XenMobile Server 10.3.x

Oct 13, 2016

Info zu XenMobile Server 10.3.6

Oct 13, 2016

Sie können ein direktes Upgrade auf XenMobile 10.3.6 Service Pack nur von XenMobile 10.3.5 aus durchführen.

> ## Hinweis
>
> Vor dem Upgrade auf XenMobile 10.3.6 müssen Sie sicherstellen, dass das Subscription Advantage-Datum Ihrer Citrix Lizenz nach dem 1. Juni 2016 liegt. Das SA-Datum steht neben der Lizenz auf dem Lizenzserver. Zum Verlängern der SA-Lizenz laden Sie die aktuelle Lizenzdatei vom Citrix Portal herunter und laden Sie sie auf den Lizenzserver hoch. Weitere Informationen finden Sie unter http://support.citrix.com/article/CTX209580.

Für das Upgrade verwenden Sie xms_10.3.6.310.bin. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben und dann auf **Releasemanagement**. Klicken Sie auf **Upgrade** und laden Sie dann die Datei xms_10.3.6.310.bin hoch. Weitere Informationen über Upgrades in der Konsole finden Sie unter Aktualisieren von XenMobile.

Anweisungen für eine neue Installation von XenMobile 10.3.6 finden Sie unter Installieren von XenMobile.

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 in XenMobile 10.3.6

Beim XenMobile 10.3.6 Release liegt der Fokus auf Qualität und Skalierbarkeit. Weitere Informationen zu den behobenen Problemen finden Sie unter Bekannte und behobene Probleme in XenMobile 10.3.6. XenMobile 10.3.6 enthält außerdem die folgenden neuen Features:

Die beträchtlichen Qualitätsverbesserungen auf dem XenMobile 10.3.6-Server führen zu besserer Leistung und Skalierbarkeit in Bereichen wie der Kommunikation zwischen XenMobile-Server und -datenbanken, bei der XenApp-Integration sowie bei Bereitstellungsbenachrichtigungen für Geräte und LDAP-Lookups.

- HDX-Enumeration wurde um ca. 40 % gegenüber XenMobile 10.3.5 verbessert.
- Wenn Sie den Befehl **Server Tuning** im Hauptmenü von XenMobile CLI (Option **5** unter **Erweiterte Einstellungen**) verwenden, werden nun im Vergleich zur Vorversion die folgenden Standardeinstellungen angewendet:

  Maximale Verbindungen auf Port 443: Der Standardwert wurde von **10000** auf **12000** erhöht.

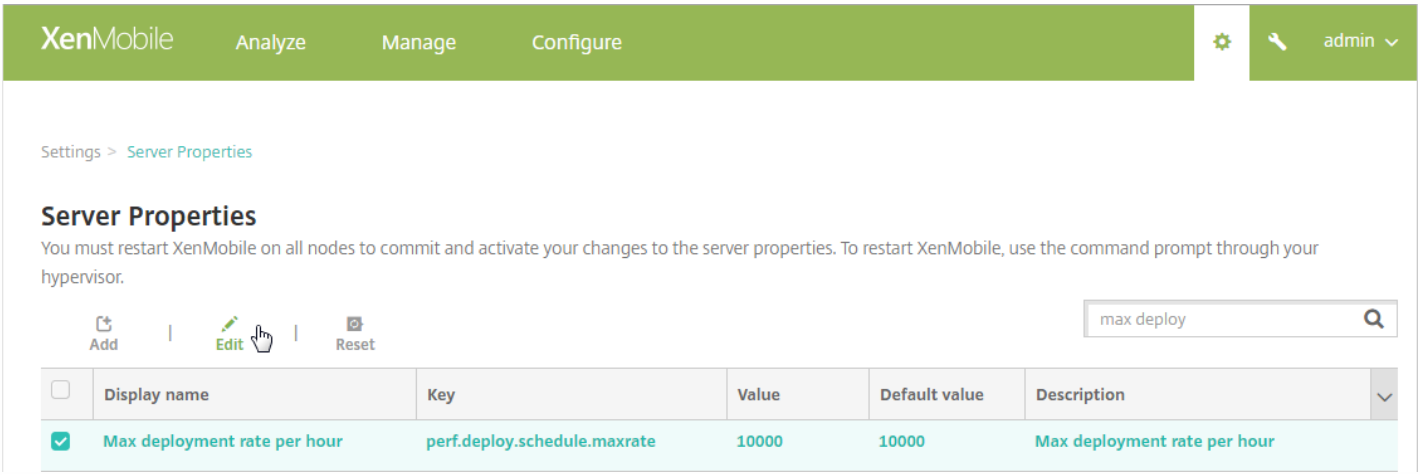
  Maximale Verbindungen auf Port 8443: Der Standardwert wurde von **10000** auf **12000** erhöht.

  Maximale Threads auf Port 443: Der Standardwert wurde von **750** auf **2000** erhöht.

  Maximale Threads auf Port 8443: Der Standardwert wurde von **750** auf **2000** erhöht.

- XenMobile sendet nun Benachrichtigungen in Phasen, um Spitzen bei Wiederverbindungsanforderungen von iOS- und Windows Phone-Geräten sowie bei für Google Cloud Messaging konfigurierten Android-Geräten zu vermeiden. Die

Bereitstellungsrate ist standardmäßig 10.000 Geräte pro Stunde. Wenn Sie die Bereitstellungsrate ändern möchten, bearbeiten Sie die Servereigenschaft **Max deployment rate** (perf.deploy.schedule.maxrate).



- XenMobile-Bereitstellungen werden nun zielgerichteter ausgeführt, da nur die Geräte bereitgestellt werden, die zu den Zielbereitstellungsgruppen gehören. Zuvor wurden alle Geräte bereitgestellt, unabhängig von der Rolle.

Worx Home

- **Protokolle mit WorxMail senden:** Wenn Benutzer zum Melden von Problemen Protokolle senden, wird WorxMail jetzt standardmäßig geöffnet. Auf diese Weise können Benutzer große Dateien problemlos senden. In früheren Versionen von Worx Home schlug das Senden großer Dateien gelegentlich fehl.

WorxMail

- **Unterstützung für Exchange Server 2016:** Sie können WorxMail jetzt mit Exchange Server 2016 integrieren. Active Sync 14 wird unterstützt, WorxMail sollte aber auch mit Active Sync 16 kompatibel sein.
- **Dateien von ShareFile (Android) anfügen:** Benutzer tippen auf **Von ShareFile anfügen**, um Dateien an E-Mails oder Kalenderereignisse anzufügen.
- **Dateien von eingeschränkten ShareFile StorageZones und Connectors (iOS) anfügen:** Mit der Option **Von ShareFile anfügen** in einer E-Mail oder einem Kalenderereignis können Benutzer Dateien nicht nur von ShareFile anfügen, sondern auch von eingeschränkten StorageZones und Connectors, wie SharePoint und Netzwerkfreigaben.
- **Kontaktdaten mit vCard-Dateien teilen:** Benutzer können Kontaktinformationen aus Anlagen importieren, die als Dateien mit der Erweiterung .vcard gesendet wurden.
- **Neuer Standard für Netzwerkzugriff:** Die Standardeinstellung für die Richtlinie **Netzwerkzugriff** im MDX Toolkit ist nun **Tunnel zum internen Netzwerk**. Durch diese Änderung sollen Konfigurationsfehler reduziert werden.

WorxWeb

- **Popups standardmäßig blockieren:** Wenn Popups für Safari standardmäßig blockiert werden sollen, legen Sie auf der XenMobile-Konsole für die Geräterichtlinie **Einschränkungen** die Option **Popups blockieren** auf **Ein** fest. Wenn **Popups blockieren** vor dem Upgrade auf Version 10.3.6 auf **Aus** festgelegt war, bleibt die Einstellung deaktiviert. Ansonsten ist die Einstellung auf **Ein** festgelegt und Popups werden in Safari blockiert.
- **Links in ShareFile öffnen:** In ShareFile 4.0 können Benutzer wählen, ob Sie Links in einem Browser oder direkt in ShareFile öffnen.

WorxChat Tech Preview

- **Unterstützung für Android:** WorxChat ist jetzt auf Android verfügbar.
- **Unterstützung für Lync 2013 und Skype for Business 2015**: Sie können WorxChat jetzt mit Lync 2013 und Skype for Business 2015 im gleichen Pool integrieren.

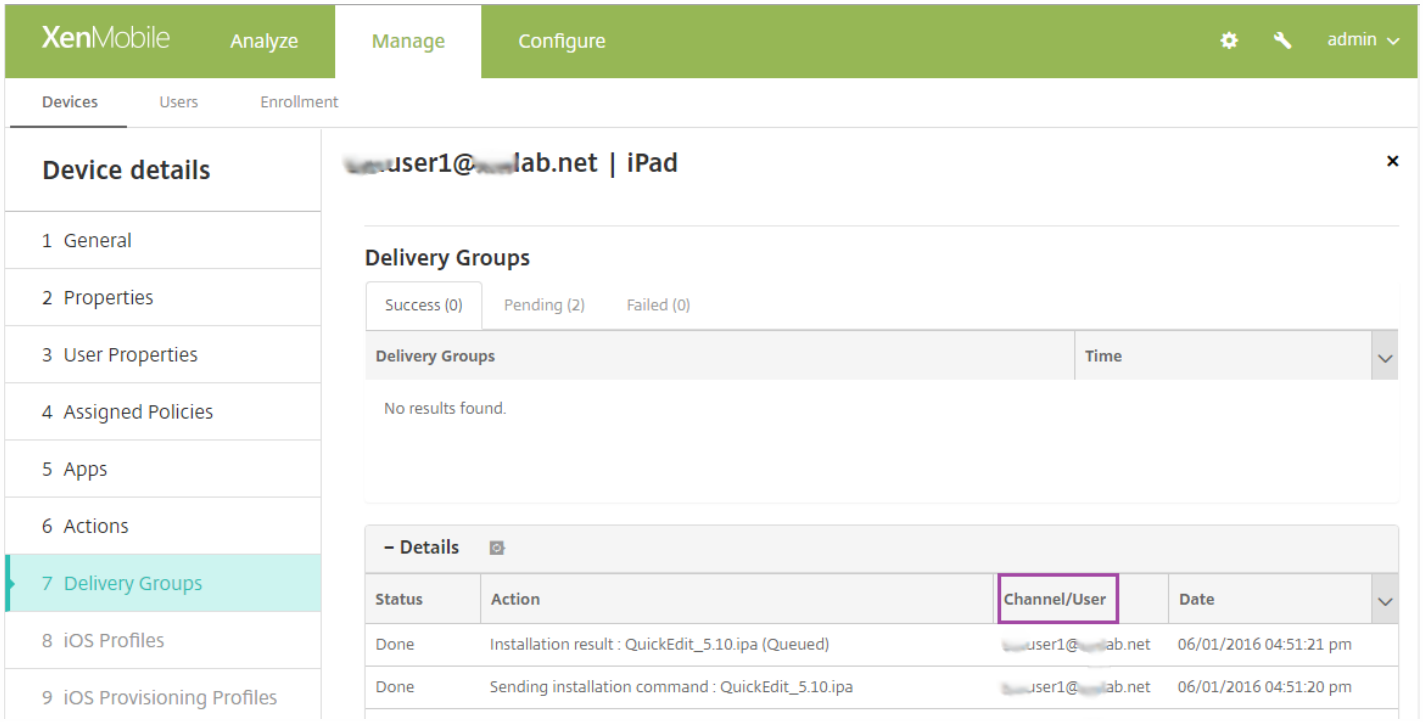
Secure Forms

- **Unterstützung für eingeschränkte ShareFile-Zonen:** Sie können Secure Forms jetzt mit eingeschränkten ShareFile-Zonen konfigurieren. Folgen Sie den Setupanleitungen unter Integrieren von Secure Forms mit ShareFile.
- **iBeacon-Funktion:** Mit der iBeacon-Technologie können Sie Beacons konfigurieren und verfolgen und Benutzern damit ermöglichen, Formulare in der mobilen App automatisch auszufüllen. Die Beaconinformationen sind enthalten, wenn Benutzer Formulare übermitteln. Weitere Informationen zum Einrichten von Beacons finden Sie unter Beacons.
- **Name des Erstellers:** Der Secure Forms Composer zeigt jetzt den Namen der Person an, die ein Formular erstellt hat. Dieses Feature erleichtert die Nachverfolgung, wenn mehrere Benutzer Zugriff auf den Composer haben.
- **Nummernbereiche:** Im Feld **Number** des Composers können Sie einen Zahlenbereich angeben, den Benutzer beim Ausfüllen von Formularen verwenden.
- **Neues Dateienamenformat:** Formulare und Anlagen, die mit der mobilen App übermittelt werden, werden mit dem Namen des Übermittlers und einem Zeitstempel gespeichert, sodass die Dateinamen nun einfacher gelesen und organisiert werden können.

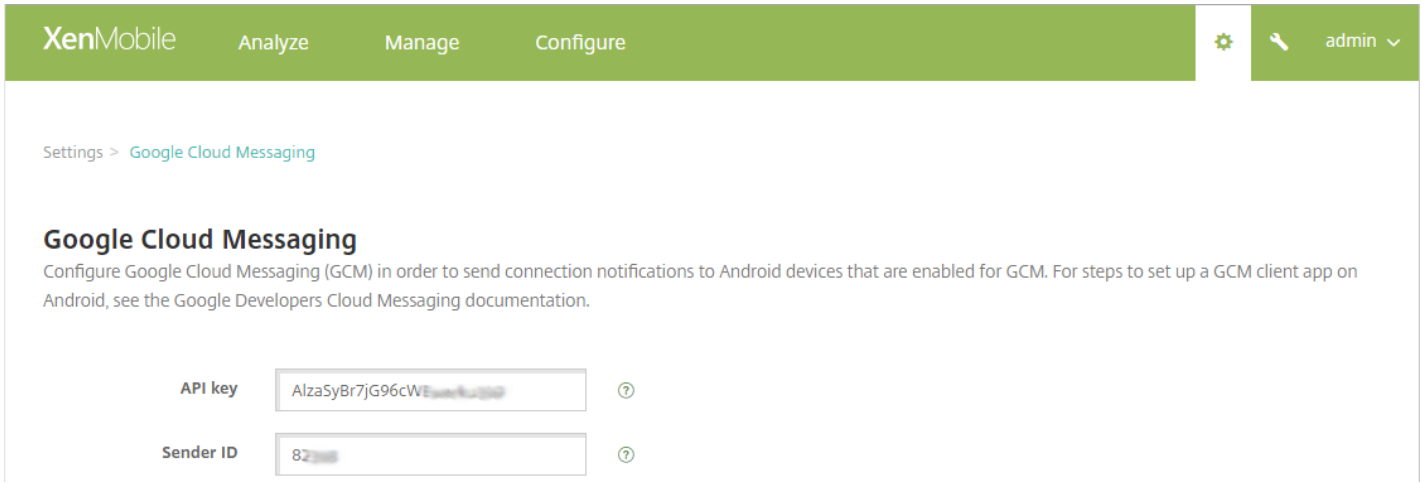
Weitere Informationen finden Sie unter Neue Features in Worx Mobile Apps.

