
   2. URL: Geben Sie die Kalender-URL ein. Sie können eine webcal://-URL oder einen http://-Link zu einer iCalendar-Datei (.ics) eingeben. Diese Angabe ist erforderlich.
   3. User name: Geben Sie den Anmeldenamen des Benutzers ein. Diese Angabe ist erforderlich.
   4. Password: Geben Sie ein optionales Benutzerkennwort ein.
   5. Use SSL: Wählen Sie aus, ob für die Verbindung mit dem Kalender Secure Socket Layer verwendet werden soll. Der Standardwert ist Aus.
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.

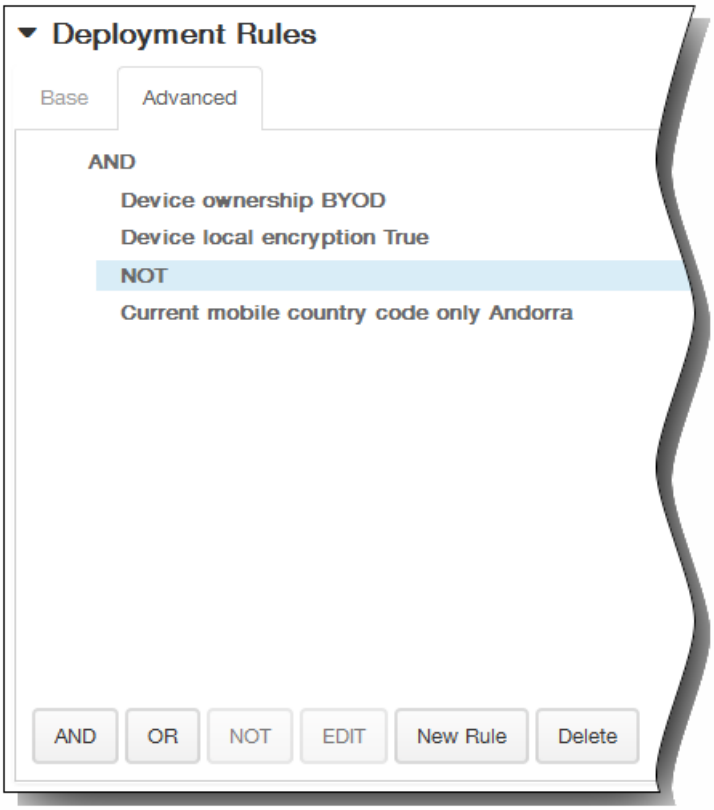
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



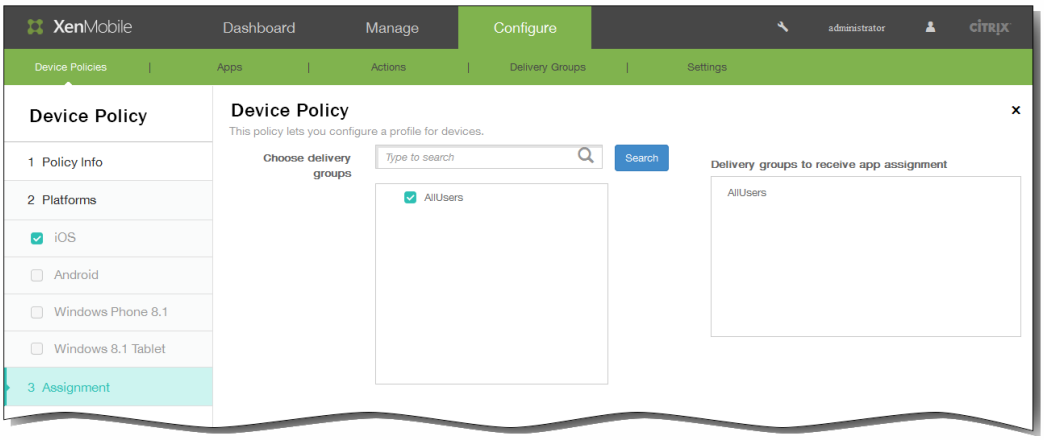
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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.



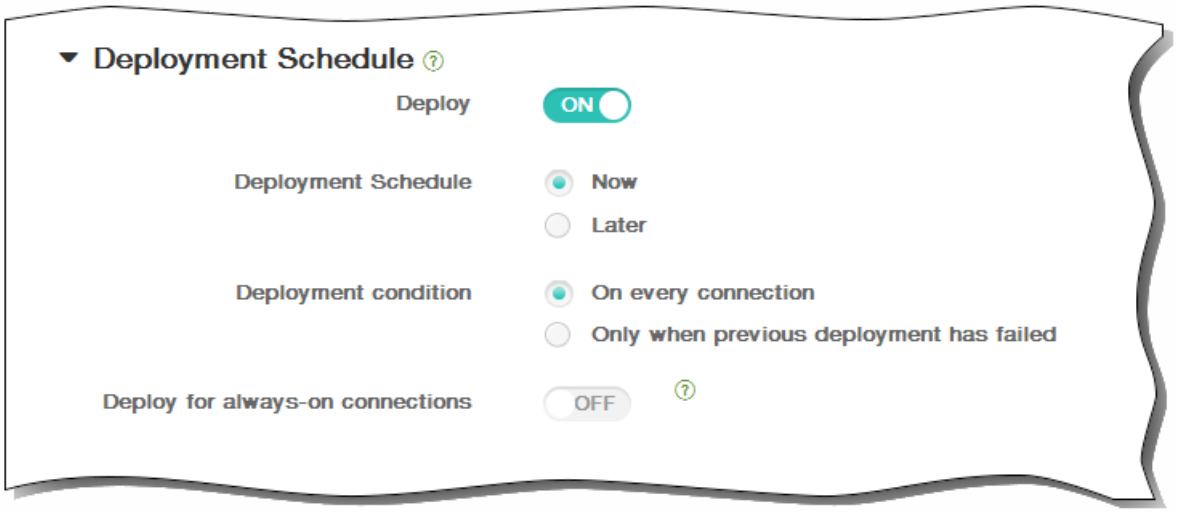
12. Klicken Sie auf Next. Die Seite Assignment für die Kalenderrichtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.



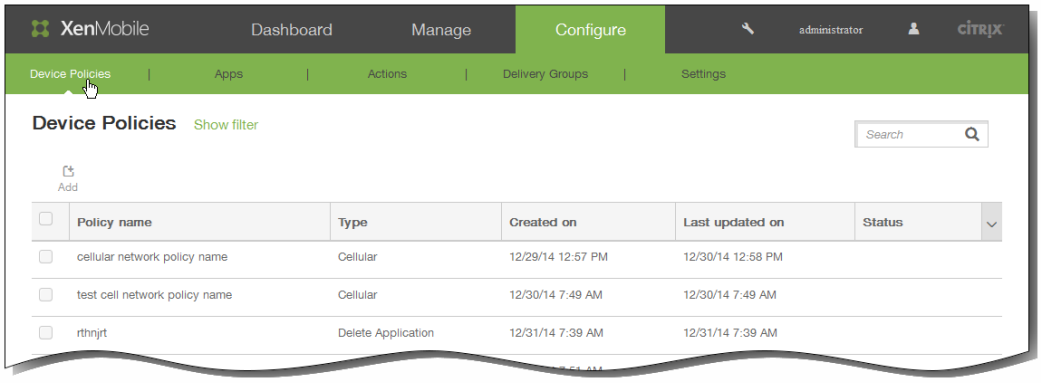
15. Klicken Sie auf Save, um die Richtlinie zu speichern.

Passcoderichtlinien für Geräte

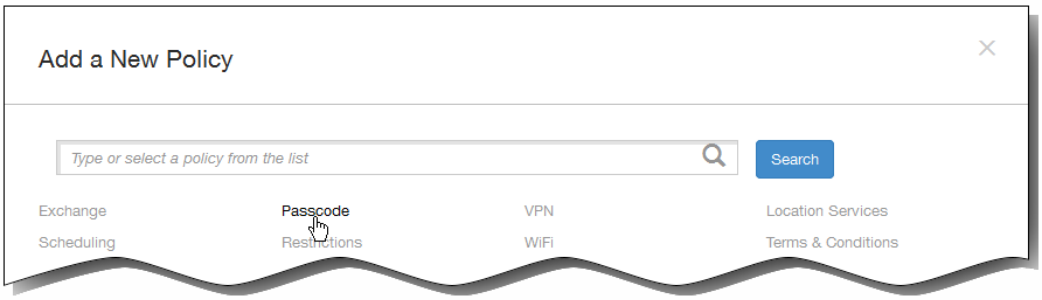
May 05, 2016

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-, 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.

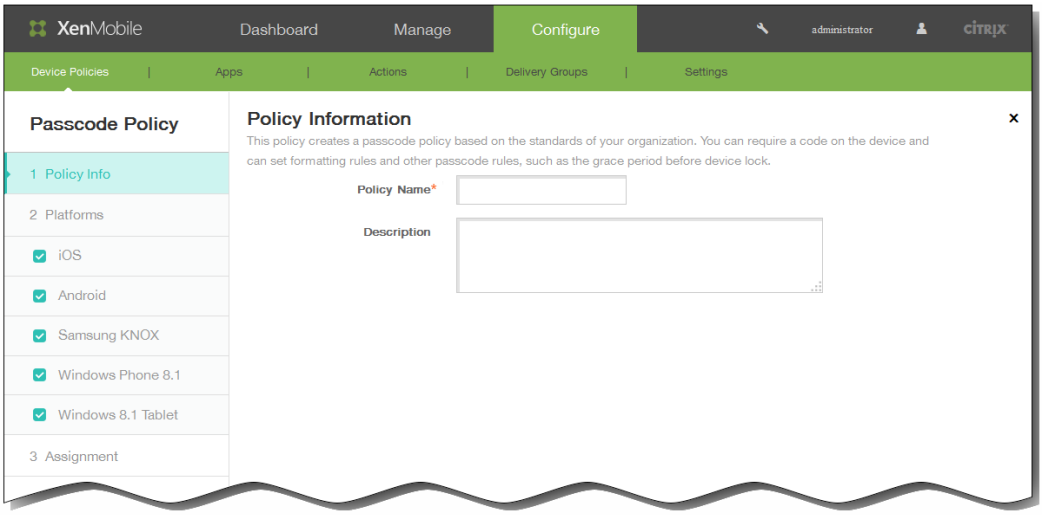
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Geräterichtlinien wird angezeigt. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen.



2. Klicken Sie auf der Seite Add New Policy auf Passcode.

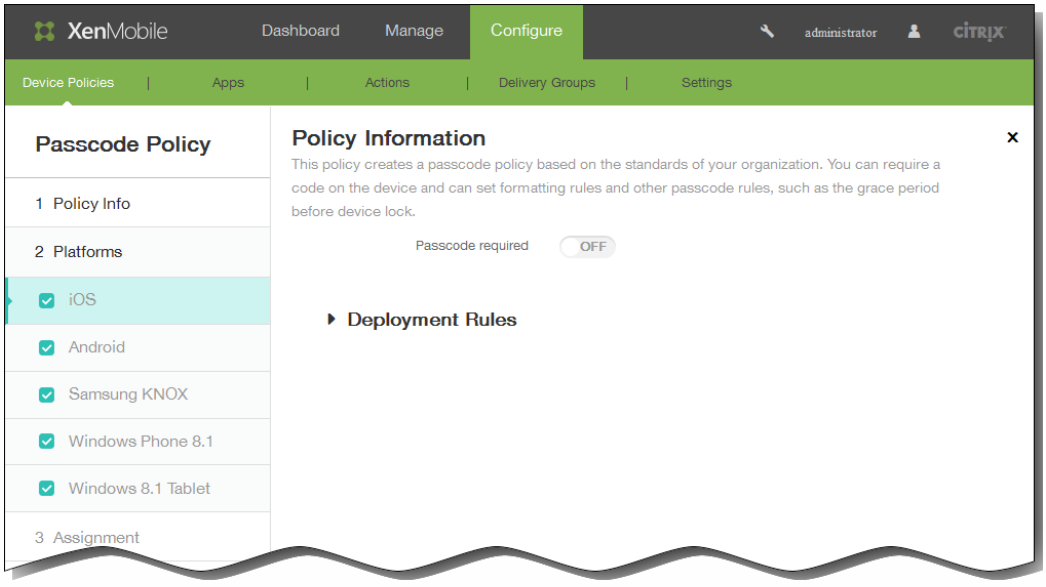


3. Geben Sie im Bereich Policy Information die folgenden Informationen ein:

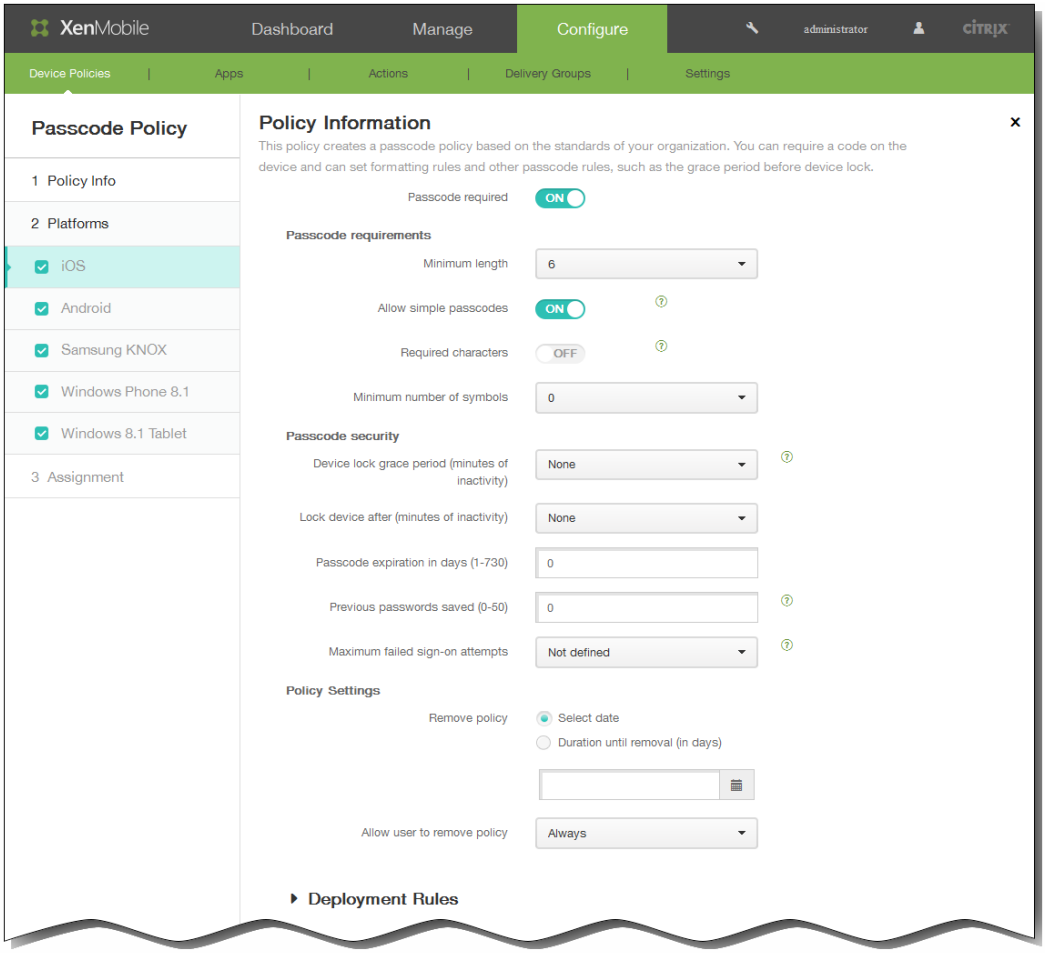


1. Richtlinienname: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
2. Beschreibung: Geben Sie optional eine Beschreibung der Richtlinie ein.
3. Klicken Sie auf Next.

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.

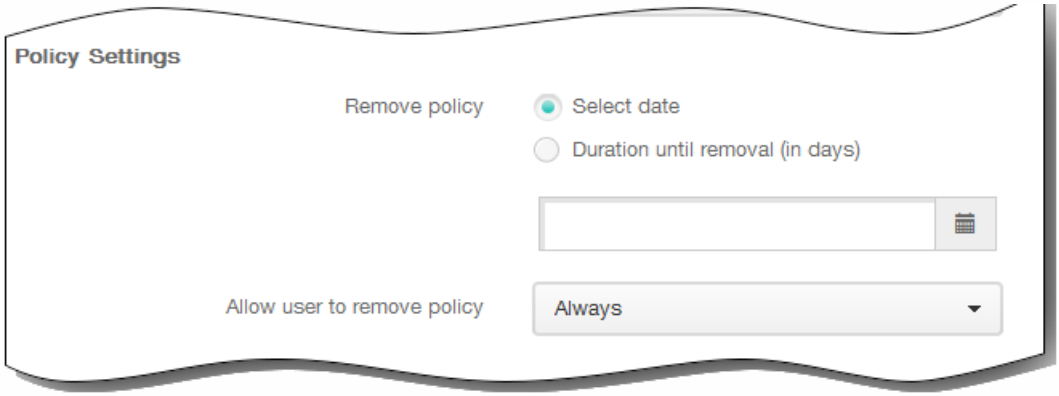
Gerät sperren nach (Minuten Inaktivität): Klicken Sie in der Liste auf den Zeitraum, den ein Gerät inaktiv sein darf, bevor es gesperrt wird. Der Standardwert ist Ohne.

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.

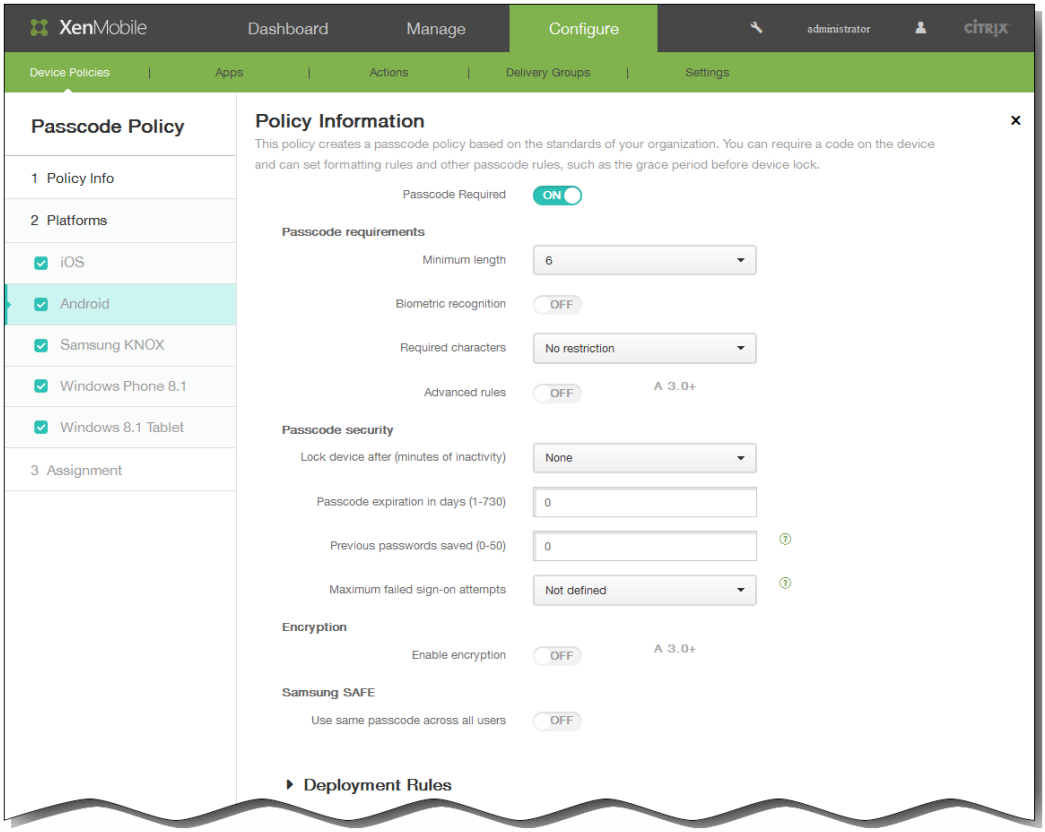
Richtlinieneinstellungen



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.

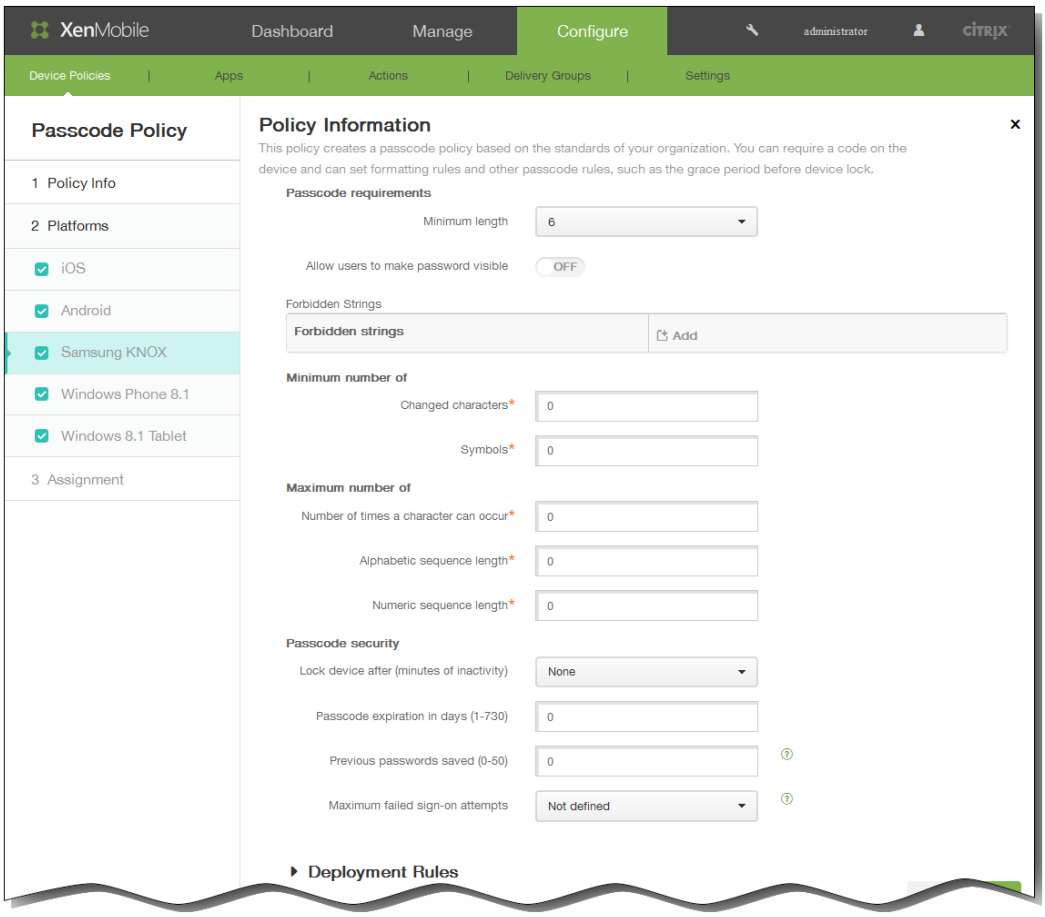
Verschlüsselung

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.

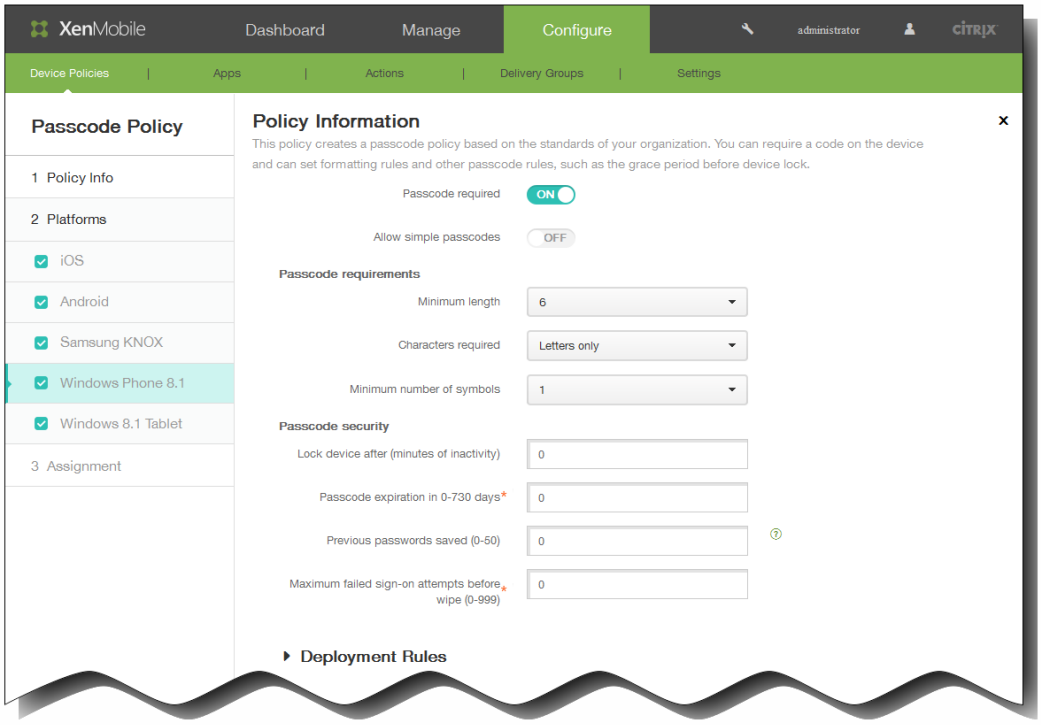
Passcodesicherheit

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

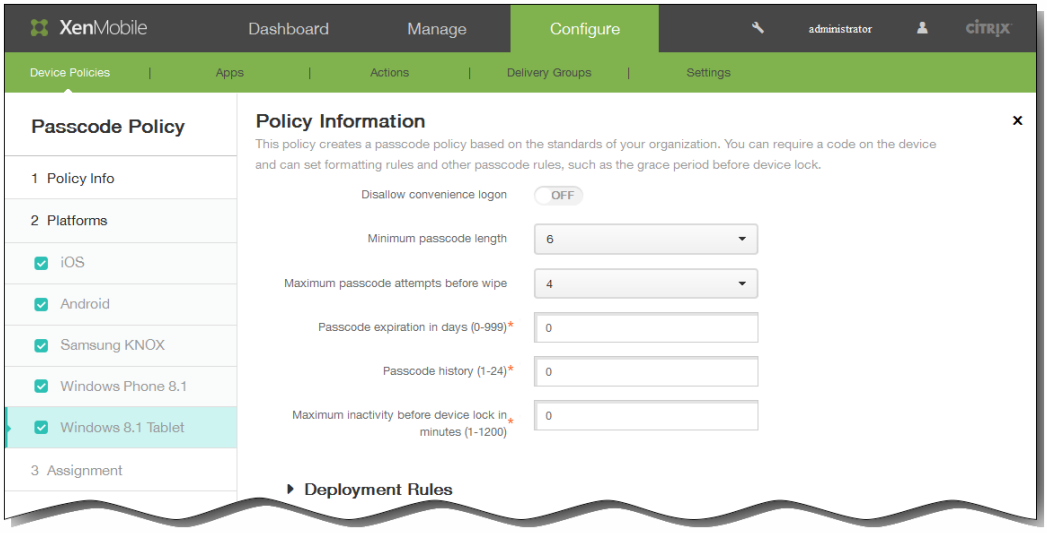
Gerät sperren nach (Minuten Inaktivität): Klicken Sie in der Liste auf den Zeitraum, den ein Gerät inaktiv sein darf, bevor es gesperrt wird. Der Standardwert ist 0.

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.

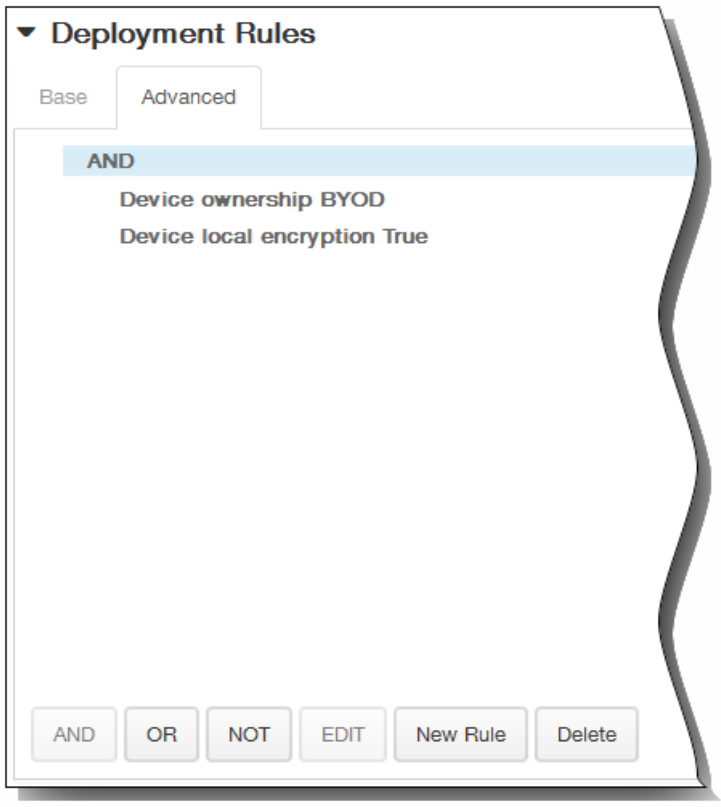
Passcode history: (1-24): Geben Sie an, wie viele verwendete Passcodes gespeichert werden sollen. Die Benutzer können keinen gespeicherten Passcode wiederverwenden. Gültige Werte sind 1-24. Sie müssen eine Zahl zwischen 1 und 24 in diesem Feld eingeben.

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.

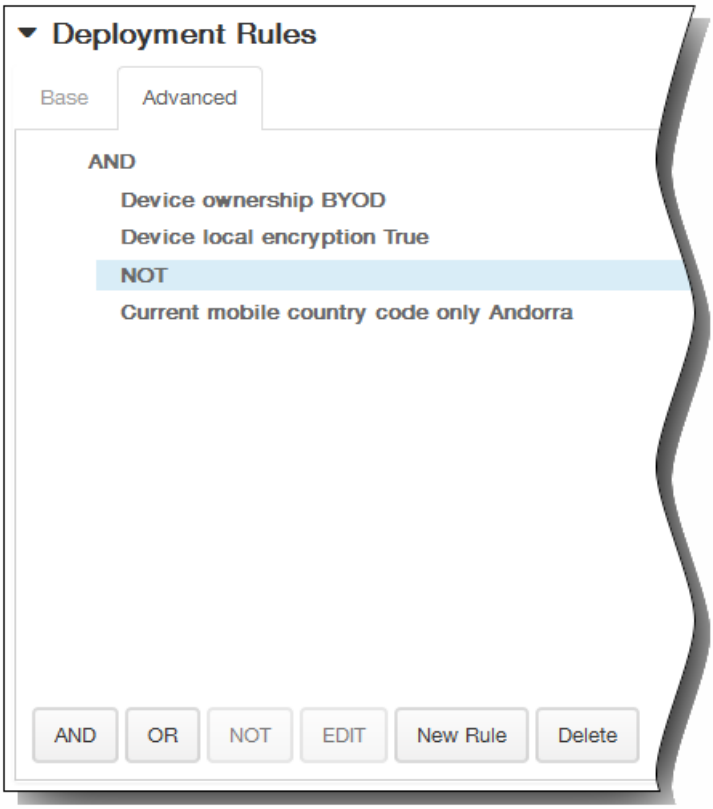
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist Alle.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



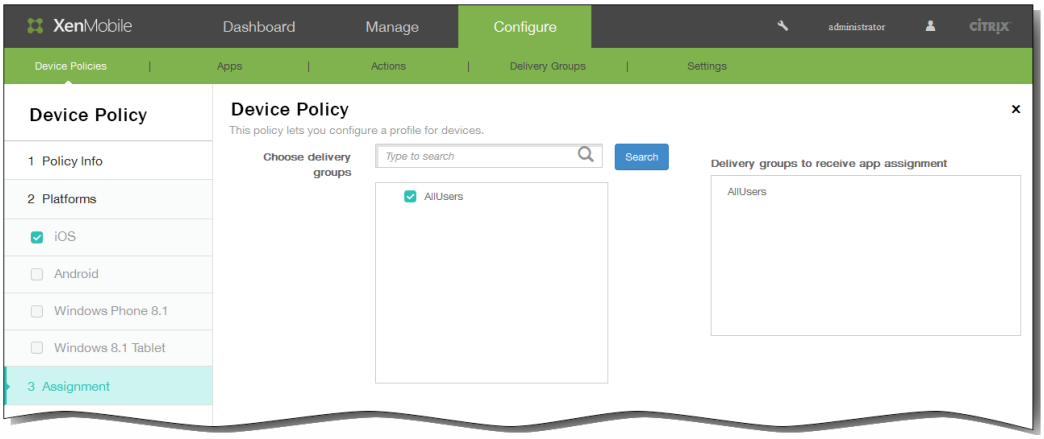
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.

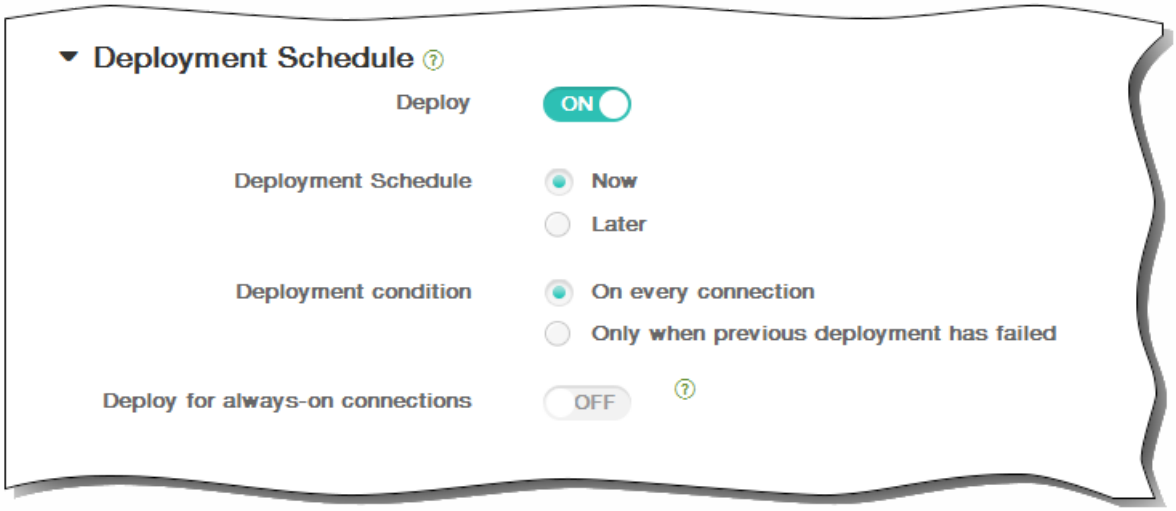


6. Klicken Sie auf Next. Die Seite Assignment für die Passcoderichtlinie wird angezeigt.
7. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen 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.

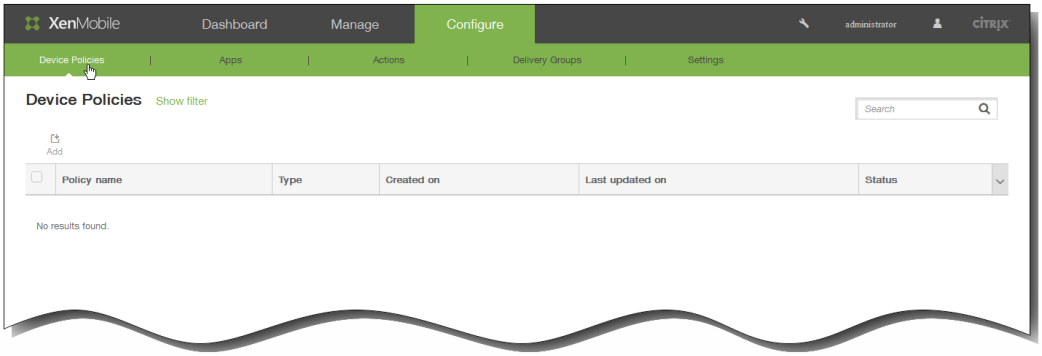
So fügen Sie eine Proxyrichtlinie für iOS-Geräte hinzu

May 05, 2016

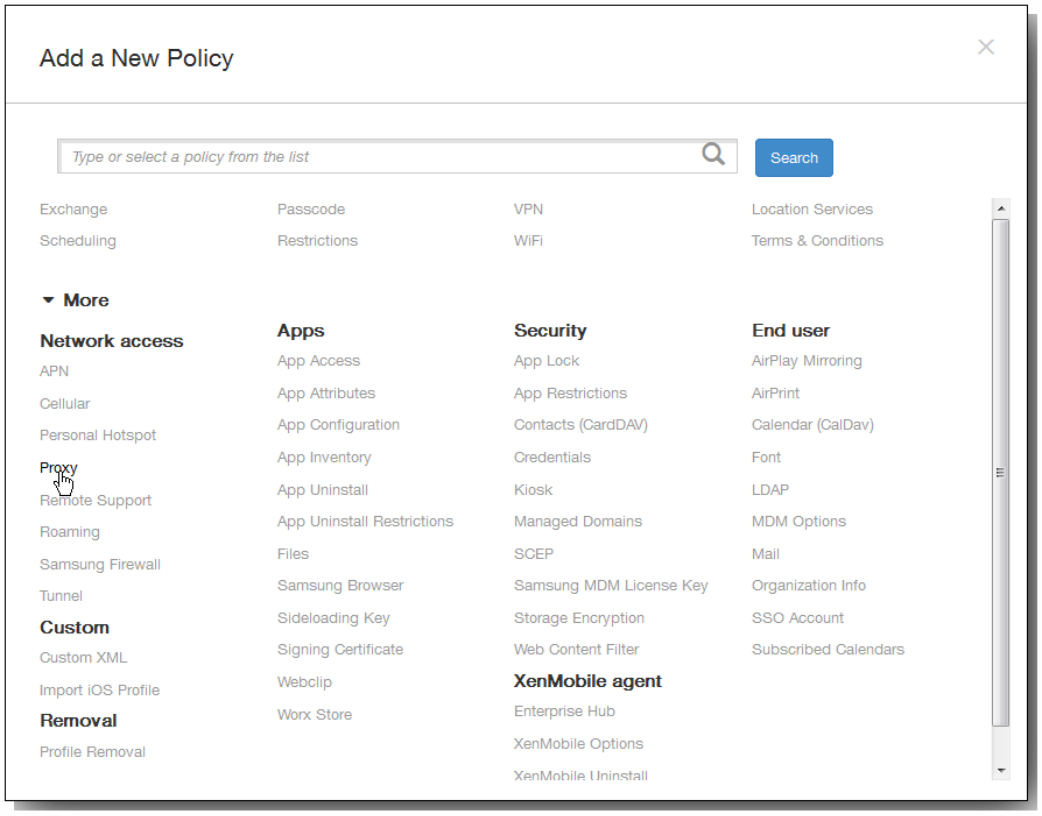
Sie können in XenMobile eine Richtlinie zum Festlegen globaler HTTP-Proxy-Einstellungen für Geräte mit iOS 6.0 oder höher hinzufügen. Sie können nur eine globale HTTP-Proxyrichtlinie pro Gerät bereitstellen.

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.

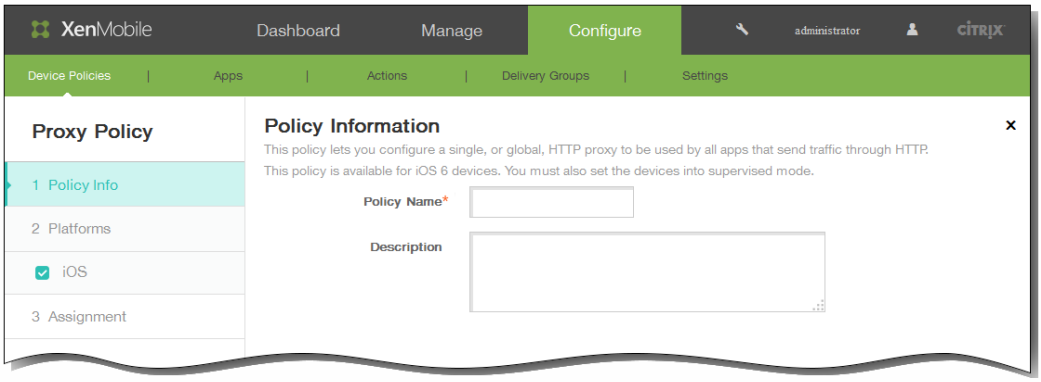
1. Klicken Sie in der XenMobile-Konsole auf ConfigureDevice Policies. Die Seite Device Policies wird angezeigt.



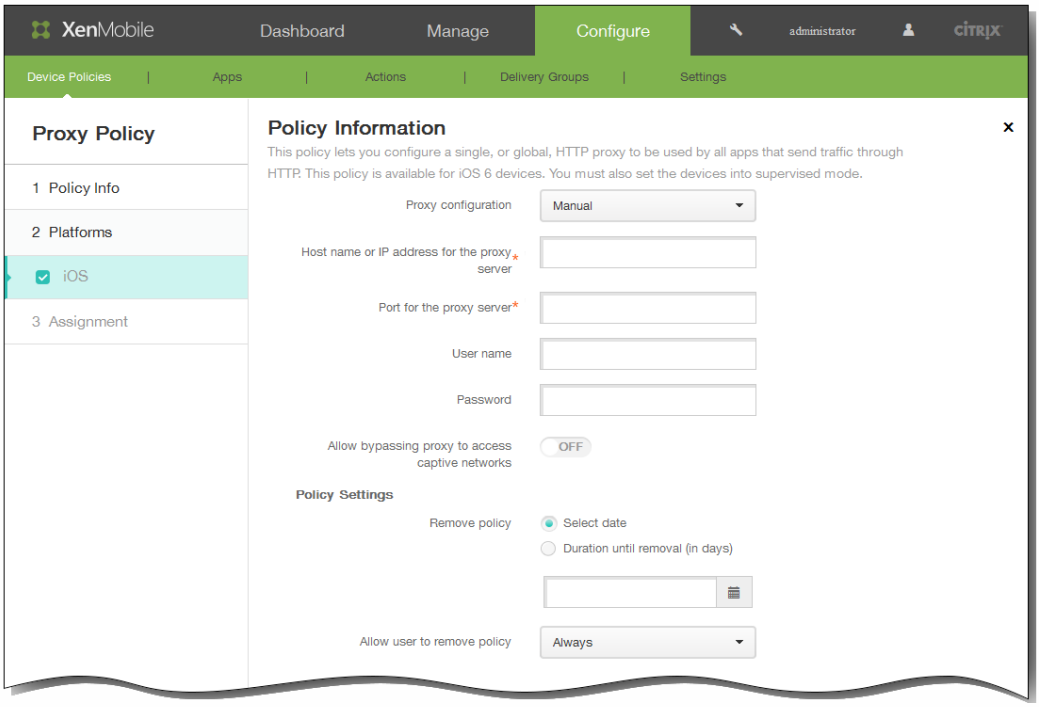
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



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.



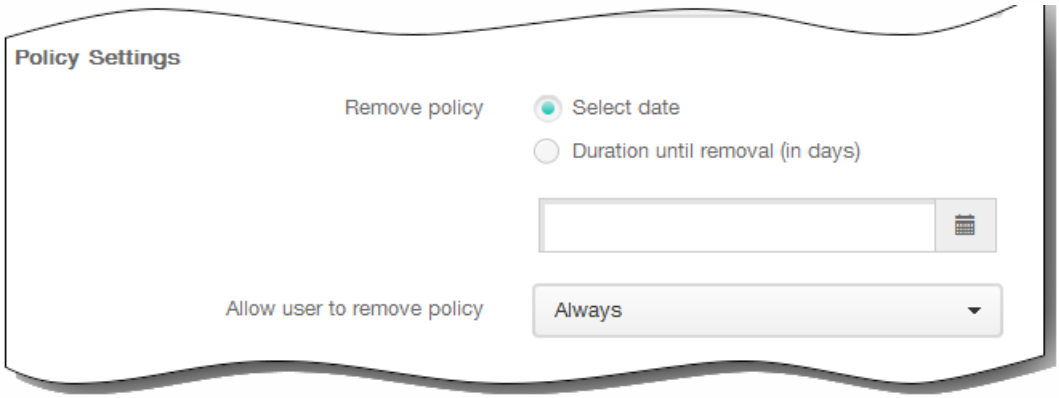
6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:
   1. Proxy configuration: Klicken Sie auf Manual oder Automatic, um festzulegen, wie der Proxy auf den Geräten der Benutzer konfiguriert wird. In der folgenden Tabelle werden die Optionen für jede Proxykonfiguration 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	–

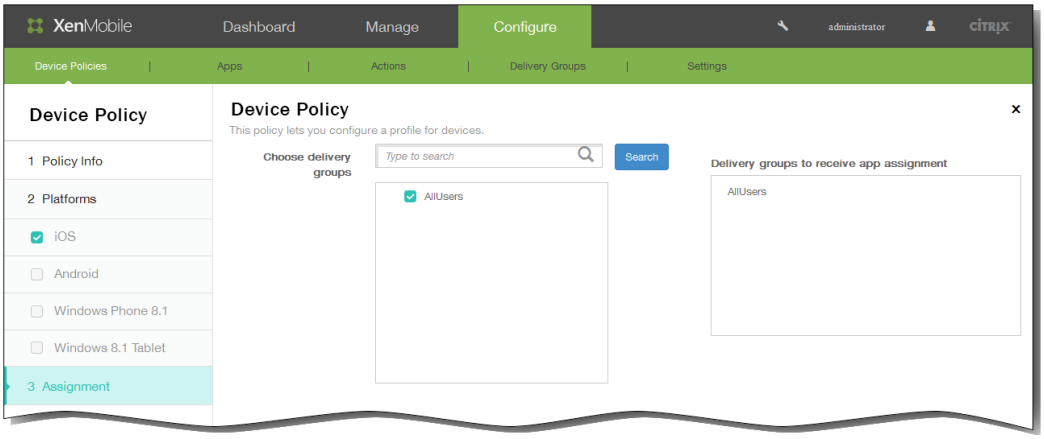
Port for the proxy server	Manuell Erforderlich	Automatisch –
User name	Optional	–
Password	Optional	–
Proxy PAC URL	–	Optional
Allow direct connection if PAC is unreachable	–	OFF

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.

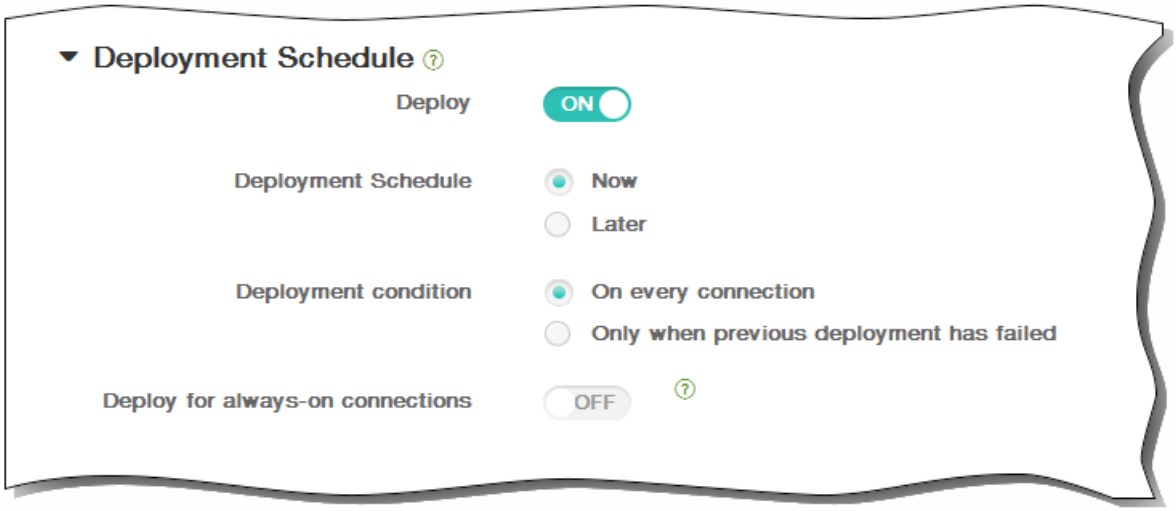


11. Klicken Sie auf Next. Die Seite Assignment für die Proxyrichtlinie wird angezeigt.
12. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen 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

May 05, 2016

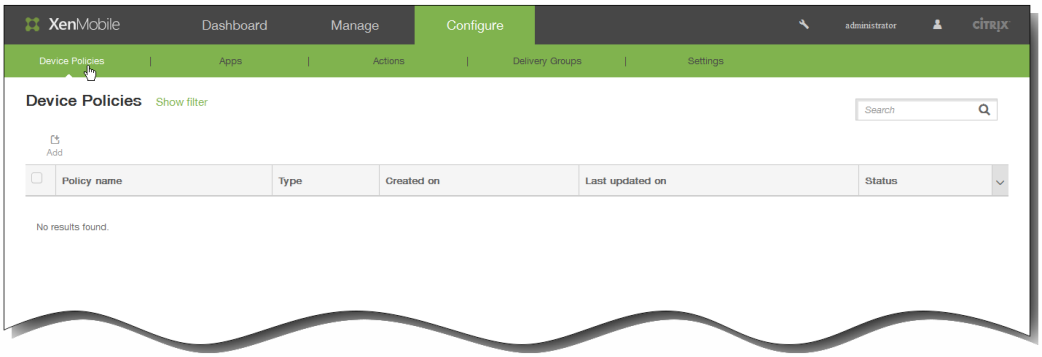
Sie erstellen eine Remotesupportrichtlinie in XenMobile, um Remotezugriff auf Samsung KNOX-Geräte zu erhalten. Sie können Support zweierlei Art konfigurieren:

- **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.

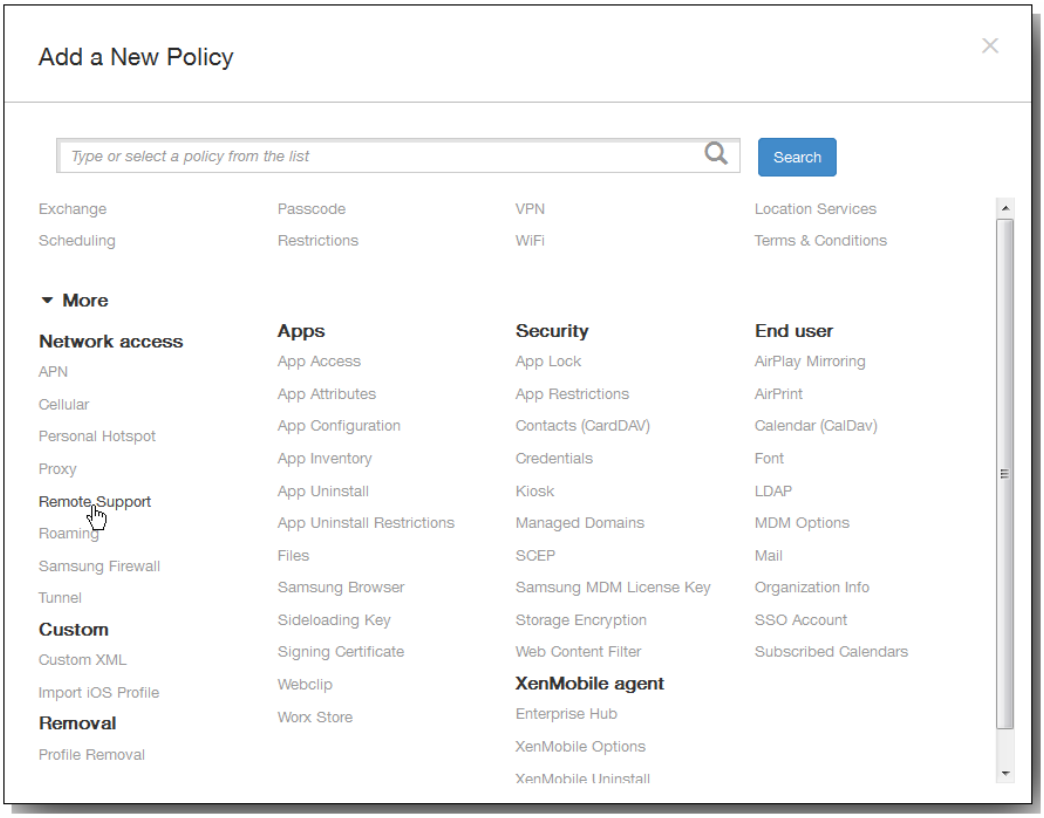
Hinweis: Zum Implementieren der Richtlinie müssen Sie die folgenden Schritte ausführen:

- 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

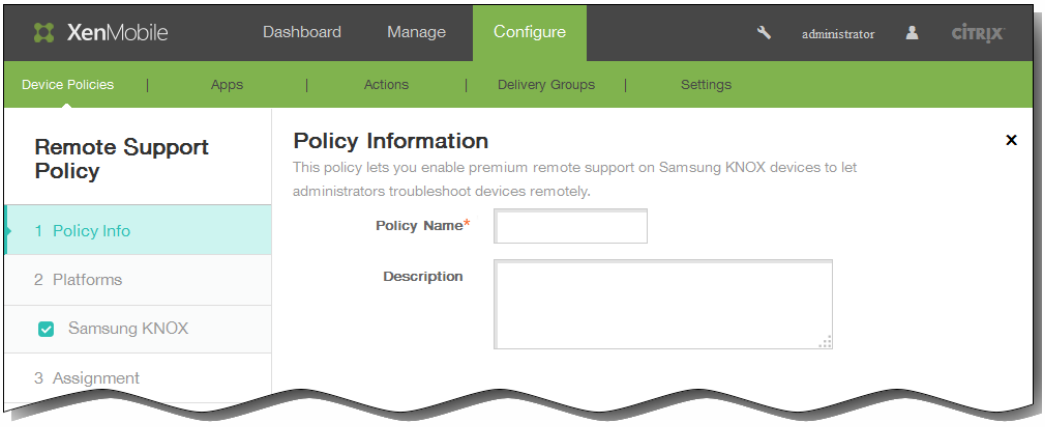
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



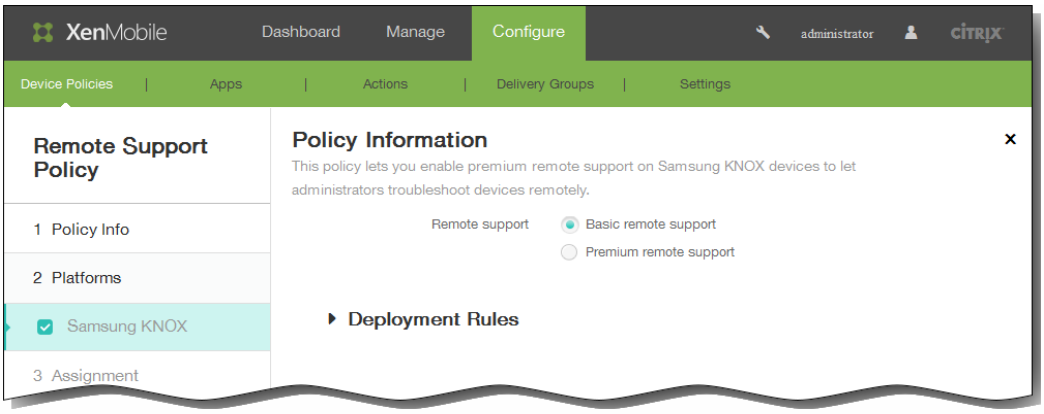
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



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

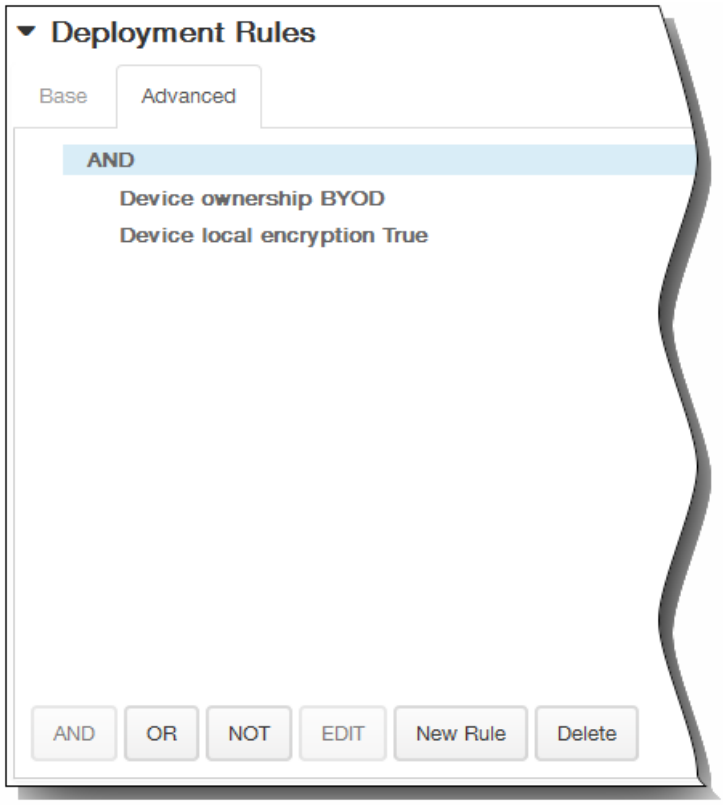


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite mit Plattforminformationen für Samsung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

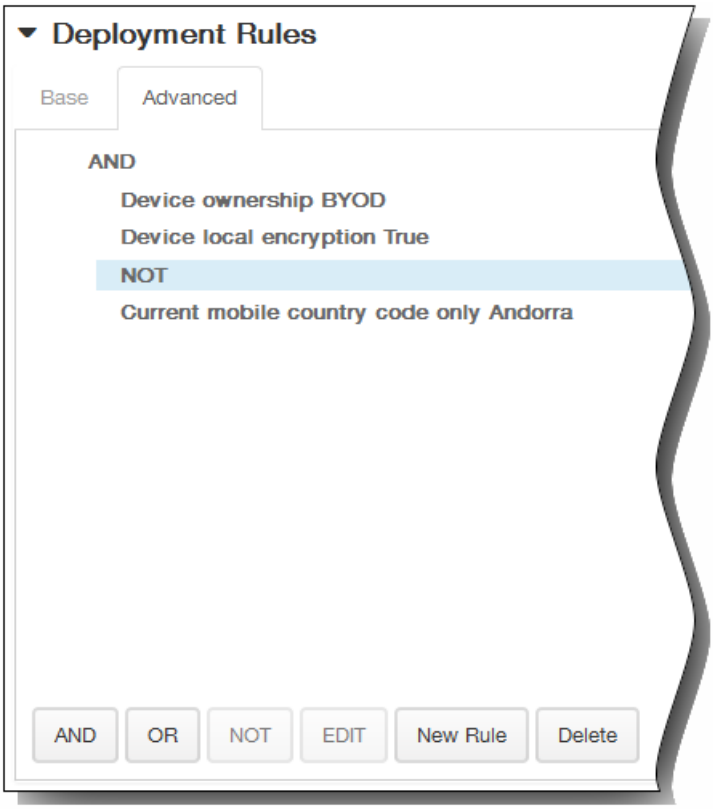
   1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
      1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
      2. Klicken Sie auf New Rule, um Bedingungen 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.



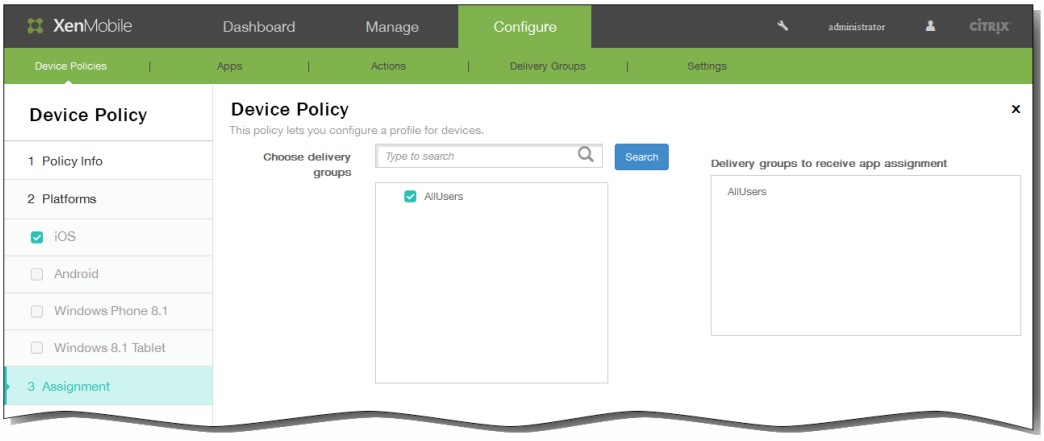
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



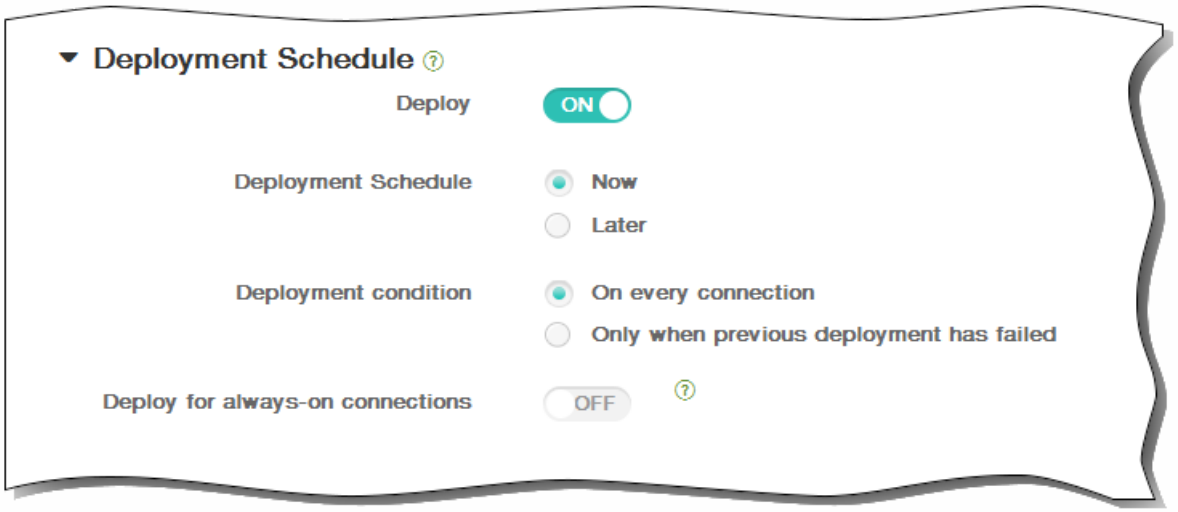
8. Klicken Sie auf Next. Die Seite Assignment für die Remotesupportrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.

Beschränkungsrichtlinien für Geräte

May 05, 2016

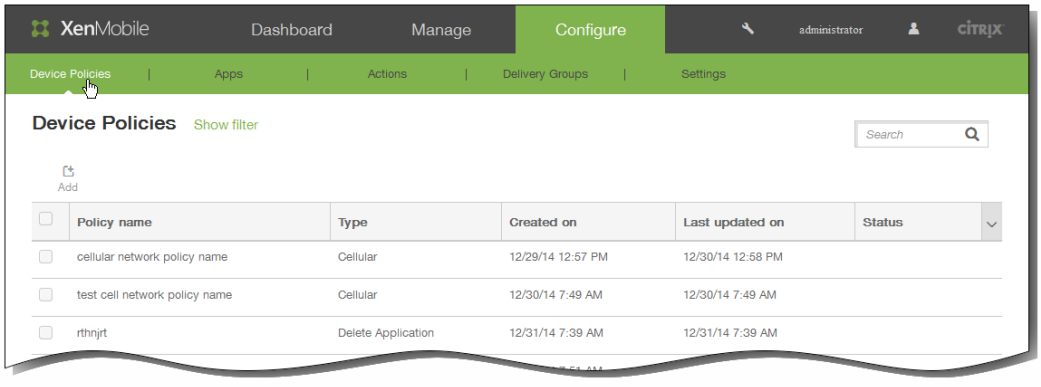
Sie können eine Geräterichtlinie in XenMobile hinzufügen, um Features und Funktionalität auf den Geräten der Benutzer einzuschränken. Einschränkungsrichtlinien können für folgende Plattformen konfiguriert werden: iOS, Samsung SAFE, Windows 8.1-Tablet, Windows Phone 8.1 und Amazon. Jede Plattform erfordert 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 (
— zugelassen
) festgelegt. Hauptausnahme bildet das Feature "Security - Force" dessen Standardwert OFF (
— nicht zugelassen
) ist.
Tipp: Alle Optionen, die Sie auf ON festlegen, bedeuten, dass die Benutzer den entsprechenden Vorgang ausführen oder das Feature verwenden
— können
. Beispiel:

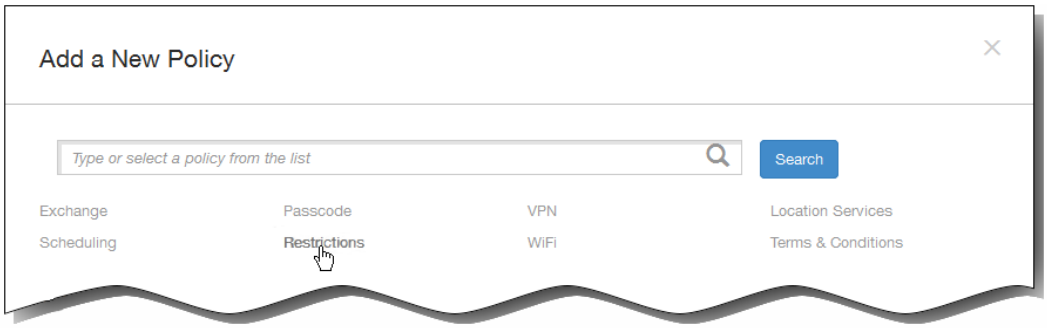
- Camera: Bei Auswahl von ON können Benutzer die Kamera auf Geräten verwenden. Bei Auswahl von OFF können Benutzer die Kamera auf Samsung SAFE-Geräten nicht verwenden.
- **Screen shots**: Bei Auswahl von ON können Benutzer Screenshots auf den Geräten erstellen. Bei Auswahl von OFF können Benutzer keine Screenshots auf den Geräten erstellen.

Hinweis: Einige iOS-Einschränkungen gelten nur für bestimmte iOS-Versionen (die Seite in der XenMobile-Konsole enthält dann einen entsprechenden Hinweis). Einige Optionen werden außerdem nur angewendet, wenn das Gerät im betreuten Modus ist. 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. 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.

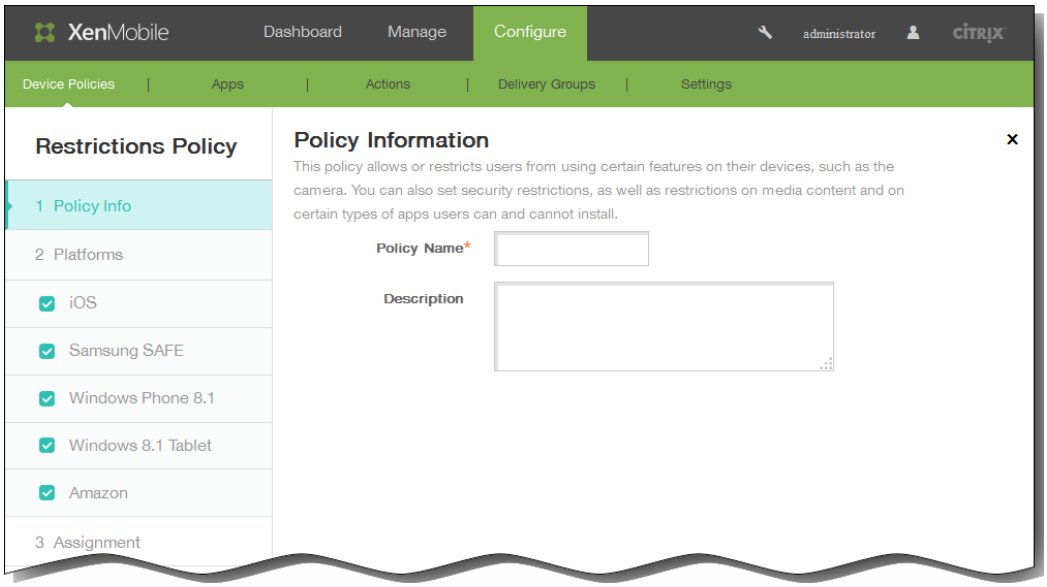
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



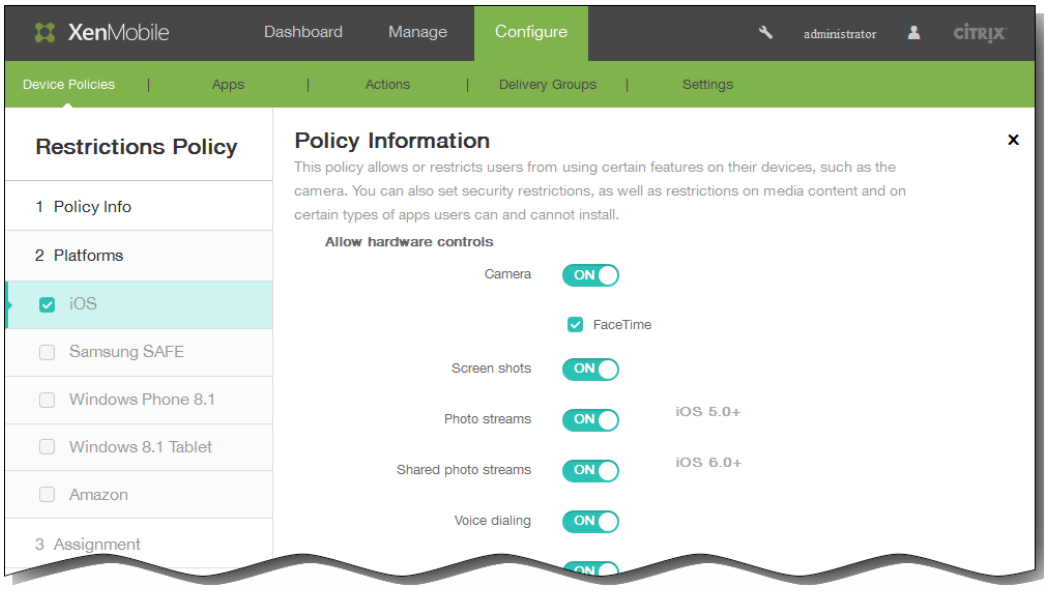
2. Klicken Sie auf Add. Die Seite Add a New Policy wird angezeigt.



3. Klicken Sie auf Restrictions.
   Die Seite Restrictions Policy wird angezeigt.



4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. 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.
   - Bei Auswahl von iOS konfigurieren Sie die folgenden Einstellungen:



- Allow hardware controls:

  Camera; FaceTime

  Screen shots

  Photo streams (verfügbar in iOS 5.0 oder höher)

  Shared photo streams (verfügbar in iOS 6.0 oder höher)

  Voice dialing

  Siri:
  - Allow while device is locked: Lassen Sie die Option gemäß dem Standardwert aktiviert oder deaktivieren Sie das Kontrollkästchen.
  - Siri profanity filter: Lassen Sie die Option gemäß dem Standardwert deaktiviert oder aktivieren Sie das Kontrollkästchen. In der Standardeinstellung ist das Feature eingeschränkt.

  Installing apps

- Allow apps:

  YouTube

  iTunes Store

  In-app purchases: Require iTunes password for purchases: Lassen Sie die Option gemäß dem Standardwert deaktiviert oder aktivieren Sie das Kontrollkästchen (verfügbar in iOS 5.0 oder höher). In der Standardeinstellung ist das Feature eingeschränkt.

  Safari:
  - Autofill: Lassen Sie die Option gemäß dem Standardwert aktiviert oder deaktivieren Sie das Kontrollkästchen.
  - Force fraud warning: Lassen Sie die Option gemäß dem Standardwert deaktiviert oder aktivieren Sie das Kontrollkästchen. In der Standardeinstellung ist das Feature eingeschränkt.
  - Enable JavaScript: Lassen Sie die Option gemäß dem Standardwert aktiviert oder deaktivieren Sie das

Kontrollkästchen.

- Block pop-ups: Lassen Sie die Option gemäß dem Standardwert deaktiviert oder aktivieren Sie das Kontrollkästchen. In der Standardeinstellung ist das Feature eingeschränkt.

Wählen Sie unter Accept cookies eine der folgenden Optionen:

- Always
- Never
- From visited sites only
  Die Standardeinstellung ist Always.

- Network - Allow iCloud actions:

  Documents and data sync (verfügbar in iOS 5.0 und höher)

  Device backup (verfügbar in iOS 5.0 und höher)

  Automatic sync while roaming

  iCloud keychain (verfügbar in iOS 7.0 und höher)

- Security - Force:

  Encrypted backups Standardwert ist OFF.

  Limited ad tracking (verfügbar in iOS 7.0 und höher) Standardwert ist OFF

  Passcode on first Airplay pairing (verfügbar in iOS 7.0 und höher) Standardwert ist OFF

- Security - Allow:

  Accepting untrusted SSL certificates (verfügbar in iOS 5.0 und höher)

  Automatic update to certificate trust settings (verfügbar in iOS 7.0 und höher)

  Documents from managed apps in unmanaged apps

  Documents from unmanaged apps in managed apps

  Diagnostic submission to Apple

  Touch ID to unlock device (verfügbar in iOS 7.0 und höher)

  Passbook notifications when locked (verfügbar in iOS 6.0 und höher)

  Handoff (verfügbar in iOS 8.0 und höher)

  iCloud sync for managed apps (verfügbar in iOS 8.0 und höher)

  Backup for enterprise books (verfügbar in iOS 8.0 und höher)

  Notes and highlights sync for enterprise books (verfügbar in iOS 8.0 und höher)

- Supervised only settings - Allow:

  Internet results in Spotlight (verfügbar in iOS 8.0 und höher)

Erase all content and settings (verfügbar in iOS 8.0 und höher)

Configuring restriction (verfügbar in iOS 8.0 und höher)

Installing configuration profiles (verfügbar in iOS 6.0 und höher)

AirDrop (verfügbar in iOS 7.0 und höher)

iMessage (verfügbar in iOS 6.0 und höher)

Siri user-generated content (verfügbar in iOS 7.0 und höher)

iBooks (verfügbar in iOS 6.0 und höher)

Removing apps (verfügbar in iOS 7.0 und höher)

Game Center (verfügbar in iOS 6.0 und höher)

- Add friends: Lassen Sie die Option gemäß dem Standardwert aktiviert oder deaktivieren Sie das Kontrollkästchen.
- Multiplayer gaming: Lassen Sie die Option gemäß dem Standardwert aktiviert oder deaktivieren Sie das Kontrollkästchen.

Modifying account settings (verfügbar in iOS 7.0 und höher)

Modifying app cellular data settings (verfügbar in iOS 7.0 und höher)

Modifying Find My Friends settings (verfügbar in iOS 7.0 und höher)

Pairing with non-Configurator hosts (verfügbar in iOS 7.0 und höher)

Single App bundle ID: Geben Sie in App name eine oder mehrere Apps ein.

- Security - Show in lock screen:

  Control Center (verfügbar in iOS 7.0 und höher)

  Notification (verfügbar in iOS 7.0 und höher)

  Today view

- Media content - Allow:

  Explicit music, podcasts, and iTunes U material

  Explicit sexual content in iBooks (verfügbar in iOS 6.0 und höher)

  Ratings region: Klicken Sie in der Liste auf ein Land. Der Standardwert ist United States.

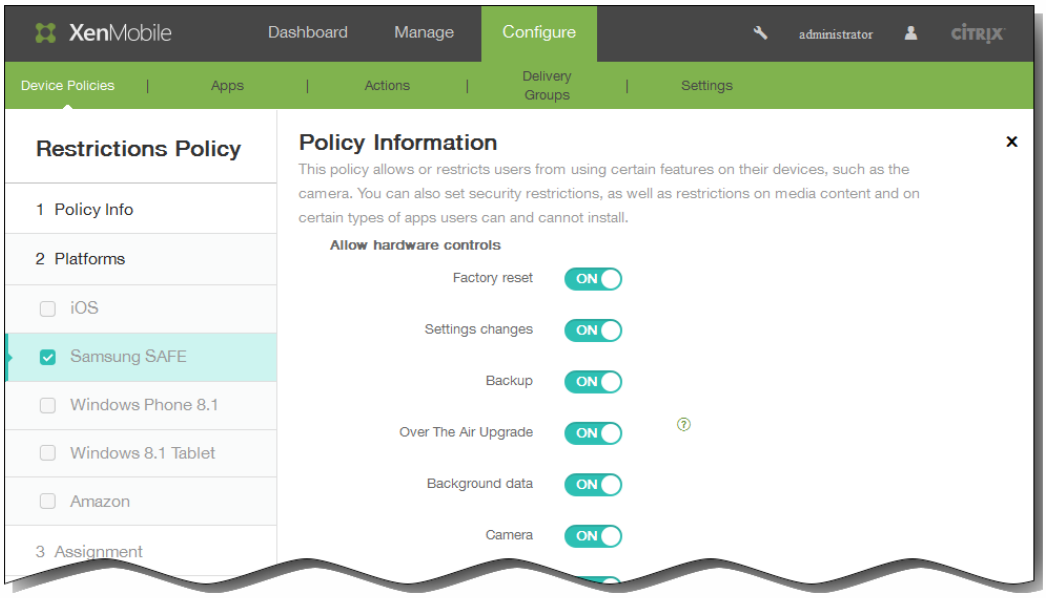
  Movies: Klicken Sie auf eine der folgenden Optionen: Allow all movies, Block movies, G, PG, PG-13, R, NC-17; Standardwert ist Allow all movies.

  TV Shows: Klicken Sie auf eine der folgenden Optionen: Allow all TV shows, Block TV shows, TV-Y, TV-Y7, TV-G, TV-PG, TV-PG14, TV-MA; Standardwert ist Allow all TV Shows.

  Apps: Klicken Sie auf eine der folgenden Optionen: Allow all apps, Block apps, 4+, 9+, 12+, or 17+; Standardwert ist Allow all apps.

- Bei Auswahl von Samsung SAFE konfigurieren Sie die folgenden Einstellungen:

  Hinweis: Einige Optionen sind nur unter Samsung Mobile Device Management API 4.0 oder höher verfügbar. Diese sind durch "MDM 4.0 and later" gekennzeichnet.



  - Allow hardware controls:

    Factory Reset

    Settings changes

    Backup

    Over The Air Upgrade (MDM 4.0 and later)

    Background data

    Camera

    Zwischenablage

    Clipboard share (MDM 4.0 and later)

    Home key

    Microphone

    Mock location

    NFC (Near Field Communication) (MDM 4.0 and later)

    Power off (MDM 4.0 and later)

    Screenshot

SD card

Voice Dialer (MDM 4.0 and later)

SBeam (MDM 4.0 and later)

SVoice (MDM 4.0 and later)

- Allow apps:

  Browser

  YouTube

  GooglePlay/Marketplace

  Allow No-Google Play apps

  Stop system app (MDM 4.0 and later)

- Network:

  Bluetooth; Tethering

  WiFi; Tethering, Direct (MDM 4.0 and later)

  Tethering

  Cellular data

  Allow roaming. Der Standardwert ist OFF.

  Only secure connections

  Android beam (MDM 4.0 and later)

  Audio record (MDM 4.0 and later)

  Video record (MDM 4.0 and later)

  Location services

  Limit by day (MB): Geben Sie die täglich zugelassene Anzahl MB ein. Der Standardwert ist 0, wodurch dieses Feature deaktiviert wird. (MDM 4.0 und höher)

  Limit by week (MB): Geben Sie die wöchentlich zugelassene Anzahl MB ein. Der Standardwert ist 0, wodurch dieses Feature deaktiviert wird. (MDM 4.0 und höher)

  Limit by month (MB): Geben Sie die monatlich zugelassene Anzahl MB ein. Der Standardwert ist 0, wodurch dieses Feature deaktiviert wird. (MDM 4.0 und höher)

- Allow USB actions:

  Debugging

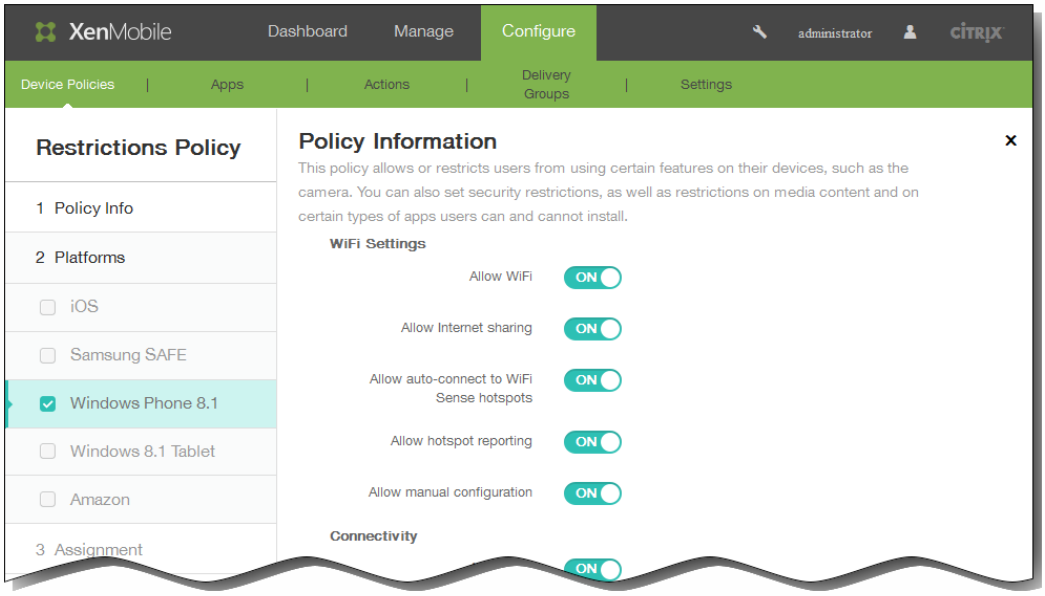
  Host storage

Mass storage

Kies media player

Tethering

- Bei Auswahl von Windows Phone 8.1 konfigurieren Sie die folgenden Einstellungen:



- WiFi Settings:

  Allow WiFi

  Allow Internet sharing

  Allow auto-connect to WiFiSense hotspots

  Allow hotspot reporting

  Allow manual configuration

- Connectivity:

  Allow NFC (Near Field Communication)

  Allow bluetooth

  Allow VPN over cellular

  Allow VPN over cellular while roaming

  Allow USB connection

  Allow cellular data roaming

- Accounts:

  Allow Microsoft account connection

  Allow non-Microsoft email

- Search:

  Allow search to use location

  Filter adult content (Standardwert ist OFF)

  Allow Bing Vision to store images

- System:

  Allow storage card

  Allow location services

  Allow use of camera

  Telemetry: Klicken Sie auf eine der folgenden Einstellungen: Allowed, Not Allowed, Allowed except for secondary data request. Der Standardwert ist Allowed.

- Security:

  Allow manual root certificate installation

  Require device encryption Der Standardwert ist OFF.

  Allow copy and paste

  Allow screen capture

  Allow voice recording

  Allow Save As of Office files

  Allow action center notifications

  Allow Cortana

  Allow sync of device settings

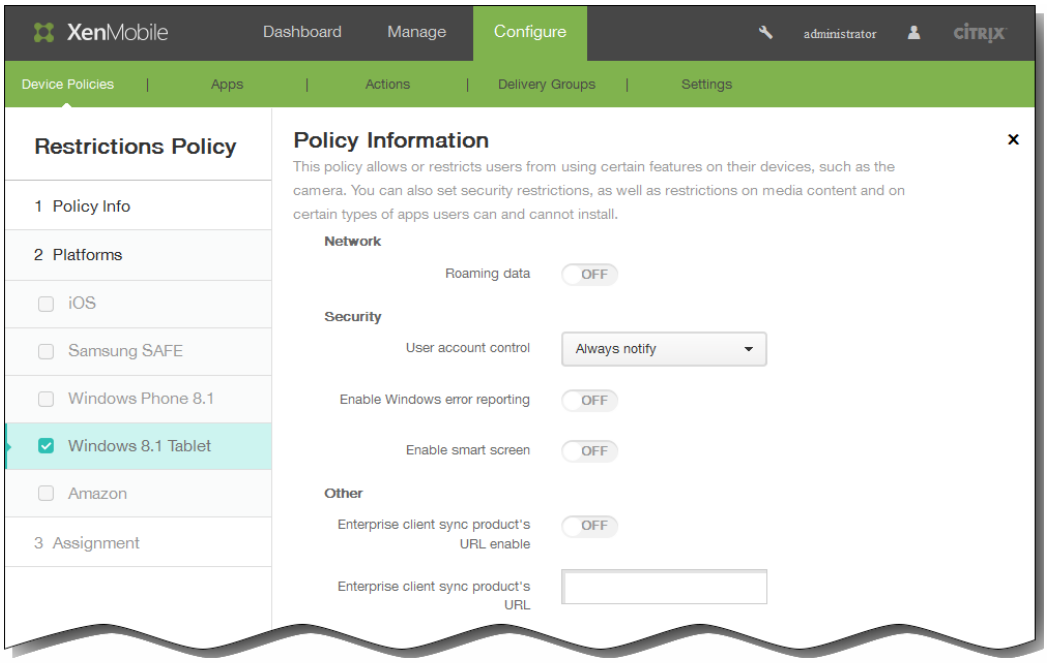
- Apps:

  Allow store access

  Allow developer unlock

  Allow web browser access

- Bei Auswahl von Windows 8.1 tablet konfigurieren Sie die folgenden Einstellungen:



- Network:

  Roaming data

- Security:

  User account control: Klicken Sie in der Liste auf eine der folgenden Einstellungen: Always notify, Notify app changes, Notify app changes (no dim), Never notify. Der Standardwert ist Always notify.

  Enable Windows error reporting

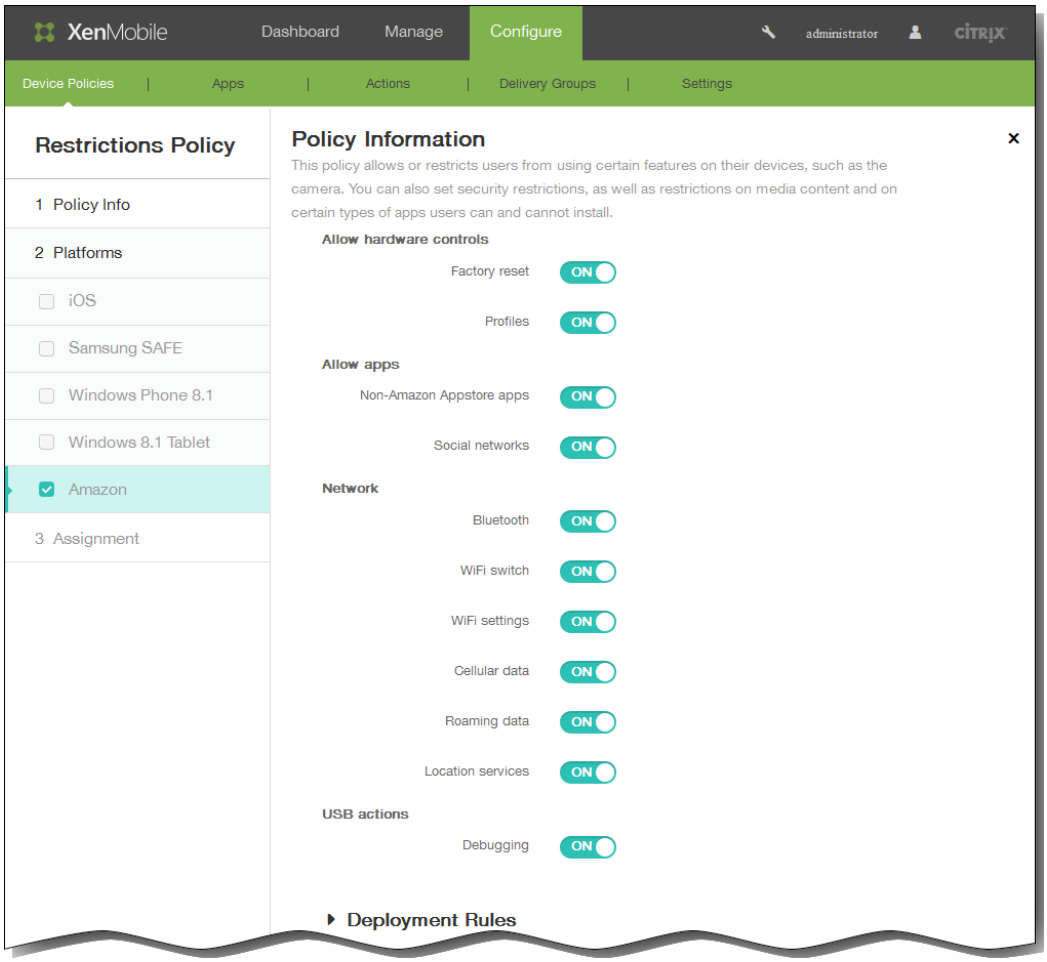
  Enable smart screen

- Other:

  Enterprise client sync product's URL enable

  Enterprise client sync product's URL: Geben Sie eine gültige URL ein.

- Bei Auswahl von Amazon konfigurieren Sie die folgenden Einstellungen:



- Allow hardware controls:

  Factory reset

  Profile

- Allow apps:

  Non-Amazon Appstore apps

  Social networks

- Network:

  Bluetooth

  WiFi switch

  WiFi settings

  Cellular data

  Roaming data

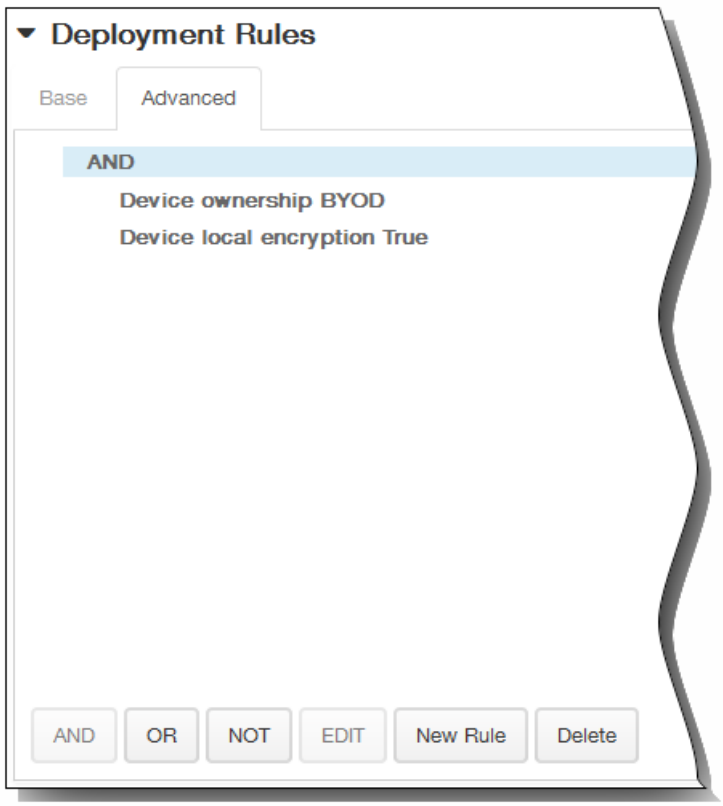
  Location services

- USB actions:

  Debugging

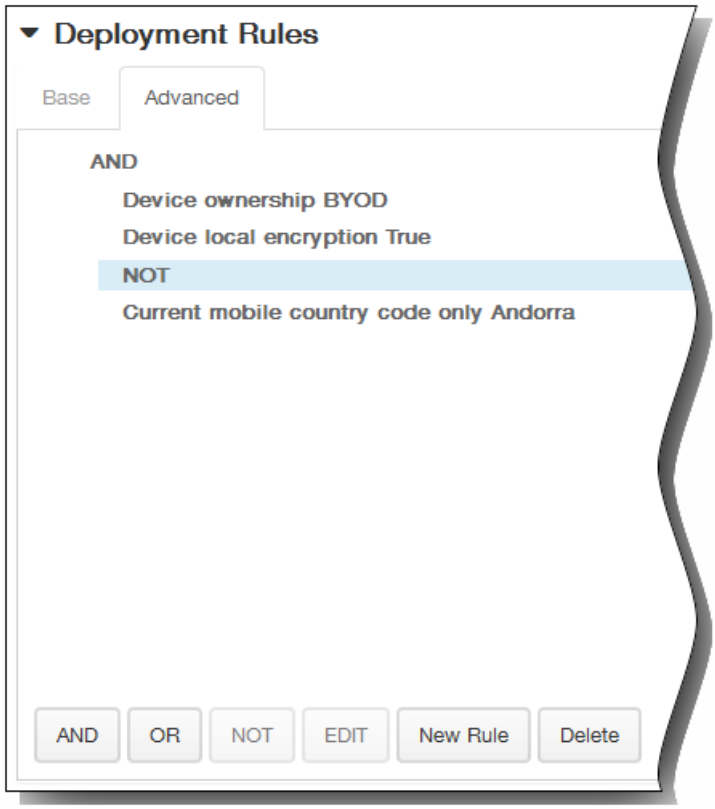
6. Erweitern Sie Deployment Rules und konfigurieren Sie dann die folgenden Einstellungen: Die Registerkarte Base wird standardmäßig angezeigt.