- **Unterstützung für weitere Citrix Komponentenversionen:**
  - NetScaler Gateway 10.5.x, 11.0.x und 11.1.x (lokales XenMobile)
  - NetScaler Gateway 10.5.57.7 (XenMobile Cloud)
  - XenApp und XenDesktop 7.9 und 7.8
  - StoreFront 3.6
  - Lizenzserver 11.13.1.2
- **Positivliste mit WiFi-Netzwerken:** Mit der Richtlinie für die Positivliste mit WiFi-Netzwerken können Sie zulässige Netzwerke angeben. Apps funktionieren nur, wenn eine Verbindung mit einem der in der Liste aufgeführten Netzwerke besteht. Dieses Feature ist nur im MDM+MAM-Modus verfügbar.
- **ShareFile-Unterstützung für gemeinsam genutzte Geräte:** Die ShareFile Mobile App Version 4.4 unterstützt nun gemeinsam genutzte Geräte im MDM+MAM-Modus, sodass mehrere Benutzer ein Gerät gemeinsam verwenden können, ohne sich erneut anzumelden. Weitere Informationen finden Sie unter Gemeinsam genutzte Geräte in XenMobile.
- **Handhabung von Symbolen (iOS):** App-Entwickler können Symboldateien nun im Stammordner des App-Bündels statt in info.plist platzieren. Damit das Toolkit die Symboldateien findet, müssen ihre Namen eines der folgenden Formate haben:
  - icon.png
  - icon-60x2.pn
  - icon-72.png
  - icon-76.png
- **Verbesserte Synchronisierung von E-Mails (iOS):** Durch Aktualisierungen bei der E-Mail-Synchronisierung und ShareFile-Integration ist die E-Mail-Synchronisierung nun zuverlässiger.
- **Zusätzliche Geräteinformationen:** Die Seite **Gerätedetails** in der XenMobile-Konsole enthält jetzt die Spalte **Kanal/Benutzer**, die das Ziel einer Bereitstellungsaktion auf dem Gerät anzeigt. Das Ziel kann der Benutzer sein, der das Gerät registriert hat, ein eingecheckter Benutzer auf einem gemeinsam genutzten Gerät oder Systemeinstellungen bzw.

Bereitstellungsaktionen, die nicht an einen bestimmten Benutzer gebunden sind. Mit diesen Informationen können Sie den Bereitstellungsvorgang besser verfolgen, besonders, wenn viele Benutzer ein Gerät oder viele Container auf einer bestimmten Plattform wie Mac OS X handhaben.



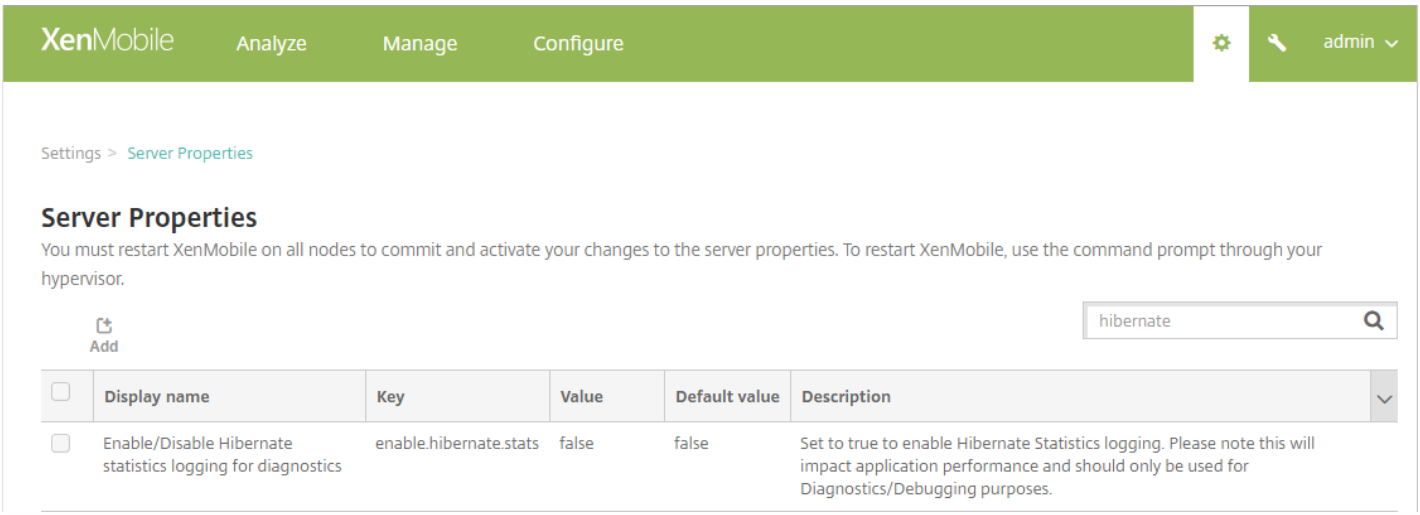
- **Neue Seite in der XenMobile-Konsole:** Die XenMobile-Konsole enthält eine neue Seite unter **Einstellungen > Google Cloud Messaging**, wo Sie den **API-Schlüssel** und die **Absender-ID** für GCM festlegen. Zuvor gab es diese Elemente nur in den **Servereigenschaften**.



- **Protokollierung der Ruhezustandsstatistiken für die Diagnose:** XenMobile bietet nun einen Protokollierungsbericht für die Statistiken des Ruhezustands, eine Komponente für XenMobile-Verbindungen mit Microsoft SQL Server, um Leistungsprobleme der Anwendung zu beheben.

  Sie aktivieren die Protokollierung der Ruhezustandsstatistiken, indem Sie die Servereigenschaft zum Aktivieren/Deaktivieren der Protokollierung der Ruhezustandsstatistiken für die Diagnose (enable.hibernate.stats) auf

true festlegen. Standardmäßig ist die Protokollierung deaktiviert, da sie sich auf die Leistung auswirkt. Aktivieren Sie die Protokollierung nur für kurze Zeit, um das Erstellen einer großen Protokolldatei zu vermeiden. XenMobile schreibt die Protokolle in das Verzeichnis /opt/sas/logs/hibernate_stats.log.



- **Updates im Android-App-Store:** Der Android-App-Store zeigt nur eine aktualisierte App-Version an, wenn die auf dem Android-Gerät installierte Version älter ist als die Version im App-Store.
- **XenMobile Analyzer:** Wenn Sie sich bei einem Problem mit der XenMobile-Umgebung an den Citrix Support wenden, kann dies Ihr Unternehmen Zeit und Geld kosten. Mit XenMobile Analyzer können Sie verbreitete Probleme selbst analysieren, bevor Sie sich an den Support wenden. XenMobile Analyzer unterstützt zahlreiche Anwendungsfälle und Bereitstellungsoptionen, darunter MDM, MDM + MAM und MAM-Only, fünf verschiedene Authentifizierungsszenarien und iOS- sowie Android-Umgebungen.

  Mit XenMobile Analyzer haben Sie folgende Möglichkeiten:
  - Überprüfen der Umgebung auf Probleme und Empfehlen von Lösungen. Mit XenMobile Analyzer finden Sie Probleme mit Geräten, der Benutzerregistrierung und der Authentifizierung.
  - Tiefgehende Diagnose anhand schrittweiser Anleitungen.
  - Hinweise auf Tools zum Prüfen der Bereitschaft für WorxMail und der Serververbindungen.
  - Direkter Link zum Citrix Support, falls die Problemlösung nicht gelingt.

  Weitere Informationen finden Sie unter XenMobile Analyzer.
- **XenMobile Autodiscovery:** Bis dato erforderte die Aktivierung von Autodiscovery ein Supportticket. Über das Autodiscovery-Dienstportal können Sie Autodiscovery selbst einrichten. In dem Portal werden Sie durch die Schritte zum Beanspruchen der Domäne und anschließend zum Erstellen von Autodiscovery-Datensätzen geführt. Weitere Informationen finden Sie unter XenMobile Autodiscovery-Dienst.

Bekannte und behobene Probleme in XenMobile 10.3.6

Jul 28, 2016

Die folgenden Probleme sind in XenMobile 10.3.6 bekannt oder wurden behoben:

Bekannte Probleme

Wenn Benutzer versuchen, ihre persönlichen Geräte mit einem Microsoft-Unternehmenskonto zu registrieren, schlägt die Registrierung fehl. [#597037]

Benutzer, die sich bei XenMobile über ein Azure Active Directory-Konto registrieren, können sich auch nach dem Löschen oder Widerrufen des Geräts ohne Autorisierung erneut registrieren. Dies ist ein Drittanbieterproblem. [#628865]

Nach dem Aktualisieren von XenMobile auf 10.3.6 in einer Clusterkonfiguration kann die Registrierung von iOS-Geräten fehlschlagen. Einen Workaround enthält dieser Knowledge-Artikel. [#650061]

Behobene Probleme

XenMobile-Administratoren, die versuchen, auf die XenMobile-Konsole zuzugreifen, werden möglicherweise stattdessen zum XenMobile-Selbsthilfeportal geleitet. Dies kann passieren, wenn XenMobile-Administratorgruppen mit rollenbasiertem Steuerungszugriff erstellt werden und eine Gruppe von einer Active Directory-Organisationseinheit in eine andere verschoben wird. [#585032]

Mit diesem Fix wird sichergestellt, dass die Werte, die ein Benutzer für die Protokollgröße und die Höchstzahl an Backup-Protokolldateien festlegt, richtig in XenMobile konfiguriert werden und der Rollover der Dateien richtig ausgeführt wird. In der XenMobile-Konsole werden die aktualisierten Werte jedoch u. U. nicht angezeigt, wie im bekannten Problem #551199 erläutert. [#597772]

In XenMobile-Editionen, die MDM und MAM umfassen, werden iOS-Geräte nicht immer vollständig registriert. Das Gerät ist u. U. für MDM registriert, aber nicht für MAM, oder es ist für MAM registriert, jedoch nicht für MDM. [#610847]

Wenn Sie eine Exchange ActiveSync-Geräterichtlinie für Windows konfigurieren und in den Bereitstellungsregeln die Option **Nur bei Fehler in der vorherigen Bereitstellung** ausgewählt wird, tritt das folgende Problem auf: Wenn Windows Phone-Benutzer den E-Mail-Synchronisierungszeitraum für Exchange Server ändern, wird die Änderung des Benutzers überschrieben, wenn XenMobile das nächste Mal eine Exchange ActiveSync-Richtlinie per Push auf dem Windows-Gerät bereitstellt. [#616725]

Wenn Sie in einer Datenbank mit einer großen Datenmenge nach einem Gerät oder Benutzer in der XenMobile-Konsole suchen, führt dies zu einer Spitze bei der CPU-Auslastung auf dem SQL Server und die Suche dauert u. U. mehr als 1 Minute. [#618371]

Wenn Benutzer von iOS-Geräten sich in Worx Home registrieren, reagiert Worx Home gelegentlich bis zu zwei Minuten lang nicht, bevor Benutzer aufgefordert werden, eine Worx-PIN zu erstellen. Wenn dieses Problem auftritt und Benutzer dann den WorxStore öffnen, reagiert Worx Home erneut nicht mehr. [#619945]

Das Senden von SMS-Benachrichtigung vom XenMobile-Server zu Geräten, auf denen Windows 10 ausgeführt wird, schlägt möglicherweise fehl. [#621229]

Wenn Sie eine untergeordnete Active Directory-Gruppe einer übergeordneten Gruppe mit mehr als 1.500 Mitglieder hinzufügen, werden Aktionen, die Sie in der XenMobile-Konsole ausführen, z. B. das Zuweisen von Bereitstellungsgruppen, nicht auf die Benutzer in der hinzugefügten untergeordneten Gruppe angewendet. [#622523]

Nach dem Registrieren von iOS-Geräten werden Benutzer nicht aufgefordert, die erforderlichen Anwendungen zu installieren, bis sie den WorxStore öffnen oder versuchen, eine App manuell hinzufügen. [#622789]

Benutzer können sich bei Worx Home nicht authentifizieren, wenn nach einem Upgrade von XenMobile 9.0 auf XenMobile 10.1 die LDAP-Option "Benutzersuche nach" auf "sAMAccountName" festgelegt und anschließend ein Upgrade auf XenMobile 10.3.x ausgeführt wurde. [#624340]

Richtlinienbereitstellungen und RBAC-Rollenzuweisung können fehlschlagen, wenn für einen Benutzer die explizite UPN nicht mit der impliziten UPN übereinstimmt. [#624612]

In geclusterten Serverbereitstellungen können Probleme in Hazelcast mit der verteilten Zuordnung und der Konnektivität mit dem SQL-Server dazu führen, dass der XenMobile-Server gelegentlich nicht mehr reagiert, sodass Anmeldungen und Registrierungen fehlschlagen. [#624931]

Wenn ein Android-Gerät zum ersten Mal eine Verbindung mit dem XenMobile-Server herstellt oder eine Wiederverbindung erfolgt, ist der Download von Android-Apps langsam oder schlägt fehlt. [#625199]

Benutzern von Worx Home 10.3 wird u. U. die App-Liste nicht angezeigt, wenn der XenMobile-Konsole eine öffentliche App hinzugefügt wird, deren Name oder Beschreibung das ASCII-Zeichen 16 (das Escapezeichen für Datenzeilen) enthält. [#627059]

Geclusterte Server reagieren gelegentlich nicht mehr, wenn eine verteilte Hazelcast-Zuordnung implementiert wurde. [#627114]

Wenn zwei Serverinstanzen auf XenMobile 10.3 aktualisiert und eine Zeit lang ausgeführt wurden, reagiert der erste Server nicht mehr. [#628270]

Nach einer erfolgreichen Registrierung können iOS-Geräte sich manchmal nicht bei WorxStore anmelden und die folgende Meldung wird angezeigt: "Unable to fetch the required assets to continue. Please try again." Dieses Problem tritt auf, weil der XenMobile-Server das Gerät nicht anhand der MAM-Geräte-ID findet. [#629900]

Geräte, die aus der XenMobile-Konsole gelöscht wurden, lassen weiterhin Zugriff auf MAM-Ressourcen zu. [#630137]

Gelegentlich wird selektives Löschen auf iOS-Geräten ausgeführt. [#630466]

In XenMobile 10.3.x werden in der Kategorienansicht von Worx Home keine HDX-Apps angezeigt. Der Ordner "Sonstiges", der HDX-Apps standardmäßig in der Kategorienansicht früherer XenMobile-Versionen enthielt, wird möglicherweise nicht angezeigt. [#631439]

Wenn Benutzer ein Gerät registrieren, ist die MDM-Registrierung erfolgreich, aber bei der MAM-Registrierung tritt gelegentlich ein Fehler auf und die Apps werden gesperrt. [#632073]

Android-Apps, die mit Android SDK-Version 22 oder höher kompiliert oder mit Dexguard schwach verschlüsselt werden, werden nicht in XenMobile hochgeladen. [#632146]

Gelegentlich werden Benutzer nach der Registrierung in Worx Home dazu aufgefordert, Worx Home zu deinstallieren und neu zu installieren. [#633095]

Wenn Sie einen selektiven oder vollständigen Löschvorgang durchführen oder mit der XenMobile-Konsole ein Konto oder Gerät löschen, werden die VPP-Lizenzen für die Apps, die auf dem Gerät konfiguriert waren, gelegentlich nicht freigegeben. [#633366]

Einige VPP-Lizenzen haben negative IDs, z. B. -123441212. In diesem Fall können Sie die öffentlichen Apps nicht bereitstellen. [#631443]

Wenn Benutzer ein Gerät registrieren, stürzt Worx Home manchmal mit einer 403 Fehlermeldung ab und meldet, dass der App-Store gesperrt ist. Es kann auch vorkommen, dass Benutzer sich erfolgreich registrieren, aber dass dann beim Herunterladen einer App der gleiche Fehler auftritt oder in einer Fehlermeldung angezeigt wird, dass Details nicht abgerufen werden können. [#633515]

Wenn Benutzer versuchen, für Windows-basierte Geräte eine WiFi-Geräterichtlinie mit einem gemeinsamen Schlüssel in der XenMobile-Konsole zu konfigurieren und sie ändern den Authentifizierungstyp in WPA (Persönlich) oder WPA-2 (Persönlich), wird die Option für den gemeinsamen Schlüssel nicht wie erwartet angezeigt. [#633897]

Wenn ein NetScaler als Weiterleitungsproxy konfiguriert ist, geben die Konnektivitätsprüfungen in XenMobile 10.3 falsche Ergebnisse zurück. [#633902]

Nach dem Upgrade auf XenMobile 10.3.5 sind Geräte nicht mehr im MAM-Modus registriert. Darüber hinaus schlägt die Bereitstellungen von Richtlinien und Apps für Geräte fehl, die im MDM+MAM-Modus registriert sind. [#634034]

In XenMobile-Editionen, die MDM und MAM umfassen, schlägt die MAM-Authentifizierung bei autorisierten DEP-Geräten möglicherweise fehl, wenn für das Suchfeld "Benutzer" in den LDAP-Einstellungen samAccountName festgelegt ist. Die Worx Home-Registrierung wird daher möglicherweise nicht abgeschlossen und das Gerät wird u. U. nur im MDM registriert. [#637599]

Skalierbarkeit und Leistung von XenMobile

Oct 13, 2016

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.

Die Angaben in diesem Artikel dienen als Richtlinie zur Bestimmung von Leistung und Skalierbarkeit einer XenMobile 10.3.6-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.

Skalierbarkeit	Maximal 45.000 Geräte	
Anmelderaten	Onboarding (Erstverwendung)	Maximal 833 Geräte pro Stunde
	Vorhandene Benutzer	Maximal 2.812 Geräte pro Stunde
Konfiguration	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	XenMobile-Servercluster mit 6 Knoten
	Datenbank	Externe Microsoft SQL Server-Datenbank

> **Important**
>
> Die Automatisierungsanforderung für diesen Bericht ist 1.000 bis 60.000 Geräte. Anforderungen, die 60.000 Geräte übersteigen, gehen über diesen Bericht hinaus.

In diesem Abschnitt werden die Active Directory-Konfiguration, die Anzahl der XenMobile-Richtlinien, Anzahl und Typ von Anwendungen, die simulierten Benutzeraktionen und die simulierten Administratoraktionen des Testprofils für die einzelnen Hardwarekonfigurationen und Arbeitslasten beschrieben.

> **Hinweis**
>
> Das Testprofil ist für die Verwendung von mehr Ressourcen ausgelegt, als die zum Testen der Skalierbarkeit für vorherige XenMobile-Versionen verwendeten Profile. Daher sind die neuen Testergebnisse nicht direkt mit den Skalierbarkeitsergebnissen früherer Versionen vergleichbar.

Active Directory-Konfiguration:

- 100.000 eindeutige Active Directory-Benutzer
- 200.000 eindeutige Active Directory-Gruppen
- 5 Verschachtelungsebenen für AD-Gruppen
- 200 Benutzer pro AD-Gruppe

Bereitstellungsgruppen:
- 20 Bereitstellungsgruppen
- Jeder Bereitstellungsgruppe 50 Apps zugewiesen
- 10 AD-Gruppen pro Bereitstellungsgruppe

XenMobile-Geräterichtlinien:
- 300 Geräterichtlinien
- 20 Geräterichtlinien pro Benutzer

Anwendungen
- 200 native Apps aus einem öffentlichen Store
- 50 native Apps zur Verteilung im Unternehmen
- 100 Web- und SaaS-Apps (Software as a Service)
- 50 Apps pro Benutzer

XenMobile-Benutzeraktionen:
- 50 konfigurierte Aktionen insgesamt
- WorxStore-Starts:

- Erstmalsbenutzer (FTU): 4
- Mehrfachbenutzer (RU): 1

- App-Starts:
  - MDX: 1
  - Web/SaaS: 1
- 150 STA-Prüfungen pro Benutzer

XenMobile-Administratoraktivitäten:

- Auflisten von Geräten (zur Simulation von Helpdeskanrufen): 32 Vorgänge je 8 Stunden, einer alle 15 bis 20 Minuten
- Erstellen von Berichten: 2 Mal je 8 Stunden

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 60.000 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.
- Die Verbindungsanzahl pro Benutzersitzung auf NetScaler ist ein wichtiger Gesichtspunkt.
- Zur Erzielung einer maximalen Skalierbarkeit wurden CPU- und RAM-Ressourcen in XenMobile erhöht.
- Die Konfiguration mit 6 Clusterknoten war die größte geprüfte Konfiguration. Eine Skalierung über 6 Knoten hinaus erfordert eine zusätzliche XenMobile-Implementierung.

Die folgende Tabelle 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.

Erwartete Gerätezahl	1.000	10.000	30.000	45.000
Tatsächliche Gerätezahl	1.000	9.998	29.977	44.991
Anmelderate				
Onboarding (Erstverwendung)	250	625	833	833
Vorhandene Benutzer (nur Worx)	1.000	1.666	3.750	883
Konfiguration				
Referenzumgebung	VPX-XenMobile, eigenständig	MPX-XenMobile, eigenständig	MPX-XenMobile, Cluster (3)	MPX-XenMobile, Cluster (6)
NetScaler Gateway	VPX mit 2 GB RAM 2 virtuelle CPUs	MPX-10500	MPX-11500	MPX-11500
XenMobile-Modus	Eigenständig*	Eigenständig*	Cluster	Cluster
XenMobile-Cluster	nicht zutreffend	nicht zutreffend	3	6
XenMobile – virtuelles Gerät	8 GB RAM und 4 virtuelle CPUs	8 GB RAM und 4 virtuelle CPUs	16 GB RAM und 6 virtuelle CPUs	16 GB RAM und 8 virtuelle CPUs
Active Directory (AD)	8 GB RAM und 4 virtuelle CPUs	8 GB RAM und 4 virtuelle CPUs	16 GB RAM und 4 virtuelle CPUs	16 GB RM und 4 virtuelle CPUs
Datenbank	Externe Schicht	Extern: Microsoft SQL Server Speicher: 16 GB vCPUs: 12	Extern: Microsoft SQL Server Speicher: 32 GB vCPUs: 12	Extern: Microsoft SQL Server Speicher: 48 GB vCPUs: 16

MPX-XenMobile, Cluster (3)

Cluster

Cluster

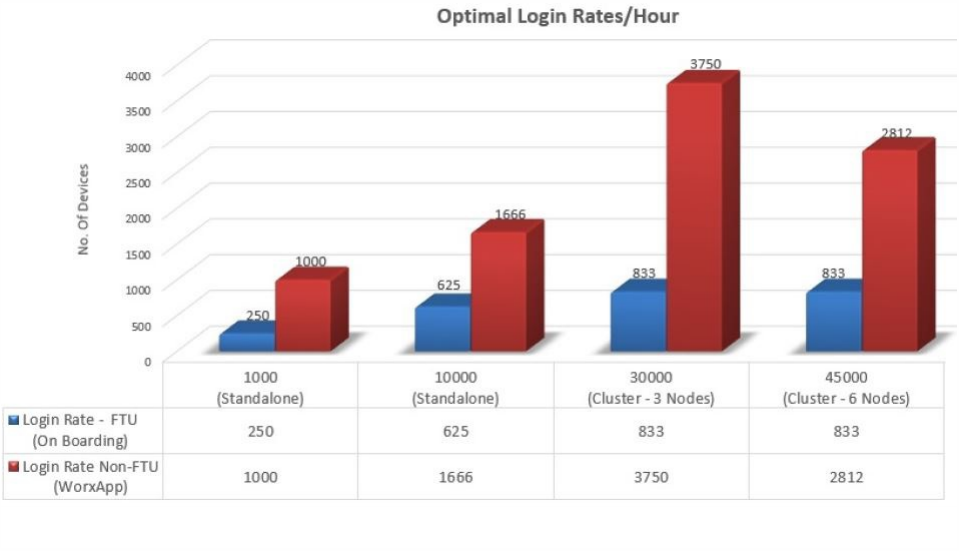
Cluster	
Cluster	
8 GB RAM und 4 virtuelle CPUs	
8 GB RAM und 4 virtuelle CPUs	

*Eigenständige Bereitstellungen werden für Apps, bei denen eine hohe Verfügbarkeit erforderlich ist, nicht empfohlen. Citrix empfiehlt den meisten Kunden hoch verfügbare Clusterbereitstellungen.

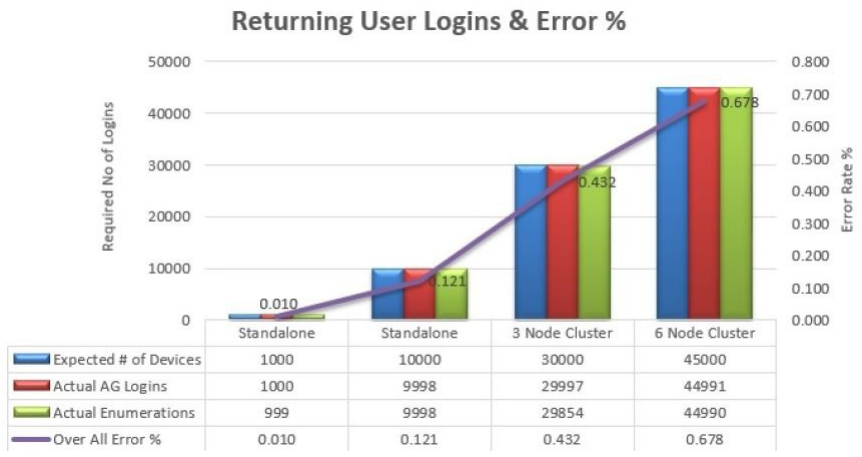
Hinweis: Wenn Sie bei der Dimensionierung des Systems die empfohlenen Raten überschreiten oder die Hardwareempfehlungen nicht beachten, treten die nachfolgenden Probleme auf.

Die folgenden Informationen bieten zusätzliche aufgezeichnete Datenpunkte, die die Ergebnisse in der Tabelle oben beeinflussen.

- Registrierungs- bzw. Anmeldelatenz (Roundtripzeit)
  - Durchschnittliche Latenz insgesamt: 0,5 bis 1,5 Sekunden
  - Durchschnittliche Latenz bei NetScaler Gateway-Anmeldungen: > 120 bis 440 ms
  - Durchschnittliche Latenz bei Worx Store-Anforderungen: 2 bis 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
  - Langsame Reaktionszeit der XenMobile-Konsole bei hohen Lasten



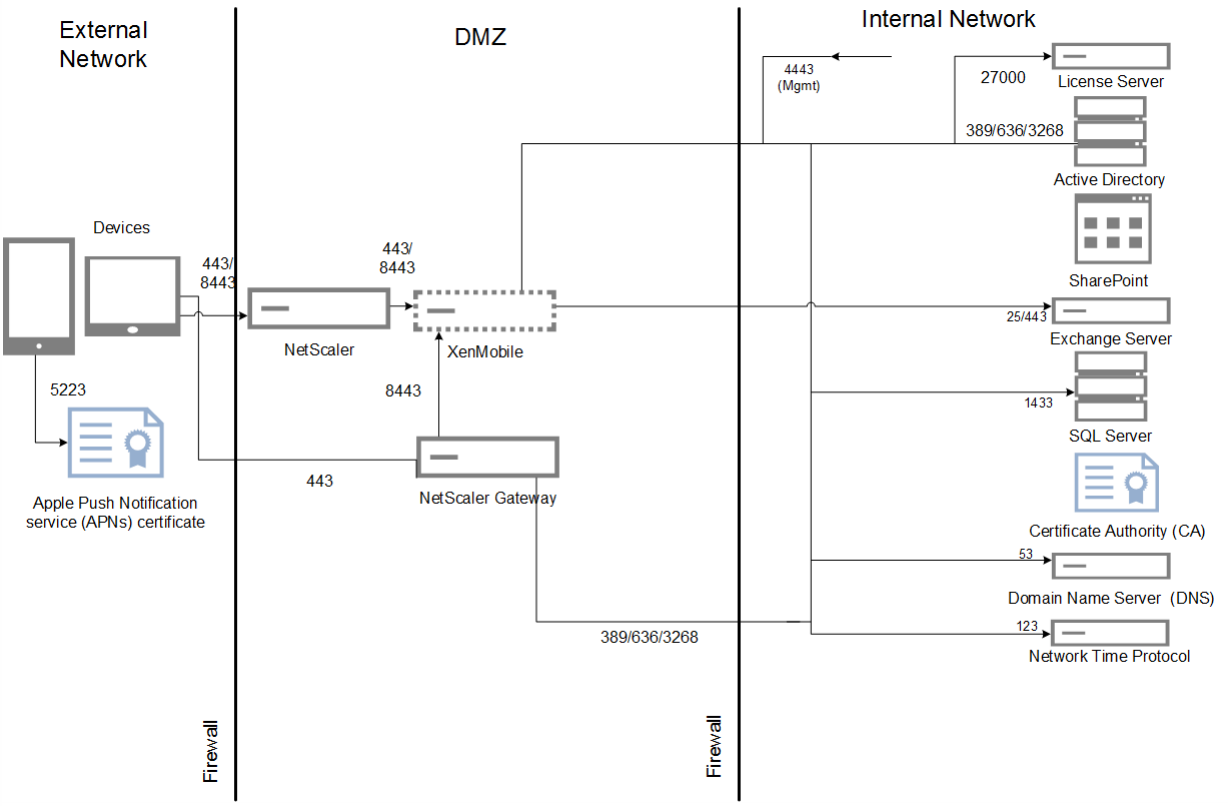
	1000 (Standalone)	10000 (Standalone)	30000 (Cluster - 3 Nodes)	45000 (Cluster - 6 Nodes)
Login Rate - FTU (On Boarding)	250	625	833	833
Login Rate Non-FTU (WorxApp)	1000	1666	3750	2812



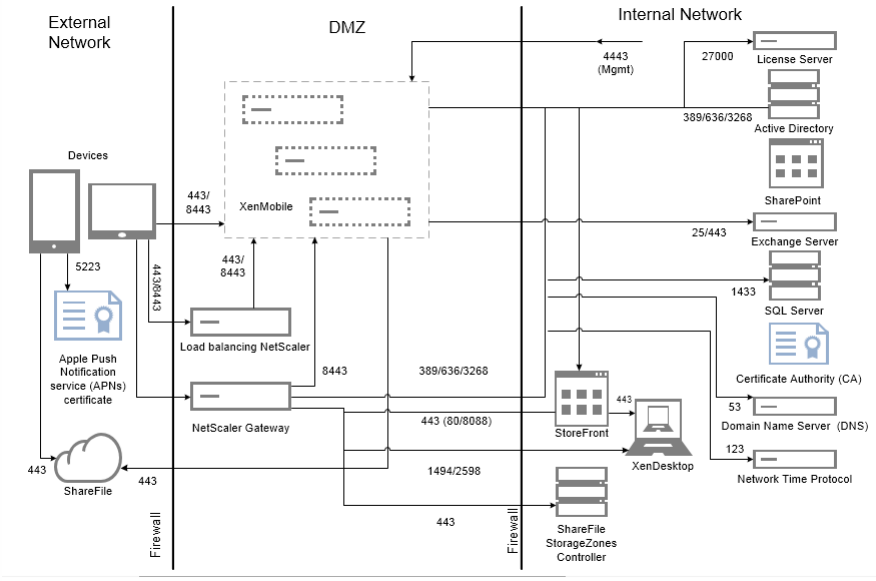
	Standalone	Standalone	3 Node Cluster	6 Node Cluster
Expected # of Devices	1000	10000	30000	45000
Actual AG Logins	1000	9998	29997	44991
Actual Enumerations	999	9998	29854	44990
Over All Error %	0.010	0.121	0.432	0.678

Der Fehlerprozentsatz in der Abbildung oben enthält Fehler insgesamt bei Anforderungen für alle Vorgänge und nicht nur für Anmeldungen. Der Fehlerprozentsatz liegt für jeden Testlauf im akzeptablen Bereich von 1 % 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 MAM über HTTP für 10.000 oder mehr Geräte.