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.

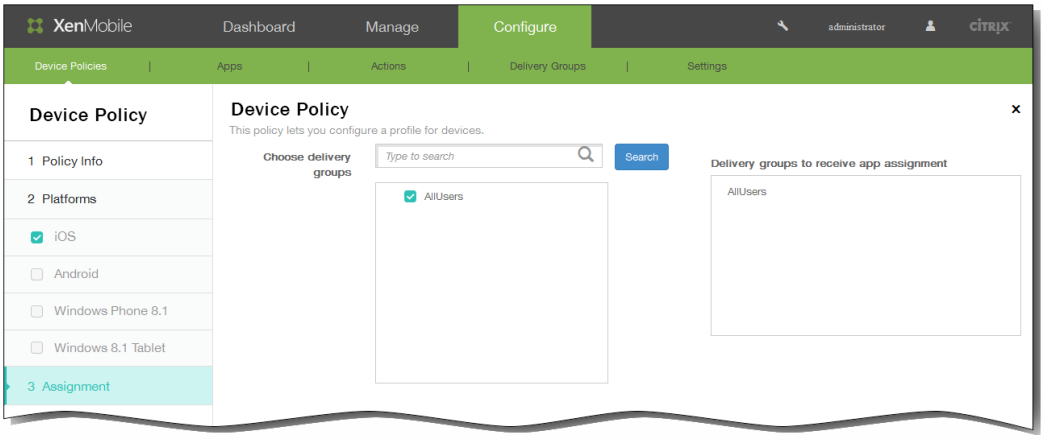


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.

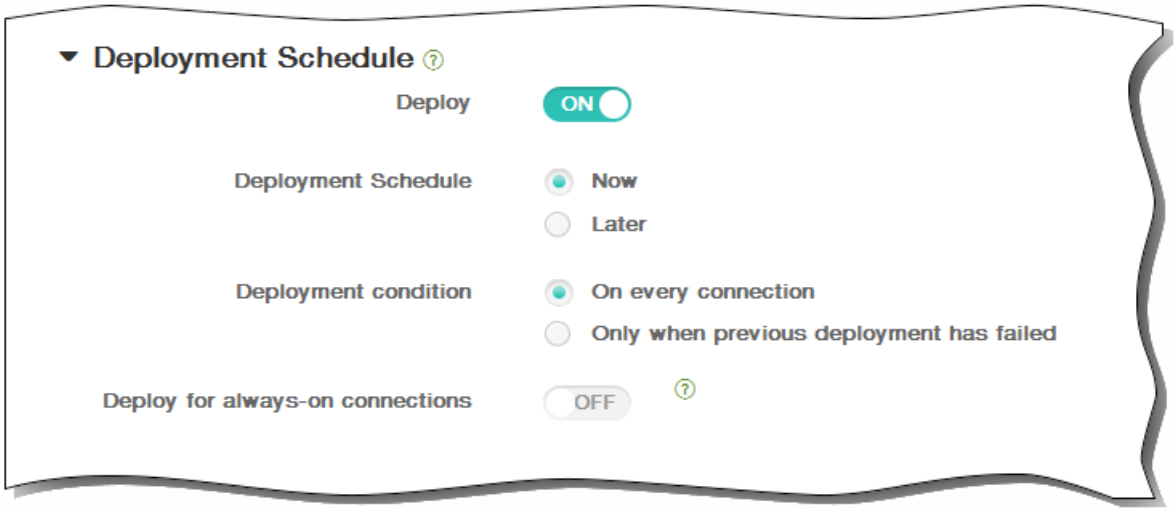


7. Nach Abschluss der Konfiguration der Einstellungen für eine oder mehrere Plattformen klicken Sie auf Next. Es wird die Seite Assigment angezeigt.
8. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen 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.



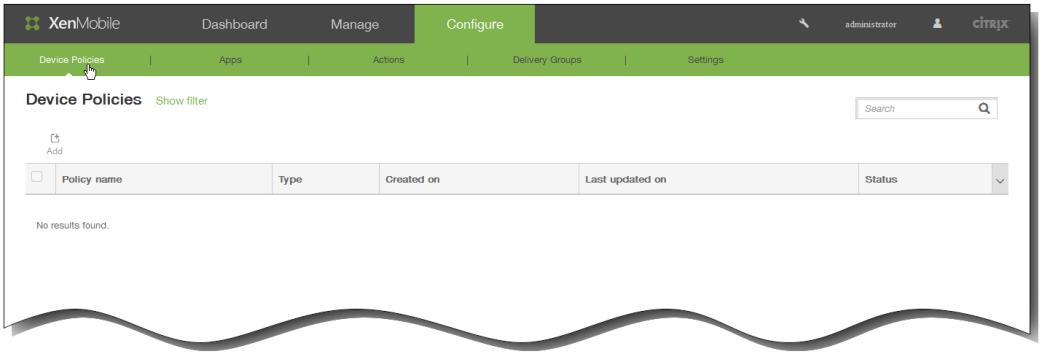
10. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Roamingrichtlinie für iOS-Geräte hinzu

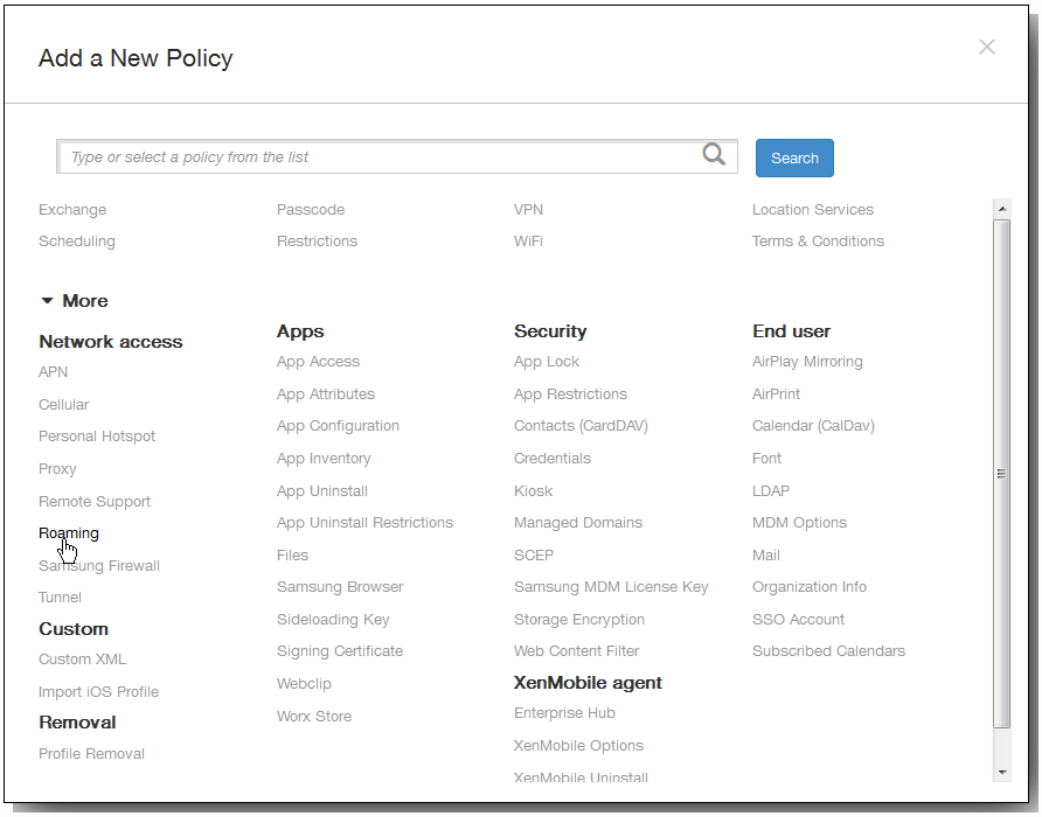
May 05, 2016

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.

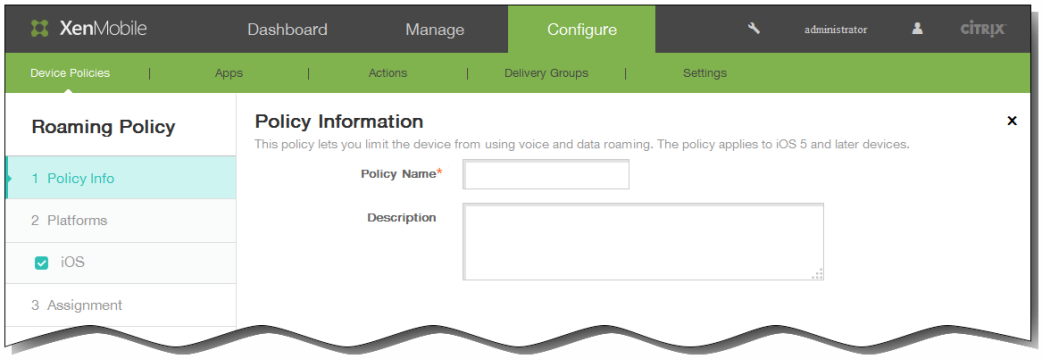
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



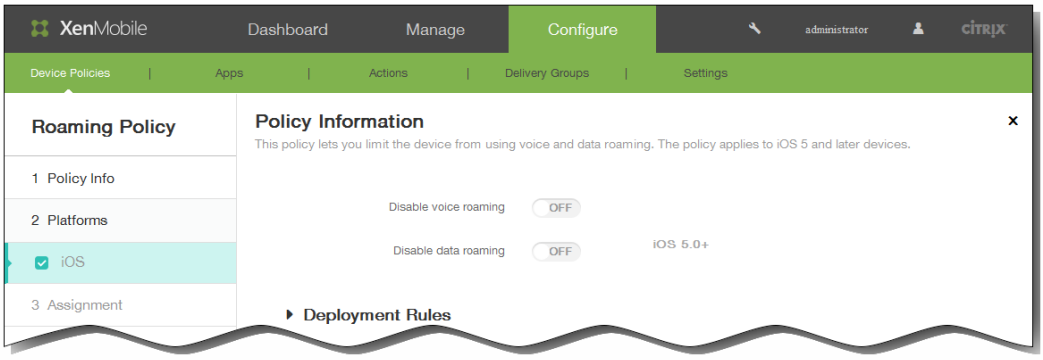
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



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

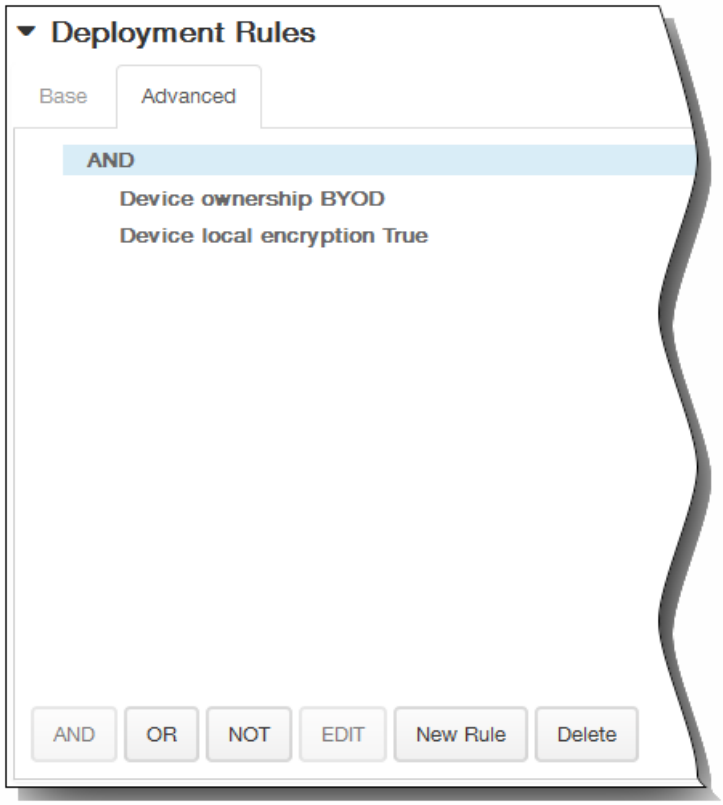


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite iOS Platform Information wird angezeigt.



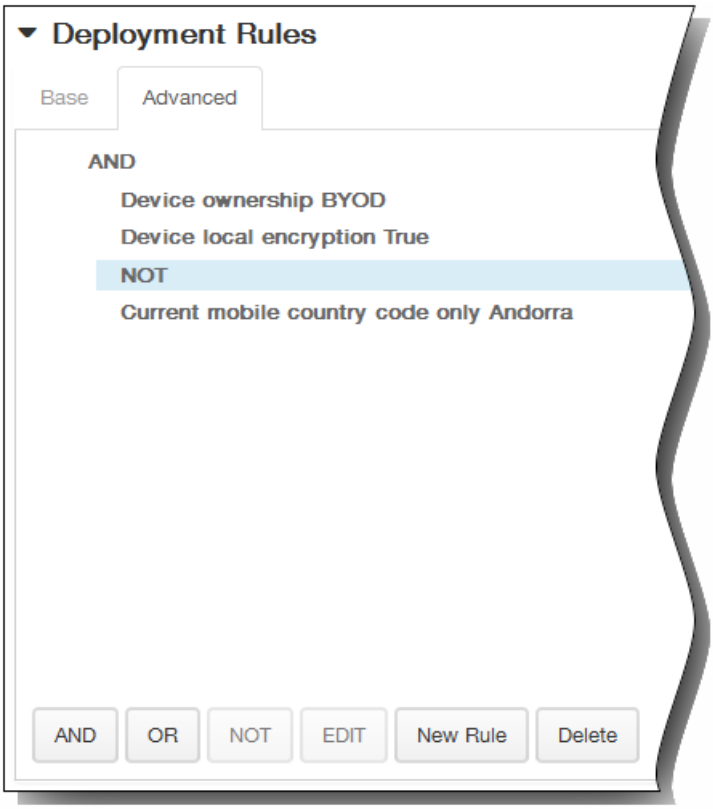
6. Geben Sie auf der Seite iOS Platform Information die folgenden Informationen ein:
   1. Disable voice roaming: Wählen Sie aus, ob das Sprachroaming deaktiviert werden soll. Wird diese Option deaktiviert, dann wird Datenroaming automatisch auch deaktiviert. Die Standardeinstellung ist OFF, Sprachroaming 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 noch einmal 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.

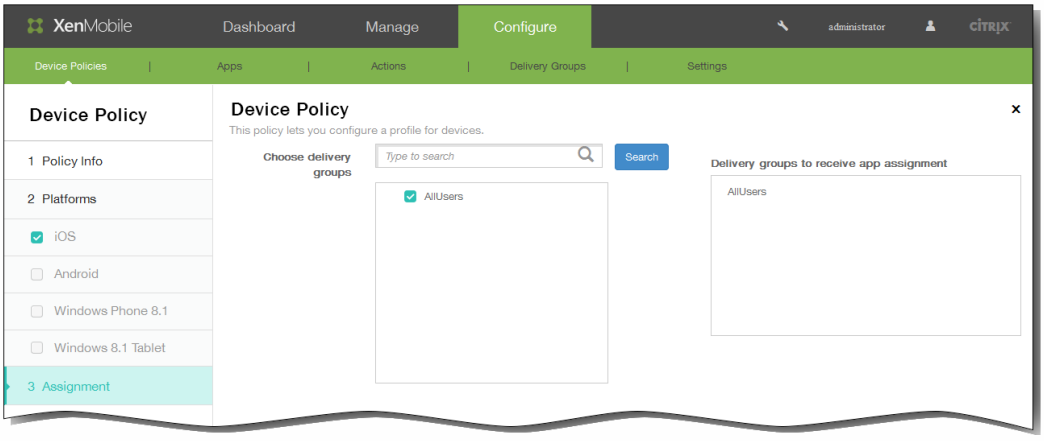


   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
    1. Klicken Sie auf AND, OR oder NOT.
    2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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 noch einmal 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.



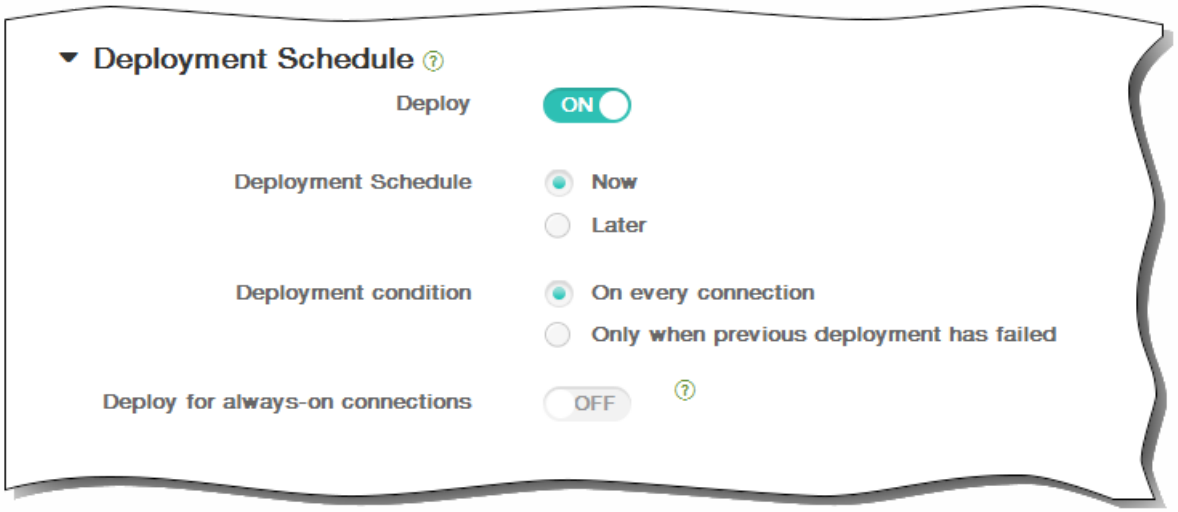
8. Klicken Sie auf Next. Die Seite Assignment für die Roamingrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen 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.



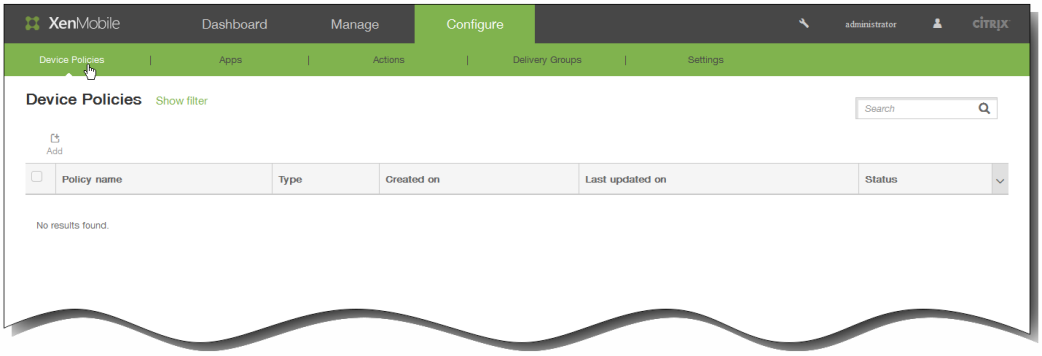
11. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine SCEP-Richtlinie für iOS-Geräte hinzu

May 05, 2016

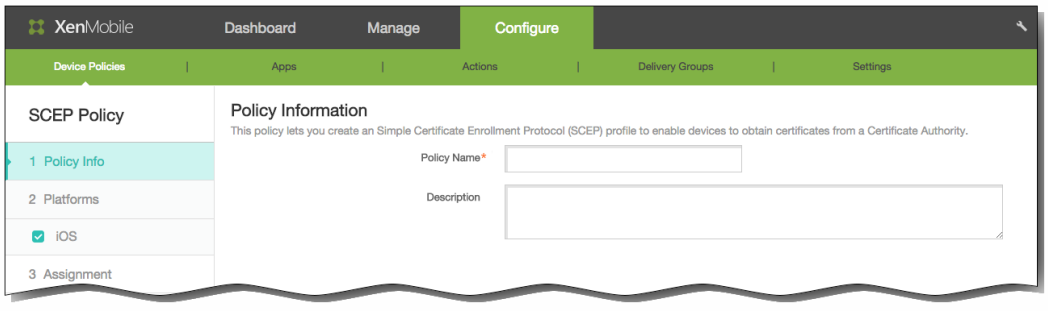
Mit dieser Richtlinie können Sie iOS-Geräte für den Empfang eines Zertifikats über Simple Certificate Enrollment Protocol (SCEP) von einem externen SCEP-Server konfigurieren. Wenn Sie Zertifikate mit SCEP von einer mit XenMobile verbundenen PKI auf Geräten bereitstellen möchten, erstellen Sie eine PKI-Entität 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.

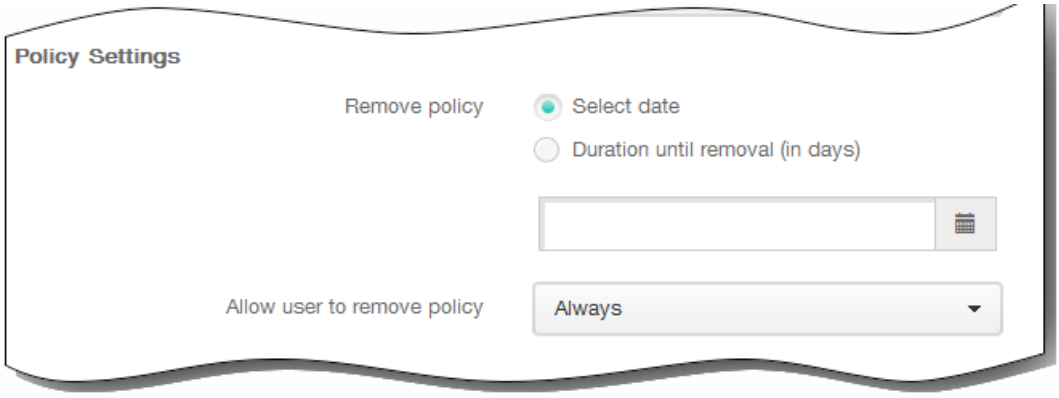
3. Klicken Sie auf der Seite Add a New Policy auf More und dann unter Security auf SCEP.
   Die Seite SCEP Policy wird angezeigt.



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.

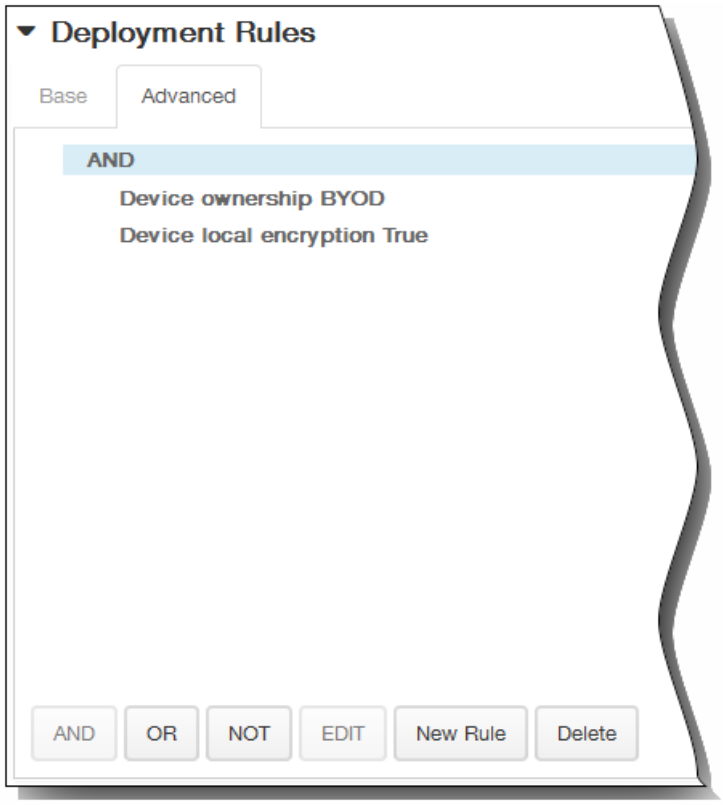
5. Klicken Sie auf Next.
   Die Seite iOS Platform Information wird angezeigt.

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. Beispiel: /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar steht für [[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]. Sie können OIDs in Form von Zahlen mit Punkten und Abkürzungen für Land (C), Ort (L), Staat (ST), Unternehmen (O), Organisationseinheit (OU) und allgemeinen Namen (CN) darstellen.
   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.

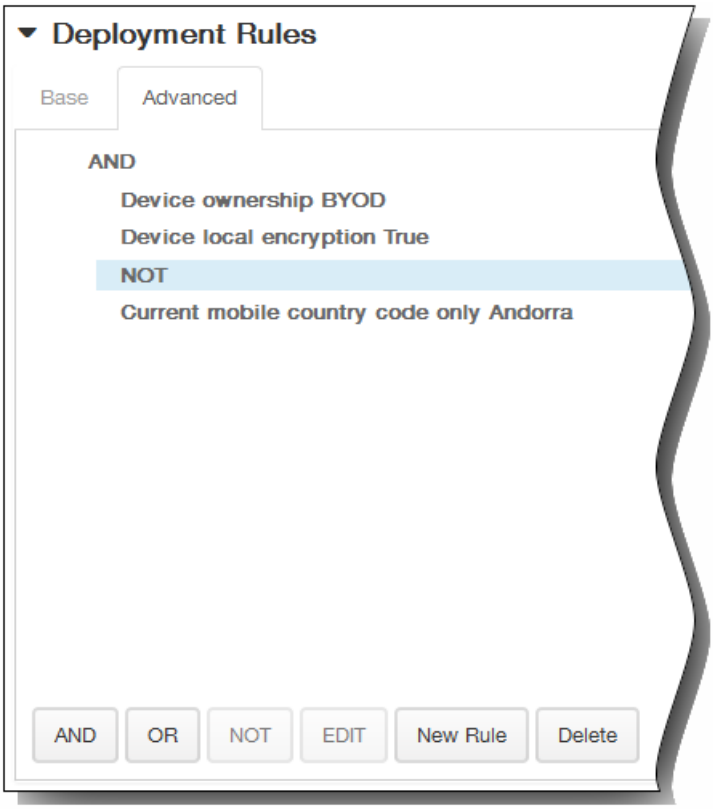
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen 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.



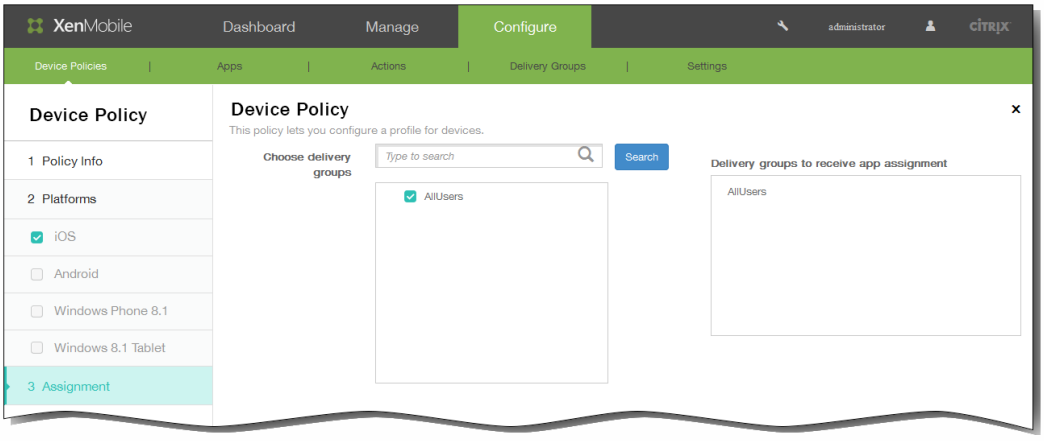
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



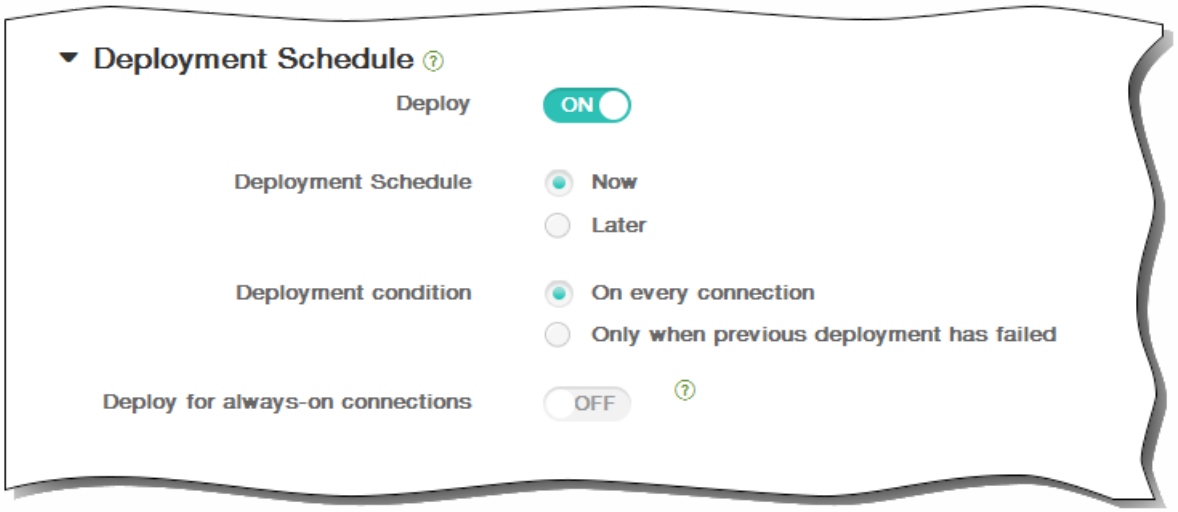
12. Klicken Sie auf Next. Die Seite Assignment für die SCEP-Richtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen 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

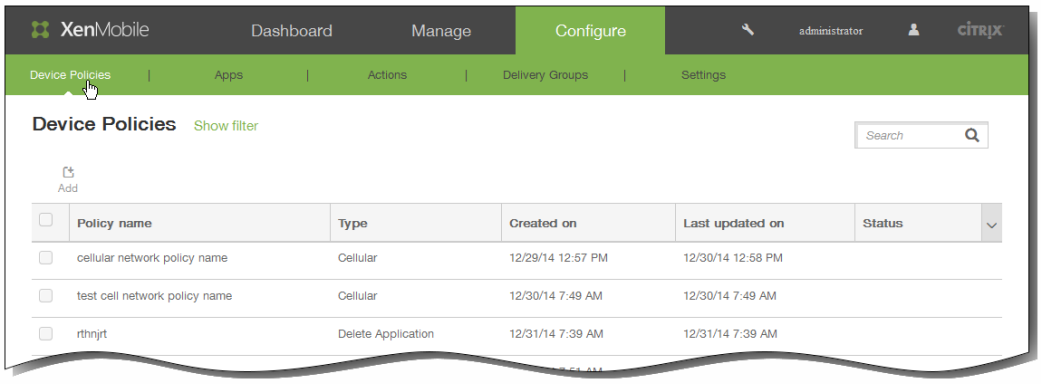
May 05, 2016

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.

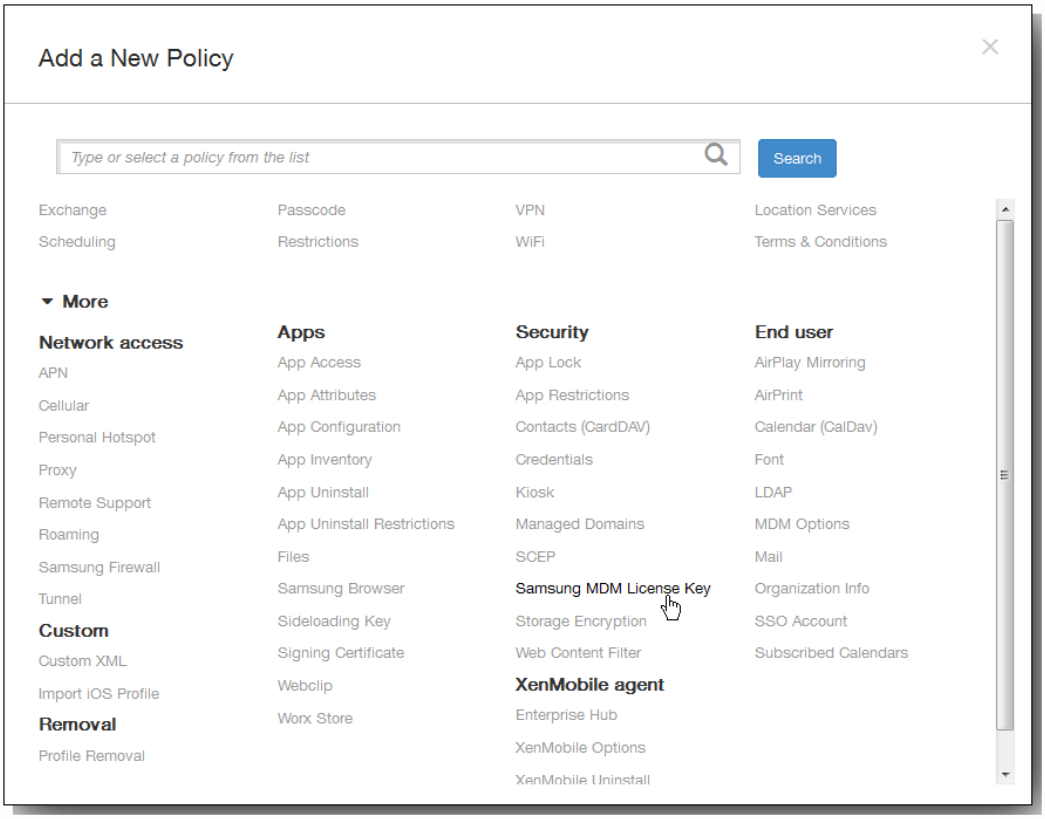
Bevor Sie SAFE-Richtlinien und -Einschränkungen bereitstellen können, müssen Sie die SAFE-APIs durch Bereitstellen des integrierten Samsung Enterprise License Management-Schlüssels (ELM) auf Geräten aktivieren. Zum Aktivieren der Samsung KNOX-API müssen Sie zusätzlich zur Bereitstellung des ELM-Schlüssels 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.

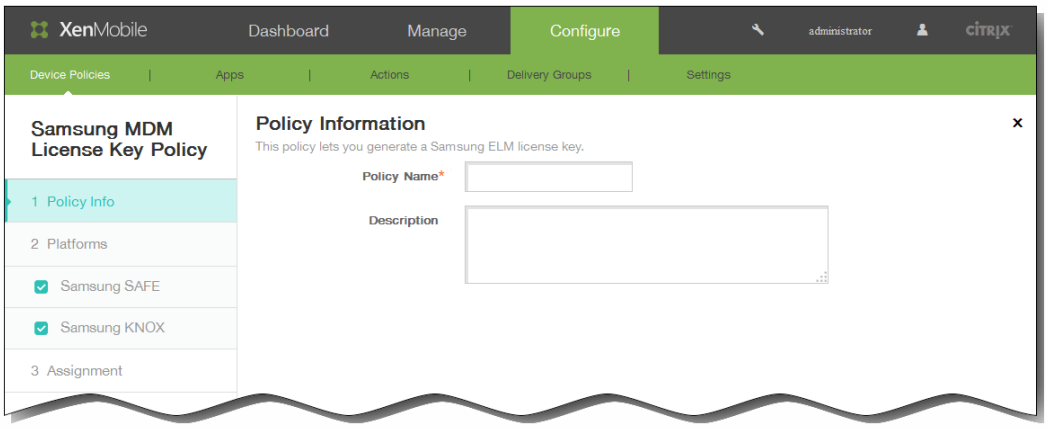
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



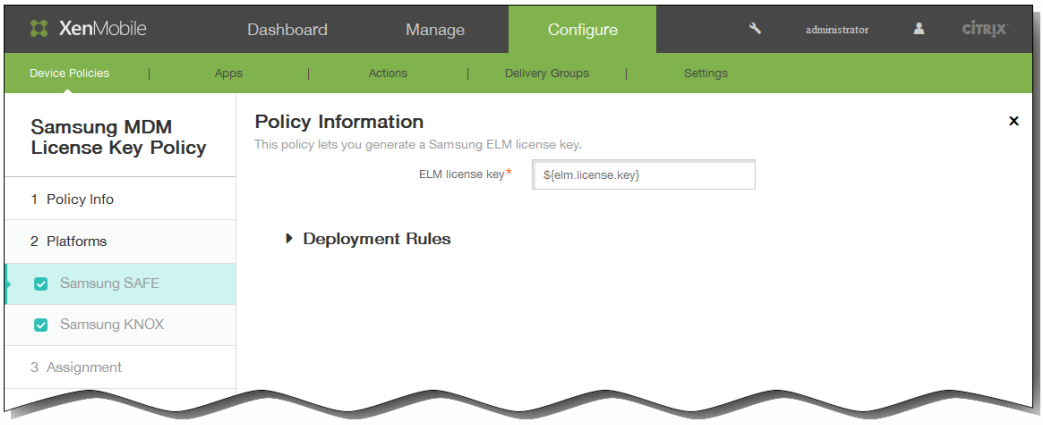
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter Security auf Samsung MDM Licence Key. Die Seite Samsung MDM License Key Policy wird angezeigt.

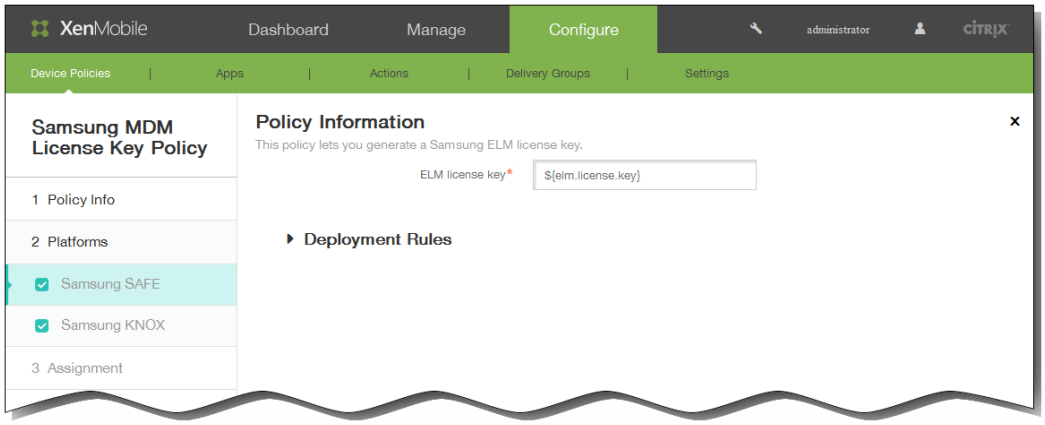


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Policy Platforms wird angezeigt.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

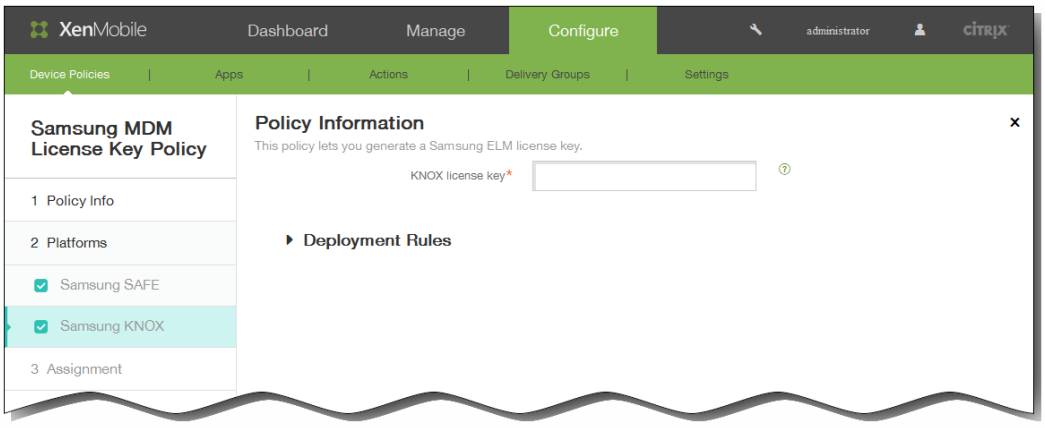


6. Wählen Sie unter Platforms die Samsung-Plattformen aus, für die Sie diese Richtlinie erstellen möchten. Deaktivieren Sie alle Plattformen, die Sie nicht in die Richtlinie einschließen möchten.

   - 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:

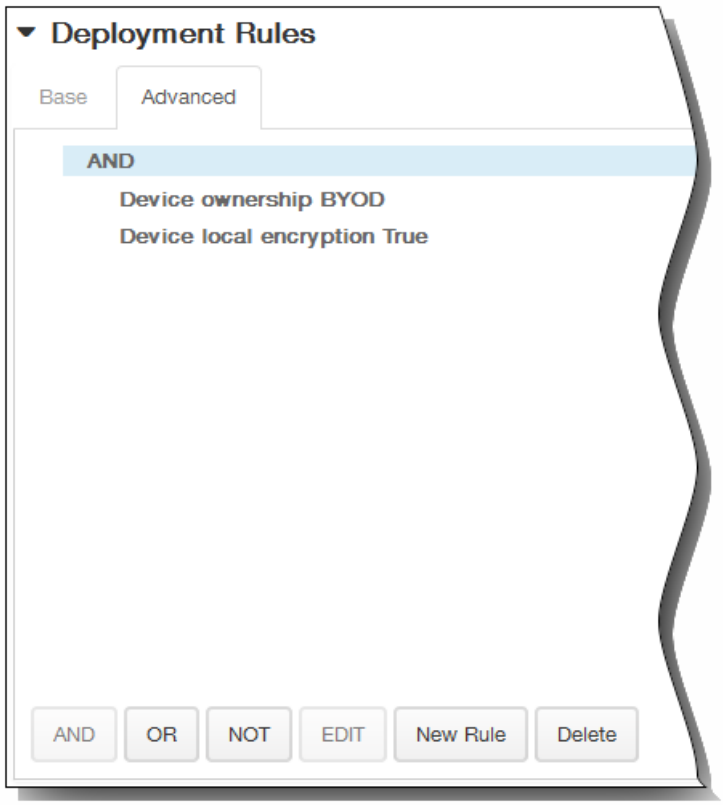


   - Bei Auswahl von Samsung KNOX geben Sie für KNOX license key den 25-stelligen KNOX-Lizenzschlüssel ein:



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

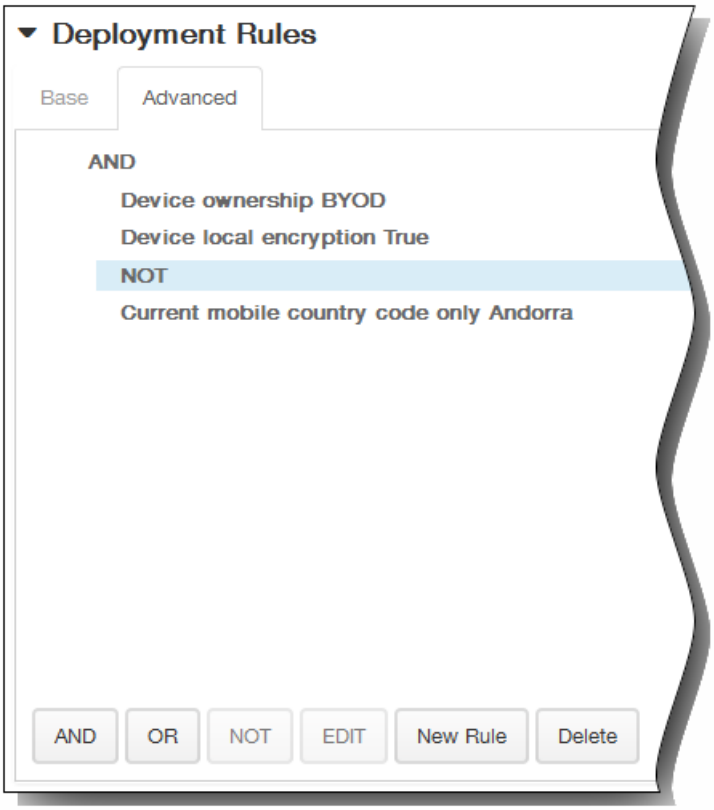
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



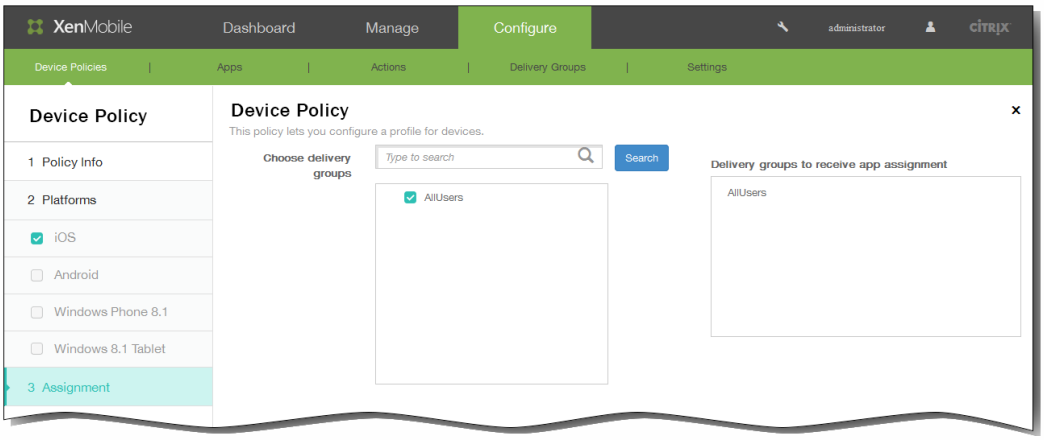
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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.



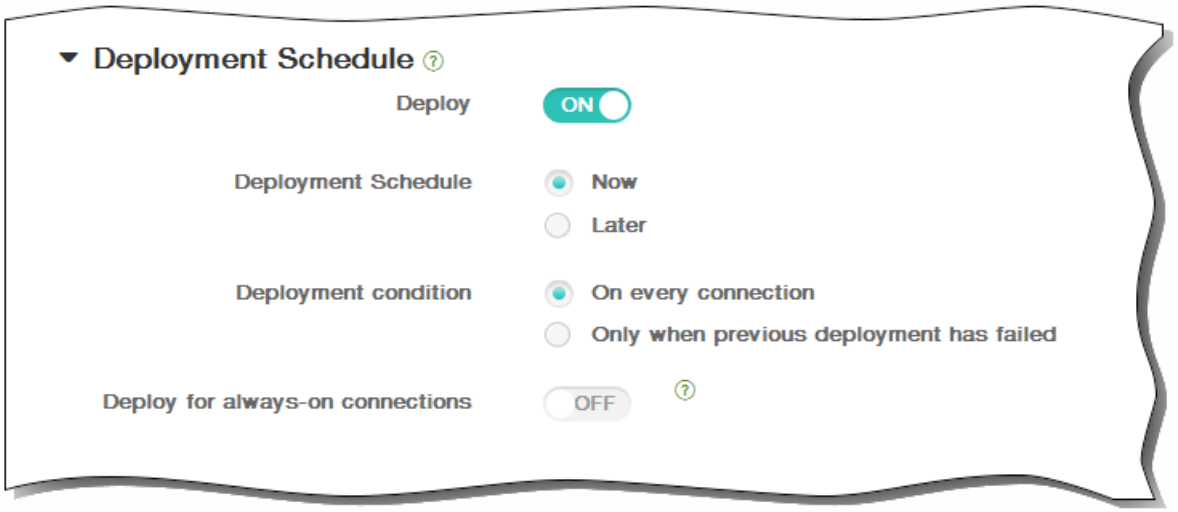
8. Klicken Sie auf Next. Die Seite Samsung MDM License Key Policy wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden 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

May 05, 2016

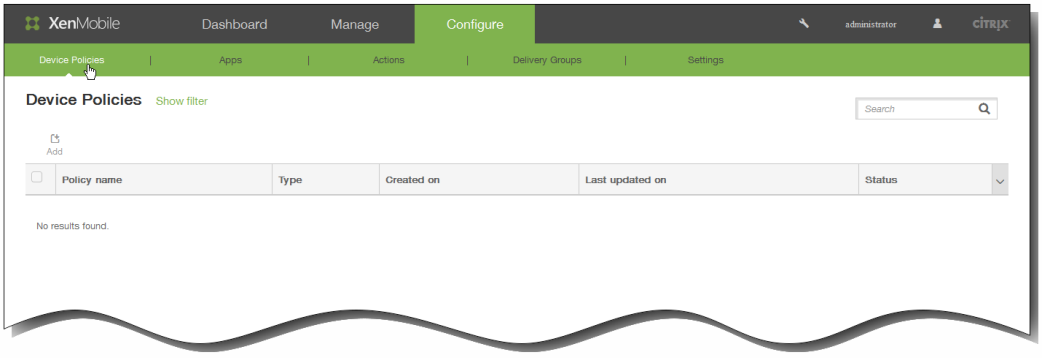
Sie erstellen Speicherverschlüsselungsrichtlinien in XenMobile, um den internen und externen Speicher zu verschlüsseln und – je nach Gerät –, um zu verhindern, dass Benutzer die Gerätespeicherkarte verwenden.

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:

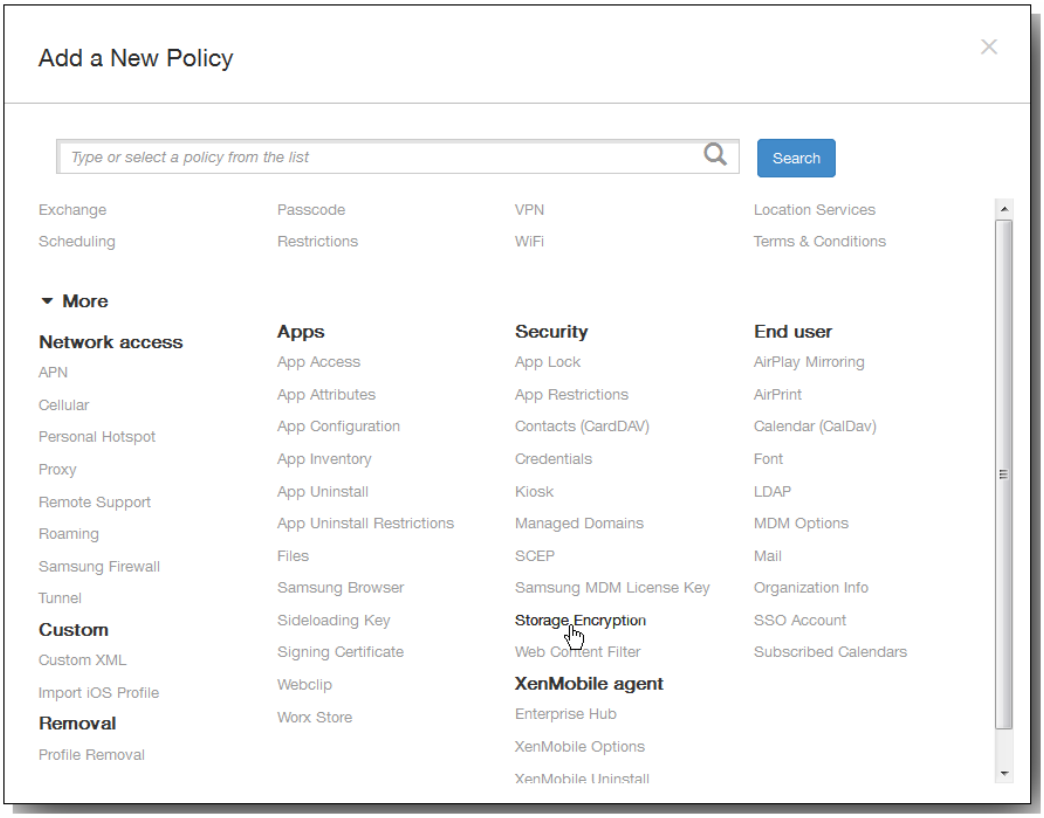
Hinweis: Vergewissern Sie sich vor der Konfiguration dieser Richtlinie, dass bei Samsung SAFE-Geräten die folgenden Anforderungen erfüllt sind:

- 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.

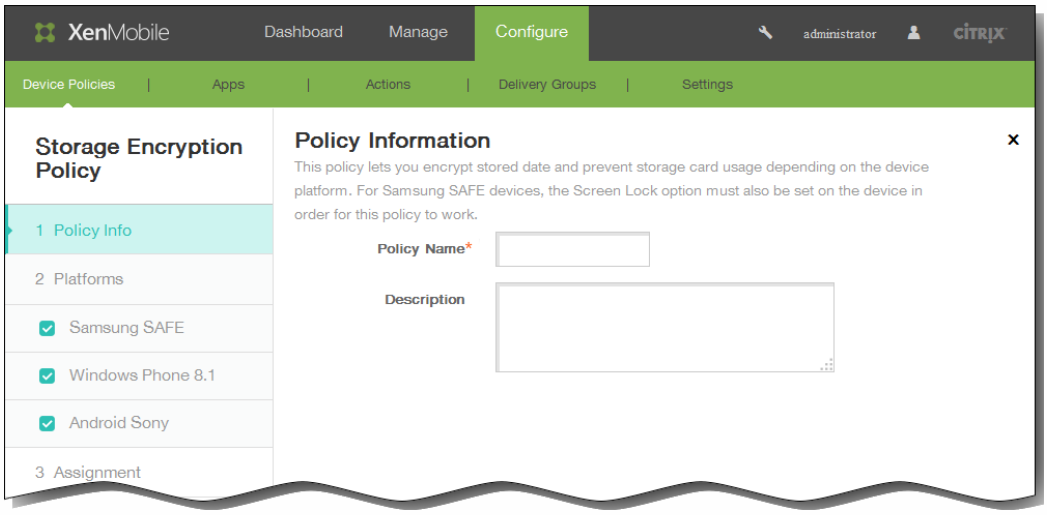
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



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

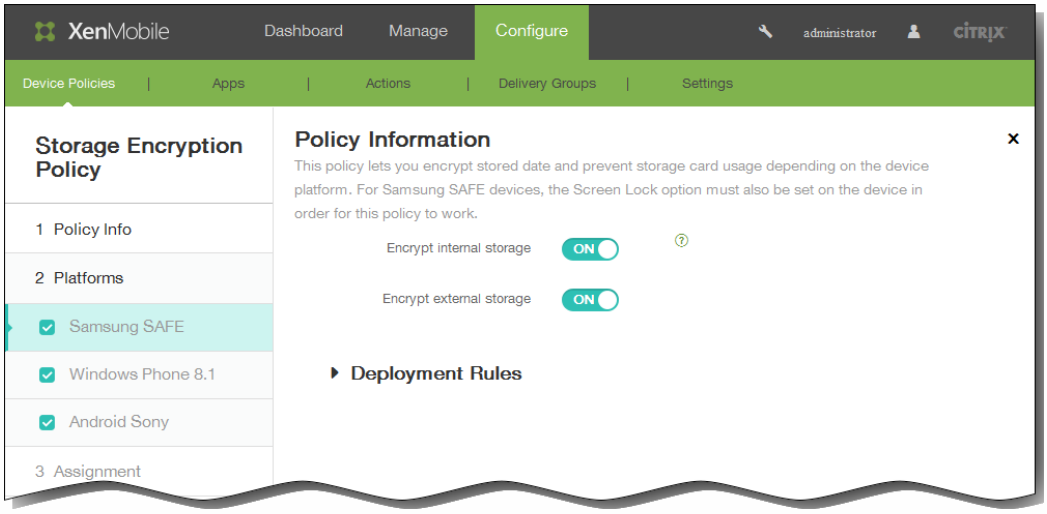


3. Klicken Sie auf More und dann unter Security auf Storage Encryption. Die Seite Storage Encryption Policy wird angezeigt.

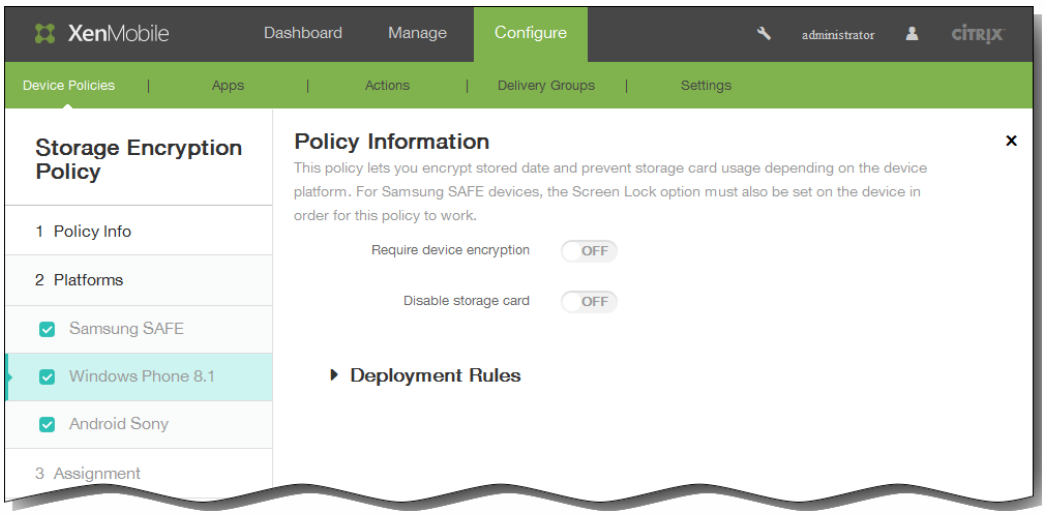


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Policy Platforms wird angezeigt.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

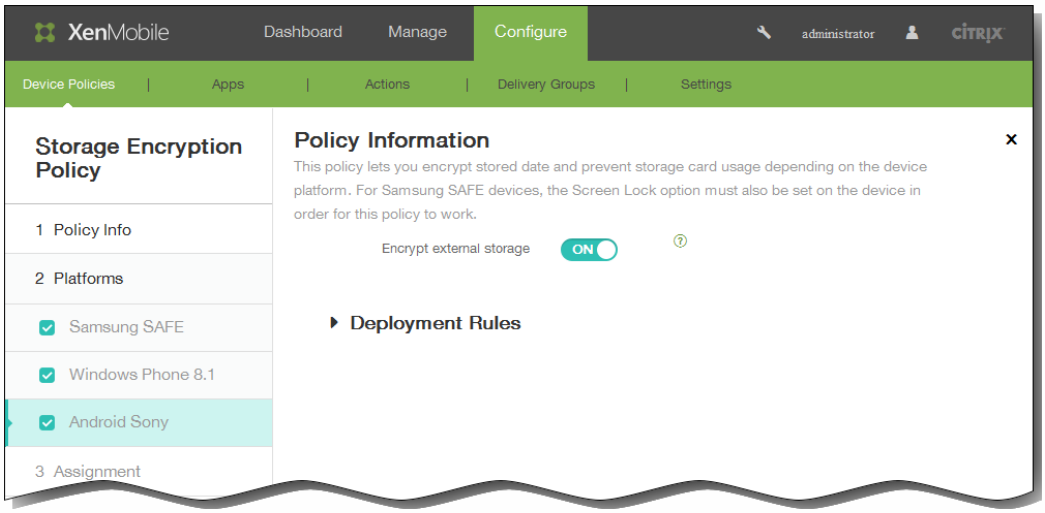
6. Wählen Sie unter Platforms die Plattformen aus, für die Sie diese Richtlinie konfigurieren möchten. Deaktivieren Sie alle anderen ggf. ausgewählten Plattformen.
   - Bei Auswahl von Samsung SAFE:
     - Encrypt internal storage: Wählen Sie aus, ob der interne Speicher auf Geräten verschlüsselt werden 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.

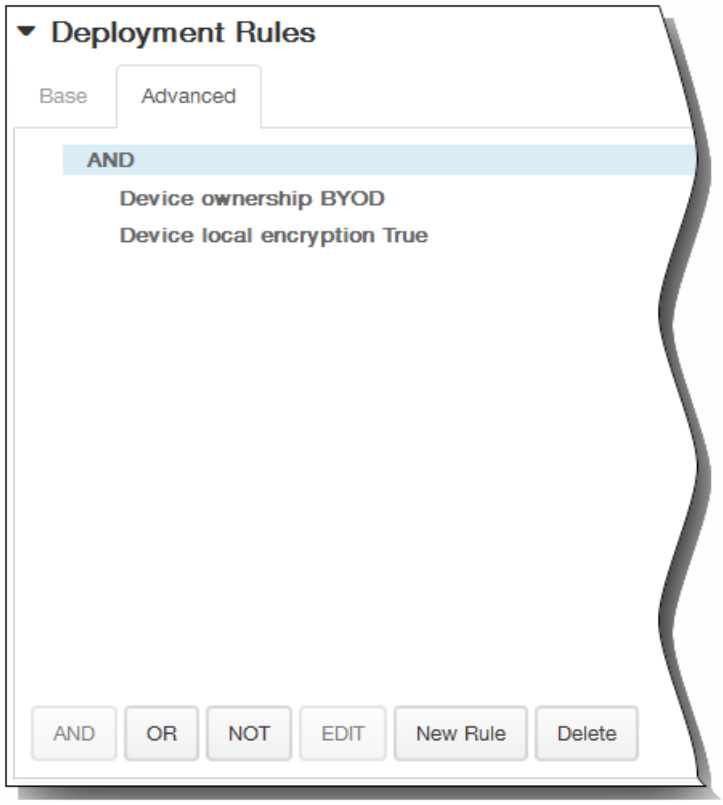


   - Wenn Sie Android Sony ausgewählt haben, wählen Sie für Encrypt external storage aus, ob der externe Speicher auf Geräten verschlüsselt werden soll. Für das Gerät muss ein Kennwort mit Zahlen und Buchstaben oder Symbolen erforderlich sein. Die Standardeinstellung ist ON.



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

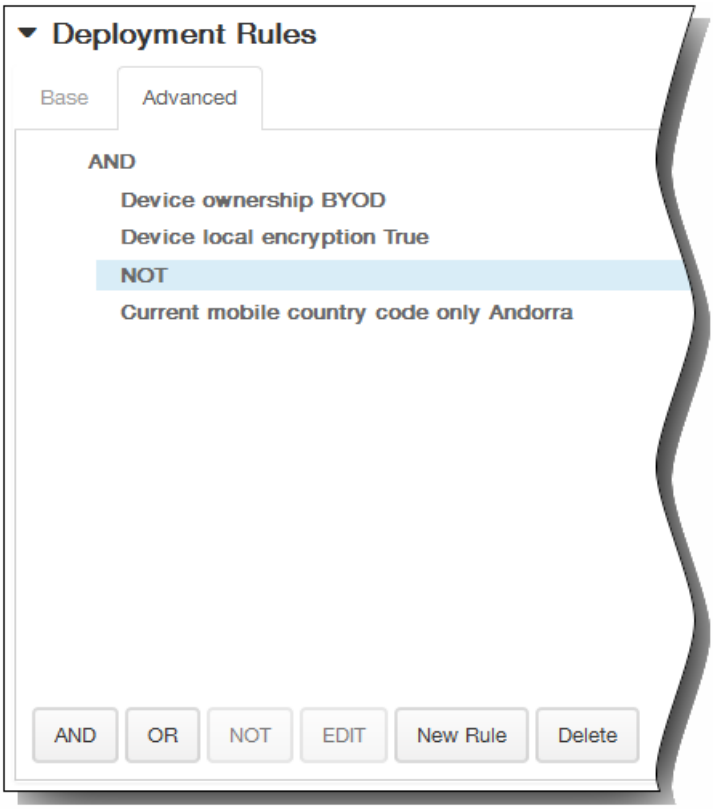
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
    3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
    4. Klicken Sie noch einmal 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.



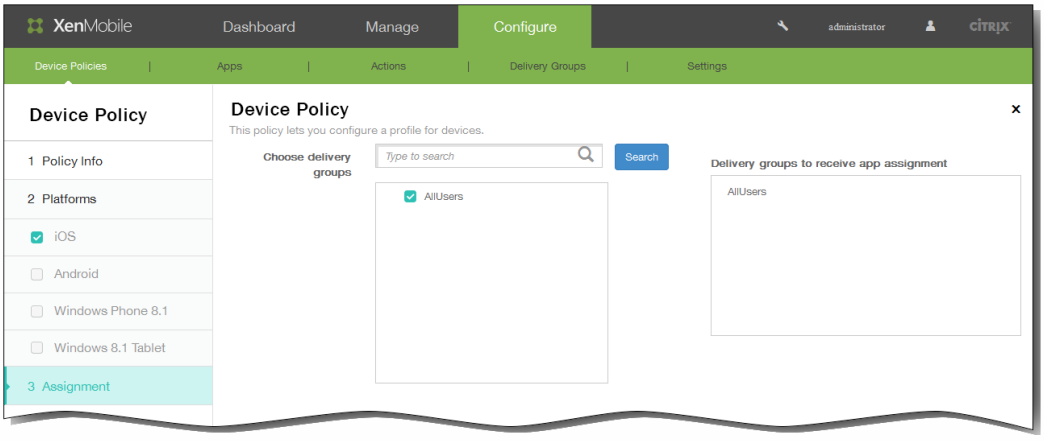
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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 noch einmal 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.



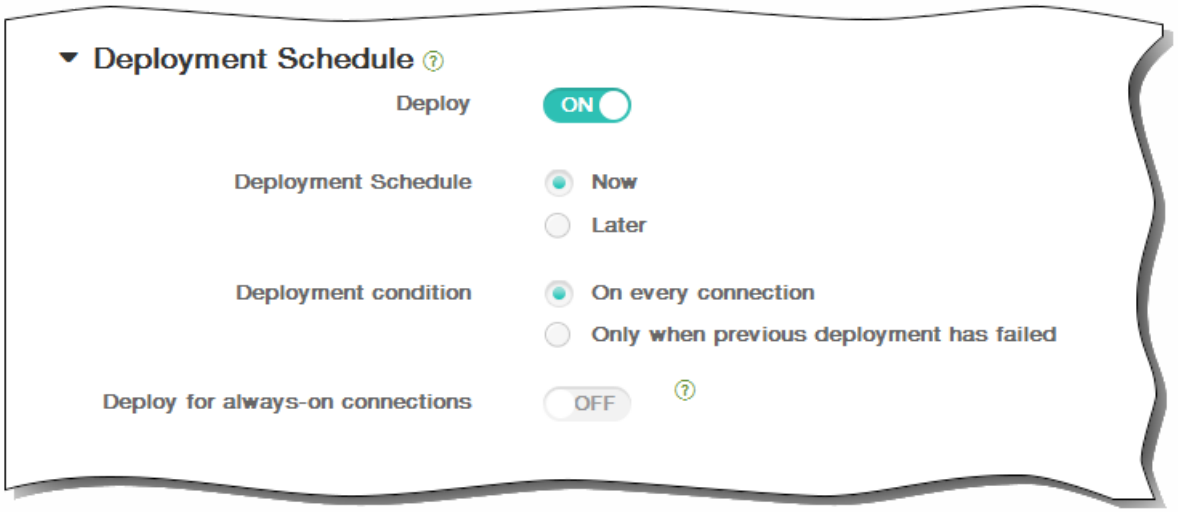
8. Klicken Sie auf Next. Die Seite Assignment für die Speicherverschlüsselungsrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese 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.



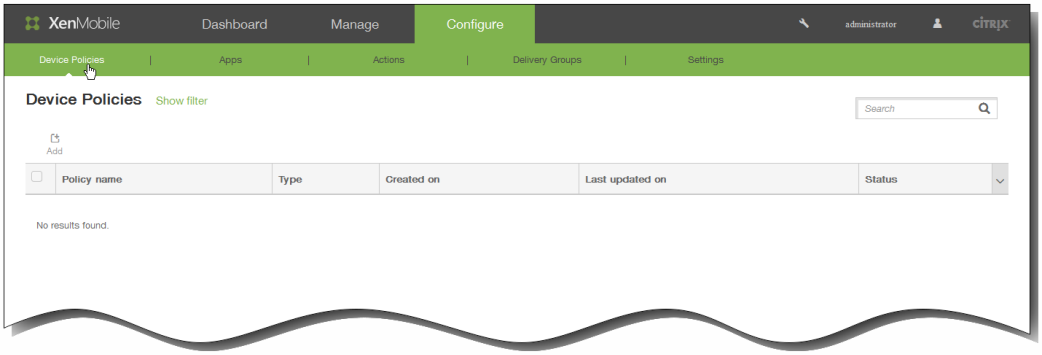
11. Klicken Sie auf Save, um die Richtlinie zu speichern.

So fügen Sie eine Webinhaltsrichtlinie für iOS-Geräte hinzu

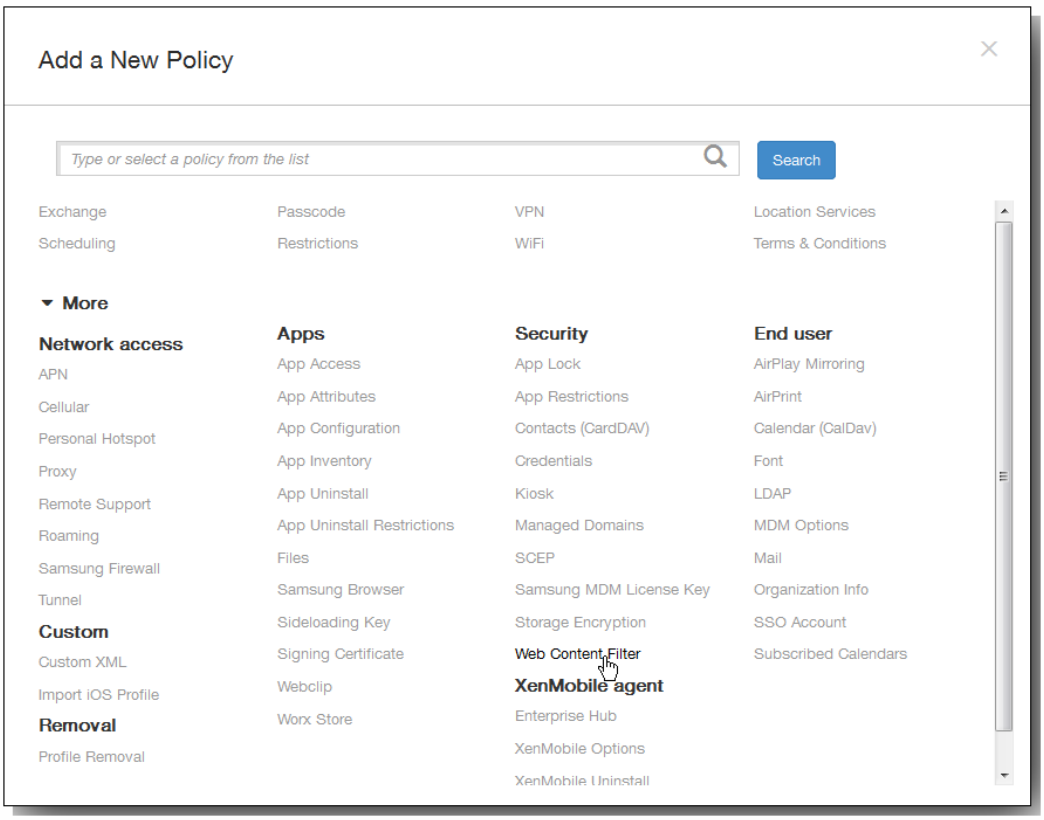
May 05, 2016

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.

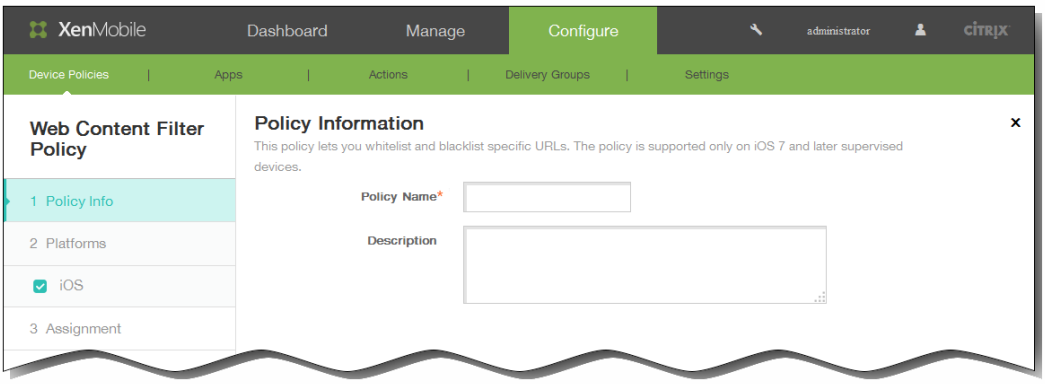
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



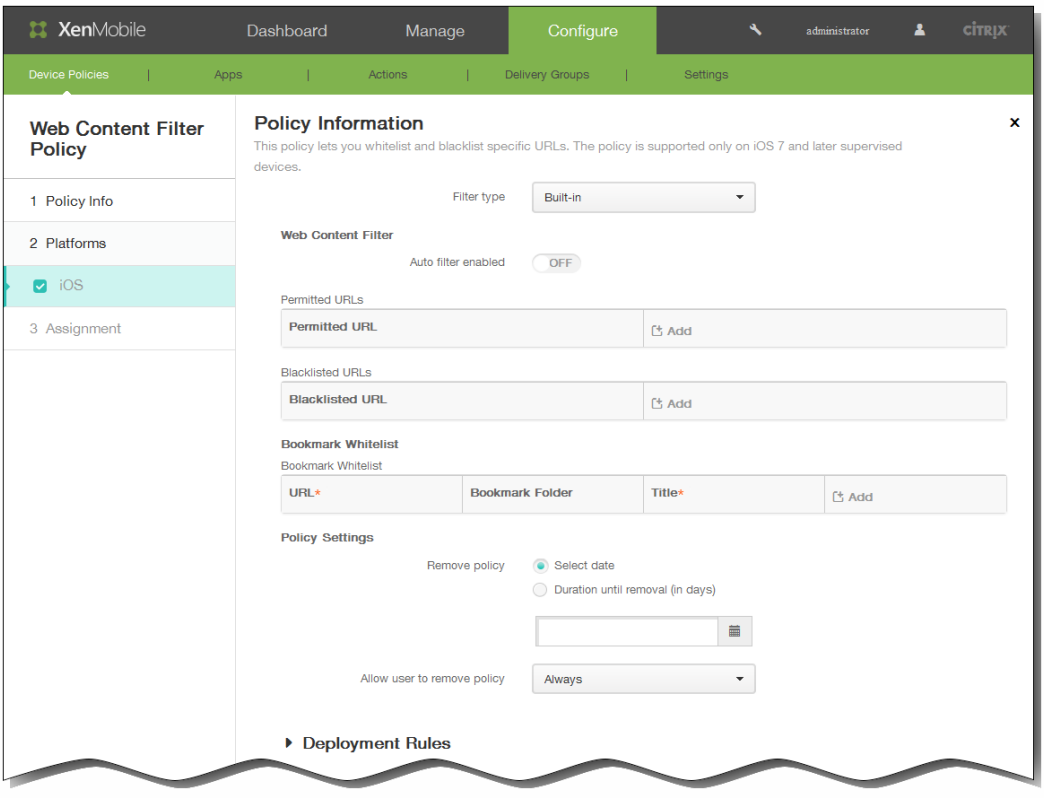
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add a New Policy wird angezeigt.



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:

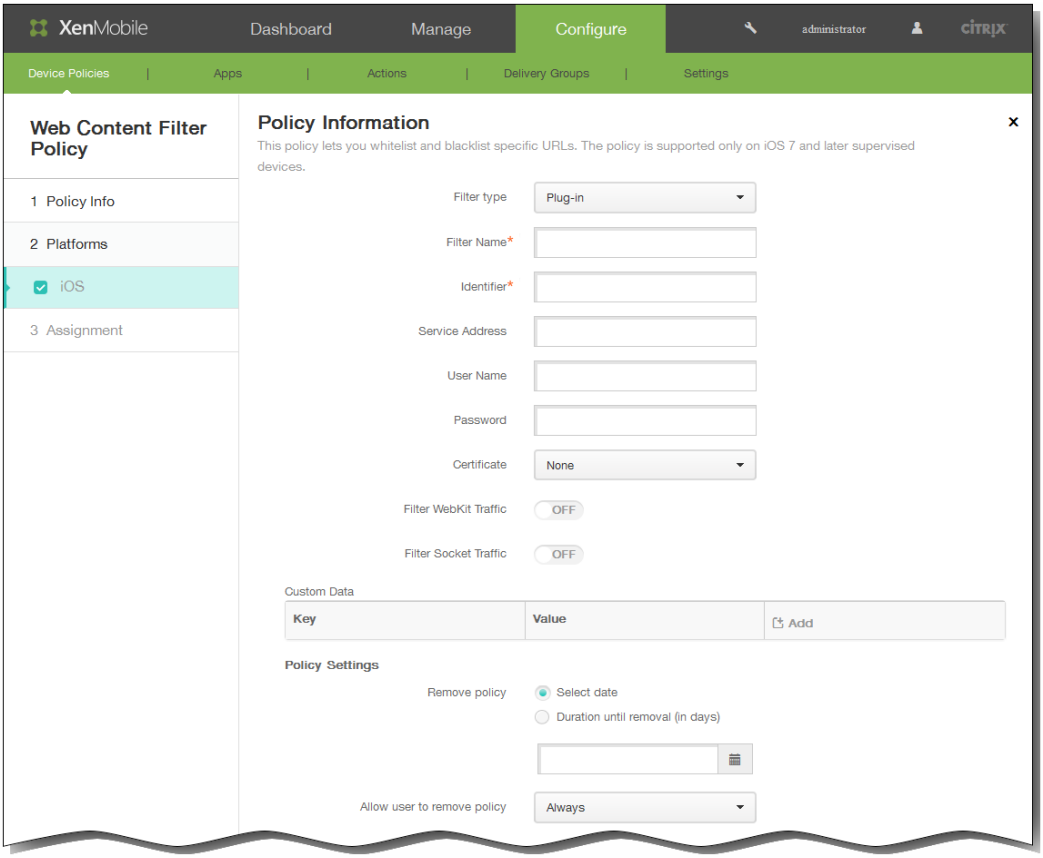
   1. Geben Sie die URL der Website ein, die gesperrt werden soll. Die URL muss mit "http://" bzw. "https://" beginnen.
   2. Klicken Sie auf Save, um die Website der Sperrliste hinzuzufügen, oder auf Cancel, um den Vorgang abzubrechen.
   3. Wiederholen Sie die Schritte i und ii für jede Website, die Sie 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



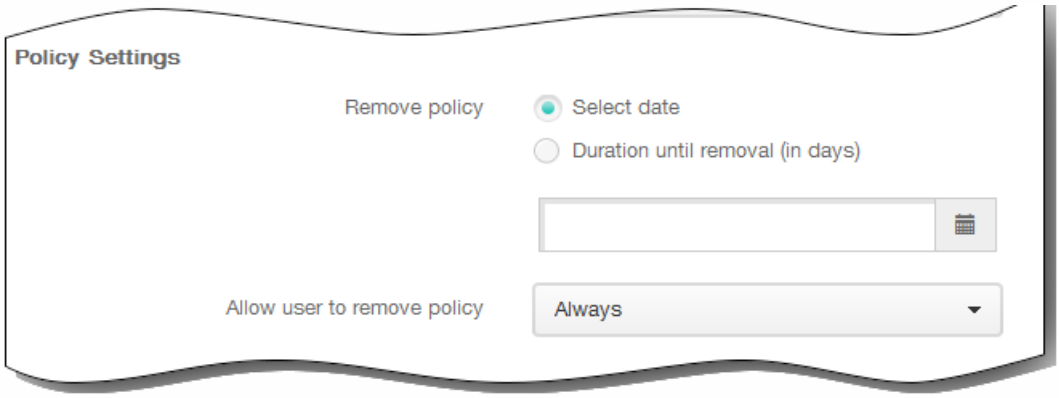
1. Filter name: Geben Sie einen eindeutigen Namen für den Filter ein.
2. Identifier: Geben Sie die Paket-ID des Filterdienst-Plug-Ins ein.
3. Service address: Geben Sie optional eine Serveradresse ein. Gültige Formate sind IP-Adressen, Hostnamen oder URLs.
4. User name: Geben Sie optional einen Benutzernamen 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.

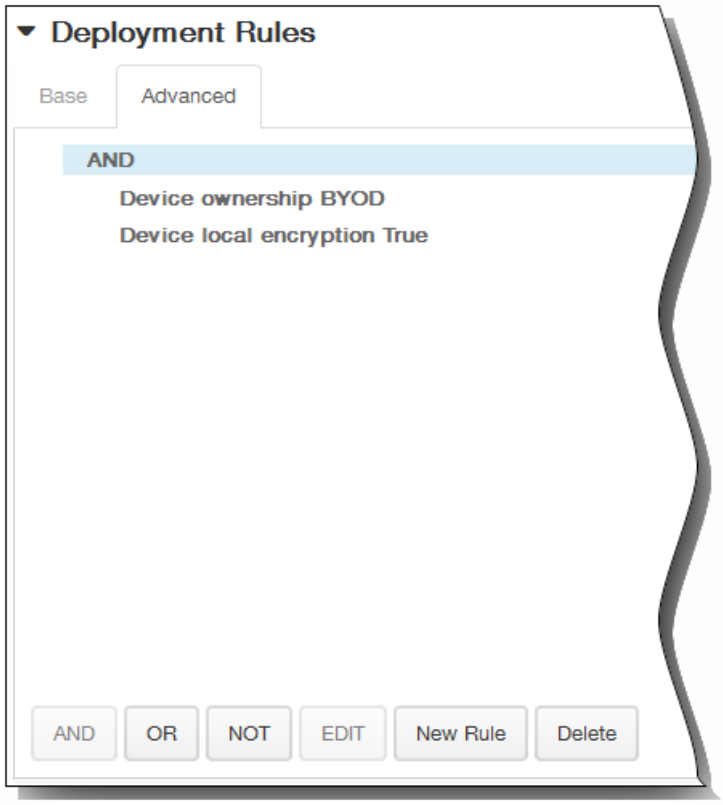
7. Klicken Sie unter Policy Settings für Remove policy auf Select date oder Duration until removal (in days).

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.

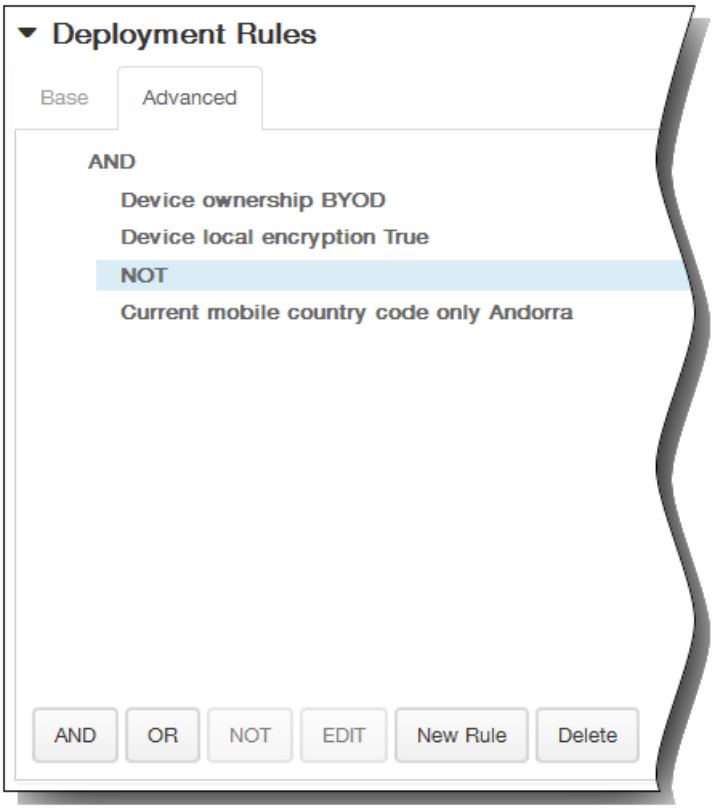
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen 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.



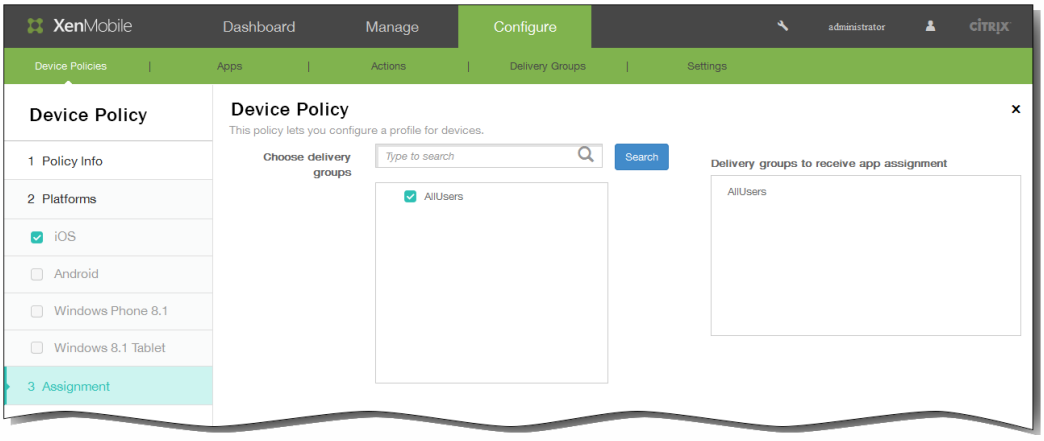
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



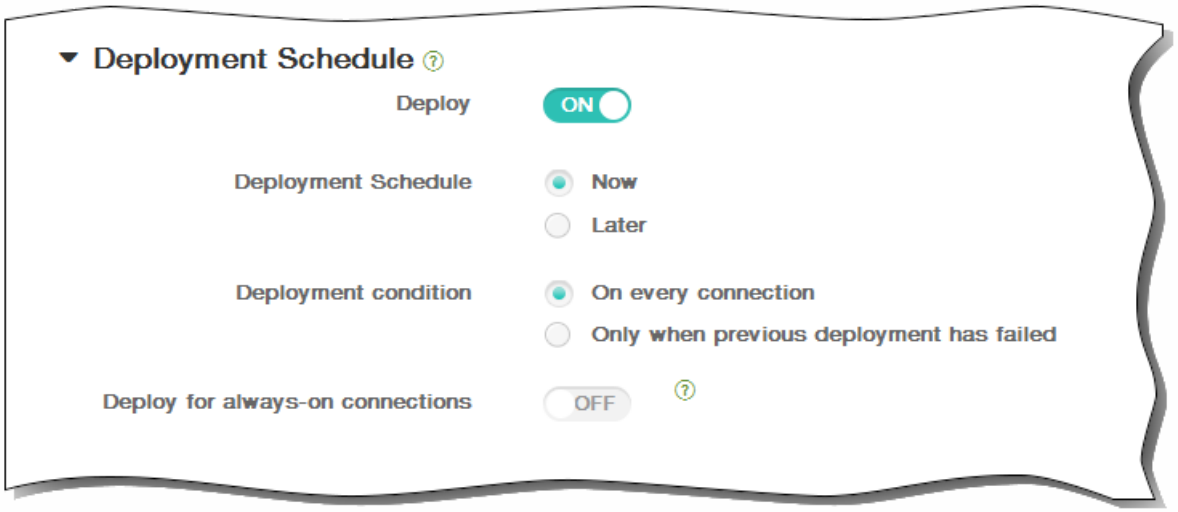
12. Klicken Sie auf Next. Die Seite Assignment für die Webinhaltsfilterrichtlinie wird angezeigt.
13. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.



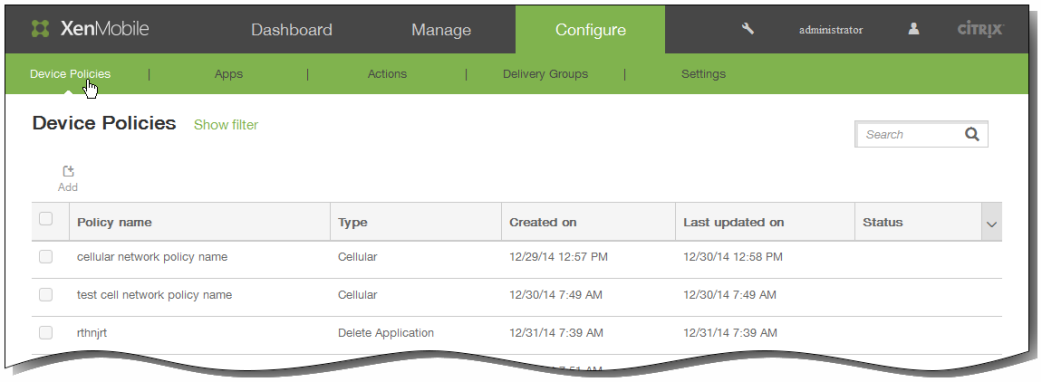
15. Klicken Sie auf Save, um die Richtlinie zu speichern.

Samsung-Browserrichtlinien für Geräte

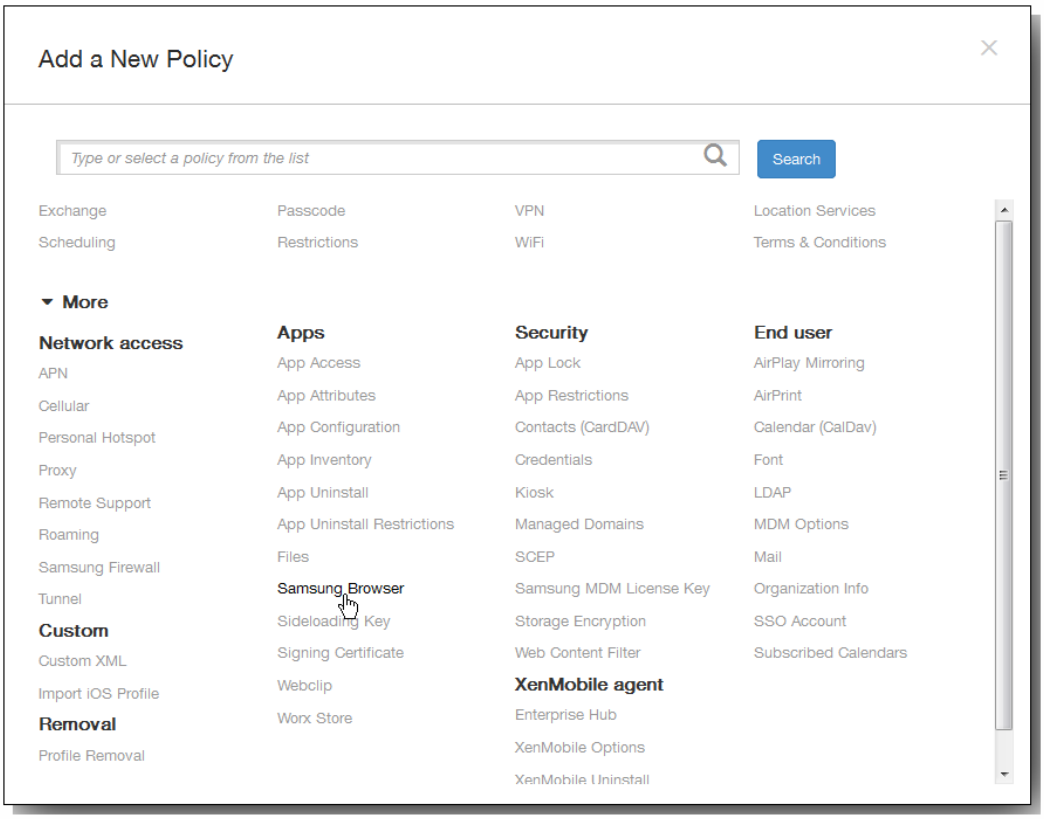
May 05, 2016

Sie können Samsung-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.