Die Tests wurden an XenMobile Enterprise zur Benchmarkerstellung ausgeführt. Zum Testen sowohl kleiner und als auch großer Bereitstellungen wurden 1000 bis 60.000 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.

Benutzerarbeitslasten werden wie folgt definiert:

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.

Anmerkungen und Annahmen

Die folgenden Szenarios sind nicht Teil der Skalierbarkeitstests. Diese Szenarios werden ggf. für zukünftige Verbesserungen bei Skalierbarkeitstests einbezogen:

- Die Paketbereitstellung wird nicht getestet.
- Die Windows-Plattform wird nicht getestet.

Bereitstellung von Richtlinien per Push wird für iOS- und Android-Geräte getestet.
Jedes XenMobile unterstützt maximal 10.000 gleichzeitige Verbindungen.

Die Tests wurden unter idealen Bedingungen in einem LAN durchgeführt, um Netzwerklatenzprobleme außen vor zu halten. In einer Produktionsumgebung hängt die Skalierbarkeit auch von der für die Benutzer verfügbaren Bandbreite ab, insbesondere bei App-Downloads.

Wiederverbindungstests

Wiederverbindungstests wurden getrennt von Erstverwendungstests und Tests von Szenarios mit zurückkehrenden Benutzern ausgeführt.

Wiederverbindungstests wurden für bis zu 15.000 Geräte durchgeführt.

Die für Android unterstützte Wiederverbindungsrate ist 17 Geräte pro Sekunde. Die Wiederverbindungsrate für iOS ist 8 Geräte pro Sekunde. Um dies zu erreichen, wurde die maximale Threadzahl in der Datei /opt/sas/tomcat/conf/server.xml auf 1000 festgelegt.

HINZUFÜGEN: INFORMATIONEN ZU EMPFOHLENEN GERÄTEWIEDERVERBINDUNGSRICHTLINIEN

On-Boarding (FTU)-Arbeitslast
Die Onboarding-Arbeitslast entsteht beim ersten Zugriff eines Benutzers auf die XenMobile-Umgebung. Diese Arbeitslast umfasste folgende Vorgänge:
- Automatische Ermittlung
- Registrierung
- 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) einschließlich Gerätestatusprüfungen
- Richtlinienbereitstellung per Push (iOS)
- Minimale WorxMail- und WorxWeb-Verbindungen (VPN-Tunnel): zwei Verbindungen
- Installation erforderlicher Apps über XenMobile

Die Arbeitslastparameter werden in der folgenden Tabelle definiert:

Geräte	Registrierte Geräte	Enumerationen	Enumerierte Apps pro Gerät	WorxStore-Starts pro Gerät	Web-/SaaS-SSO pro Gerät	MDX-App-Downloads pro Gerät	Erforderliche App-Downloads, ausgelöst über XenMobile-Server	Per Push bereitgestellte Richtlinien pro Gerät (iOS)
1000	1000	1000	50	4	40	10	2	20

10000	10000	10000	50	4	40	10	2	20
30000	30000	30000	50	4	40	10	2	20
60000	60000	60000	50	4	40	10	2	20

Arbeitslast für vorhandene Benutzer mit ausschließlich Worx-Verbindungen

Die folgende Tabelle zeigt die Arbeitslast vorhandener Benutzer (mit ausschließlich Worx-Verbindungen). Diese Arbeitslast simulierte einen Benutzer mit WorxMail- und WorxWeb-Apps. Diese Simulation wurde zum Messen der NetScaler Gateway-Skalierbarkeit innerhalb der XenMobile-Konfiguration verwendet. Da nur die beiden Worx-Apps verwendet werden, ist die Last des Netzwerks minimal. Bei der WorxWeb-App greifen Benutzer auf interne Websites zu, die keinen XenMobile-Server-SSO auslösen. Dieser Modus umfasste folgende Vorgänge:

- Authentifizierung (NetScaler Gateway und XenMobile)
- WorxMail- und WorxWeb-Verbindungen (VPN-Tunnel): vier Verbindungen

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

Geräte	Enumerationen	Enumerierte Apps pro Gerät	VPN-Tunnel pro Gerät[1]
1000	1000	50	3
10000	10000	50	3
30000	30000	50	3
60000	60000	50	3

1. Die Anzahl der VPN-Tunnel entspricht WorxMail- und WorxWeb-Verbindungen.

Die Verbindungsprofile für WorxMail und WorxWeb werden in der folgenden Tabelle aufgeführt:

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)

Diese Empfehlungen basieren auf den WorxMail- und WorxWeb-Profilen, mit denen eine
mittlere Arbeitslast automatisiert wird. 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 für die Apps verwendeten Profile sollen eine "sehr hohe" Arbeitslast automatisieren. In den folgenden Tabellen sind die WorxMail- und WorxWeb-Profildetails dargestellt.

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

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.
- Das NetScaler-Sitzungstimeout ist 60 Minuten.
- In NetScaler Gateway wurde für SSL-Transaktionen ein 2048-Bit-Schlüssel verwendet.

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.

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

Komponente	Version
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0,824
Externe Datenbank	Microsoft SQL Server 2014

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

Anbieter	Genuine Intel
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).

Skalierbarkeit und Leistung von XenMobile

Jul 28, 2016

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.

Die Angaben in diesem Artikel dienen als Richtlinie zur Bestimmung von Leistung und Skalierbarkeit einer XenMobile 10.3.6-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.

Skalierbarkeit	Maximal 45.000 Geräte	
Anmelderaten	Onboarding (Erstverwendung)	Maximal 833 Geräte pro Stunde
	Vorhandene Benutzer	Maximal 2.812 Geräte pro Stunde
Konfiguration	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	XenMobile-Servercluster mit 6 Knoten
	Datenbank	Externe Microsoft SQL Server-Datenbank

> **Important**
>
> Die Automatisierungsanforderung für diesen Bericht ist 1.000 bis 60.000 Geräte. Anforderungen, die 60.000 Geräte übersteigen, gehen über diesen Bericht hinaus.

In diesem Abschnitt werden die Active Directory-Konfiguration, die Anzahl der XenMobile-Richtlinien, Anzahl und Typ von Anwendungen, die simulierten Benutzeraktionen und die simulierten Administratoraktionen des Testprofils für die einzelnen Hardwarekonfigurationen und Arbeitslasten beschrieben.

> **Hinweis**
>
> Das Testprofil ist für die Verwendung von mehr Ressourcen ausgelegt, als die zum Testen der Skalierbarkeit für vorherige XenMobile-Versionen verwendeten Profile. Daher sind die neuen Testergebnisse nicht direkt mit den Skalierbarkeitsergebnissen früherer Versionen vergleichbar.

Active Directory-Konfiguration:

- 100.000 eindeutige Active Directory-Benutzer
- 200.000 eindeutige Active Directory-Gruppen
- 5 Verschachtelungsebenen für AD-Gruppen
- 200 Benutzer pro AD-Gruppe

Bereitstellungsgruppen:
- 20 Bereitstellungsgruppen
- Jeder Bereitstellungsgruppe 50 Apps zugewiesen
- 10 AD-Gruppen pro Bereitstellungsgruppe

XenMobile-Geräterichtlinien:
- 300 Geräterichtlinien
- 20 Geräterichtlinien pro Benutzer

Anwendungen
- 200 native Apps aus einem öffentlichen Store
- 50 native Apps zur Verteilung im Unternehmen
- 100 Web- und SaaS-Apps (Software as a Service)
- 50 Apps pro Benutzer

XenMobile-Benutzeraktionen:
- 50 konfigurierte Aktionen insgesamt
- WorxStore-Starts:

- Erstmalsbenutzer (FTU): 4
- Mehrfachbenutzer (RU): 1

- App-Starts:
  - MDX: 1
  - Web/SaaS: 1
- 150 STA-Prüfungen pro Benutzer

XenMobile-Administratoraktivitäten:

- Auflisten von Geräten (zur Simulation von Helpdeskanrufen): 32 Vorgänge je 8 Stunden, einer alle 15 bis 20 Minuten
- Erstellen von Berichten: 2 Mal je 8 Stunden

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 60.000 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.
- Die Verbindungsanzahl pro Benutzersitzung auf NetScaler ist ein wichtiger Gesichtspunkt.
- Zur Erzielung einer maximalen Skalierbarkeit wurden CPU- und RAM-Ressourcen in XenMobile erhöht.
- Die Konfiguration mit 6 Clusterknoten war die größte geprüfte Konfiguration. Eine Skalierung über 6 Knoten hinaus erfordert eine zusätzliche XenMobile-Implementierung.

Die folgende Tabelle 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.

Erwartete Gerätezahl	1.000	10.000	30.000	45.000
Tatsächliche Gerätezahl	1.000	9.998	29.977	44.991
Anmelderate				
Onboarding (Erstverwendung)	250	625	833	833
Vorhandene Benutzer (nur Worx)	1.000	1.666	3.750	883
Konfiguration				
Referenzumgebung	VPX-XenMobile, eigenständig	MPX-XenMobile, eigenständig	MPX-XenMobile, Cluster (3)	MPX-XenMobile, Cluster (6)
NetScaler Gateway	VPX mit 2 GB RAM 2 virtuelle CPUs	MPX-10500	MPX-11500	MPX-11500
XenMobile-Modus	Eigenständig*	Eigenständig*	Cluster	Cluster
XenMobile-Cluster	nicht zutreffend	nicht zutreffend	3	6
XenMobile – virtuelles Gerät	8 GB RAM und 4 virtuelle CPUs	8 GB RAM und 4 virtuelle CPUs	16 GB RAM und 6 virtuelle CPUs	16 GB RAM und 8 virtuelle CPUs
Active Directory (AD)	8 GB RAM und 4 virtuelle CPUs	8 GB RAM und 4 virtuelle CPUs	16 GB RAM und 4 virtuelle CPUs	16 GB RM und 4 virtuelle CPUs
Datenbank	Externe Schicht	Extern: Microsoft SQL Server Speicher: 16 GB vCPUs: 12	Extern: Microsoft SQL Server Speicher: 32 GB vCPUs: 12	Extern: Microsoft SQL Server Speicher: 48 GB vCPUs: 16

MPX-XenMobile, Cluster (3)

Cluster

Cluster

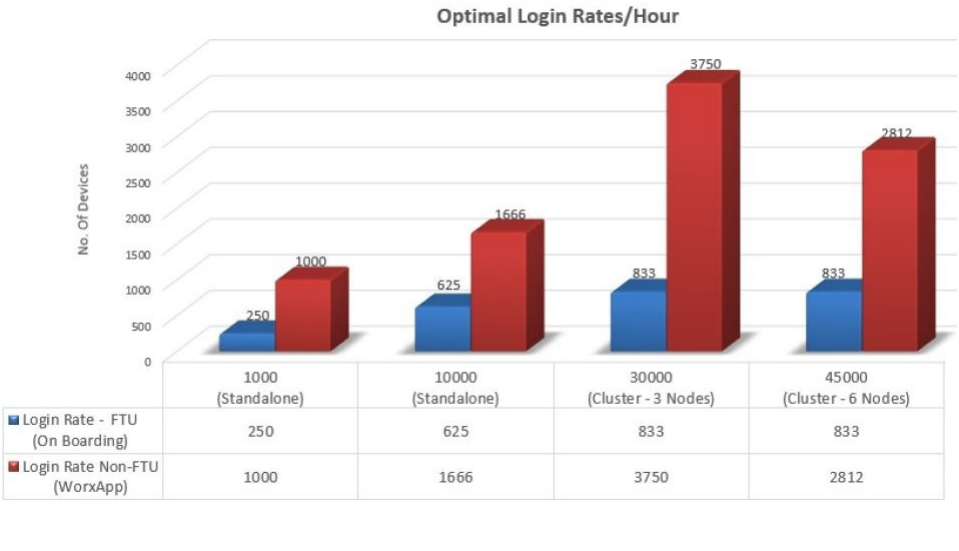
Cluster
Cluster
8 GB RAM und 4 virtuelle CPUs
8 GB RAM und 4 virtuelle CPUs

*Eigenständige Bereitstellungen werden für Apps, bei denen eine hohe Verfügbarkeit erforderlich ist, nicht empfohlen. Citrix empfiehlt den meisten Kunden hoch verfügbare Clusterbereitstellungen.

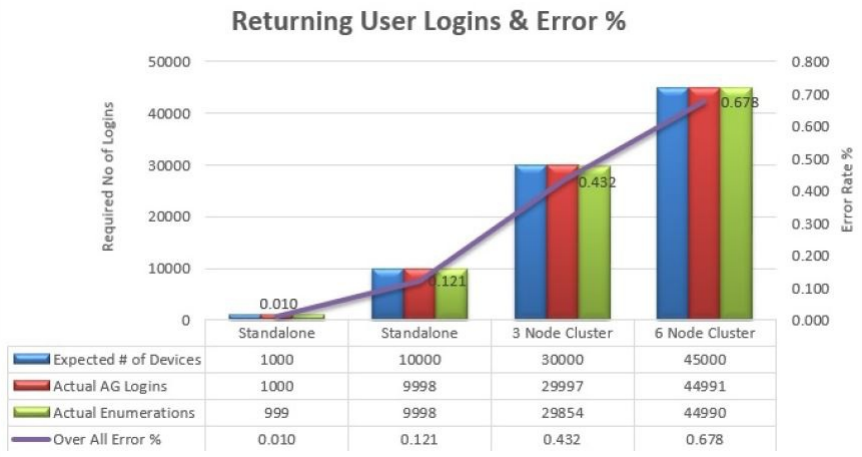
Hinweis: Wenn Sie bei der Dimensionierung des Systems die empfohlenen Raten überschreiten oder die Hardwareempfehlungen nicht beachten, treten die nachfolgenden Probleme auf.