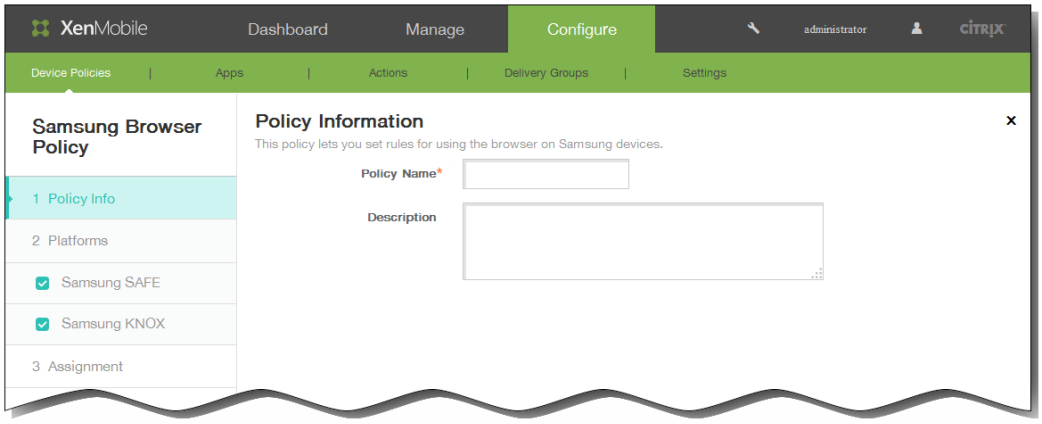
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



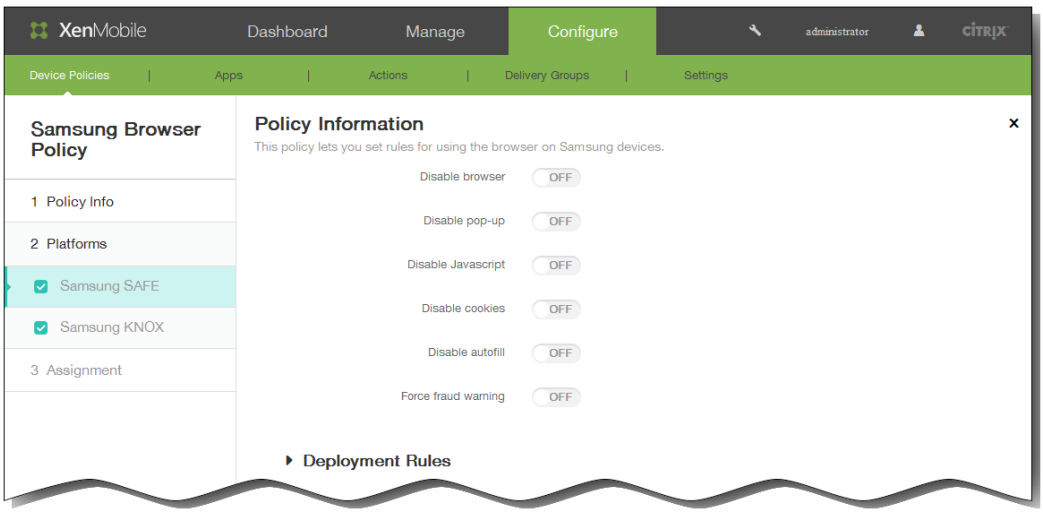
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld Add New Policy wird angezeigt.



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.

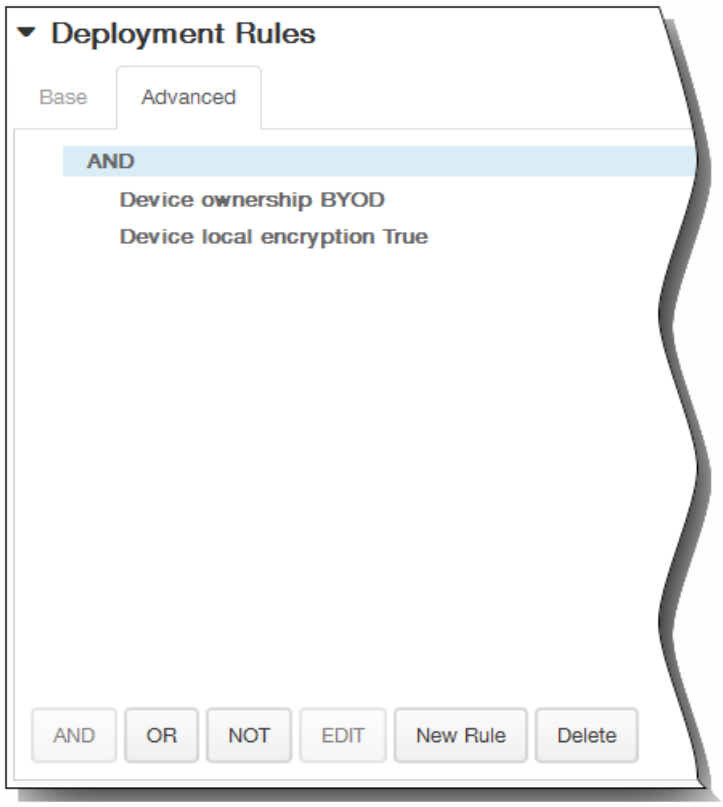


6.
7. Wählen Sie unter Platforms die gewünschten Samsung-Plattformen aus. Wenn Sie nur eine Plattform konfigurieren möchten, deaktivieren Sie die andere und legen Sie die folgenden Einstellungen fest:
   1. Disable browser: Wählen Sie aus, ob der Samsung-Browser auf den Geräten komplett deaktiviert werden 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.

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

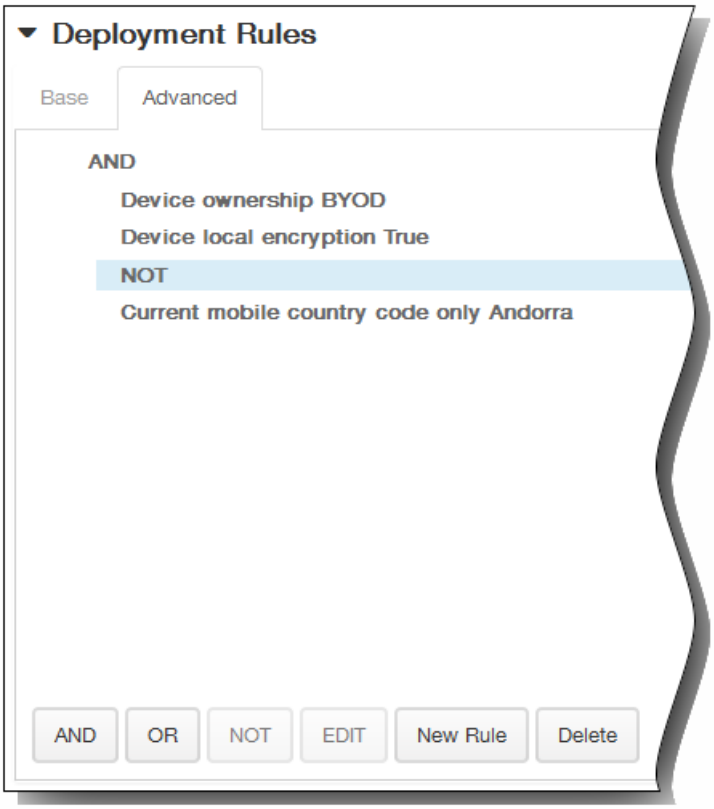
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



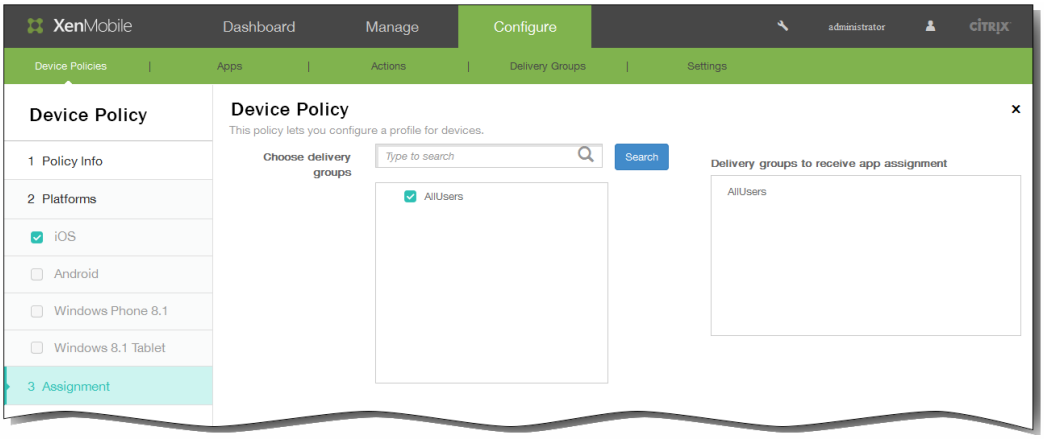
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.

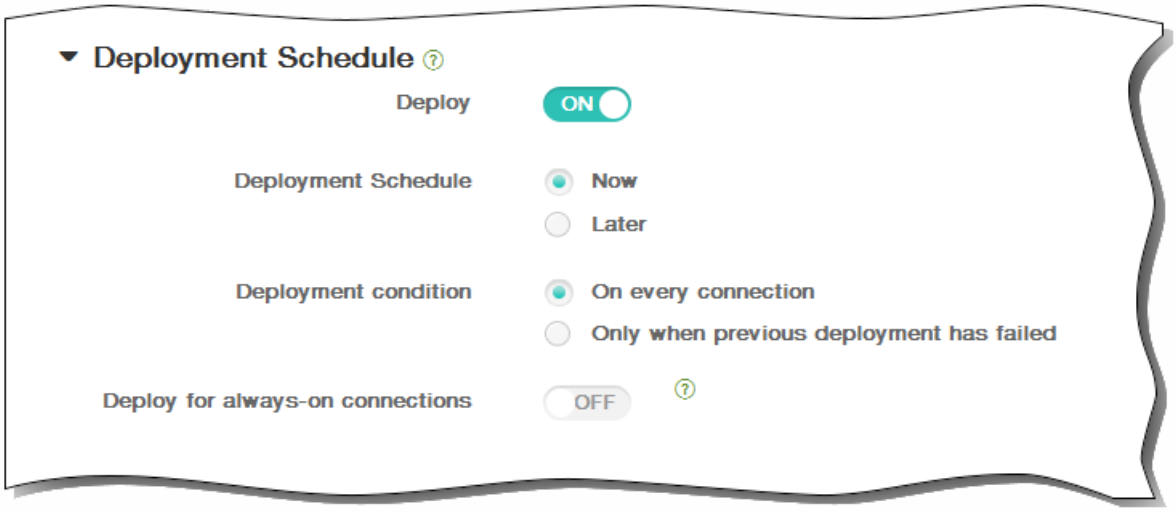


9. Klicken Sie auf Next. Die Seite Samsung Browser Device Policy wird angezeigt.
10. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden 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. 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.



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

So fügen Sie eine Sideloadingrichtlinie für Windows 8.1-Tablets hinzu

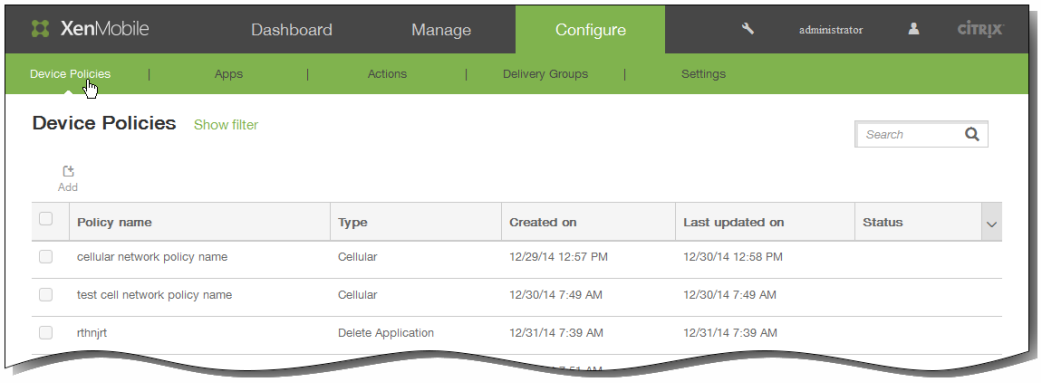
May 05, 2016

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.

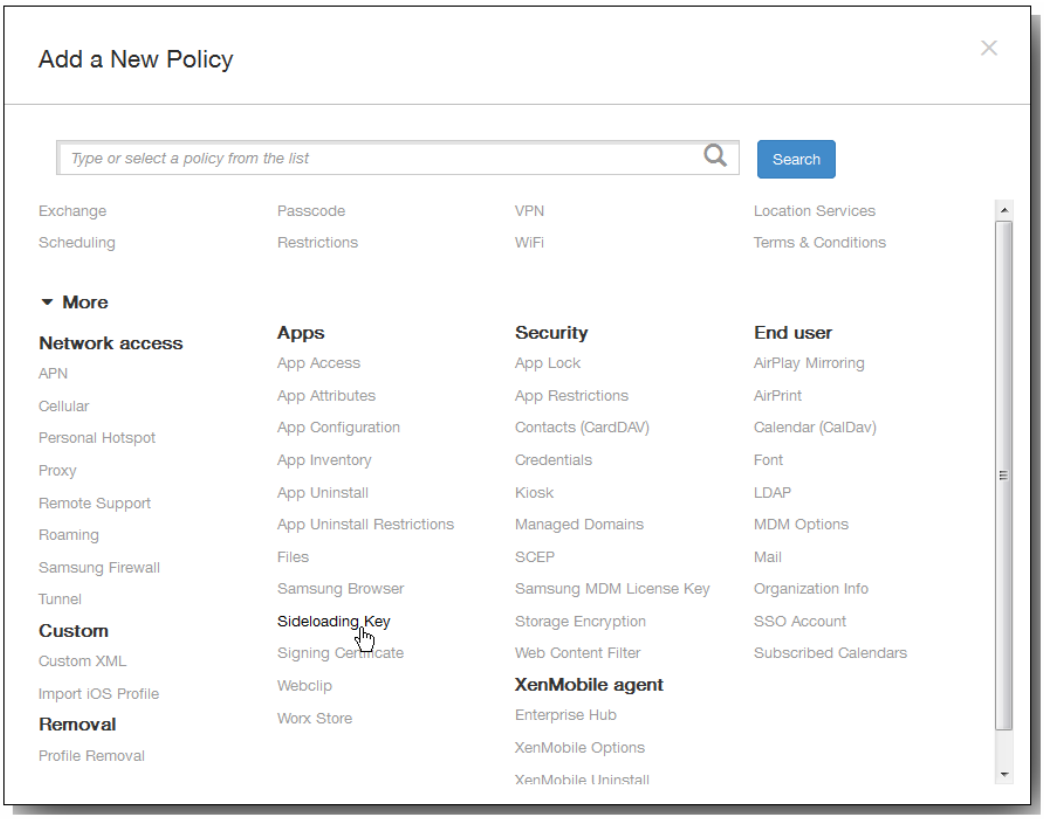
Sie benötigen zum Erstellen der Richtlinie die folgenden Informationen:

- 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

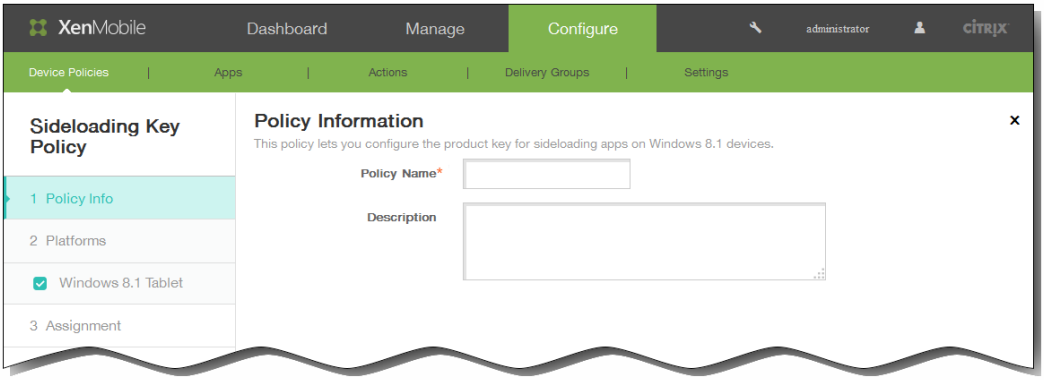
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



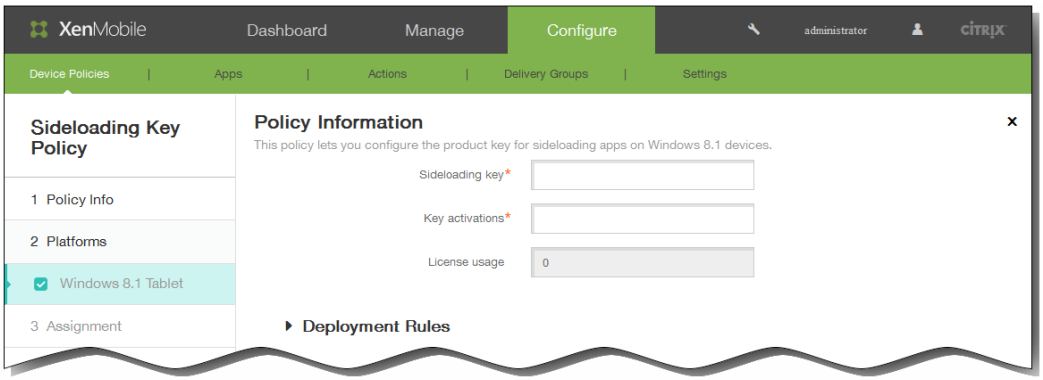
2. Klicken Sie auf Add. Das Dialogfeld Add New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter Apps auf Sideloading Key. Die Seite Sideloading Key Policy wird angezeigt.

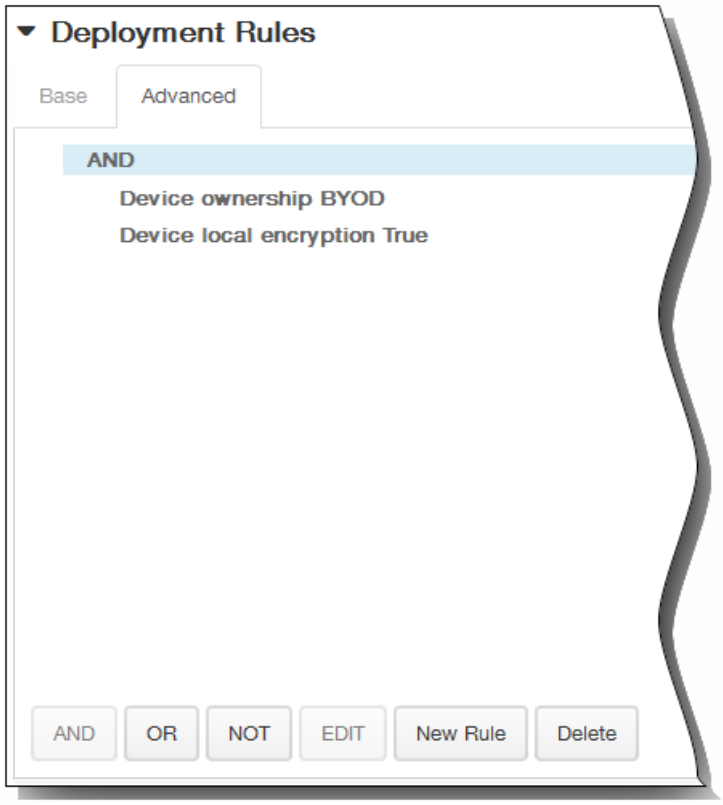


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next.
   Die Seite Windows 8.1 Tablet Platform wird 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.

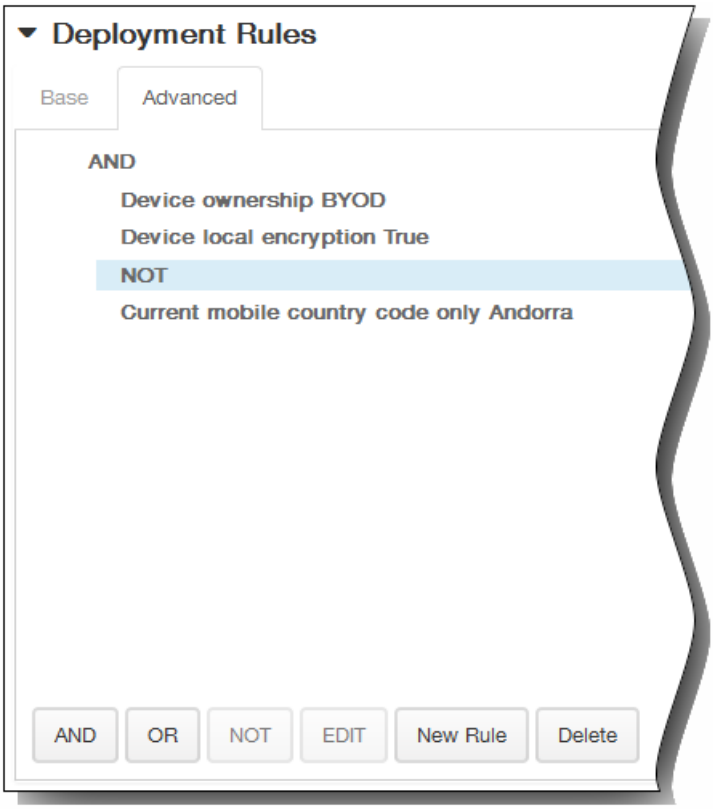
   1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
      1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
      2. Klicken Sie auf New Rule, um Bedingungen 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.



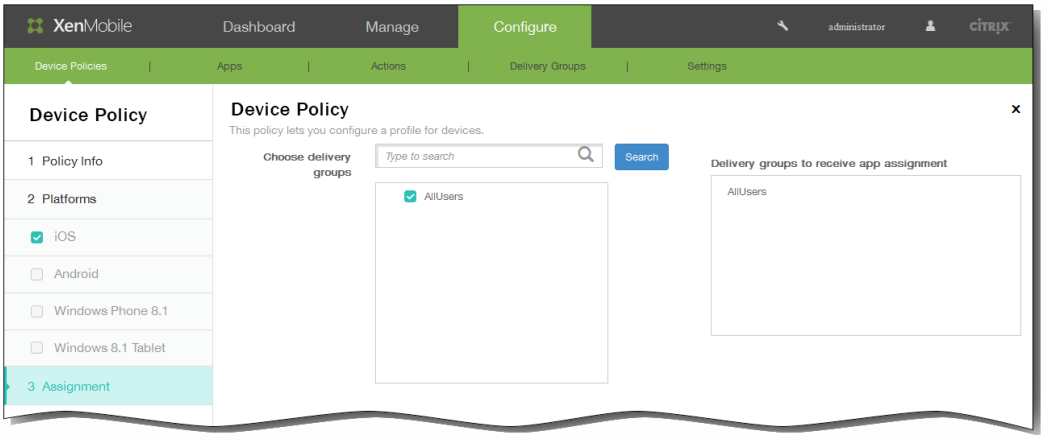
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



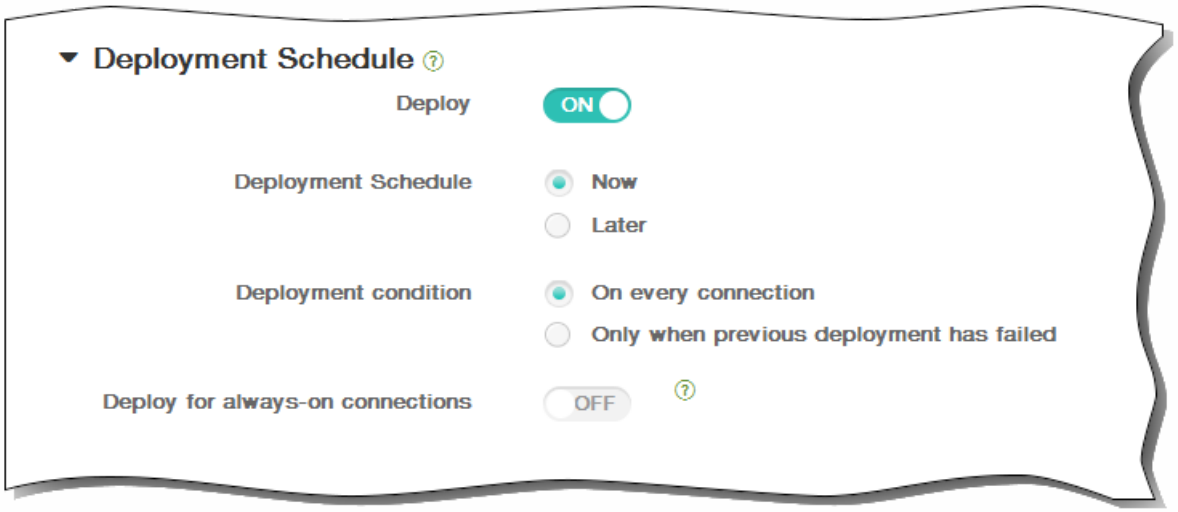
8. Klicken Sie auf Next. Die Seite Assignment für die Sideloadingrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.

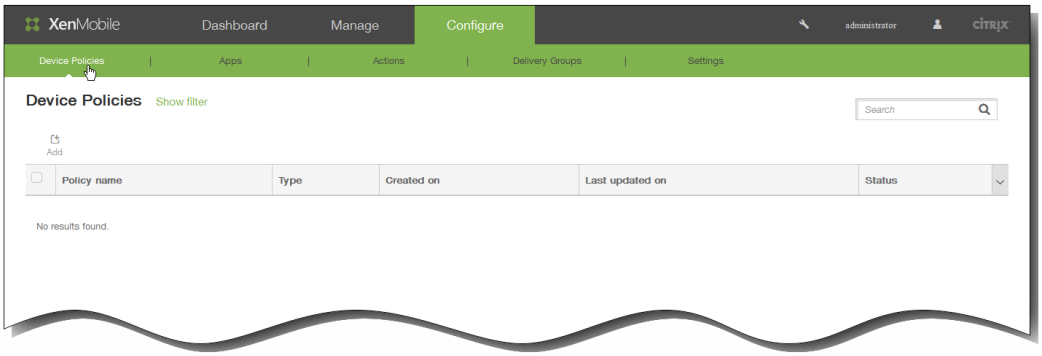


So fügen Sie eine Signaturzertifikat-Richtlinie für Windows 8.1-Tablets hinzu

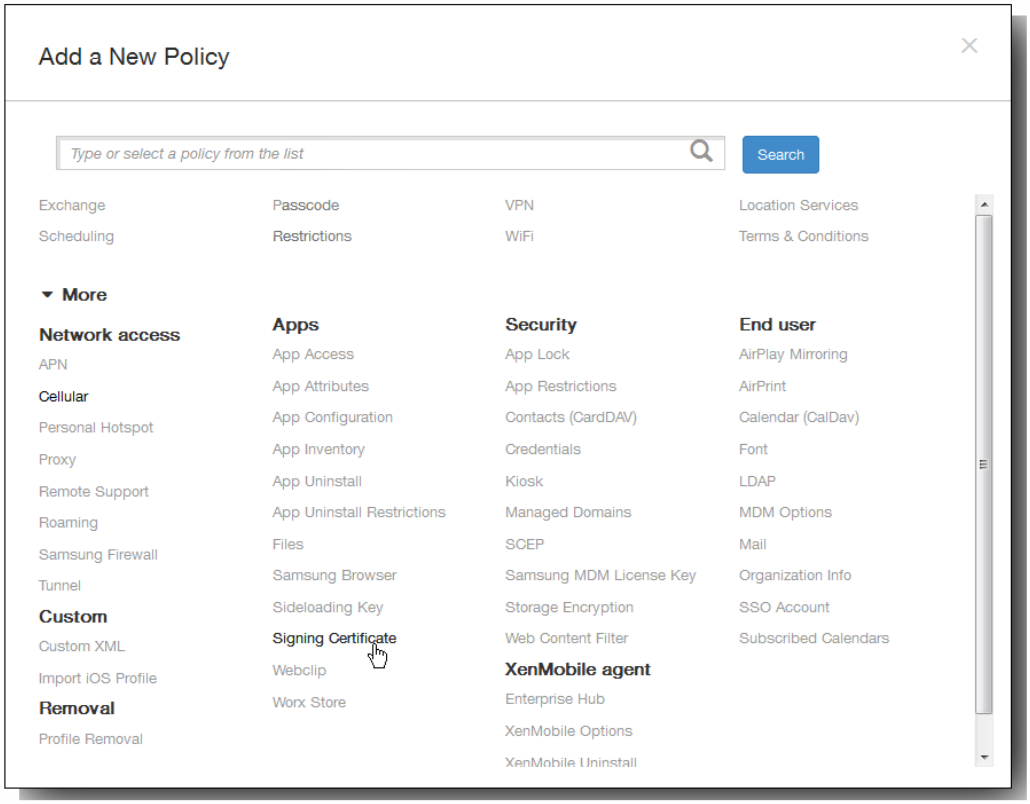
May 05, 2016

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.

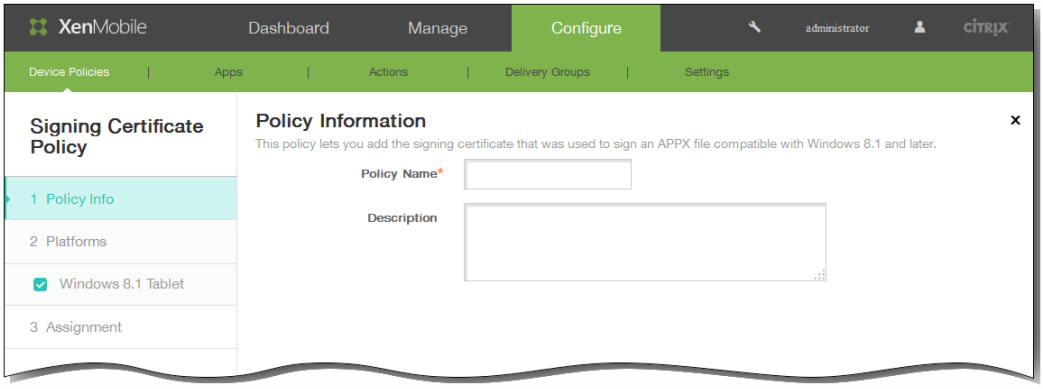
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



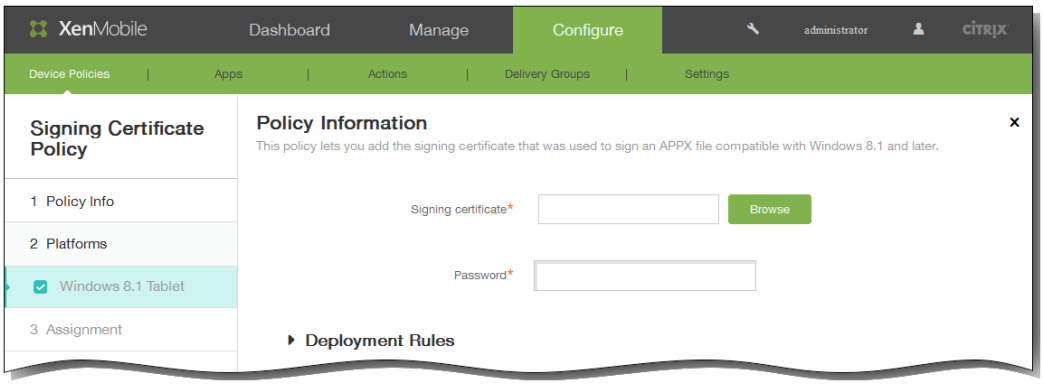
2. Klicken Sie auf Add, um eine neue Richtlinie hinzuzufügen. Wenn Sie auf Add klicken, wird das Dialogfeld Add a New Policy angezeigt.



3. Klicken Sie auf More und dann unter Apps auf Signing Certificate. Die Seite Signing Certificate Policy wird angezeigt.

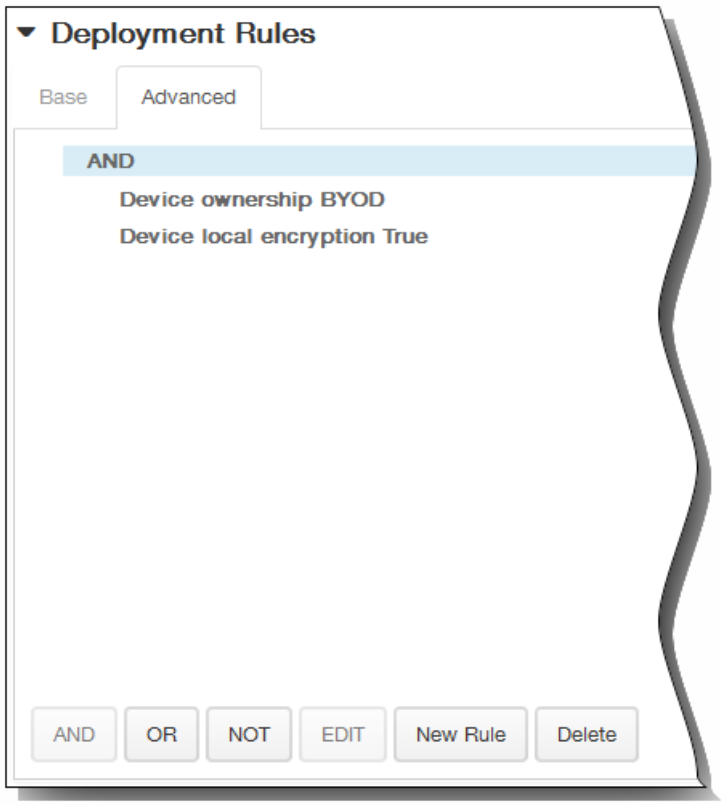


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung für die Richtlinie ein.
5. Klicken Sie auf Next. Die Seite Platform Information wird angezeigt.



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.

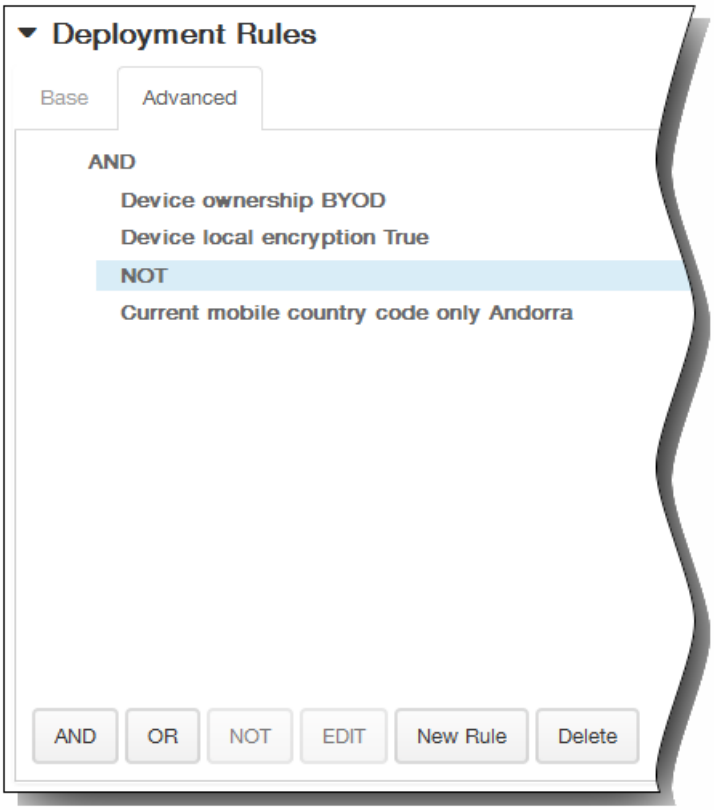
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen 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.



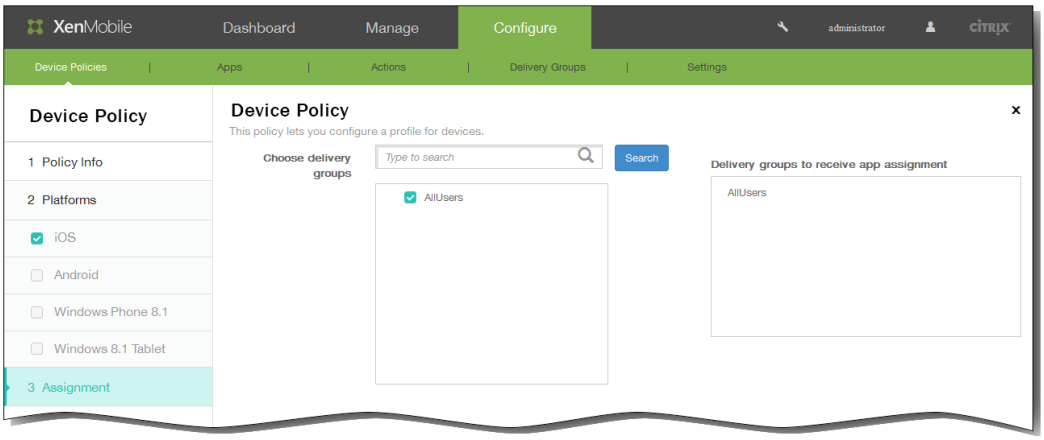
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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.



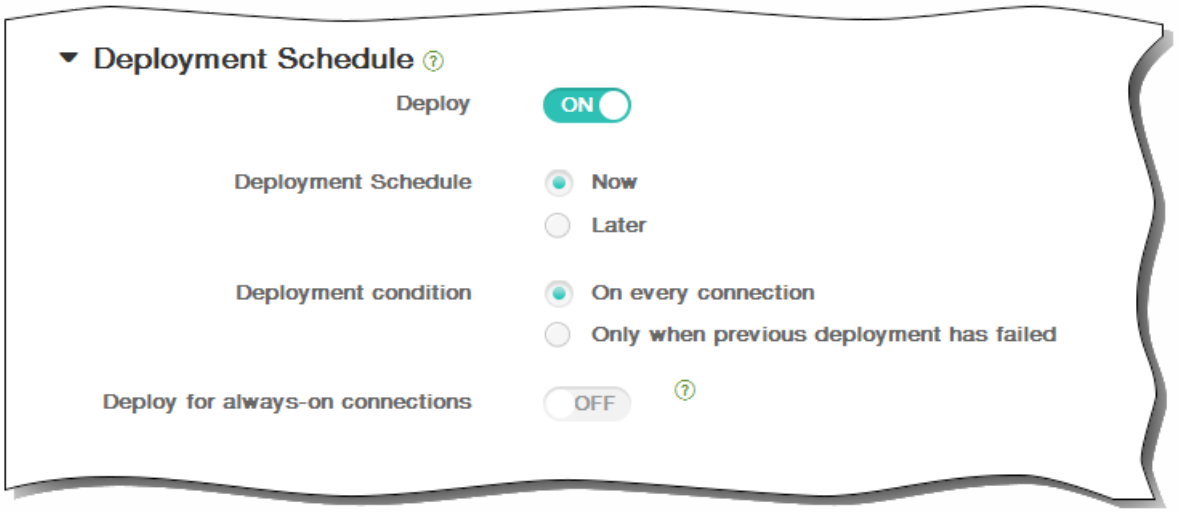
8. Klicken Sie auf Next. Die Seite Assignment wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der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



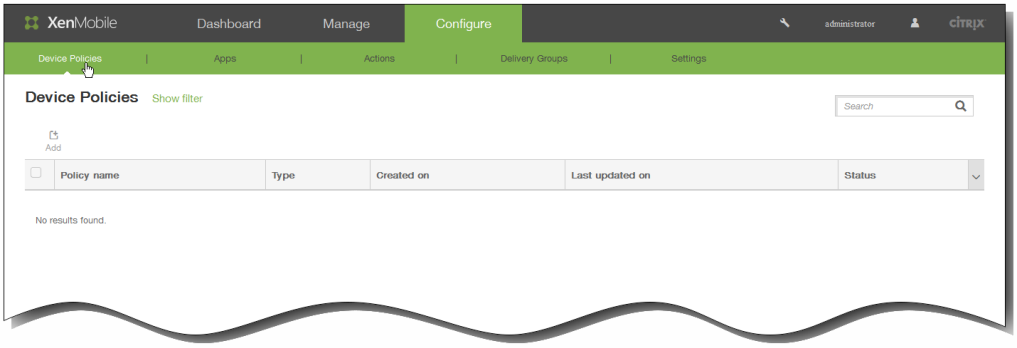
11. Klicken Sie auf Save, um die Richtlinie zu speichern.

May 05, 2016

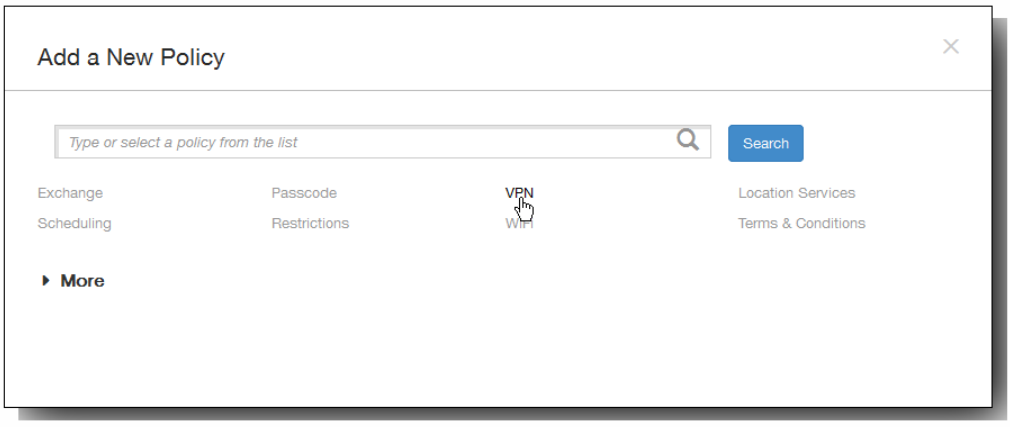
Sie können in XenMobile eine Geräterichtlinie hinzufügen, um die Einstellungen für ein VPN (virtuelles privates Netzwerk) für eine sichere Verbindung zwischen Geräten und Unternehmensressourcen zu konfigurieren. VPN-Richtlinien können für folgende Plattformen konfiguriert werden: iOS, Samsung SAFE, Samsung 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

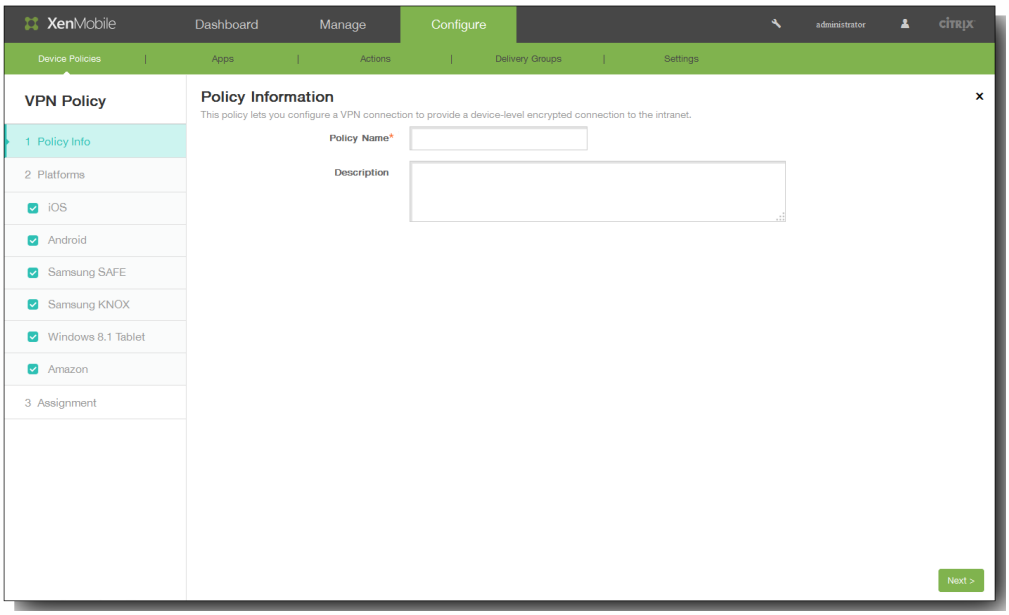
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



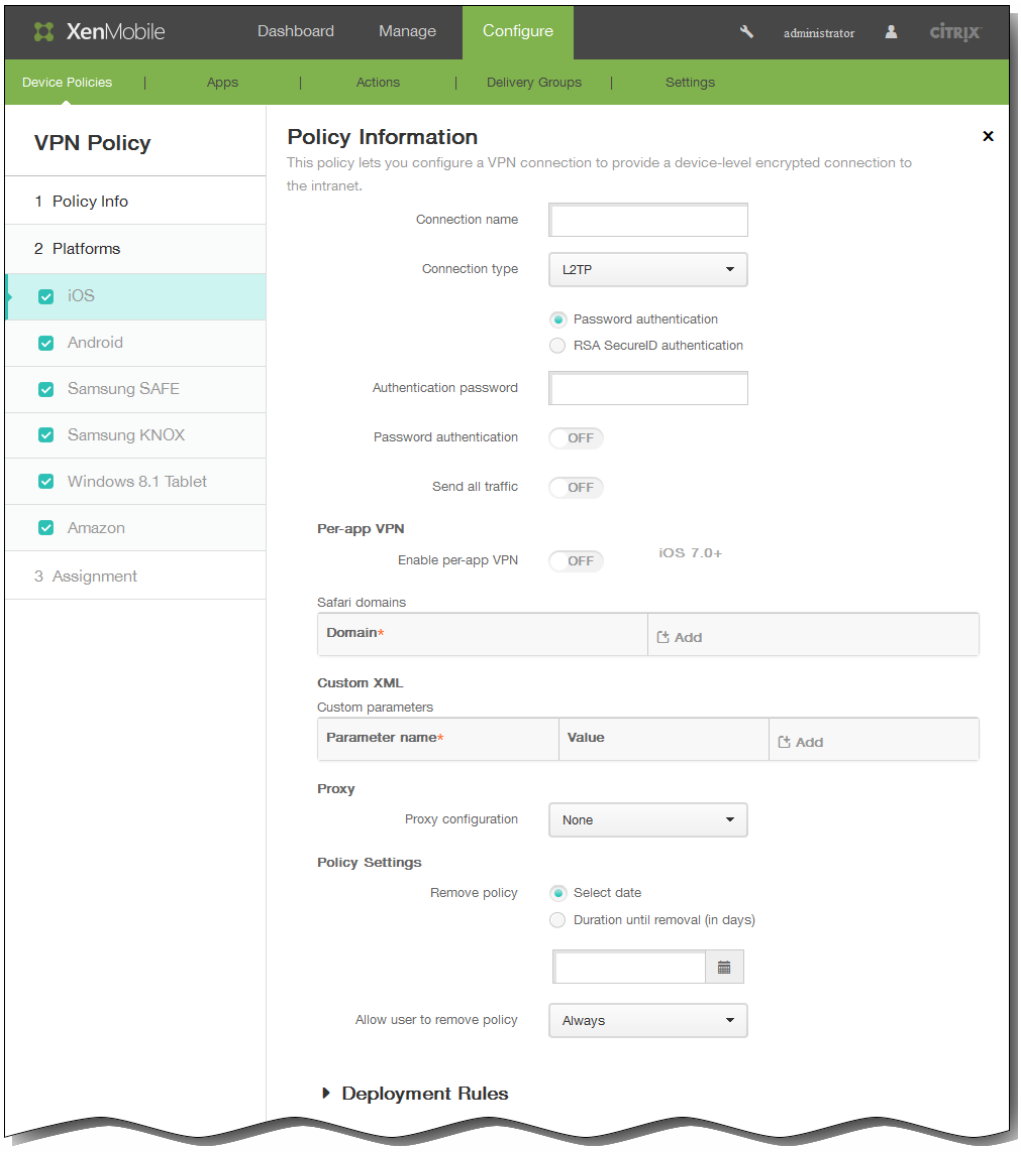
2. Klicken Sie auf Add. Das Dialogfeld Add a New Policy wird angezeigt.



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	**Password**	**Zertifikat** Erforderlich, wenn Enable VPN on demand = ON	**Shared Secret**
Use hybrid authentication	–	–	OFF
Eingabeaufforderung für Kennwort	–	–	OFF
Auth password	Optional	–	–

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	–	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 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	Password	Zertifikat	Shared Secret
	–	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.

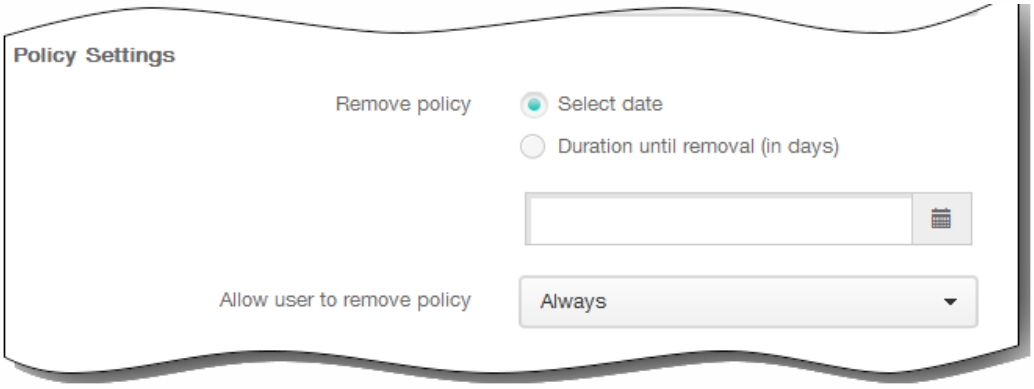
	Password	**Zertifikat**	**Shared Secret**
Group name	–	–	Optional
Eingabeaufforderung für Kennwort	–	–	OFF
Auth password	Optional	–	OFF
Identity credential	–	Keine	–
Prompt for PIN when connecting	–	OFF	–
Enable VPN on demand	–	OFF	–

On Demand Domain	Password	Zertifikat	Shared Secret
	–	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.

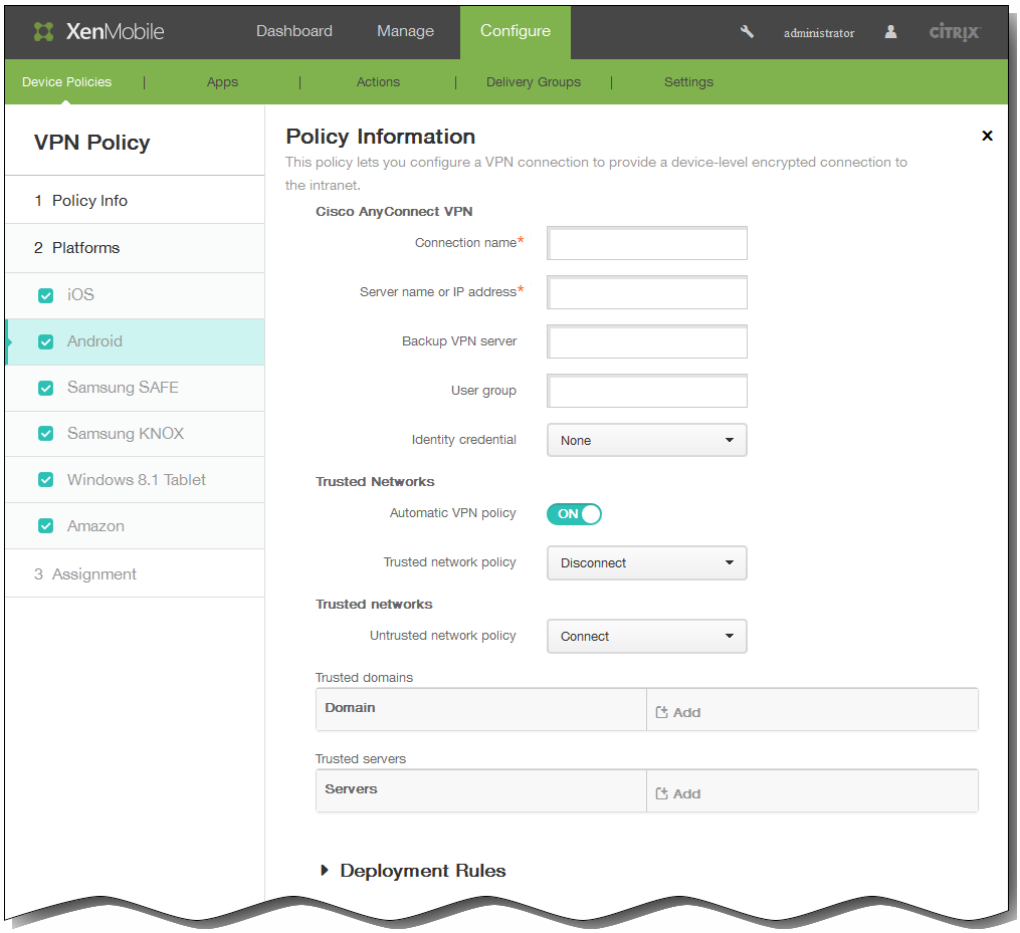
	Manuell	Automatisch
Host name or IP address for the proxy server	Erforderlich	–
Port for the proxy server	Erforderlich	–
User name	Optional	–
Password	Optional	–
Proxy server URL	–	Erforderlich

Richtlinieneinstellungen



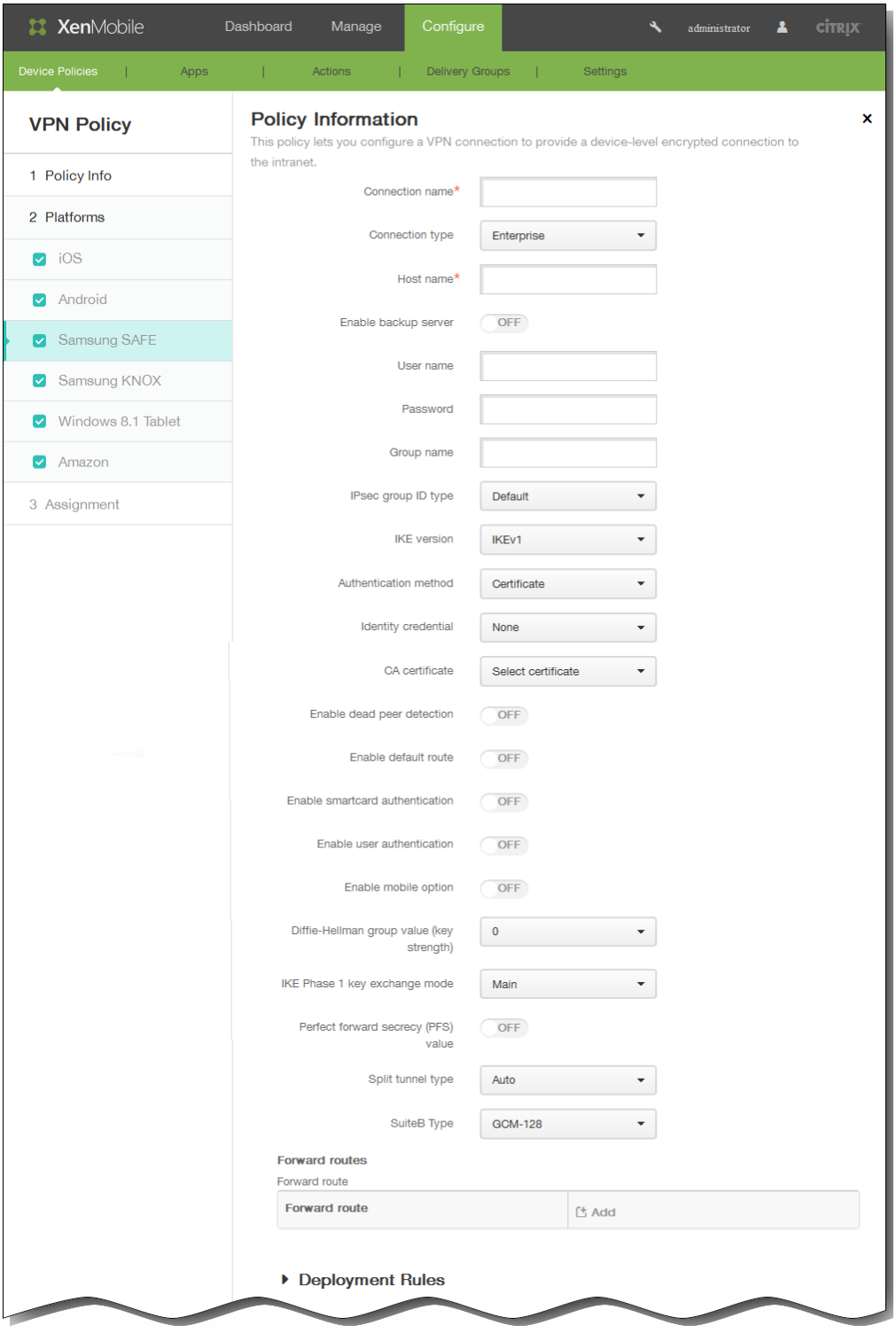
1. Klicken Sie unter Policy Settings für Remove policy auf Select date oder Duration until removal (in days).
2. Bei Auswahl von Select date klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
3. Klicken Sie in der Liste Allow user to remove policy auf Always, Password required oder 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

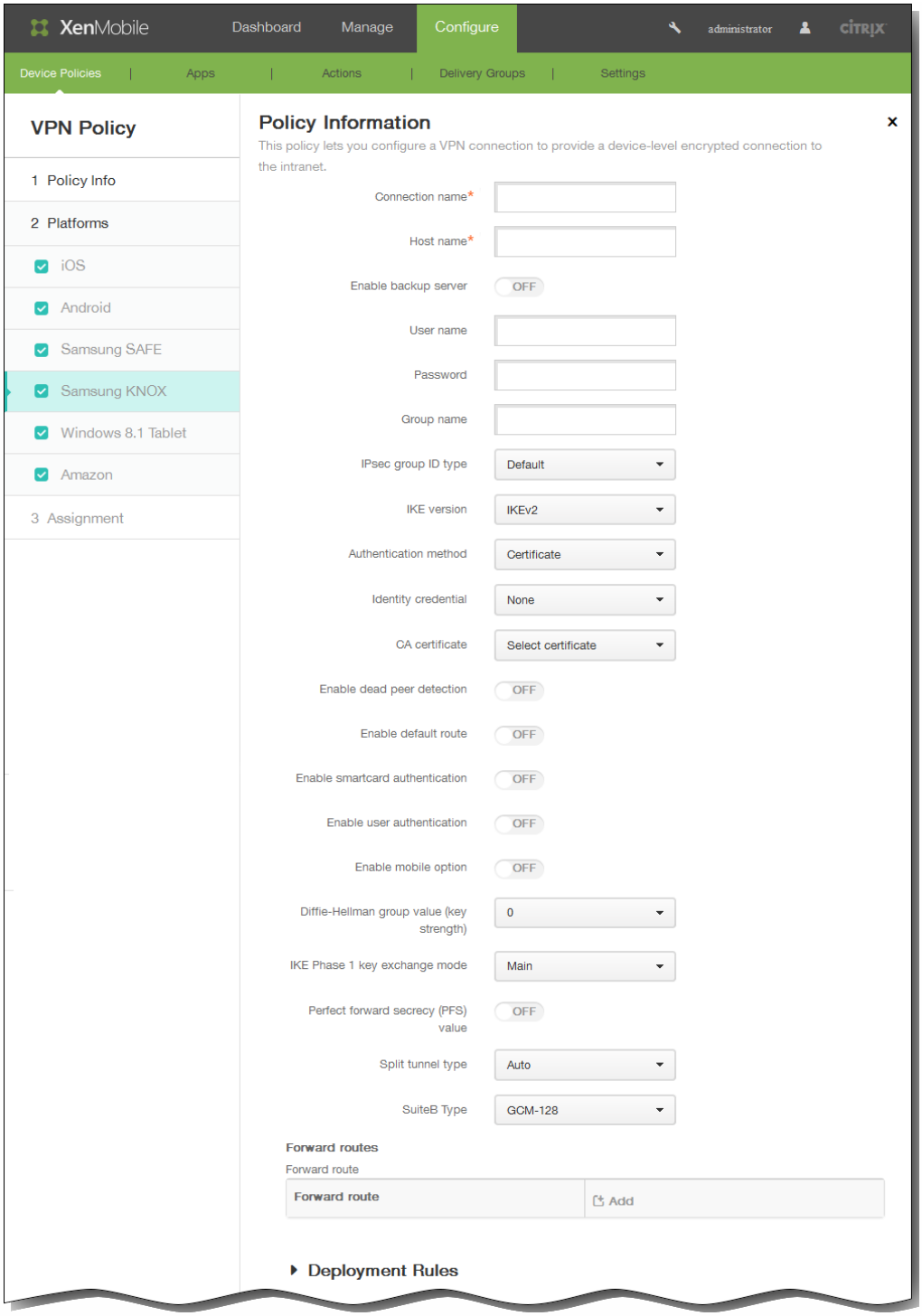
In der folgenden Tabelle werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	L2TP with pre-shared key	**L2TP with certificate**	**PPTP**	**Enterprise**				
Host name	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 Enable mobile option	**L2TP with pre-shared key** –	– **L2TP with certificate** –	– **PPTP** –	Off **Enterprise** Off				
Diffie-Hellman group value (key strength)	–	–	–	0				
IKE Phase 1 key exchange mode	–	–	–	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.

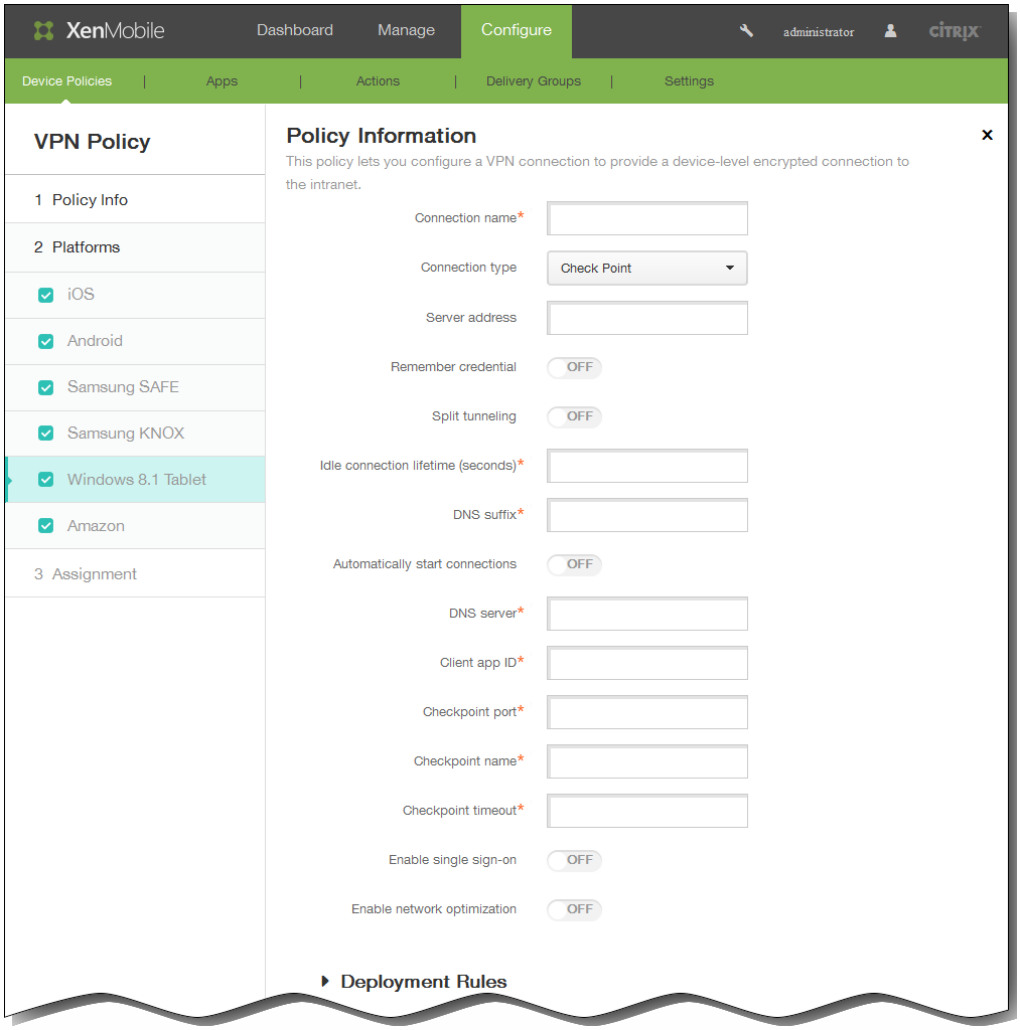
9. Authentication method: Klicken Sie in der Liste auf die Authentifizierungsmethode.
   - Certificate: zertifikatbasierte Authentifizierung
   - Pre-shared key: Authentifizierung mit einem vorinstallierten Schlüssel
   - Hybrid RSA: Hybridauthentifizierung mit RSA-Zertifikaten
   - EAP MD5: Extensible 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

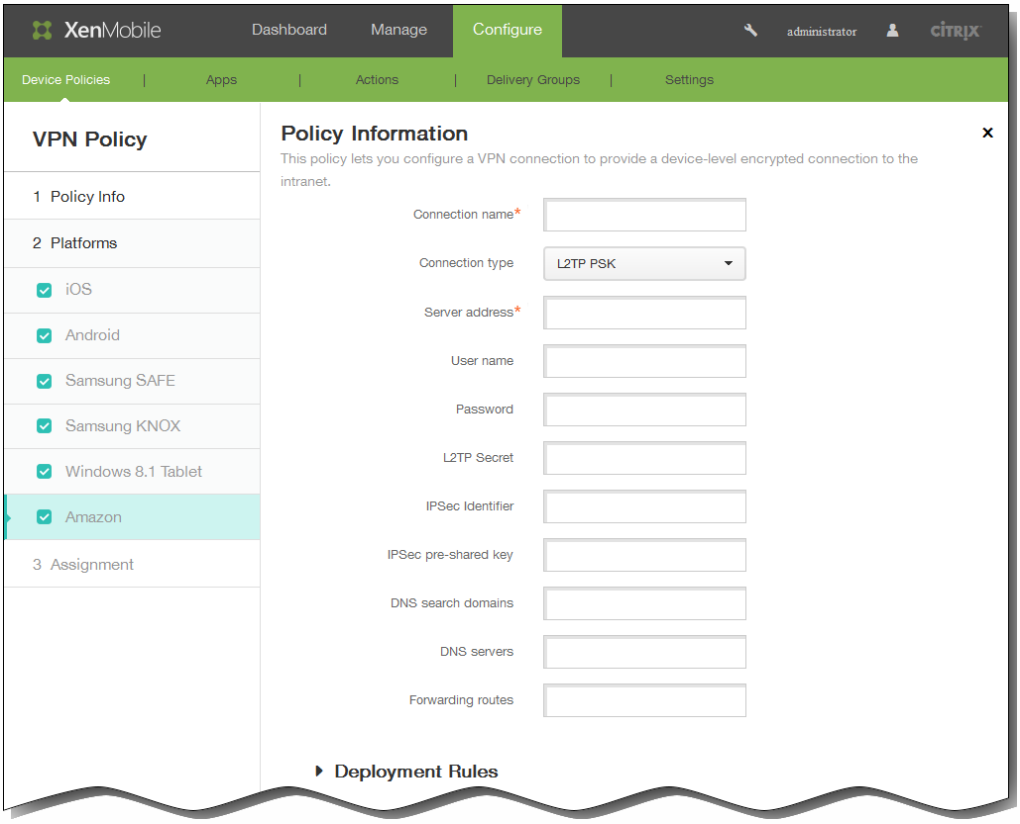
   In der folgenden Tabelle werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich 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	SonicWALL OFF	Check Point OFF	Juniper OFF	Microsoft Word OFF	F5 OFF
Idle connection lifetime (seconds)	Erforderlich	Erforderlich	Erforderlich	Erforderlich	Erforderlich
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 VPN server name	– **SonicWALL** –	– **Check Point** –	– **Juniper** –	Erforderlich **Microsoft Word** Erforderlich	– **F5** –
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

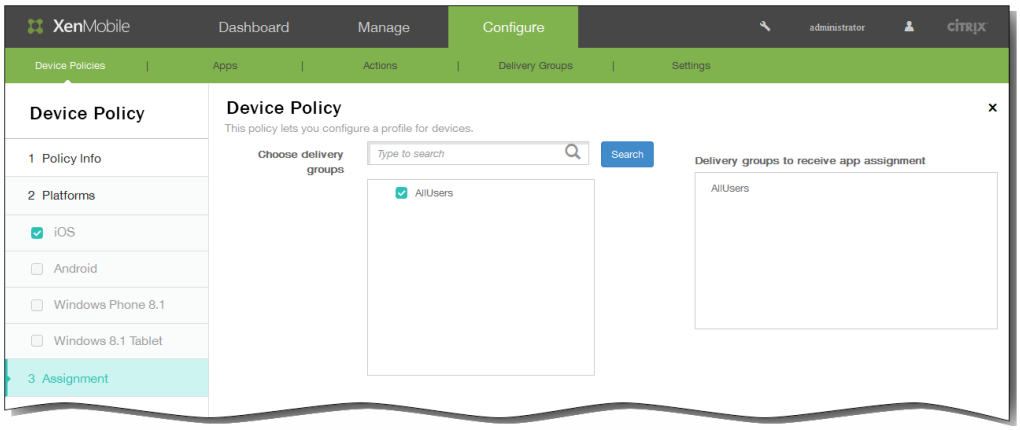
In der folgenden Tabelle werden die Konfigurationsoptionen für die einzelnen Verbindungsmethoden aufgeführt. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich 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	–	–	–
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.

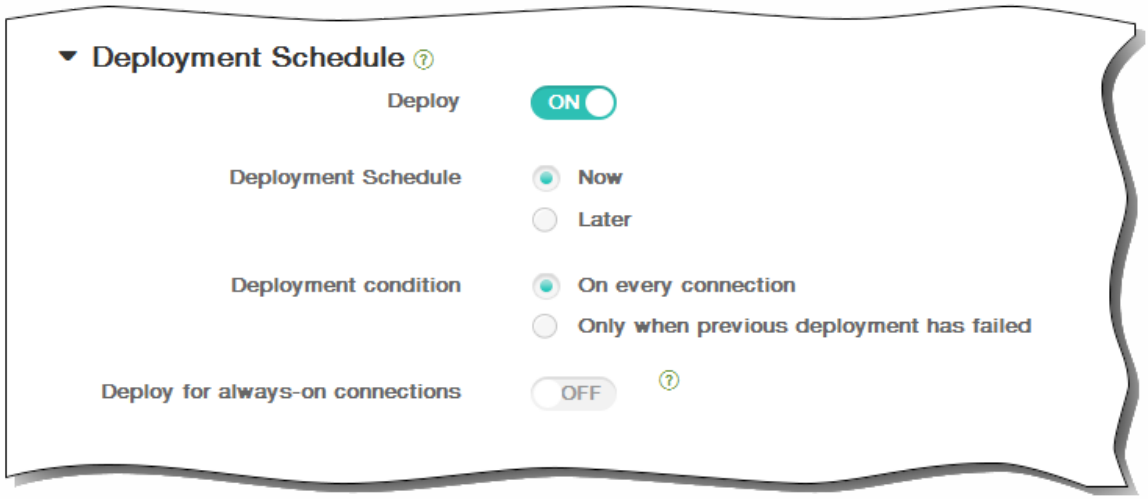
6. Nach Abschluss der Konfiguration der Einstellungen für eine oder mehrere Plattformen klicken Sie auf Next. Es wird dann die Seite Assigment für die VPN-Richtlinie angezeigt.

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.

May 05, 2016

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.

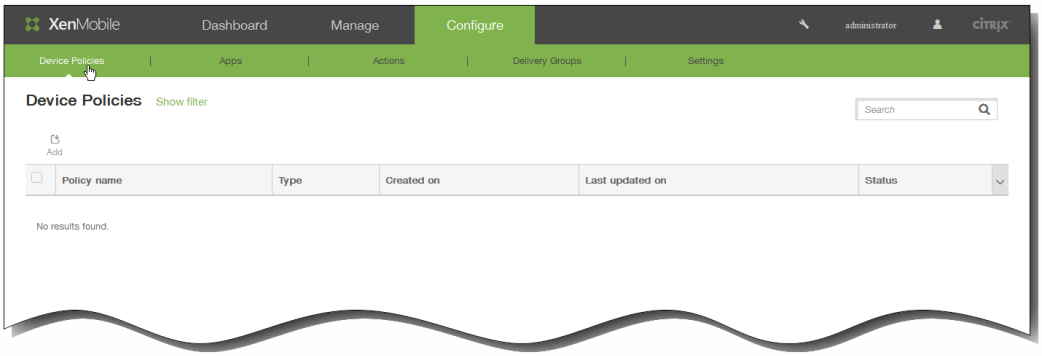
WiFi-Einstellungen können für folgende Plattformen konfiguriert werden: iOS, Android, Windows Phone 8.1 und Windows 8.1-Tablets. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Artikel detailliert beschrieben.

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

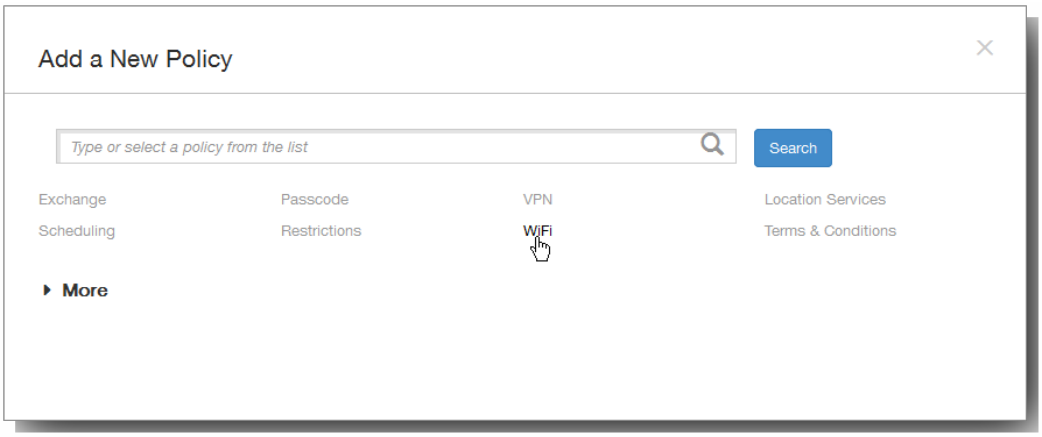
- Erstellen Sie alle Bereitstellungsgruppen, die Sie verwenden möchten.
- Halten Sie Namen und Typ des Netzwerks bereit.
- Planen Sie die zu verwendenden Authentifizierungs-/Sicherheitstypen.
- Halten alle ggf. erforderlichen Proxyserverinformationen bereit.
- Installieren Sie alle erforderlichen Zertifizierungsstellenzertifikate.
- Halten Sie alle erforderlichen gemeinsamen Schlüssel bereit.

So erstellen Sie eine neue WiFi-Geräterichtlinie

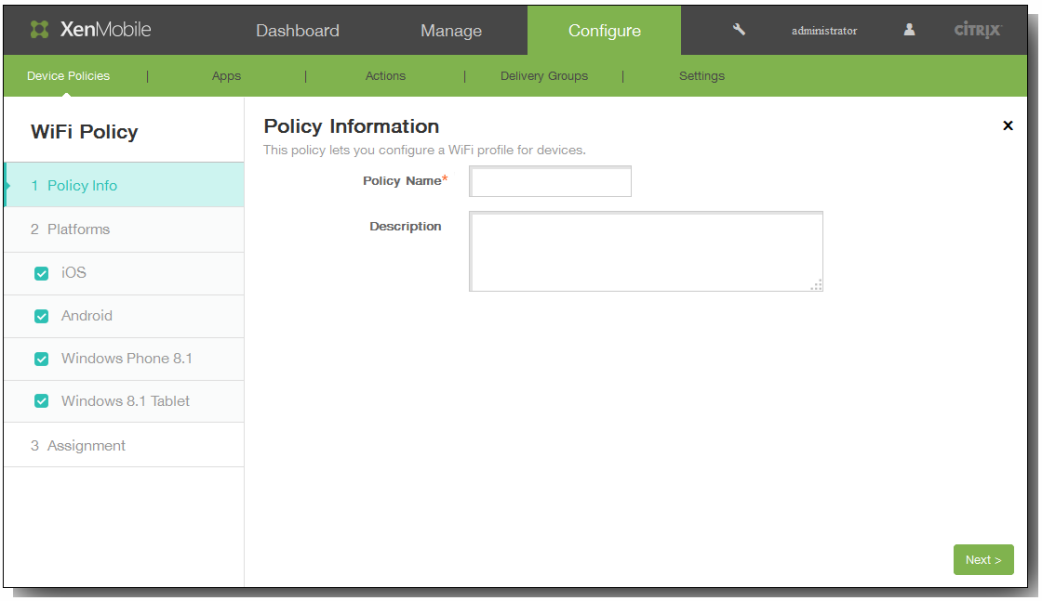
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



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	–	–	–	–	MSCHAPv2 (wenn TTLS	**MSCHAPv2 (wenn TTLS**	MSCHAPv2 (wenn TTLS

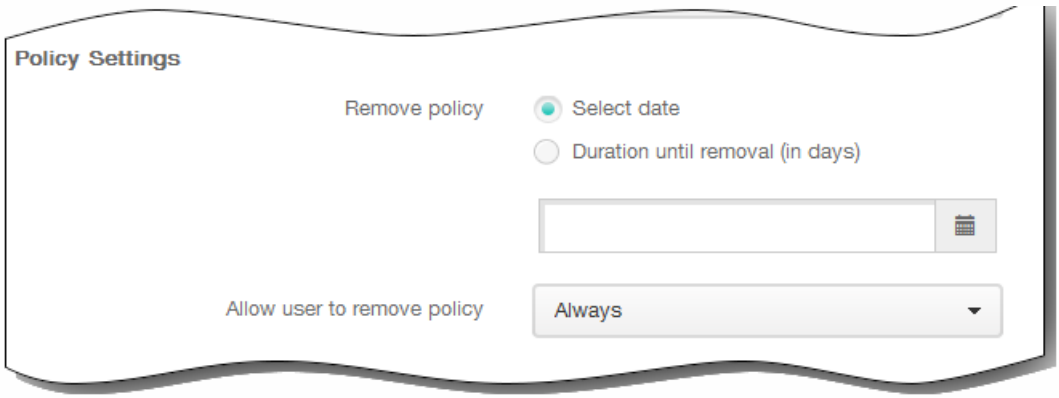
(TTLS) Outer identity	**Keine**	**WEP**	**WPA/WPA2 Personal**	**Any (Personal)**	**WEP Enterprise** = On)	**WPA/WPA2 Enterprise** = On)	**Any (Enterprise)** = On)
	–	–	–	–	Optional (wenn PEAP, TTLS oder EAP-FAST = On)	Optional (wenn PEAP, TTLS oder EAP-FAST = On)	Optional (wenn PEAP, TTLS oder EAP-FAST = On)
Use 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

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.

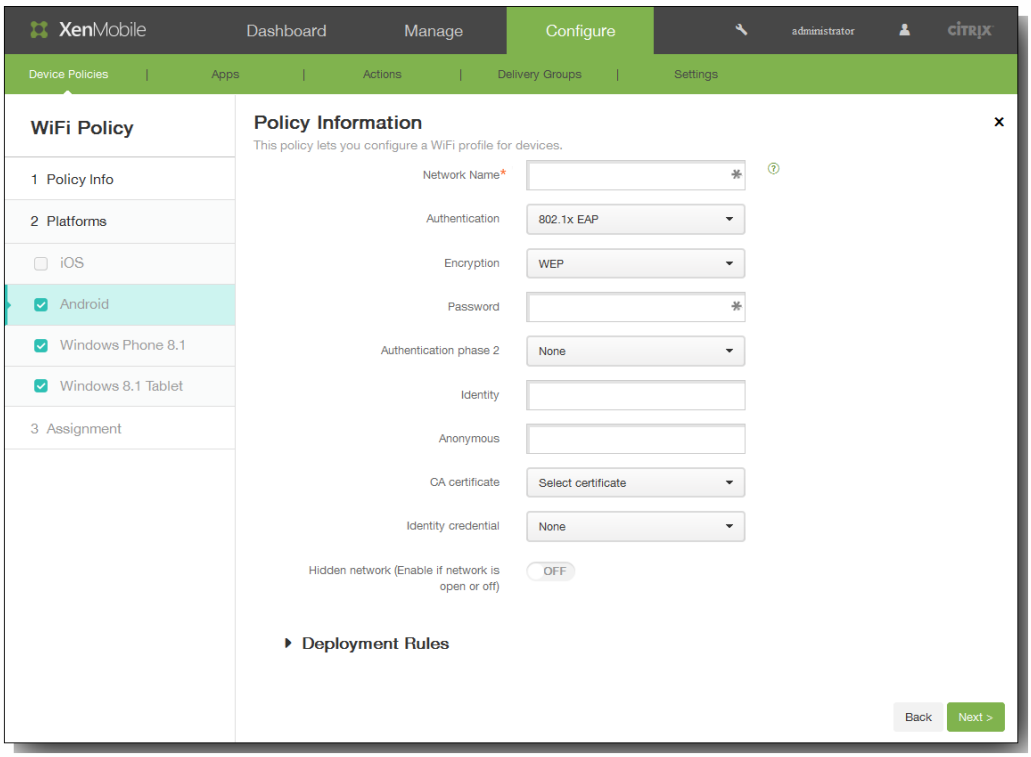
	Manuell	Automatisch
Host name or IP address for the proxy server	Erforderlich	–
Port for the proxy server	Erforderlich	–
User name	Optional	–
Password	Optional	–
Proxy server URL	–	Erforderlich
Allow direct connection if PAC is unreachable	–	On (iOS 7.0 und höher)

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

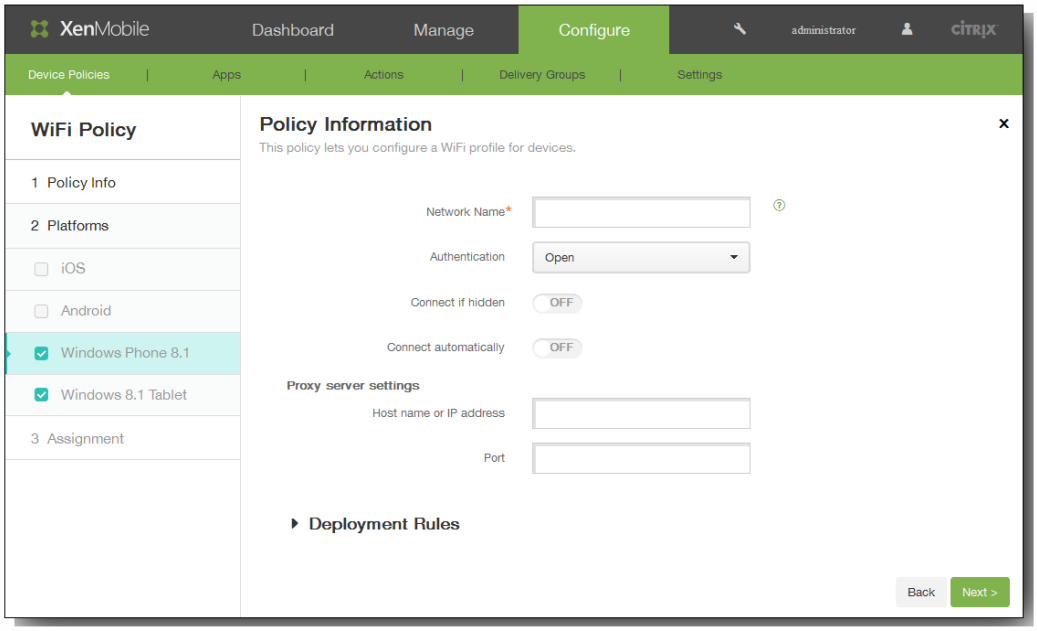
   In der folgenden Tabelle werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), 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	Open	Shared	WPA	WPA-PSK	WPA2	WPA2-PSK	802.1 EAP
Anonymous	–	–	–	–	–	–	Optional
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

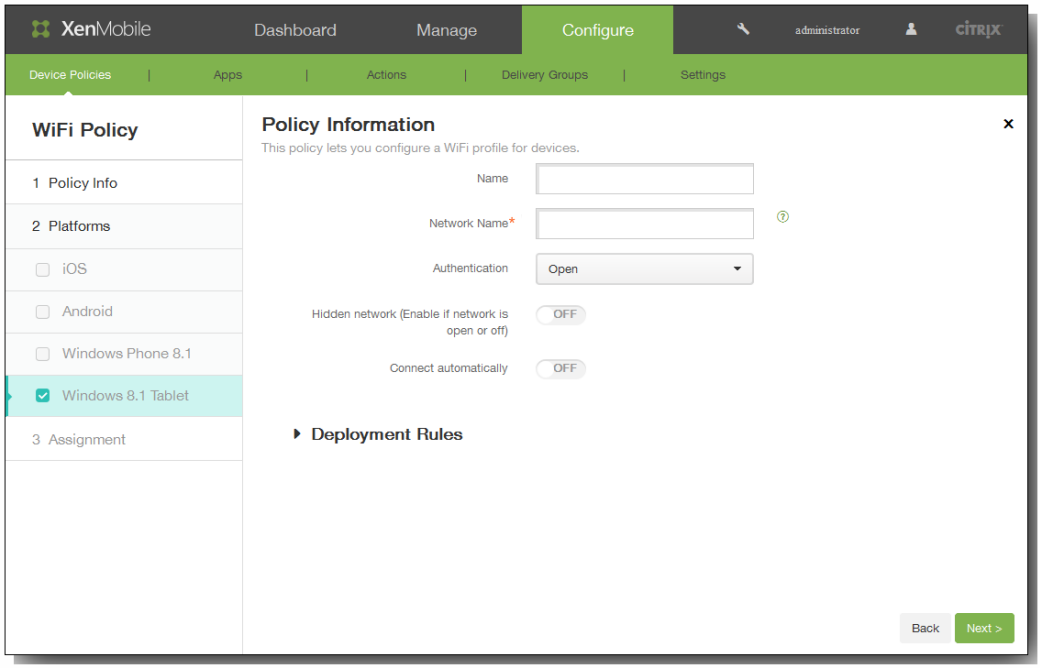
   In der folgenden Tabelle werden die Optionen aufgeführt, die für die einzelnen Verbindungsmethoden konfiguriert werden müssen. In jeder Zelle wird der Standardwert für die jeweilige Option angegeben, sofern einer existiert, andernfalls enthält die Zelle einen Hinweis darauf, ob die Option nicht relevant (–), erforderlich oder optional ist.

	Open	WPA Personal	WPA-2 Personal	WPA-2 Enterprise
Verschlüsselung	–	AES	AES	AES

Shared key	Open	WPA Personal	WPA-2 Personal	WPA-2 Enterprise
		Optional	Optional	

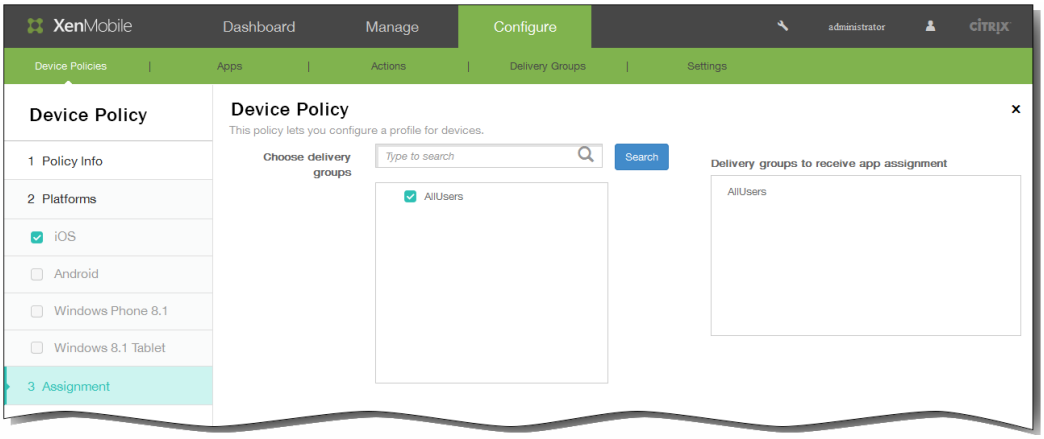
3. Connect if hidden: Wählen Sie aus, ob eine Verbindung hergestellt werden soll, wenn das Netzwerk ausgeblendet ist.
4. Connect automatically: Wählen Sie aus, ob automatisch eine Verbindung mit dem Netzwerk hergestellt werden soll.
5. Host name or IP address: Geben Sie den Namen oder die IP-Adresse eines Proxyservers ein.
6. Port: Geben Sie die Portnummer des Proxyservers ein.

Bei Auswahl von Windows 8.1 tablet konfigurieren Sie die folgenden Einstellungen:



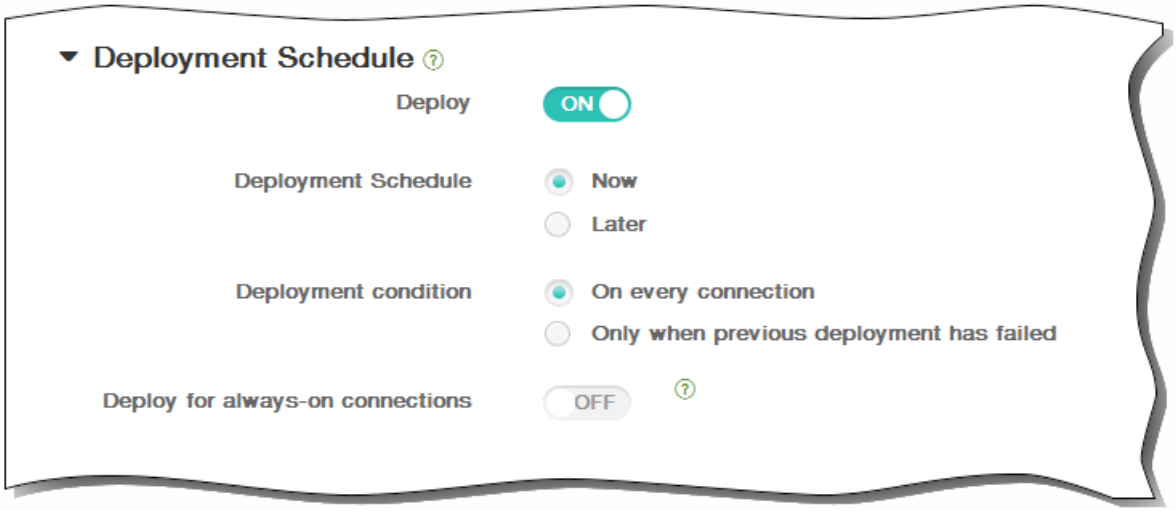
1. Name: Geben Sie einen Namen für das Netzwerk ein.
2. Network name: Geben Sie die SSID ein, die in der Liste der verfügbaren Netzwerke auf den Geräten der Benutzer angezeigt wird.
3. Authentication: Klicken Sie in der Liste auf den Typ der Authentifizierung, der für die WiFi-Verbindung verwendet werden 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.

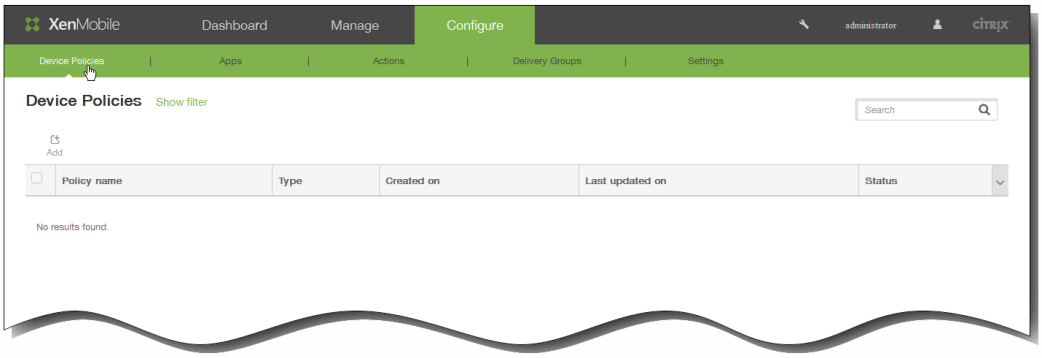
May 05, 2016

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.