Die folgenden Informationen bieten zusätzliche aufgezeichnete Datenpunkte, die die Ergebnisse in der Tabelle oben beeinflussen.

- Registrierungs- bzw. Anmeldelatenz (Roundtripzeit)
  - Durchschnittliche Latenz insgesamt: 0,5 bis 1,5 Sekunden
  - Durchschnittliche Latenz bei NetScaler Gateway-Anmeldungen: > 120 bis 440 ms
  - Durchschnittliche Latenz bei Worx Store-Anforderungen: 2 bis 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
  - Langsame Reaktionszeit der XenMobile-Konsole bei hohen Lasten



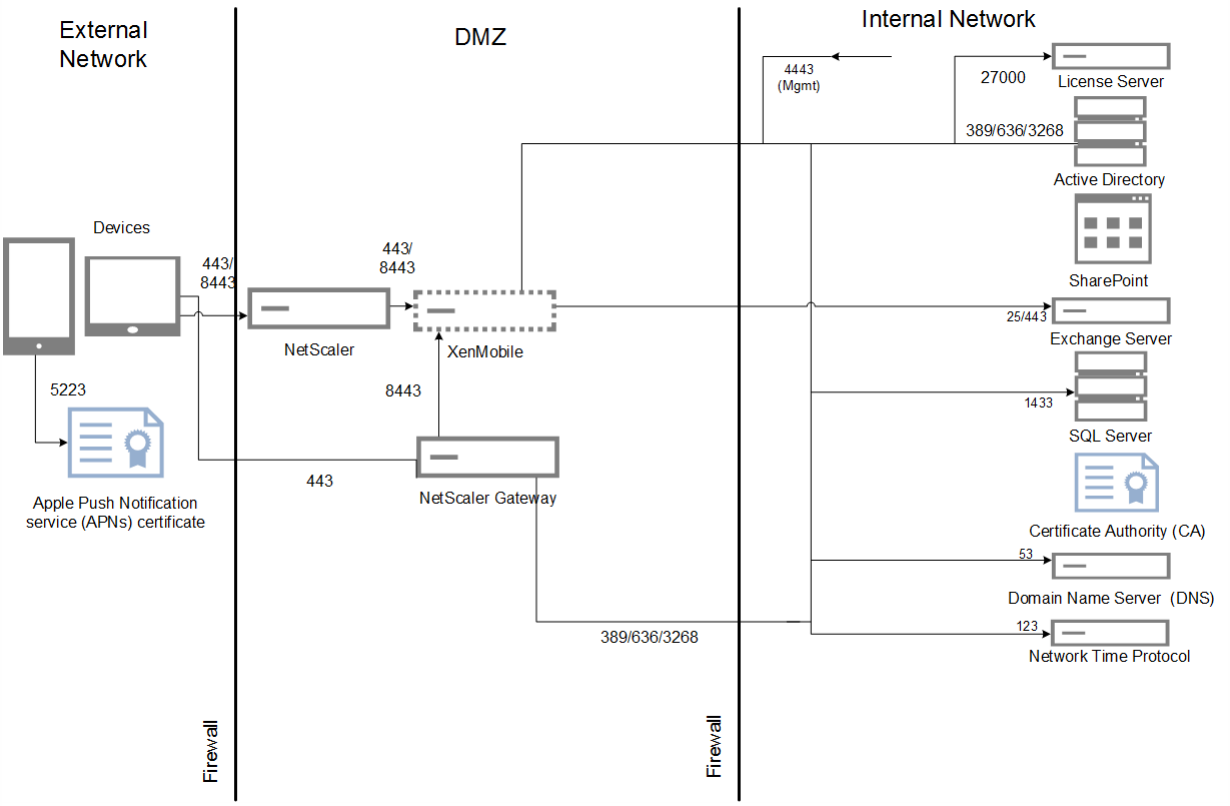
	1000 (Standalone)	10000 (Standalone)	30000 (Cluster - 3 Nodes)	45000 (Cluster - 6 Nodes)
Login Rate - FTU (On Boarding)	250	625	833	833
Login Rate Non-FTU (WorxApp)	1000	1666	3750	2812



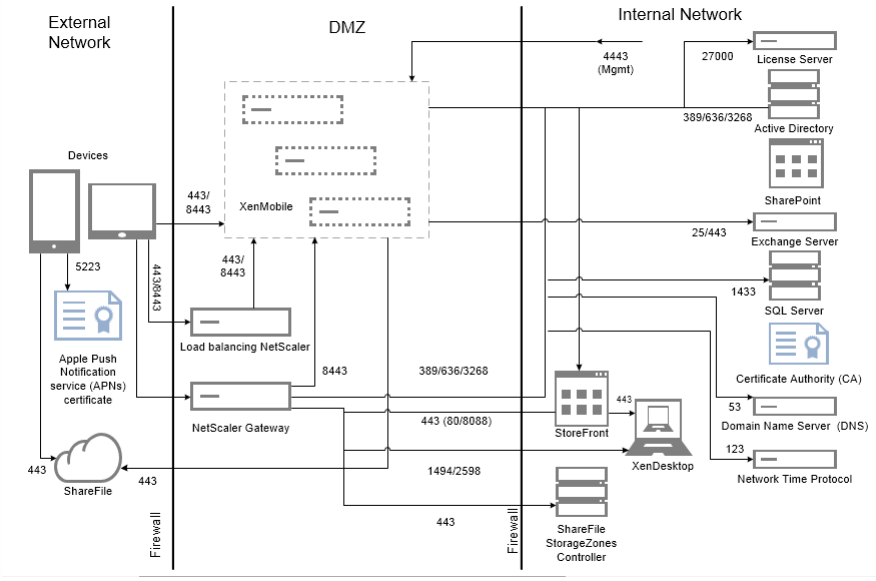
	Standalone	Standalone	3 Node Cluster	6 Node Cluster
Expected # of Devices	1000	10000	30000	45000
Actual AG Logins	1000	9998	29997	44991
Actual Enumerations	999	9998	29854	44990
Over All Error %	0.010	0.121	0.432	0.678

Der Fehlerprozentsatz in der Abbildung oben enthält Fehler insgesamt bei Anforderungen für alle Vorgänge und nicht nur für Anmeldungen. Der Fehlerprozentsatz liegt für jeden Testlauf im akzeptablen Bereich von 1 % 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 MAM über HTTP für 10.000 oder mehr Geräte.



Die Tests wurden an XenMobile Enterprise zur Benchmarkerstellung ausgeführt. Zum Testen sowohl kleiner und als auch großer Bereitstellungen wurden 1000 bis 60.000 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.

Benutzerarbeitslasten werden wie folgt definiert:

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.

Anmerkungen und Annahmen

Die folgenden Szenarios sind nicht Teil der Skalierbarkeitstests. Diese Szenarios werden ggf. für zukünftige Verbesserungen bei Skalierbarkeitstests einbezogen:

- Die Paketbereitstellung wird nicht getestet.
- Die Windows-Plattform wird nicht getestet.

Bereitstellung von Richtlinien per Push wird für iOS- und Android-Geräte getestet.
Jedes XenMobile unterstützt maximal 10.000 gleichzeitige Verbindungen.

Die Tests wurden unter idealen Bedingungen in einem LAN durchgeführt, um Netzwerklatenzprobleme außen vor zu halten. In einer Produktionsumgebung hängt die Skalierbarkeit auch von der für die Benutzer verfügbaren Bandbreite ab, insbesondere bei App-Downloads.

Wiederverbindungstests

Wiederverbindungstests wurden getrennt von Erstverwendungstests und Tests von Szenarios mit zurückkehrenden Benutzern ausgeführt.

Wiederverbindungstests wurden für bis zu 15.000 Geräte durchgeführt.

Die für Android unterstützte Wiederverbindungsrate ist 17 Geräte pro Sekunde. Die Wiederverbindungsrate für iOS ist 8 Geräte pro Sekunde. Um dies zu erreichen, wurde die maximale Threadzahl in der Datei /opt/sas/tomcat/conf/server.xml auf 1000 festgelegt.

HINZUFÜGEN: INFORMATIONEN ZU EMPFOHLENEN GERÄTEWIEDERVERBINDUNGSRICHTLINIEN

On-Boarding (FTU)-Arbeitslast
Die Onboarding-Arbeitslast entsteht beim ersten Zugriff eines Benutzers auf die XenMobile-Umgebung. Diese Arbeitslast umfasste folgende Vorgänge:
- Automatische Ermittlung
- Registrierung
- 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) einschließlich Gerätestatusprüfungen
- Richtlinienbereitstellung per Push (iOS)
- Minimale WorxMail- und WorxWeb-Verbindungen (VPN-Tunnel): zwei Verbindungen
- Installation erforderlicher Apps über XenMobile

Die Arbeitslastparameter werden in der folgenden Tabelle definiert:

Geräte	Registrierte Geräte	Enumerationen	Enumerierte Apps pro Gerät	WorxStore-Starts pro Gerät	Web-/SaaS-SSO pro Gerät	MDX-App-Downloads pro Gerät	Erforderliche App-Downloads, ausgelöst über XenMobile-Server	Per Push bereitgestellte Richtlinien pro Gerät (iOS)
1000	1000	1000	50	4	40	10	2	20

10000	10000	10000	50	4	40	10	2	20
30000	30000	30000	50	4	40	10	2	20
60000	60000	60000	50	4	40	10	2	20

Arbeitslast für vorhandene Benutzer mit ausschließlich Worx-Verbindungen

Die folgende Tabelle zeigt die Arbeitslast vorhandener Benutzer (mit ausschließlich Worx-Verbindungen). Diese Arbeitslast simulierte einen Benutzer mit WorxMail- und WorxWeb-Apps. Diese Simulation wurde zum Messen der NetScaler Gateway-Skalierbarkeit innerhalb der XenMobile-Konfiguration verwendet. Da nur die beiden Worx-Apps verwendet werden, ist die Last des Netzwerks minimal. Bei der WorxWeb-App greifen Benutzer auf interne Websites zu, die keinen XenMobile-Server-SSO auslösen. Dieser Modus umfasste folgende Vorgänge:

- Authentifizierung (NetScaler Gateway und XenMobile)
- WorxMail- und WorxWeb-Verbindungen (VPN-Tunnel): vier Verbindungen

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

Geräte	Enumerationen	Enumerierte Apps pro Gerät	VPN-Tunnel pro Gerät[1]
1000	1000	50	3
10000	10000	50	3
30000	30000	50	3
60000	60000	50	3

1. Die Anzahl der VPN-Tunnel entspricht WorxMail- und WorxWeb-Verbindungen.

Die Verbindungsprofile für WorxMail und WorxWeb werden in der folgenden Tabelle aufgeführt:

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)

Diese Empfehlungen basieren auf den WorxMail- und WorxWeb-Profilen, mit denen eine
mittlere Arbeitslast automatisiert wird. 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 für die Apps verwendeten Profile sollen eine "sehr hohe" Arbeitslast automatisieren. In den folgenden Tabellen sind die WorxMail- und WorxWeb-Profildetails dargestellt.

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

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.
- Das NetScaler-Sitzungstimeout ist 60 Minuten.
- In NetScaler Gateway wurde für SSL-Transaktionen ein 2048-Bit-Schlüssel verwendet.

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.

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

Komponente	Version
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0,824
Externe Datenbank	Microsoft SQL Server 2014

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

Anbieter	Genuine Intel
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).

Info zu XenMobile Server 10.3.5

Oct 13, 2016

Sie können in der XenMobile-Konsole von den folgenden Releases ein direktes Upgrade auf XenMobile 10.3.5 durchführen:

- XenMobile 10.3 Rolling Patch 1
- XenMobile 10.3
- XenMobile 10.1 Rolling Patch 4
- XenMobile 10,1

Für das Upgrade verwenden Sie xms_10.3.5.354.bin. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben und dann auf **Releasemanagement**. Klicken Sie auf **Upgrade** und laden Sie dann die Datei xms_10.3.5.354.bin hoch. Weitere Informationen über Upgrades in der Konsole finden Sie unter Aktualisieren von XenMobile.

Anweisungen für eine neue Installation von XenMobile 10.3.5 finden Sie unter Installieren von XenMobile.

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 in XenMobile 10.3.5

XenMobile 10.3.5 bietet Fehlerbehebungen und die folgenden neuen Features:

Das Cloud Services-Team kann Ihre XenMobile Server-Cloudbereitstellung von Version 10.3 auf Version 10.3.5 ohne Ausfallzeiten aktualisieren.

Sie können zulassen, dass Benutzer von Android M vier Berechtigungsarten aktivieren oder blockieren. Wenn Benutzer sich in Worx Home registrieren, werden ihnen vier Meldungen angezeigt, in denen sie die folgenden Berechtigungen für Worx Home zulassen oder verweigern können:

- Zugriff auf Geräteinformationen, damit Worx Home ordnungsgemäß funktioniert
- Die Fähigkeit, Telefonanrufe zu tätigen und zu verwalten
- Zugriff auf Fotos, Medien und Dateien auf dem Gerät
- Zugriff auf den Standort des Geräts

Ab diesem Release können Sie zulassen, dass iOS-Benutzer sich bei Worx Home und den Worx-Apps mit Touch ID erneut authentifizieren. Wenn auf iOS 8- und iOS 9-Geräten Single Sign-On für Worx Home und Touch ID aktiviert sind, ersetzt dies die Verwendung einer PIN. Benutzer müssen weiterhin eine PIN eingeben, wenn Onlineauthentifizierung über NetScaler Gateway erforderlich ist. Dies ist in den folgenden Situationen erforderlich:

- Die Sitzung des Benutzers ist abgelaufen.
- Der Benutzer startet das Gerät neu.
- Worx Home wird zurzeit nicht ausgeführt und der Benutzer startet Worx Home oder eine MDX-App.

In der XenMobile-Konsole können Sie nun Registrierungsprofile für Android- und iOS-Geräte auf der neuen Seite **Konfigurieren > Registrierungsprofile** erstellen. Ein Registrierungsprofil gilt für alle Servermodi. Sie können mehrere Registrierungsprofile erstellen und verschiedenen Bereitstellungsgruppen zuweisen.

Hinweis: Die Seite **Registrierungsprofile** gilt nicht für Windows-Geräte. Informationen zur Registrierung von Windows-Geräten finden Sie unterWindows-Geräte.

Das Gerätelimit pro Benutzer wurde in früheren Releases über die Servereigenschaft **Anzahl der Geräte pro Benutzer** festgelegt. Die Servereigenschaft ist inzwischen veraltet. Sie konfigurieren das Gerätelimit auf der neuen Seite **Konfigurieren > Registrierungsprofil**. Zuvor konnten Sie die Geräteanzahl nur für MDM begrenzen. Jetzt können Sie die Geräteanzahl auch für MAM begrenzen.

Standardmäßig ist die Anzahl der Geräte, die ein Benutzer registrieren kann, unbegrenzt. Weitere Informationen finden Sie unter Geräteregistrierungslimit.

XenMobile 10.3.5 bietet Unterstützung im WorxStore für Hebräisch und traditionelles Chinesisch.

Mit XenMobile 10.3.5 wird ein neuer ausschließlicher MAM-Servermodus eingeführt. Zur Unterscheidung des älteren und des neuen MAM-Modus wird in der Citrix Dokumentation der neuere Modus als ausschließlicher MAM-Modus bezeichnet und der vorherige MAM-Modus als "Legacy-MAM-Modus". Die Legacy-MAM-Modus-Funktionalität ist genau wie vorher. Citrix plant nicht, die Funktionalität für zukünftige Releases zu erweitern.

Der ausschließliche MAM-Modus wird verwendet, wenn für die Servermoduseigenschaft in XenMobile **MAM** eingestellt ist. Geräte werden im MAM-Modus registriert.

Die Legacy-MAM-Funktionalität gilt, wenn für die Servermoduseigenschaft in XenMobile **ENT** eingestellt ist, und Benutzer sich gegen die Geräteverwaltung entscheiden. Geräte werden im MDM+MAM-Modus registriert. Im MAM+MDM-Modus wird Benutzern, die die Geräteverwaltung ablehnen, weiterhin die Legacy-MAM-Funktionalität bereitgestellt, unabhängig davon, ob sie ein Upgrade auf XenMobile 10.3.5 durchführen.

Hinweis: In früheren Versionen hatte das Einstellen der Servermoduseigenschaft auf **MAM** den gleichen Effekt wie die Einstellung **ENT**: Geräte wurden im MDM+MAM-Modus registriert; Benutzer, die die MDM-Verwaltung ablehnen, erhalten die Legacy-MAM-Funktionalität.

Die Vorteile des ausschließlichen MAM-Modus umfassen zusätzliche Verschlüsselung (nicht nur Gerätepasscodes), mobile VPNs und ein besserer Datenschutz für Endbenutzer. Der ausschließliche MAM-Modus ist daher für BYO-Geräte geeignet.

Wenn Ihr aktueller XenMobile-Servermodus auf MAM festgelegt ist, können Sie ein Upgrade auf den neuen ausschließlichen MAM-Modus durchführen, um von den folgenden Features zu profitieren, die zuvor nur für MDM verfügbar waren. Diese Features sind nicht für Windows Phone verfügbar.

- Zertifikatbasierte Authentifizierung
  Der ausschließliche MAM-Modus unterstützt die zertifikatbasierte Authentifizierung. Benutzer haben kontinuierlichen Zugriff auf ihre Apps, selbst wenn das Active Directory-Kennwort abläuft. Wenn Sie für MAM-Geräte auf die

zertifikatbasierte Authentifizierung umstellen, müssen Sie ein NetScaler Gateway konfigurieren. In XenMobile ist unter **Einstellungen > NetScaler Gateway** die Option **Benutzerzertifikat für Authentifizierung bereitstellen** standardmäßig auf **Aus** festgelegt, sodass die Authentifizierung durch Benutzername und Kennwort erfolgt. Ändern Sie die Einstellung auf **Ein**, um Zertifikatauthentifizierung zu aktivieren.

- **Selbsthilfeportal** ermöglicht Endbenutzern das Sperren und Löschen ihrer eigenen Apps. Diese Aktionen können für alle Apps auf dem Gerät durchgeführt werden. Sie können App-Sperre und App-Löschen unter **Konfigurieren > Aktionen** konfigurieren.
- **Alle Registrierungsmodi**, einschließlich Hohe Sicherheit", Einladungs-URL und Zweifaktor, werden unter **Verwalten > Registrierung** konfiguriert.
- **Geräteregistrierungslimit** für Android- und iOS-Geräte. Die Servereigenschaft **Anzahl der Geräte pro Benutzer** befindet sich nun auf der Seite **Konfigurieren > Registrierungsprofile** und gilt nun ebenfalls für den neuen ausschließlichen MAM-Modus.
- **Ausschließliche MAM-APIs:** Für Geräte im ausschließlichen MAM-Modus können Sie REST-Dienste mit einem beliebigen REST-Client und Dienste, die über die XenMobile-Konsole verfügbar gemacht werden, mit der XenMobile-REST-API aufrufen.
- Die in diesem Release verfügbaren ausschließlichen MAM-APIs ermöglichen Ihnen Folgendes:
  - Einladungs-URL und Einmal-PIN senden
  - Apps auf Geräten sperren und löschen

> **Important**
>
> Für den neuen ausschließlichen MAM-Modus müssen Sie XenMobile wie in diesem Abschnitt beschrieben konfigurieren und Benutzer müssen ihre Geräte neu registrieren. Stellen Sie Benutzern den vollqualifizierten Domänennamen (FQDN) für den XenMobile-Server bereit, den sie für die Registrierung benötigen.
>
> Im neuen ausschließlichen MAM-Modus werden Geräte, wie im ENT-Modus, mit dem FQDN des XenMobile-Servers registriert. (Im Legacy-MAM-Modus werden Geräte mit dem NetScaler Gateway-FQDN registriert).

Auswirkungen dieses Upgrades auf registrierte Geräte

In der folgenden Tabelle wird aufgeführt, wie die neuen Features in XenMobile 10.3.5 sich auf registrierte Geräte auswirken.

Geräte, die aktuell wie folgt registriert sind:	XenMobile 10.3.5 bietet	Aufgaben des Administrators	Aufgaben des Benutzers
MDM • Servermodus = MDM	• Fehlerbehebung • Neue Features	Installieren Sie XenMobile 10.3.5	Keine
MDM+MAM • Servermodus = ENT • Benutzer haben	• Fehlerbehebung • Neue Features	Installieren Sie XenMobile 10.3.5	Keine

Geräteverwaltung gewählt			
MAM • Servermodus = ENT • Benutzer haben Geräteverwaltung abgelehnt	• Fehlerbehebung • Neue Features Hinweis: In diesem Fall werden Geräte im Legacy-MAM-Modus registriert. Wenn Sie diesen Benutzern die neue MAM-Funktionalität bieten möchten, richten Sie einen neuen XenMobile-Server für sie ein.	Installieren Sie XenMobile 10.3.5	Keine
MAM • Servermodus = MAM	• Fehlerbehebung • Neue Features • Optionales Upgrade auf den neuen ausschließlichen MAM-Modus	Legacy-MAM-Modus weiter verwenden: Installieren Sie XenMobile 10.3.5 Upgrade auf MAM-Modus: 1. Installieren Sie XenMobile 10.3.5 2. Informationen über zusätzliche erforderliche Konfigurationen finden Sie unter "Konfigurationsübersicht für den ausschließlichen MAM-Modus".	Keine Geräte neu registrieren

Konfigurationsübersicht für den ausschließlichen MAM-Modus

Ausschließlicher MAM-Modus bezieht sich auf den MAM-Servermodus bei Verwendung von Enterprise- oder Advanced-Lizenzen. Der ausschließliche MAM-Modus unterscheidet sich vom *MAM+MDM-Modus*, der verwendet wird, wenn der Servermodus Ihres XenMobile-Servers ENT ist. Im MAM+MDM-Modus wird Benutzern, die die Geräteverwaltung ablehnen, die Legacy-MAM-Funktionalität bereitgestellt, unabhängig davon, ob sie ein Upgrade auf XenMobile 10.3.5 durchführen.

> **Important**
>
> Die Legacy-MAM-Funktionalität funktioniert genauso wie bei früheren Releases und wird in zukünftigen Releases nicht verbessert.

In der folgenden Tabelle ist aufgeführt, welcher Servermodus für einen bestimmten Lizenztyp und gewünschten Gerätemodus verwenden werden sollte:

Ihre Lizenzen sind für Edition	Geräte in diesem Modus registrieren	Servermodus festlegen auf
ENT / ADV / MDM	MDM-Modus	MDM
ENT / ADV	MAM-Modus (bzw. ausschließlicher MAM-Modus)	MAM
ENT / ADV	MDM+MAM-Modi	ENT Benutzer, die die Geräteverwaltung ablehnen, verwenden den Legacy-MAM-Modus.

Unter folgenden Bedingungen *müssen* Sie den ausschließlichen MAM-Modus konfigurieren:

- Der **Servermodus** Ihres XenMobile-Servers ist **MAM** und Sie möchten den neuen ausschließlichen MAM-Modus verwenden, um die zusätzlichen Features zu nutzen.
- Sie möchten einen XenMobile-Server einrichten, um allen Benutzern, die eine Verbindung mit diesem Server herstellen, die Funktionalität des ausschließlichen MAM-Modus zu bieten.

Der ausschließliche MAM-Modus erfordert die folgenden allgemeinen Konfigurationsschritte:

1. Installieren Sie XenMobile 10.3.5 oder führen Sie ein Upgrade durch.
2. Überprüfen Sie unter **Verwalten > Geräte** den **Servermodus**. Wenn der **Servermodus** auf **MDM** oder **ENT** eingestellt ist, dürfen Sie die Schritte in diesem Verfahren nicht ausführen, da dies zu einer Konfiguration führt, die die Geräteverwaltung nicht unterstützt.
3. Öffnen Sie auf dem XenMobile-Server und in der Firewall die Ports 8443 und 443 für das Internet, damit Geräte eine Verbindung mit dem XenMobile-Server herstellen können. Registrierungen müssen auf dem XenMobile-Server erfolgen.
4. Wenn Sie ein Upgrade auf einem Server durchführen, auf dem der **Servermodus** bereits auf **MAM** festgelegt ist, fahren Sie mit dem nächsten Schritt fort. Wenn Sie XenMobile 10.3.5 neu installieren, ist der **Servermodus** des XenMobile-Server standardmäßig **ENT**. Sie aktivieren den ausschließlichen MAM-Modus, indem Sie die Servereigenschaft **Servermodus** auf **MAM** festlegen. Weitere Informationen finden Sie unter Konfigurieren des Servermodus für ausschließlichen MAM-Modus.
5. Wenn Sie zertifikatbasierte Authentifizierung verwenden möchten, konfigurieren Sie XenMobile und Ihr NetScaler Gateway, sodass zertifikatbasierte Authentifizierung unterstützt wird. In XenMobile ist unter **Einstellungen > NetScaler Gateway** die Option **Benutzerzertifikat für Authentifizierung bereitstellen** standardmäßig auf **Aus** festgelegt, sodass die Authentifizierung durch Benutzername und Kennwort erfolgt. Ändern Sie die Einstellung auf **Ein**. Informationen zur Konfiguration finden Sie unter Zertifikatauthentifizierung im ausschließlichen MAM-Modus.
6. Achten Sie bei der Auswahl oder beim Einrichten einer Benachrichtigungsvorlage für die Verwendung mit dem ausschließlichen MAM-Modus darauf, dass SMTP die einzige unterstützte Methode zum Senden von Registrierungseinladungen ist.
7. Wenn Ihre Benutzer auf den neuen ausschließlichen MAM-Modus aktualisiert werden, stellen Sie ihnen die FQDN für den XenMobile-Server bereit und teilen Sie ihnen mit, dass sie sich erneut registrieren müssen.
   Im neuen ausschließlichen MAM-Modus werden Geräte, wie im ENT-Modus, mit dem FQDN des XenMobile-Servers registriert. (Im Legacy-MAM-Modus werden Geräte mit dem NetScaler Gateway-FQDN registriert).

In der folgenden Tabelle werden die Unterschiede zwischen den Legacy-MAM-Funktionen (XenMobile 10.3 und XenMobile

10.3.5) und dem neuen ausschließlichen MAM-Modus (XenMobile 10.3.5) aufgeführt.

Registrierungsszenarios und andere Features	XenMobile 10,3 Legacy-MAM (Servermodus ist ENT)	XenMobile 10.3.5 Legacy-MAM (Servermodus ist ENT)	XenMobile 10.3.5 Ausschließlicher MAM-Modus (Servermodus ist MAM)
Zertifikatauthentifizierung	Nicht unterstützt.	Nicht unterstützt.	Unterstützt. Für die Zertifikatauthentifizierung ist NetScaler Gateway erforderlich.
Bereitstellungsanforderungen	XenMobile-Server muss nicht direkt von Geräten aus zugänglich sein.	XenMobile-Server muss nicht direkt von Geräten aus zugänglich sein.	XenMobile-Server muss von Geräten aus zugänglich sein.
Registrierungsoption	Verwenden Sie den NetScaler Gateway-FQDN oder lehnen Sie die Registrierung ab.	Verwenden Sie den NetScaler Gateway-FQDN oder lehnen Sie die Registrierung ab.	Verwenden Sie den XenMobile-Server-FQDN.
Registrierungsmethoden	Benutzername + Kennwort	Benutzername + Kennwort	Benutzername + Kennwort, Hohe Sicherheit, Einladungs-URL, Einladungs-URL + PIN, Einladungs-URL + Kennwort, Zweifaktor, Benutzername + PIN
Apps sperren und löschen	Unterstützt.	Unterstützt.	Unterstützt.
Selbsthilfeportaloptionen zum Sperren und Löschen von Apps	Nicht unterstützt.	Nicht unterstützt.	Unterstützt.
App-Löschen - Verhalten	Apps bleiben auf dem Gerät, sind aber nicht verwendbar. Konto wird nur auf dem Client gelöscht.	Apps bleiben auf dem Gerät, sind aber nicht verwendbar. Konto wird nur auf dem Client gelöscht.	Apps bleiben auf dem Gerät, sind aber nicht verwendbar. Konto wird nur auf dem Client gelöscht.
		Mit Ereignissen, Geräteeigenschaften und	Mit Ereignissen, Geräteeigenschaften und

Automatisierte Aktionen für ausschließliche MAM-Benutzer.	Nicht unterstützt.	Benutzereigenschaften verbundene Aktionen werden unterstützt. Automatisierte Aktionen für installierte Apps werden nicht unterstützt.	Benutzereigenschaften verbundene Aktionen werden unterstützt. Automatisierte Aktionen für installierte Apps werden nicht unterstützt.
Integrierte Aktion beim Löschen eines Active Directory-Benutzers	Nicht unterstützt.	App-Löschen wird unterstützt.	App-Löschen wird unterstützt.
Registrierungslimit	Unterstützt nur für MDM, Konfiguration über eine Servereigenschaft.	Unterstützt, Konfiguration über ein Registrierungsprofil.	Unterstützt, Konfiguration über ein Registrierungsprofil.
Softwarebestand	Unterstützt; XenMobile listet auf dem Gerät installierte Apps auf	Unterstützt; XenMobile listet auf dem Gerät installierte Apps auf	Nicht unterstützt.

In einer MAM-Only-Bereitstellung von XenMobile können Sie einen XenMobile-Servercluster in der DMZ oder im internen Netzwerk bereitstellen. In jedem Szenario erfolgt die Authentifizierung über NetScaler Gateway.