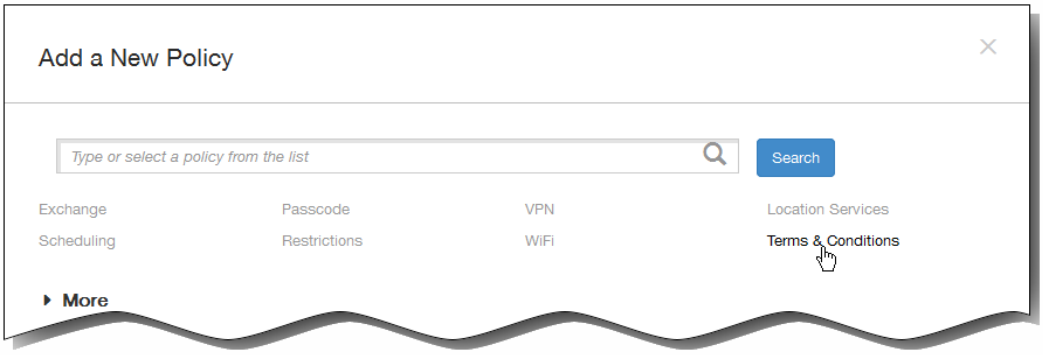
Sie können mehrere Richtlinien für Nutzungsbestimmungen in unterschiedlichen Sprachen erstellen, wenn Ihr Unternehmen internationale Benutzer hat und Sie möchten, dass diese die Nutzungsbestimmungen in ihrer Muttersprache annehmen.

Hinweis: Nutzungsbestimmungen müssen als PDF-Dateien vorliegen.

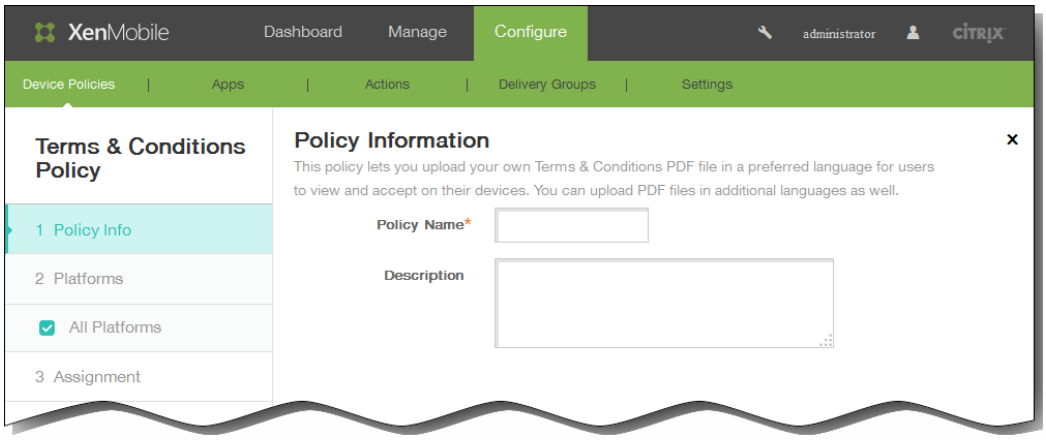
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



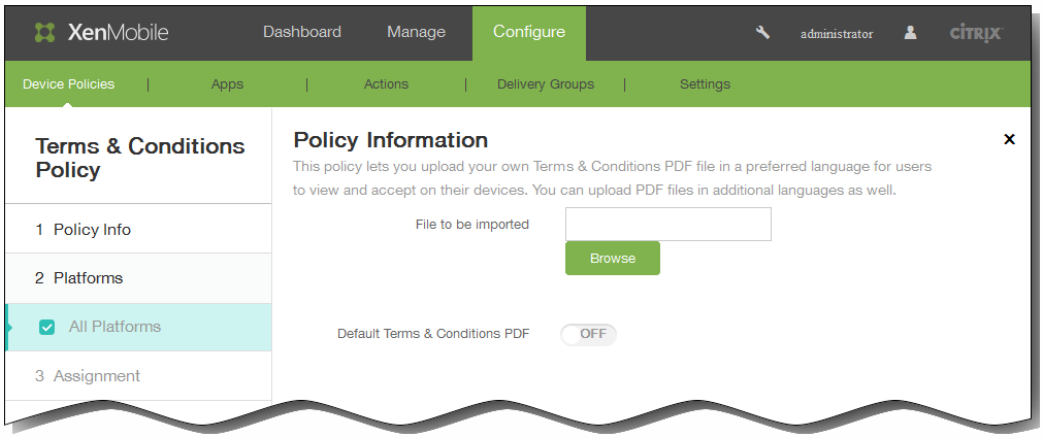
2. Klicken Sie auf Add. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf Terms & Conditions. Die Seite Terms & Conditions Policy wird angezeigt.

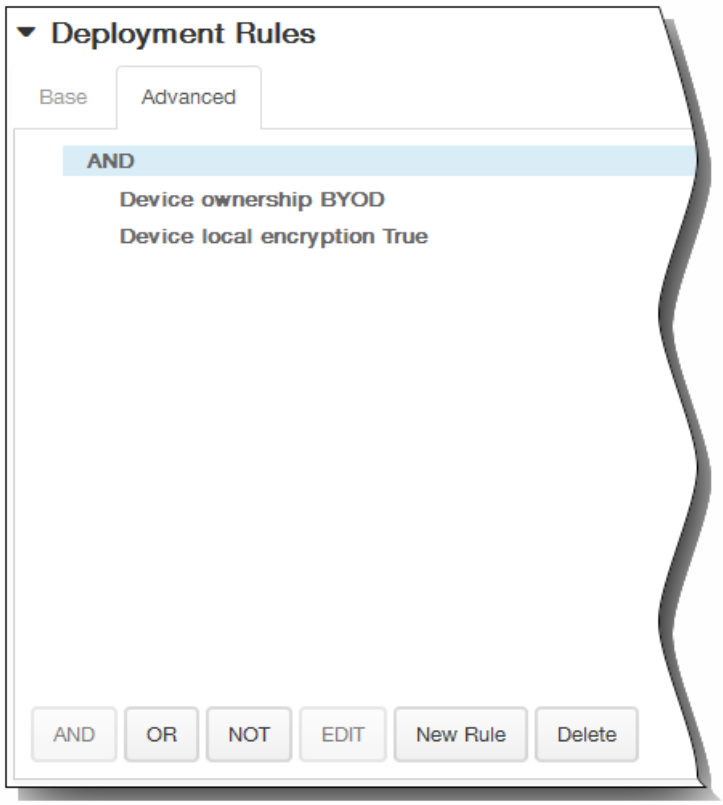


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Informationsseite All Platforms wird angezeigt.



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.

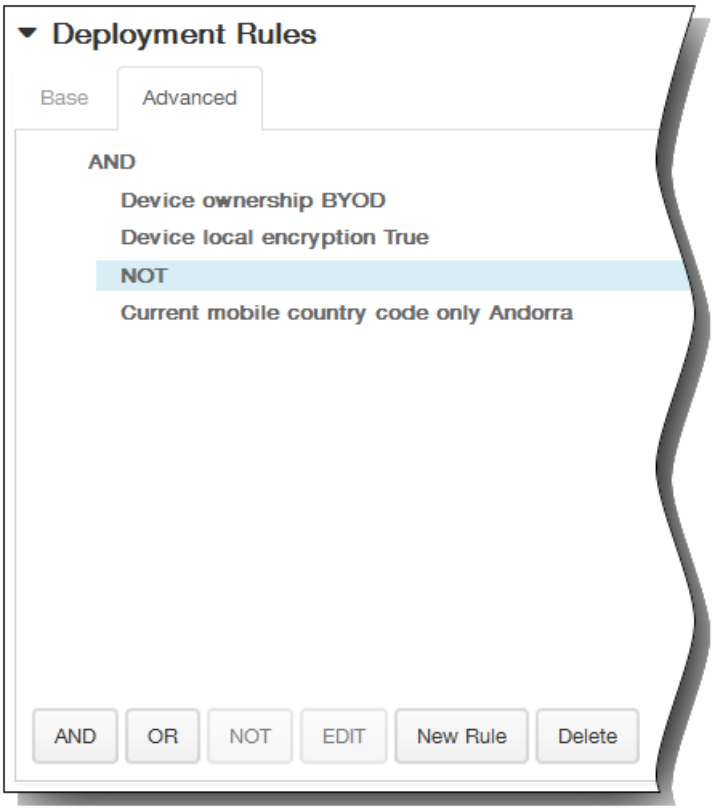
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
   1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
   2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
   3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
   4. Klicken Sie noch einmal 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.



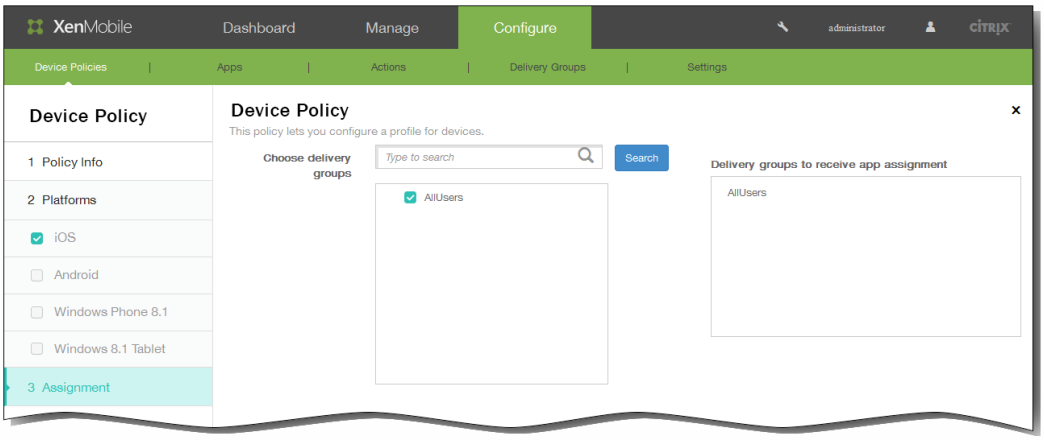
   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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 noch einmal 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.



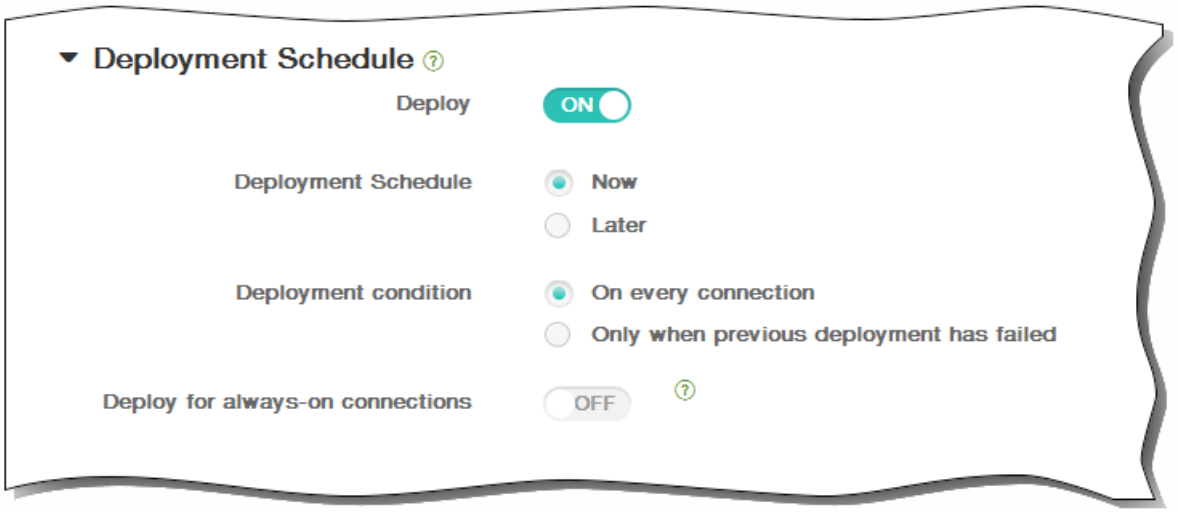
8. Klicken Sie auf Next. Die Seite Assignment für die Nutzungsbestimmungen-Richtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten 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.

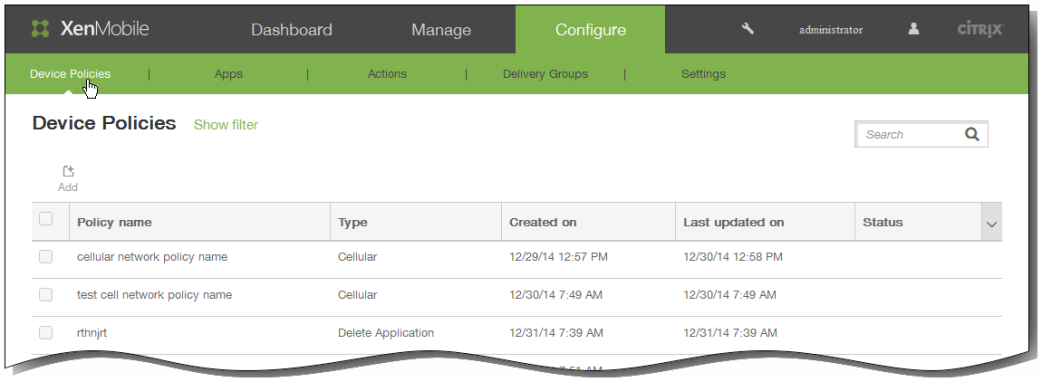


11. Klicken Sie auf Save, um die Richtlinie zu speichern.

May 05, 2016

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.

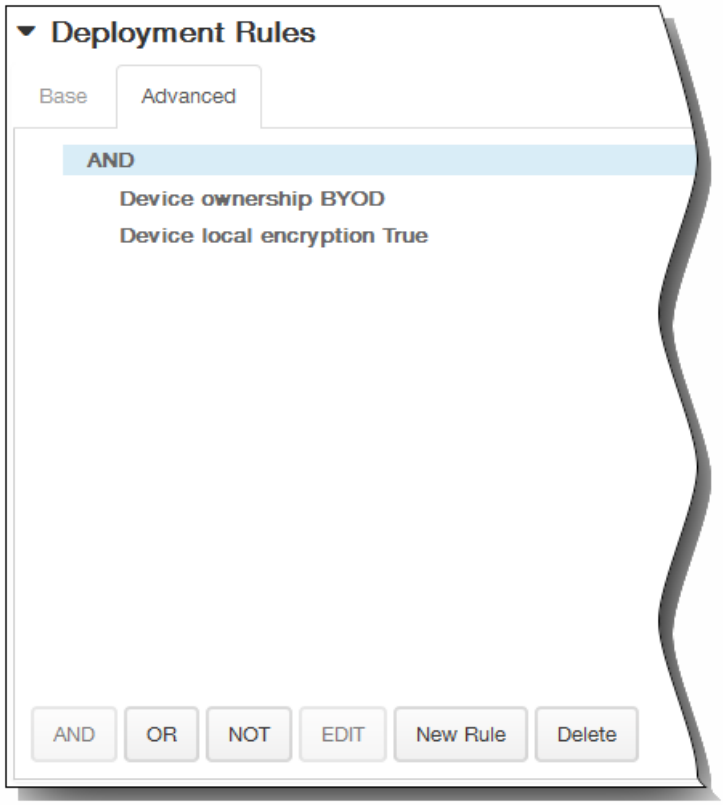


2. Klicken Sie auf der Seite Add a New Policy auf More > Worx Store.
3. Geben Sie auf der Seite Worx Store Policy im Bereich Policy Information folgende Informationen ein und klicken Sie auf Next.
    1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
    2. Description: Geben 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.

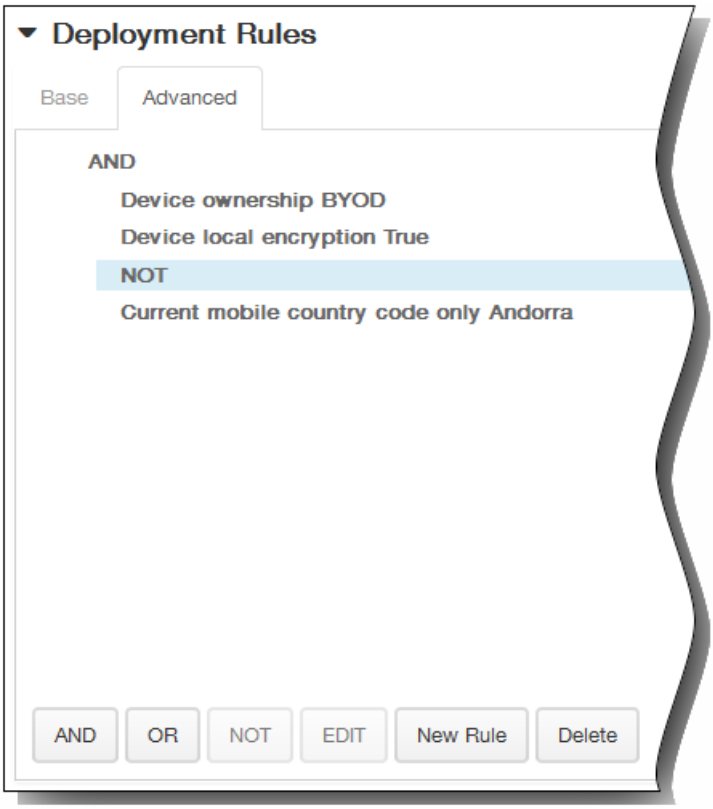
2. Klicken Sie auf New Rule, um Bedingungen zu definieren.
3. Klicken Sie in der Liste auf Bedingungen wie Device ownership oder BYOD (siehe Abbildung oben).
4. Klicken Sie erneut auf New Rule, wenn Sie weitere Bedingungen hinzufügen möchten. Sie können beliebig viele Bedingungen hinzufügen.

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

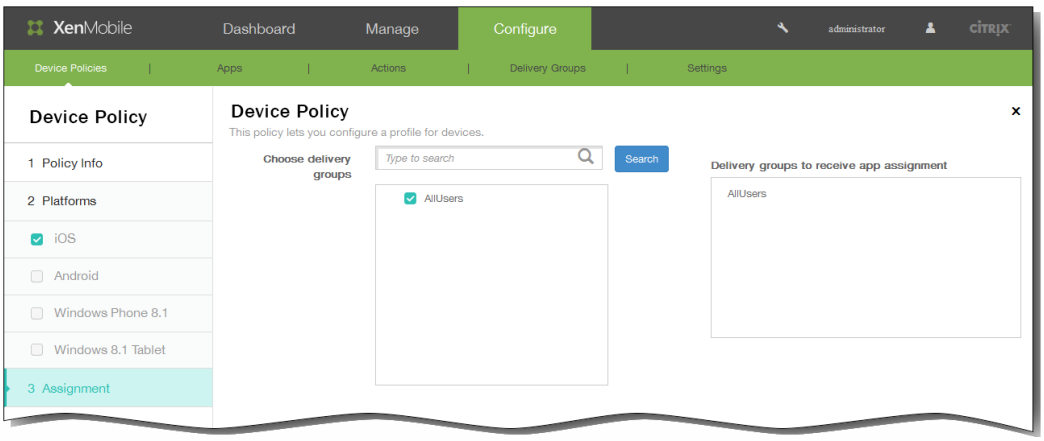


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.

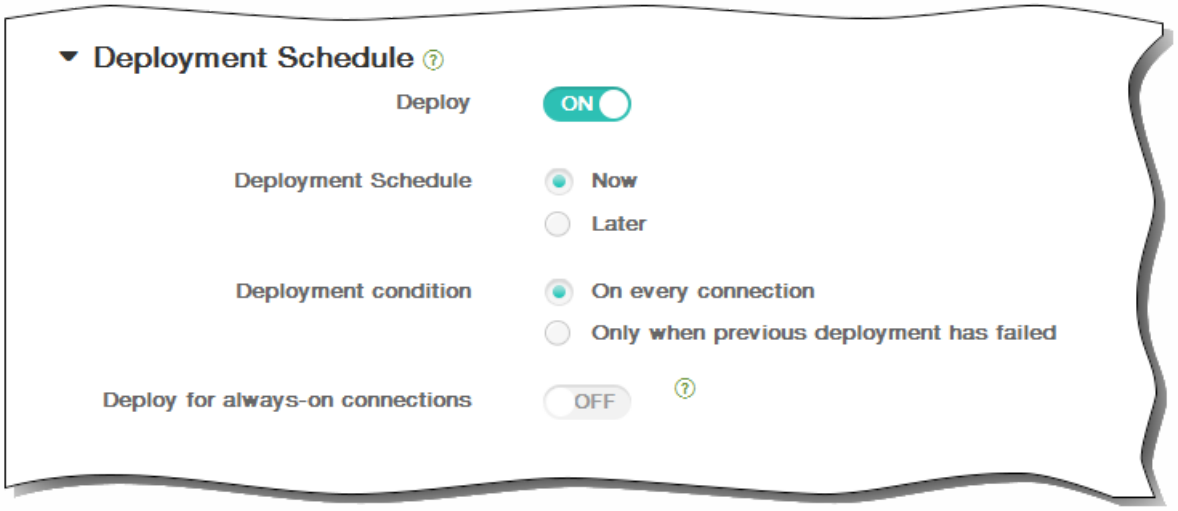


9. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
   1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert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

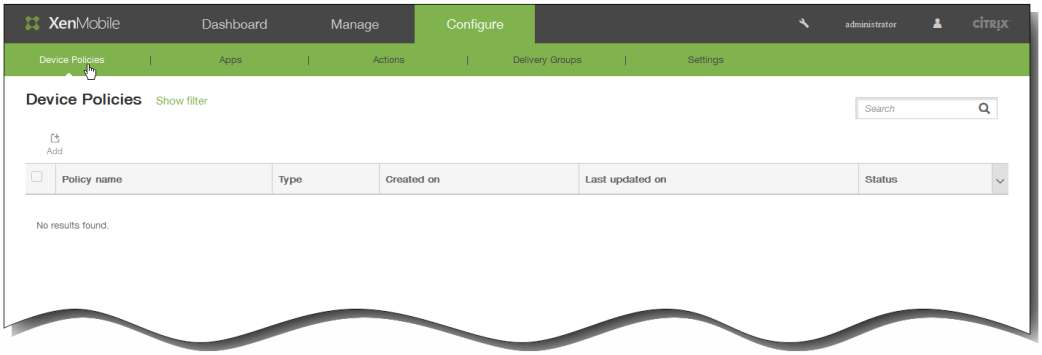


10. Klicken Sie auf Save, um die Richtlinie zu speichern.

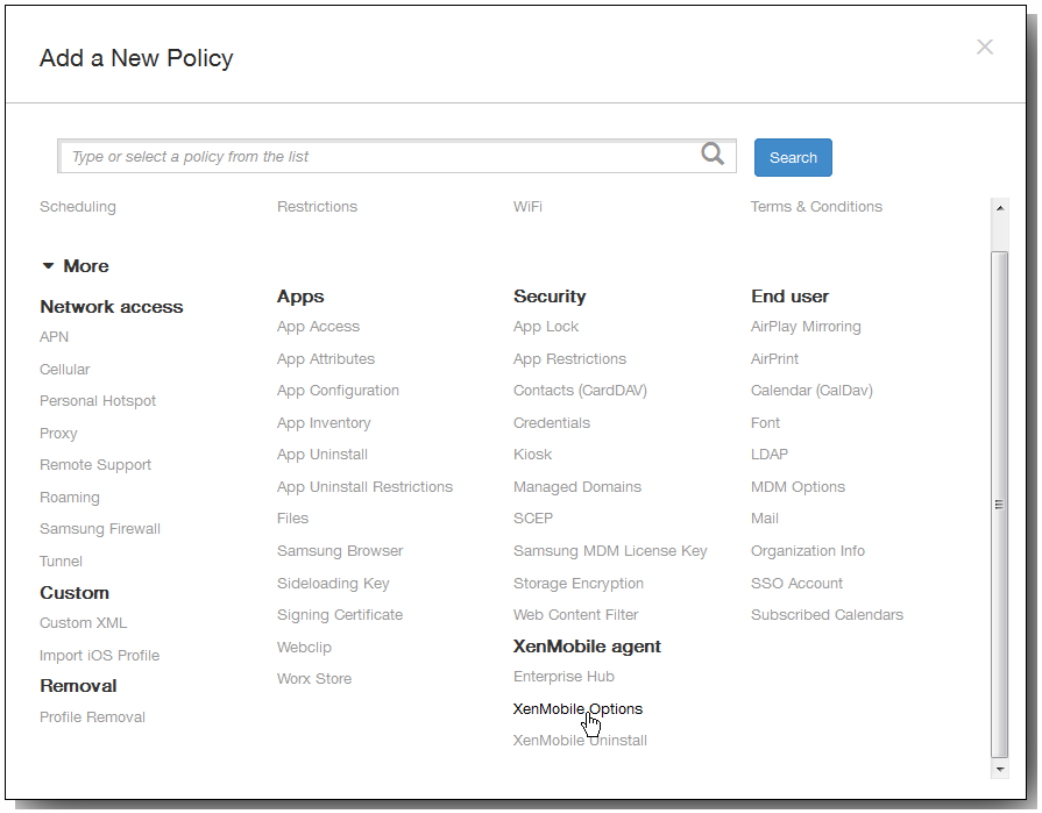
May 05, 2016

Sie fügen eine XenMobile-Optionsrichtlinie hinzu, um das Worx Home-Verhalten für Verbindungen zwischen XenMobile und Android- bzw. Symbian-Geräten zu konfigurieren.

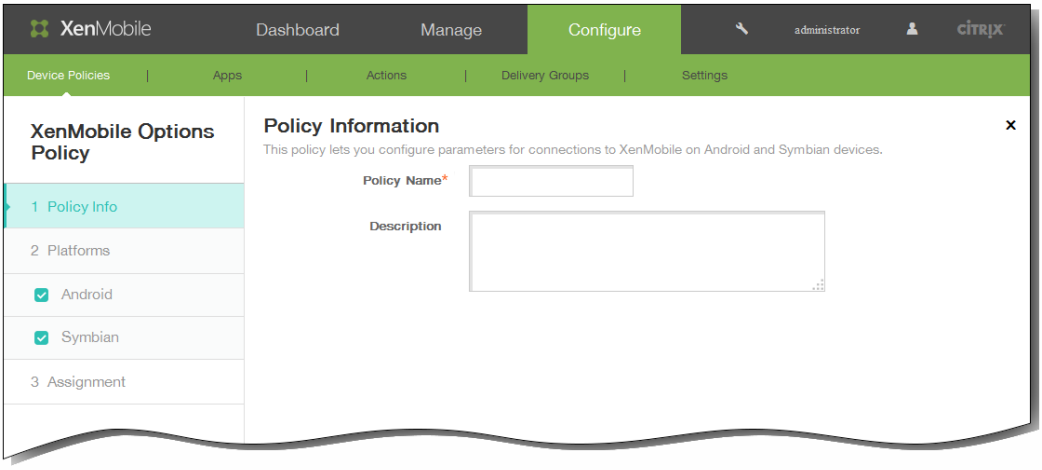
1. Klicken Sie in der XenMobile-Konsole auf Configure > Device Policies. Die Seite Device Policies wird angezeigt.



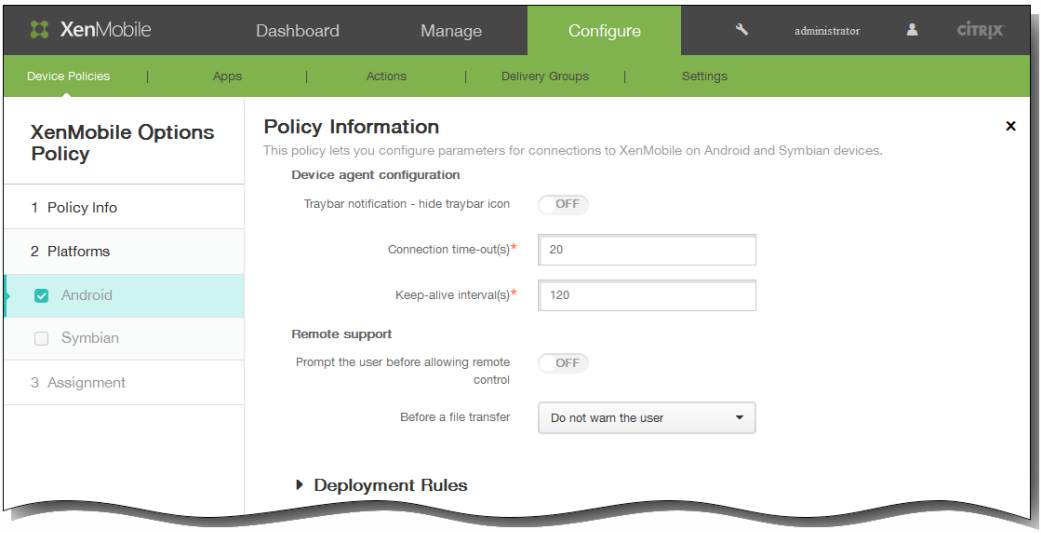
2. Klicken Sie auf Add. Das Dialogfeld Add a New Policy wird angezeigt.



3. Klicken Sie auf More und dann unter XenMobile agent auf XenMobile Options. Die Seite XenMobile Options Policy wird angezeigt.



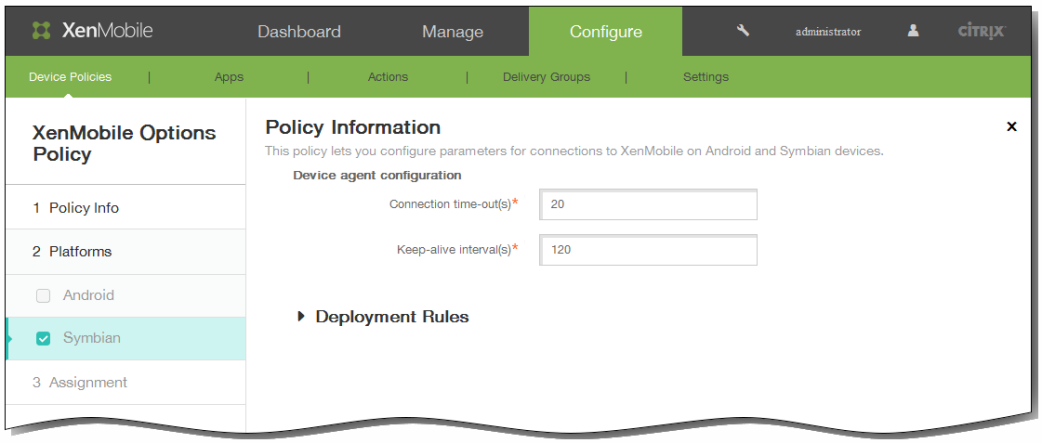
4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
   3. Klicken Sie auf Next.
5. Wählen Sie unter Platforms die gewünschten 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.

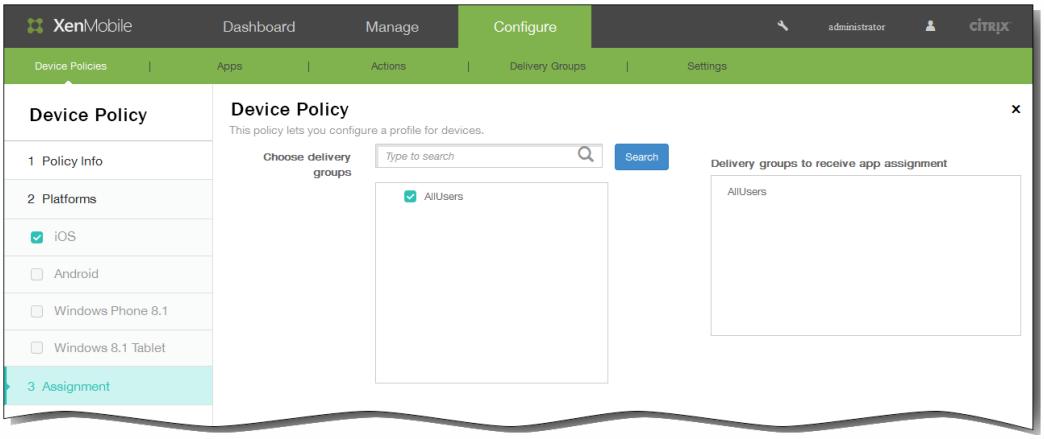
5. Before a file transfer: Wählen Sie in der Liste aus, ob Benutzer bei einer Dateiübertragung gewarnt oder um Erlaubnis gebeten werden sollen.

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.

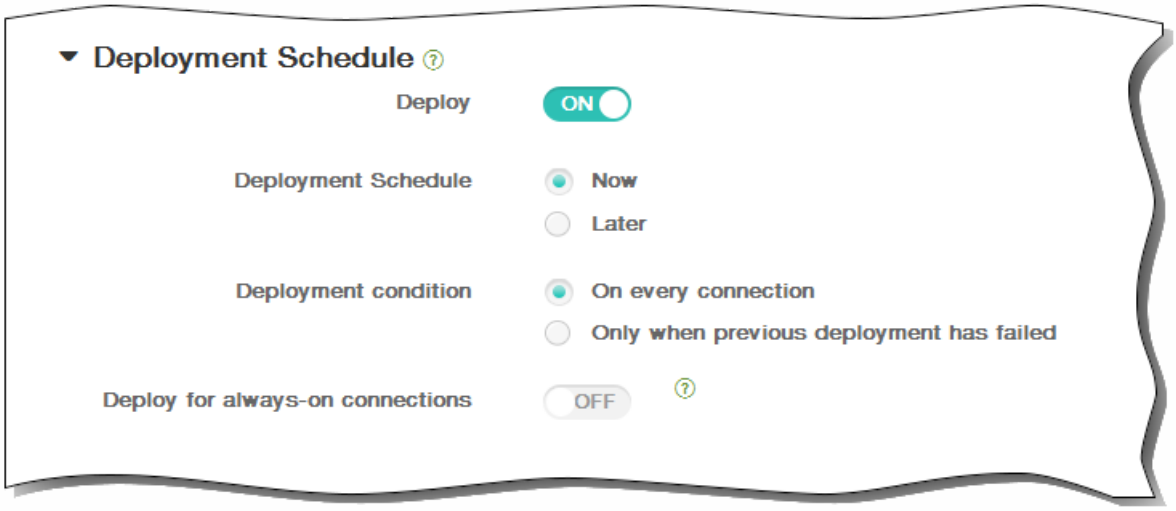


8. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
   1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert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

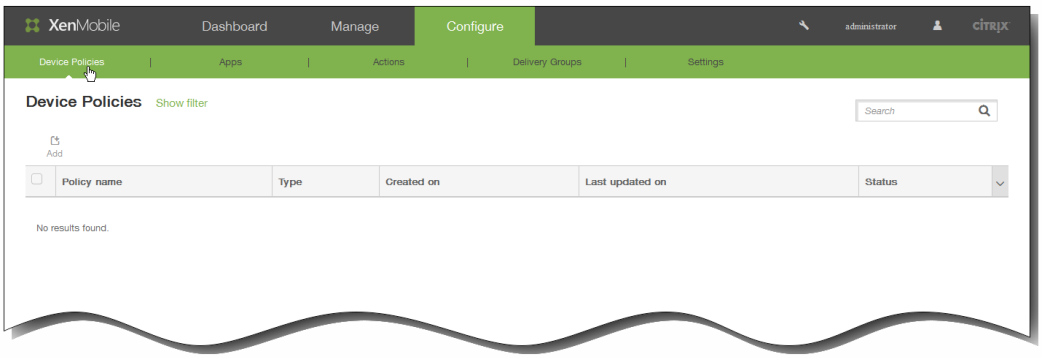


9. Klicken Sie auf Save, um die Richtlinie zu speichern.

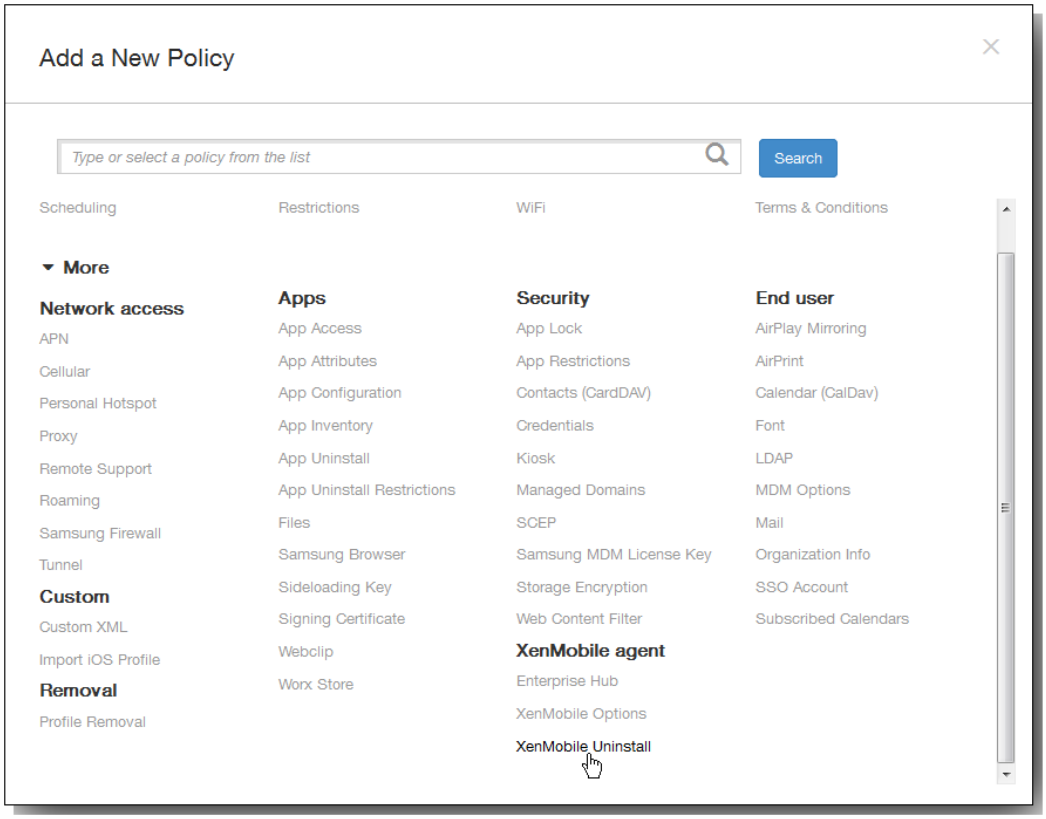
May 05, 2016

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.

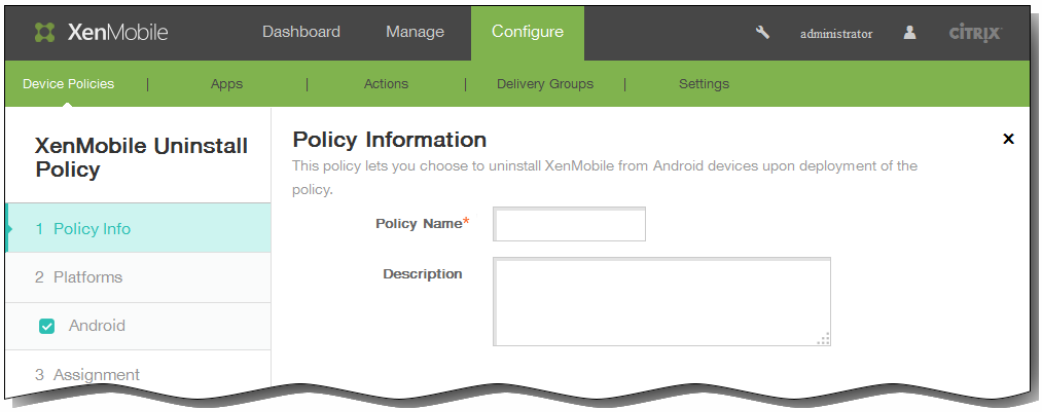


2. Klicken Sie auf Add. Das Dialogfeld Add a New Policy wird angezeigt.

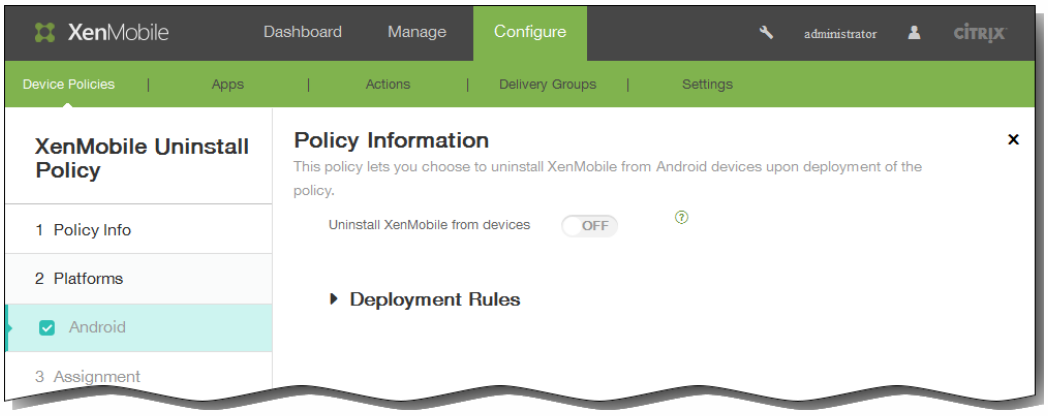


3. Klicken Sie auf More und dann unter XenMobile agent auf XenMobile Uninstall. Die Seite XenMobile Uninstall Policy wird

angezeigt.

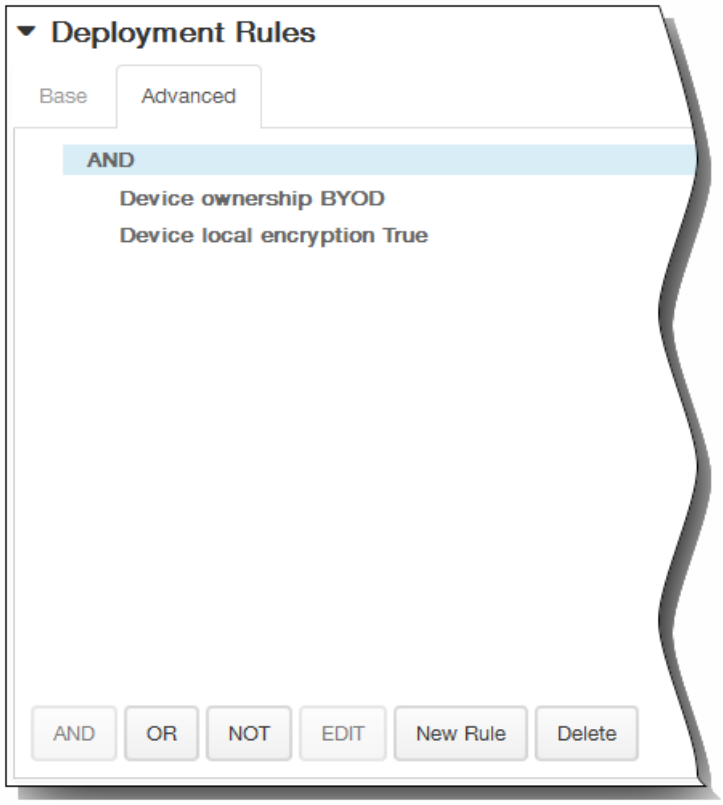


4. Geben Sie im Bereich Policy Information die folgenden Informationen ein:
   1. Policy Name: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
   2. Description: Geben Sie optional eine Beschreibung der Richtlinie ein.
5. Klicken Sie auf Next. Die Informationsseite Android Platform wird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

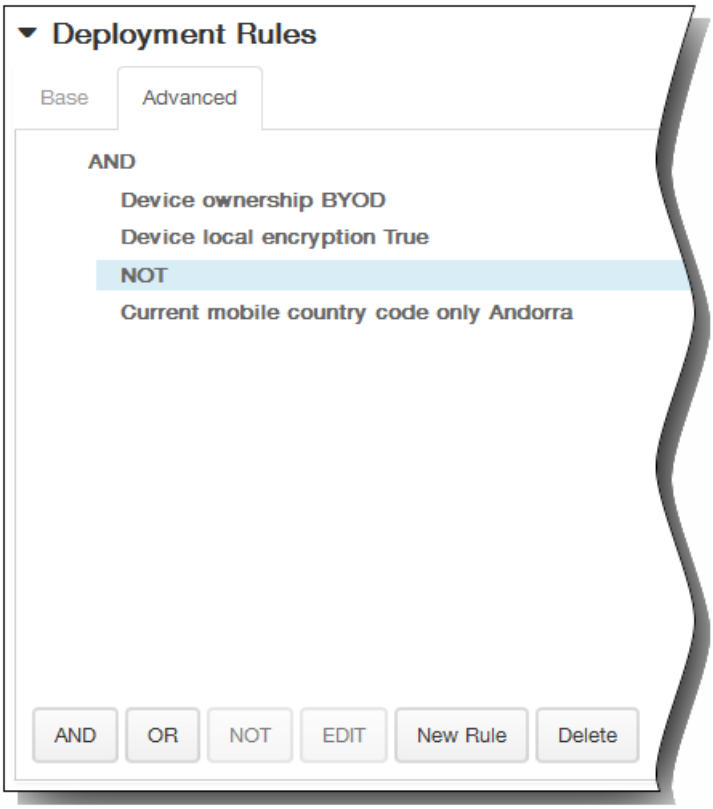
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die Richtlinie bereitgestellt werden soll.
    1. Sie können die Richtlinie bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist All.
    2. Klicken Sie auf New Rule, um Bedingungen 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.



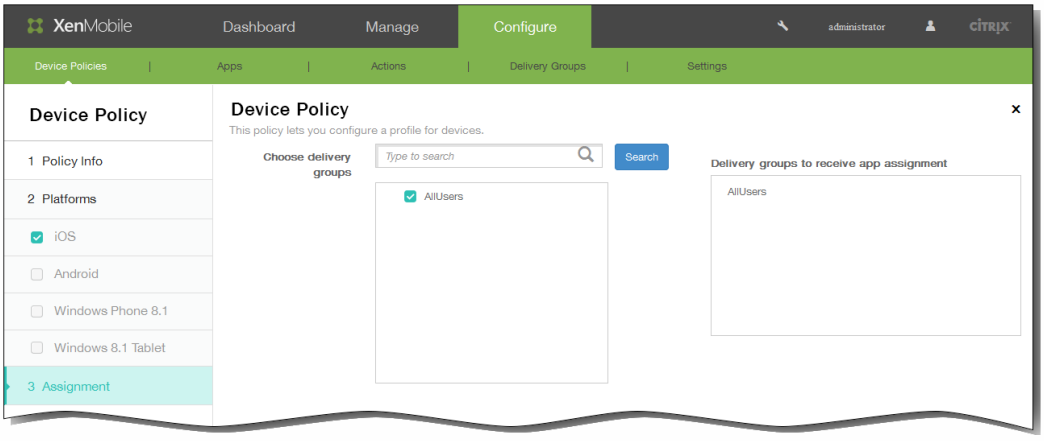
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



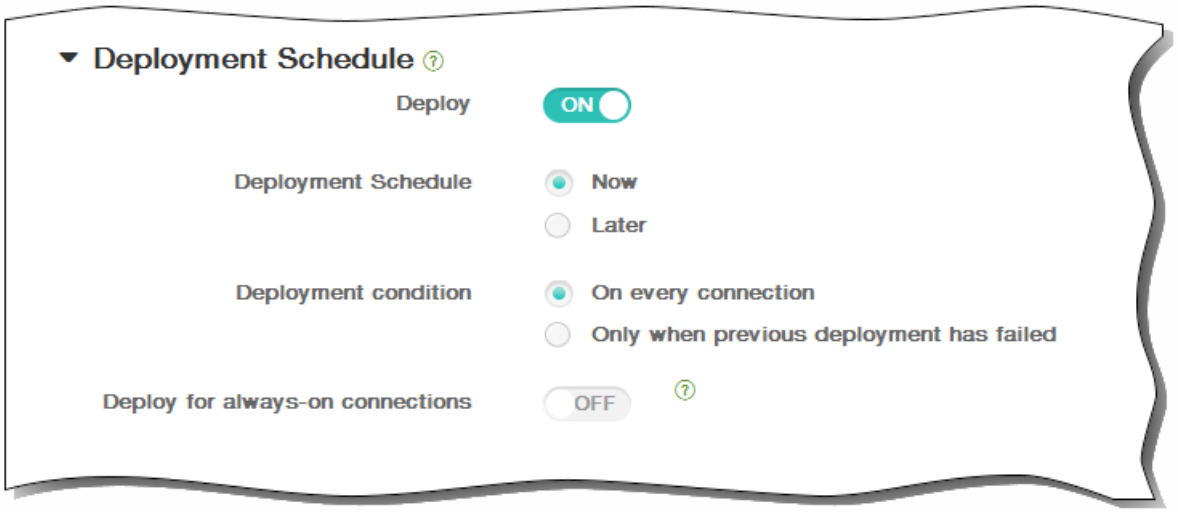
8. Klicken Sie auf Next. Die Seite Assignment für die XenMobile-Deinstallationsrichtlinie wird angezeigt.
9. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese 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.

May 05, 2016

Zur Verwendung des Apple Configurators brauchen Sie einen Apple-Computer mit OS X 10.7.2 oder höher.

> 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.

May 05, 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.

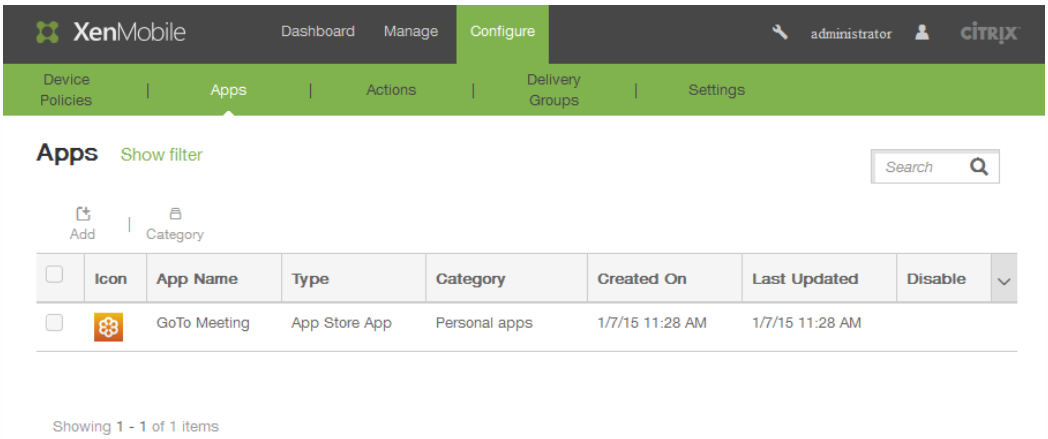
Funktionsweise von Weblinks

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 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

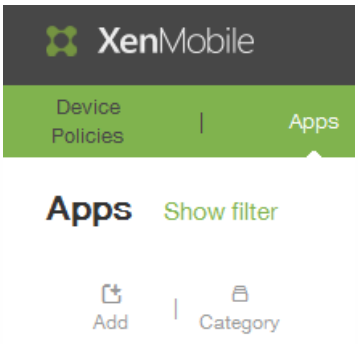
Hinweis: Nachdem Sie Apps hinzugefügt haben, werden diese in der Tabelle auf der Seite "Apps" angezeigt, wo Sie sie bearbeiten oder kategorisieren können.

So fügen Sie App-Kategorien hinzu

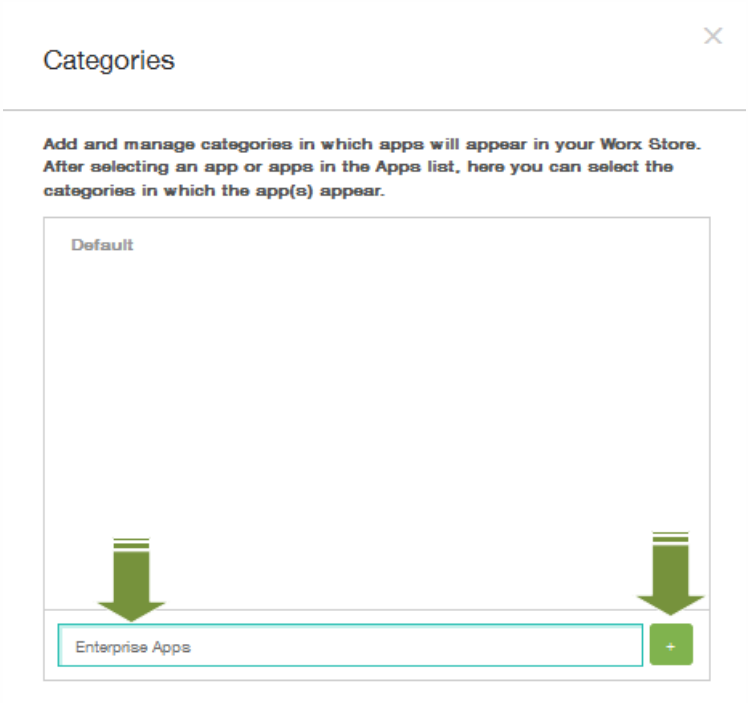
Wenn Benutzer sich bei Worx Home anmelden, erhalten sie eine Liste der Apps, Weblinks und Stores, die Sie in XenMobile

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.

1. Klicken Sie in der XenMobile-Konsole auf Configure > Apps. Die Seite Apps wird angezeigt.
2. Klicken Sie auf der Seite Apps auf Category.



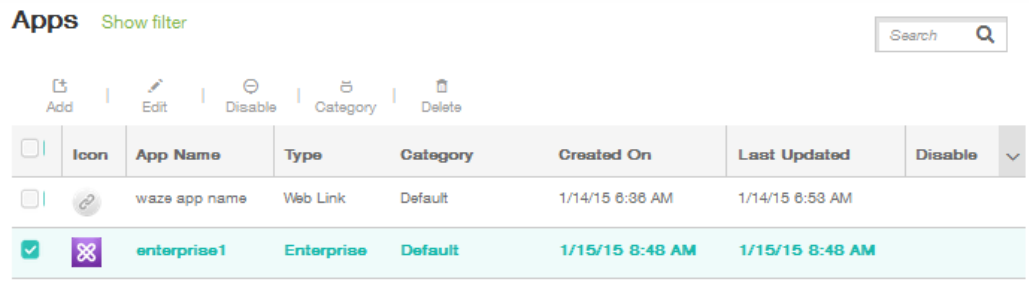
3. Geben Sie im Dialogfeld Categories den Namen der Kategorie ein, die Sie hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) . Geben Sie beispielsweise *Enterprise Apps* ein und klicken Sie auf das Pluszeichen (+).



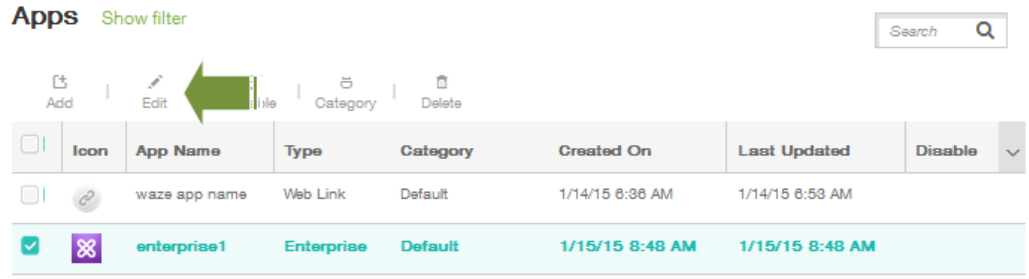
Die neu erstellte Kategorie wird hinzugefügt und wird im gleichen Dialogfeld Categories angezeigt. Wenn keine Kategorien konfiguriert sind, wird nur die Kategorie **Default** angezeigt.

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.

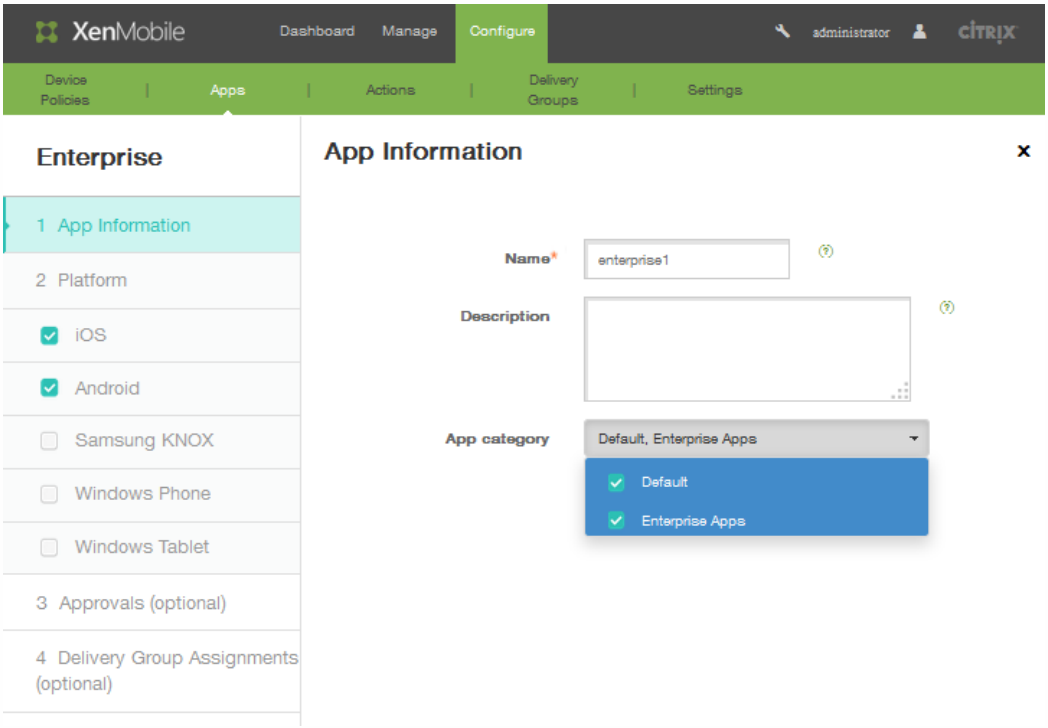


6. Klicken Sie auf Edit, um die App zu kategorisieren.

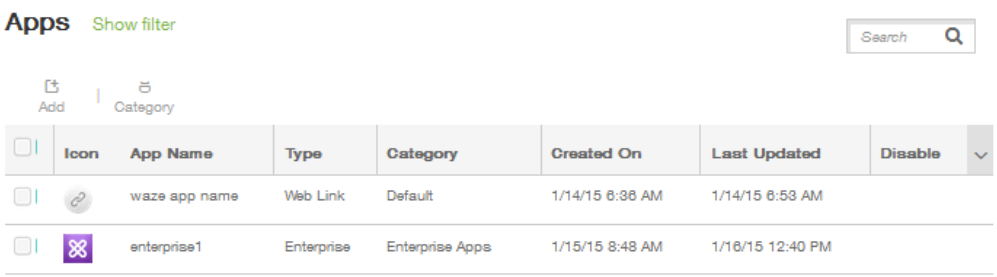


Die Seite App Information wird angezeigt.

7. Wenden Sie die gewünschte Kategorie an, indem Sie das zugehörige Kontrollkästchen in der Liste App category aktivieren.



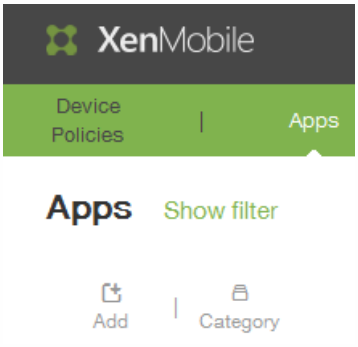
8. Klicken Sie jeweils auf Next, um die weiteren Seiten der App-Konfiguration auszufüllen.
9. Klicken Sie auf der letzten Seite auf Save, um die Kategorie anzuwenden. Die neu erstellte Kategorie wird auf die App angewendet und in der App-Tabelle angezeigt.



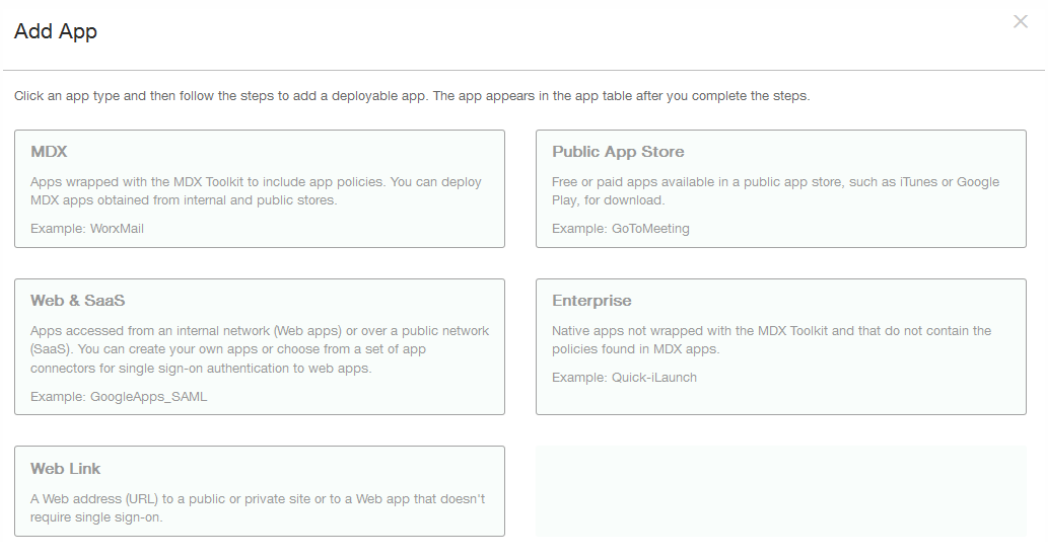
May 05, 2016

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.

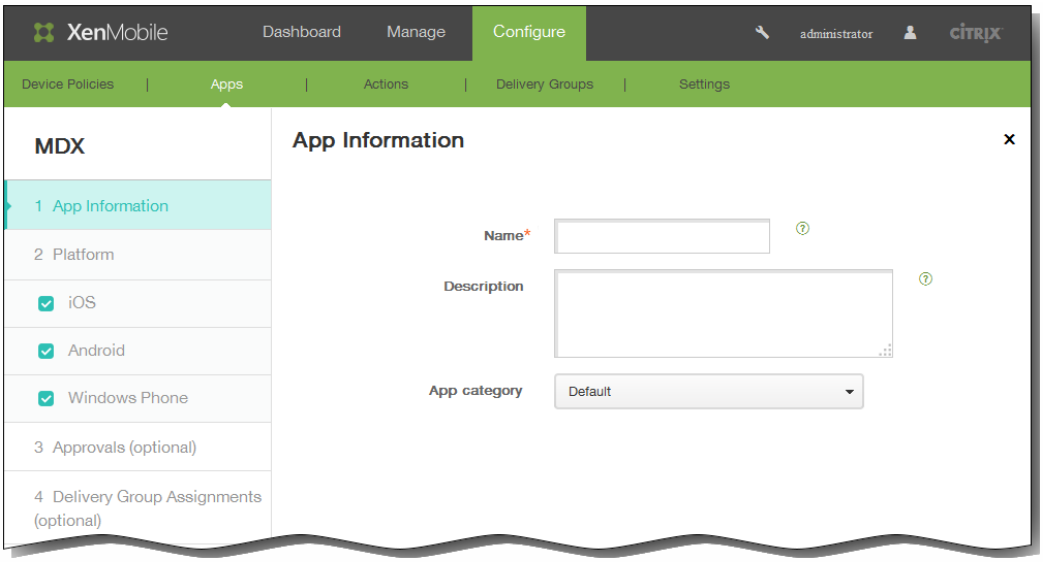
1. Klicken Sie in der XenMobile-Konsole auf Configure > Apps. Die Seite Apps wird angezeigt.
2. Klicken Sie auf Hinzufügen.



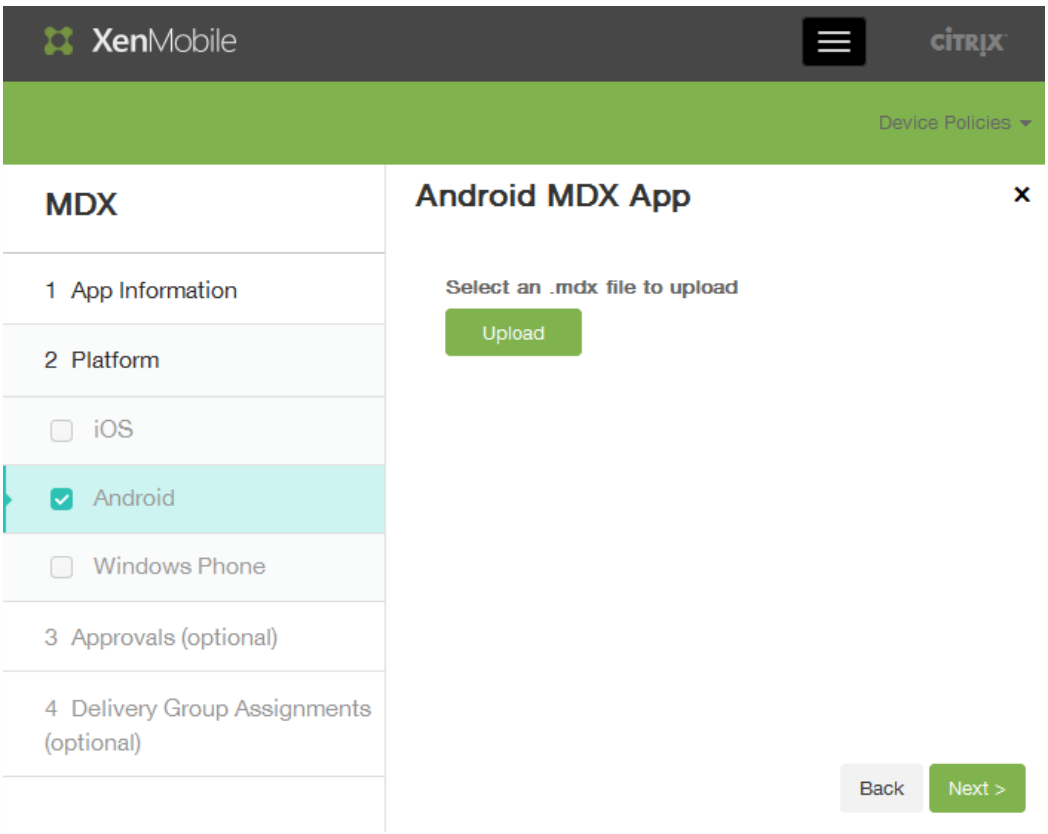
3. Klicken Sie auf der Seite Add App auf MDX.



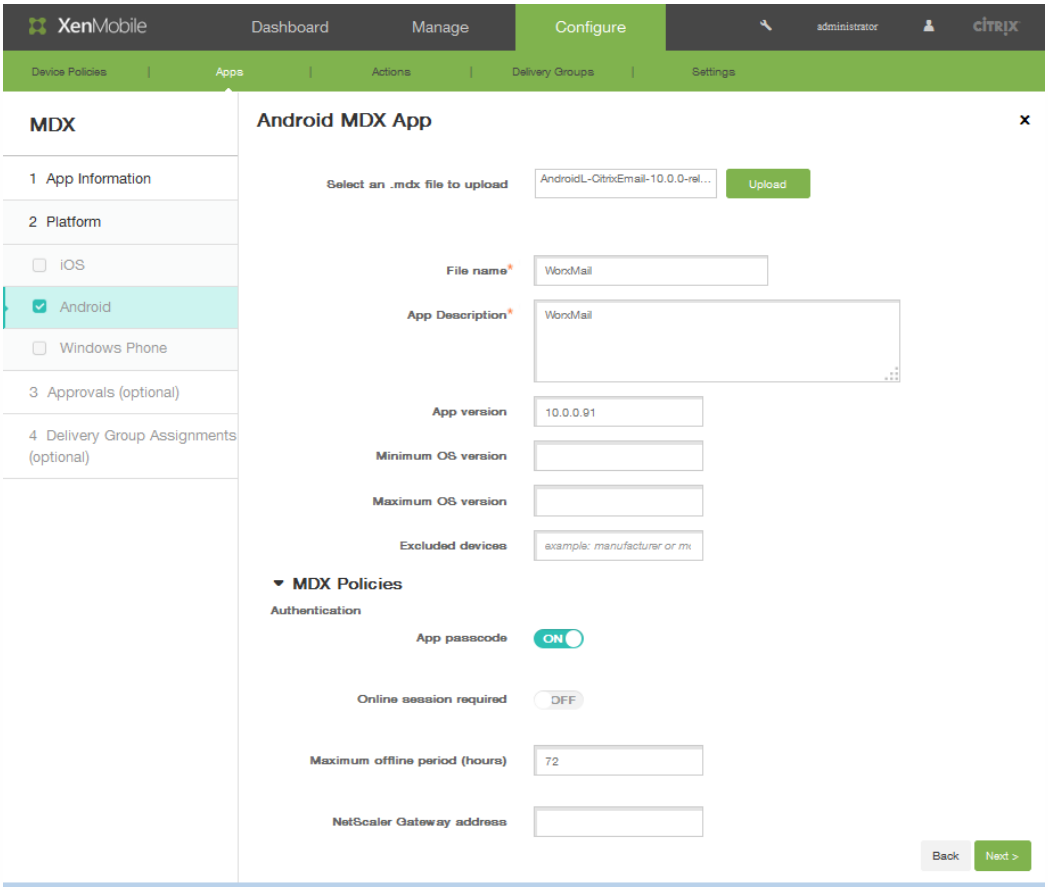
4. Geben Sie auf der Seite App Information unter Name einen Namen und optional unter Description eine Beschreibung für die App ein. Diese Felder werden für interne Zwecke verwendet. Wenn Sie Apps für mehrere Geräte hinzufügen, verwenden Sie die Kontrollkästchen im linken Bereich des Bildschirms, um diese 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.

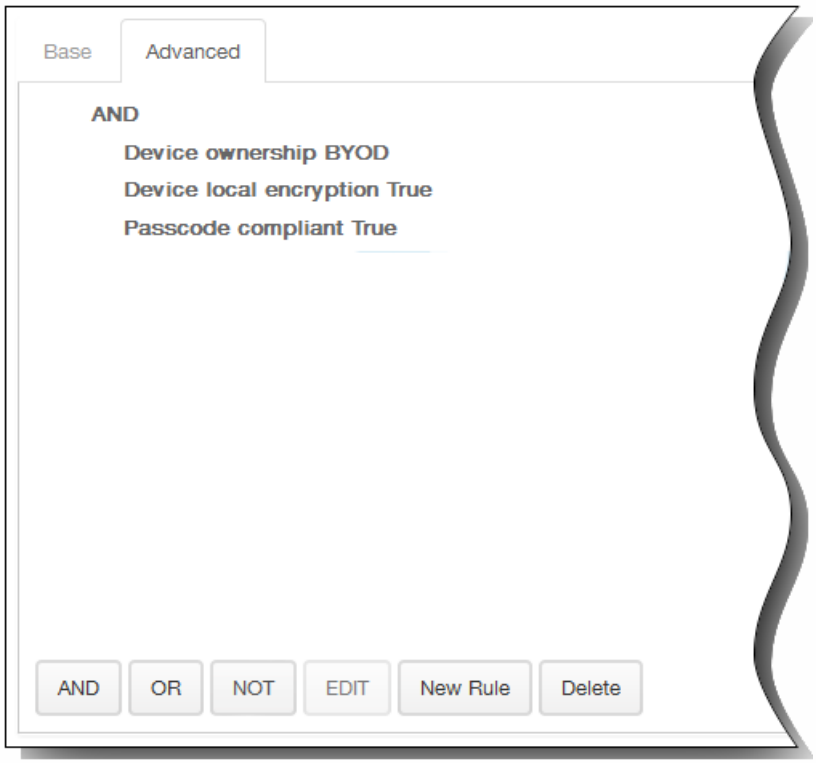


Die Felder für die App-Details und MDX-Richtlinien werden angezeigt.



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.

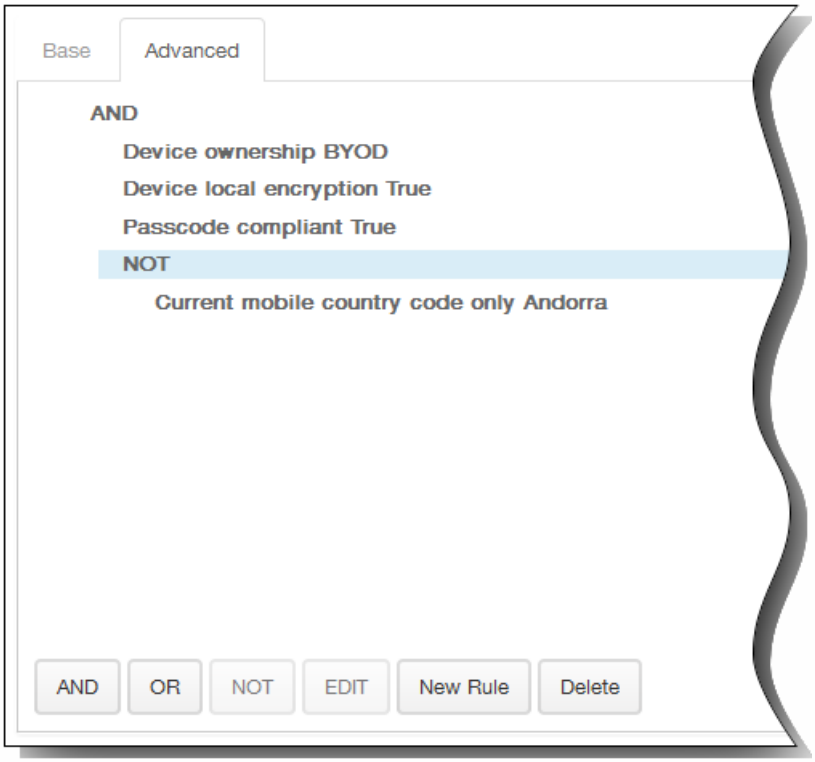
1. Klicken Sie in der Liste auf Optionen, um festzulegen, wann die App bereitgestellt werden soll.
    1. Sie können die App bereitstellen, wenn alle Bedingungen oder wenn spezifische Bedingungen erfüllt sind. Die Standardeinstellung ist Alle.
    2. Klicken Sie auf Neue Regel, um Bedingungen zu definieren.
    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.
2. Klicken Sie auf die Registerkarte Erweitert, um die Regeln mit booleschen Optionen zu kombinieren.



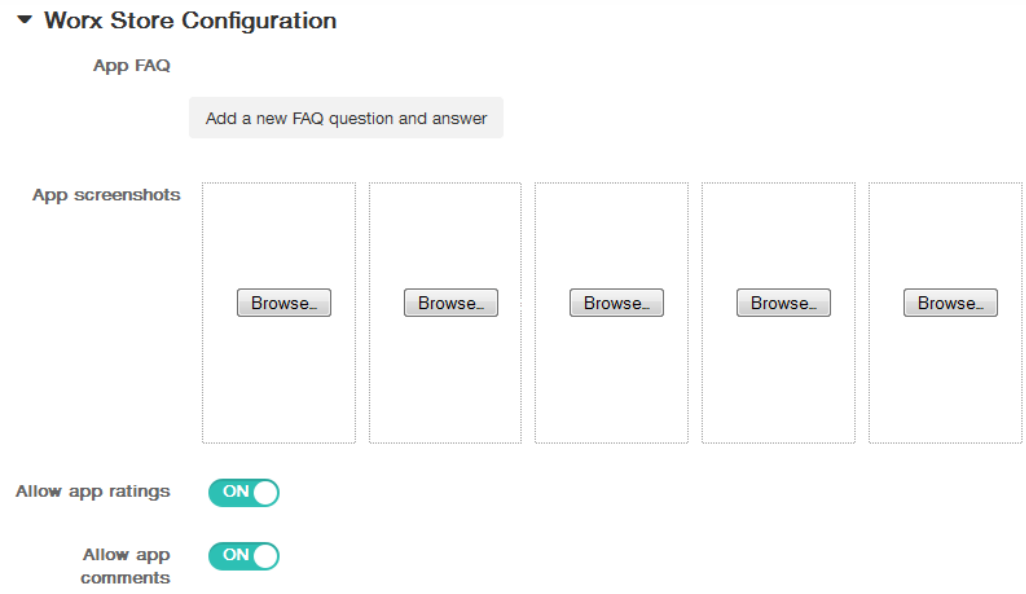
Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
    1. Klicken Sie auf 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 EDIT klicken, um die Bedingung zu ändern, oder auf Delete, um die Bedingung zu löschen.

    3. Klicken Sie erneut auf Neue Regel, 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.

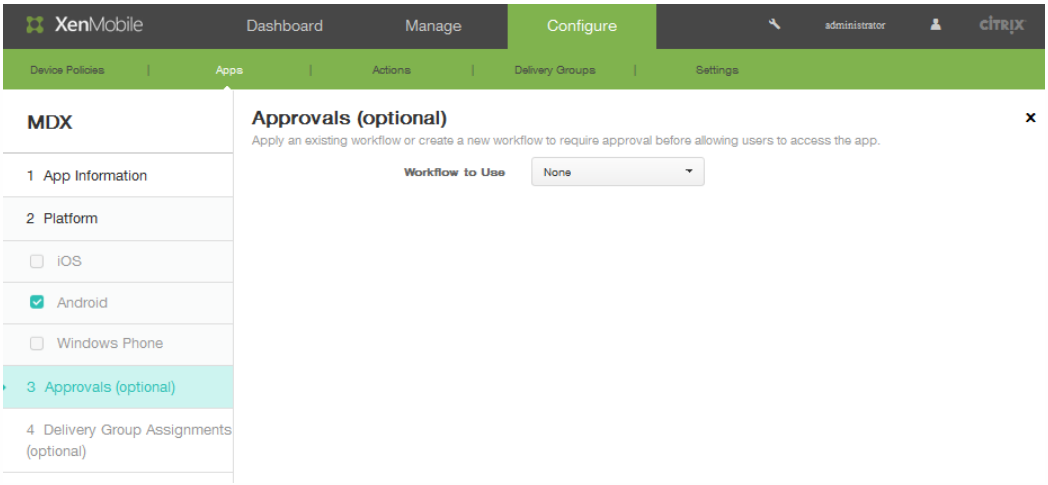


11. Erweitern Sie Worx Store Configuration, um FAQ für die App oder Bildschirmaufnahmen zur Klassifizierung des App im Worx Store hinzuzufügen. Die hochgeladene Grafik muss im PNG-Format sein. Sie können keine GIF- oder JPEG-Bilder hochladen.

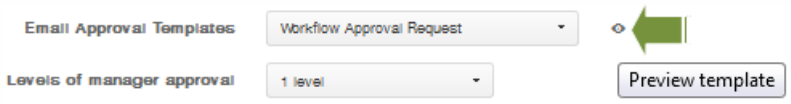


Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.

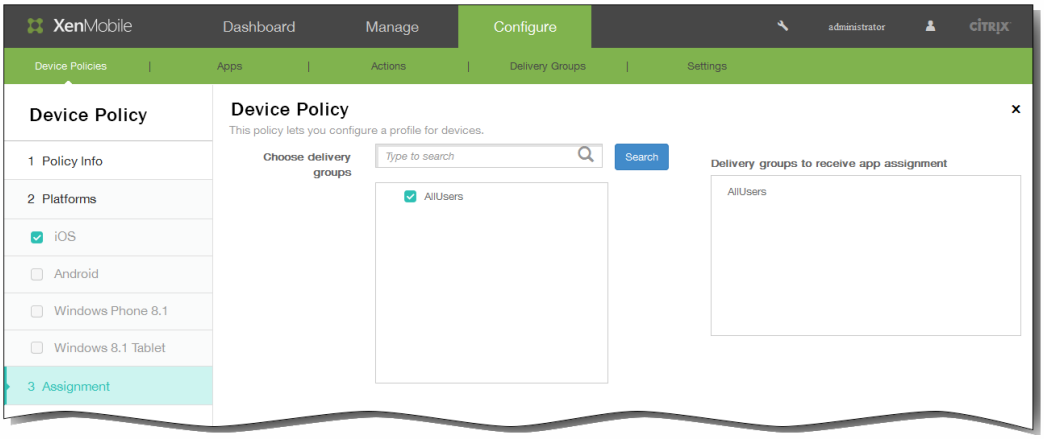
12. Klicken Sie unter Allow app comments auf ON, um eine Kommentierung der App durch die Benutzer zuzulassen.
13. Klicken Sie auf Next. Die Seite Approvals wird angezeigt.



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.

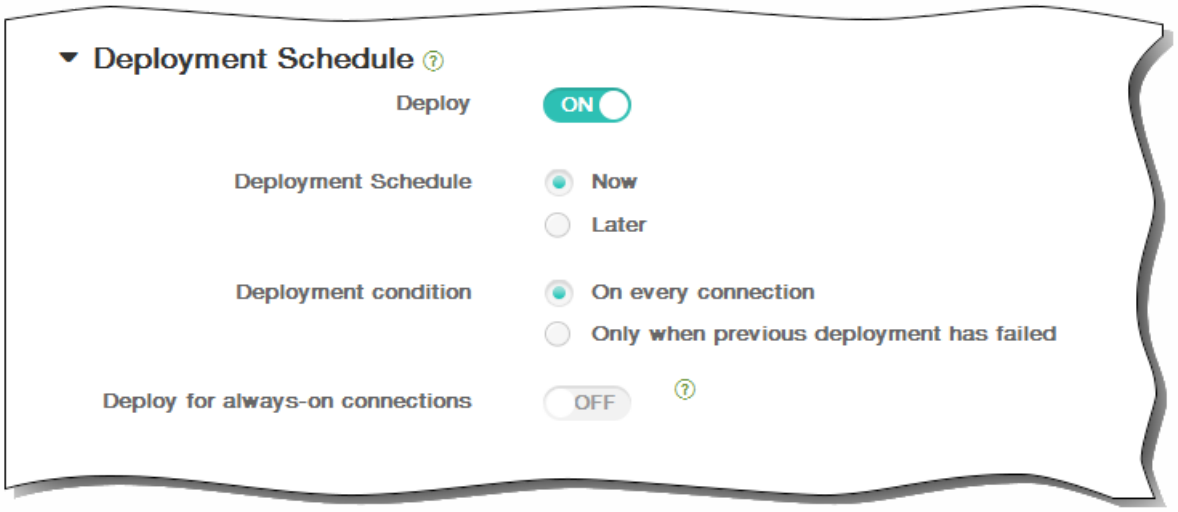


    4. Klicken Sie unter **Levels of manager approval** auf eine Stufe zwischen None und 3. .
    5. Klicken Sie unter **Select Active Directory domain** auf die Domäne.
    6. Geben Sie unter Find additional required approvers optional weitere Freigabeberechtigte ein und klicken Sie auf Search.
15. Klicken 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 Bereitstellungsgruppen für App-Zuweisung angezeigt.



17. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
    1. Klicken Sie neben Bereitstellen auf EIN, um die Bereitstellung zu planen, oder auf AUS, um die Bereitstellung zu verhindern. Die Standardeinstellung ist EIN. Wenn Sie AUS auswählen, müssen keine anderen Optionen konfiguriert werden.
    2. Klicken Sie neben Bereitstellungszeitplan auf Jetzt oder Später. Die Standardeinstellung ist Jetzt.
    3. Wenn Sie auf Später klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
    4. Klicken Sie neben Bereitstellungsbedingung auf Bei jeder Verbindung oder auf Nur bei Fehler in der vorherigen Bereitstellung. Die Standardeinstellung ist Bei jeder Verbindung.
    5. Klicken Sie neben Bereitstellen für immer aktive Verbindungen auf EIN oder AUS. Die Standardeinstellung ist AUS. Hinweis: Diese Option gilt, wenn Sie unter Settings > Server Properties den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" 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 Speichern. In der XenMobile-Konsole werden die App-Informationen angewendet.

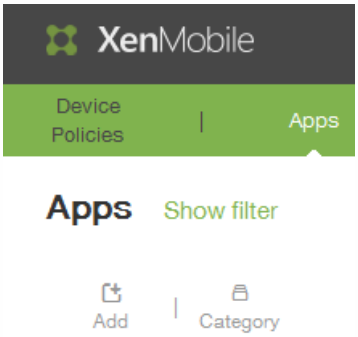
May 05, 2016

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.

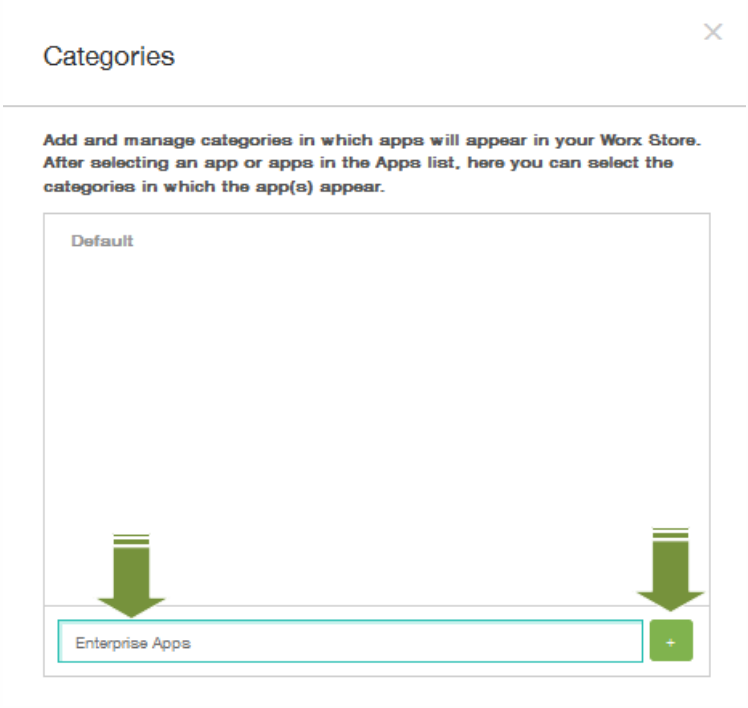
Kategorien werden in XenMobile auf der Seite Apps konfiguriert. Wenn Sie eine App, einen Weblink oder einen Store konfiguriert bzw. bearbeitet haben, können Sie diese(n) einer Kategorie zuweisen.

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.

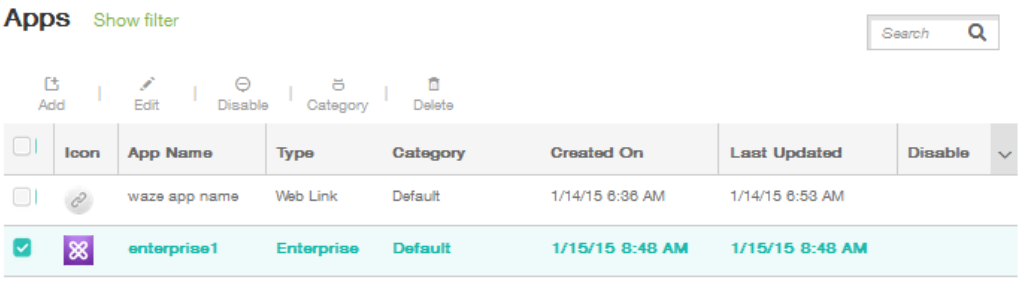


3. Geben Sie im Dialogfeld Categories den Namen der Kategorie ein, die Sie hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) . Geben Sie beispielsweise *Enterprise Apps* ein und klicken Sie auf das Pluszeichen (+).

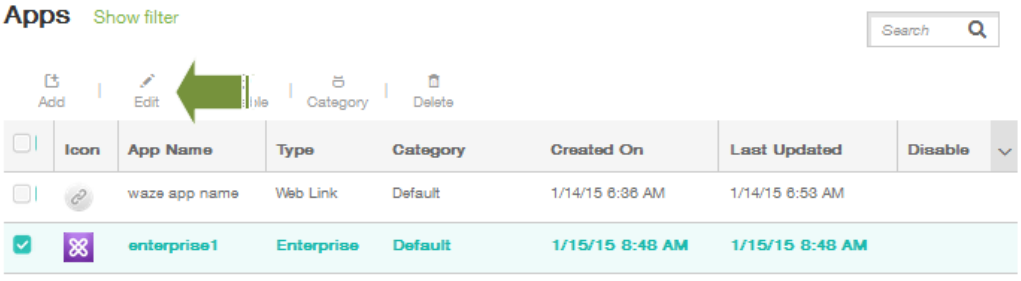


Die neu erstellte Kategorie wird hinzugefügt und wird im gleichen Dialogfeld Categories angezeigt. Wenn keine Kategorien konfiguriert sind, wird nur die Kategorie **Default** angezeigt.

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.

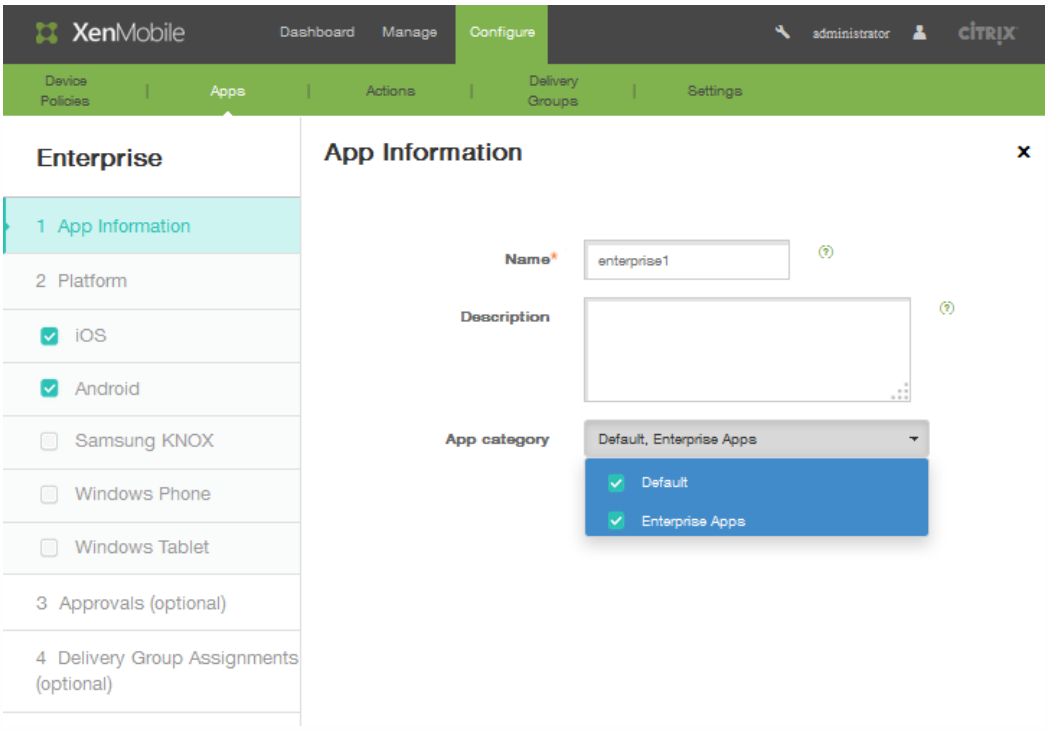


6. Klicken Sie auf Edit, um die App zu kategorisieren.

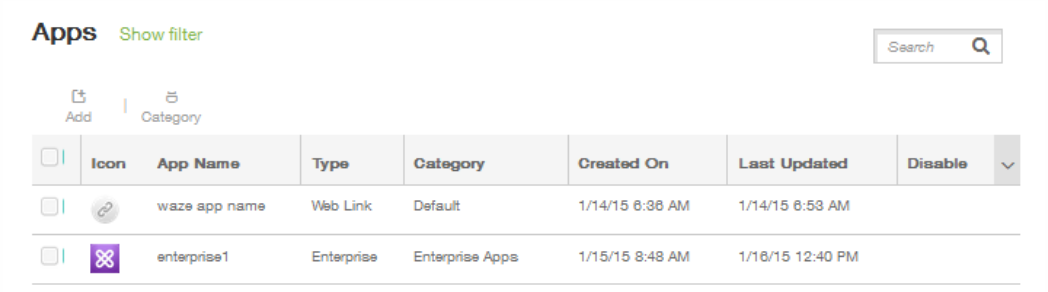


Die Seite App Information wird angezeigt.

7. Wenden Sie die gewünschte Kategorie an, indem Sie das zugehörige Kontrollkästchen in der Liste App category aktivieren.



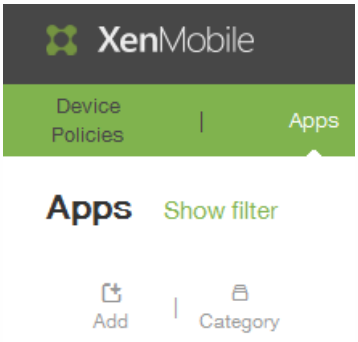
8. Klicken Sie jeweils auf Next, um die weiteren Seiten der App-Konfiguration auszufüllen.
9. Klicken Sie auf der letzten Seite auf Save, um die Kategorie anzuwenden. Die neu erstellte Kategorie wird auf die App angewendet und in der App-Tabelle angezeigt.



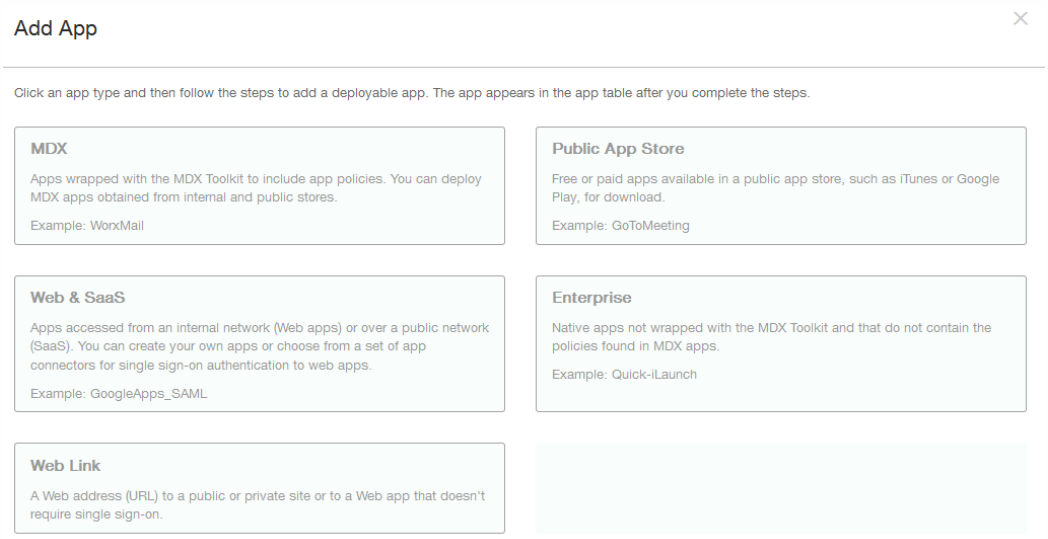
May 05, 2016

Sie können XenMobile kostenlose oder kostenpflichtige Apps, die in einem öffentlichen App Store (z. B. iTunes oder Google Play) verfügbar sind, hinzufügen. Beispiel: GoToMeeting.

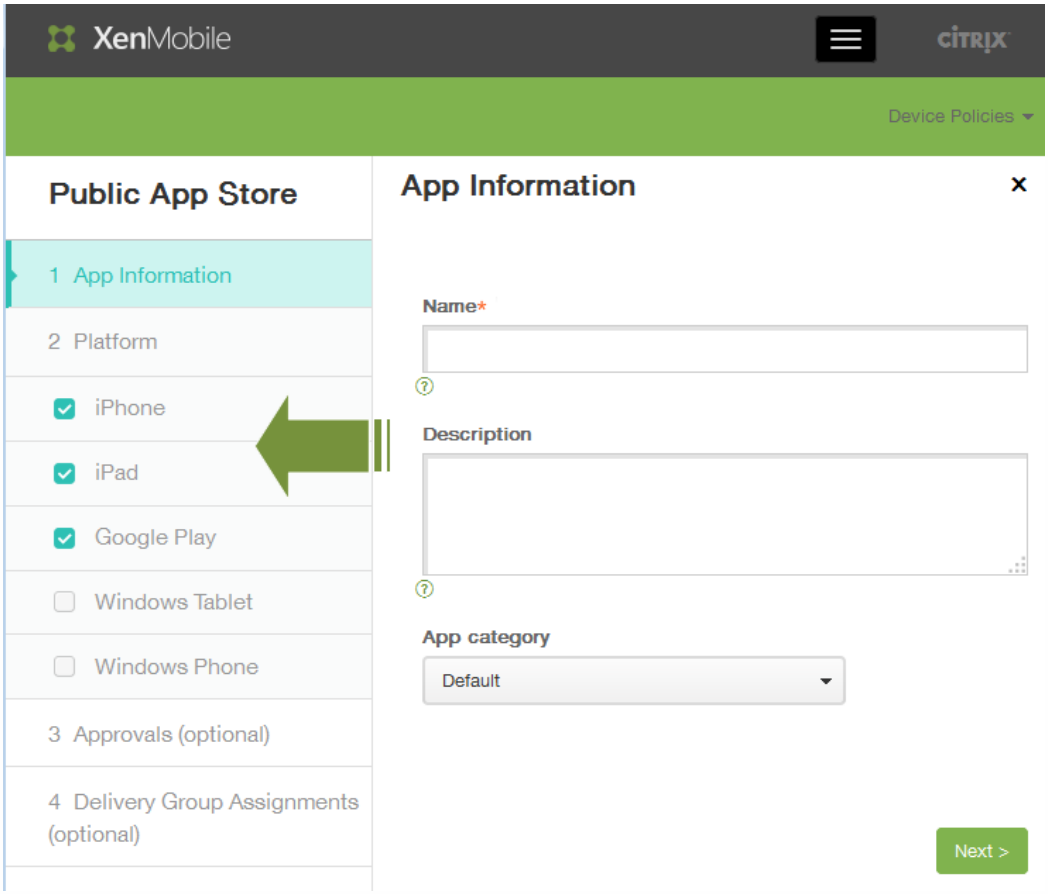
1. Klicken Sie in der XenMobile-Konsole auf Configure > Apps. Die Seite Apps wird angezeigt.



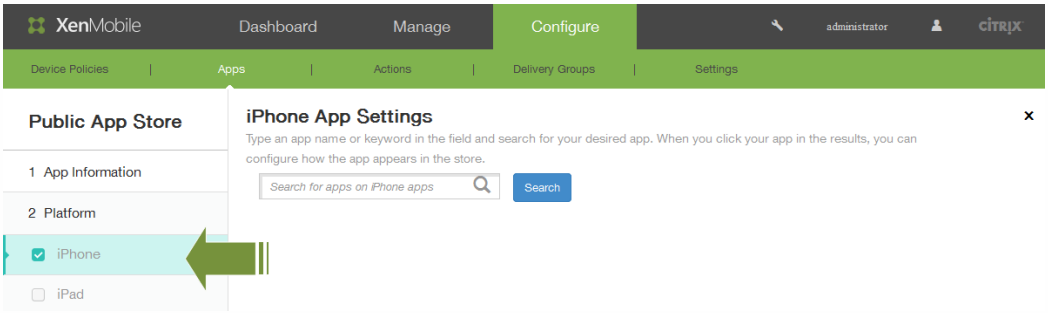
2. Klicken Sie auf Add.
3. Klicken Sie auf der Seite Add App auf Public App Store.



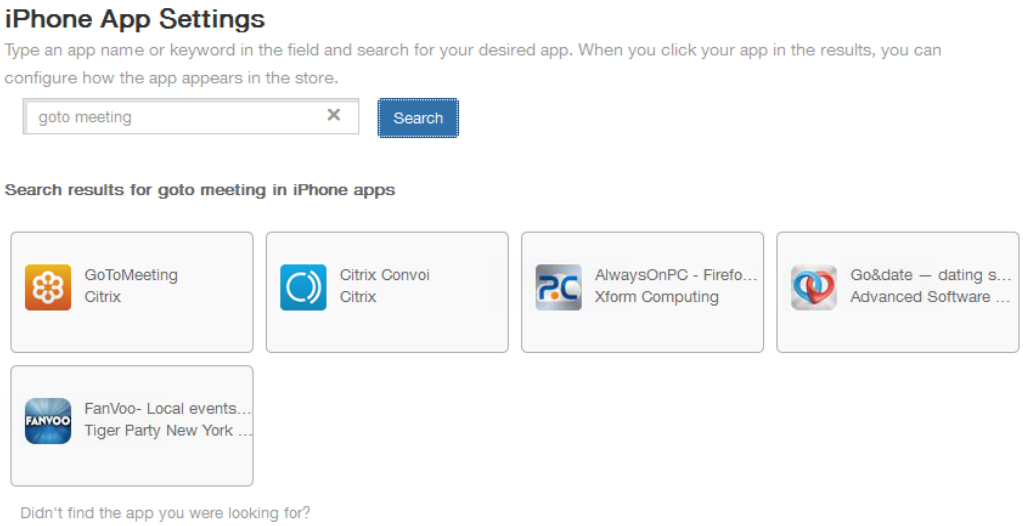
4. Geben Sie auf der Seite App Information unter Name einen Namen und unter Description eine Beschreibung für die App ein. Diese Felder werden für interne Zwecke verwendet. Wenn Sie Apps für mehrere Geräte (z. B. iPhone, iPad und Google Play) hinzufügen, verwenden Sie die Kontrollkästchen im linken Bereich des Bildschirms, um diese auszuwählen.



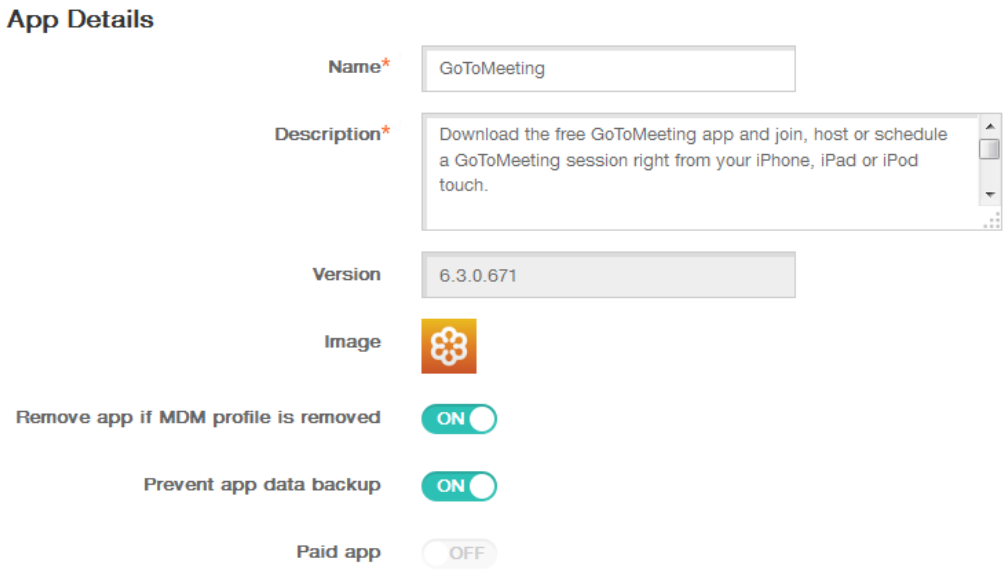
5. Klicken Sie in der Liste App category auf die App-Kategorie.
6. Klicken Sie auf Next.
7. Geben Sie auf der Seite Platform im Suchfeld für den Plattformtyp einen App-Namen oder ein Schlüsselwort ein, um die App zu suchen, die Sie hinzufügen möchten. Wenn Sie beispielsweise eine iPhone-App zum Hinzufügen 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).

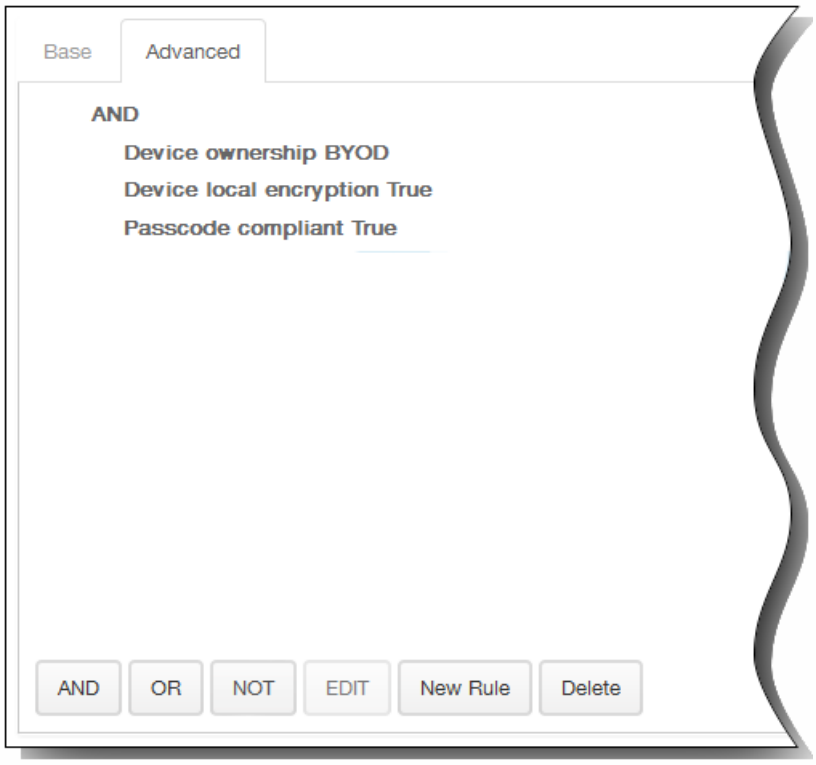


8. Klicken Sie auf eine App im Ergebnis, um vorzugeben, wie diese im Store angezeigt werden soll. Die Felder auf der Seite App Details enthalten bereits Informationen über die gewählte App (einschließlich Namen, Beschreibung, Versionsnummer und zugewiesenes Bild). Falls erforderlich, ändern Sie Namen und Beschreibung der App.



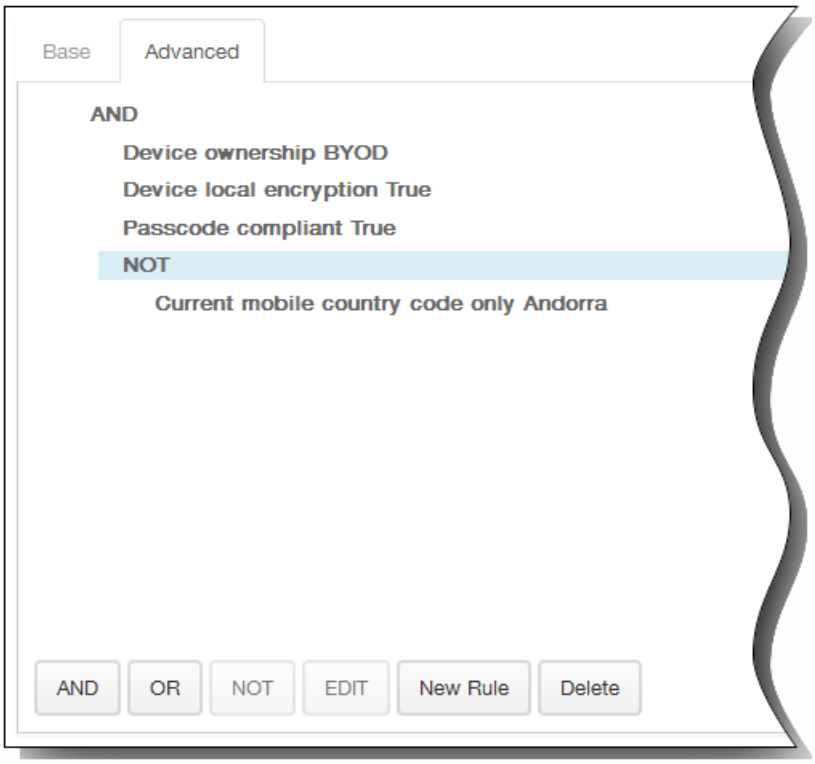
   1. Klicken Sie unter Remove app if MDM profile is removed auf ON, wenn die App bei Entfernen des MDM-Profils auch entfernt werden soll. Standardmäßig ist diese Option auf ON festgelegt.
   2. Klicken Sie unter "Prevent app data backup" auf ON, wenn Sie verhindern möchten, dass durch die App Daten gesichert 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 noch einmal 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.

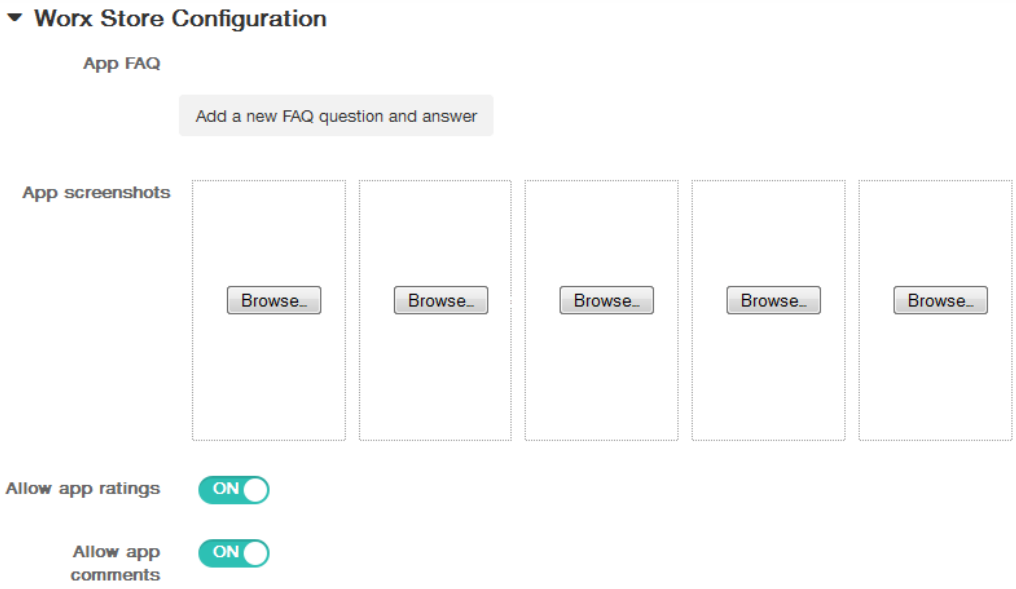


   Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, 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 noch einmal 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.

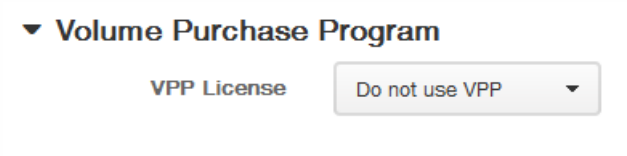


10. Erweitern Sie Worx Store Configuration, um FAQ für die App oder Bildschirmaufnahmen zur Klassifizierung des App im Worx Store hinzuzufügen. Die hochgeladene Grafik muss im PNG-Format sein. Sie können keine GIF- oder JPEG-Bilder hochladen.

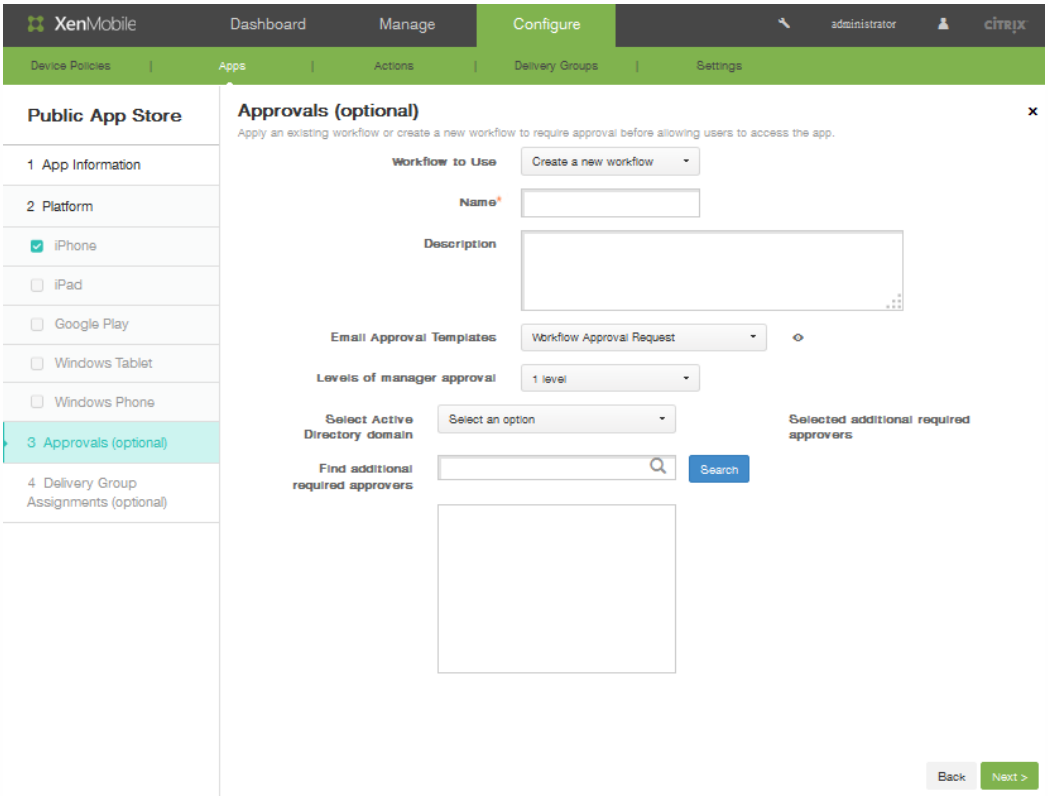


   Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.
11. Klicken Sie unter Allow app comments auf ON, um eine Kommentierung der App durch die Benutzer zuzulassen.
12. Erweitern Sie Volume Purchase Program und klicken Sie in der Liste VPP license auf Upload a VPP license file, wenn

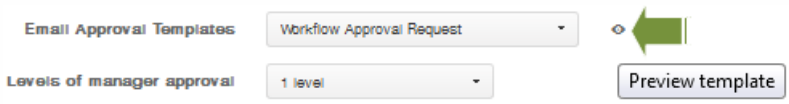
XenMobile der App eine VPP-Lizenz zuweisen können soll.



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.

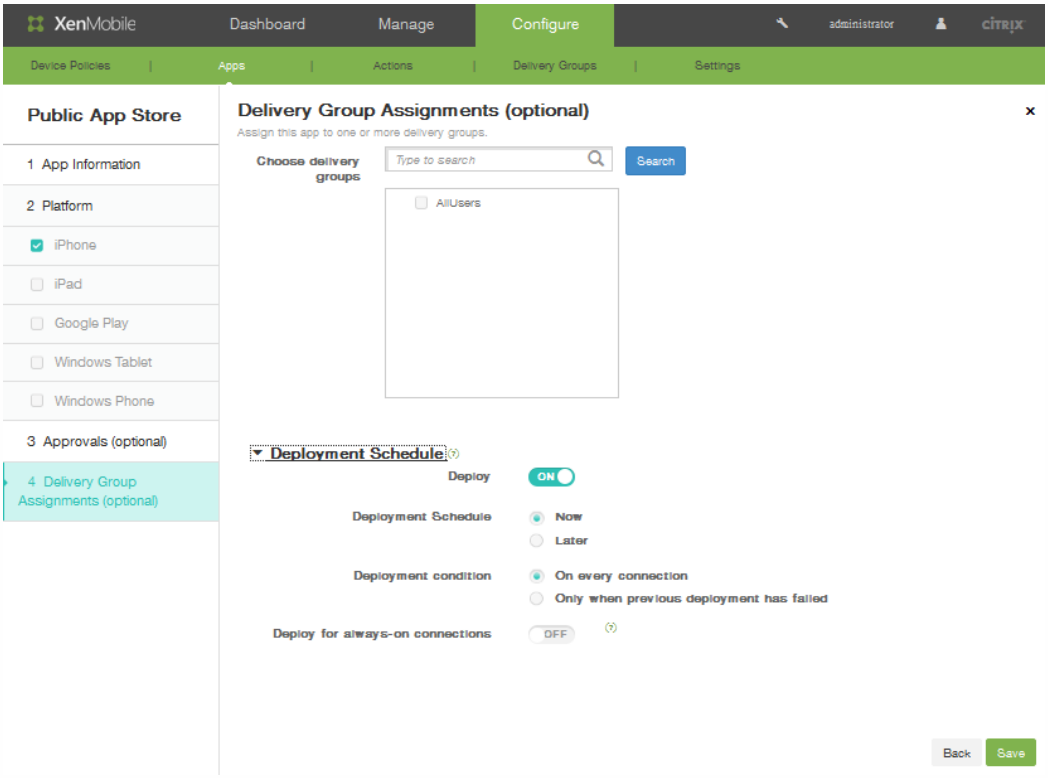


15. Wenn Sie einen neuen Workflow erstellen, werden in der XenMobile-Konsole nun Konfigurationsoptionen für den Freigabeprozess angezeigt. Die betreffenden Felder werden in den nachfolgenden Schritten erläutert. Konfigurieren Sie diese Felder, wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist. Die hochgeladene VPP-Datei gilt nur für das alte Programm für Volumenlizenzen von Apple. Bei dem neuen Programm werden Lizenzen automatisch basierend auf den vom Unternehmen erworbenen Lizenzen behandelt. Diese Informationen werden unter **Settings > iOS VPP** konfiguriert.
    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 Speichern. In der XenMobile-Konsole werden die App-Informationen angewendet.

May 05, 2016

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.

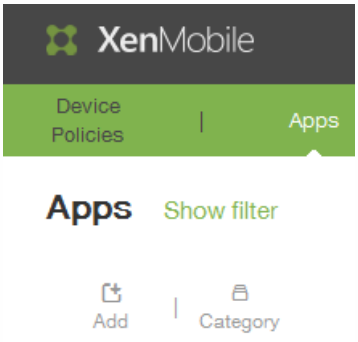
Bei der Konfiguration eines Connectors werden folgende Parameter angegeben:

- 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.

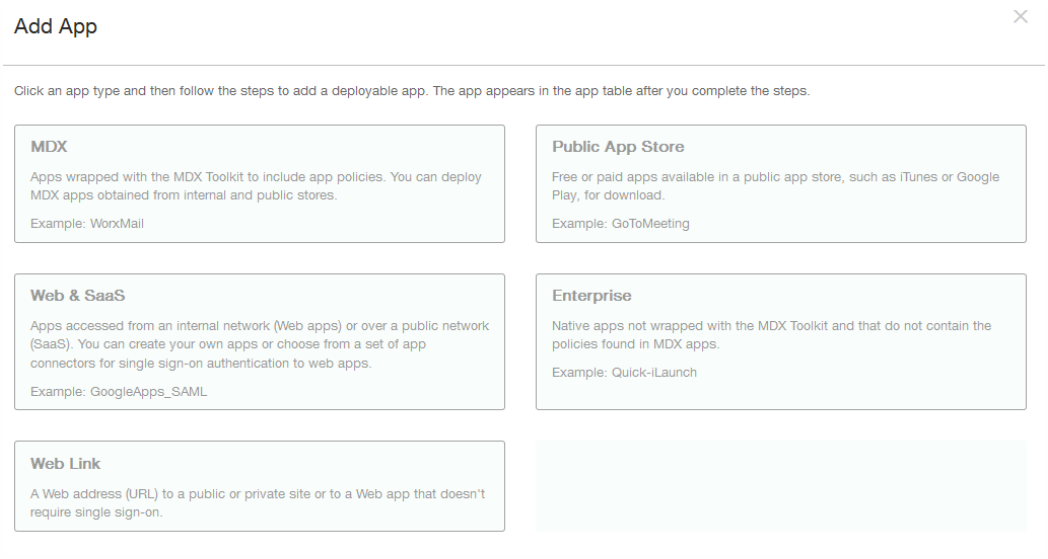
Wenn eine App nur für SSO verfügbar ist, speichern Sie nach der oben beschriebenen Konfiguration die Einstellungen. Die App wird dann auf der Registerkarte Apps in der XenMobile-Konsole angezeigt.

So fügen Sie einen App-Connector in XenMobile hinzu

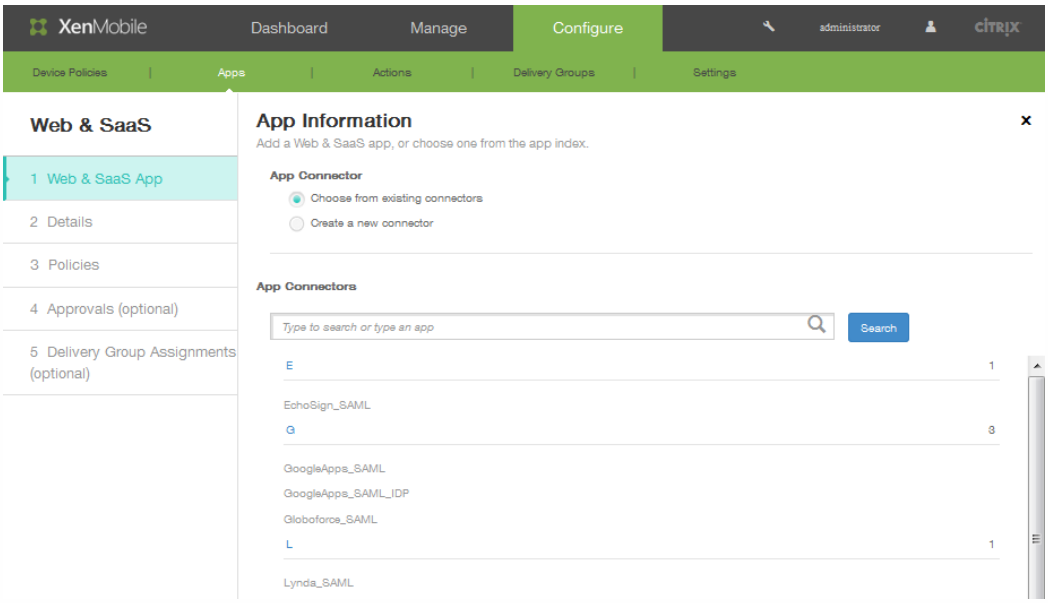
1. Klicken Sie in der XenMobile-Konsole auf Configure > Apps. Die Seite Apps wird geöffnet.
2. Klicken Sie auf der Seite Apps auf **Add**.



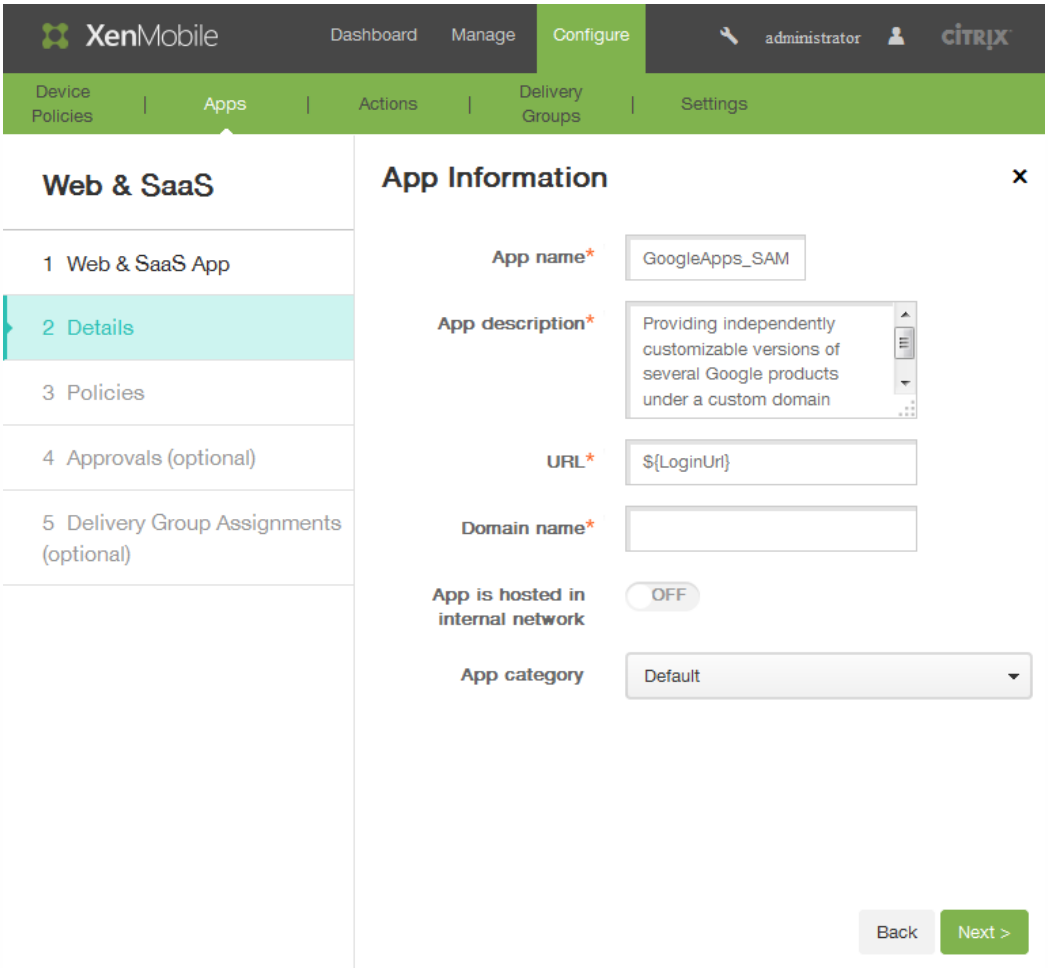
3. Klicken Sie auf der Seite **Add App** auf **Web & SaaS**.



4. Klicken Sie auf der Seite App Information auf Choose from existing connector oder Create a new connector.

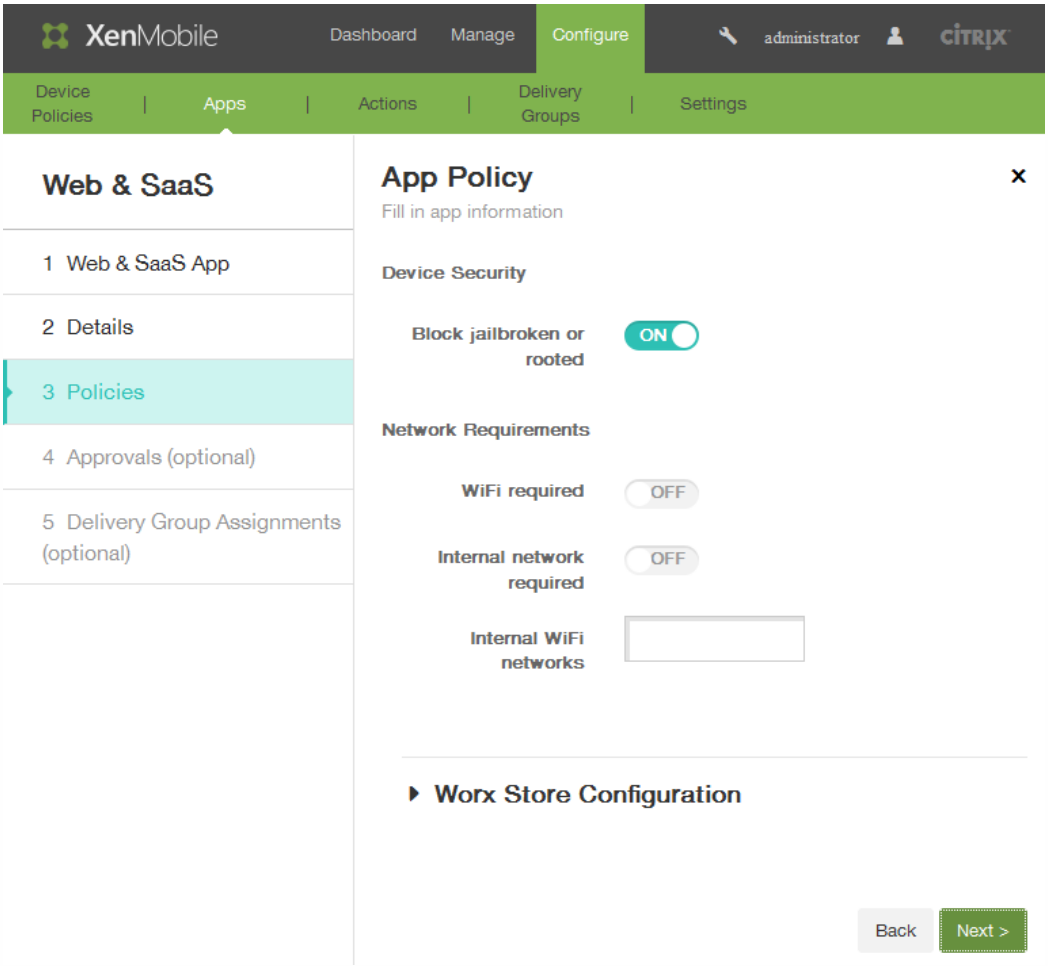


5. Wenn Sie auf eine App in der Liste klicken, wird die Seite Details geöffnet. Die Felder App name, Description und URL sind bereits ausgefüllt.

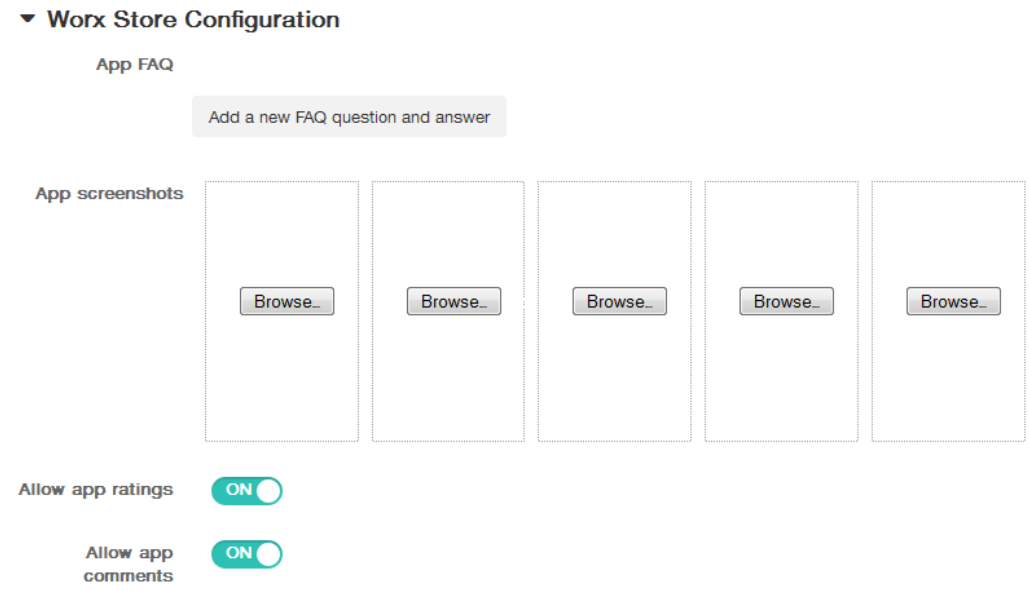


1. Geben Sie unter URL ggf. die Webadresse der App ein oder behalten Sie die Standardadresse bei.
2. Klicken Sie unter App is hosted in internal network auf ON, wenn die App auf einem Server im internen Netzwerk ausgeführt wird. Wenn Benutzer von einem Remotestandort aus eine Verbindung mit der internen 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.

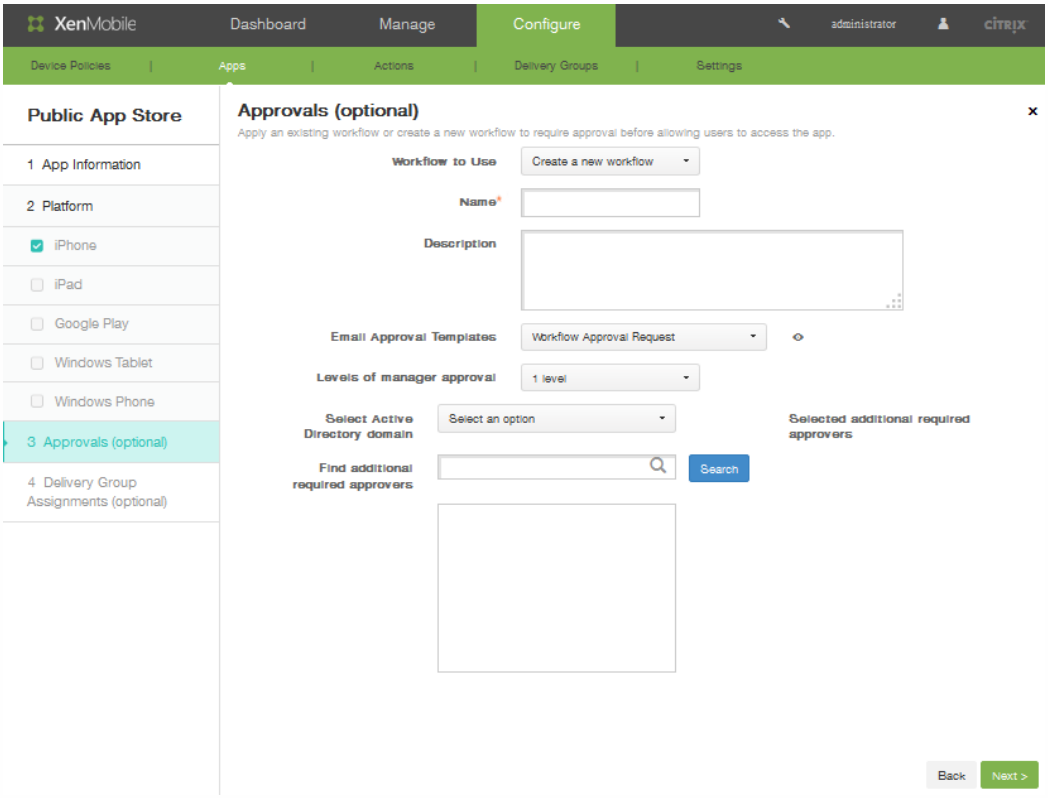


7. Klicken Sie unter Device Security für Block jailbroken or rooted auf ON.
8. Konfigurieren Sie unter Network Requirements die folgenden Einstellungen:
   1. Klicken Sie für WiFi required auf ON und geben Sie interne WiFi-Netzwerke an.
   2. Klicken Sie für Internal network required auf ON, wenn ein 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.



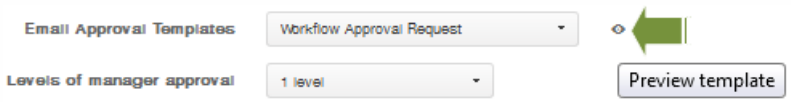
Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.

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.



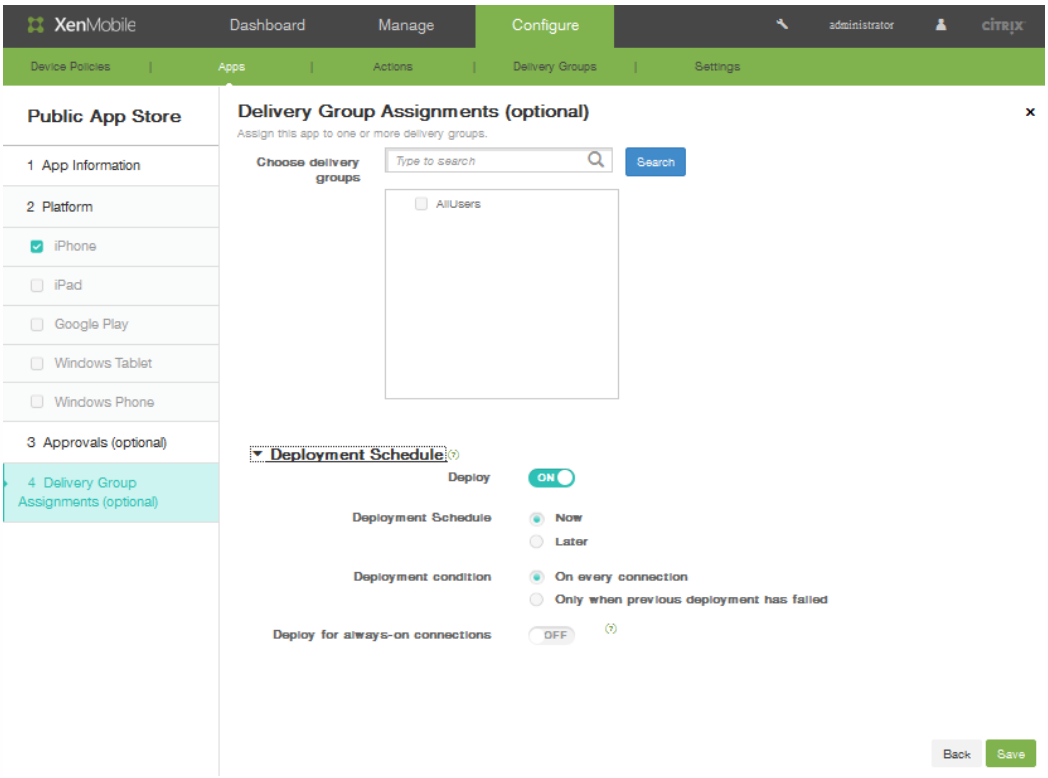
13. Wenn Sie einen neuen Workflow erstellen, werden in der XenMobile-Konsole nun Konfigurationsoptionen für den Freigabeprozess angezeigt. Die betreffenden Felder werden in den nachfolgenden Schritten erläutert. Konfigurieren Sie diese Felder, wenn für das Erstellen von Benutzerkonten eine Genehmigung 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.

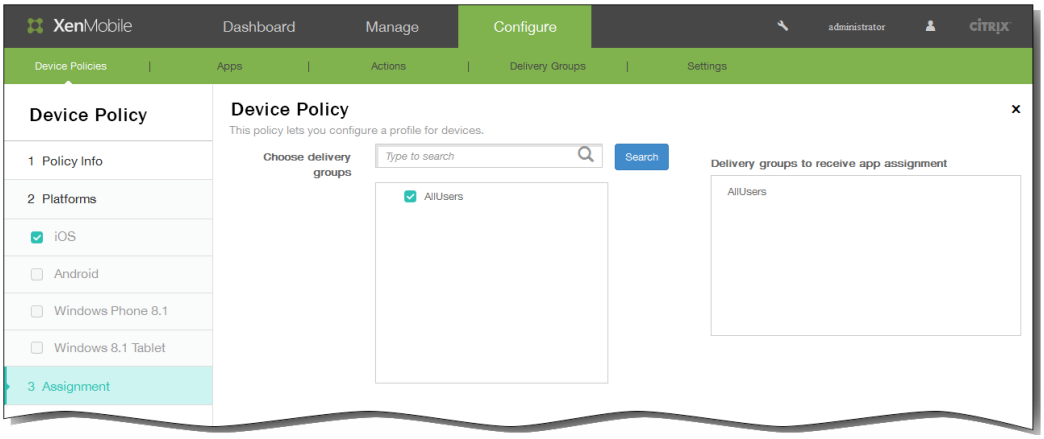


4. Klicken Sie unter **Levels of manager approval** auf eine Stufe zwischen None und 3.
5. Klicken Sie unter **Select Active Directory domain** auf die Domäne.
6. Geben Sie unter Find additional required approvers optional weitere Freigabeberechtigte ein und klicken Sie auf Search.

14. Klicken Sie auf Next.
15. Weisen Sie die App auf der Seite **Delivery Groups Assignment** optional einer oder mehreren Bereitstellungsgruppen zu.

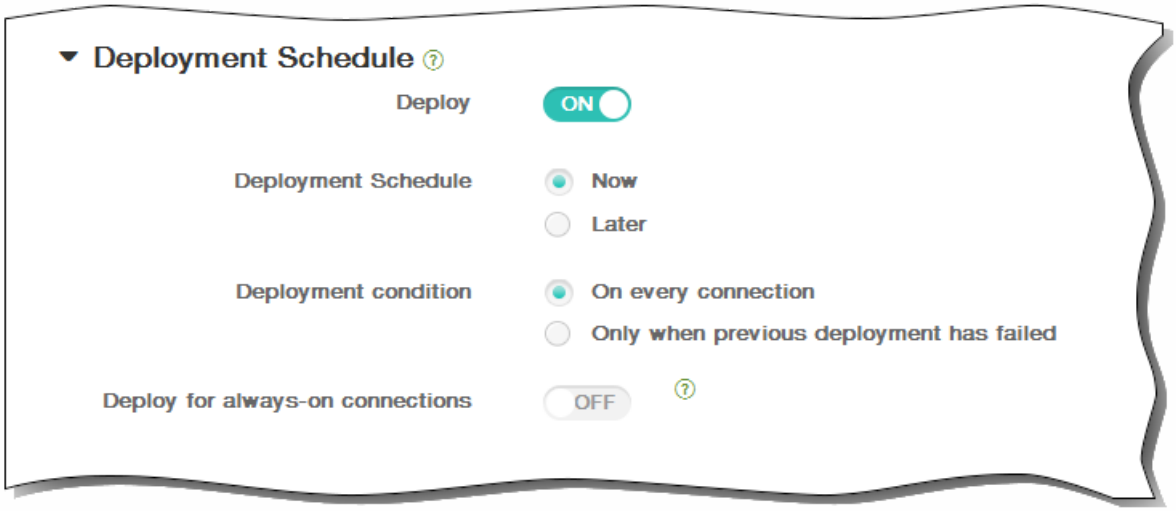


16. Machen Sie neben Choose delivery groups eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden rechts in der Liste Delivery groups to receive app assignment angezeigt.



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 **Speichern**.

May 05, 2016

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

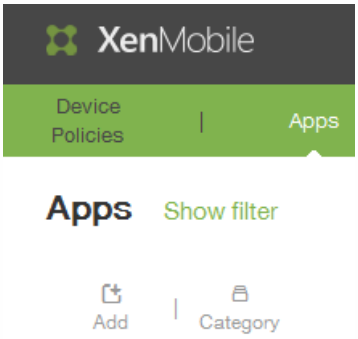
May 05, 2016

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):

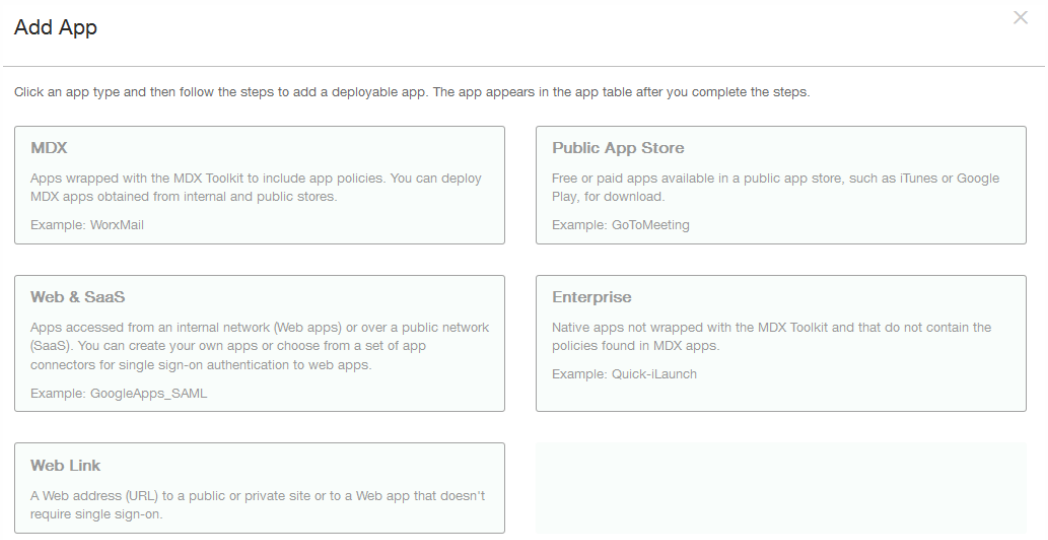
- iOS (.ipa)
- Android (.apk)
- Samsung KNOX (.apk)
- Windows Phone (.xap oder .appx)
- Windows Tablet (.appx)

So erstellen Sie eine Unternehmensapp

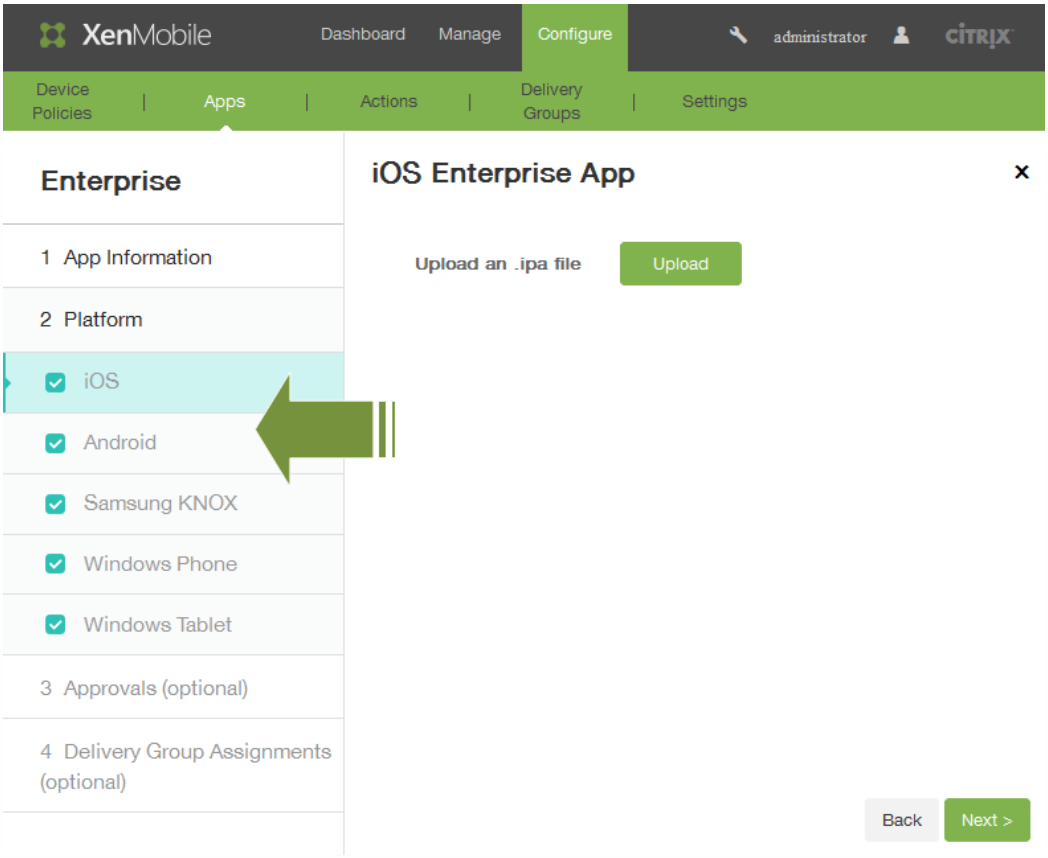
1. Klicken Sie in der XenMobile-Konsole auf Configure > Apps.
2. Klicken Sie auf der Seite "Apps" auf **Add**.



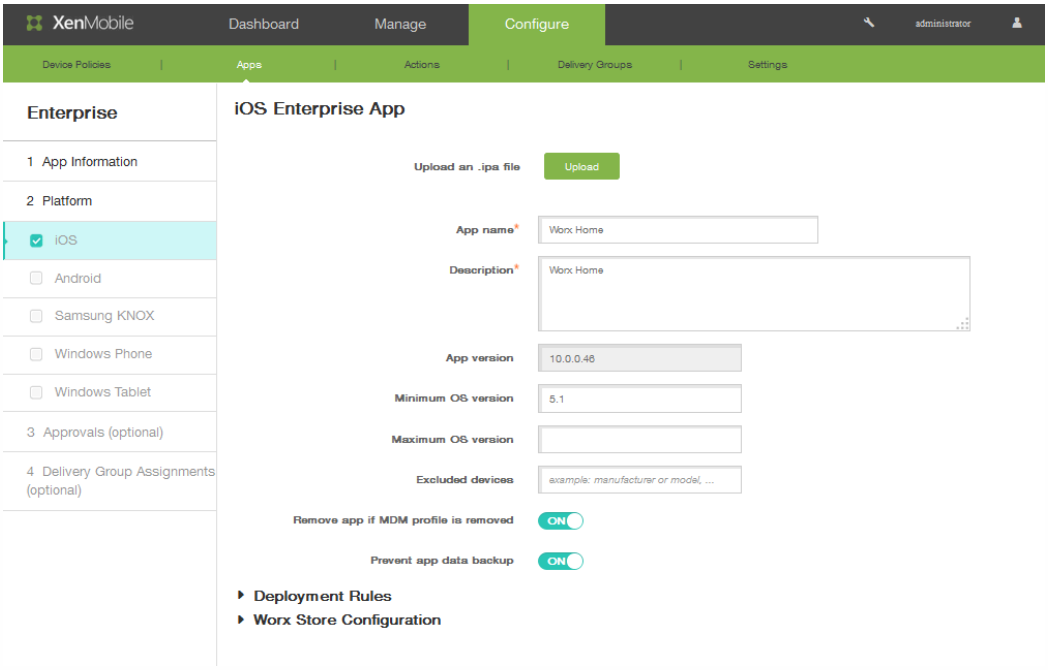
3. Klicken Sie auf der Seite Add App auf **Enterprise**.



4. Klicken Sie im Katalog auf New enterprise app.
5. 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.
      Hinweis: Wenn Sie eine zweite App mit derselben Webadresse konfigurieren möchten, müssen Sie dieser App einen anderen Namen geben.
   3. Klicken Sie unter **App category** auf eine Kategorie und dann auf Next.
6. Wählen Sie im Bereich Platform links die Geräteplattformen aus, für die Sie die App hinzufügen möchten (z. B. iOS oder Android).

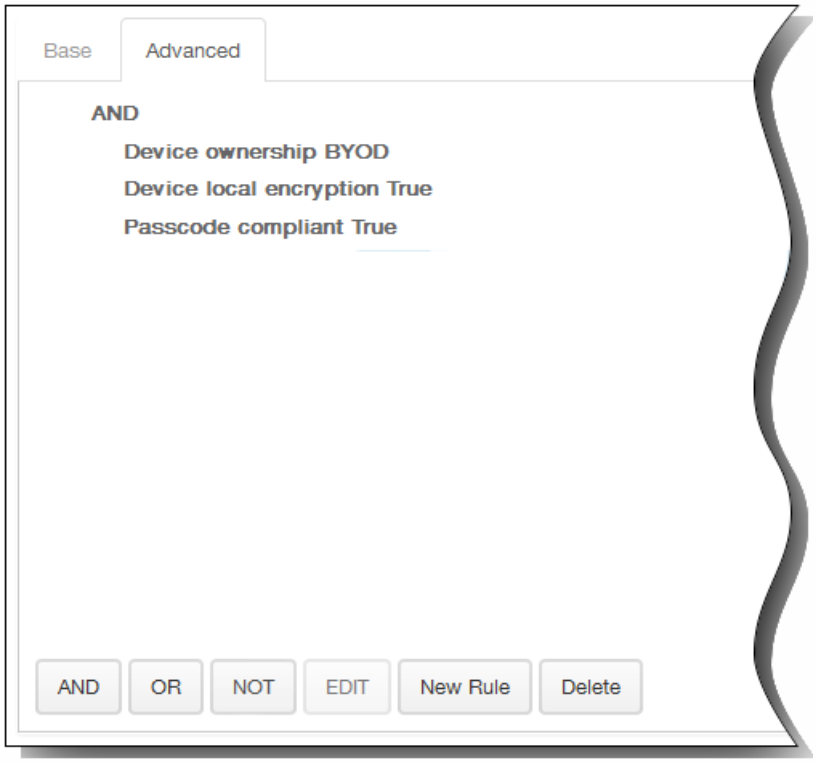


7. Klicken Sie auf Upload, navigieren Sie zum Speicherort der Datei und klicken Sie dann auf Next. Die Seite mit den App-Informationen für den Plattformtyp wird angezeigt. Die Felder enthalten bereits Informationen zu der gewählten App (einschließlich Name, Beschreibung, Versionsnummer und zugeordnetes Bild). Falls erforderlich, ändern Sie Namen und Beschreibung der App.



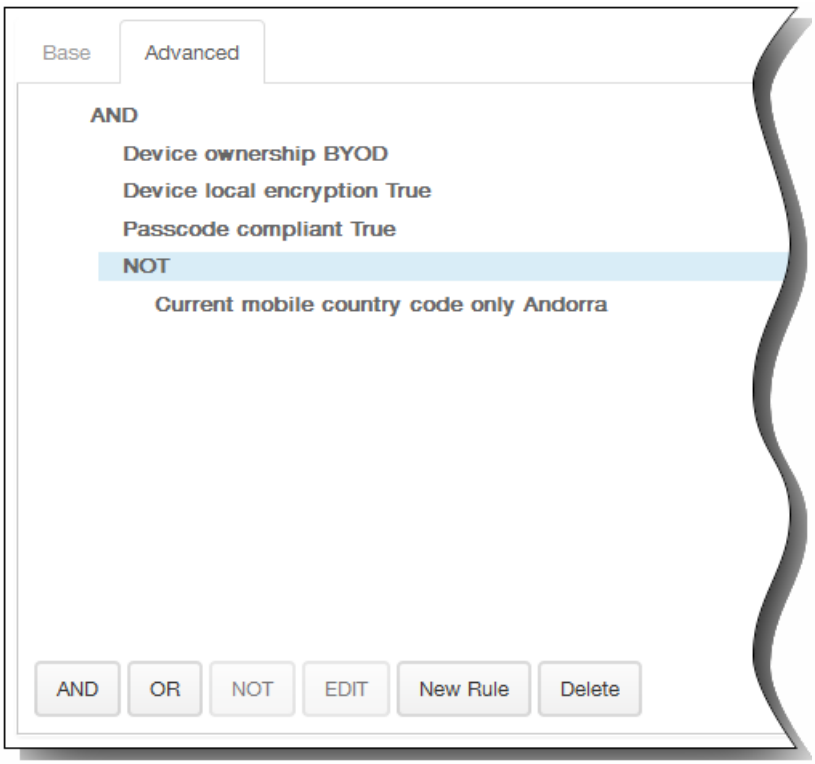
8. Klicken Sie unter Remove app if MDM profile is removed auf ON, wenn die App bei Entfernen des MDM-Profils auch entfernt werden soll. Standardmäßig ist diese Option auf ON festgelegt.
9. Klicken Sie unter Prevent app data backup auf ON, wenn Sie verhindern möchten, dass durch die App Daten gesichert werden. Standardmäßig ist diese Option auf ON festgelegt.
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 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.

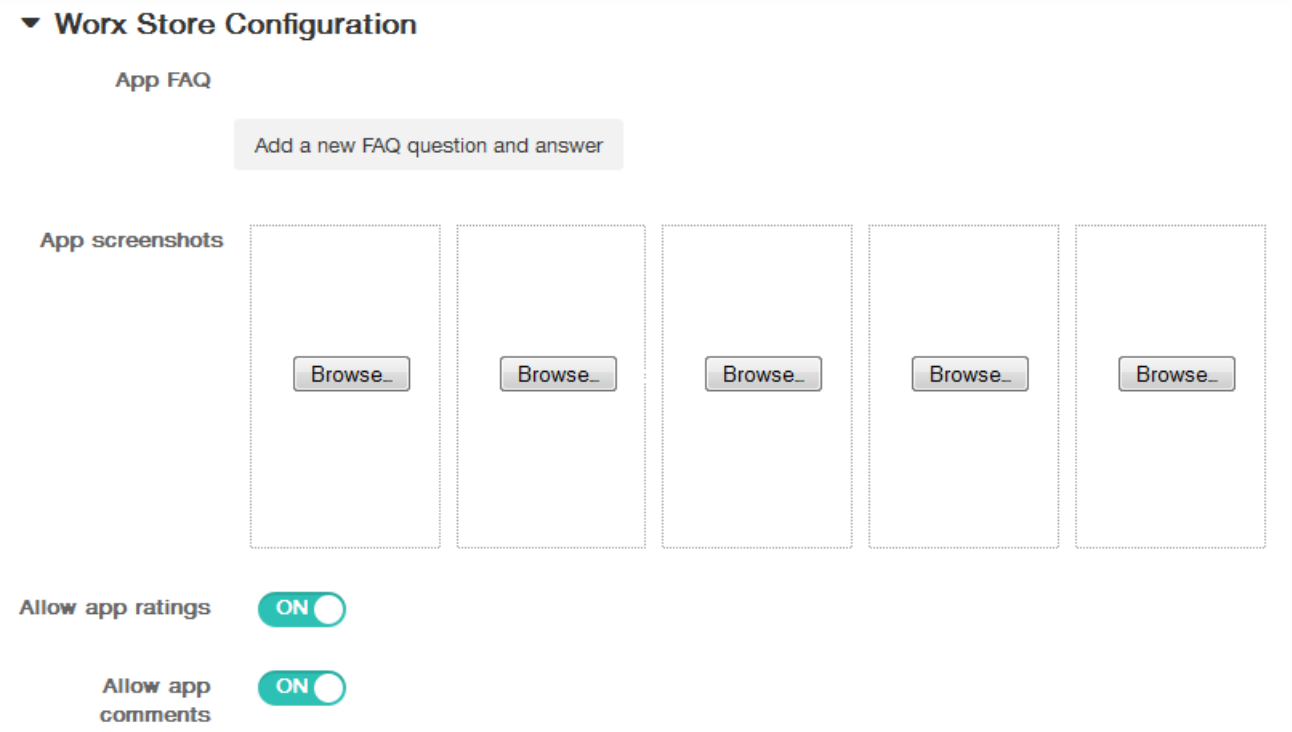


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.



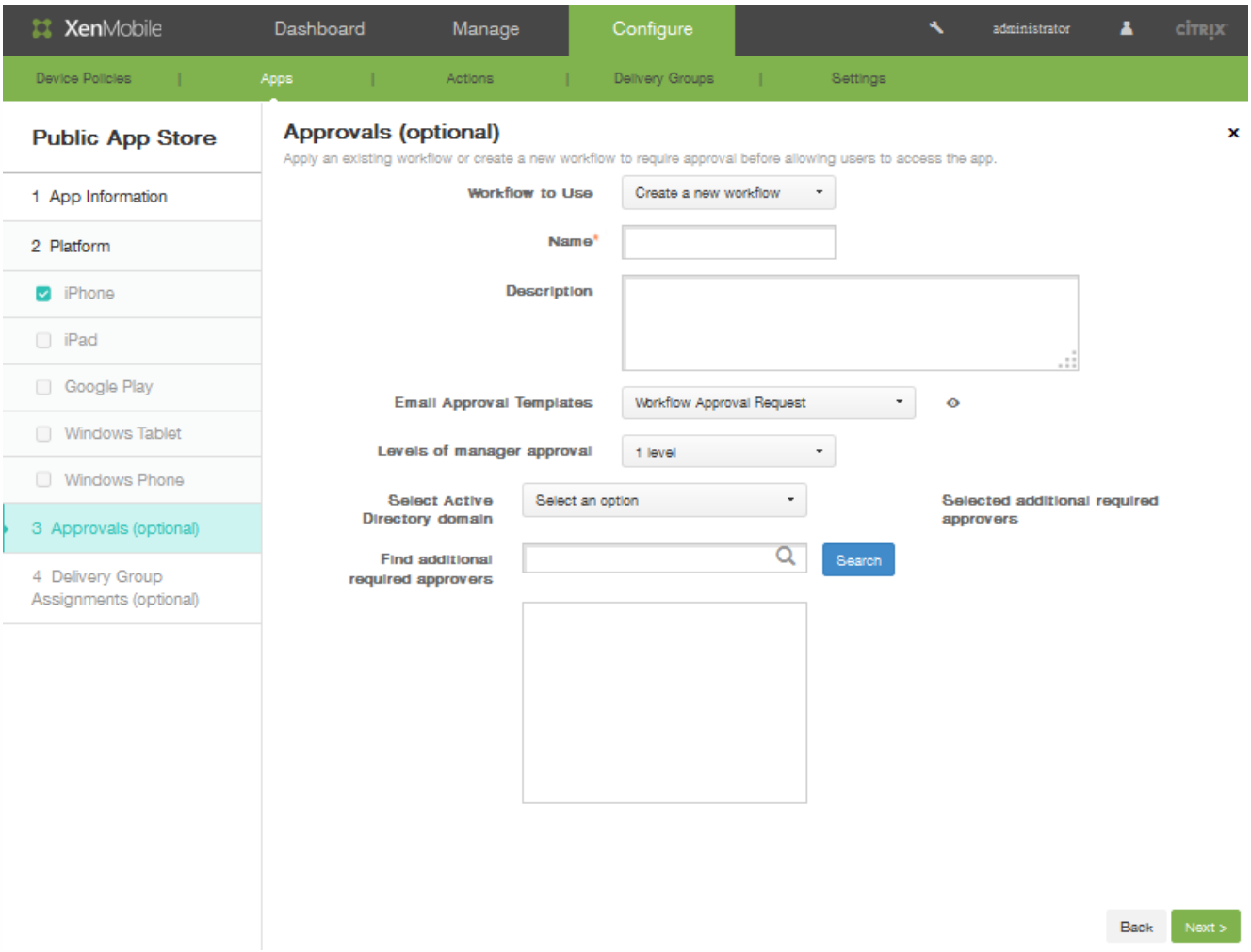
11. Erweitern Sie Worx Store Configuration, um FAQ für die App oder Bildschirmaufnahmen zur Klassifizierung des App im Worx Store hinzuzufügen. Die hochgeladene Grafik muss im PNG-Format sein. Sie können keine GIF- oder JPEG-Bilder hochladen.



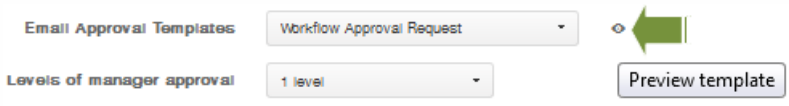
Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.

12. Klicken Sie unter Allow app comments auf ON, um eine Kommentierung der App durch die Benutzer zuzulassen.
13. Klicken Sie auf Next.

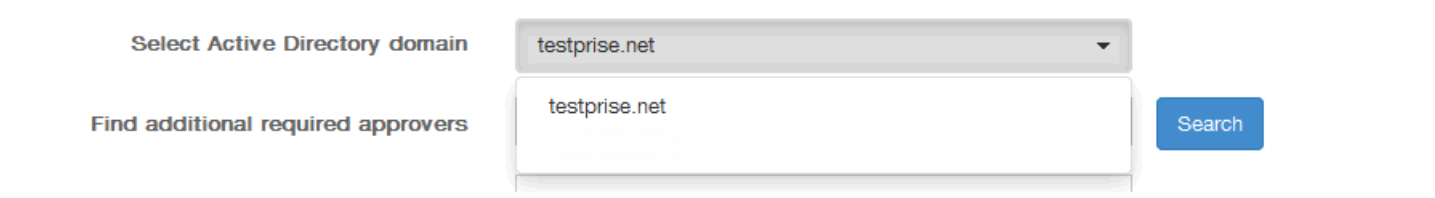
14. Klicken Sie auf der Seite Approvals in der Liste Workflow to use optional auf einen Workflow oder auf Create a new workflow.



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. 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.

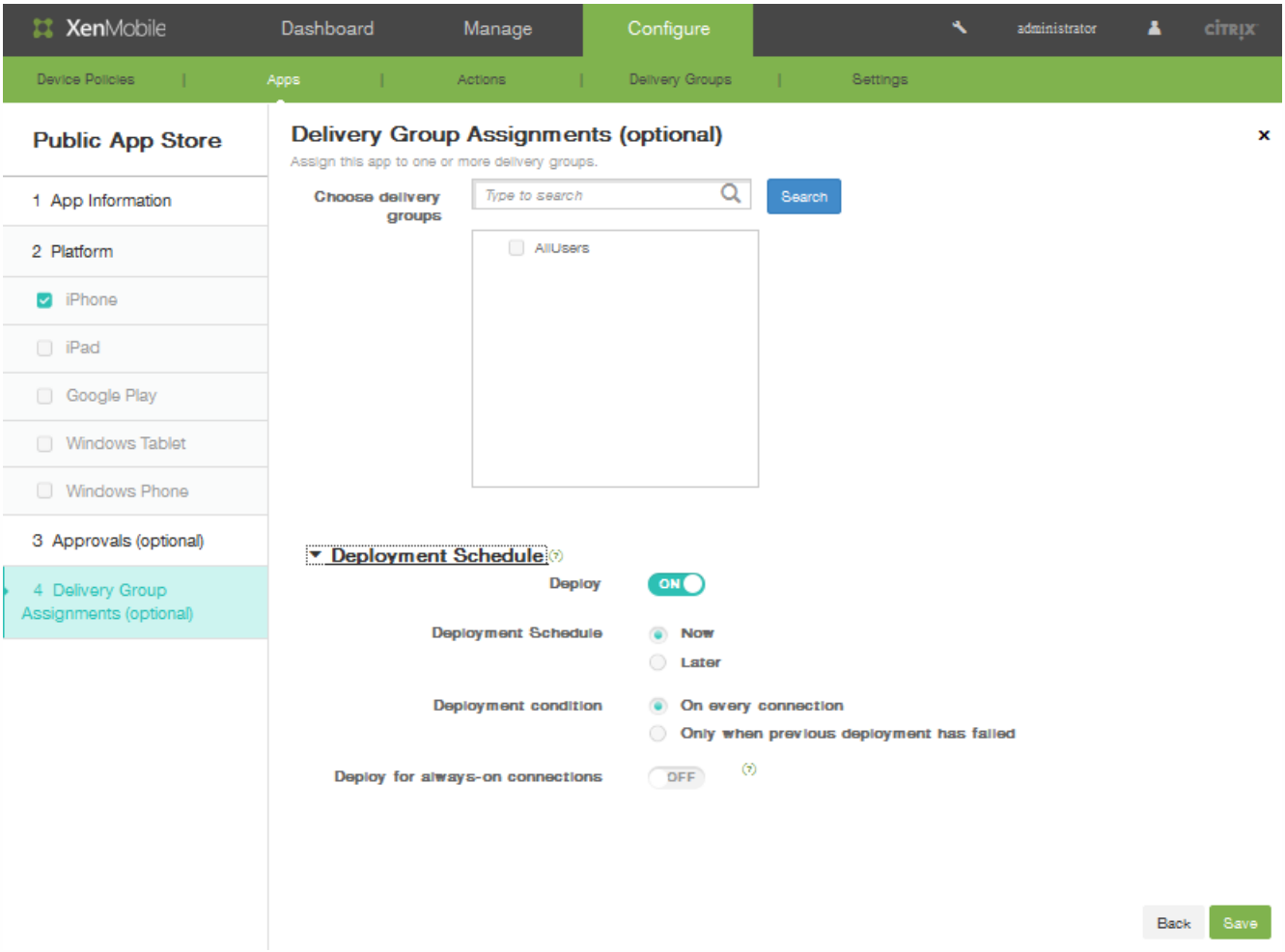


    4. Klicken Sie unter **Levels of manager approval** auf eine Stufe zwischen None und 3.
    5. Wählen Sie unter **Select Active Directory domain** die Domäne aus dem Dropdownmenü aus. Die Liste enthält nur Active Directory-Mitgliedsdomänen (z. B. testprise.net):



6. Geben Sie unter Find additional required approvers optional weitere Freigabeberechtigte ein und klicken Sie auf Search.

16. Weise Sie die App auf der Seite **Delivery Groups Assignment** optional einer oder mehreren Bereitstellungsgruppen zu.



17. Suchen Sie unter Choose delivery groups die Bereitstellungsgruppe(n). Aktivieren Sie das Kontrollkästchen **All Users**, um die App allen XenMobile-Benutzern zuzuweisen.
18. 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.

19. Klicken Sie auf Speichern.

May 05, 2016

In XenMobile können Sie eine Webadresse (URL) für eine öffentliche oder private Website oder eine Web-App, die kein Single Sign-On erfordert, einrichten.

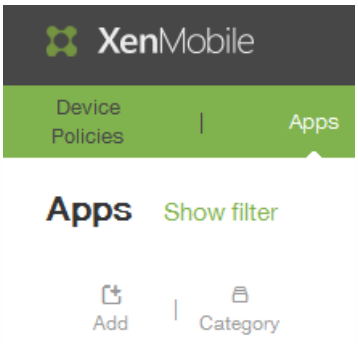
Sie können Weblinks über die Registerkarte Apps in der XenMobile-Konsole konfigurieren. Wenn Sie die Konfiguration des Weblinks abgeschlossen haben, wird der Link als Symbol in der Liste der App-Tabelle angezeigt. Der Link wird mit der Liste der verfügbaren Anwendungen und Desktops angezeigt, wenn Benutzer sich bei Worx Home anmelden.

Für den hinzuzufügenden Link müssen Sie die folgenden Informationen angeben:

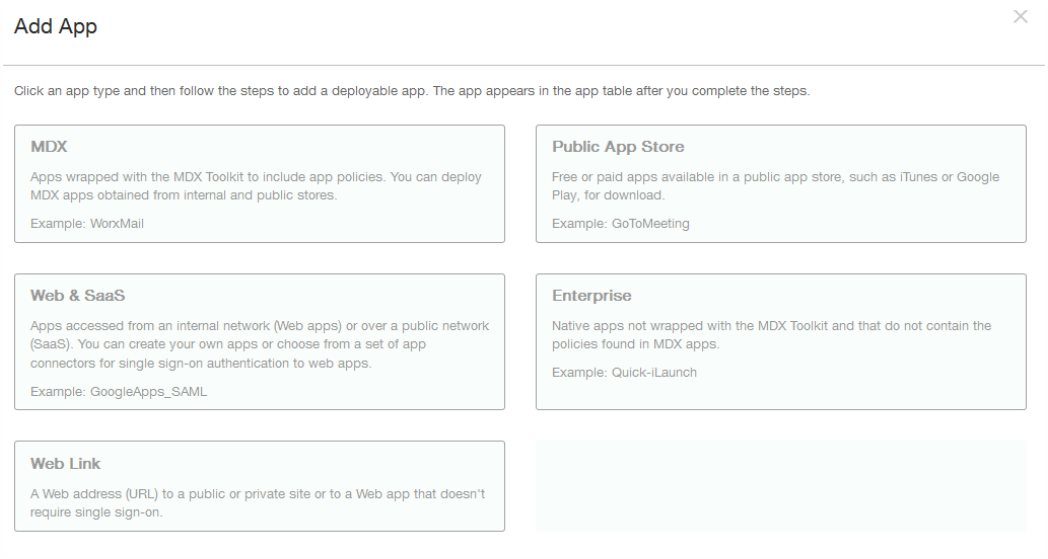
- Name für den Link
- Beschreibung des Links
- Webadresse (URL)
- Category
- Rolle
- Bild im PNG-Format (optional)

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.

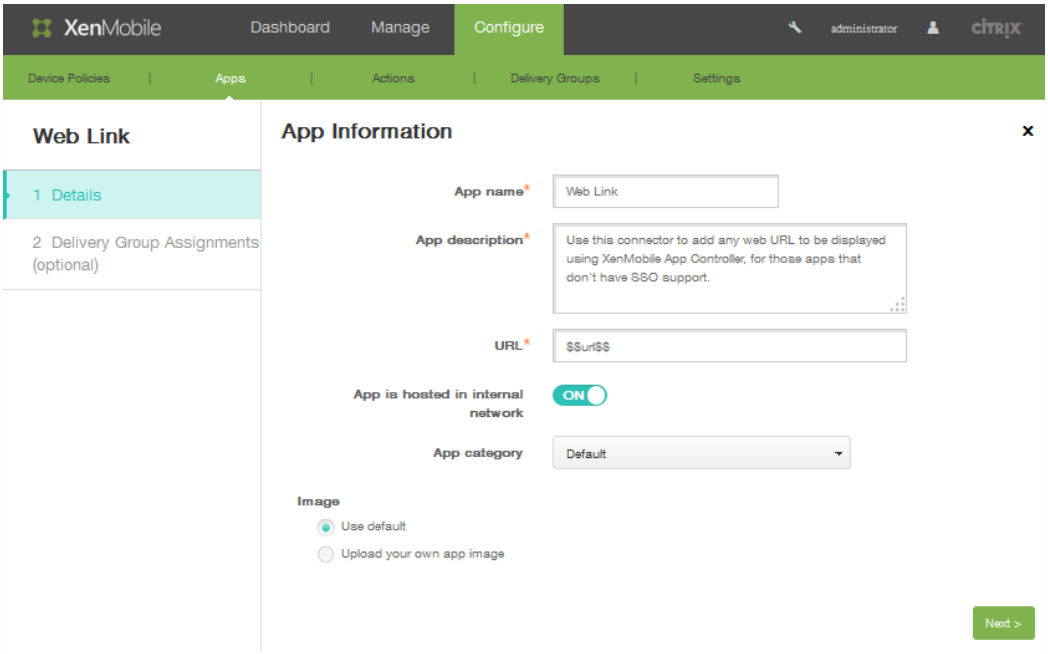


3. Klicken Sie auf der Seite Add App auf Web Link.

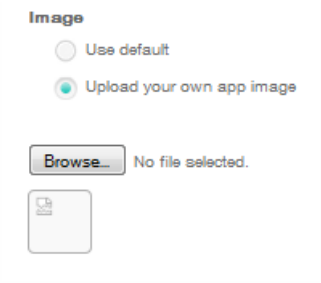


Die Seite App Information wird angezeigt.

4. Die Felder App name, Description und URL sind bereits ausgefüllt.

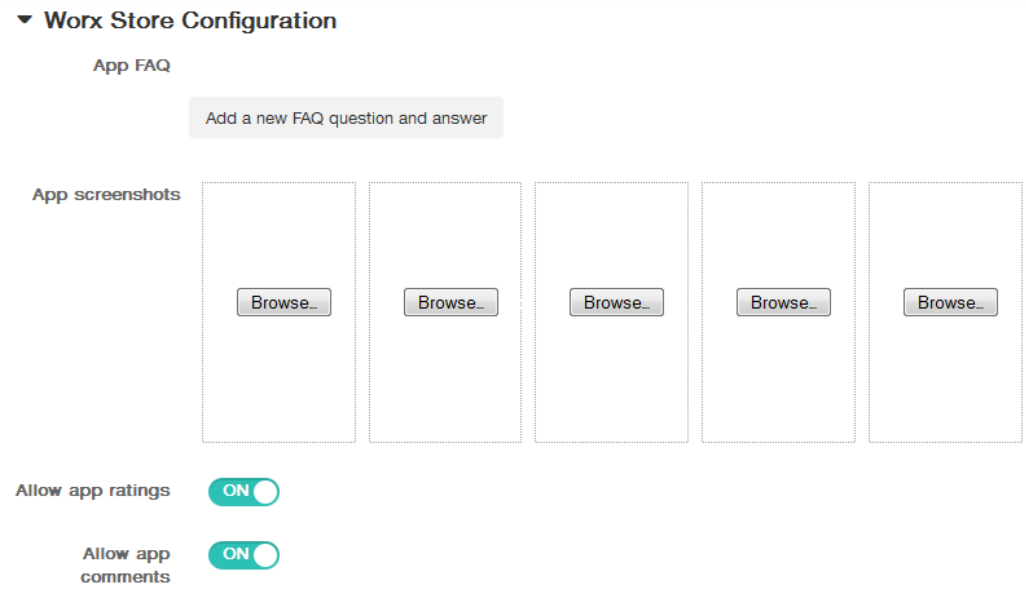


1. Geben Sie unter URL ggf. die Webadresse der App ein oder behalten Sie die Standardadresse bei.
2. Klicken Sie unter App is hosted in internal network auf ON, wenn die App auf einem Server im internen Netzwerk ausgeführt wird. Wenn Benutzer von einem Remotestandort aus eine Verbindung mit der internen 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:



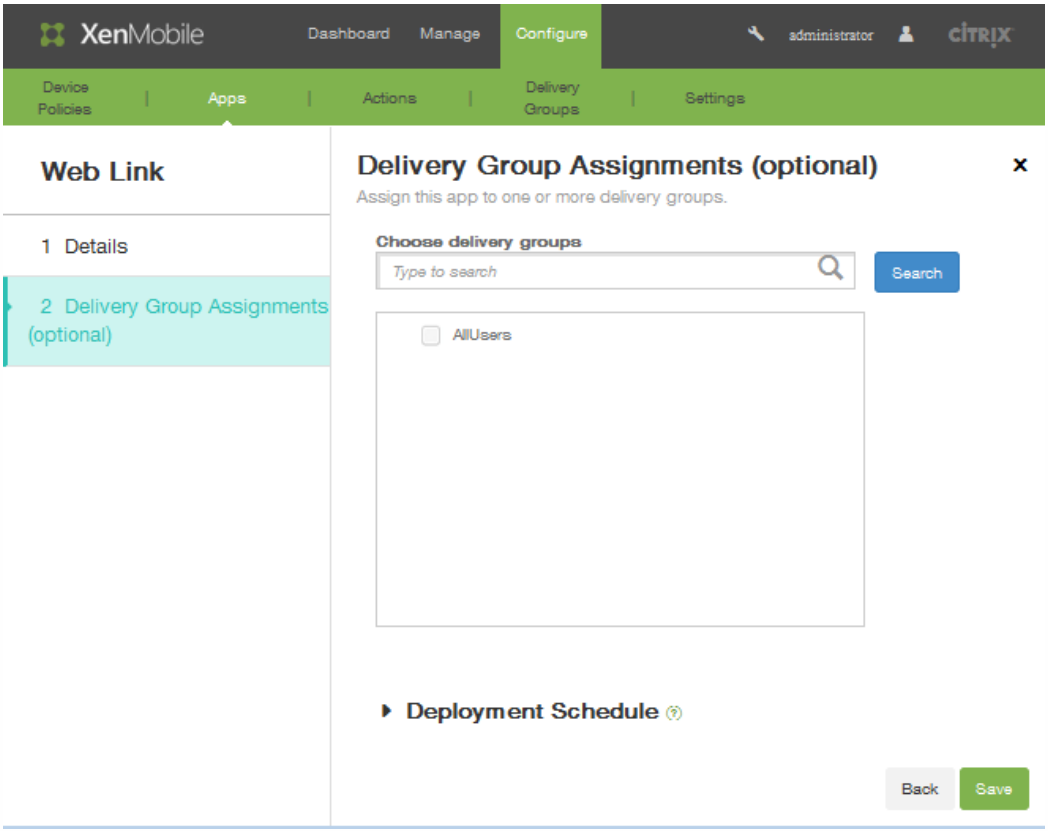
Bilder müssen im PNG-Format vorliegen.

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.

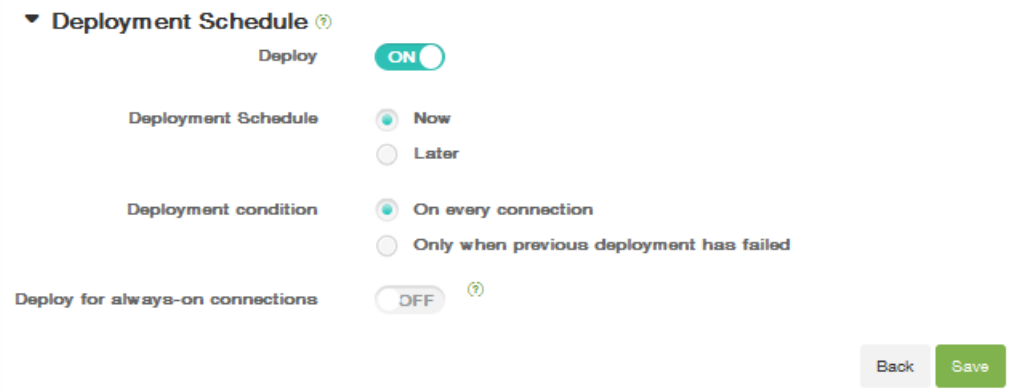


Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.

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.

May 05, 2016

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.

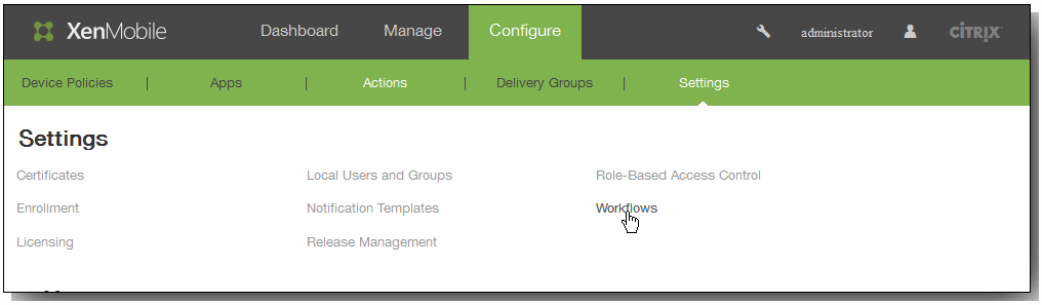
Bei der Erstkonfiguration von XenMobile werden auch die Einstellungen für Workflow-E-Mails konfiguriert. Diese Einstellungen müssen konfiguriert werden, damit Workflows verwendet werden können. Sie können die Einstellungen für Workflow-E-Mails jederzeit ändern. Diese Einstellungen umfassen E-Mail-Server, 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

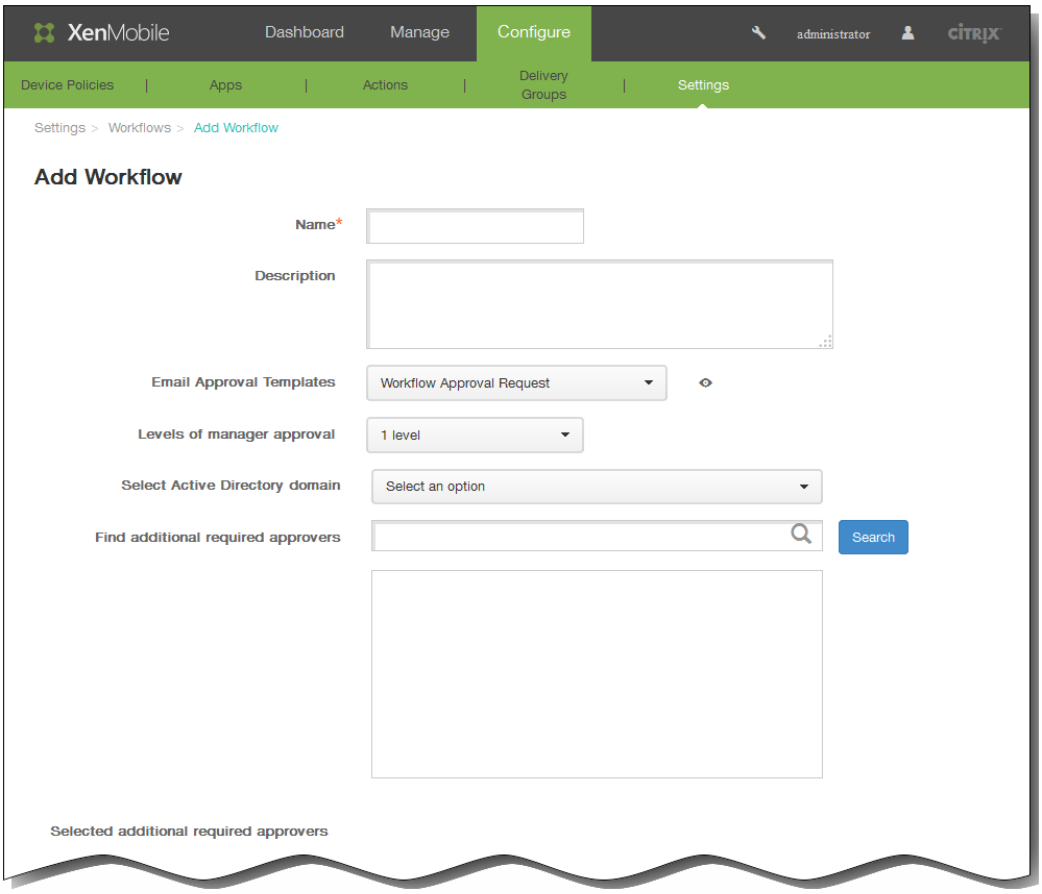
Sie können bis zu drei Ebenen für die Genehmigung von Benutzerkonten durch leitende Mitarbeiter zuweisen. Wenn noch weitere Personen zum Genehmigen eines Benutzerkontos berechtigt sein sollen, können Sie anhand des Namens oder der E-Mail-Adresse weitere genehmigende Personen suchen und auswählen. Wenn 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.