Im Gegensatz zu einer XenMobile Enterprise-Bereitstellung sind XenMobile NetScaler Connector (XNC) und XenMobile Mail Manager (XMM) nicht erforderlich.

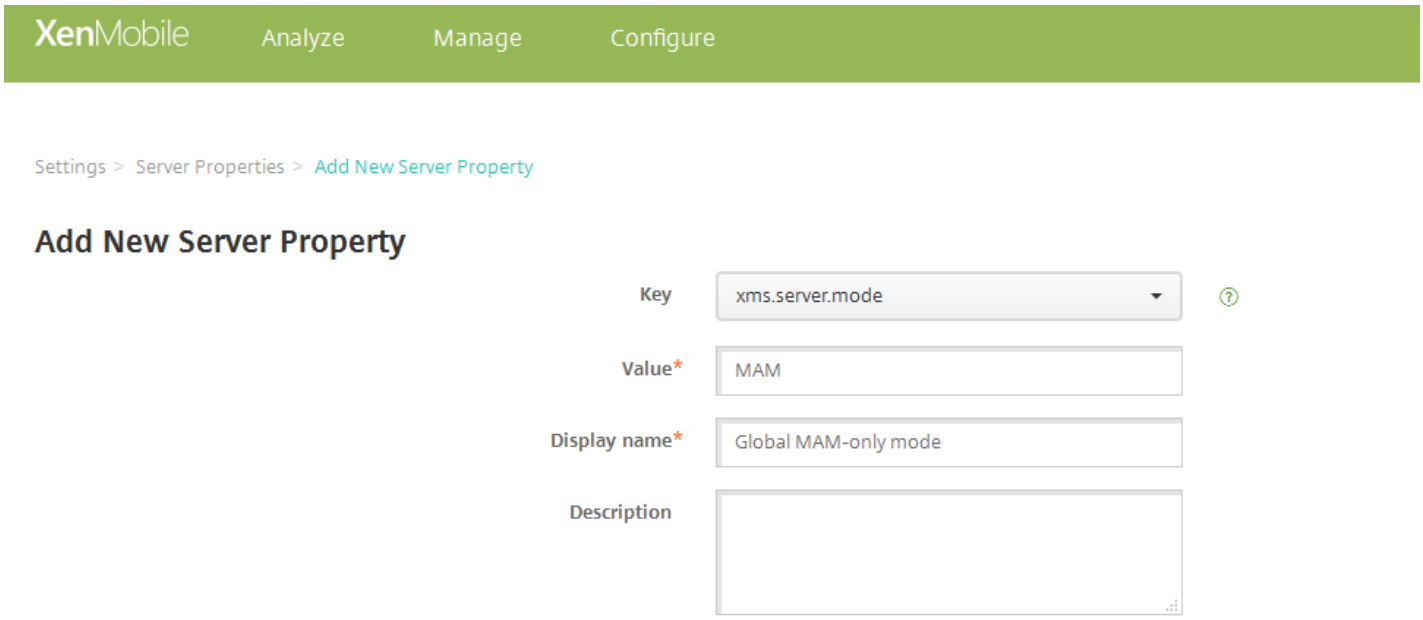
Ein Architekturdiagramm finden Sie im Artikel Reference Architecture for On-Premises Deployments in der XenMobile-Bereitstellungsdokumentation.

- Erforderliche Apps werden nicht automatisch installiert. Benutzer müssen sie manuell aus dem WorxStore hinzufügen.
- Benutzer von iOS-Geräten müssen dem iOS Developer-Zertifikat vertrauen. Benutzer von Android-Geräten müssen die Einstellung aktivieren, die das Installieren aus den App-Stores von Drittanbietern zulässt.
- Benutzer erhalten nur in WorxStore App-Updatebenachrichtigungen.
- Wenn ein Benutzer Worx Home entfernt oder seine Registrierung bei Worx Home aufhebt, verbleiben die installierten Apps auf dem Gerät, bis der Benutzer sie entfernt.
- Der Nur-MAM-Modus unterstützt APNs oder Google Cloud Messaging.
- Die XenMobile-Konsole enthält nicht den Status von Geräten mit Jailbreak oder Rooting, die im Nur-MAM-Modus registriert sind. Die Richtlinie **Mit Jailbreak oder Root blockieren** funktioniert jedoch für diese Geräte.

Nach einer Neuinstallation ist der Server standardmäßig im ENT-Modus. Konfigurieren Sie den Server wie folgt, um den ausschließlichen MAM-Modus für XenMobile 10.3.5 zu aktivieren:

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol oben rechts, um die Seite **Einstellungen** anzuzeigen.
2. Klicken Sie auf der Seite **Einstellungen** auf **Servereigenschaften**.
3. Klicken Sie auf **Hinzufügen**.
4. Klicken Sie in **Schlüssel** auf **xms.server.mode**.
5. Geben Sie **MAM** in **Wert** ein.
6. Geben Sie in **Anzeigename** eine Beschreibung ein. Diese wird in der Tabelle **Servereigenschaften** angezeigt.

Geben Sie optional eine Beschreibung ein und klicken Sie dann auf **Speichern**.



Important

Wenn Sie die Eigenschaft xms.server.mode auf den ausschließlichen MAM-Modus festgelegt haben, werden in der XenMobile-Konsole weiterhin Bereiche angezeigt, für die der MDM-Modus gilt, z. B. Geräteeigenschaften. Diese Einstellungen funktionieren jedoch nicht.

Zertifikatauthentifizierung im ausschließlichen MAM-Modus

Jul 28, 2016

Zum Verwenden von Zertifikatauthentifizierung im ausschließlichen MAM-Modus müssen Sie den Microsoft-Server, den XenMobile-Server und den NetScaler Gateway-Server konfigurieren. Die folgenden allgemeinen Schritte werden in diesem Artikel ausführlich erläutert.

Auf dem Microsoft-Server:

1. Fügen Sie der Microsoft Management Console ein Zertifikat-Snap-In hinzu.
2. Fügen Sie der Zertifizierungsstelle (ZS) eine Vorlage hinzu.
3. Erstellen Sie ein PFX-Zertifikat vom ZS-Server.

Auf dem XenMobile-Server:

1. Laden Sie das Zertifikat in XenMobile hoch.
2. Erstellen Sie die PKI-Entität für zertifikatbasierte Authentifizierung.
3. Konfigurieren Sie Anmeldeinformationsanbieter.
4. Konfigurieren Sie NetScaler Gateway, um ein Benutzerzertifikat für die Authentifizierung bereitzustellen.

In NetScaler Gateway:

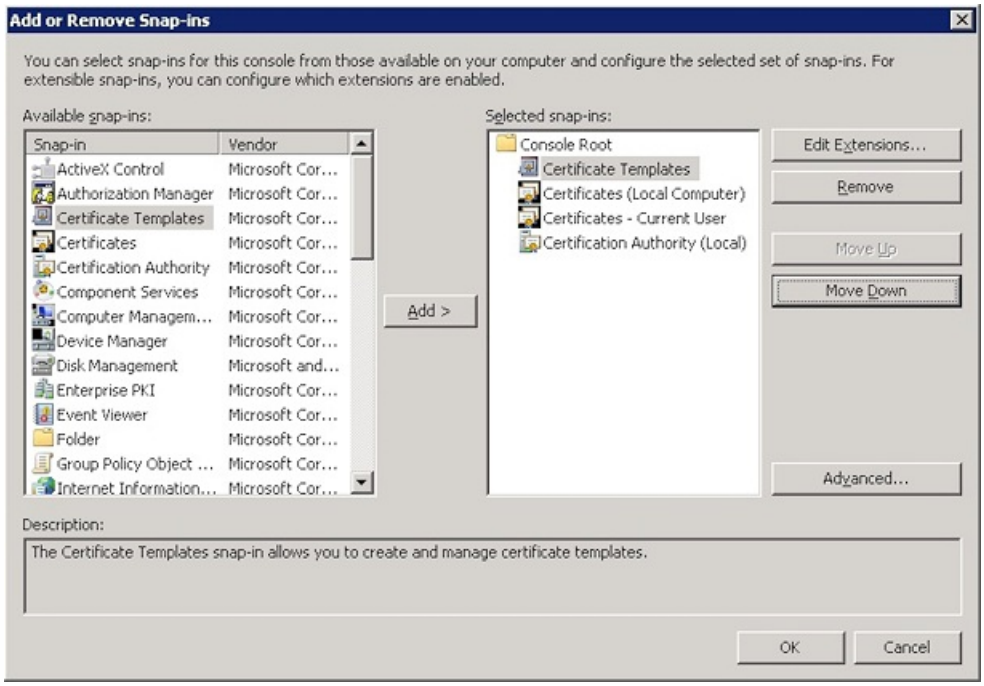
1. Konfigurieren Sie NetScaler Gateway für die Zertifikatauthentifizierung im ausschließlichen XenMobile MAM-Modus.

Hinzufügen eines Zertifikat-Snap-Ins zur Microsoft Management Console

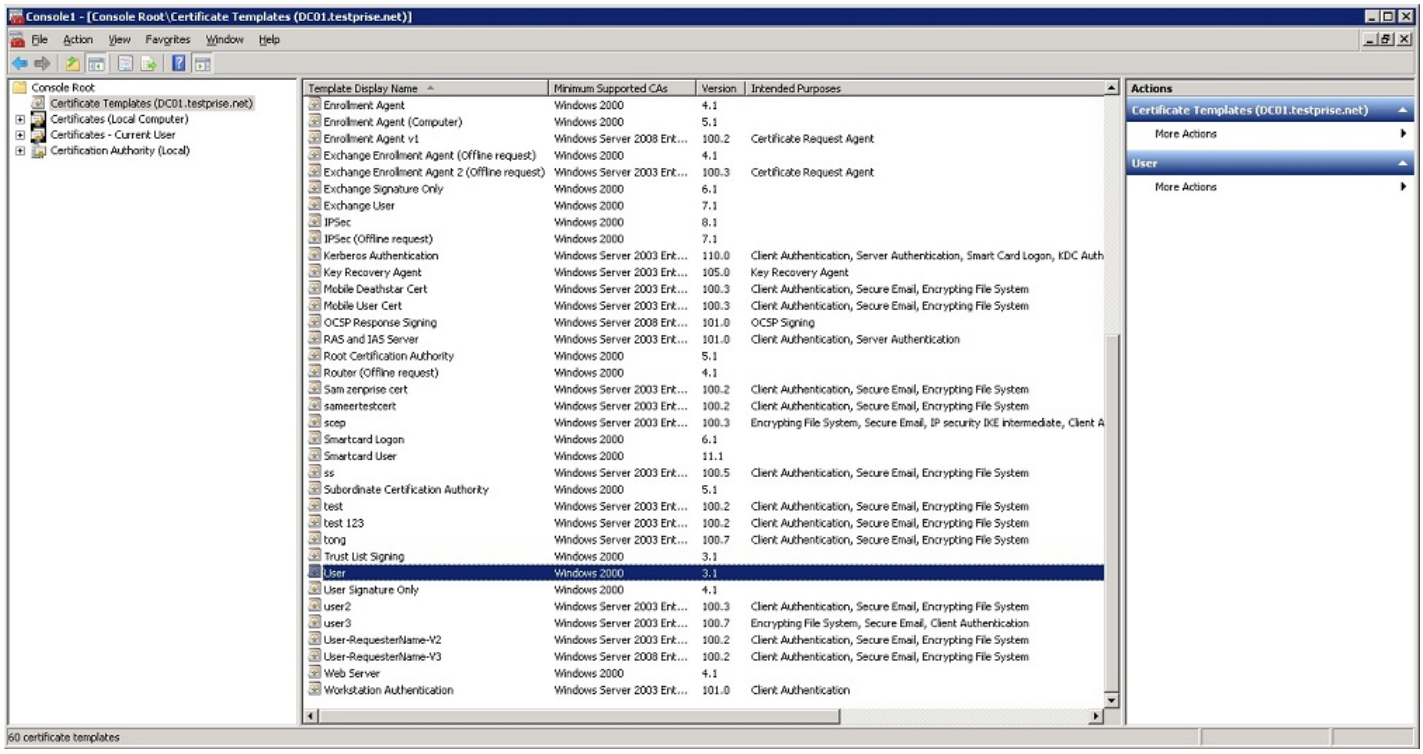
1. Öffnen Sie die Konsole und klicken Sie auf **Snap-In hinzufügen/entfernen**.

2. Fügen Sie die folgenden Snap-Ins hinzu:

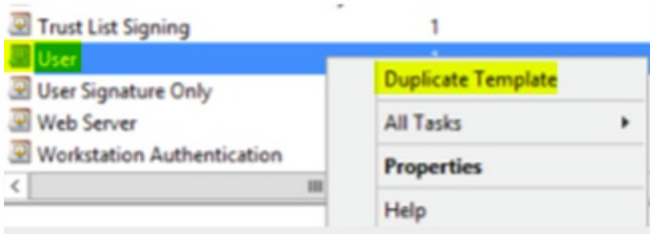
    Zertifikatvorlagen
    Zertifikate (Lokaler Computer)
    Zertifikate – aktueller Benutzer
    Zertifizierungsstelle (Lokal)



3. Erweitern Sie **Zertifikatvorlagen**.



4. Wählen Sie die Vorlage **Benutzer** und dann **Doppelte Vorlage**.

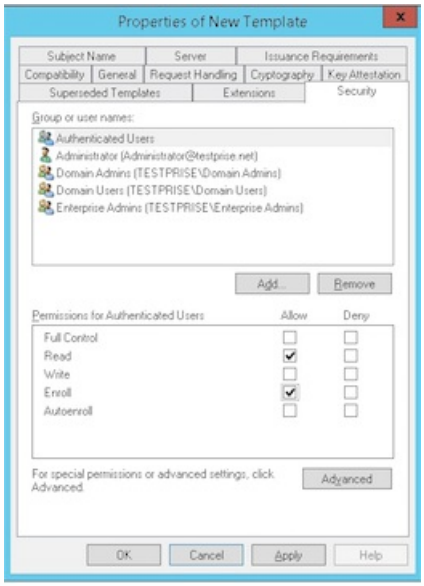


5. Geben Sie den Anzeigenamen der Vorlage an.

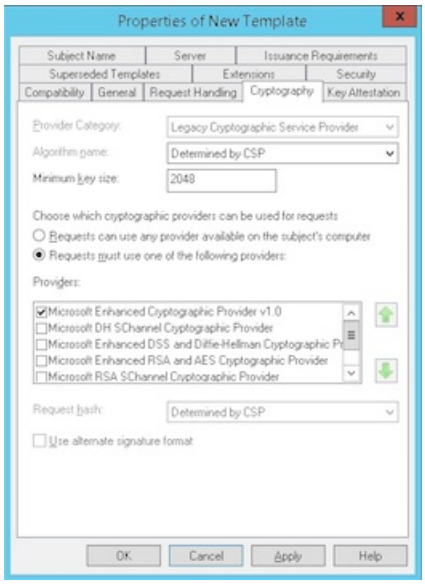
> **Wichtig:** Aktivieren Sie das Kontrollkästchen **Zertifikat in Active Directory veröffentlichen** nur bei Bedarf. Wenn diese Option aktiviert ist, werden alle Benutzer-Clientzertifikate in Active Directory erstellt/bereitgestellt, wodurch Ihre Active Directory-Datenbank überladen werden kann.