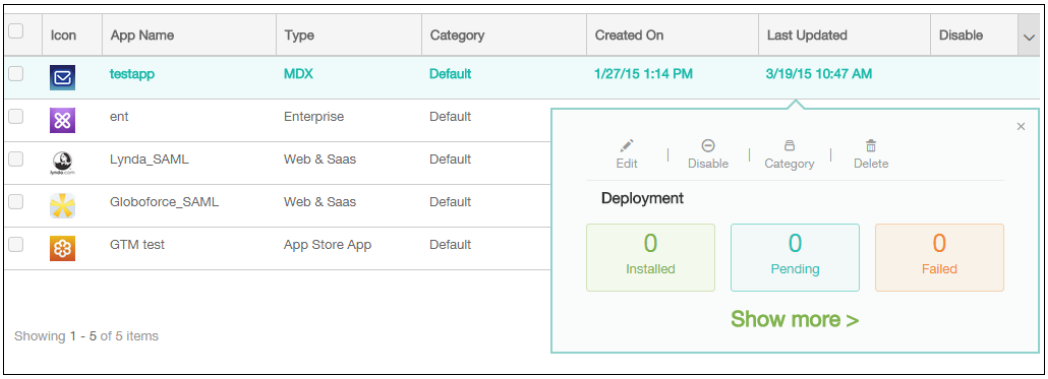
So zeigen Sie Details an und löschen einen Workflow

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.

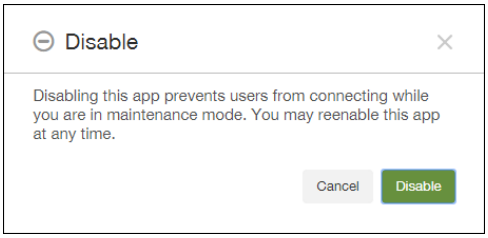
May 05, 2016

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.

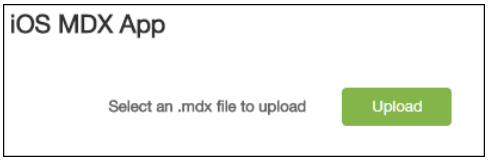


   2. Klicken Sie im Bestätigungsdialogfeld auf Disable.



   Als Status der App wird in der Tabelle nun Disabled angezeigt.

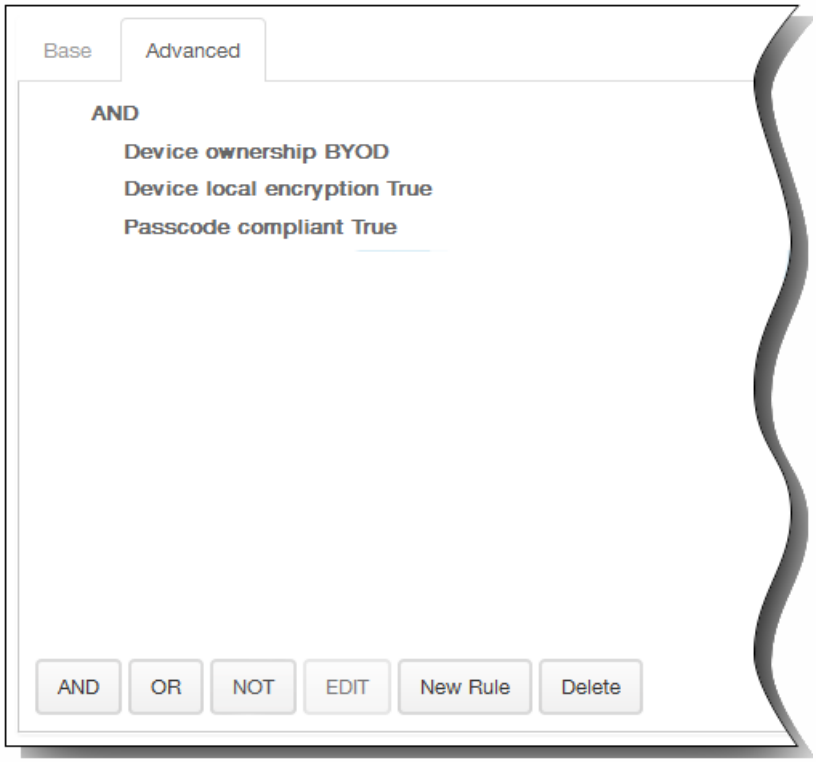
   Hinweis: Durch Deaktivieren werden Apps in den Wartungsmodus versetzt. Benutzer können nach der Abmeldung keine Verbindung mit deaktivierten Apps mehr herstellen. Das Deaktivieren von Apps ist optional, wird aber von Citrix empfohlen, um Probleme bei der App-Funktionalität zu vermeiden. Probleme können 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.

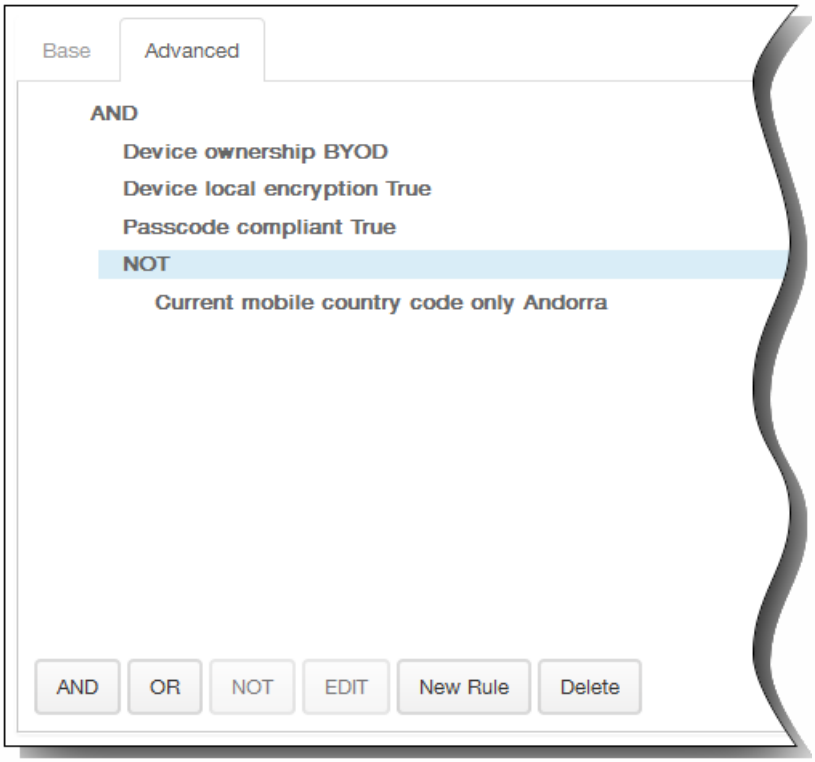
6. Klicken Sie auf Next und behalten Sie in den Schritten 8 bis 14 die Einstellungen bei, bzw. nehmen Sie Änderungen für das Upgrade vor.
7. Erweitern Sie Deployment Rules. Standardmäßig wird die Registerkarte Base angezeigt.

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.

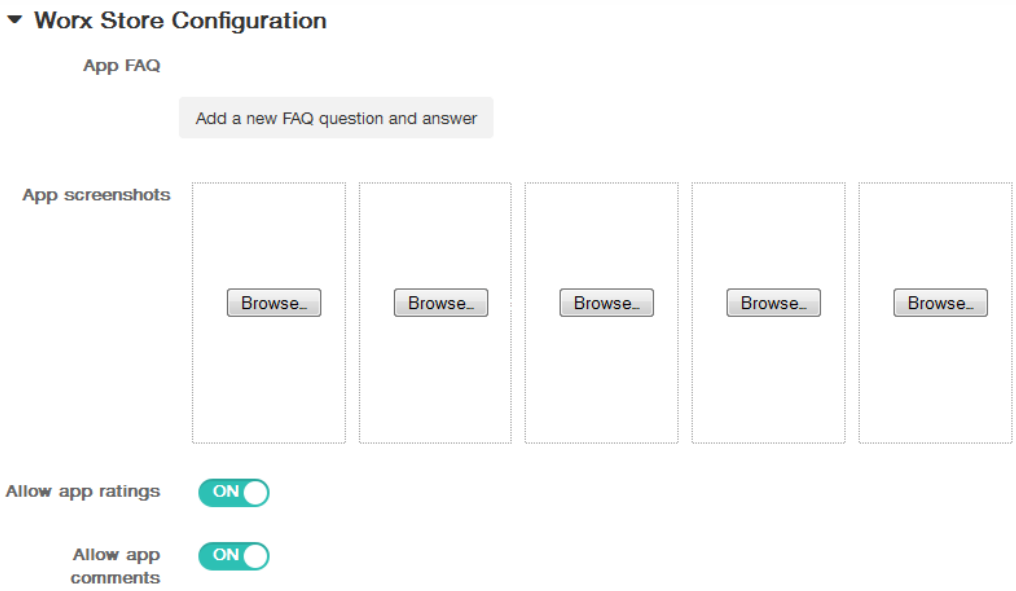


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

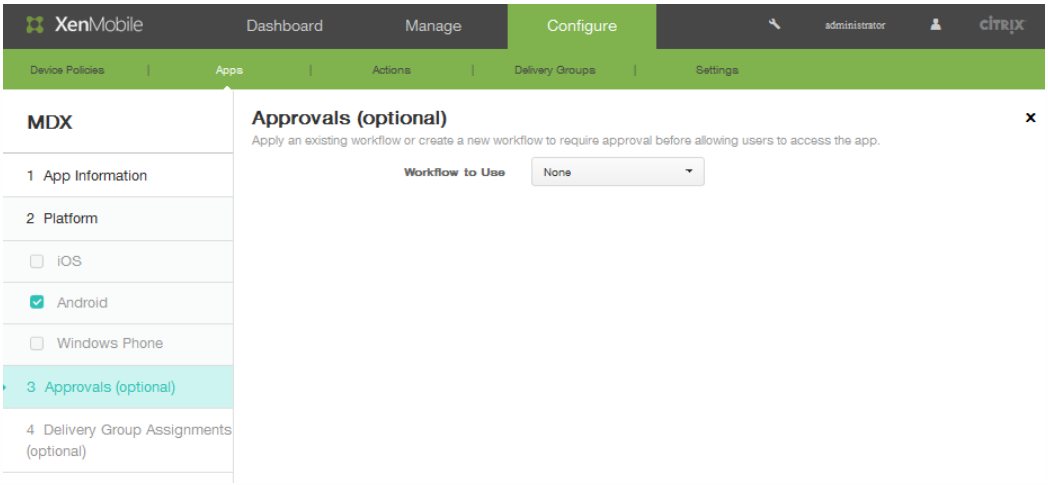
3. Sie können erweiterte boolesche Logik zum Kombinieren, Bearbeiten und Hinzufügen von Regeln verwenden.
   1. Klicken Sie auf AND, OR oder NOT.
   2. Wählen Sie in den nun angezeigten Listen die Bedingungen aus, die Sie der Regel hinzufügen möchten, und klicken Sie dann auf das Pluszeichen (+) auf 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.



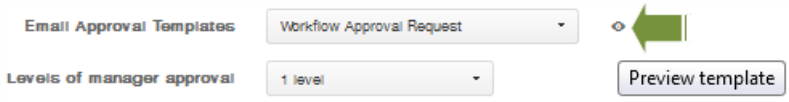
8. Erweitern Sie Worx Store Configuration, um FAQ für die App oder Bildschirmaufnahmen zur Klassifizierung des App im Worx Store hinzuzufügen. Die hochgeladene Grafik muss im PNG-Format sein. Sie können keine GIF- oder JPEG-Bilder hochladen.



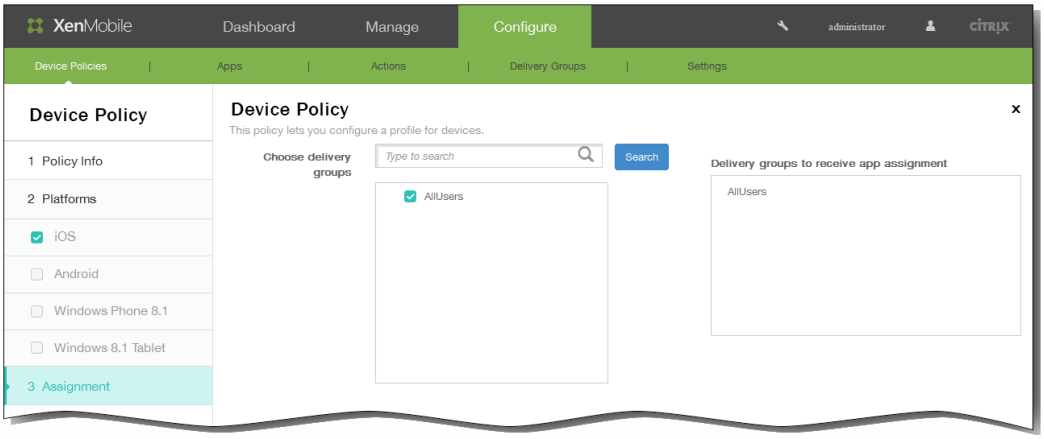
   Klicken Sie unter Allow app ratings auf ON, um eine Bewertung der App durch die Benutzer zuzulassen.
9. Klicken Sie unter Allow app comments auf ON, um eine Kommentierung der App durch die Benutzer zuzulassen.
10. Klicken Sie auf Next. Die Seite Approvals wird angezeigt.



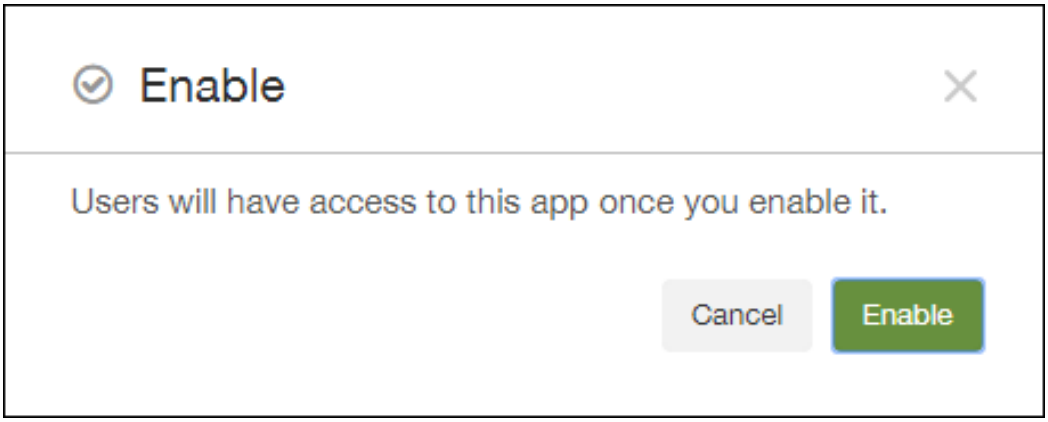
11. Wenn Sie einen neuen Workflow erstellen, werden in der XenMobile-Konsole nun Konfigurationsoptionen für den Freigabeprozess angezeigt. Die betreffenden Felder werden in den nachfolgenden Schritten erläutert. Konfigurieren Sie diese Felder, wenn für das Erstellen von Benutzerkonten eine Genehmigung 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.

May 05, 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 Verwalten von Worx Home.

May 05, 2016

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.

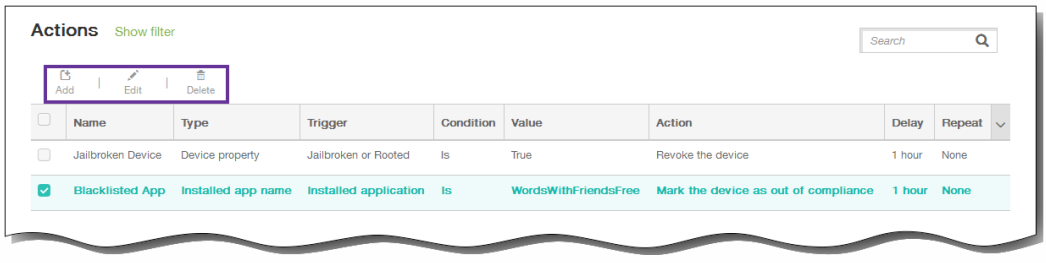
Sie können folgende automatische Auswirkungen festlegen:

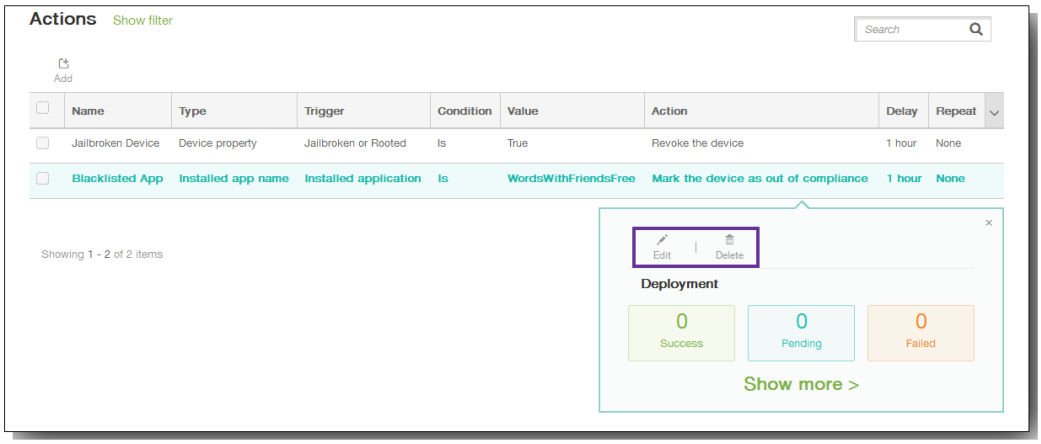
- Vollständige oder selektive Datenlöschung
- Einstufung von Geräten als nicht richtlinientreu
- Widerrufen von Geräten
- Senden einer Benachrichtigung an Benutzer mit der Aufforderung zur Problembehebung

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.

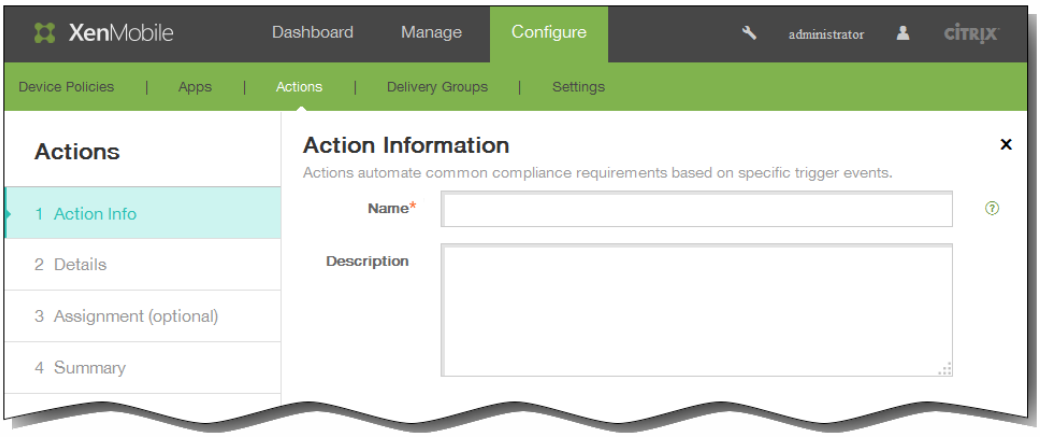
1. Klicken Sie in der XenMobile-Konsole auf Configure > Actions. Die Seite Actions wird angezeigt.

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.

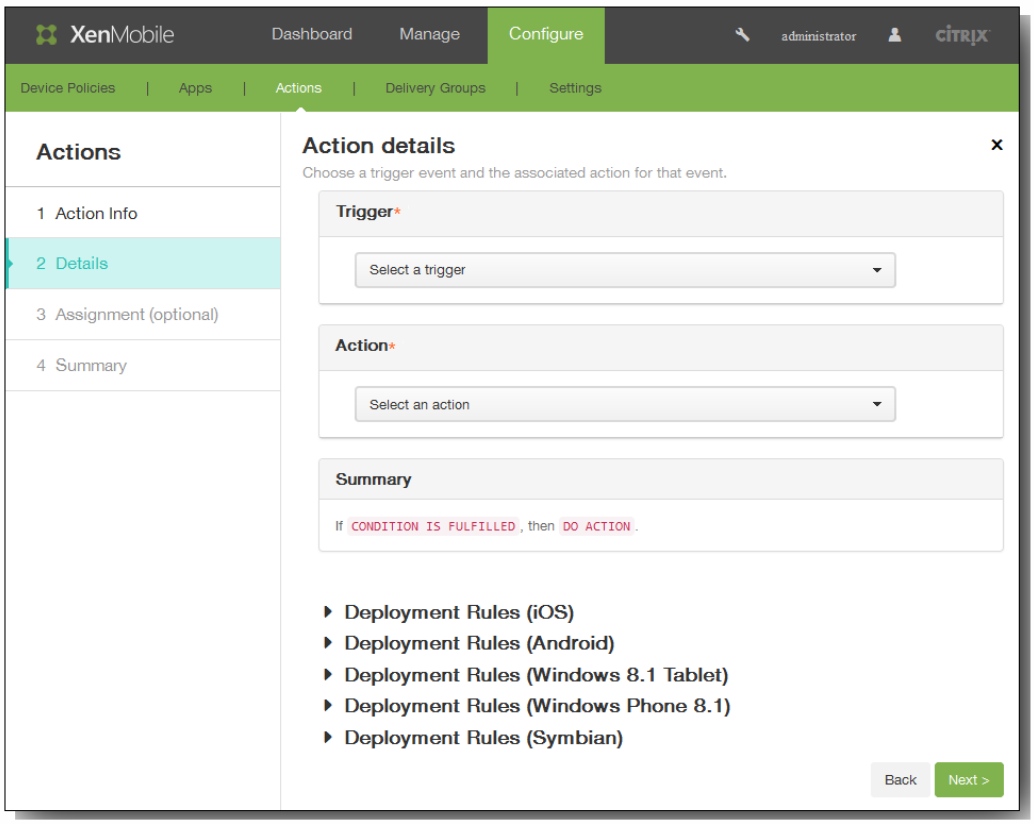




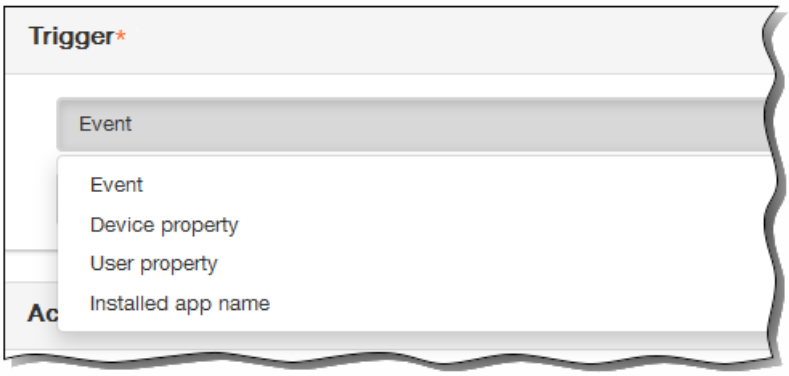
Die Seite Action Information wird angezeigt.



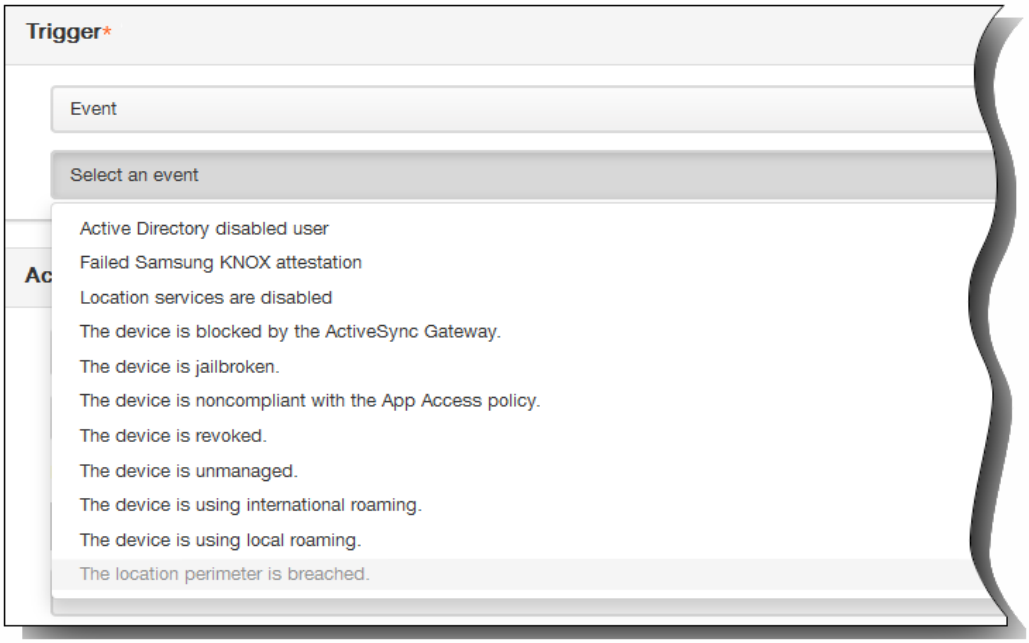
3. Konfigurieren Sie auf der Seite Action Information die folgenden Informationen:
   1. Name: Geben Sie einen Namen zur Identifizierung der Aktion ein. Diese Angabe ist erforderlich.
   2. Beschreibung: Geben Sie eine Beschreibung der Aktion ein.
4. Klicken Sie auf Next. Die Seite Action details wird 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.



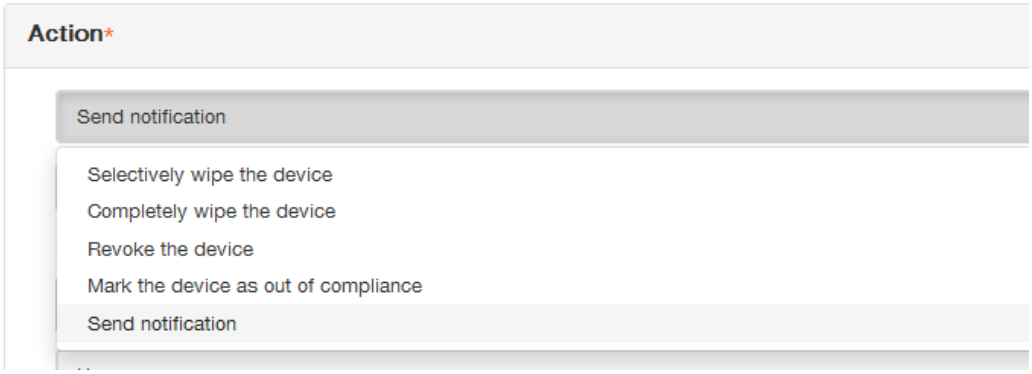
5. Konfigurieren Sie auf der Seite Action details die folgenden Informationen:
   1. Klicken Sie in der Liste Trigger auf den Auslösertyp für die Aktion. Es gibt folgende Auslöser:
      - Event: reagiert auf ein festgelegtes Ereignis.
      - Device property: prüft Geräte im MDM-Modus auf ein Attribut 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.

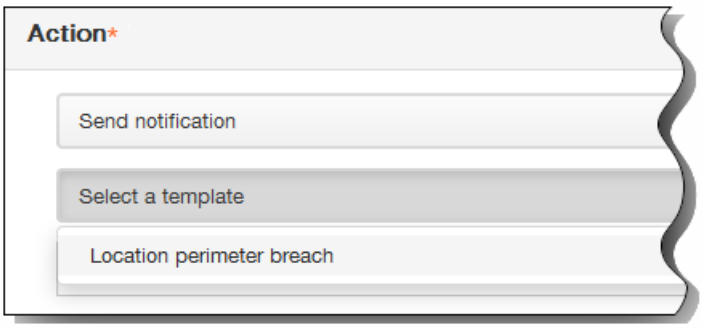


3. Klicken Sie in der Liste Action auf die Aktion, die ausgeführt werden soll, wenn das Auslöserkriterium erfüllt wird. Mit Ausnahme von Send notification können Sie für alle Optionen einen Zeitraum festlegen, in dem Benutzer das für den Auslöser ursächliche Problem beheben können. Wenn das Problem in diesem Zeitraum nicht behoben wird, wird die ausgewählte Aktion durchgeführt.



Bei den restlichen Schritten dieses Verfahrens wird erläutert, wie Sie eine Benachrichtigung senden.

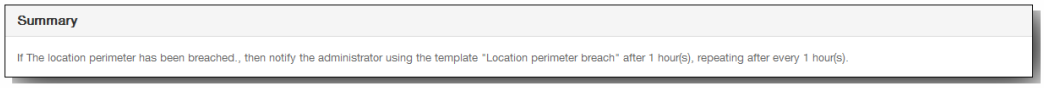
4. Wählen Sie in der nächsten Liste die Vorlage für die Benachrichtigung aus. Für das ausgewählte Ereignis relevante Benachrichtigungsvorlagen werden angezeigt.
   Hinweis: Sie können Benutzer nur benachrichtigen, wenn Sie unter Settings Benachrichtigungsserver für SMTP und SMS konfiguriert haben, damit 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.



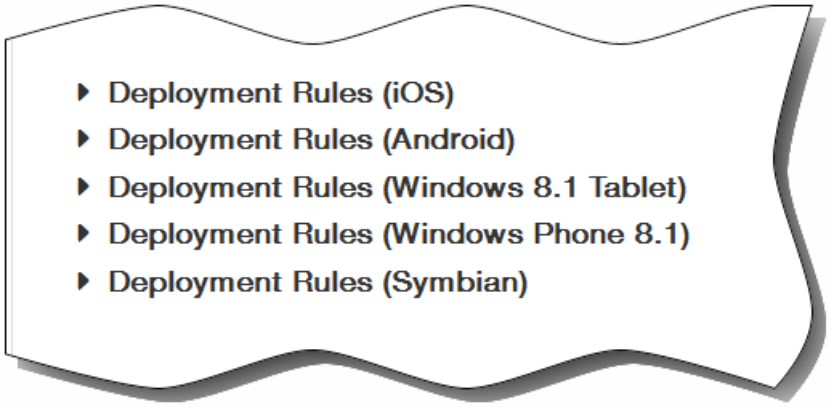
Hinweis: Nach Auswahl der Vorlage können Sie eine Vorschau davon anzeigen indem Sie auf Preview notification message klicken.

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.

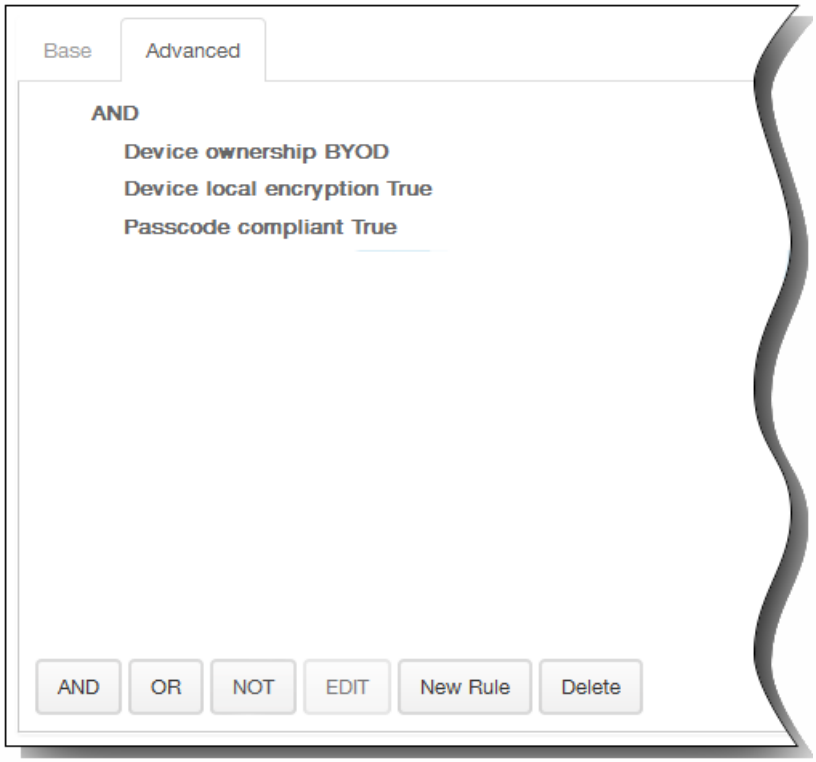


Nach dem Konfigurieren der Aktion können Sie für jede Plattform, d. h. iOS, Android, Windows 8.1 Tablet, Windows Phone 8.1 und Symbian, separat Bereitstellungsregeln festlegen. Führen Sie hierfür die Schritte 6 bis 9 für jede gewünschte Plattform aus.



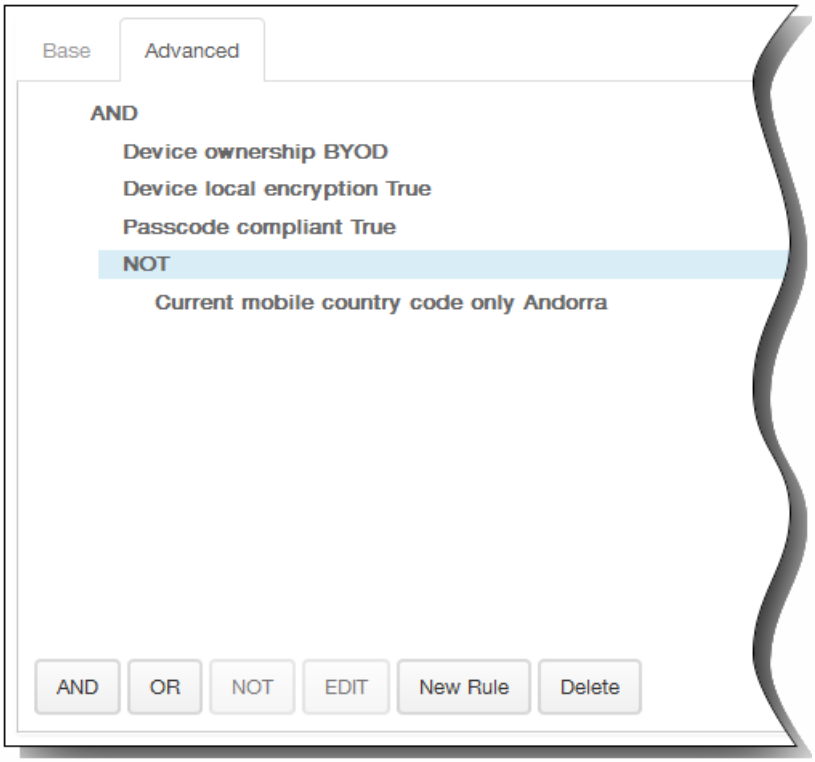
6. Erweitern Sie Deployment Rules. Standardmäßig wird die Registerkarte Base angezeigt.

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.

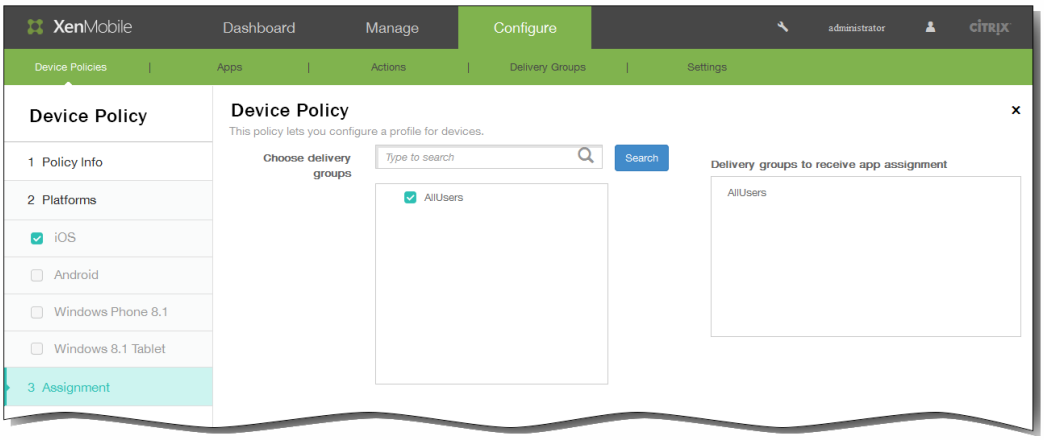


Die Bedingungen, die Sie auf der Registerkarte Base ausgewählt haben, werden angezeigt.

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.

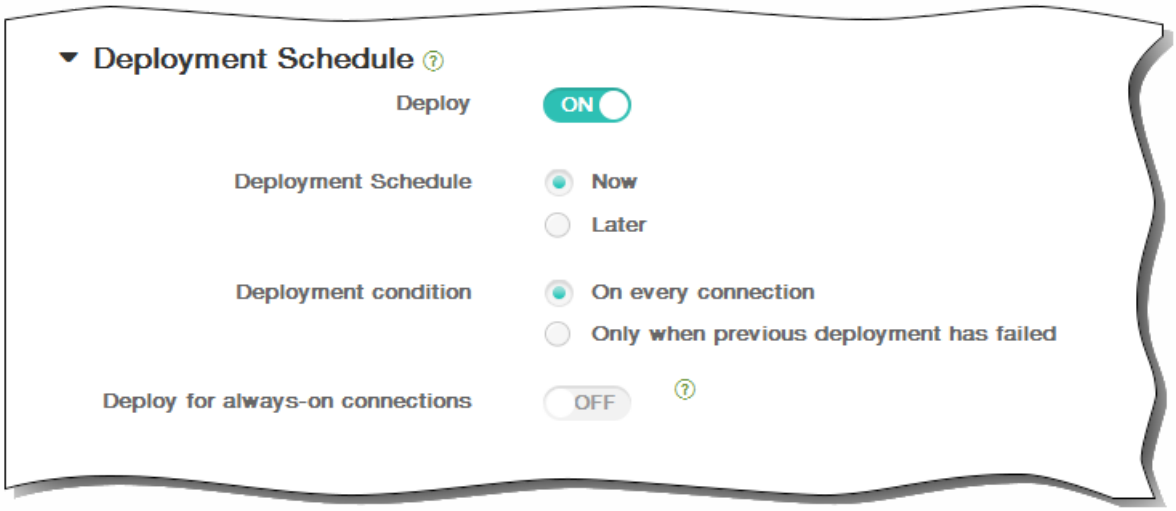


9. Erweitern Sie Deployment Schedule und konfigurieren Sie folgende Einstellungen:
   1. Klicken Sie neben Deploy auf ON, um die Bereitstellung zu planen, oder auf OFF, um die Bereitstellung zu verhindern. Die Standardeinstellung ist ON. Wenn Sie OFF auswählen, müssen keine anderen Optionen konfiguriert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

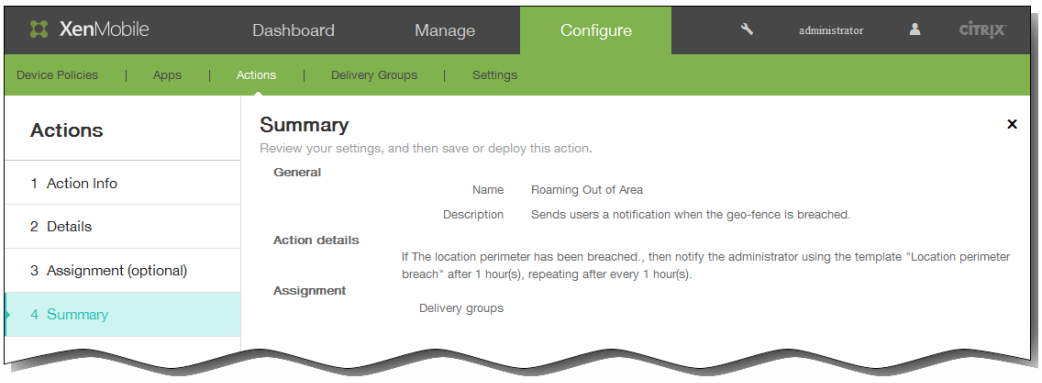
Die Standardeinstellung ist On every connection.

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.

May 05, 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.

So erstellen Sie angepasstes Worx Store-Branding für iOS-Geräte

Oct 13, 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

May 05, 2016

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.

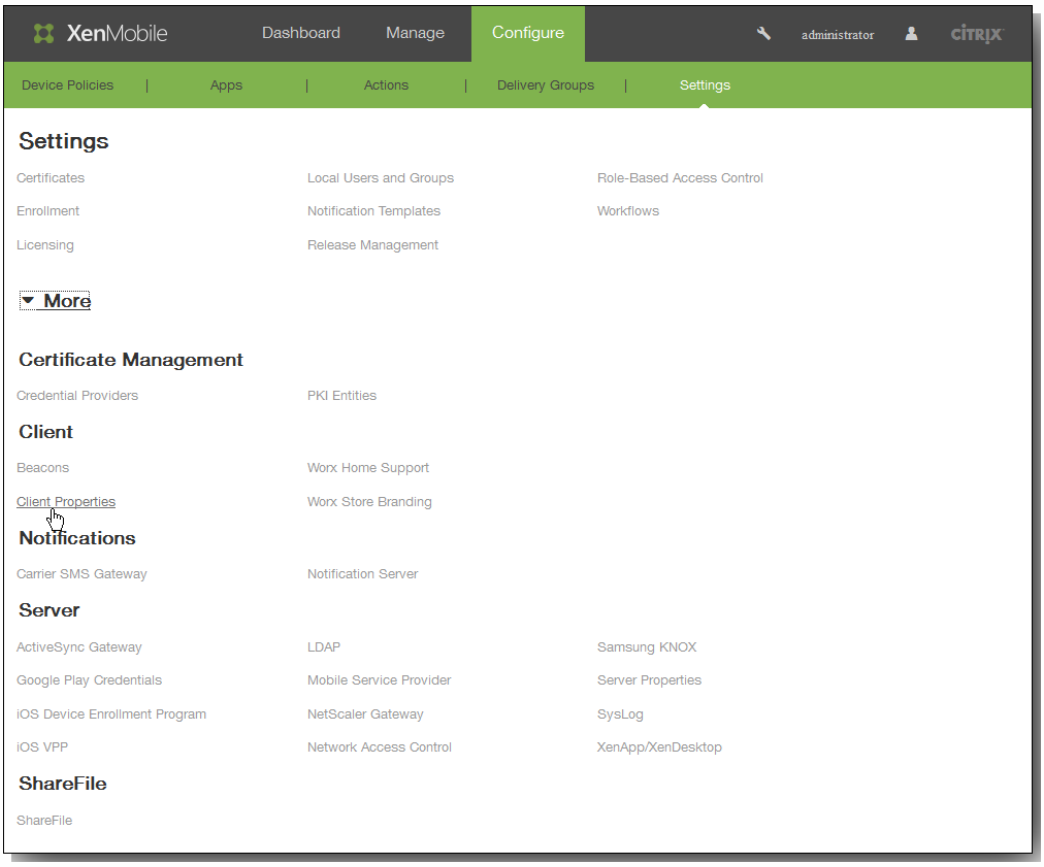
So erstellen, bearbeiten oder löschen Sie Clienteigenschaften

May 05, 2016

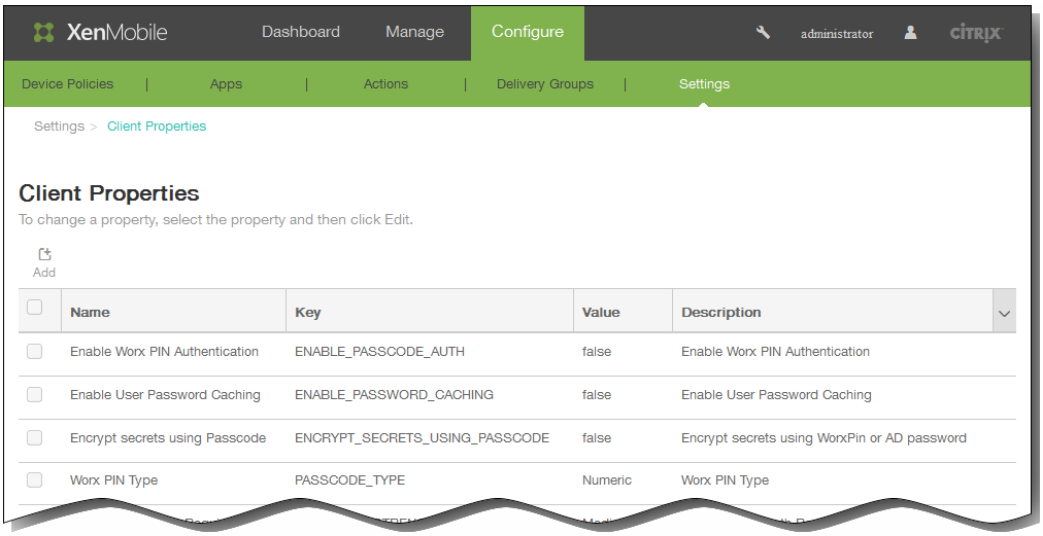
Clienteigenschaften enthalten Informationen, die direkt in Worx Home auf den Geräten der Benutzer bereitgestellt werden. Diese Eigenschaften werden zum Konfigurieren erweiterter Einstellungen, z. B. der Worx-PIN, verwendet. Clienteigenschaften sind beim Citrix Support erhältlich.

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.

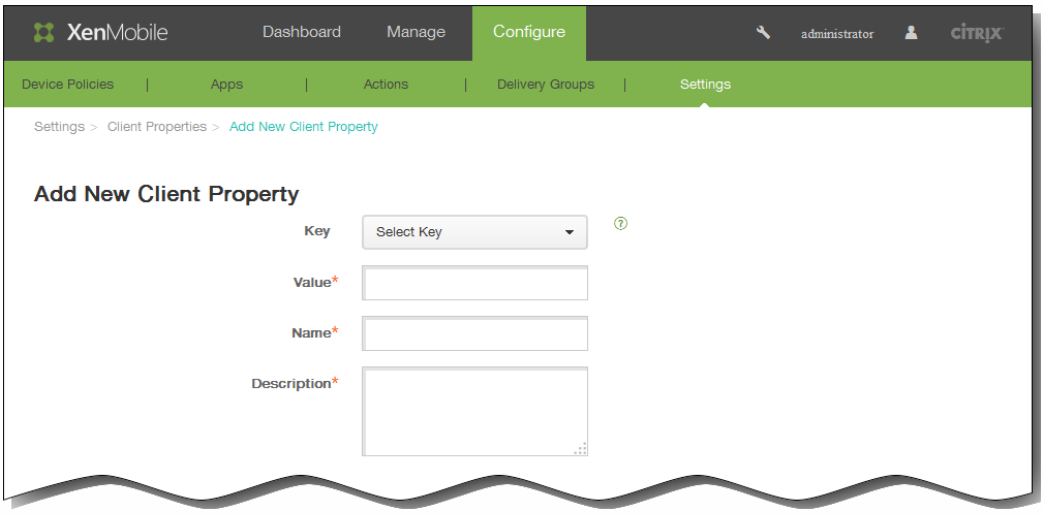


Die Seite Client Properties wird angezeigt. Auf dieser Seite können Sie die Clienteigenschaften hinzufügen, bearbeiten und löschen.



So fügen Sie eine Clienteigenschaft hinzu

1. Klicken Sie auf der Seite Client Properties auf Add. Die Seite Add New Client Property wird angezeigt.

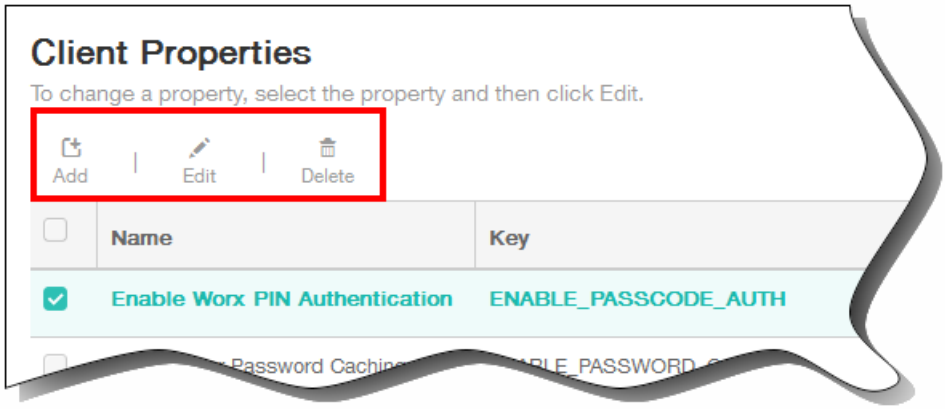


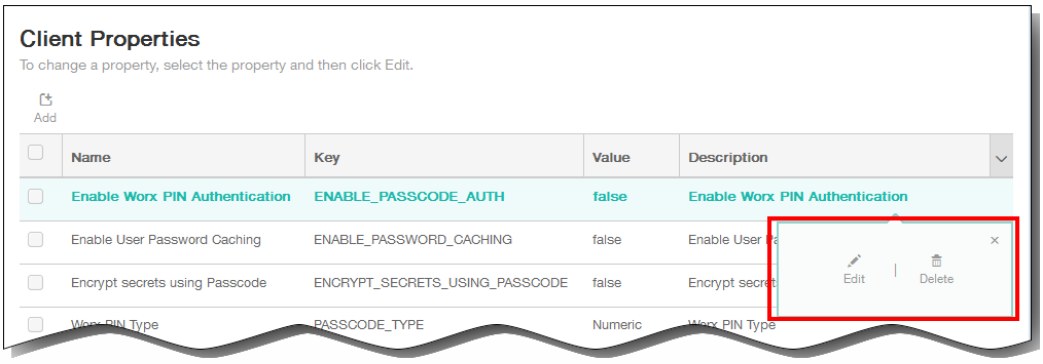
2. Geben Sie auf der Seite Add New Client Property die folgenden Informationen ein:
   Hinweis: Alle Felder müssen ausgefüllt werden.
   1. Key: Klicken Sie in der Liste auf den Eigenschaftsschlüssel, den Sie hinzufügen möchten.
      Wichtig: Wenden Sie sich an den Citrix Support, bevor Sie Änderungen 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

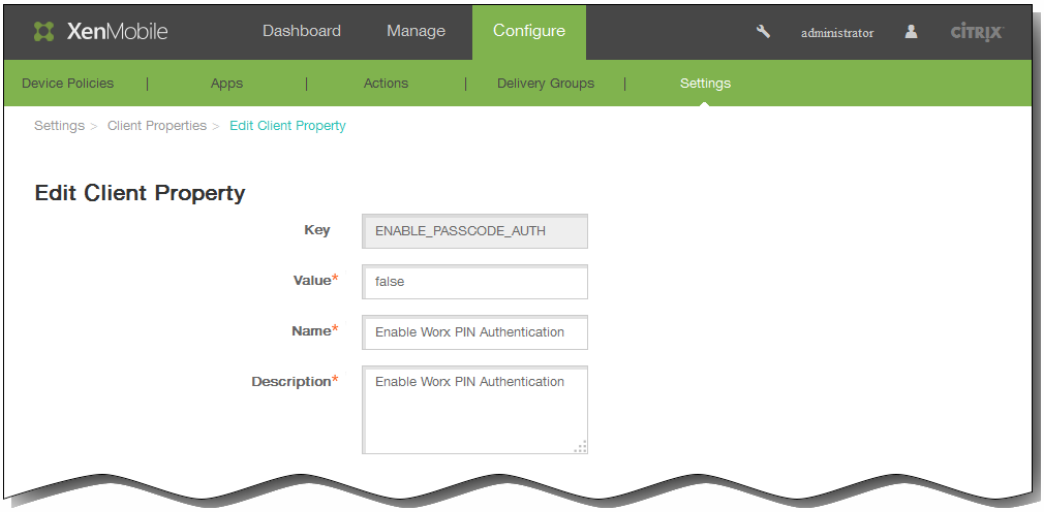
1. Wählen Sie in der Tabelle Client Properties die gewünschte Clienteigenschaft aus.
   Hinweis: Wenn Sie das Kontrollkästchen neben einer Clienteigenschaft auswählen, wird das Menü mit den Optionen oberhalb der Liste der Clienteigenschaften eingeblendet. Wenn Sie auf eine andere Stelle im Eintrag klicken, 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.

Clienteigenschaftenreferenz

Oct 13, 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)

XenMobile-Servereinstellungen

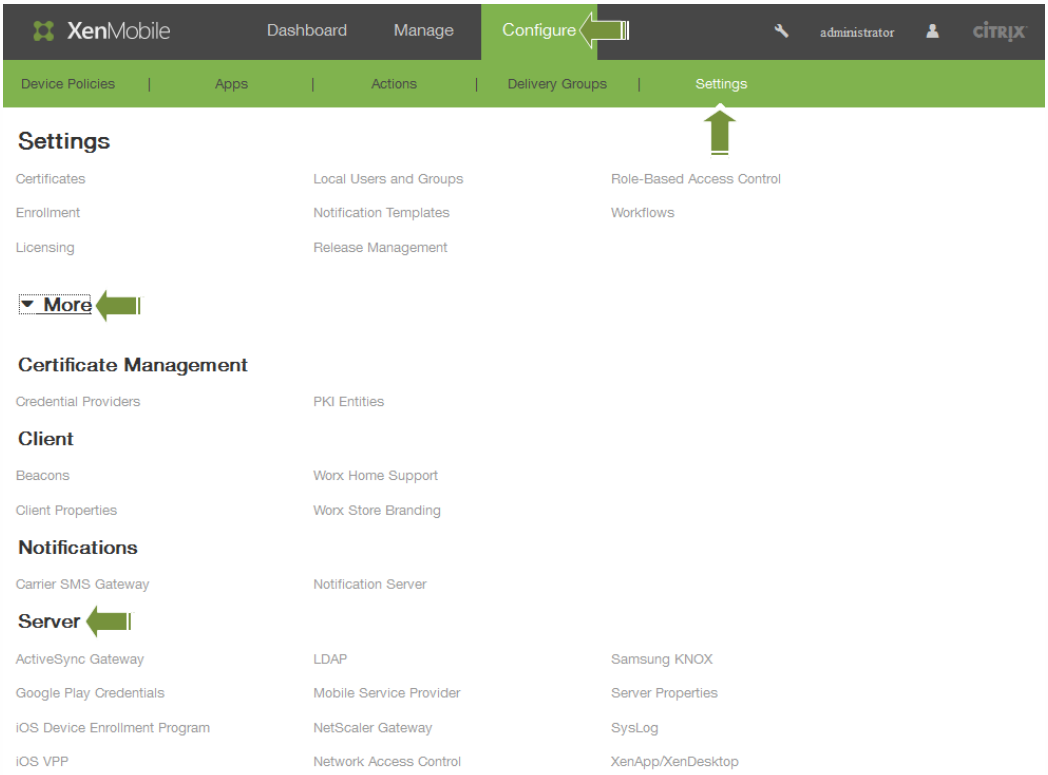
May 05, 2016

Sie können die XenMobile-Servereinstellungen über die XenMobile-Webkonsole konfigurieren.

Bei der Serverkonfiguration stehen folgende Optionen zur Verfügung:

ActiveSync Gateway	iOS VPP	NetScaler Gateway	Servereigenschaften
Google Play-Anmeldeinformationen	LDAP	Network Access Control	SysLog
Registrierungsprogramm für iOS-Geräte	Mobilfunkanbieter	Samsung KNOX	XenApp/XenDesktop

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

May 05, 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.

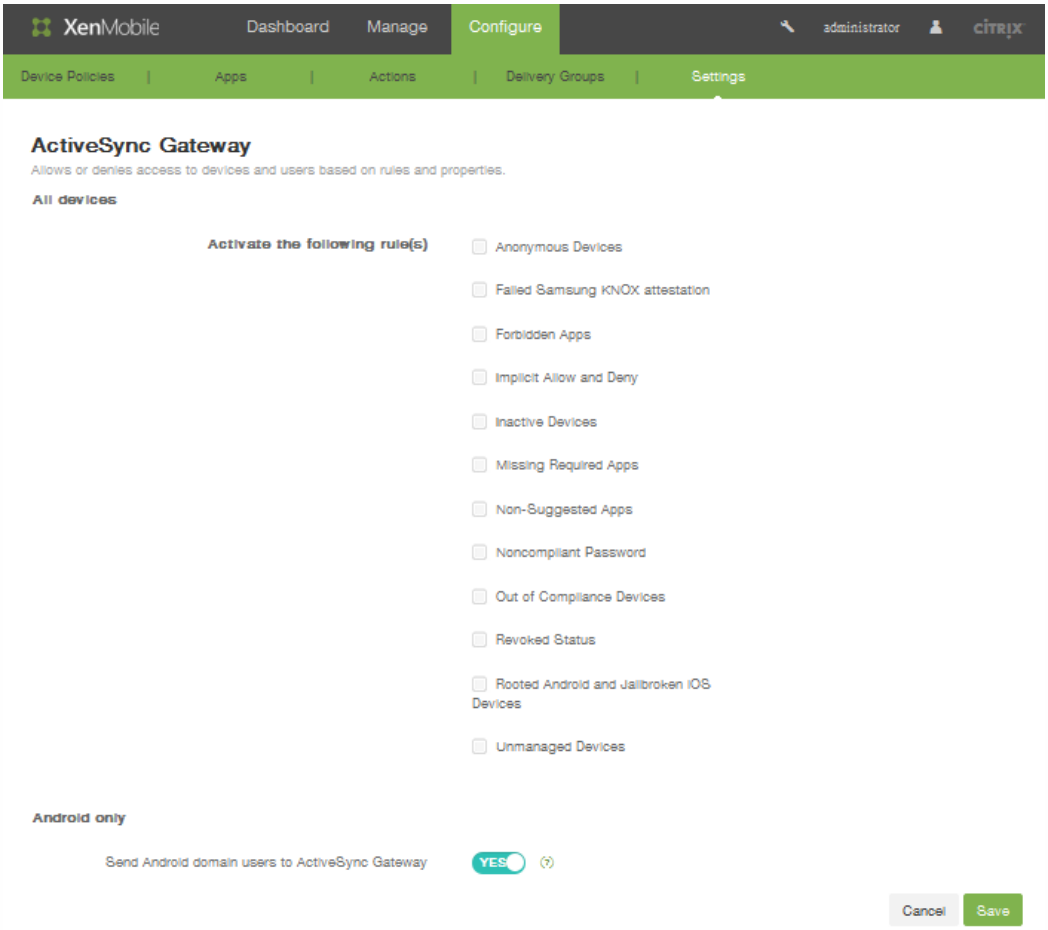
Unmanaged Devices: Prüft, ob ein Gerät verwaltet, d. h. von XenMobile kontrolliert wird. Beispielsweise ist ein Gerät im MAM-Modus oder ein nicht registriertes Gerät nicht verwaltet.

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 Konfigurationsseite **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

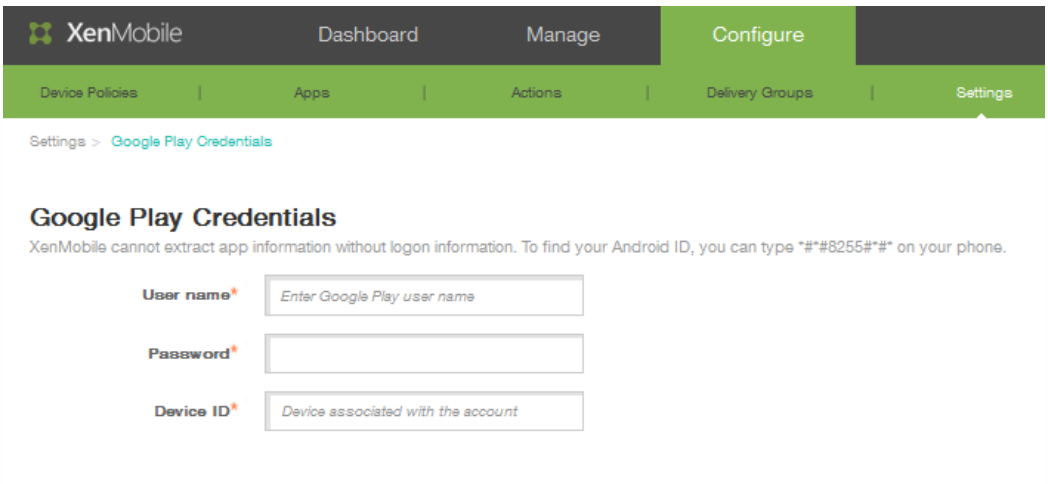
May 05, 2016

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

May 05, 2016

Sie können in XenMobile ein Registrierungsprogramm für iOS-Geräte einrichten. Über das Feature können iOS-Geräte Apple-Server über ein Profil benachrichtigen, durch das der Assistent zur Geräteeinrichtung angepasst wird und bestimmten Geräten zugewiesen wird.

So konfigurieren Sie das Registrierungsprogramm für iOS-Geräte in XenMobile

Damit Sie fortfahren können, müssen Sie ein Apple DEP-Konto (Device Enrollment Program) auf deploy.apple.com erstellen. Nachdem Sie das DEP-Konto erstellt haben, richten Sie einen virtuellen MDM-Server ein, damit XenMobile und Apple kommunizieren können. Dazu müssen Sie einen öffentlichen XenMobile-Schlüssel nach Apple hochladen. Wenn Apple den öffentlichen Schlüssel erhalten hat, wird ein Servertoken zurückgegeben, das Sie in XenMobile importieren. Mit den folgenden Schritten erstellen Sie die Verbindung zwischen XenMobile und Apple.

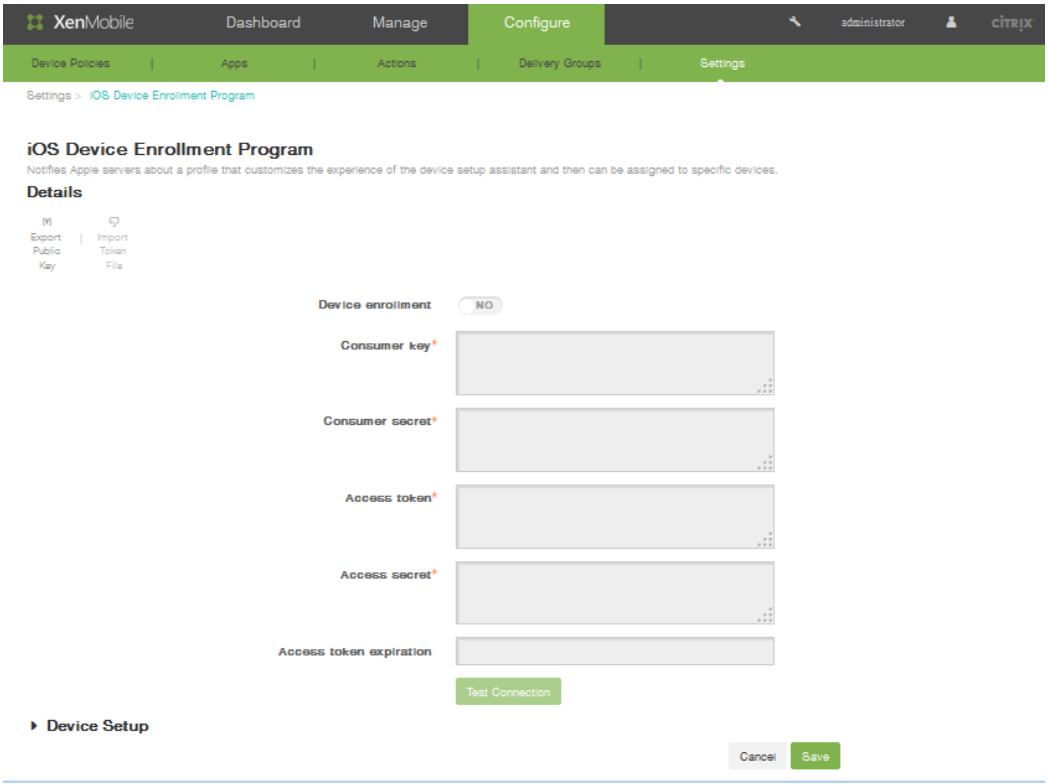
1. Um den öffentlichen Schlüssel für Apple zu erhalten, klicken Sie auf der Seite **iOS Device Enrollment Program** unter **Settings > More**, auf **Export Public Key** und speichern Sie die Datei auf Ihrem Computer.

2. Navigieren Sie zu deploy.apple.com, melden Sie sich bei Ihrem DEP-Konto an und folgen Sie den Anweisungen zum Einrichten eines MDM-Servers. Im Rahmen dieses Prozesses stellt Apple ein Servertoken bereit.

3. Legen Sie auf der Seite **iOS Device Enrollment Program** für **Device enrollment** die Einstellung **Yes** fest und klicken Sie auf **Import Token File**, damit XenMobile das Servertoken von Apple hinzugefügt wird.

4. Das Feld **Server tokens** wird automatisch ausgefüllt, wenn die Tokendatei nach XenMobile hochgeladen wurde.

5. Klicken Sie auf **Test Connectivity**, um zu testen, ob XenMobile und Apple kommunizieren. Wenn der Verbindungstest fehlschlägt, überprüfen Sie, ob alle erforderlichen Ports offen sind, denn dies ist die wahrscheinlichste Fehlerursache. Weitere Informationen zu den Ports, die in XenMobile offen sein müssen, finden Sie unter Portanforderungen.



Konfigurieren Sie in **Details** die folgenden Einstellungen für die DEP-Konfiguration:

- Device enrollment: Klicken Sie auf YES.
- Consumer key: Geben Sie den Verbraucherschüssel ein.
- Consumer secret: Geben Sie ein Verbrauchergeheimnis ein.
- Access token: Geben Sie das Zugriffstoken ein.
- Access secret: Geben Sie das Geheimnis für das Zugriffstoken ein.
- Access token expiration: Geben Sie optional das Ablaufdatum des Zugriffstokens an.
- Klicken Sie auf Test Connection, um die Verbindung zu prüfen.

- Erweitern Sie Device Setup und konfigurieren Sie folgende Einstellungen:
  - Business unit: Geben Sie den Namen der Geschäftseinheit ein.
  - Support phone number: Geben Sie die Telefonnummer des Supports ein.
  - Support email address: Geben Sie optional die E-Mail-Adresse des Supports ein.
  - Unique service ID: Geben Sie optional eine eindeutige Dienst-ID ein.

- Konfigurieren Sie unter Device Settings die folgenden Geräteeinstellungen für das Registrierungsprogramm für iOS-Geräte:
  - Allow or deny pairing: Klicken Sie auf Allow, um die Verwaltung des Geräts über Apple-Tools (iTunes und Apple Configurator) zuzulassen.

> ## Hinweis
>
> Wenn Sie die Kopplung zulassen und Apple Configurator verwenden, wählen Sie unter **Supervised mode** die Option **YES**.

- - Device profile removal: Wenn auf dem Gerät ein Profil verwendet werden soll, das remote entfernt werden kann, klicken Sie auf Allow.
  - Require device enrollment: Aktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass Benutzer die Registrierung überspringen.

- Konfigurieren Sie unter Device Setup folgende Einstellungen:
  - Location services: Klicken Sie auf Set up, um das Teilen des Standorts durch das Gerät zuzulassen, oder auf Skip, um dies zu verhindern.
  - Restore from backup: Klicken Sie auf Set up, damit das Gerät Daten aus einer Sicherungsdatei wiederherstellen kann.
  - Apple and iCloud: Klicken Sie auf Set up, wenn das Gerät die Apple-ID und iCloud verwenden soll.
  - Terms and Conditions: Klicken Sie auf Set up.
  - Passcode: Klicken Sie auf Set up, um für die Geräteregistrierung einen Passcode zu verwenden.
  - Siri: Klicken Sie auf Set up, um die Verwendung von Siri für das Gerät zu ermöglichen.
  - Touch ID: Klicken Sie auf Set up um die Verwendung von Touch ID für das Gerät zu ermöglichen.
  - Apple Pay: Klicken Sie auf Set up, um die Verwendung von Apple Pay für das Gerät zu ermöglichen.
  - Zoom: Klicken Sie auf Set up, um die Zoomfunktion zu aktivieren.
  - Diagnostics: Klicken Sie auf Set up, damit das Gerät Diagnosedaten teilen kann.

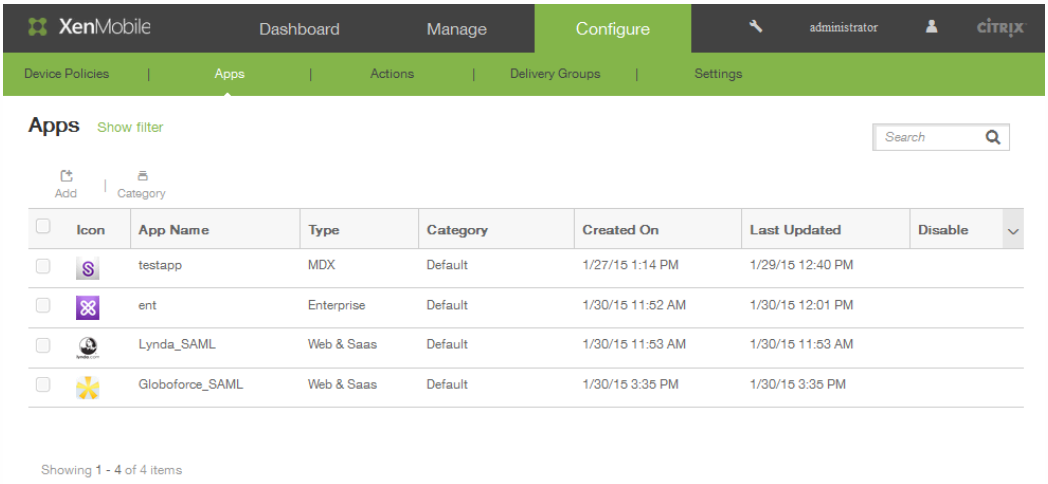
- Klicken Sie auf Save.

iOS VPP

May 05, 2016

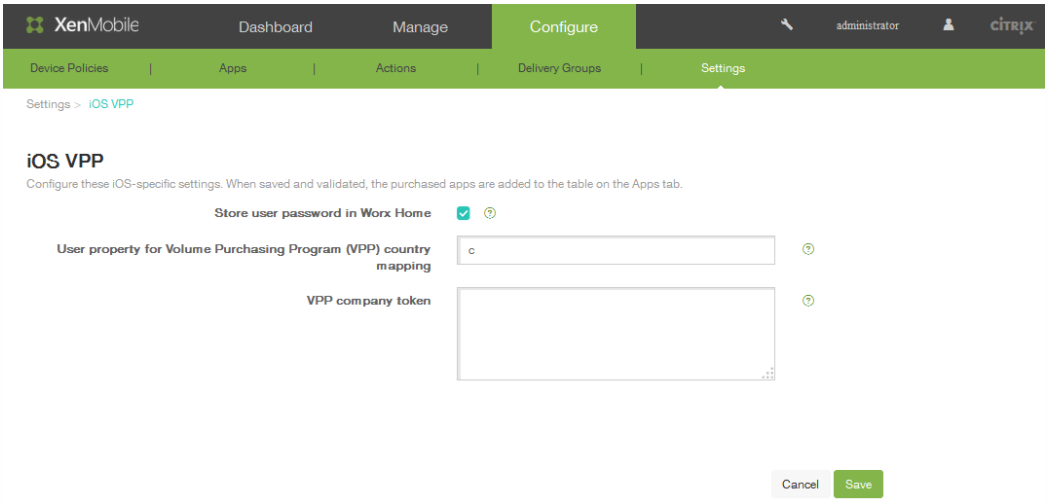
Sie können Einstellungen für das iOS-Programm für Volumenlizenzen (Volume Purchase Plan, VPP) in XenMobile konfigurieren. Das iOS VPP vereinfacht Suche, Erwerb und Verteilung von Apps und anderen Daten in großer Zahl. Das VPP ist eine einfache skalierbare Lösung zur Inhaltsverwaltung in einem Unternehmen.

Wenn Sie die iOS VPP-Einstellungen in XenMobile gespeichert und geprüft haben, werden die erworbenen Apps der Tabelle auf der Apps-Registerkarte in der XenMobile-Konsole hinzugefügt.



So konfigurieren Sie das iOS VPP in XenMobile

1. Klicken Sie in der XenMobile-Konsole auf Configure > Settings > More > iOS VPP.
   Die Seite zur Konfiguration des iOS VPP wird angezeigt.

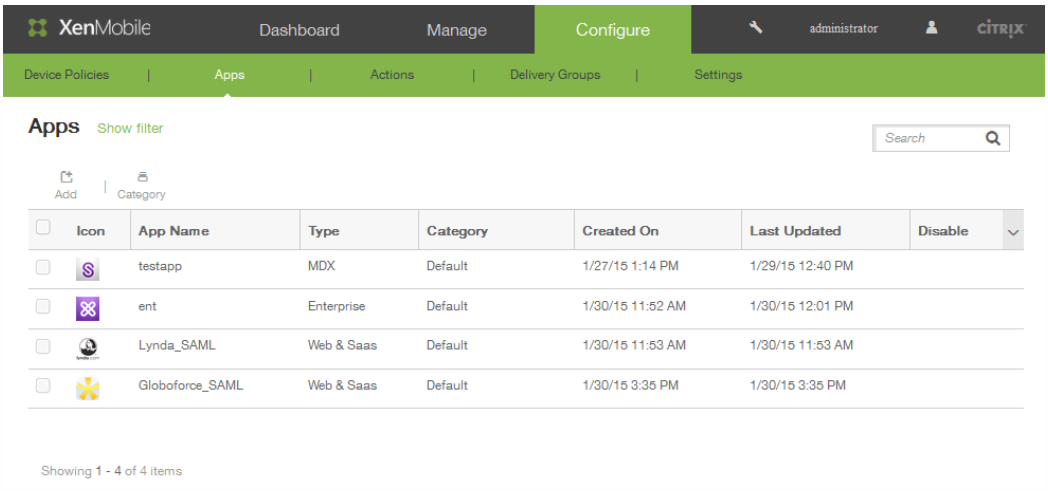


2. Wählen Sie unter Store user password in Worx Home das Kontrollkästchen zum sicheren Speichern eines

Benutzernamens und Kennworts in Worx Home für die XenMobile-Authentifizierung.

3. Geben Sie unter User property for Volume Purchasing Program (VPP) country mapping einen Code ein, um das Herunterladen aus landesspezifischen App-Stores zuzulassen.
   Diese Zuweisung wird zur Auswahl des Eigenschaftenpools des VPPs verwendet. Mit der Benutzereigenschaft "United States" können beispielsweise keine Apps heruntergeladen werden, wenn deren VPP-Code in Deutschland verteilt wird. Weitere Informationen über den Länderzuweisungscode erhalten Sie beim VPP-Administrator.

4. Geben Sie für VPP company token ein Token ein, das das vom VPP-Dienst beim Kauf eines Artikels aus dem Apple App Store über ein Unternehmenskonto generierte Token repräsentiert. Das Token wird zum Prüfen der VPP-Lizenz verwendet. Wenn Sie beispielsweise ein Apple VPP-Konto der Kategorie "Business" haben, besuchen Sie https://vpp.itunes.com, klicken Sie auf **Business** und melden Sie sich mit Ihren Apple-VPP-Anmeldeinformationen an, um die entsprechenden Informationen abzurufen.
5. Klicken Sie auf Speichern. Die Informationen werden dann in der App-Tabelle angezeigt:



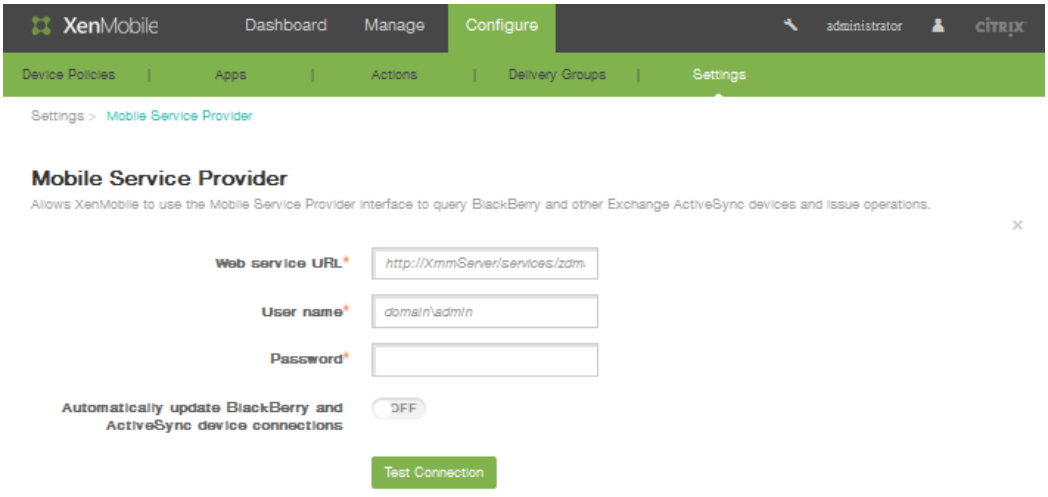
Mobilfunkanbieter

May 05, 2016

Sie können XenMobile für die Verwendung der Mobilfunkanbieter-Schnittstelle zum Abfragen von BlackBerry- und anderen Exchange ActiveSync-Geräten und Auslösen von Vorgängen konfigurieren.

So konfigurieren Sie den Mobilfunkanbieter

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



2. Geben Sie unter Web service URL die URL des Webdiensts ein, z. B. http://XmmServer/services/xdmservice.
3. Geben Sie unter User name den Benutzernamen im Format domain\admin ein.
4. Geben Sie unter Password das Kennwort ein.
5. Klicken Sie für Automatically update BlackBerry and ActiveSync device connections auf "ON", wenn Sie diese Option aktivieren möchten. Die Standardeinstellung ist OFF.
6. Klicken Sie auf Test connection, um die Verbindung zu prüfen.
7. Klicken Sie auf Speichern.

Network Access Control

May 05, 2016

Wenn Sie ein Gerät zur Netzwerkzugriffssteuerung (NAC) in Ihrem Netzwerk verwenden, beispielsweise eine Cisco ISE, können Sie in XenMobile Filter aktivieren, mit denen Benutzergeräte basierend auf Regeln oder Eigenschaften als NAC-richtlinientreu bzw. nicht NAC-richtlinientreu eingestuft werden. Wenn ein verwaltetes Gerät in XenMobile nicht die vorgegebenen Kriterien erfüllt und daher als nicht richtlinientreu eingestuft wird, wird es vom NAC-Gerät im Netzwerk blockiert.

Wählen Sie in der XenMobile-Konsole mindestens ein Kriterium für die Richtlinientreue von Geräten aus der Liste aus.

XenMobile unterstützt die folgenden NAC-Richtlinientreuefilter:

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.

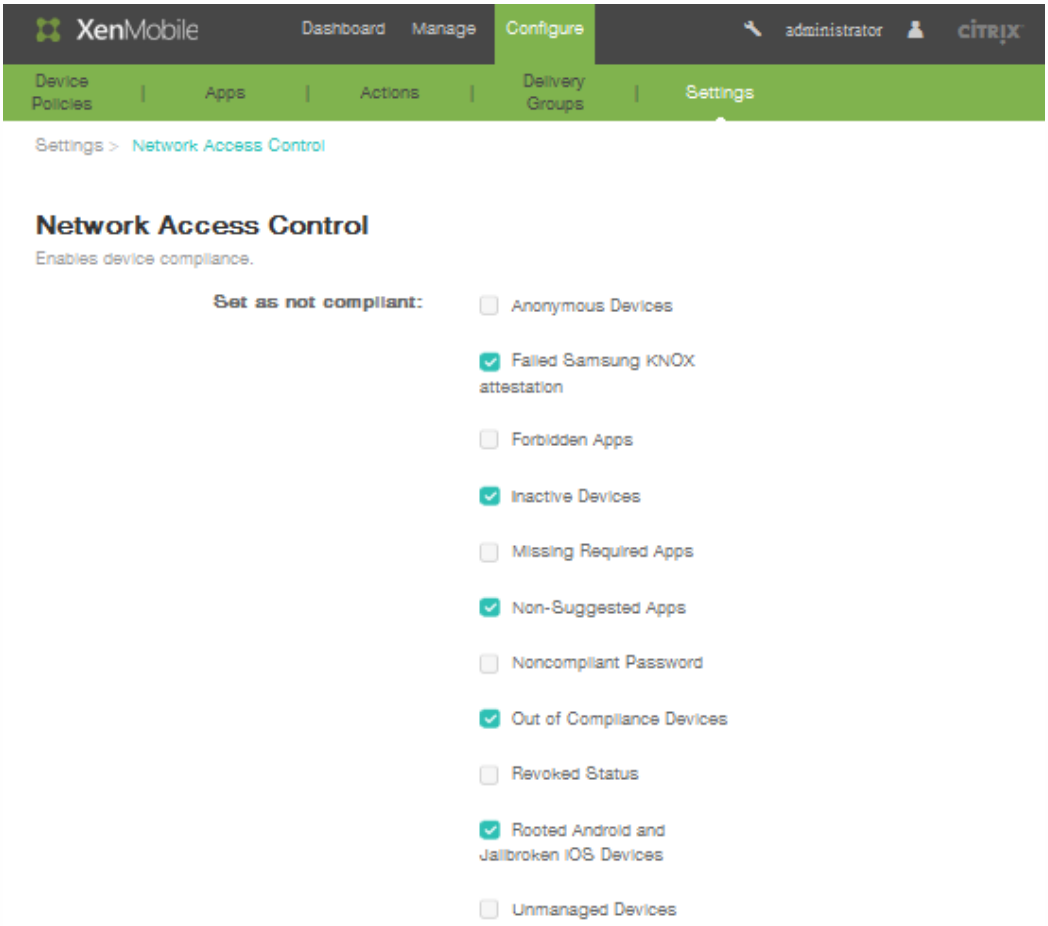
Send Android domain users to ActiveSync Gateway: Klicken Sie auf **YES**, damit XenMobile Android-Geräteinformationen an das ActiveSync Gateway sendet. Durch Aktivieren dieser Option wird sichergestellt, dass XenMobile

Android-Geräteinformationen an das ActiveSync Gateway für den Fall sendet, dass XenMobile den ActiveSync-Bezeichner für den Android-Gerätebenutzer nicht hat.

> ## Hinweis
>
> Durch den Filter "Implizit richtlinientreu/nicht richtlinientreu" wird der Standardwert nur auf Geräten festgelegt, die von XenMobile verwaltet werden. Beispiel: Alle Geräte mit einer gesperrten App bzw. solche, die nicht registriert sind, werden als nicht richtlinientreu eingestuft und durch das NAC-Gerät vom Netzwerk ausgeschlossen.

So konfigurieren Sie Network Access Control in XenMobile

1. Klicken Sie in der XenMobile-Konsole auf **Configure > Settings > More > Network Access Control**. Die Konfigurationsseite **Network Access Control** wird angezeigt.



2. Aktivieren Sie die Kontrollkästchen für die gewünschten Filter unter **Set as not compliant**.
3. Klicken Sie auf **Save**.

Samsung KNOX

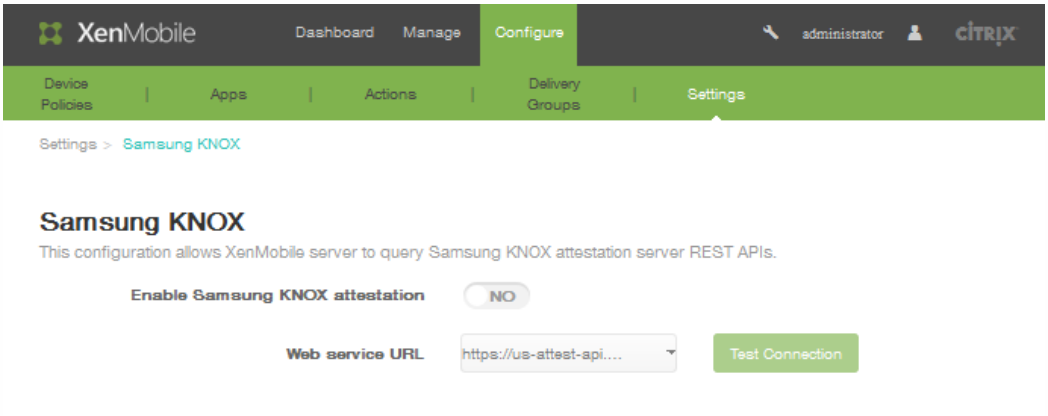
May 05, 2016

Sie können XenMobile für die Abfrage der REST-APIs des Samsung KNOX-Nachweisservers konfigurieren.

Samsung KNOX nutzt Sicherheitsmerkmale der Hardware, die mehrere Schutzstufen für Betriebssystem und Apps bieten. Eine Schutzstufe besteht im Nachweis auf der Plattform. Ein Nachweisserver bietet die Überprüfung der Kernsystemsoftware eines Mobilgeräts (z. B. Bootloader und Kernel) zur Laufzeit basierend auf Daten, die während eines vertrauenswürdigen Starts gesammelt wurden.

So aktivieren Sie den Samsung KNOX-Nachweis

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



2. Klicken Sie für Enable Samsung KNOX attestation auf **YES**.
3. Wenn Sie in Schritt 2 auf YES klicken, wird die Option **Web service URL** aktiviert. Wählen Sie in der Liste den gewünschten Nachweisserver aus.
4. Klicken Sie auf **Test Connection**, um die Verbindung zu prüfen.
5. Klicken Sie auf **Speichern**.

Servereigenschaften

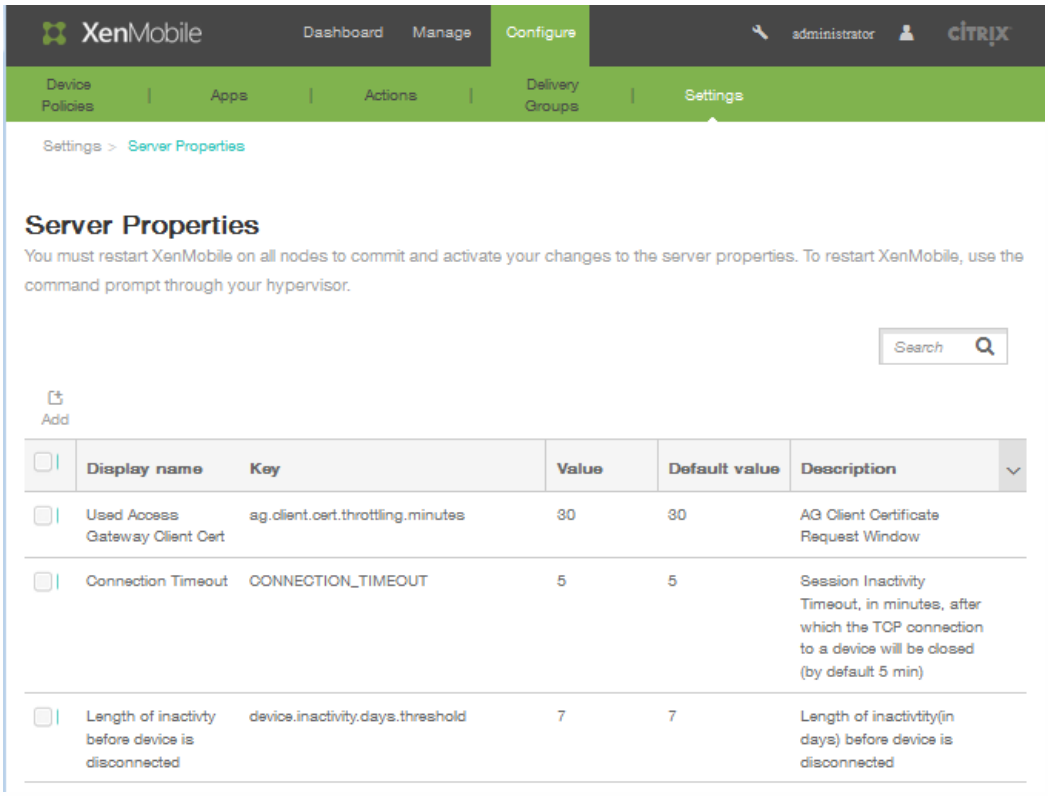
May 05, 2016

In XenMobile können Eigenschaften auf den Server anwenden. Wenn Sie Änderungen vornehmen, müssen Sie XenMobile auf allen Knoten neu starten, damit die Änderungen übergeben und aktiviert werden.

Hinweis: Zum Neustarten von XenMobile verwenden Sie die Eingabeaufforderung durch den Hypervisor.

So konfigurieren Sie Servereigenschaften in XenMobile

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



2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf Add, um eine neue Servereigenschaft hinzuzufügen.
   - Wählen Sie in der Tabelle eine Eigenschaft aus und klicken Sie dann in dem nun angezeigten Menü auf Edit.
3. Wenn Sie in Schritt 2 auf Add geklickt haben, konfigurieren Sie die folgenden Felder:

- Key: Wählen Sie in der Liste den geeigneten Schlüssel aus.
  Hinweis: Bei Schlüsseln wird Groß- und Kleinschreibung unterschieden. Bevor Sie Änderungen vornehmen, müssen Sie sich an den Citrix Support wenden oder einen speziellen Schlüssel anfordern.

- **Value**: Geben Sie einen Wert ein, je nachdem, welchen Schlüssel Sie ausgewählt haben.
- **Display name**: Geben Sie einen Namen für die neue Eigenschaft ein, der in der Tabelle der Servereigenschaften angezeigt werden soll.

- **Description**: Geben Sie optional eine Beschreibung der neuen Servereigenschaft ein und klicken Sie dann auf Save.

SysLog

May 05, 2016

Sie können XenMobile zum Senden von Protokolldateien an einen syslog-Server konfigurieren. Sie brauchen den Hostnamen oder die IP-Adresse des Servers.

Syslog ist ein Standardprotokoll für die Protokollierung mit zwei Komponenten: einem Überwachungsmodul (dies wird auf dem Gerät ausgeführt) und einem Server, der auf einem Remotesystem ausgeführt werden kann. Syslog verwendet UDP (User Data Protocol) für Datenübertragungen.

Sie können den Server zum Sammeln folgender Datentypen konfigurieren:

- Systemprotokolle, die Aktionen von XenMobile enthalten
- Überwachungsprotokolle, die eine chronologische Auflistung der Systemaktivitäten im Zusammenhang mit XenMobile enthalten

Von einem syslog-Server über ein Gerät gesammelte Protokolldaten werden in einer Protokolldatei in Form von Meldungen gespeichert. Diese Meldungen enthalten normalerweise die folgenden Informationen:

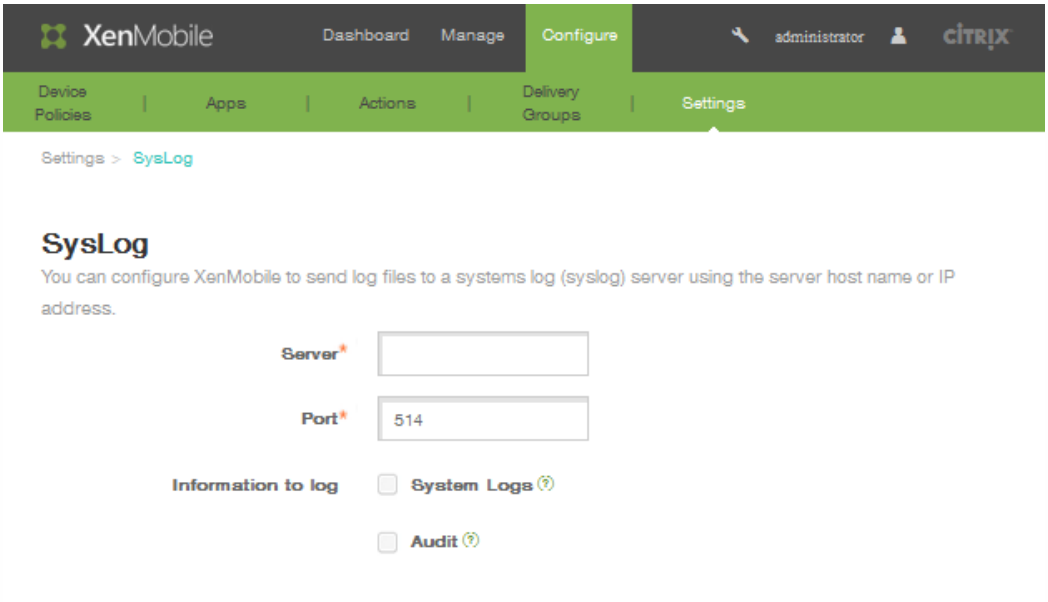
- IP-Adresse des Geräts, das die Protokollmeldung generiert hat
- Zeitstempel
- Meldungstyp
- Dringlichkeitsstufe des Ereignisses (Critical, Error, Notice, Warning, Informational, Debug, Alert, or Emergency)
- Meldungstext

Sie können anhand dieser Informationen die Ursache einer Warnung analysieren und ggf. Maßnahmen ergreifen.

> ## Hinweis
>
> Für XenMobile-Cloudbereitstellungen unterstützt Citrix keine Syslog-Integration mit einem lokalen Systemprotokollserver. Sie können die Protokolle von der Supportseite in der XenMobile-Konsole herunterladen. Klicken Sie zum Abrufen der Systemprotokolle auf "Download All". Weitere Informationen finden Sie unter Anzeigen und Analysieren von Protokolldateien in XenMobile.

So konfigurieren Sie einen Systemprotokollserver in XenMobile

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



2. Geben Sie für Name die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des syslog-Servers ein.
3. Geben Sie unter Port die Portnummer ein. In der Standardeinstellung ist dieser Port auf 514 eingestellt.
4. Aktivieren oder deaktivieren Sie nach Bedarf unter Information to log die Optionen System Logs und Audit.
   - Systemprotokolle, die Aktionen von XenMobile enthalten
   - Überwachungsprotokolle, die eine chronologische Auflistung der Systemaktivitäten im Zusammenhang mit XenMobile enthalten
5. Klicken Sie auf **Speichern**.

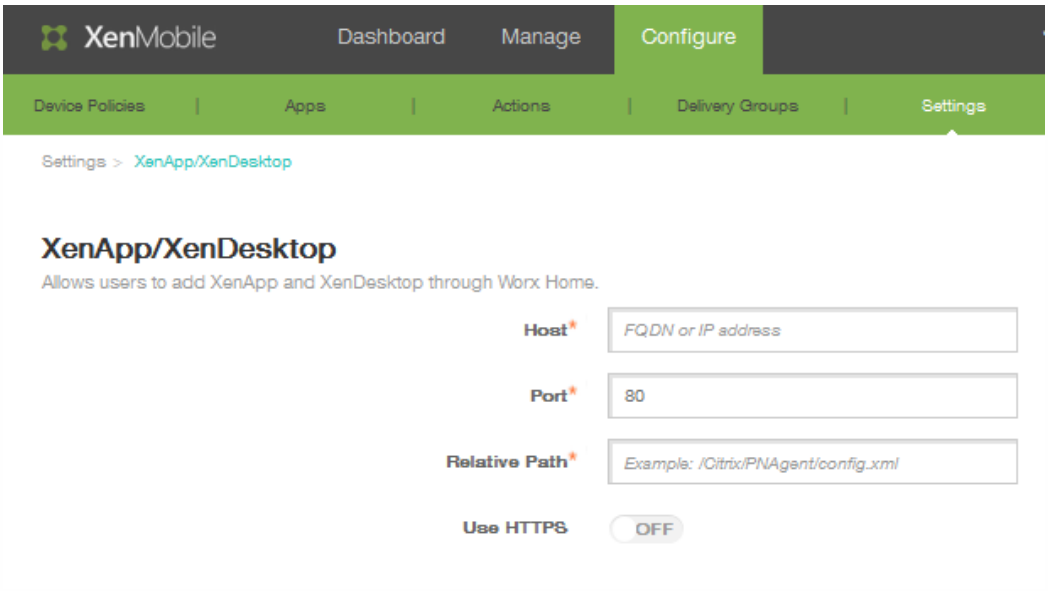
So konfigurieren Sie XenApp und XenDesktop

May 05, 2016

XenMobile kann Apps aus XenApp und XenDesktop sammeln und Benutzern von Mobilgeräten im Worx Store zur Verfügung stellen. Die Benutzer abonnieren Apps direkt im Worx Store und starten sie über Worx Home. Receiver muss zum Starten der Apps auf den Geräten der Benutzer installiert, jedoch nicht konfiguriert sein.

Zum Konfigurieren dieser Einstellung benötigen Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse und die Portnummer von StoreFront oder der Webinterface-Site.

1. Klicken Sie in der XenMobile-Konsole auf **Configure > Settings > More > XenApp/XenDesktop**.
   Die Seite XenApp/XenDesktop wird angezeigt.



2. Geben Sie für Host den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse von StoreFront oder der Webinterface-Site ein.
3. Geben Sie für Port die Portnummer von StoreFront oder der Webinterface-Site ein. Der Standardwert ist 80.
4. Geben Sie unter Relative Path den Pfad ein. Beispiel: /Citrix/Store/PNAgent/config.xml
5. Wählen Sie für Use HTTPS die Einstellung ON, um die sichere Authentifizierung zwischen StoreFront oder der Webinterface-Site und dem Clientgerät zu aktivieren. Der Standardwert ist OFF.
6. Klicken Sie auf **Save**.

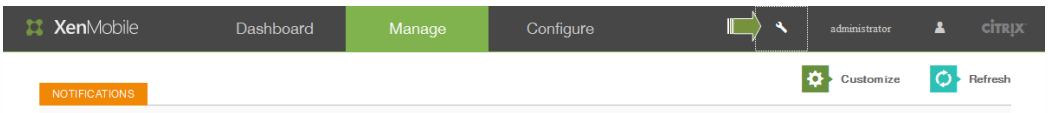
Support und Wartung von XenMobile

Oct 13, 2016

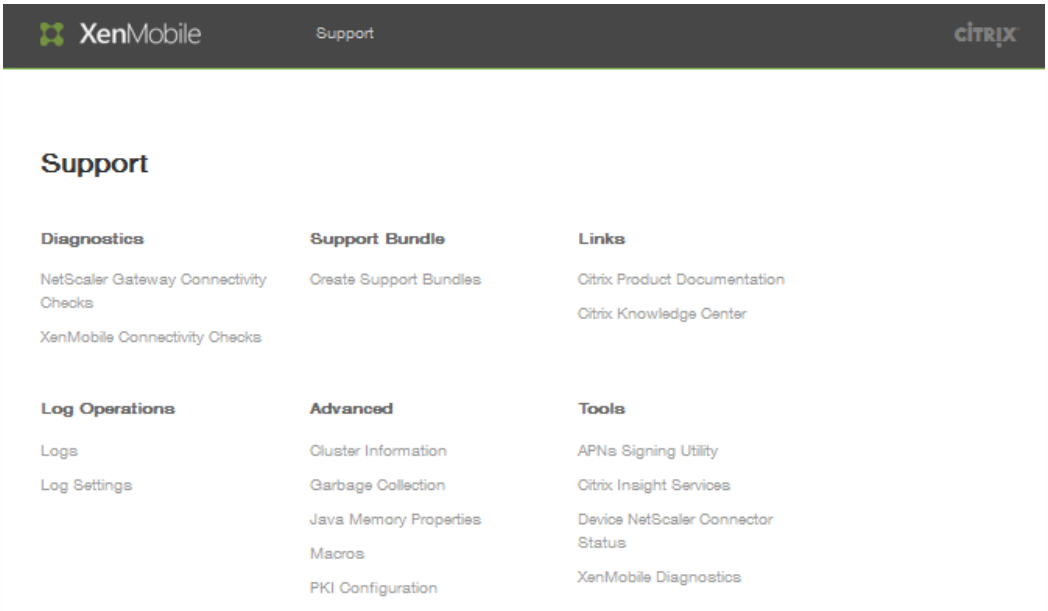
Verwenden Sie die Seite "XenMobile Support" für den Zugriff auf eine Reihe von Supportinformationen und -tools. Sie können Vorgänge auch über die Befehlszeilenschnittstelle ausführen. Einzelheiten finden Sie unter Optionen für die XenMobile-Befehlszeilenschnittstelle.

So greifen Sie auf die Supportseite zu

Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben.



Die Seite Support wird in einer neuen Browserregisterkarte geöffnet:



Verwenden Sie die Seite XenMobile-Support für Folgendes:

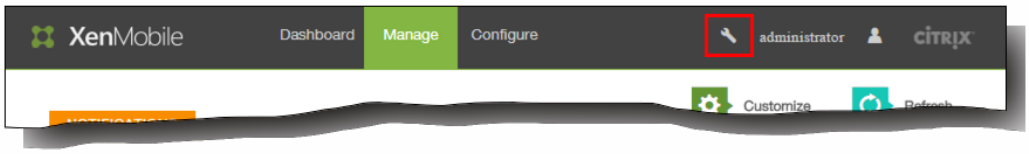
- Diagnose
- Erstellen von Supportpaketen
- Zugriff auf Links zur Citrix Produktdokumentation und Knowledge Center
- Zugriff auf Protokollvorgänge
- Auswahl aus einer Reihe erweiterter Informationen und Konfigurationsoptionen
- Zugriff auf diverse Tools und Hilfsprogramme

Durchführen von Verbindungsüberprüfungen

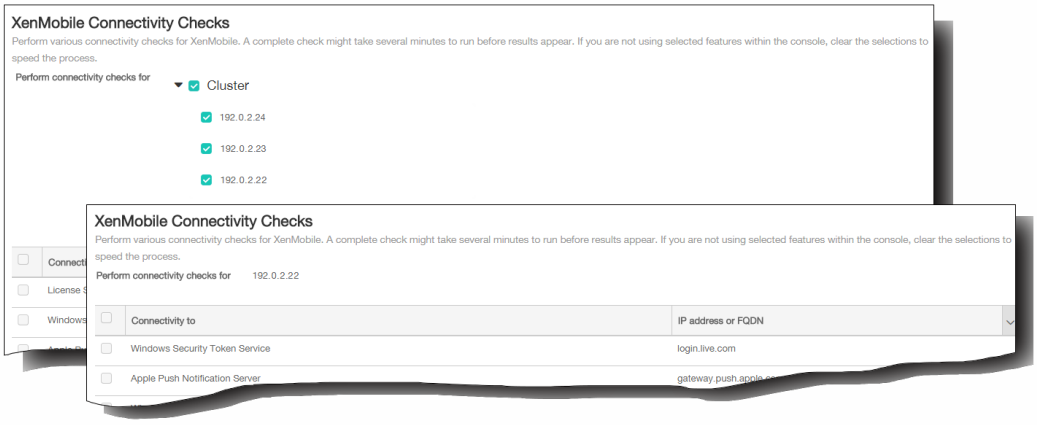
May 05, 2016

Über die Seite "XenMobile Support" können Sie die Verbindung zwischen XenMobile und NetScaler Gateway sowie anderen Servern und Speicherorten prüfen. Zum Aufrufen der Supportseite führen Sie die folgenden Schritte aus:

1. Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben. Das Schraubenschlüsselsymbol steht auf allen Seiten der XenMobile-Konsole zur Verfügung. Sie werden u. U. aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben.



Die neue Browserregisterkarte "XenMobile Support" wird geöffnet. Wenn die XenMobile-Umgebung Clusterknoten enthält, werden alle Knoten angezeigt.



Prüfen von XenMobile-Verbindungen

1. Klicken Sie auf der Seite Support auf XenMobile Connectivity Checks. Die Seite XenMobile Connectivity Checks wird angezeigt.
2. Wählen Sie die Server aus, deren Verbindung geprüft werden soll, und klicken Sie dann auf Test Connectivity. Die Ergebnisse werden angezeigt.
3. Wählen Sie einen Server in der Tabelle Test Results aus, um detaillierte Ergebnisse für ihn anzuzeigen.

Prüfen von NetScaler Gateway-Verbindungen

1. Klicken Sie auf der Seite Support auf NetScaler Gateway Connectivity Checks. Die Seite NetScaler Gateway Connectivity Checks wird angezeigt.
2. Klicken Sie auf Add. Das Dialogfeld Add NetScaler Gateway Server wird angezeigt.
3. Geben Sie unter NetScaler Gateway Management IP die IP-Adresse des Servers mit NetScaler Gateway ein, den Sie testen möchten.

Hinweis: Wenn Sie einen NetScaler Gateway-Server prüfen, der bereits hinzugefügt wurde, wird die IP-Adresse bereitgestellt.

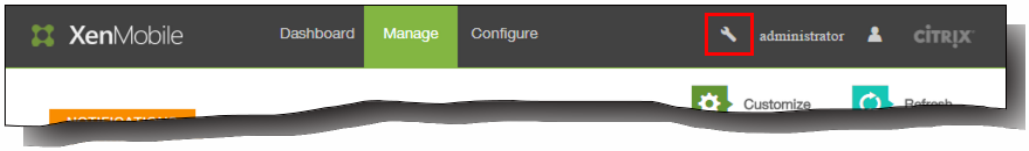
4. Geben Sie die Administratoranmeldeinformationen für das NetScaler Gateway ein.
   Hinweis: Wenn Sie einen NetScaler Gateway-Server prüfen, der bereits hinzugefügt wurde, wird der Benutzername bereitgestellt.
5. Klicken Sie auf Add. Das NetScaler Gateway wird der Tabelle auf der Seite NetScaler Gateway Connectivity Checks hinzugefügt.
6. Klicken Sie auf Test Connectivity. Das Ergebnis wird in der Tabelle Test Results angezeigt.
7. Wählen Sie einen Server in der Tabelle Test Results aus, um detaillierte Ergebnisse für ihn anzuzeigen.

Erstellen von Supportpaketen in XenMobile

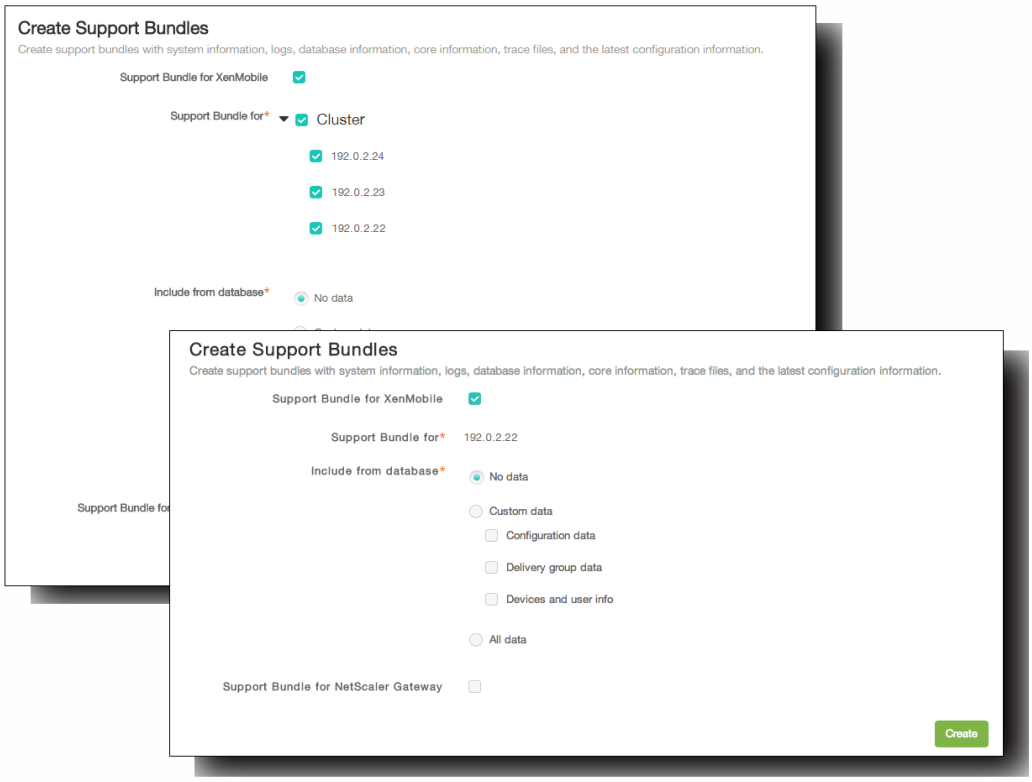
May 05, 2016

Wenn Sie ein Problem an Citrix melden oder beheben möchten, erstellen Sie ein Supportpaket und laden dieses an Citrix Insight Services (CIS) hoch.

1. Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben. Das Schraubenschlüsselsymbol steht auf allen Seiten der XenMobile-Konsole zur Verfügung.
   Hinweis: Sie werden u. U. aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben.



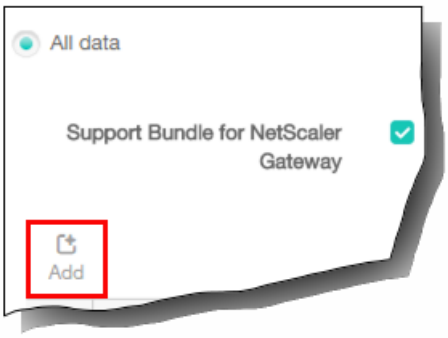
   XenMobile Support wird in einer neuen Browserregisterkarte geöffnet.
2. Klicken Sie auf der Seite Support auf Create Support Bundles. Die Seite Create Support Bundles wird angezeigt. Wenn die XenMobile-Umgebung Clusterknoten enthält, werden alle Knoten angezeigt.



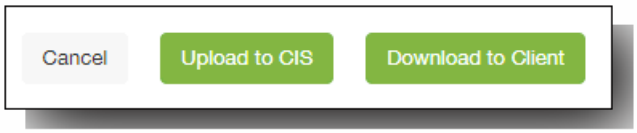
3. Stellen Sie sicher, dass das Kontrollkästchen Support Bundle for XenMobile aktiviert ist.
4. Wenn die XenMobile-Umgebung Clusterknoten enthält, können Sie unter Support Bundle for beliebige oder alle Knoten für die Datensammlung auswählen.
5. Führen Sie unter Include from Database einen der folgenden Schritte aus:

- Klicken Sie auf No data.
- Klicken Sie auf Custom data und wählen Sie nach Bedarf die gewünschten Daten aus:
  - Configuration data: Zertifikatkonfigurationen und Device Manager-Richtlinien.
  - Delivery group data: Informationen zu App-Bereitstellungsgruppen mit App-Typen und Details zur App-Bereitstellungsrichtlinie.
  - Devices and user info: Geräterichtlinien, Apps, Aktionen und Bereitstellungsgruppen.
- Klicken Sie auf All data.

6. Wählen Sie Support Bundle for NetScaler Gateway, wenn Sie Supportpakete von NetScaler Gateway einschließen möchten, und führen Sie die folgenden Schritte aus:
   1. Klicken Sie auf Add.



   Das Dialogfeld Add NetScaler Gateway Server wird angezeigt.
   2. Geben Sie unter NetScaler Gateway Management IP die NetScaler-Verwaltungs-IP-Adresse für das NetScaler Gateway ein, von dem Sie das Supportpaket beziehen möchten.
   Hinweis: Wenn Sie ein Paket von einem NetScaler Gateway-Server erstellen, der bereits hinzugefügt wurde, wird die IP-Adresse bereitgestellt.
   3. Geben Sie unter User name und Password die Anmeldeinformationen für den Zugriff auf den Server ein, auf dem das NetScaler Gateway ausgeführt wird.
   Hinweis: Wenn Sie ein Paket von einem NetScaler Gateway-Server erstellen, der bereits hinzugefügt wurde, wird der Benutzername bereitgestellt.
   4. Klicken Sie auf Add. Das neue NetScaler Gateway-Supportpaket wird der Tabelle hinzugefügt.
   5. Wiederholen Sie Schritt 6 zum Hinzufügen weiterer NetScaler Gateway-Supportpakete nach Bedarf.
7. Klicken Sie auf Create. Das Supportpaket wird erstellt und zwei neue Schaltfläche werden angezeigt: Upload to CIS und Download to Client.

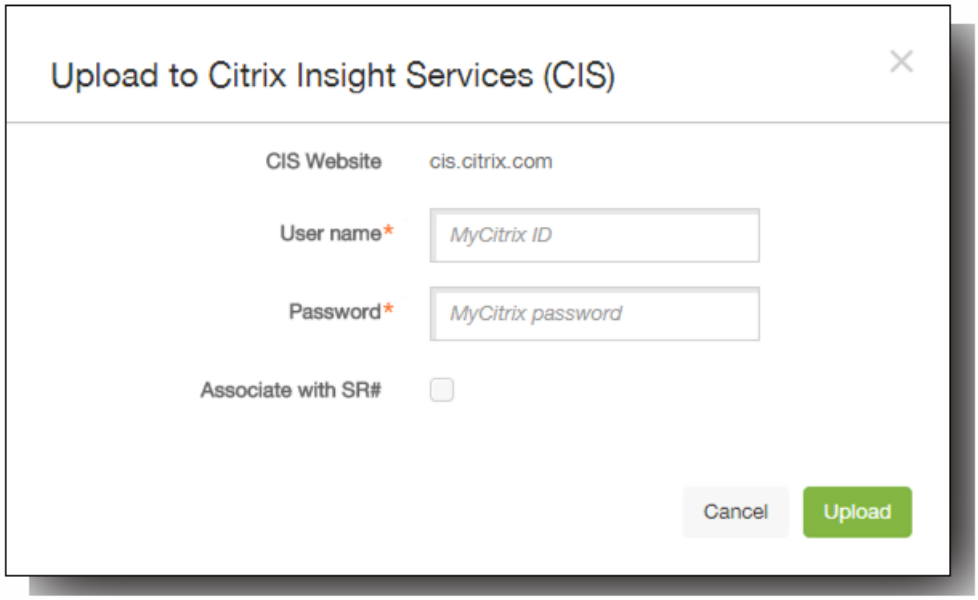


Fahren Sie mit den Schritten unter **Hochladen von Supportpaketen in Citrix Insight Services** bzw. **Herunterladen von Supportpaketen auf einen Client** fort.

Hochladen von Supportpaketen an Citrix Insight Services

Nach dem Erstellen eines Supportpakets können Sie das Paket an Citrix Insight Services (CIS) hochladen oder auf Ihren Computer herunterladen. Hier wird erläutert, wie Sie das Paket in CIS hochladen.

1. Klicken Sie auf der Seite Create Support Bundles auf Upload to CIS. Das Dialogfeld Upload to Citrix Insight Services (CIS) wird angezeigt.



2. Geben Sie unter User Name Ihre MyCitrix-ID ein.
3. Geben Sie unter Password Ihr MyCitrix-Kennwort ein.
4. Wenn Sie das Paket mit einer vorhandenen Dienstanforderung verbinden möchten, wählen Sie das Kontrollkästchen Associate with SR# aus und geben Sie in die beiden neu angezeigten Felder Folgendes ein:
   1. Geben Sie unter SR# die achtstellige Dienstanforderungsnummer ein, der Sie das Paket zuordnen möchten.
   2. Geben Sie unter SR Description eine Beschreibung der Dienstanforderung ein.
5. Klicken Sie auf Upload. Das Supportpaket wird an CIS hochgeladen.

Herunterladen von Supportpaketen auf einen Client

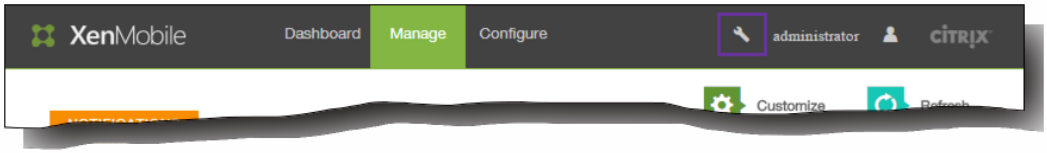
Nach dem Erstellen eines Supportpakets können Sie das Paket an CIS hochladen oder auf Ihren Computer herunterladen. Wenn Sie ein Problem allein behandeln möchten, laden Sie das Supportpaket auf Ihrem Computer herunter.
Klicken Sie auf der Seite Create Support Bundles auf Download to Client. Das Paket wird auf Ihren Computer heruntergeladen.

So zeigen Sie die Debugprotokolldatei an

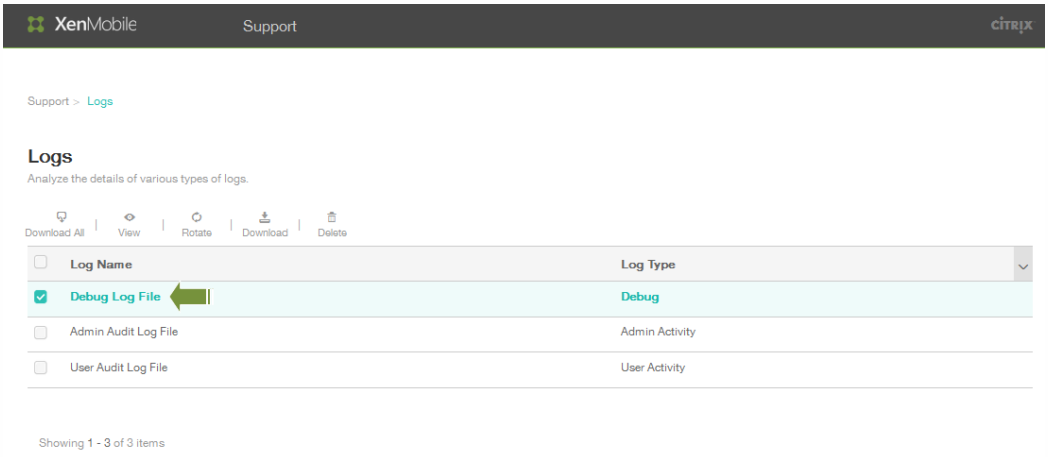
May 05, 2016

Wenn Sie ein Problem an Citrix melden oder beheben möchten, erstellen Sie ein Supportpaket und laden dieses an Citrix Insight Services (CIS) hoch.

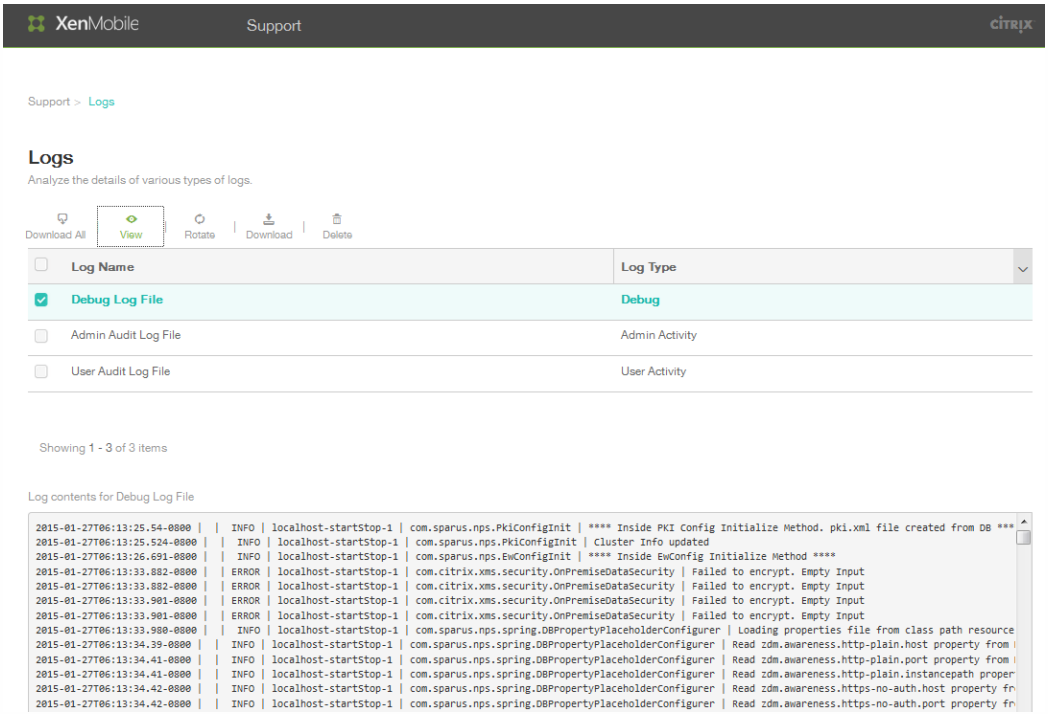
1. Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben. Das Schraubenschlüsselsymbol steht auf allen Seiten der XenMobile-Konsole zur Verfügung.



2. Klicken Sie auf der Seite Support auf Logs. Die Seite Logs wird angezeigt.



3. Wählen Sie Debug Log File aus und klicken Sie auf View, um den Inhalt des Protokolls anzuzeigen.



Nach Analyse der Protokolldatei verwenden Sie die Option Download File zum Speichern der Daten oder klicken Sie auf Delete, um den Inhalt des Protokolls aus der Datenbank zu löschen.

So konfigurieren Sie die Einstellungen für Protokolle

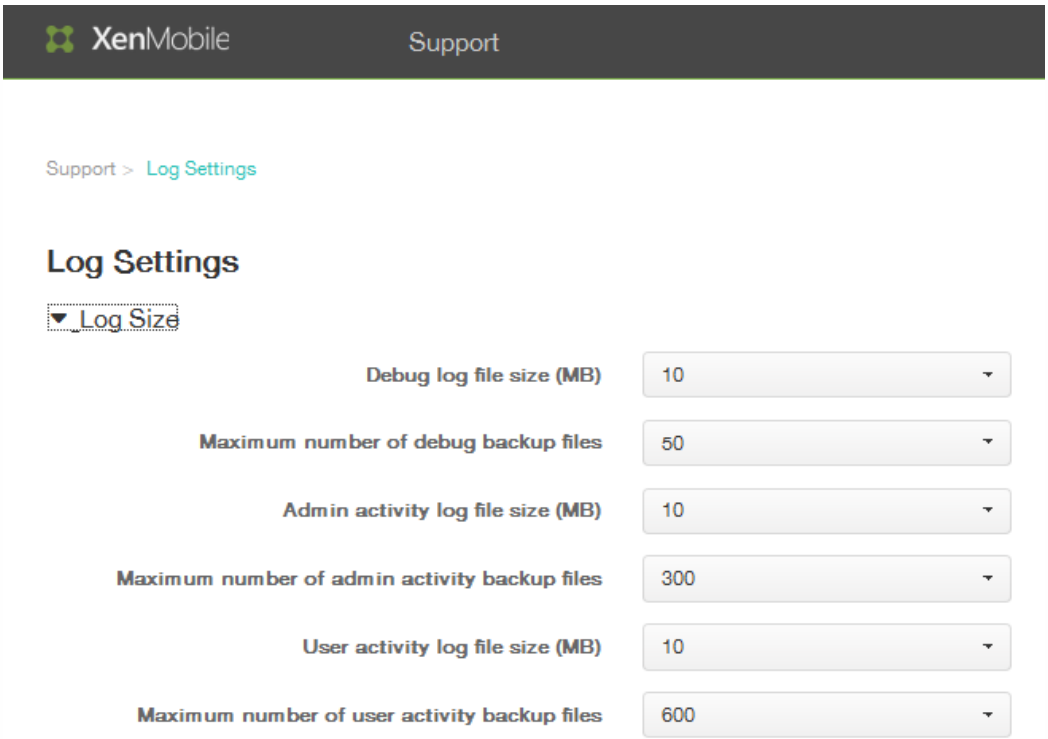
May 05, 2016

Sie können Protokolleinstellungen konfigurieren, um die Ausgabe der von XenMobile generierten Protokolle anzupassen. Klicken Sie in der XenMobile-Konsole auf Support > Log Settings für den Zugriff auf die folgenden Optionen:

- Log Size: Verwenden Sie diese Option, um die Größe der Protokolldatei und die maximale Anzahl der Sicherungsdateien der Protokolldatei in der Datenbank zu steuern. Der Größenwert gilt für jedes von XenMobile unterstützte Protokoll (Debugprotokoll, Administratoraktivitätsprotokoll und Benutzeraktivitätsprotokoll).
- Log Level: Mit dieser Option ändern Sie den Klassennamen, den Unterklassennamen, die Protokollebene und die Dauerhaftigkeit der Einstellungen.
- Customer Logger: Verwenden Sie diese Option zum Erstellen einer benutzerdefinierten Protokollierung. Benutzerdefinierte Protokolle erfordern einen Klassennamen und eine Protokollebene.

So konfigurieren Sie die Protokollgrößenoptionen

1. Klicken Sie auf Support > Log Settings und erweitern Sie Log Size.



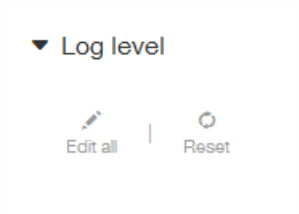
2. Wählen Sie in der Liste Debug log file size (MB) eine Größe zwischen 5 und 20 MB aus, um die maximale Größe der Debugdatei zu ändern. Standardmäßig ist die Größe der Datei auf 10 MB festgelegt.
3. Wählen Sie in der Liste Maximum number of debug backup files aus, wie viele Sicherungskopien der Debugdatei maximal auf dem Server gespeichert werden sollen (5-300). Standardmäßig werden von XenMobile 50 Sicherungsdateien auf dem Server gespeichert.
4. Wählen Sie in der Liste Admin activity log eine Größe zwischen 5 und 20 MB aus. Standardmäßig ist die Größe der Datei auf 10 MB festgelegt.
5. Wählen Sie in der Liste Maximum number of admin backup files aus, wie viele Sicherungskopien der Administratoraktivitätsprotokolldatei maximal auf dem Server gespeichert werden sollen (5-300). Standardmäßig werden

von XenMobile 300 Sicherungsdateien auf dem Server gespeichert.

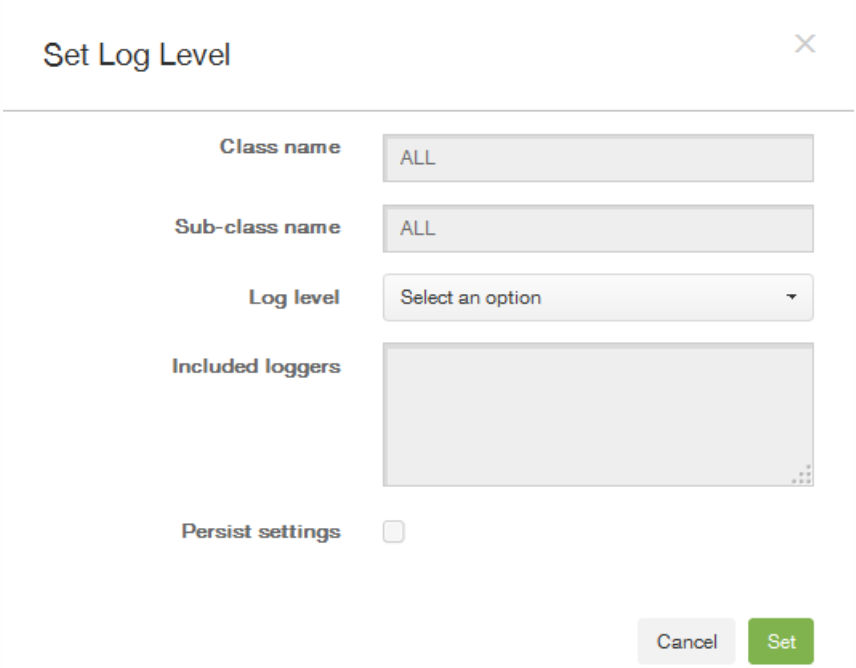
6. Wählen Sie in der Liste User activity log eine Größe zwischen 5 und 20 MB aus. Standardmäßig ist die Größe der Datei auf 10 MB festgelegt.
7. Wählen Sie in der Liste Maximum number of admin backup files aus, wie viele Sicherungskopien der Administratoraktivitätsprotokollddatei maximal auf dem Server gespeichert werden sollen (5-300). Standardmäßig werden von XenMobile 300 Sicherungsdateien auf dem Server gespeichert.

So konfigurieren Sie die Protokollebene

1. Klicken Sie auf Support > Log Settings und erweitern Sie Log level, um die Konfigurationsoptionen anzuzeigen. Klicken Sie auf Edit all, um die Elemente der Protokollebene zu konfigurieren.



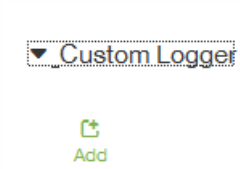
Das Dialogfeld Set Log Level wird angezeigt.



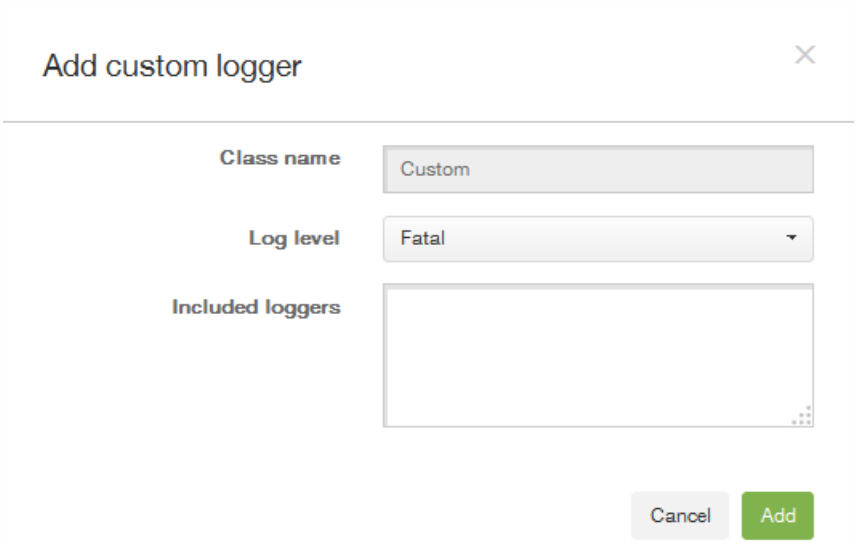
2. Geben Sie für Class Name einen Klassennamen ein. Standardeinstellung für dieses Feld ist All.
3. Geben Sie für Sub-class name einen Unterklassennamen ein. Standardeinstellung für dieses Feld ist All.
4. Wählen Sie in der Liste Log level die Protokollebene aus. Es stehen die Stufen Fatal, Error, Warning, Info, Debug, Trace und Off zur Auswahl. Im Feld Included Loggers wird die konfigurierte Protokollebene für jede konfigurierte Klasse angezeigt.
5. Wenn Sie die Protokollebeneneinstellungen beibehalten möchten, klicken Sie auf das Kontrollkästchen Persist settings.
6. Klicken Sie auf Set, um die Änderungen zu übergeben.

So fügen Sie eine benutzerdefinierte Protokollierung hinzu

1. Zum Hinzufügen einer benutzerdefinierten Protokollierung klicken Sie für Custom Logger auf Add.



Das Dialogfeld Add custom logger wird angezeigt.

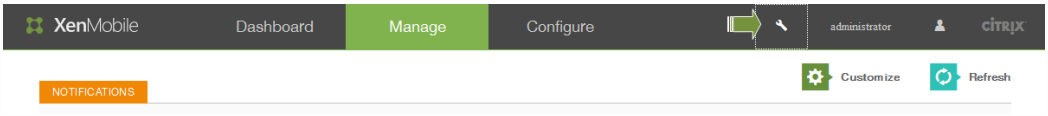


2. Geben Sie für Class name einen Klassennamen ein.
3. Wählen Sie in der Liste Log level die Protokollebene aus. Es stehen die Stufen Fatal, Error, Warning, Info, Debug, Trace und Off zur Auswahl. Im Feld Included Loggers wird die konfigurierte Protokollebene für jede konfigurierte Klasse angezeigt.
4. Klicken Sie auf Add.

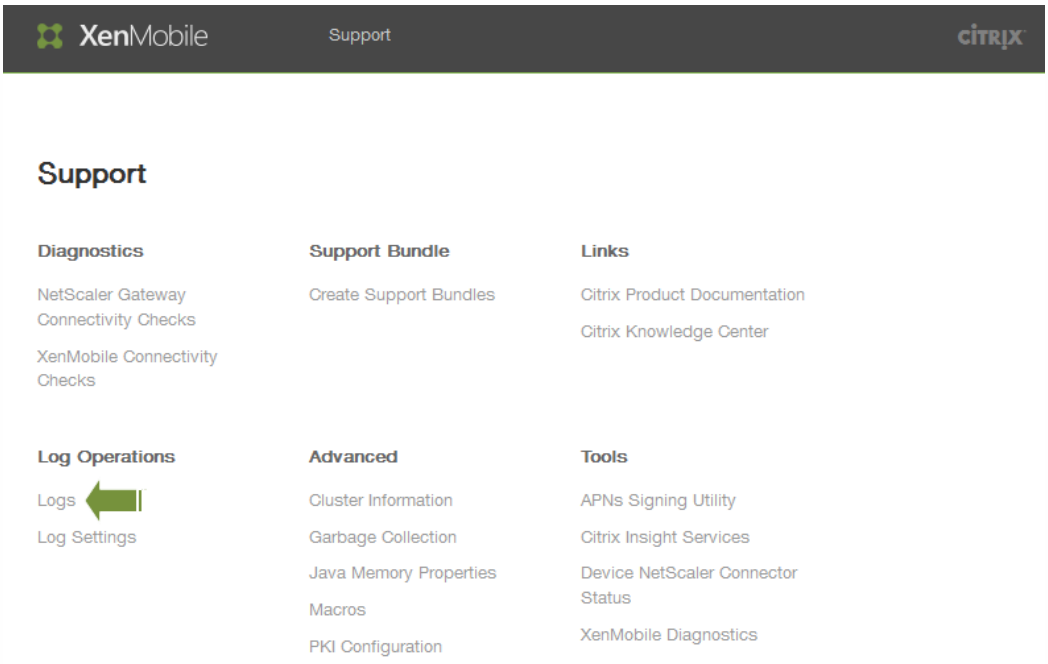
Anzeigen und Analysieren von Protokolldateien in XenMobile

May 05, 2016

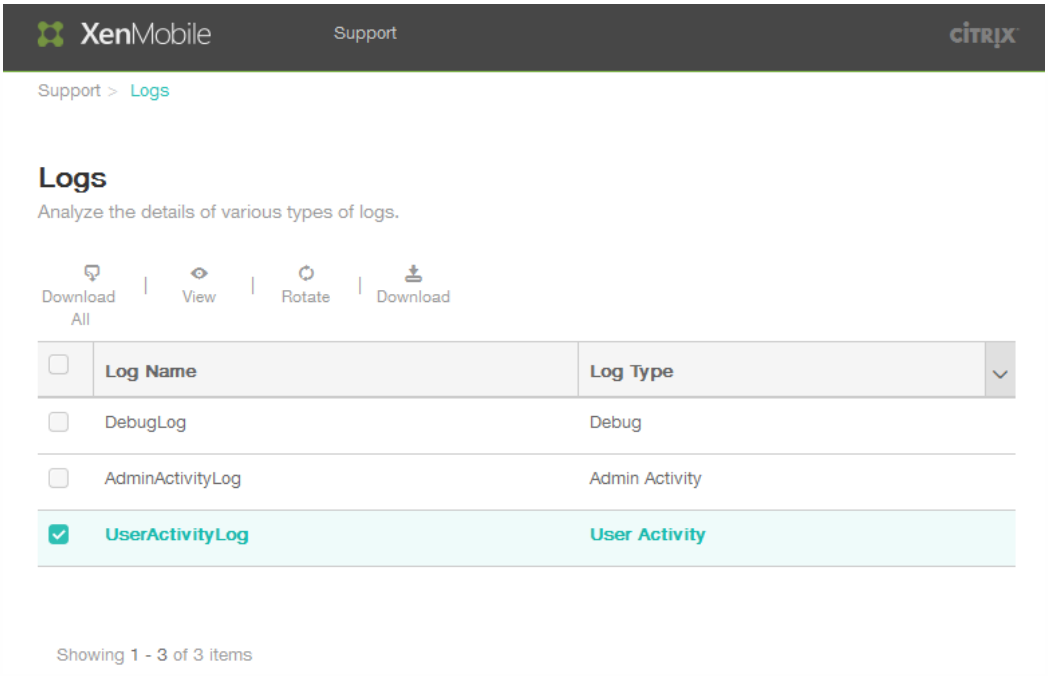
1. Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben. Die Seite Support wird in einem neuen Browserfenster geöffnet.



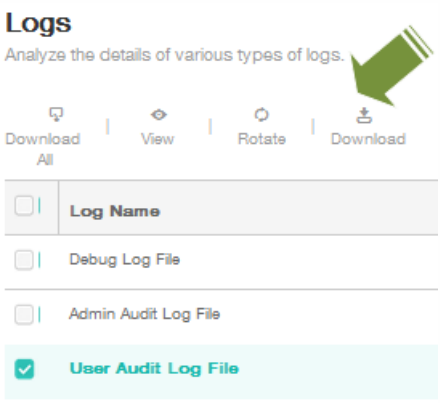
2. Klicken Sie unter Log Operations auf **Logs**. Die Seite **Logs** wird angezeigt. Einzelne Protokolle werden in einer Tabelle angezeigt.



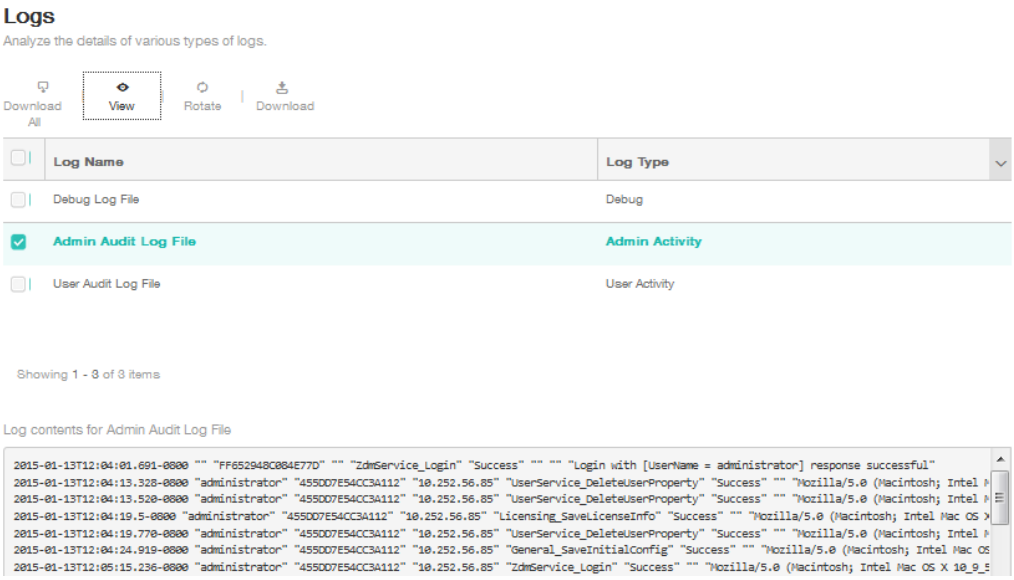
3. Wählen Sie das Protokoll aus, das Sie anzeigen möchten. Ein Debugprotokoll enthält nützliche Informationen für den Citrix Support, z. B. Fehlermeldungen und serverbezogene Aktionen. Benutzeraktivitätsprotokolle enthalten Informationen über die einzelnen konfigurierten Benutzer. Die Seite **Logs** wird angezeigt. Einzelne Protokolle werden in einer Tabelle angezeigt.



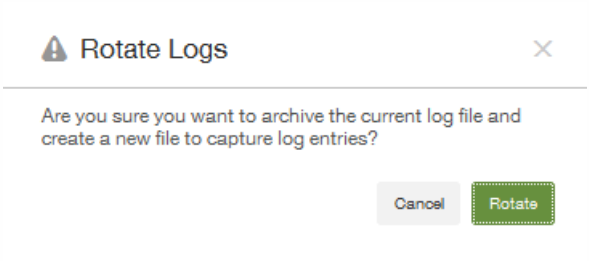
4. Am Tabellenanfang stehen folgende Aktionen zur Verfügung:
   - Download All: Es werden alle Protokolle im System (Debug-, Benutzeraktivitäts-/Administratoraktivitäts-, Serverprotokolle usw.) heruntergeladen. Mit Download können Sie ausgewählte Protokolle speichern; es werden auch archivierte Protokolle heruntergeladen.



   - View: zeigt den Inhalt des Protokolls unterhalb der Tabelle an.



- Delete: löscht das ausgewählte Protokolldatei dauerhaft.
- Rotate: Archiviert die aktuelle Protokolldatei und erstellt eine neue Datei zum Erfassen von Einträgen. Ein Dialogfeld wird angezeigt, wenn eine Protokolldatei archiviert wird. Klicken Sie auf Rotate, um fortzufahren.



Optionen für die XenMobile-Befehlszeilenschnittstelle

May 05, 2016

Sie haben jederzeit Zugriff auf die nachfolgend aufgeführten Optionen für die Befehlszeilenschnittstelle (CLI) auf dem Hypervisor, auf dem Sie XenMobile installiert haben (Citrix XenServer, Microsoft Hyper-V oder VMware ESXi).

Die folgenden Optionen stehen im Hauptmenü und den ersten vier Untermenüs (Configuration, Clustering, System und Troubleshooting) zur Verfügung.

Hauptmenü

```
------------------------------

[0] Configuration

[1] Clustering

[2] System

[3] Troubleshooting

[4] Help

[5] Log Out

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

Choice: [0 - 5]
```

Optionen des Menüs "Configuration"

Wenn Sie im Hauptmenü "Configuration" auswählen, werden folgende Optionen angezeigt:

```
[0] Back to Main Menu

[1] Network

[2] Firewall

[3] Database

[4] Listener Ports

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

Choice: [0 - 4]

------------------------------
```

Bei Auswahl der Option "Network" werden Sie zum Durchführen eines Neustarts und zum Speichern der Änderungen aufgefordert.

Wenn Sie "Firewall" auswählen, werden folgende Aufforderungen zur Konfiguration angezeigt:

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]:

Wenn Sie "Database" auswählen, werden folgende Aufforderungen zur Konfiguration angezeigt:

Type: [mi]

Use SSL (y/n) [y]:

Upload Root Certificate (y/n) [y]:

Copy or Import (c/i) [c]:

Optionen des Menüs "Clustering"

Wenn Sie im Hauptmenü "Clustering" auswählen, werden folgende Optionen angezeigt:

[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]

Wenn Sie das Clustering aktivieren, wird die folgende Meldung angezeigt:

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.

Wenn Sie das Clustering nicht aktivieren, wird die folgende Meldung angezeigt:

You have chosen to disable clustering. Access to port 80 is not needed. Please disable it.

Wenn Sie Option [3], die Positivliste für Clustermitglieder auswählen und Clustering deaktiviert haben, wird die folgende Meldung angezeigt:

Cluster is disabled. Please enable it.

Wenn Clustering aktiviert ist, werden die folgenden Optionen angezeigt:

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:

Wenn Sie Option [4] zum Aktivieren oder Deaktivieren der SSL-Abladung auswählen, wird die folgende Meldung angezeigt:

Enabling SSL offload will open port 80 for everyone. Please configure Access white list under Firewall settings for restricted access.

Wenn Sie Option [5] zum Anzeigen der Hazelcast-Cluster auswählen, werden die folgenden Optionen angezeigt:

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"

Wenn Sie im Hauptmenü "System" auswählen, werden folgende Optionen angezeigt:

---

[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"

Wenn Sie im Hauptmenü "Troubleshooting" auswählen, werden folgende Optionen angezeigt:

---

[0] Back to Main Menu

[1] Network Utilities

[2] Logs

[3] Support Bundle

Choice: [0 - 3]

Wenn Sie die Option "Network Utilities" auswählen, werden folgende Optionen angezeigt:

---

[0] Back to Troubleshooting Menu

[1] Network Information

[2] Show Routing Table

[3] Show Address Resolution Protocol (ARP) Table

[4] PING

[5] Traceroute

[6] DNS Lookup

[7] Network Trace

Choice: [0 - 7]

Wenn Sie die Option "Logs" auswählen, werden folgende Optionen angezeigt:

Logs Menu

---

[0] Back to Troubleshooting Menu

[1] Display Log File

Choice: [0 - 1]

XenMobile 10-APIs

May 05, 2016

Sie können in XenMobile 10 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

WSDL-Name (Web Service Definition Language)	Aufruf
	getDeviceInfo
	getDeviceInformationForUser
	getDeviceProperties
	getLastUser
	getManagedStatus
	getMasterKeyList
	getSoftwareInventory
	getStrongID
	getUserDevices
	isEnforceSSL
	isEnforceStrongAuthentication
	locateDevice
	lockDevice
	putDeviceProperties
	registerDeviceForUser
	removeDevice
	resetDeploymentState
	revoke
	unlockDevice

WSDL-Name (Web Service Definition Language)	Aufruf
	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

May 05, 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.

Bekannte Probleme

- 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.

Behobene Probleme

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.

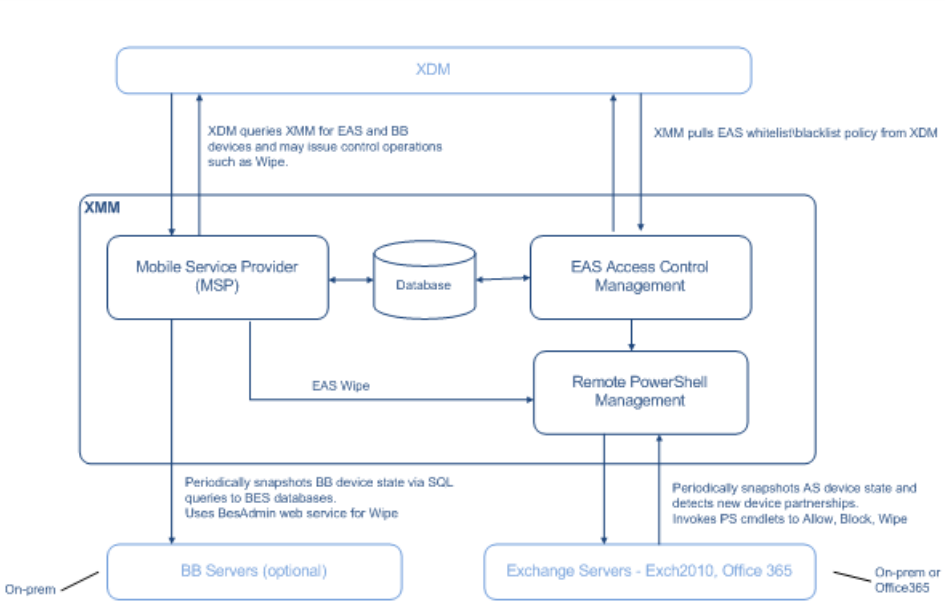
Protokollierung

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 13, 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

May 05, 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

Voraussetzungen für XenMobile Mail Manager

- 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

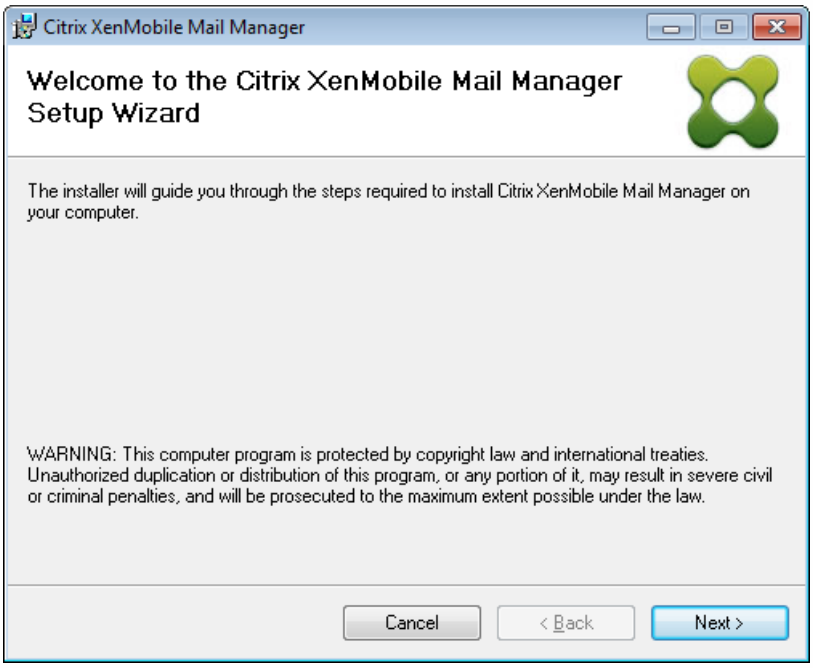
- **Berechtigungen**: Die rollenbasierte Zugriffssteuerung (RBAC) für Exchange geht über den Rahmen dieser Dokumentation hinaus. Prinzipiell muss das im Konfigurations-UI für Exchange festgelegte Konto in der Lage sein, eine Verbindung mit Office 365 herzustellen und vollständigen Zugriff zum Ausführen 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

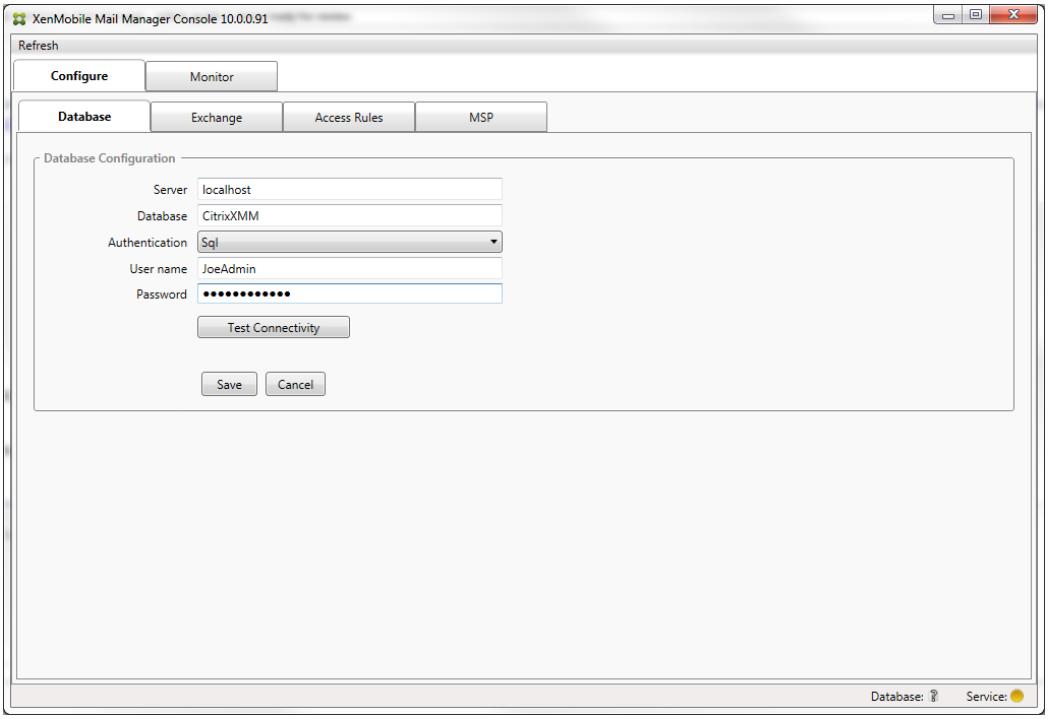
May 05, 2016

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.

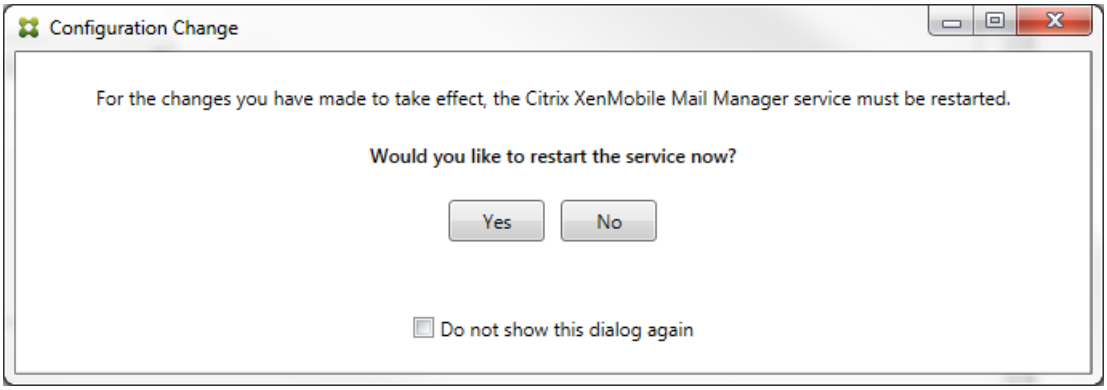


2. Öffnen Sie XenMobile Mail Manager über das Startmenü .
3. Konfigurieren Sie die folgenden Datenbankeigenschaften:
   1. Wählen Sie die Registerkarte Configure > Database.
   2. Geben Sie den Namen des SQL Server-Computers ein (standardmäßig "localhost").
   3. Behalten Sie den Standarddatenbanknamen "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.

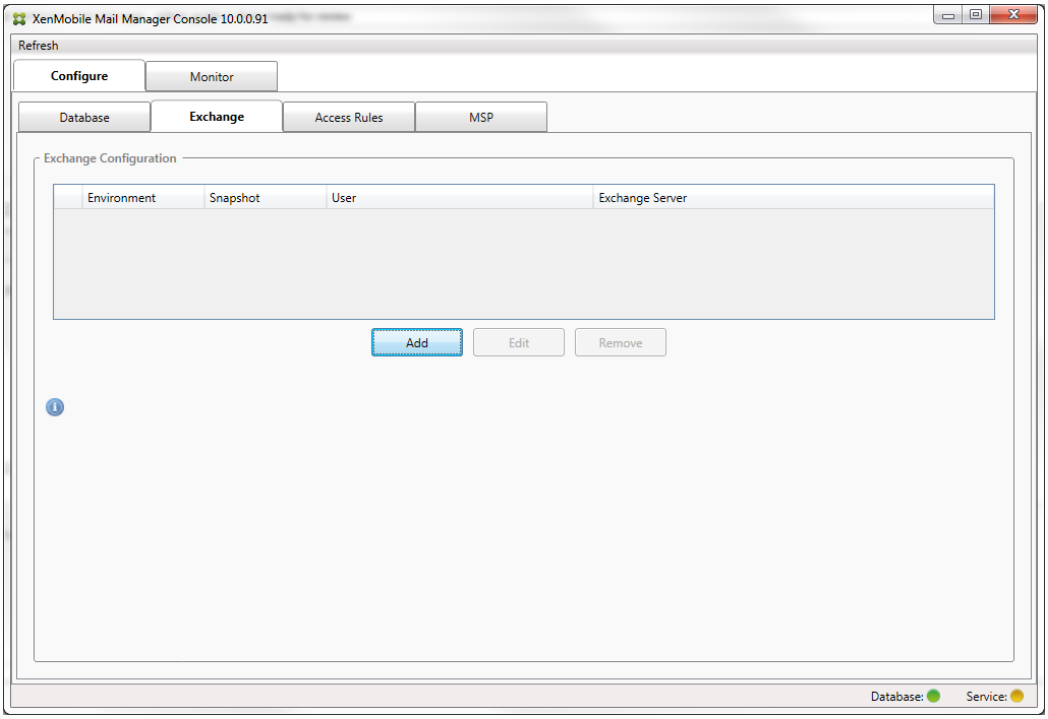


5. Klicken Sie auf Test Connectivity, um zu prüfen, ob eine Verbindung mit dem SQL Server-Computer hergestellt werden kann, und klicken Sie auf Save.

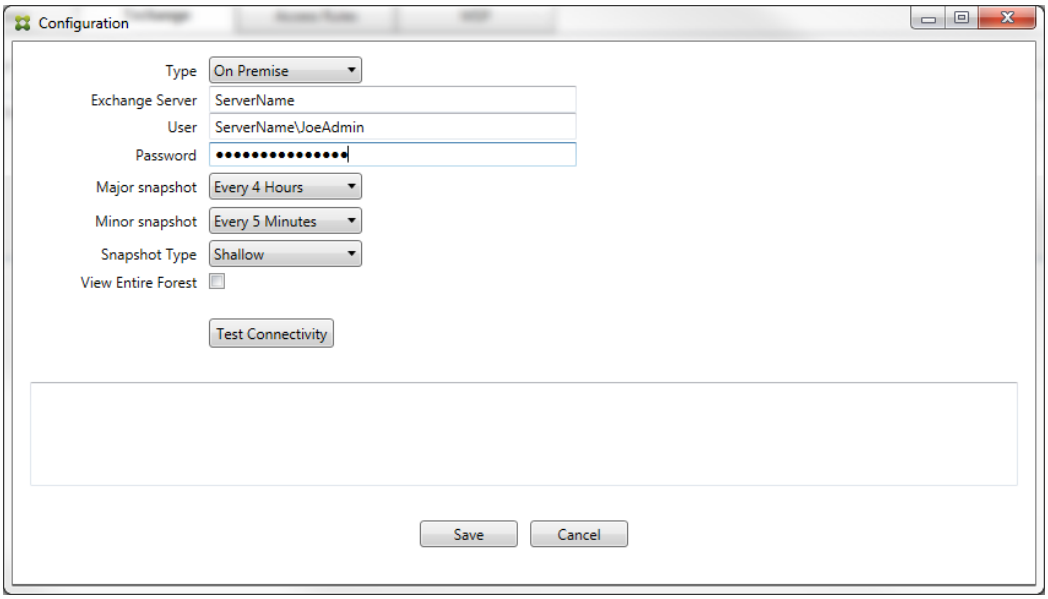
4. Eine Meldung fordert Sie zum Neustarten des Diensts auf. Klicken Sie auf Yes.



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.

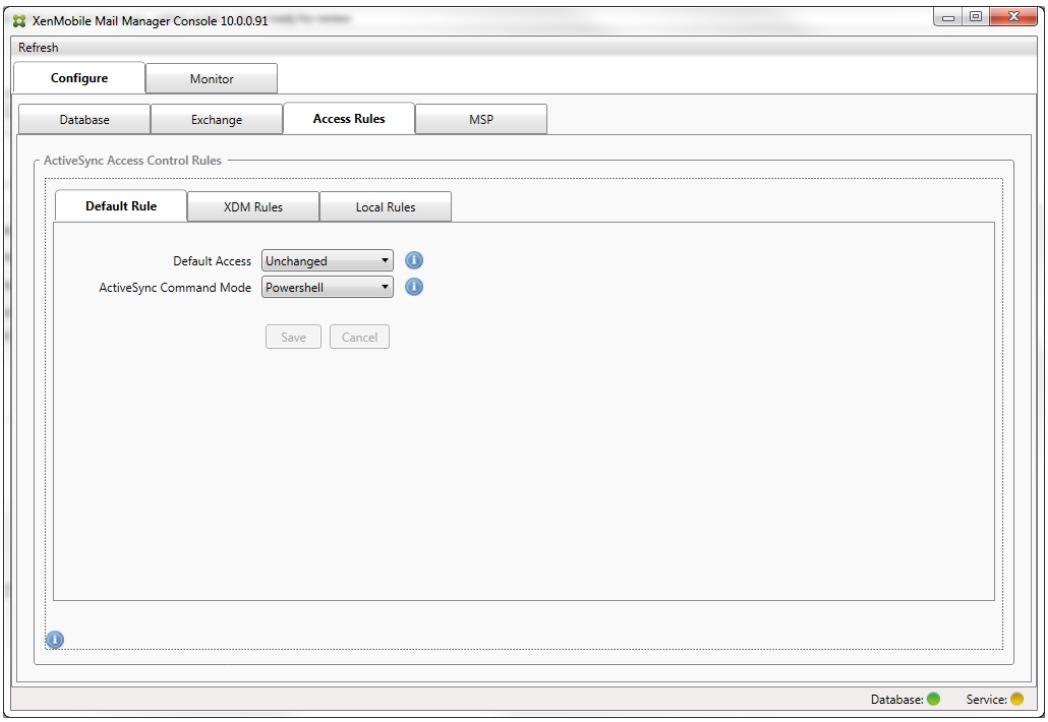


5. Wenn Sie On Premise auswählen, geben Sie den Namen des für Remote-PowerShell-Befehle verwendeten Exchange-Servers ein.
6. Geben Sie den Benutzernamen einer Windows-Identität ein, die die unter "Anforderungen" aufgeführten Berechtigungen auf dem Exchange Server-Computer hat.
7. Geben Sie für Password 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

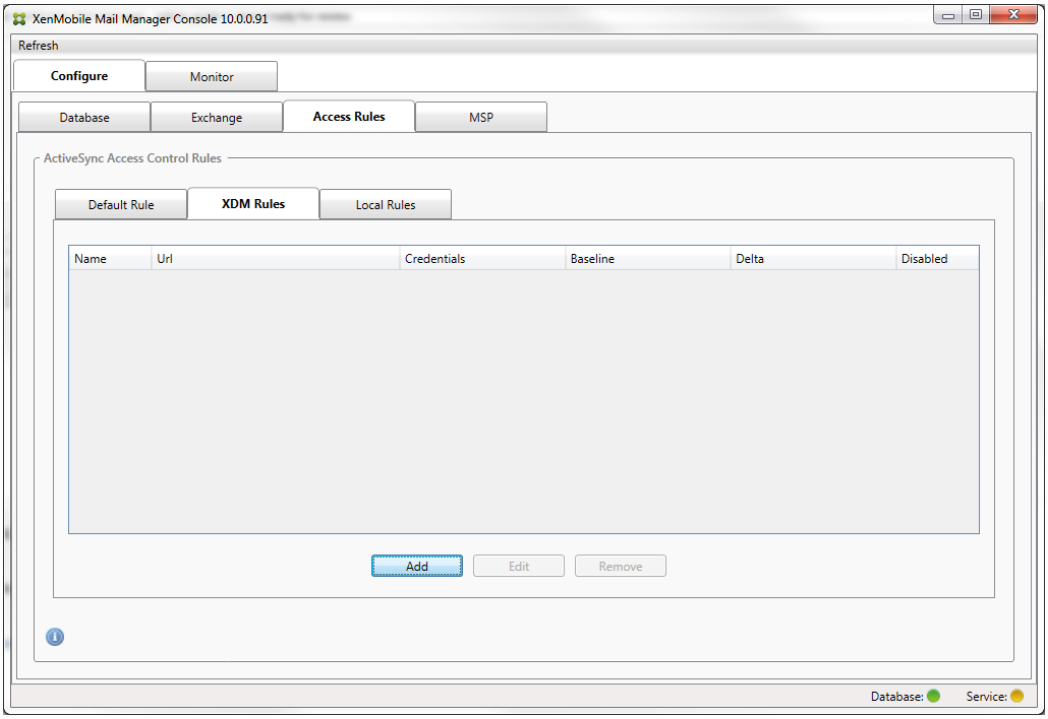
erstellt und reichen zur Ausführung aller Funktionen der Exchange ActiveSync-Zugriffssteuerung von XenMobile Mail Manager aus. Tiefe Snapshots (Deep) brauchen wesentlich länger und sind nur erforderlich, wenn Mobile Service Provider für ActiveSync aktiviert ist (dadurch kann XenMobile nicht verwaltete 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.

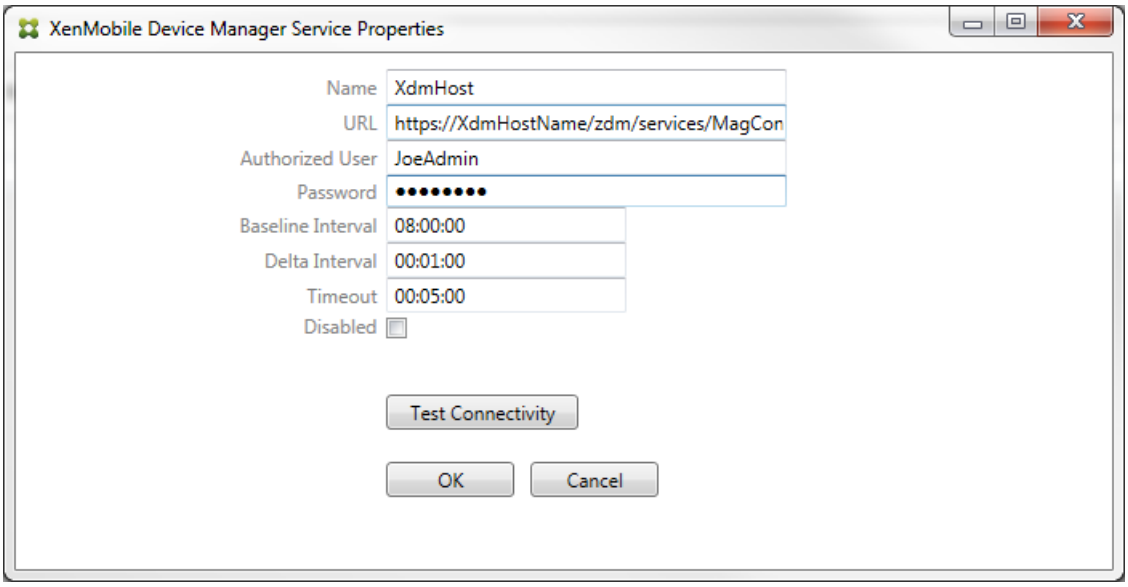
6. Konfigurieren Sie die Zugriffsregeln:
   1. Wählen Sie die Registerkarte Configure > Access Rules.



   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.



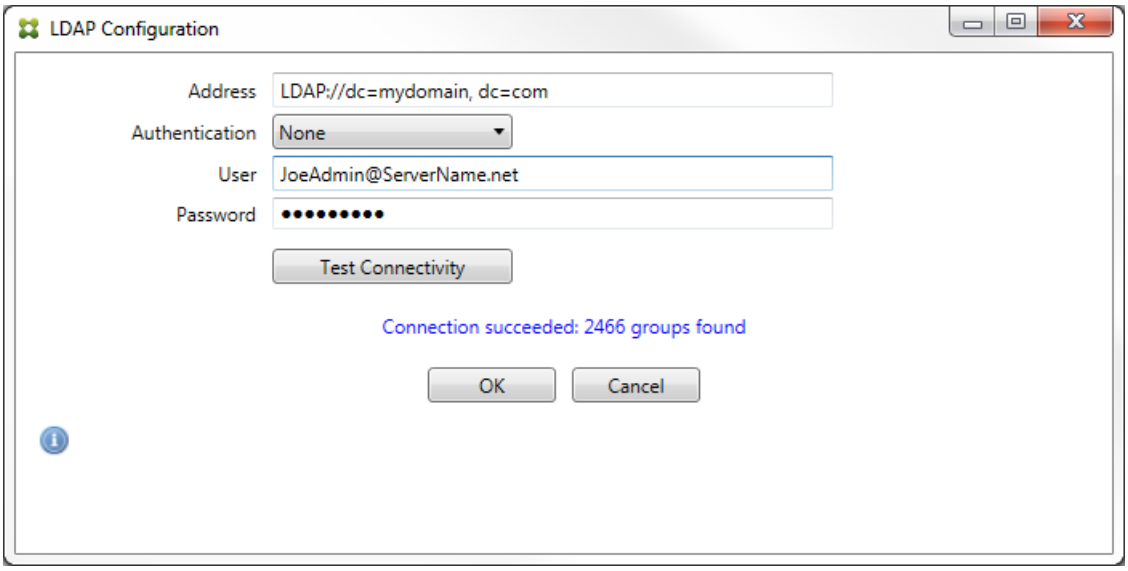
1. Klicken Sie auf Add.
2. Geben Sie einen Namen für die XDM-Regel ein, z. B. "XdmHost".



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.

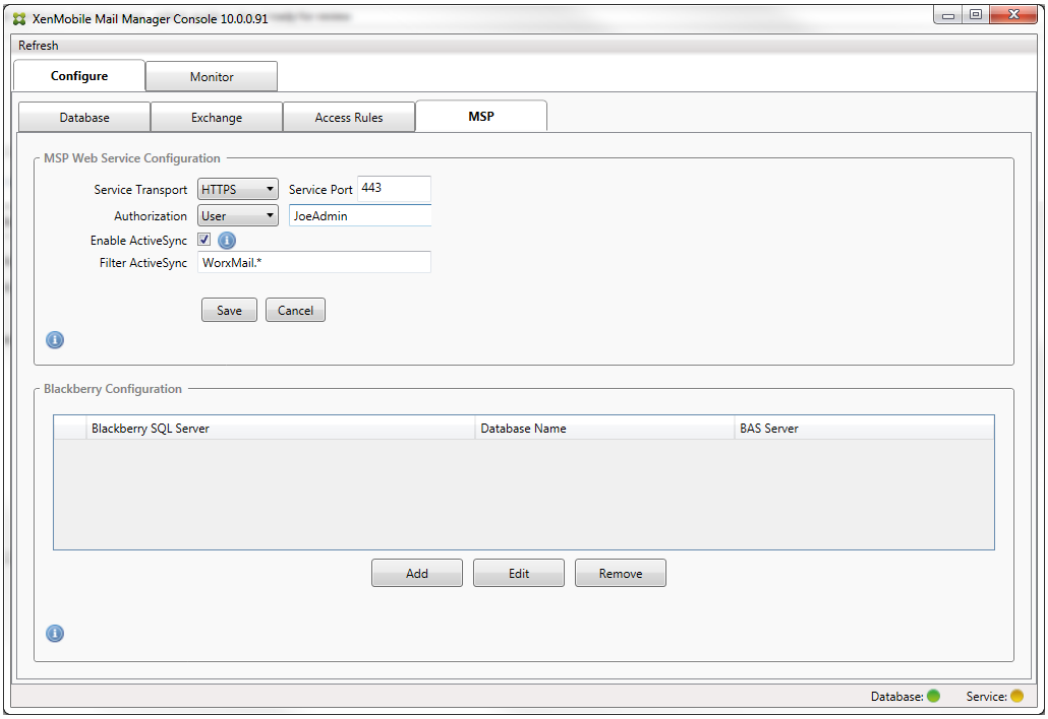
8. Klicken Sie auf die Registerkarte Local Rules.

1. Wenn Sie lokale Regeln für Active Directory-Gruppen erstellen möchten, klicken Sie auf Configure LDAP und konfigurieren Sie dann die LDAP-Verbindungseigenschaften.



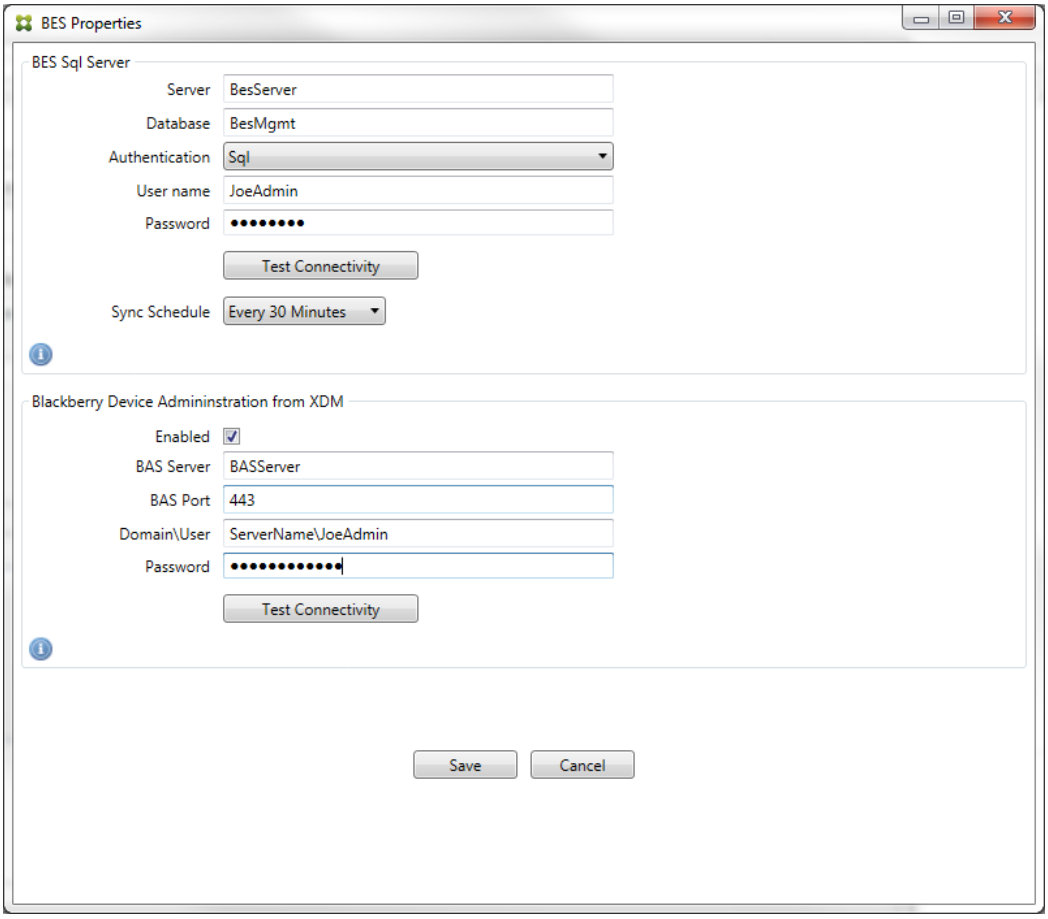
2. Sie können lokale Regeln basierend auf den Parametern ActiveSync Device ID, Device Type, AD Group, User oder UserAgent hinzufügen. Wählen Sie in der Liste den geeigneten Schlüssel aus. Weitere Informationen finden Sie unter Zugriffsregeln in XenMobile Mail Manager.
3. Geben Sie Text oder Textteile 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.



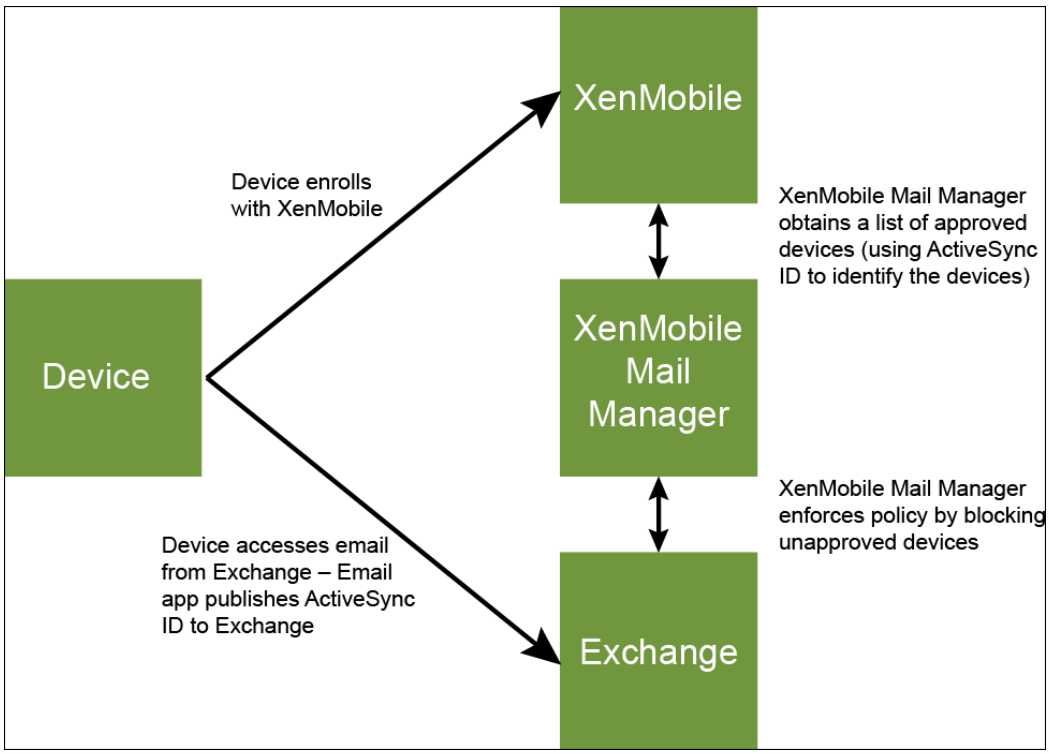
3. Geben Sie den Namen der BES-Verwaltungsdatenbank ein.
4. Wählen Sie den Authentifizierungsmodus aus. Bei Auswahl von "Windows Integrated" wird das Benutzerkonto des XenMobile Mail Manager-Diensts für die Verbindung mit dem BES SQL-Server verwendet.
   Hinweis: Wenn "Windows Integrated" auch für die 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

May 05, 2016

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

May 05, 2016

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.

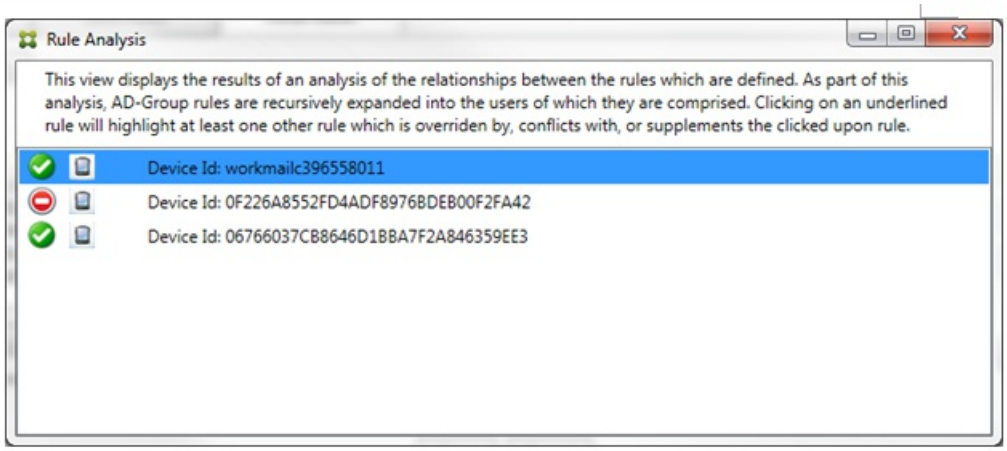
Terminologie:

- **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.

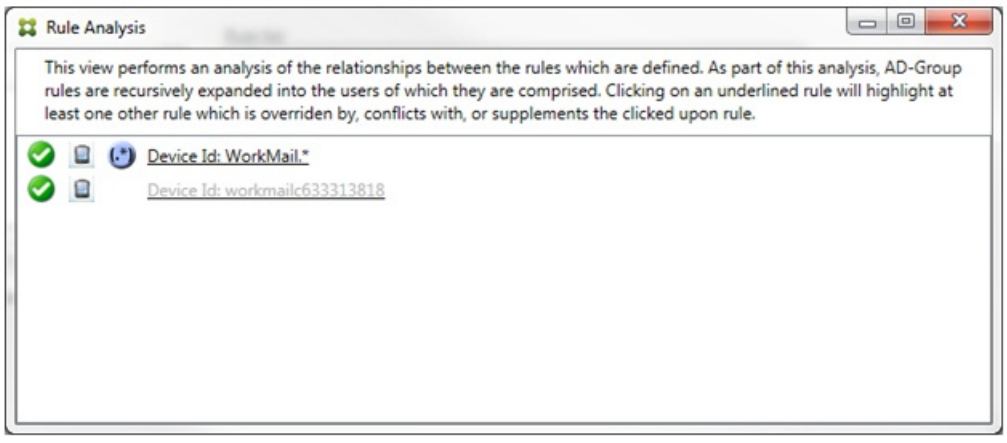
- **Ancillary rule** (Nebenregel): Eine Nebenregel hängt durch eine Außerkraftsetzung, einen Konflikt oder eine Ergänzungsbeziehung mit einer primären Regel zusammen. Solche Regeln werden durch einen gestrichelten Rahmen optisch hervorgehoben. Jede primäre Regel kann beliebig viele Nebenregeln haben. 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

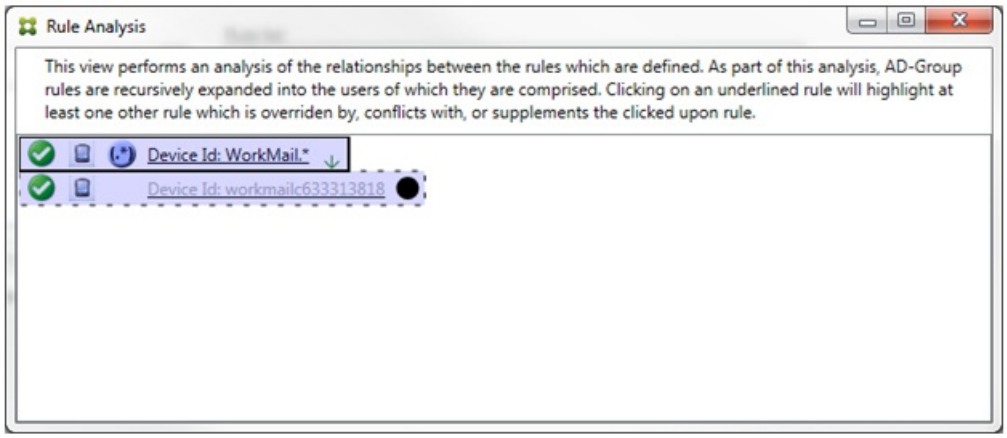
Wenn keine Konflikte, Außerkraftsetzungen oder Ergänzungen vorliegen, enthält das Dialogfeld Rule Analysis keine unterstrichenen Einträge. Das Klicken auf Elemente hat keine Auswirkung, es wird z. B. normal angezeigt, welches Element ausgewählt ist.



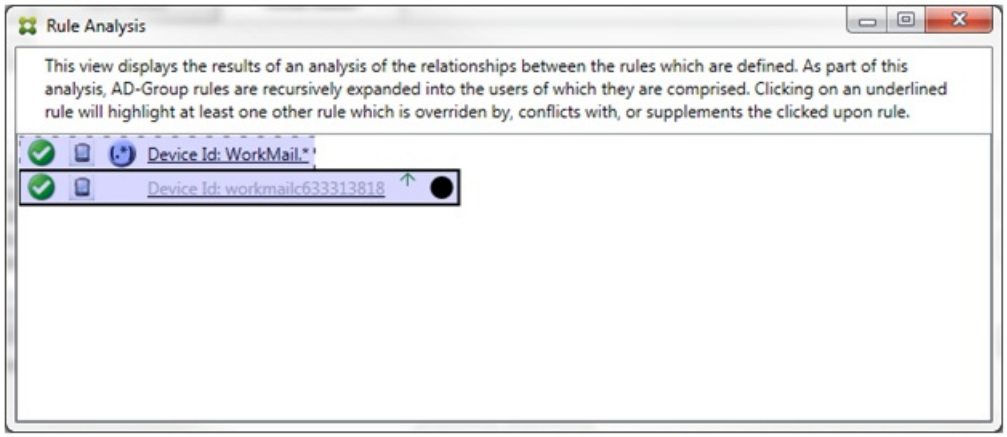
Wenn eine Außerkraftsetzung vorliegt, werden mindestens zwei Regeln unterstrichen dargestellt: die primäre Regel und die Nebenregel(n). Mindestens eine Nebenregel erscheint in einer helleren Schrift, um anzuzeigen, dass sie durch eine höhere Regel außer Kraft gesetzt wird. Sie können auf die außer Kraft 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:



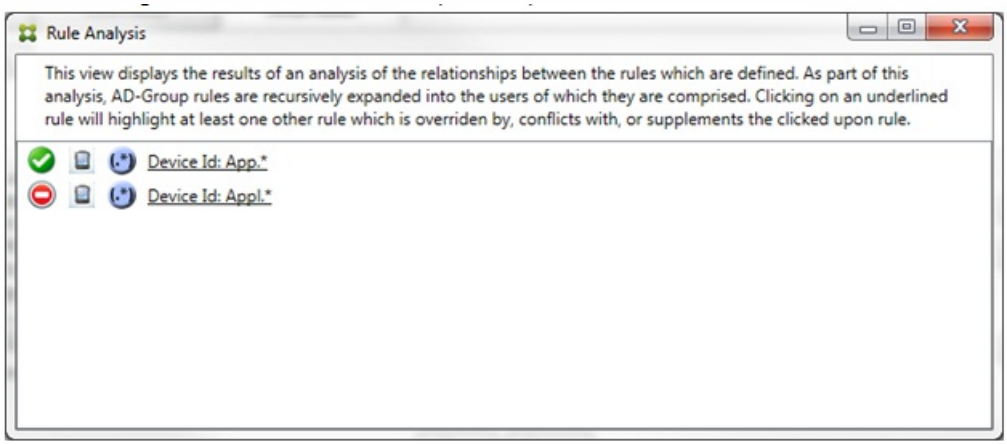
In diesem Beispiel ist die Regel mit regelmäßigen Ausdrücken WorkMail.* die primäre Regel (angezeigt durch den durchgehenden Rahmen) und die normale Regel workmailc633313818 ist eine Nebenregel (angezeigt durch den gestrichelten Rahmen). Der schwarze Punkt neben der Nebenregel weist deutlich darauf hin, 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:



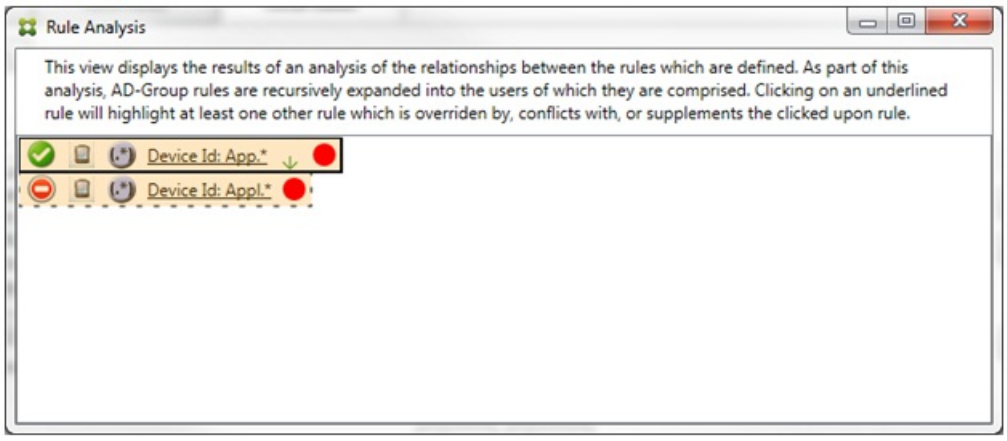
Im vorherigen Beispiel ist die Regel mit regelmäßigen Ausdrücken WorkMail.* die Nebenregel (angezeigt durch den gestrichelten Rahmen) und die normale Regel workmailc633313818 ist eine primäre Regel (angezeigt durch den durchgehenden Rahmen). In diesem einfachen Beispiel ist der Unterschied nicht groß. 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:

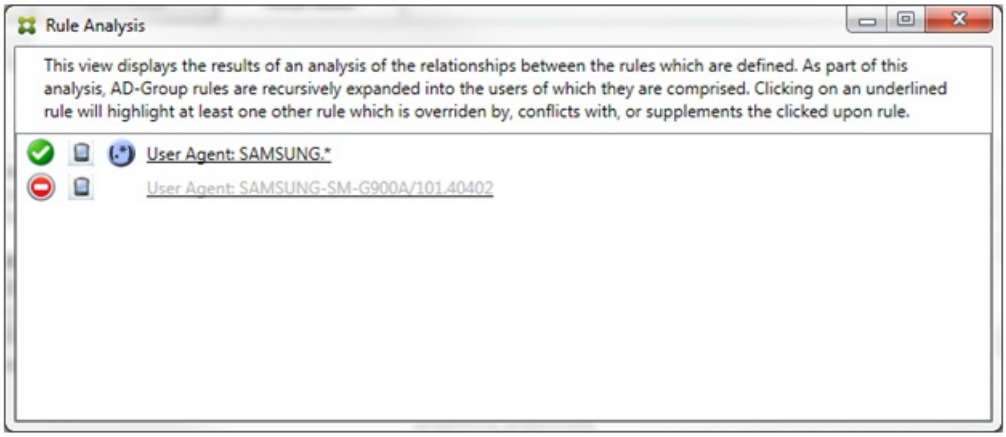


Eine Untersuchung der beiden Regeln mit regelmäßigen Ausdrücken ergibt, dass die erste alle Geräte, deren ID "App" enthält, zulässt und die zweite alle Geräte, deren ID "Appl" enthält, blockiert. Obwohl die zweite Regel alle Geräte, deren ID "Appl" enthält, blockiert, wird kein Gerät, auf das die Regel zutrifft, je blockiert, da die zulassende Regel eine höhere Priorität hat. Nach dem Klicken auf die erste Regel wird das Dialogfeld folgendermaßen angezeigt:



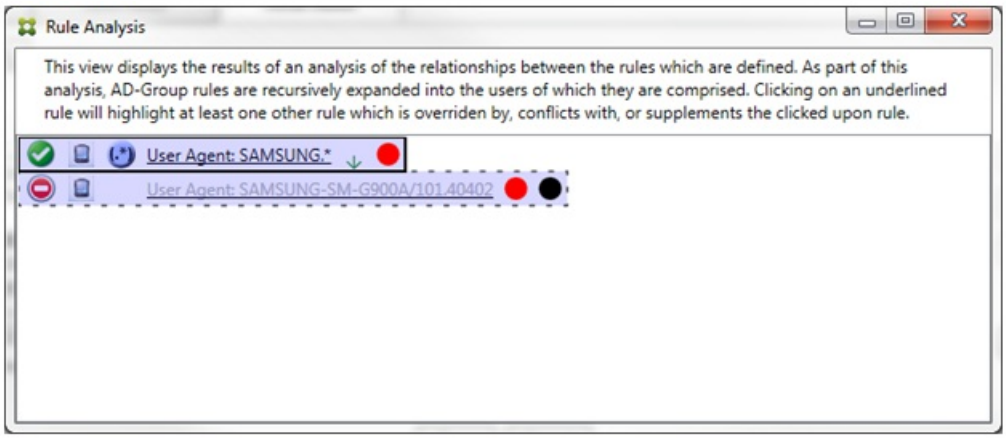
Im vorherigen Szenario wird sowohl die primäre Regel (mit dem regelmäßigen Ausdruck "App.*") und die Nebenregel (mit dem regelmäßigen Ausdruck "Appl.*") gelb markiert angezeigt. Dies ist ein einfacher optischer Warnhinweis auf den Umstand, dass mehrere Regeln mit regelmäßigem Ausdruck für ein einzelnes 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.



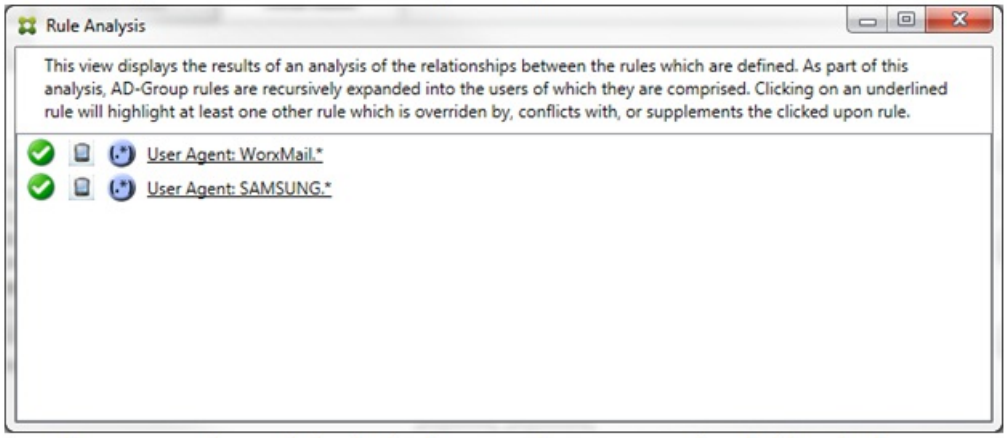
Im vorherigen Beispiel ist leicht zu erkennen, dass die erste Regel (mit dem regelmäßigen Ausdruck SAMSUNG.*) die nächste Regel (normale Regel SAMSUNG-SM-G900A/101.40402) außer Kraft setzt und überdies ein Konflikt beim Zugriffszustand (primäre Regel = Zulassen, Nebenregel = Blockieren) vorliegt. Die 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:

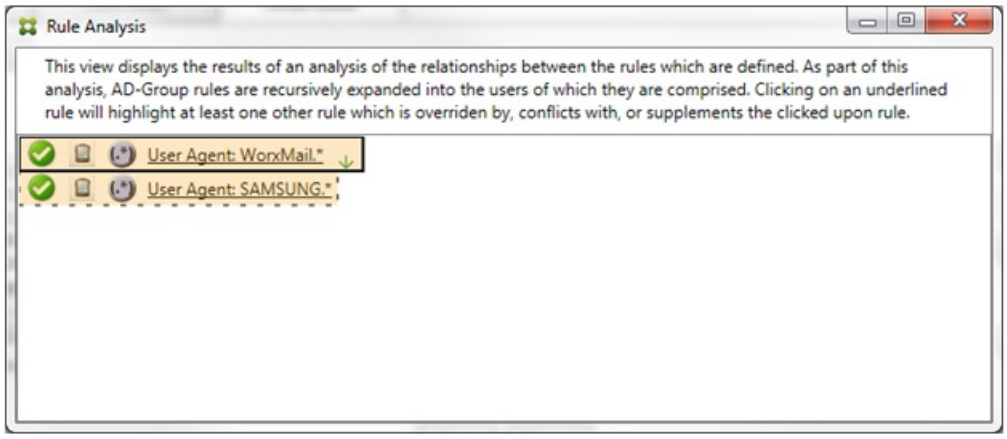


Die primäre Regel (mit dem regelmäßigen Ausdruck SAMSUNG.*) ist mit einem roten Punkt gekennzeichnet, um anzuzeigen, dass ihr Zugriffszustand im Widerspruch mit dem von mindestens einer Nebenregel steht. Die Nebenregel (normale Regel SAMSUNG-SM-G900A/101.40402) ist mit einem roten Punkt gekennzeichnet, 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:



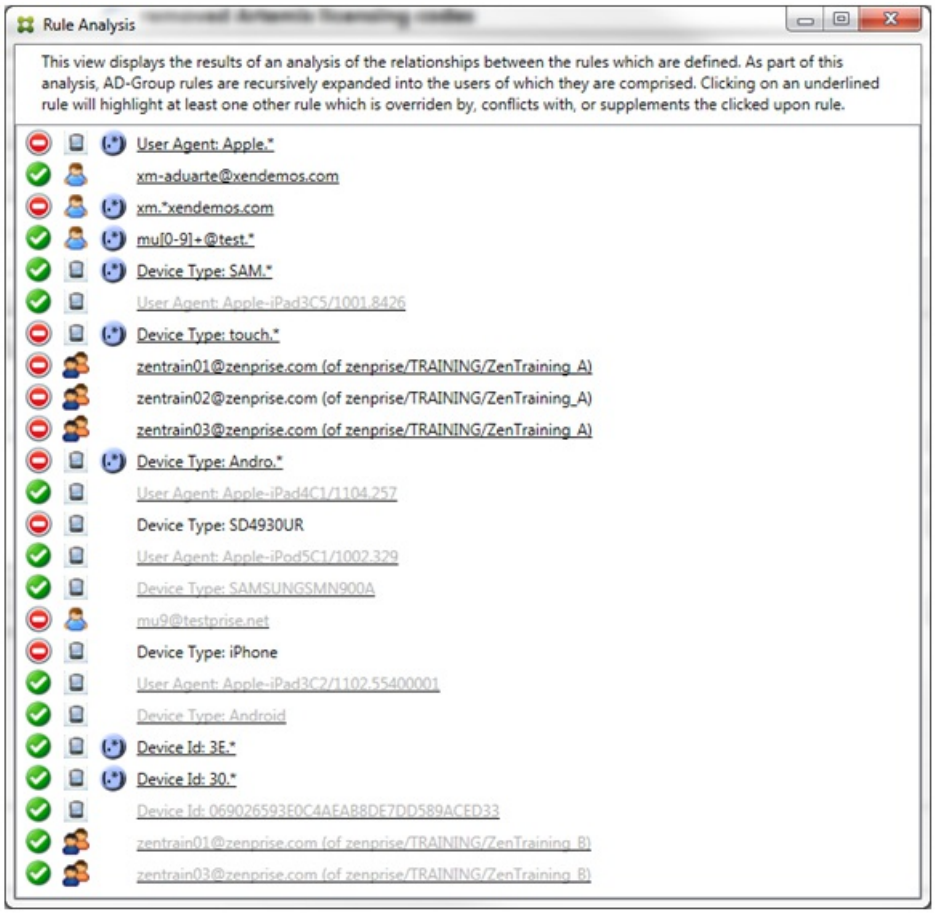
Es ist leicht zu erkennen, dass beide Regeln solche mit regelmäßigen Ausdrücken sind, und beide auf das Feld "ActiveSync device ID" in XenMobile Mail Manager angewendet werden. Nach dem Klicken auf die erste Regel sieht das Dialogfeld folgendermaßen aus:



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

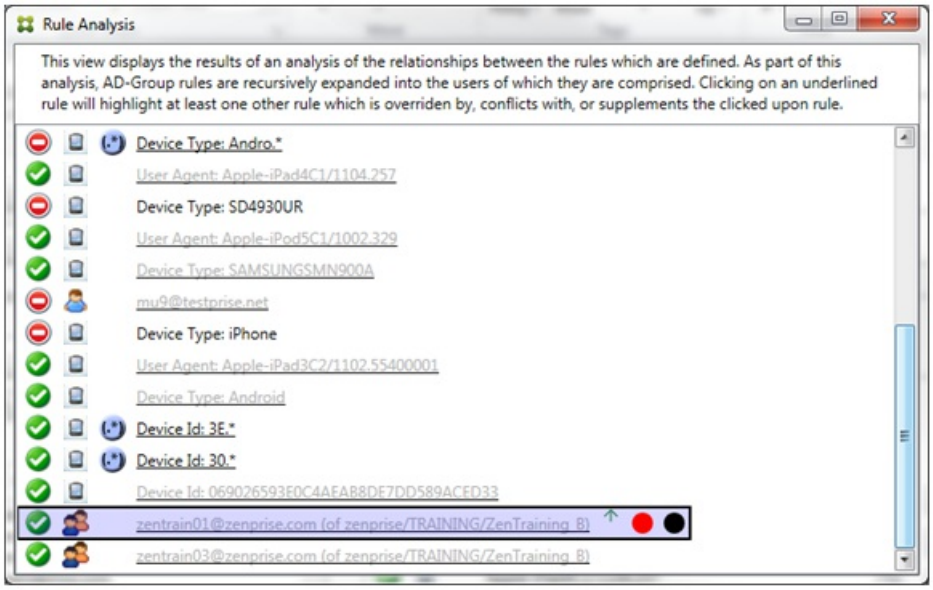
Es sind viele Außerkraftsetzungen, Konflikte oder Ergänzungen möglich, die hier nicht alle mit einem Beispiel vorgestellt werden können. Im Folgenden werden anhand eines Negativbeispiels die immensen Vorzüge des visuellen Konstrukts der Regelanalyse gezeigt. Die meisten Elemente in der folgenden Abbildung 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.

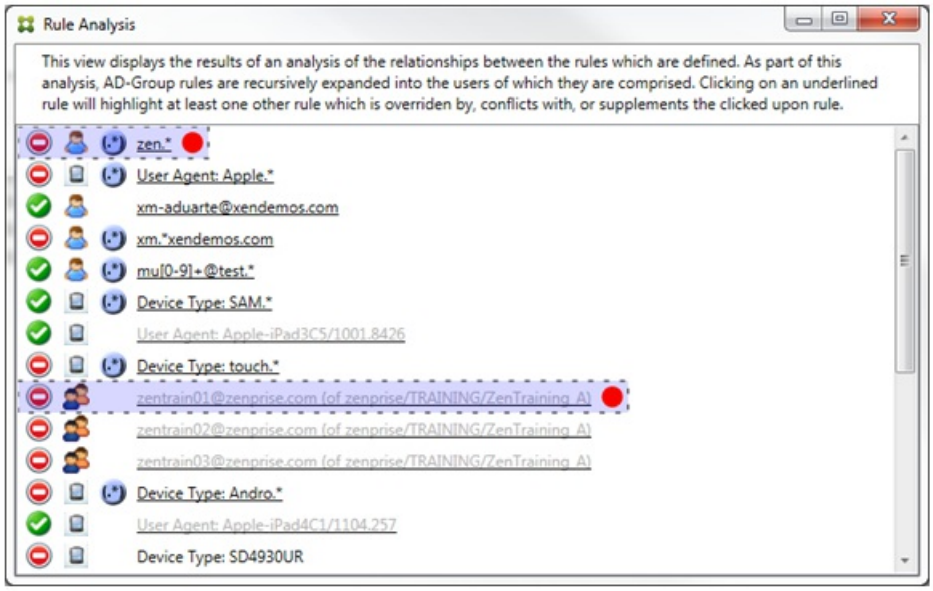
Beispiel 1: In diesem Beispiel wird untersucht, warum zentrain01@zenprise.com außer Kraft gesetzt wurde.



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.

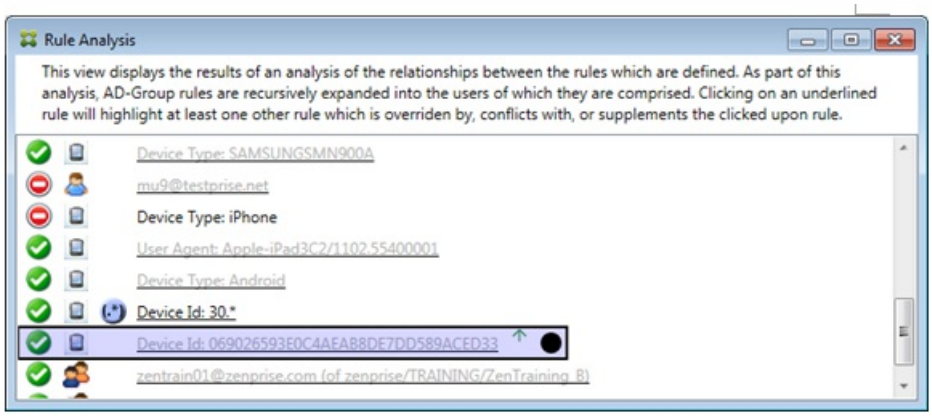
Wenn Sie einen Bildlauf nach oben durchführen, wird Folgendes angezeigt:



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

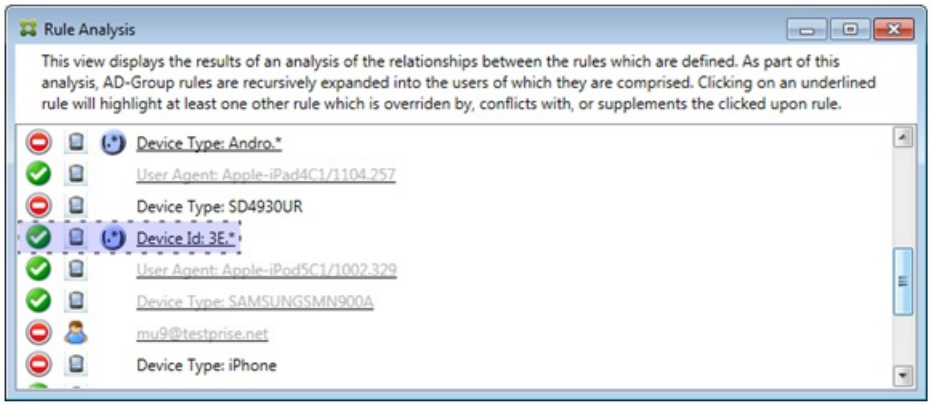
besteht das Problem darin, dass die Active Directory-Gruppenregel ZenTraining A den Benutzer zentrain01@zenprise.com enthält, die Active Directory-Gruppenregel ZenTraining B diesen Benutzer jedoch auch enthält. Da die Nebenregel eine höhere Priorität hat als die primäre Regel, wird die primäre Regel 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.

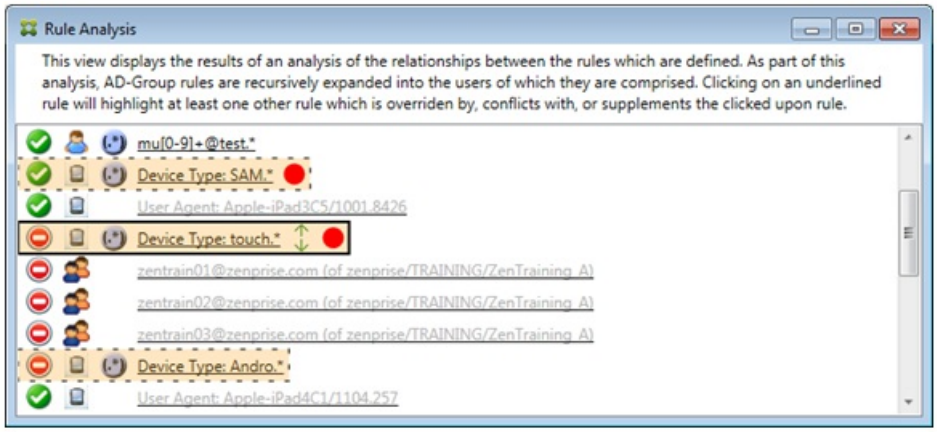


In diesem Fall wird die primäre Regel von einer einzigen Nebenregel außer Kraft gesetzt: der Regel mit der ActiveSync Geräte-ID und dem regelmäßigen Ausdruck 3E.*. Da der regelmäßige Ausdruck 3E.* auf 069026593E0C4AEAB8DE7DD589ACED33 zutrifft, würde die primäre Regel niemals ausgewertet.

Analysieren einer Ergänzung und eines Konflikts

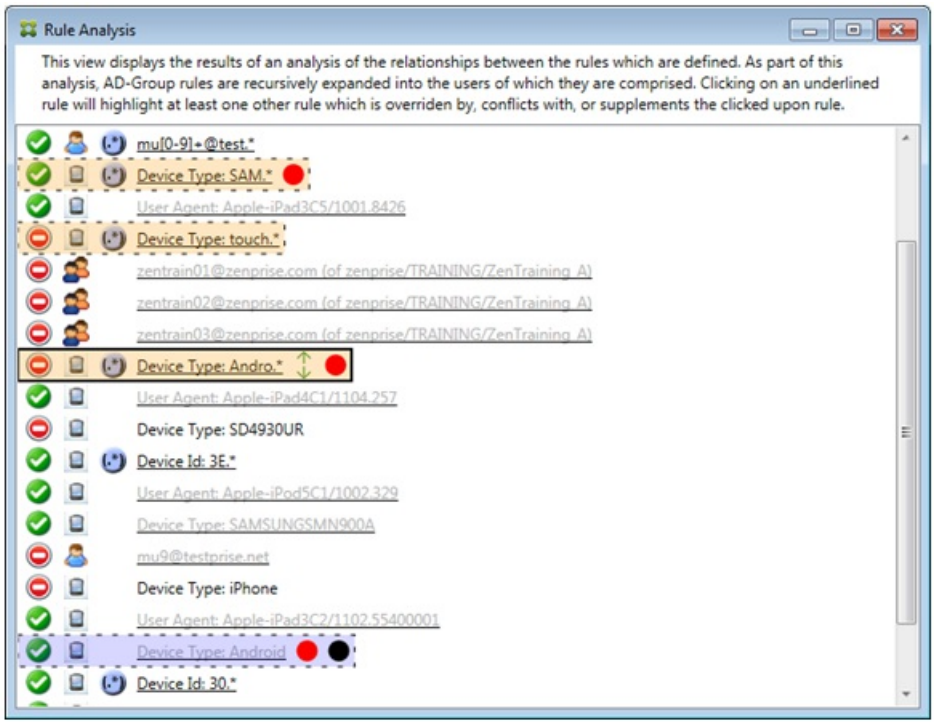
In diesem Beispiel ist die primäre Regel die ActiveSync-Gerätetypregel mit dem regelmäßigen Ausdruck touch.* Sie hat folgende Merkmale:

- 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

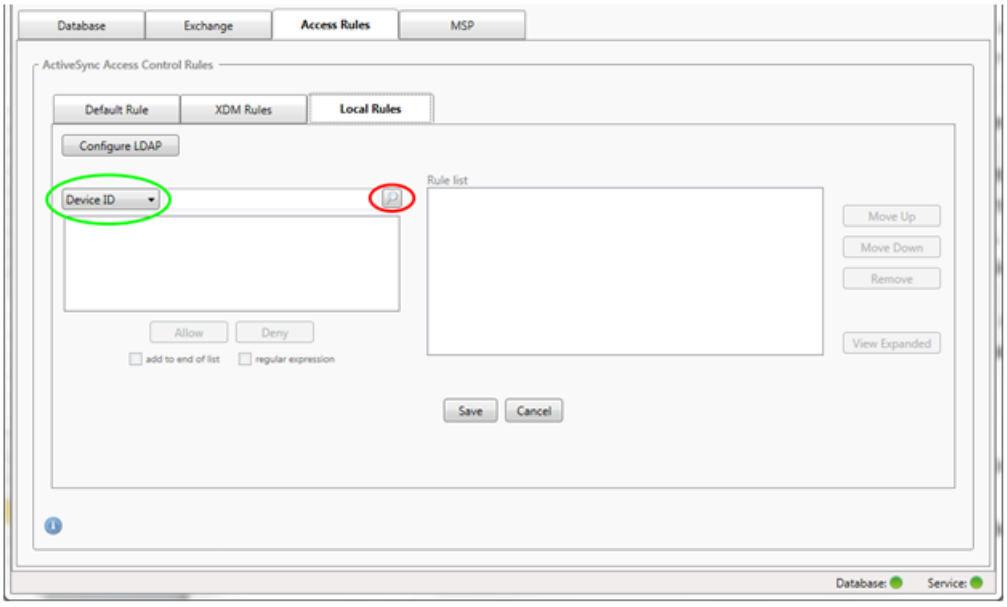
In diesem Beispiel wird demonstriert, dass Regelbeziehungen immer aus der Sicht der primären Regel dargestellt werden. Im vorherigen Beispiel wurde gezeigt, was beim Klicken auf die Gerätetypregel mit dem regelmäßigen Ausdruck touch.* angezeigt wird. Wird auf die Nebenregel Andro.* geklickt, werden andere 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.

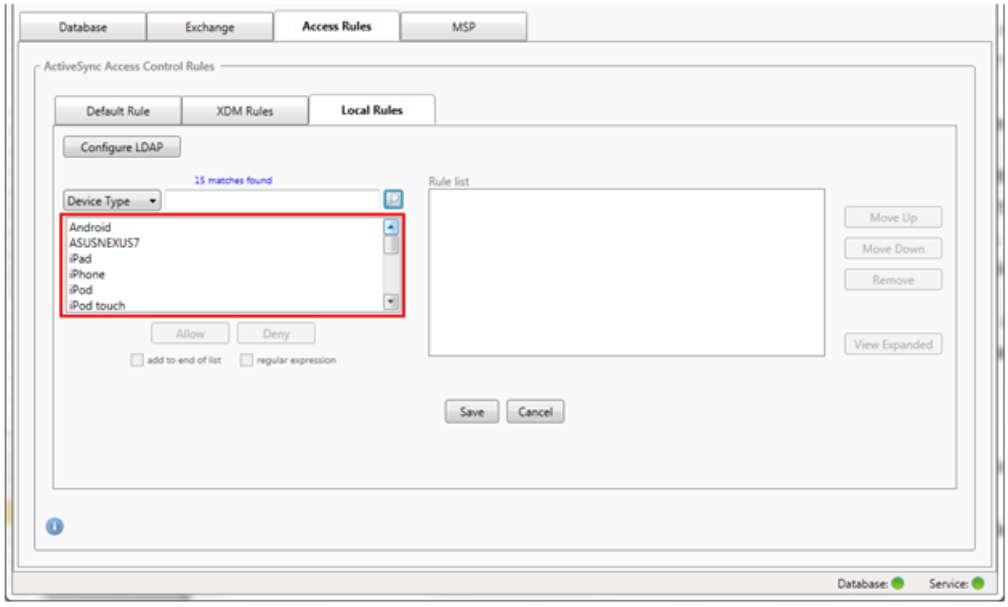
So konfigurieren Sie eine lokale Regel mit normalem Ausdruck

1. Klicken Sie auf die Registerkarte Access Rules.



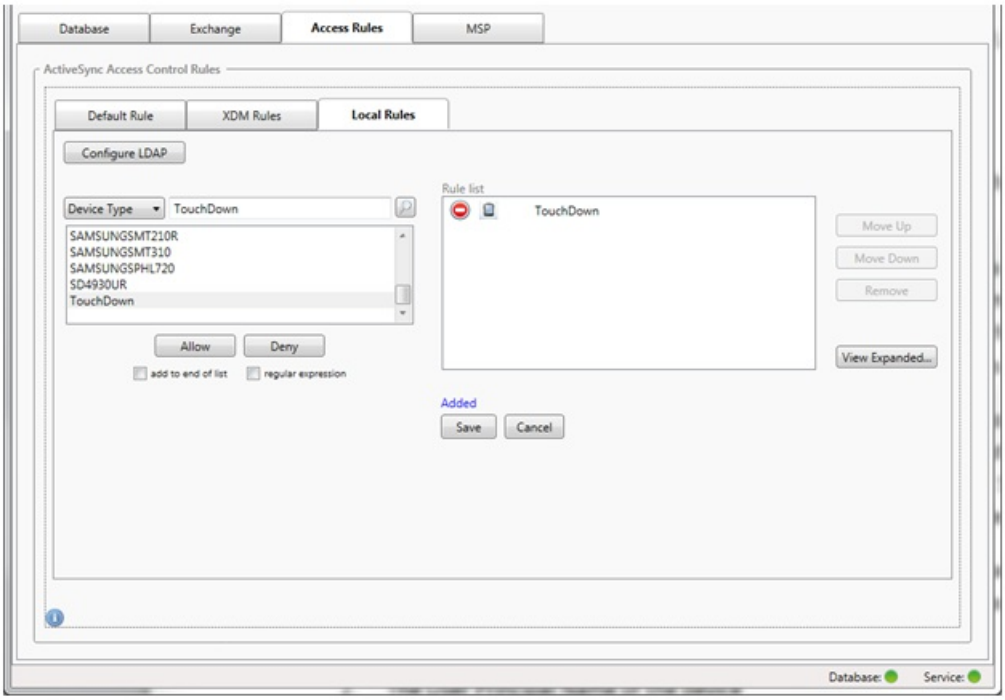
2. Wählen Sie in der Liste Device ID das Feld aus, für das Sie die lokale Regel erstellen möchten.

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.

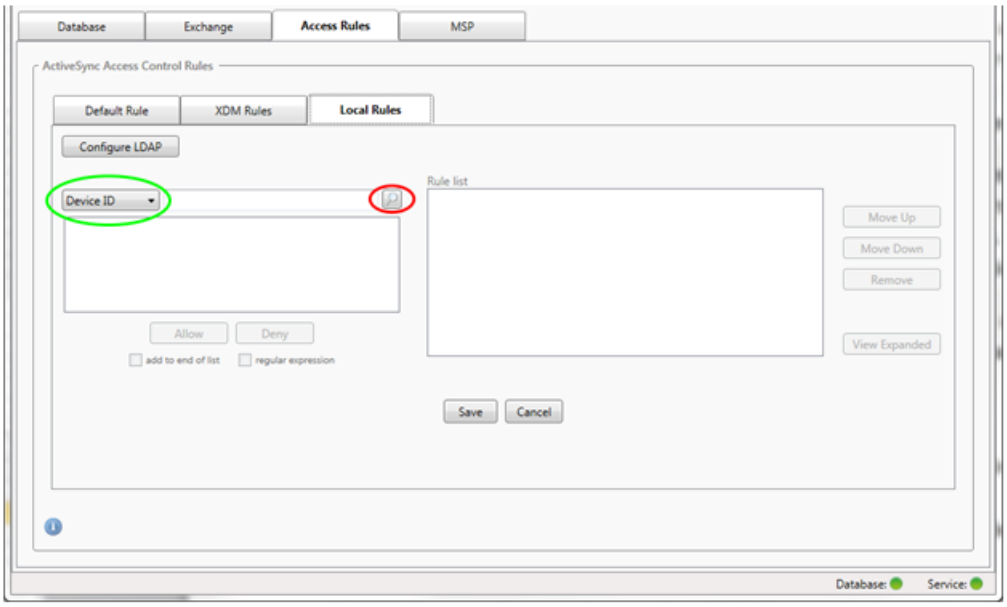


So fügen Sie einen regelmäßigen Ausdruck hinzu

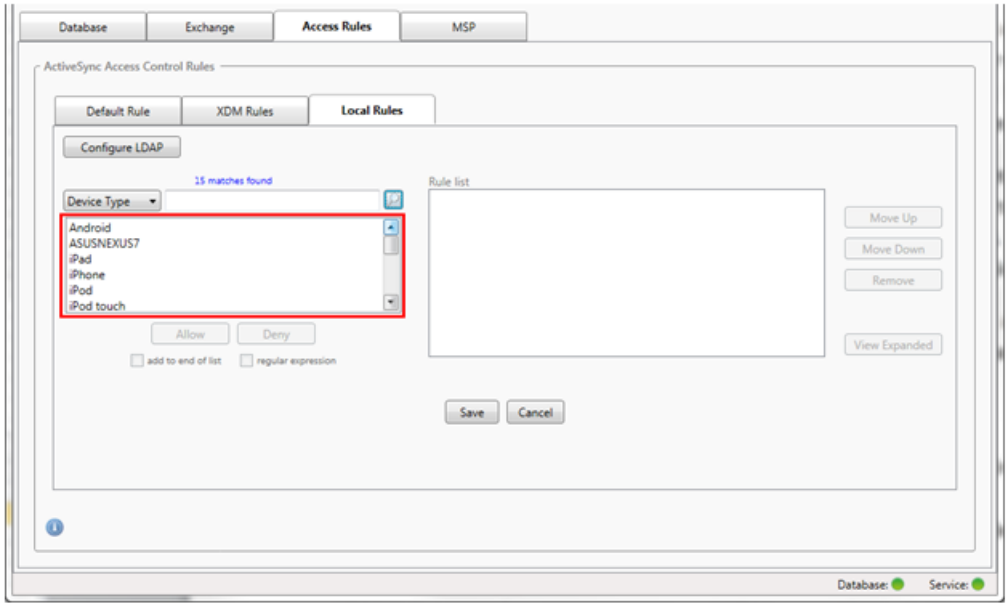
Lokale Regeln mit regelmäßigen Ausdrücken sind an dem Symbol (.*) zu erkennen. Zum Hinzufügen einer Regel mit regelmäßigem Ausdruck können Sie entweder einen Wert aus der Ergebnisliste für ein spezifisches Feld als Grundlage verwenden (sofern bereits ein größerer Snapshot durchgeführt wurde) oder den regelmäßigen Ausdruck selbst eingeben.

So erstellen Sie einen regelmäßigen Ausdruck mit einem vorhandenen Feldwert

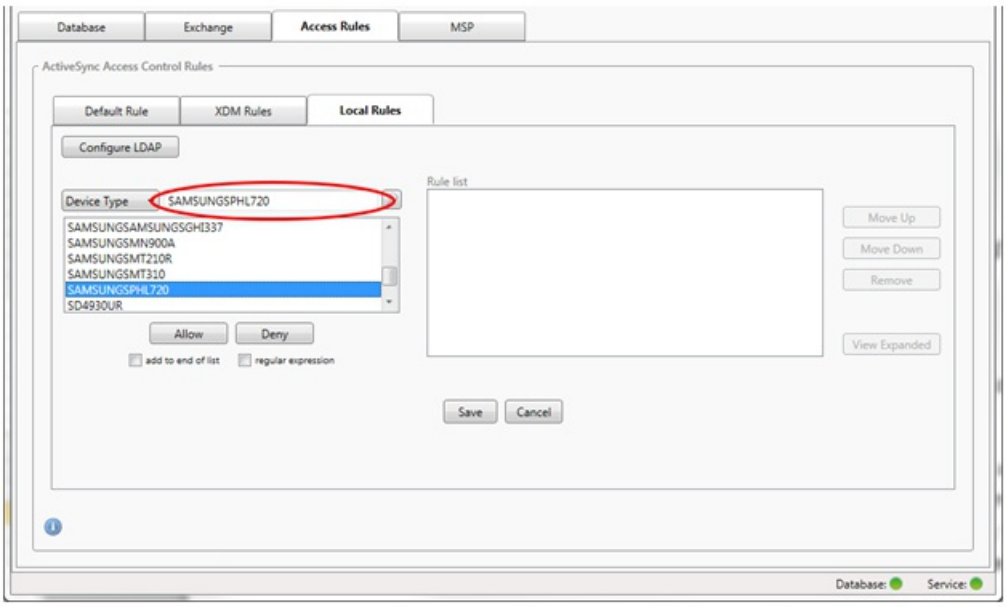
1. Klicken Sie auf die Registerkarte Access Rules.



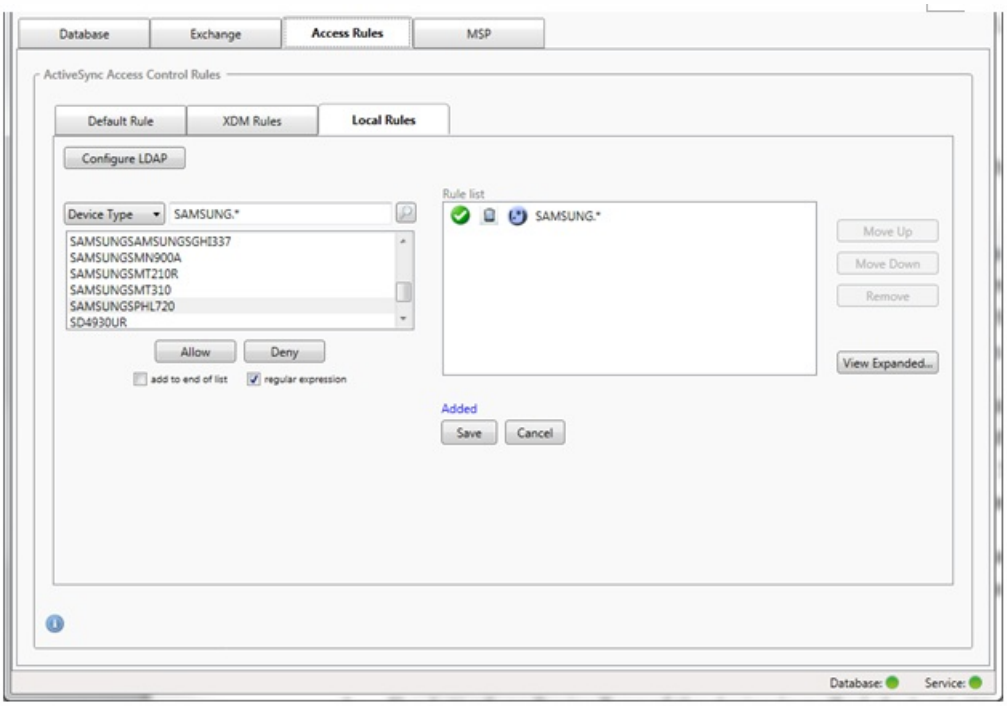
2. Wählen Sie in der Liste Device ID das Feld aus, für das Sie die lokale Regel mit einem regelmäßigen Ausdruck erstellen möchten.
3. Klicken Sie auf das Lupensymbol, um alle eindeutigen Übereinstimmungen für das ausgewählte Feld einzublenden. In diesem Beispiel wurde das Feld Device Type ausgewählt, 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.



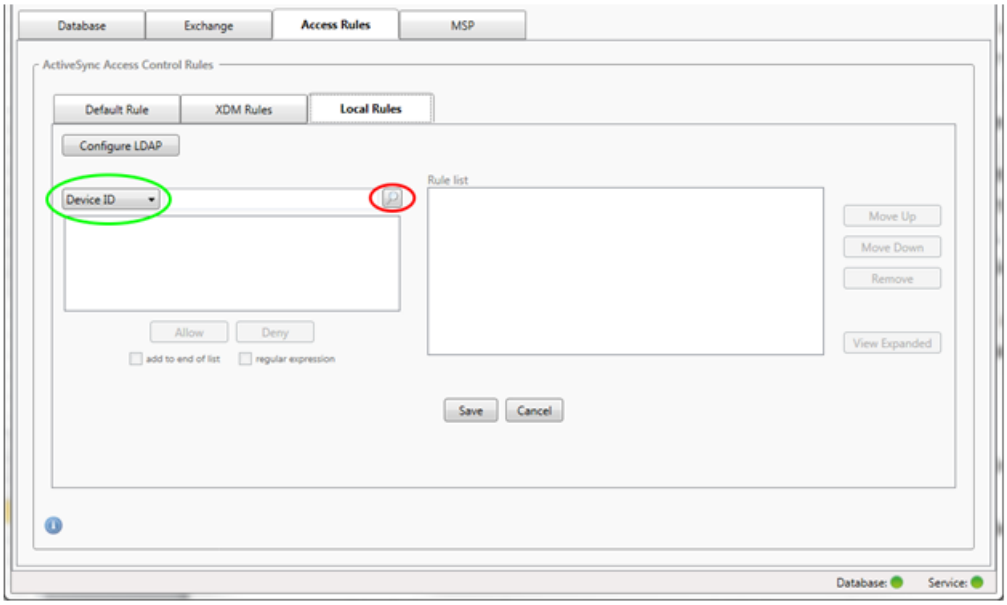
5. Damit alle Gerätetypen, deren Gerätetypwert "Samsung" enthält, zugelassen werden, fügen Sie eine Regel mit regelmäßigem Ausdruck wie folgt hinzu:
   1. Klicken Sie in das Textfeld des ausgewählten Elements.
   2. Ändern Sie den Text SAMSUNGSPHL720 in SAMSUNG.*
   3. Stellen Sie sicher, dass das Kontrollkästchen regular expression aktiviert ist.
   4. Klicken Sie auf Allow.



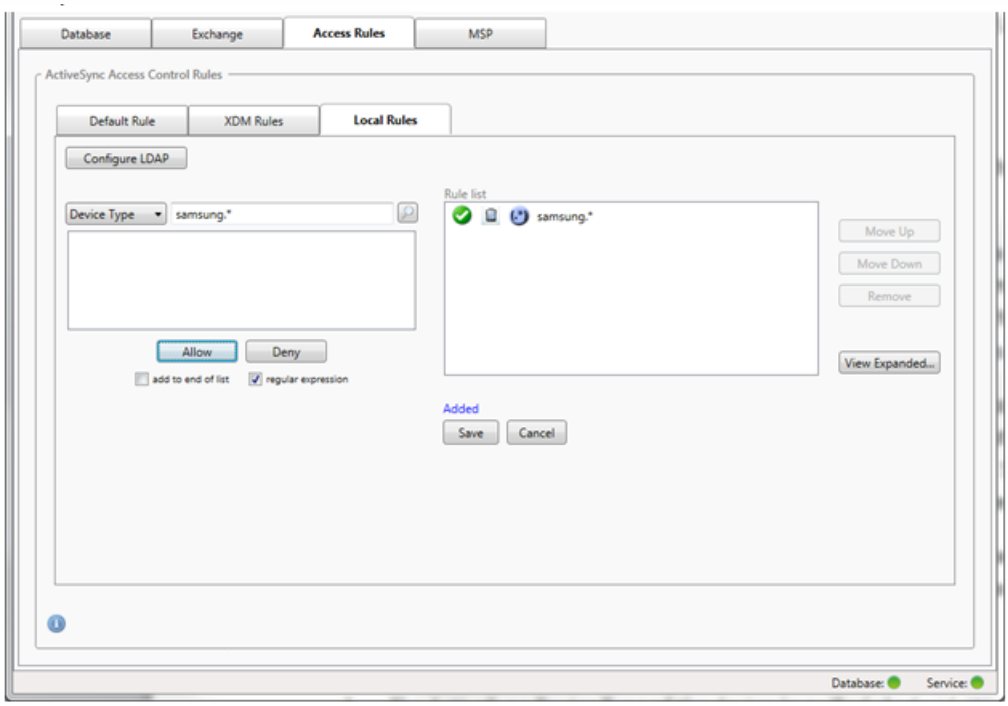
So erstellen Sie eine Zugriffsregel

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 dies samsung.*
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:

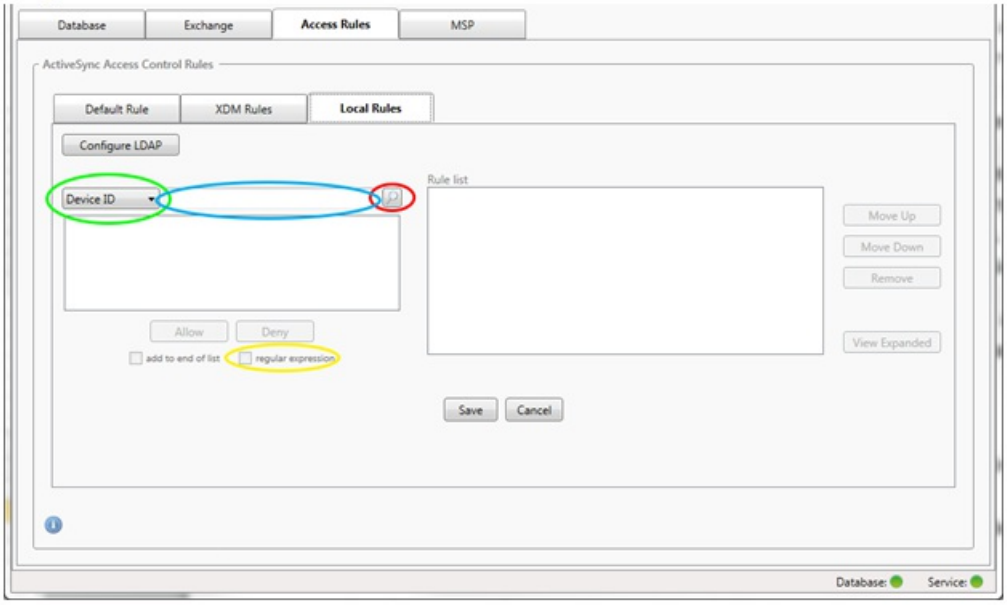


So suchen Sie Geräte

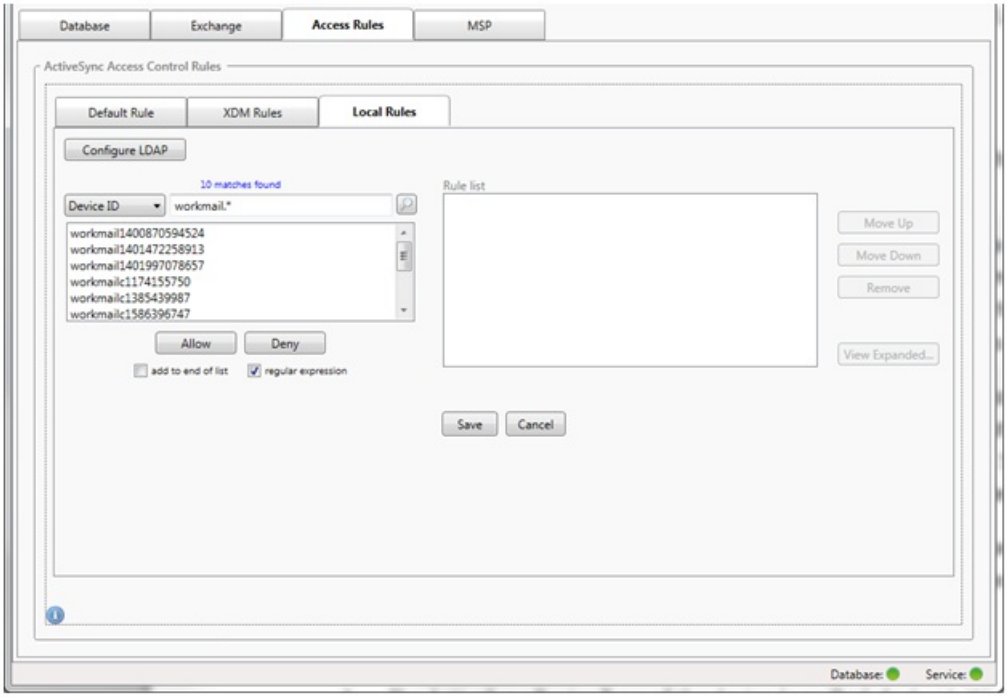
Durch Aktivieren des Kontrollkästchens "regular expression" können Sie Geräte, die dem angegebenen Ausdruck entsprechen, suchen. Dieses Feature steht nur zur Verfügung, wenn ein größerer Snapshot erfolgreich durchgeführt wurde. Sie können das Feature nutzen, selbst wenn Sie keine Verwendung regelmäßiger 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.



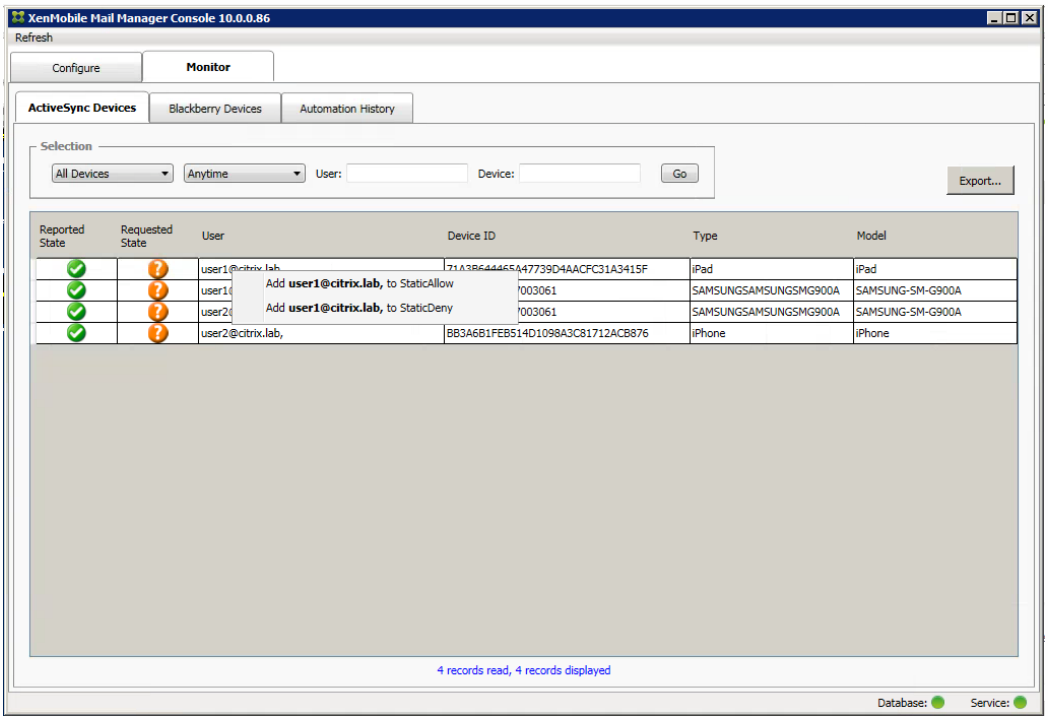
3. Klicken Sie in das Textfeld des ausgewählten Elements (blau in der Abbildung oben) und geben Sie workmail.* ein.
4. Stellen Sie sicher, dass das Kontrollkästchen regular expression aktiviert ist, und klicken Sie auf das Lupensymbol, damit Übereinstimmungen angezeigt werden (siehe folgende Abbildung).



So fügen Sie einer statischen Regel einen einzelnen Benutzer, ein einzelnes Gerät oder einen einzelnen Gerätetyp hinzu

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

May 05, 2016

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

May 05, 2016

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 13, 2016

XenMobile NetScaler Connector ist eine Lösung zur Steuerung des Zugriffs von Mobilgeräten auf Unternehmens-E-Mail, Kalender und Kontakte. Mit XenMobile NetScaler Connector können Kunden eine Liste der konformen Geräte von XenMobile an NetScaler senden, das wiederum steuert, welche Mobilgeräte mit Exchange Server im Unternehmen synchronisiert werden dürfen.

XenMobile bietet vollständigen Schutz für mobile Apps, Netzwerk und Daten und gewährleistet eine lückenlose Sicherheit und Richtlinientreue. NetScaler optimiert, schützt und steuert die Bereitstellung aller Unternehmens- und Clouddienste. Zusammen bieten die beiden Citrix Produkte Funktionalität für Skalierbarkeit, hohe Verfügbarkeit für Apps und Sicherheit, während die Kosten für Bereitstellung und Verwaltung von Mobilität reduziert werden.

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.

XenMobile bietet Richtlinien für Positivlisten und Sperrlisten für Geräte basierend auf der Einhaltung von übergeordneten Richtlinien, wie das Erkennen von Geräten mit Jailbreak oder von bestimmten Apps. Die lokalen XenMobile NetScaler Connector-Regeln werden üblicherweise zur Erweiterung der XenMobile-Regeln verwendet, wenn eine Außerkraftsetzung erforderlich ist, beispielsweise, um alle Geräte mit einem bestimmten Betriebssystem zu blockieren.

Die Hauptfeatures von XenMobile NetScaler Connector sind folgende:

- **Zugriffssteuerung für HTTP-ActiveSync-Anforderungen**: XenMobile NetScaler Connector kann die HTTP-ActiveSync-Anforderungen von Mobilgeräten an Exchange Server steuern. Sie können in XenMobile NetScaler Connector Filter erstellen, mit denen Geräte je nach von Ihnen festgelegten Regeln und Kriterien blockiert oder zugelassen werden. Wenn Sie Regeln in XenMobile NetScaler Connector festlegen, können Sie die Regeln dann in XenMobile aktivieren oder deaktivieren, um den Zugriff von Geräten auf E-Mail im Unternehmen zu verwalten.
- **Remotekonfiguration**: XenMobile steuert das von XenMobile NetScaler Connector verwendete Baseline- und Deltaintervall.
- **Protokollierung**: Auf der Registerkarte **Log** des XenMobile NetScaler Connector-Konfigurationsprogramms wird zusätzlich zu den zugelassenen und blockierten Geräten angezeigt, wenn die Verschlüsselung für ein bestimmtes Benutzergerät auf Anforderungsebene aktiviert ist.

XenMobile NetScaler Connector bietet folgende Funktionen:

- **Filterbasierte Regeln zum Blockieren oder Zulassen des Zugriffs**: XenMobile NetScaler Connector wertet Clientanfragen, die über NetScaler geleitet werden, anhand der in der Organisation gültigen Regeln aus. Das Ergebnis dieser Auswertung ist ein binärer Zustand von *Zugelassen*, in dem der Client eine Verbindung mit dem Microsoft Exchange 2010-Clientzugriffsserver (CAS) herstellen darf, oder von *Blockiert*, in dem die Clientanfrage abgewiesen und der Zugriff auf den Exchange-CAS nicht zugelassen wird. In Kombination mit den Einstellungen der XenMobile-Konsole können Sie den Zugriff auf Exchange ActiveSync-E-Mail durch Gerätebenutzer basierend auf Konformitätskriterien (z. B. Liste gesperrter Apps, Jailbreaks usw.) verhindern.
- **Zweistufiges Filtermodell**: Auf der ersten Stufe werden eingehende HTTP-Anfragen basierend auf pfadspezifischen Informationen analysiert. Auf der zweiten Ebene erfolgt die Filterung basierend auf benutzer- oder gerätespezifischen Informationen. Sie können beide Stufen konfigurieren.

- **Speicherung der Filterregeln in Konfigurationsdateien**: Spezifische Filterregeln für Benutzerkonten und Geräte in Ihrer Organisation werden in den XML-Konfigurationsdateien des Gateways gespeichert.

Ein detailliertes Architekturdiagramm finden Sie im Artikel Reference Architecture for On-Premises Deployments in der XenMobile-Bereitstellungsdokumentation.

Bereitstellen von XenMobile NetScaler Connector

May 05, 2016

Mit XenMobile NetScaler Connector können Sie NetScaler als Proxy und für den Lastausgleich bei der Kommunikation zwischen XenMobile-Server und mit XenMobile verwalteten Geräten verwenden. XenMobile NetScaler Connector kommuniziert in regelmäßigen Abständen mit XenMobile zur Synchronisierung von Richtlinien. XenMobile NetScaler Connector und XenMobile lassen sich zusammen oder separat in Clustern zusammenfassen. Ein Lastausgleich ist mit NetScaler möglich.

XenMobile NetScaler Connector-Komponenten

XenMobile NetScaler Connector besteht aus den folgenden vier Komponenten:

- XenMobile NetScaler Connector-Dienst: bietet eine REST-Webdienstschnittstelle, die von NetScaler aufgerufen werden kann, um zu bestimmen, ob eine ActiveSync-Anforderung von einem Gerät autorisiert ist.
- XenMobile-Konfigurationsdienst: Dieser Dienst kommuniziert mit Device Manager zur Synchronisierung von Device Manager-Richtlinienänderungen mit XenMobile NetScaler Connector.
- XenMobile-Benachrichtigungsdienst: Dieser Dienst sendet Benachrichtigungen über unautorisierten Gerätezugriff an Device Manager, sodass Device Manager Maßnahmen ergreifen kann, z. B. das Senden einer Erklärung an den Benutzer, warum sein Gerät blockiert wurde.
- XenMobile NetScaler-Konfigurationsprogramm: Mit dieser Anwendung kann der Administrator XenMobile NetScaler Connector konfigurieren und überwachen.

Einrichten von Überwachungsadressen für XenMobile NetScaler Connector

Damit XenMobile NetScaler Connector Anfragen von NetScaler für die Autorisierung von ActiveSync-Datenverkehr empfangen kann, müssen Sie den Port angeben, den XenMobile NetScaler Connector auf Aufrufe des NetScaler-Webdiensts überwacht.

1. Wählen Sie im Menü Start den Eintrag XenMobile NetScaler configuration utility aus.
2. Klicken Sie auf die Registerkarte Web Service und geben Sie dann die Überwachungsadressen für den XenMobile NetScaler Connector-Webdienst an. Sie können HTTP und/oder HTTPS auswählen. Residiert XenMobile NetScaler Connector auf dem gleichen Server wie XenMobile, wählen Sie Ports aus, die keinen Konflikt mit denen von XenMobile auslösen.
3. Wenn Sie die Werte konfiguriert haben, klicken Sie auf Save und dann auf Start Service, um den Webdienst zu starten.

Konfigurieren von Richtlinien für die Gerätezugriffssteuerung in XenMobile NetScaler Connector

Zum Konfigurieren einer Zugriffssteuerungsrichtlinie für verwaltete Geräte gehen Sie folgendermaßen vor:

1. Klicken Sie im XenMobile NetScaler-Konfigurationsprogramm auf die Registerkarte Path Filters.
2. Wählen Sie die erste Zeile, Microsoft-Server-ActiveSync is for ActiveSync, aus und klicken Sie auf Edit.
3. Wählen Sie in der Liste Policy die gewünschte Richtlinie aus. Bei Richtlinien, die XenMobile-Richtlinien umfassen, wählen Sie Static + ZDM: Permit Mode oder Static + ZDM: Block Mode aus. Diese Richtlinien kombinieren lokale (statische) Regeln mit denen von XenMobile. Permit Mode bedeutet, dass alle Geräte, die nicht explizit durch die Regeln identifiziert werden, Zugriff auf ActiveSync erhalten. Block Mode bedeutet, dass solche Geräte blockiert werden.
4. Wenn Sie die Richtlinien eingerichtet haben, klicken Sie auf Save.

Konfigurieren der Kommunikation mit XenMobile

Bei diesem Arbeitsgang geben Sie Namen und Eigenschaften des XenMobile-Servers (= "Config Provider") an, den Sie mit XenMobile NetScaler Connector und NetScaler verwenden möchten.

Hinweis: Es wird davon ausgegangen, dass Sie XenMobile bereits installiert und konfiguriert haben.

1. Klicken Sie im XenMobile NetScaler Connector-Konfigurationsprogramm auf die Registerkarte Config Providers und dann auf Add.
2. Geben Sie den Namen und die URL des XenMobile-Servers ein, den Sie in der Bereitstellung verwenden. Wenn Sie mehrere XenMobile-Server in einer Bereitstellung mit mehreren Mandanten haben, muss der Name für jede Serverinstanz eindeutig sein. Geben Sie unter Name beispielsweiseXMS ein.
3. Geben Sie unter Url die Webadresse des XenMobile-GCP (GlobalConfig Provider) im Format https://DeviceManagerHost/zdm/services/MagConfigService ein. Bei dem Namen von MagConfigservice wird Groß-/Kleinschreibung unterschieden.
4. Geben Sie unter Password das Kennwort des Kontos mit Administratorrechten ein, das für die grundlegende HTTP-Autorisierung auf dem XenMobile-Webserver verwendet werden soll.
5. Geben Sie unter Managing Host den Namen des Servers ein, auf dem Sie XenMobile NetScaler Connector installiert haben.
6. Geben Sie unter Baseline Interval das Intervall ein, in dem von XenMobile der aktualisierte Satz dynamischer Regeln abgerufen werden soll.
7. Geben Sie unter Request Timeout das Timeoutintervall für die Serveranforderungen an.
8. Wählen Sie unter Config Provider die Serverinstanz des Konfigurationsanbieters aus, der die Richtlinienkonfiguration bereitstellt.
9. Aktivieren Sie diese Option unter Events Enabled, wenn Secure Mobile Gateway die Blockierung eines Geräts an XenMobile melden soll. Die Option ist erforderlich, wenn Sie Secure Mobile Gateway-Regeln in Device Manager für eine automatische Aktion verwenden.
10. Klicken Sie nach Abschluss der Konfiguration des Servers auf Test Connectivity, um die Verbindung mit dem XenMobile-Server zu testen.
11. Wenn die Verbindung hergestellt wird, klicken Sie auf Save.

Bereitstellen von XenMobile NetScaler Connector für Redundanz und Skalierbarkeit

Wenn Sie Ihre XenMobile NetScaler Connector- und XenMobile-Bereitstellung skalieren möchten, installieren Sie Instanzen von XenMobile NetScaler Connector auf mehreren Windows-Servern, die alle auf die gleiche XenMobile-Instanz verweisen, und führen Sie dann einen Lastausgleich der Server mit NetScaler aus.

Es gibt zwei Modi für die XenMobile NetScaler Connector -Konfiguration:

- Im Modus ohne Freigabe kommuniziert jede XenMobile NetScaler Connector-Instanz mit einem XenMobile-Server und speichert eine eigene Kopie der daraus resultierenden Richtlinie. Beispiel: In einem XenMobile-Servercluster können Sie eine XenMobile NetScaler Connector-Instanz auf jedem XenMobile-Server ausführen. XenMobile NetScaler Connector erhält dann Richtlinien von der lokalen XenMobile-Instanz.
- In Modus mit Freigabe wird ein XenMobile NetScaler Connector-Knoten als primärer Knoten festgelegt und kommuniziert mit XenMobile. Die resultierende Konfiguration wird dann per Windows-Netzwerkfreigabe oder per Windows-Replikation (bzw. per Drittanbieter-Replikation) an die anderen Knoten weitergegeben.

Die gesamte XenMobile NetScaler Connector-Konfiguration (bestehend aus einigen XML-Dateien) ist in einem einzigen Ordner. Der XenMobile NetScaler Connector-Prozess erkennt Änderungen an jeder Datei in diesem Ordner und lädt die Konfiguration dann automatisch neu. Im Modus mit Freigabe gibt kein Failover für den primären Knoten. Bei einem Ausfall des primären Servers (z. B. durch Neustart) besteht jedoch einige Minuten lang Fehlertoleranz, da die letzte funktionsfähige Konfiguration im XenMobile NetScaler Connector-Prozess zwischengespeichert ist.

Systemanforderungen für XenMobile NetScaler Connector

Oct 13, 2016

XenMobile NetScaler Connector kommuniziert mit NetScaler über eine auf dem NetScaler-Gerät konfigurierte SSL-Brücke, über die das Gerät sämtlichen sicheren Datenverkehr direkt an XenMobile übergeben kann. Sie können XenMobile NetScaler Connector auf einem eigenen Server oder auf demselben Server wie XenMobile installieren. XenMobile NetScaler Connector erfordert die folgende Mindestsystemkonfiguration:

Komponente	Anforderungen
Computer und Prozessor	733 MHz Pentium III 733 MHz oder schneller 2.0 GHz Pentium III oder schneller (empfohlen)
NetScaler	NetScaler-Gerät mit Softwareversion 10
Memory	1 Gigabyte (GB)
Festplatte	NTFS-formatierte lokale Partition mit 150 MB freiem Speicherplatz
Betriebssystem	Microsoft Windows Server 2008 R2 oder Microsoft Windows Server 2008 SP2 (empfohlen)
Sonstige Geräte	Mit dem Hostbetriebssystem kompatibler Netzwerkadapter für die Kommunikation mit dem internen Netzwerk
Anzeige	VGA-Monitor oder höher

Auf dem Hostcomputer für XenMobile NetScaler Connector ist mindestens folgender freier Festplattenspeicher erforderlich:

- Anwendung: 10-15 MB (100 MB empfohlen)
- Protokollierung: 1 GB (20 GB empfohlen)

Informationen über unterstützte Plattformen für XenMobile NetScaler Connector finden Sie unter Unterstützte Geräteplattformen in XenMobile.

Installieren von XenMobile NetScaler Connector

May 05, 2016

Sie können XenMobile NetScaler Connector auf einem eigenen Server oder auf demselben Server wie XenMobile installieren.

Die Installation von XenMobile NetScaler Connector auf einem eigenen Server könnte sich aus folgenden Gründen anbieten:

- Der XenMobile-Server wird remote in einer Cloud (physischer Speicherort) gehostet.
- Sie möchten nicht, dass XenMobile NetScaler Connector durch Neustarts des XenMobile-Servers beeinträchtigt wird (Verfügbarkeit).
- Sie möchten die Systemressourcen des Servers vollständig für XenMobile NetScaler Connector nutzen (Leistung).

Die durch XenMobile NetScaler Connector auf einem Server verursachte CPU-Last hängt von der Zahl der verwalteten Geräte ab. Als Faustregel gilt jedoch, dass bei einer Bereitstellung von XenMobile NetScaler Connector auf demselben Server wie XenMobile ein zusätzlicher CPU-Kern bereitgestellt werden sollte. Bei hohen Gerätezahlen (über 50.000) müssen Sie möglicherweise zusätzliche Kerne bereitstellen, wenn Sie keine Clusterumgebung haben. Der Speicherbedarf von XenMobile NetScaler Connector ist zu klein, als dass zusätzlicher Speicher erforderlich wäre.

Installieren, Aktualisieren und Deinstallieren von XenMobile NetScaler Connector

May 05, 2016

1. Führen Sie XncInstaller.exe mit einem Administratorkonto aus, um XenMobile NetScaler Connector (XNC) zu installieren bzw. vorhandene Versionen zu aktualisieren oder zu deinstallieren.
2. Folgen Sie den Anweisungen auf dem Bildschirm, um den jeweiligen Vorgang abzuschließen.

Nach der Installation von XenMobile NetScaler Connector müssen Sie den XenMobile-Konfigurationsdienst und den Benachrichtigungsdienst manuell neu starten.

Deinstallieren von XNC

May 05, 2016

1. Führen Sie XncInstaller.exe mit einem Administratorkonto aus.
2. Folgen Sie den Anweisungen auf dem Bildschirm, um die Deinstallation abzuschließen.

Verwalten von XenMobile NetScaler Connector

May 05, 2016

Sie können mit XenMobile NetScaler Connector Zugriffssteuerungsregeln erstellen, durch die ActiveSync-Verbindungsanforderungen von verwalteten Geräten je nach Gerätestatus, App-Sperrlisten bzw. -Positivlisten und andere Richtlinientreuebedingungen blockiert oder zugelassen werden.

Mit dem XenMobile NetScaler Connector-Konfigurationsprogramm können Sie dynamische und statische Regeln zum Erzwingen von Richtlinien für die Unternehmens-E-Mail erstellen, mit denen Benutzer, die die Richtlinien nicht einhalten, blockiert werden. Sie können außerdem die Verschlüsselung von E-Mail-Anlagen einrichten, sodass alle Anlagen, die über Exchange Server an verwaltete Geräte gesendet werden, verschlüsselt werden und nur von autorisierten Benutzern auf verwalteten Geräten angezeigt werden können.

Auswählen eines Sicherheitsmodells für XenMobile NetScaler Connector

May 05, 2016

Permissives Modell (Zulassungsmodus)

Die Implementierung eines Sicherheitsmodells ist für eine erfolgreiche Mobilgerätebereitstellung in Organisationen jeder Größe wichtig. Obwohl es nicht unüblich ist, Zugriffssteuerung mit Schutz oder Quarantäne zu verwenden, um Zugriff auf Benutzer, Computer oder Geräte standardmäßig zuzulassen, ist dies nicht immer empfehlenswert. In jeder Organisation werden bei der Verwaltung der IT-Sicherheit andere ggf. maßgeschneiderte Methoden zum Schutz von Mobilgeräten eingesetzt.

Die gleiche Logik gilt für die Sicherheit von Mobilgeräten. Angesichts der Vielzahl verschiedener Mobilgerätetypen, der großen Zahl Mobilgeräte pro Benutzer und der Vielfalt an Betriebssystemen und Apps erscheint das permissive Modell keine gute Idee. In den meisten Organisationen ist das restriktive Modell die beste Wahl.

Citrix lässt bei der Integration von XenMobile NetScaler Connector und XenMobile folgende Konfigurationsszenarios zu:

Beim permissiven Sicherheitsmodell gilt, dass bei allem der Zugriff standardmäßig zugelassen ist. Nur durch Aufstellen von Regeln und Filtern können Elemente blockiert und Beschränkungen angewendet werden. Das permissive Sicherheitsmodell ist für Organisationen geeignet, die keine strikten Sicherheitsregelungen für Mobilgeräte haben und nur wo erforderlich durch einschränkende Steuerelemente den Zugriff blockieren (wenn eine Richtlinienregel nicht erfüllt wird).

Restriktives Modell (Blockierungsmodus)

Beim restriktiven Sicherheitsmodell gilt, dass bei nichts der Zugriff standardmäßig zugelassen ist. Alle Elemente werden bei der Sicherheitsprüfung gefiltert und untersucht. Der Zugriff wird blockiert, außer wenn die Regeln für die Zulassung des Zugriffs erfüllt werden. Das restriktive Sicherheitsmodell ist für Organisationen geeignet, in denen relativ strenge Sicherheitsvorschriften hinsichtlich der Mobilgeräte herrschen. Bei diesem Modell wird der Zugriff nur gewährt, wenn alle Regeln für das Zulassen des Zugriffs erfüllt werden.

Konfigurieren von XenMobile NetScaler Connector

May 05, 2016

Sie können XenMobile NetScaler Connector für die selektive Blockierung oder Zulassung von ActiveSync-Anforderungen basierend auf folgenden Eigenschaften konfigurieren: Active Sync Service ID, Device type, User Agent (Gerätebetriebssystem), Authorized user und ActiveSync Command.

Die Standardkonfiguration unterstützt eine Kombination aus statischen und dynamischen Gruppen. Statische Gruppen werden mit dem Konfigurationsprogramm des Secure Mobile Gateway-Controllers verwaltet. Statische Gruppen können aus bekannten Gerätekategorien bestehen, z. B. alle Geräte mit einem bestimmten Benutzer-Agent.

Dynamische Gruppen werden von einer externen Quelle, dem Gateway-Konfigurationsanbieter, gepflegt und von XenMobile NetScaler Connector regelmäßig gesammelt. XenMobile kann Gruppen zugelassener und blockierter Geräte und Benutzer in XenMobile NetScaler Connector exportieren.

Eine Richtlinie ist eine sortierte Liste von Gruppen, in der jeder Gruppe eine Aktion (zulassen oder blockieren) zugeordnet ist, und eine Liste der Gruppenmitglieder. Eine Richtlinie kann beliebig viele Gruppen enthalten. Die Reihenfolge der Gruppen in einer Richtlinie ist wichtig, weil bei einer Übereinstimmung die Aktion der Gruppe erfolgt und nachfolgende Gruppen nicht ausgewertet werden.

Mitglieder sind eine Methode für die Zuordnung der Eigenschaften einer Anforderung. Sie können einer einzelnen Eigenschaft (z. B. Geräte-ID) oder mehreren Eigenschaften entsprechen (z. B. Gerätetyp und Benutzer-Agent).

Konfigurieren von Richtlinienmodi für XenMobile NetScaler Connector

May 05, 2016

XenMobile NetScaler Connector kann in folgenden sechs Modi ausgeführt werden:

- Allow All: In diesem Richtlinienmodus erhält der gesamte XenMobile NetScaler Connector passierende Datenverkehr Zugriff. Es werden keine anderen Filterregeln verwendet.
- Deny All: In diesem Richtlinienmodus wird der gesamte XenMobile NetScaler Connector passierende Datenverkehr blockiert. Es werden keine anderen Filterregeln verwendet.
- Static Rules: Block Mode: In diesem Richtlinienmodus werden statische Regeln mit einer impliziten Blockieren-Anweisung am Ende ausgeführt. Geräte, die nicht über andere Filterregeln zugelassen werden, werden von XenMobile NetScaler Connector blockiert.
- Static Rules: Permit Mode: In diesem Richtlinienmodus werden statische Regeln mit einer impliziten Zulassen-Anweisung am Ende ausgeführt. Geräte, die nicht über andere Filterregeln blockiert werden, werden von XenMobile NetScaler Connector zugelassen.
- Static + ZDM Rules: Block Mode: In diesem Richtlinienmodus werden statische Regeln und anschließend dynamische Regeln mit einer impliziten Blockieren-Anweisung am Ende ausgeführt. Geräte werden basierend auf Filtern und Device Manager-Regeln zugelassen oder blockiert. Alle Geräte, die keinem Filter und keiner Regel entsprechen, werden blockiert.
- Static + ZDM Rules: Permit Mode: In diesem Richtlinienmodus werden statische Regeln und anschließend dynamische Regeln mit einer impliziten Zulassen-Anweisung am Ende ausgeführt. Geräte werden basierend auf Filtern und XenMobile-Regeln zugelassen oder blockiert. Alle Geräte, die keinem Filter und keiner Regel entsprechen, werden zugelassen.

Die Ausführung dynamischer Regeln durch den XenMobile NetScaler Connector-Prozess basiert auf eindeutigen ActiveSync-Kennungen von iOS- und Windows-Mobilgeräten, die von XenMobile empfangen werden. Bei Android-Geräten ist das Verhalten je nach Hersteller unterschiedlich, einige stellen ihre eindeutige ActiveSync-ID nicht einfach zur Verfügung. Ersatzweise sendet XenMobile für Android-Geräte die Benutzer-ID, damit eine Entscheidung über Zulassen und Blockieren getroffen werden kann. Hat ein Benutzer nur ein Android-Gerät, funktioniert die Zugriffssteuerung daher ordnungsgemäß. Hat ein Benutzer mehrere Android-Geräte, werden alle Geräte zugelassen, da Android-Geräte nicht einzeln unterschieden werden können. Das Gateway kann so konfiguriert werden, dass diese Geräte basierend auf der ActiveSync-Kennung, sofern diese bekannt ist, oder basierend auf Gerätetyp oder Benutzer-Agent statisch blockiert werden.

Zum Festlegen des Richtlinienmodus führen Sie im Konfigurationsprogramm des SMG-Controllers folgende Schritte aus:

1. Klicken Sie auf die Registerkarte Path Filters und dann auf Add.
2. Wählen Sie im Dialogfeld Path Properties aus der Dropdownliste Policy einen Richtlinienmodus aus und klicken Sie auf Save.

Sie können Regeln auf der Registerkarte Policies des Konfigurationsprogramms prüfen. Die Regeln werden in XenMobile NetScaler Connector der Reihe nach von oben nach unten verarbeitet. Die Richtlinien zum Zulassen werden mit einem grünen Häkchen angezeigt. Die Richtlinien zum Verweigern werden mit einem durchgestrichenen roten Kreis angezeigt. Zum Aktualisieren der Anzeige der Regeln klicken Sie auf Refresh. Sie können die Reihenfolge der Regeln auch in der Datei config.xml ändern.

Zum Testen von Regeln klicken Sie auf die Registerkarte Simulator. Geben Sie Werte in den Feldern ein. Diese können auch aus den Protokollen bezogen werden. In einer Ergebnismeldung wird Allow oder Block angezeigt.

Konfigurieren von statischen Regeln

May 05, 2016

Sie müssen statische Regeln mit Werten eingeben, die von dem ISAPI-Filter der HTTP-Anforderung der ActiveSync-Verbindung gelesen werden. Über statische Regeln kann XenMobile NetScaler Connector den Datenverkehr basierend auf folgenden Kriterien zulassen oder blockieren:

- Benutzer: XenMobile NetScaler Connector verwendet die bei der Geräteregistrierung erfasste Struktur aus autorisiertem Benutzerwert und Namen. Dies ist normalerweise "domain\username" gemäß Verweis von dem XenMobile-Server, der mit Active Directory über LDAP verbunden ist. Auf der Registerkarte Log des XenMobile NetScaler Connector-Konfigurationsprogramms werden die durch XenMobile NetScaler Connector gesendeten Werte angezeigt, wenn eine Wertstruktur ermittelt werden muss oder sich unterscheidet.
- Deviceid (ActiveSyncID): wird auch als "ActiveSyncID" des verbundenen Geräts bezeichnet. Dieser Wert ist häufig auf der spezifischen Geräteeigenschaftenseite der XenMobile-Konsole. Er kann auch auf der Registerkarte Log des XenMobile NetScaler Connector-Konfigurationsprogramms gefunden werden.
- DeviceType: XenMobile NetScaler Connector kann feststellen, ob es sich bei einem Gerät um ein iPhone, iPad oder einen anderen Gerätetyp handelt, und Geräte basierend auf diesem Kriterium blockieren oder zulassen. Wie bei anderen Werten kann das XenMobile NetScaler Connector-Konfigurationsprogramm alle verbundenen Gerätetypen, die für die ActiveSync-Verbindung verarbeitet werden, anzeigen.
- UserAgent: enthält Informationen zu dem verwendeten ActiveSync-Client. Meist entspricht der Wert einem bestimmten Betriebssystem-Build-/Versionspaar für die Mobilgeräteplattform.

Das XenMobile NetScaler Connector-Konfigurationsprogramm, das auf dem Server ausgeführt wird, verwaltet immer die statischen Regeln.

1. Klicken Sie im Konfigurationsprogramm des Secure Mobile Gateway-Controllers auf die Registerkarte Static Rules und dann auf Add.
2. Legen Sie im Dialogfeld Static Rule Properties die Werte fest, die Sie als Kriterien verwenden möchten. Beispiel: Um einen Benutzer für den Zugriff zuzulassen, geben Sie dessen Benutzernamen ein (z. B.AllowedUserund deaktivieren Sie dann das Kontrollkästchen Disabled.
3. Klicken Sie auf Speichern. Die statische Regel ist jetzt in Kraft. Zusätzlich können Sie reguläre Ausdrücke zum Definieren von Werten verwenden, Sie müssen jedoch den Regelverarbeitungsmodus in der Datei config.xml aktivieren.

Konfigurieren von dynamischen Regeln

May 05, 2016

Dynamische Regeln werden über Geräterichtlinien und -eigenschaften in Device Manager definiert. Sie können einen dynamischen XenMobile NetScaler Connector-Filter auslösen, der auf dem Verstoß gegen eine Richtlinie oder Eigenschaft basiert. XenMobile NetScaler Connector-Filter analysieren Geräte auf Verstöße gegen bestimmte Richtlinien oder Eigenschaften. Erfüllt ein Gerät die Kriterien, wird es in eine Geräteliste aufgenommen. Diese Geräteliste ist weder eine Liste zum Zulassen oder Blockieren. Es ist lediglich eine Liste der Geräte, die die Kriterien erfüllen. Mit den folgenden Konfigurationsoptionen können Sie festlegen, ob die Geräte in der Geräteliste mit XenMobile NetScaler Connector zugelassen oder blockiert werden sollen.

Hinweis: Diese dynamischen Regeln müssen in der XenMobile-Konsole konfiguriert werden.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **ActiveSync-Gateway**. Die Seite ActiveSync Gateway wird angezeigt.

3. Wählen Sie unter **Folgende Regel(n) aktivieren** eine oder mehrere Regeln aus, die Sie aktivieren möchten.

4. Klicken Sie nur für Android unter **Android-Domänenbenutzer an ActiveSync Gateway senden** auf **JA**, um sicherzustellen, dass XenMobile Android-Geräteinformationen an das Secure Mobile Gateway sendet. Wenn diese Option aktiviert ist, sendet XenMobile Android-Geräteinformationen an den XenMobile NetScaler Connector für den Fall, dass XenMobile den ActiveSync-Bezeichner für den Android-Gerätebenutzer nicht hat.

Konfigurieren von benutzerdefinierten Richtlinien durch Bearbeiten der XML-Datei von XenMobile NetScaler Connector

May 05, 2016

Sie können die grundlegenden Richtlinien der Standardkonfiguration auf der Registerkarte Policies des XenMobile NetScaler Connector-Konfigurationsprogramms anzeigen. Zum Erstellen benutzerdefinierter Richtlinien können Sie die XML-Konfigurationsdatei von XenMobile NetScaler Connector (config\config.xml) bearbeiten.

1. Suchen Sie in der Datei den Abschnitt "PolicyList" und fügen Sie diesem ein neues Policy-Element hinzu.
2. Wenn eine neue Gruppe erforderlich wird, z. B. eine zusätzliche statische Gruppe oder eine Gruppe für eine zusätzliche GKP, fügen das neue Group-Element dem Abschnitt "GroupList" hinzu.
3. Falls gewünscht, können Sie die Reihenfolge der Gruppen in einer vorhandenen Richtlinie durch Umstellen der GroupRef-Elemente ändern.

Konfigurieren der XML-Datei von XenMobile NetScaler Connector

May 05, 2016

Die Aktionen von XenMobile NetScaler Connector werden über eine XML-Konfigurationsdatei gesteuert. Unter anderem enthält die Datei die Dateigruppe und zugehörige Aktionen für den Filter bei der Auswertung von HTTP-Anforderungen. Standardmäßig heißt die Datei config.xml und ist in folgendem Verzeichnis: \Programme\Citrix\XenMobile NetScaler Connector\config\.

Die GroupRef-Knoten definieren die logischen Gruppennamen: standardmäßig "AllowGroup" und "DenyGroup".
Hinweis: Die Reihenfolge der GroupRef-Knoten im GroupRefList-Knoten spielt eine Rolle.
Der ID-Wert eines GroupRef-Knotens identifiziert einen logischen Container bzw. eine Mitgliedersammlung, der bzw. die für die Zuordnung spezifischer Benutzerkonten oder Geräte verwendet wird. Die Action-Attribute geben an, wie ein Mitglied zu behandeln ist, das einer Regel in der Sammlung entspricht. Beispiel: Ein Benutzerkonto oder Gerät, das einer AllowGroup-Regel entspricht, wird zugelassen (d. h. es erhält Zugriff auf den Exchange-CAS) und ein Benutzerkonto oder Gerät, das einer DenyGroup-Regel entspricht, wird blockiert (d. h. es erhält keinen Zugriff auf den Exchange-CAS).

Entspricht ein bestimmtes Benutzerkonto/Gerät oder eine Konto-/Gerätekombination Regeln beider Gruppen, erfolgt die Behandlung gemäß einer Rangfolgenkonvention. Die Rangfolge entspricht der Reihenfolge der GroupRef-Knoten in der Datei config.xml von oben nach unten. Die GroupRef-Knoten werden nach Priorität gewichtet. Regeln für eine bestimmte Bedingung in der Allow-Gruppe haben immer Vorrang vor Regeln für die gleiche Bedingung in Deny-Gruppe.

In der Datei config.xml sind außerdem Gruppenknoten definiert. Diese Knoten verknüpfen die logischen Container "AllowGroup" und "DenyGroup" mit externen XML-Dateien. Einträge in den externen Dateien bilden die Basis für die Filterregeln.
Hinweis: In diesem Release werden nur externe XML-Dateien unterstützt.
In der Standardinstallation sind zwei XML-Dateien in der Konfiguration implementiert: allow.xml und deny.xml.

Importieren einer Richtlinie von XenMobile

May 05, 2016

1. Klicken Sie im XenMobile NetScaler Connector-Konfigurationsprogramm auf die Registerkarte Config Providers und dann auf Add.
2. Geben Sie im Dialogfeld Config Providers unter Name den Benutzernamen eines Kontos mit Administratorrechten ein, das für die grundlegende HTTP-Autorisierung auf dem XenMobile-Server verwendet werden soll.
3. Geben Sie unter Url die Webadresse von XenMobile-Gateway Configuration Service (GCS) ein, das Format ist in der Regel https://xdmHost/xdm/services/MagConfigService. Bei dem Namen von MagConfigservice wird Groß-/Kleinschreibung unterschieden.
4. Geben Sie unter Password das Kennwort des Kontos mit Administratorrechten ein, das für die grundlegende HTTP-Autorisierung auf dem XenMobile-Server verwendet werden soll.
5. Klicken Sie auf Test Connectivity, um die Verbindung zwischen Gateway und Konfigurationsanbieter zu testen. Wenn die Verbindung fehlschlägt, überprüfen Sie, ob die lokalen Firewalleinstellungen die Verbindung gestatten, oder wenden Sie sich an den Administrator.
6. Kann die Verbindung hergestellt werden, deaktivieren Sie das Kontrollkästchen Disabled und klicken Sie dann auf Save.
7. Behalten Sie unter Managing Host den Standard-DNS-Namen des lokalen Hostcomputers bei. Diese Einstellung wird für die Koordination der Kommunikation mit XenMobile verwendet, wenn mehrere Forefront Threat Management Gateway-Server in einem Array konfiguriert sind.

Nach dem Speichern der Einstellungen öffnen Sie Gateway Configuration Service.

Konfigurieren einer Verbindung mit XenMobile NetScaler Connector

May 05, 2016

XenMobile NetScaler Connector kommuniziert mit XenMobile und anderen Remote-Konfigurationsanbietern über sichere Webdienste.

1. Klicken Sie im XenMobile NetScaler Connector-Konfigurationsprogramm auf die Registerkarte Config Providers und dann auf Add.
2. Geben Sie im Dialogfeld Config Providers unter Name den Benutzernamen eines Kontos mit Administratorrechten ein, das für die grundlegende HTTP-Autorisierung auf dem XenMobile-Server verwendet werden soll.
3. Geben Sie unter Url die Webadresse des XenMobile-GCS ein, das Format ist in der Regel https://ZdmHost/zdm/services/MagConfigService. Bei dem Namen von MagConfigservice wird Groß-/Kleinschreibung unterschieden.
4. Geben Sie unter Password das Kennwort des Kontos mit Administratorrechten ein, das für die grundlegende HTTP-Autorisierung auf dem XenMobile-Server verwendet werden soll.
5. Geben Sie unter Managing Host den XenMobile NetScaler Connector-Servernamen ein.
6. Geben Sie unter Baseline Interval das Intervall ein, in dem von Device Manager der aktualisierte Satz dynamischer Regeln abgerufen werden soll.
7. Geben Sie unter Delta Interval das Intervall ein, in dem von Device Manager Aktualisierungen an den dynamischen Regeln abgerufen werden sollen.
8. Geben Sie unter Request Timeout das Timeoutintervall für die Serveranforderungen an.
9. Wählen Sie unter Config Provider die Serverinstanz des Konfigurationsanbieters aus, der die Richtlinienkonfiguration bereitstellt.
10. Aktivieren Sie diese Option unter Events Enabled, wenn XenMobile NetScaler Connector XenMobile die Blockierung eines Geräts melden soll. Die Option ist erforderlich, wenn Sie XenMobile NetScaler Connector-Regeln in XenMobile für eine automatische Aktion verwenden.
11. Klicken Sie auf Save und anschließend auf Test Connectivity, um die Verbindung zwischen Gateway und Konfigurationsanbieter zu testen. Wenn die Verbindung fehlschlägt, überprüfen Sie, ob die lokalen Firewalleinstellungen die Verbindung gestatten, oder wenden Sie sich an den Administrator.
12. Kann die Verbindung hergestellt werden, deaktivieren Sie das Kontrollkästchen Disabled und klicken Sie dann auf Save.

Wenn Sie einen neuen Konfigurationsanbieter hinzufügen, erstellt XenMobile NetScaler Connector automatisch eine oder mehrere diesem Anbieter zugeordnete Richtlinien. Diese Richtlinien werden durch eine Vorlagendefinition im Abschnitt "NewPolicyTemplate" der Datei config\policyTemplates.xml festgelegt. Für jedes Policy-Element in diesem Abschnitt wird eine neue Richtlinie erstellt. Policy-Elemente können hinzugefügt, entfernt oder modifiziert werden, vorausgesetzt, sie entsprechen der Schemadefinition und die Standard-Ersatzzeichenfolgen (in geschweiften Klammern) werden nicht geändert. Fügen Sie als Nächstes neue Gruppen für den Anbieter hinzu und aktualisieren Sie die Richtlinie zur Berücksichtigung der neuen Gruppen.

Auswählen von Filtern für XenMobile NetScaler Connector

May 05, 2016

XenMobile NetScaler Connector-Filter analysieren Geräte auf Verstöße gegen bestimmte Richtlinien oder Eigenschaften. Erfüllt ein Gerät die Kriterien, wird es in eine Geräteliste aufgenommen. Diese Geräteliste ist weder eine Liste zum Zulassen oder Blockieren. Es ist lediglich eine Liste der Geräte, die die Kriterien erfüllen. Die folgenden Filter stehen für XenMobile NetScaler Connector in XenMobile zur Verfügung.

- Blacklisted Apps: Zulassen oder Blockieren von Geräten basierend auf Sperrlistenrichtlinien und dem Vorhandensein gesperrter Apps.
- Whitelisted Apps only: Zulassen oder Blockieren von Geräten basierend auf Positivlistenrichtlinien und dem Vorhandensein nicht in einer Positivliste aufgeführter Apps.
- Unmanaged Devices: erstellt eine Liste aller Geräte in der XenMobile-Datenbank. Das Mobile Application Gateway muss im Modus "Blockieren" bereitgestellt werden.
- Rooted Android /Jailbroken iOS Devices: erstellt eine Liste aller Geräte, die als gerootet markiert wurden, und lässt den Zugriff zu bzw. blockiert ihn auf der Basis des entsprechenden Gerätestatus.
- Out of Compliance Devices: ermöglicht das Zulassen bzw. Blockieren von Geräten auf der Basis der Einhaltung firmeninterner IT-Richtlinien. Die Richtlinientreue ist eine willkürliche Einstellung, die durch die Geräteeigenschaft Out of Compliance definiert ist, einem booleschen Flag, das entweder True oder False sein kann. (Sie können diese Eigenschaft manuell unter Auswahl des Werts erstellen oder mit automatischen Aktionen auf einem Gerät, wenn das Gerät die Kriterien erfüllt bzw. nicht erfüllt.)
  - Out of Compliance = True: Wenn ein Gerät die Vorgaben und Richtliniendefinitionen der IT-Abteilung nicht erfüllt, wird das Gerät als nicht richtlinientreu eingestuft.
  - Out of Compliance = False: Wenn ein Gerät die Vorgaben und Richtliniendefinitionen der IT-Abteilung erfüllt, wird das Gerät als richtlinientreu eingestuft.
- Noncompliant password: erstellt eine Liste aller Geräte ohne Passcode.
- Revoked Status: erstellt eine Liste aller widerrufenen Geräte und lässt den Zugriff zu bzw. blockiert ihn auf der Basis des entsprechenden Gerätestatus.
- Inactive devices: erstellt eine Liste von Geräten, die innerhalb eines bestimmten Zeitraums nicht mit XenMobile kommuniziert haben und daher als inaktiv eingestuft werden, und lässt den Zugriff zu bzw. blockiert ihn auf der Basis des entsprechenden Gerätestatus.
- Anonymous Devices: dient zum Zulassen oder Blockieren von Geräten, die bei XenMobile registriert sind, bei denen die Identität des Benutzers jedoch unbekannt ist. Beispielsweise kann dies ein registrierter Benutzer sein, dessen Active Directory-Kennwort abgelaufen ist, oder ein Benutzer, der sich mit unbekannten Anmeldeinformationen registriert hat.
- Implicit Allow / Deny: erstellt eine Liste aller Geräte, die keines der anderen Filterkriterien erfüllen, und lässt den Zugriff zu bzw. blockiert ihn für diese Geräte. Die Option Implicit Allow/Deny gewährleistet, dass der XenMobile NetScaler Connector-Status auf der Registerkarte Devices aktiviert ist und für die Geräte angezeigt wird. Die Option Implicit Allow/Deny steuert zudem alle anderen XenMobile NetScaler Connector-Filter, die nicht ausgewählt wurden. Beispielsweise werden bei Auswahl des entsprechenden Filters Geräte mit der Eigenschaft Blacklisted Apps von XenMobile NetScaler Connector blockiert, für alle anderen Filter gilt die Einstellung "Zulassen", wenn die Option Implicit Allow/Deny auf Allow festgelegt wurde.

Simulieren von ActiveSync-Datenverkehr mit XenMobile NetScaler Connector

May 05, 2016

Sie können XenMobile NetScaler Connector zum Simulieren des ActiveSync-Datenverkehrs unter Ihren Richtlinien verwenden. Klicken Sie im XenMobile NetScaler Connector-Konfigurationsprogramm auf die Registerkarte Simulations. Das Ergebnis zeigt, wie Ihre Richtlinien nach den von Ihnen konfigurierten Regeln angewendet werden.

Überwachen von XenMobile NetScaler Connector

May 05, 2016

Das XenMobile NetScaler Connector-Konfigurationsprogramm bietet eine detaillierte Protokollierung, anhand derer Sie den gesamten von Secure Mobile Gateway zugelassenen bzw. blockierten Datenverkehr über den Exchange-Server überwachen können.

Auf der Registerkarte Log wird der Verlauf der von NetScaler zur Autorisierung an XenMobile NetScaler Connector weitergeleiteten ActiveSync-Anforderungen angezeigt.

Außerdem können Sie die Ausführung des XenMobile NetScaler Connector-Webdiensts prüfen, indem Sie die folgende URL in einen Browser auf dem XenMobile NetScaler Connector-Server eingeben: http:///services/ActiveSync/Version. Wird die Produktversion als Zeichenfolge zurückgegeben, wird der Webdienst ausgeführt.