6. Wählen Sie als Vorlagentyp "Windows 2003 Server". Wählen Sie in Windows 2012 R2-Server unter **Kompatibilität** die Option **Zertifizierungsstelle** und legen Sie als Empfänger "Windows 2003" fest.

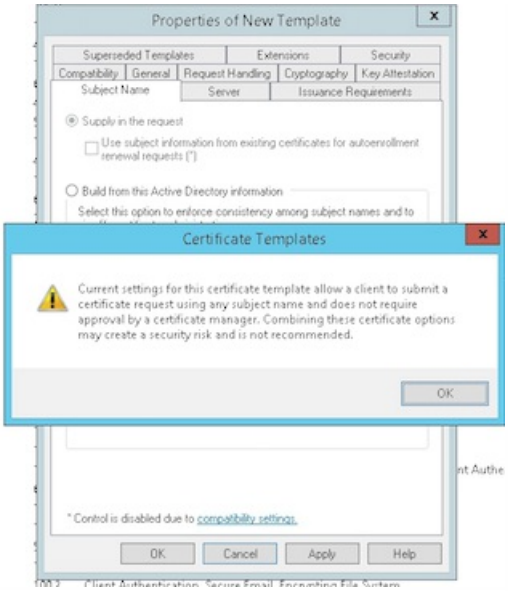
7. Wählen Sie unter **Sicherheit** in der Spalte **Zulassen** die Option **Registrieren** für die authentifizierten Benutzer aus.



8. Stellen Sie unter **Kryptografie** die Schlüsselgröße zur Verfügung, die Sie während der Konfiguration von XenMobile eingeben müssen.



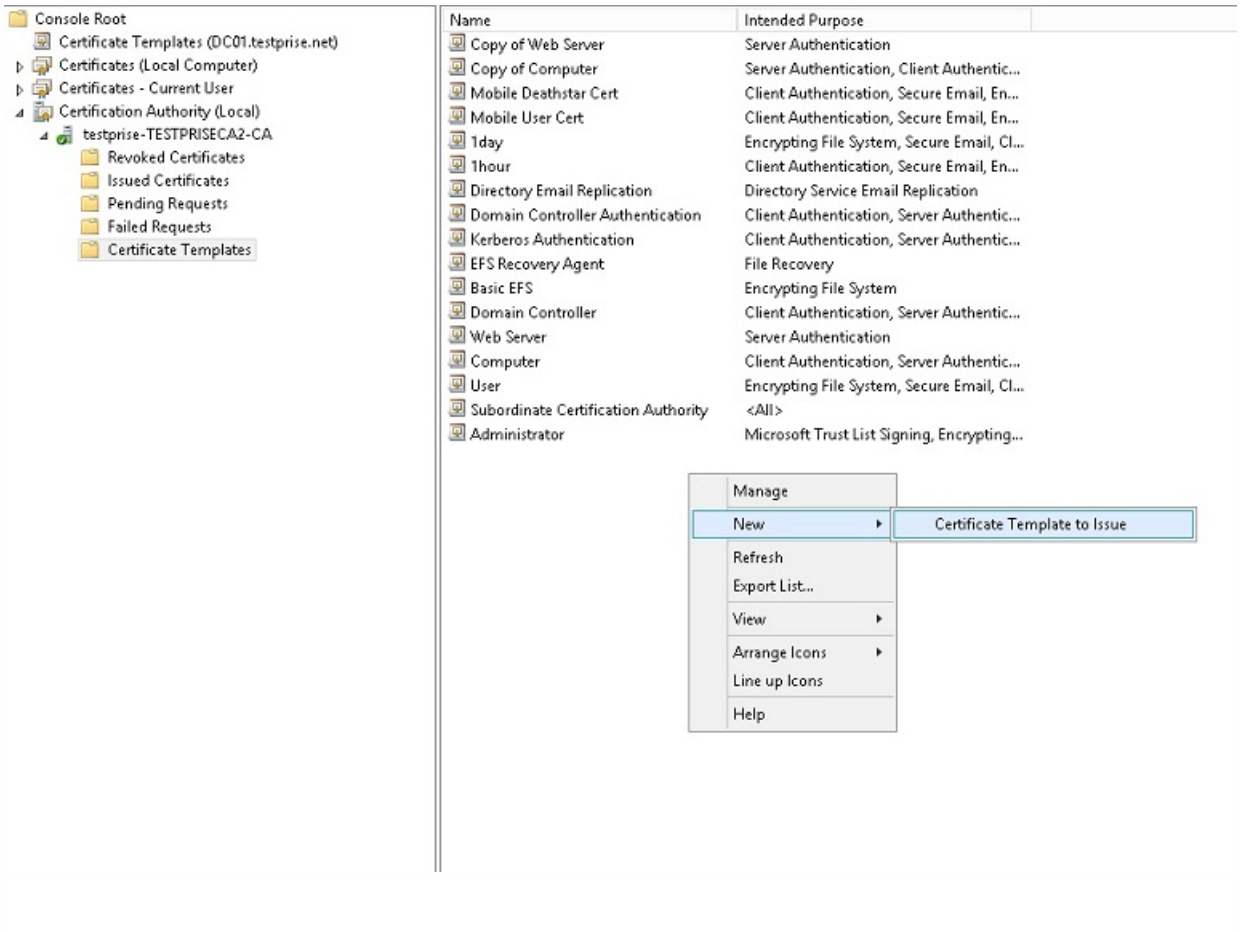
9. Wählen Sie unter **Antragstellername** die Option **Informationen werden in der Anforderung angegeben** aus. Wenden Sie die Änderungen an und speichern Sie.



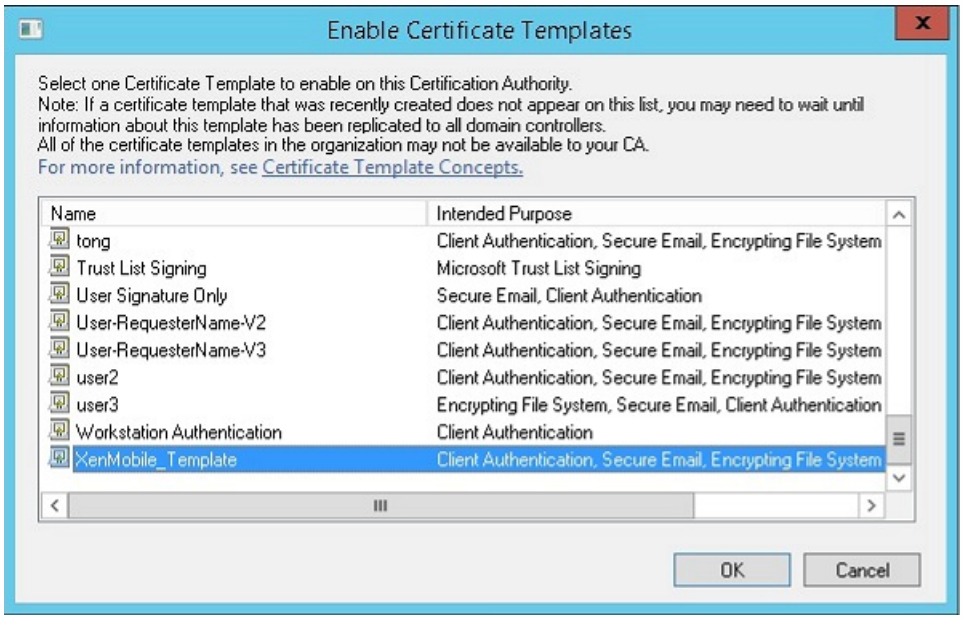
Hinzufügen der Vorlage zur Zertifizierungsstelle

1. Navigieren Sie zu **Zertifizierungsstelle** und wählen Sie **Zertifikatvorlagen**.

2. Klicken Sie mit der rechten Maustaste in den rechten Bereich und wählen Sie **Neu > Auszustellende Zertifikatvorlage**.



3. Wählen Sie die im vorherigen Schritt erstellte Vorlage und klicken Sie auf **OK**, um sie der Zertifizierungsstelle hinzuzufügen.

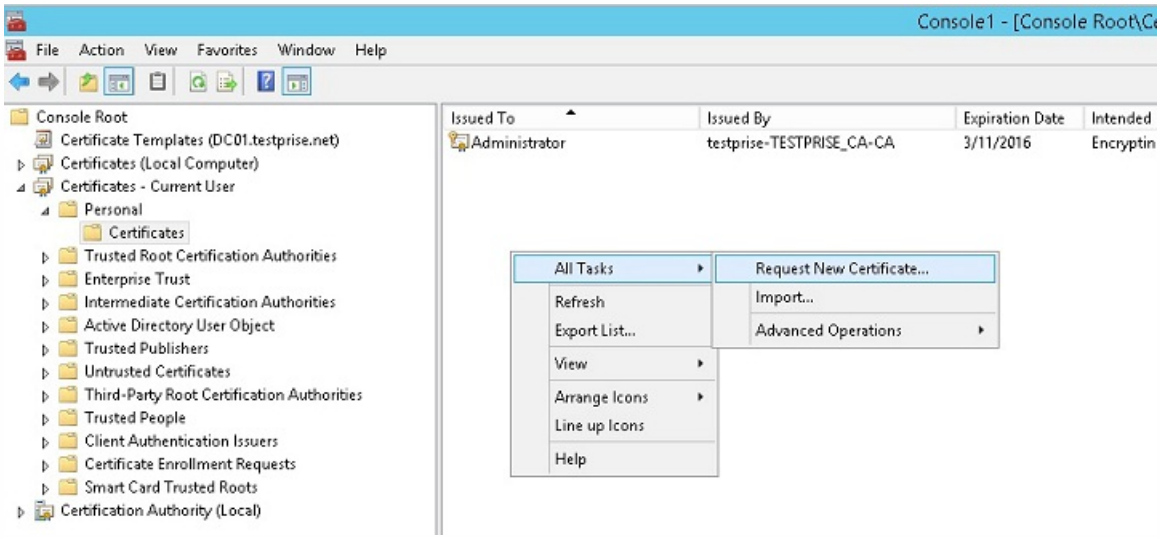


Erstellen eines PFX-Zertifikats vom ZS-Server

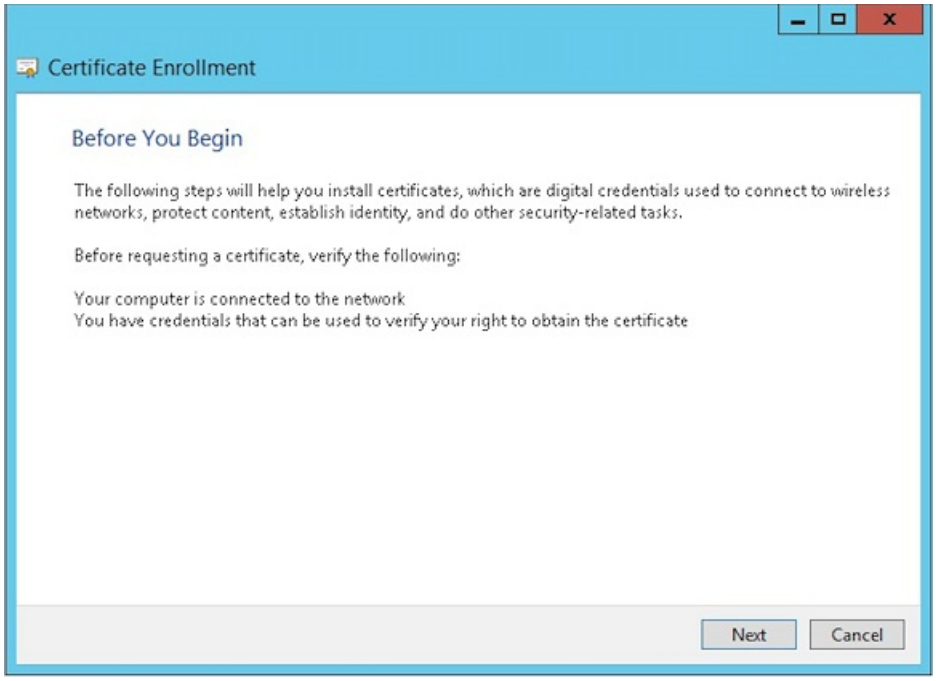
1. Erstellen Sie mit dem Dienstkonto, mit dem Sie sich angemeldet haben, ein PFX-Benutzerzertifikat. Diese PFX-Datei wird in XenMobile hochgeladen, um ein Benutzerzertifikat im Namen der Benutzer anzufordern, die ihre Geräte registrieren.

2. Erweitern Sie **Zertifikate** unter **Aktueller Benutzer**.

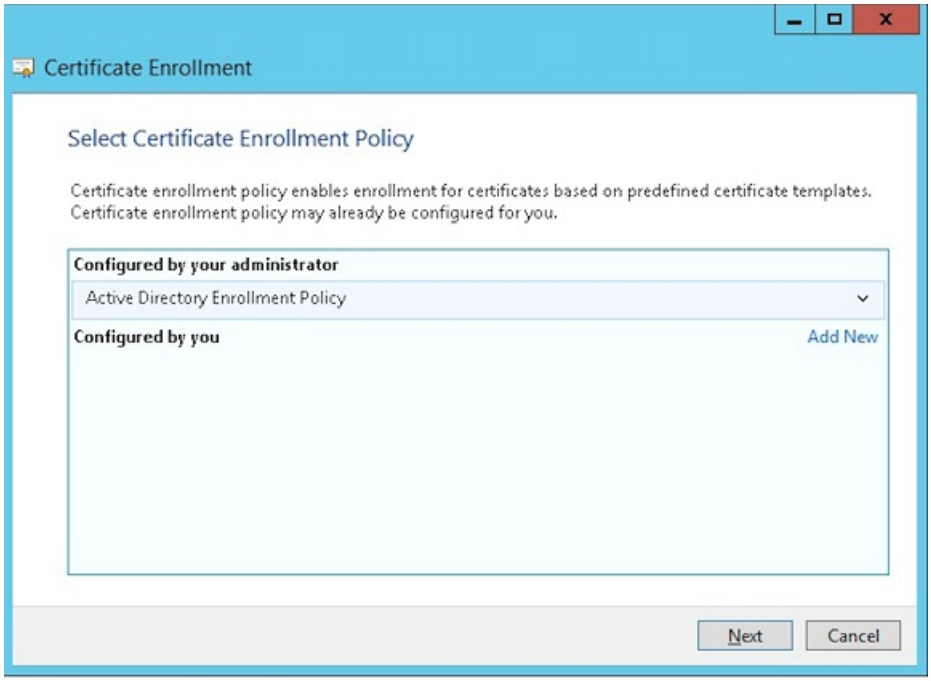
3. Klicken Sie mit der rechten Maustaste in den rechten Bereich und klicken Sie auf **Neues Zertifikat anfordern**.



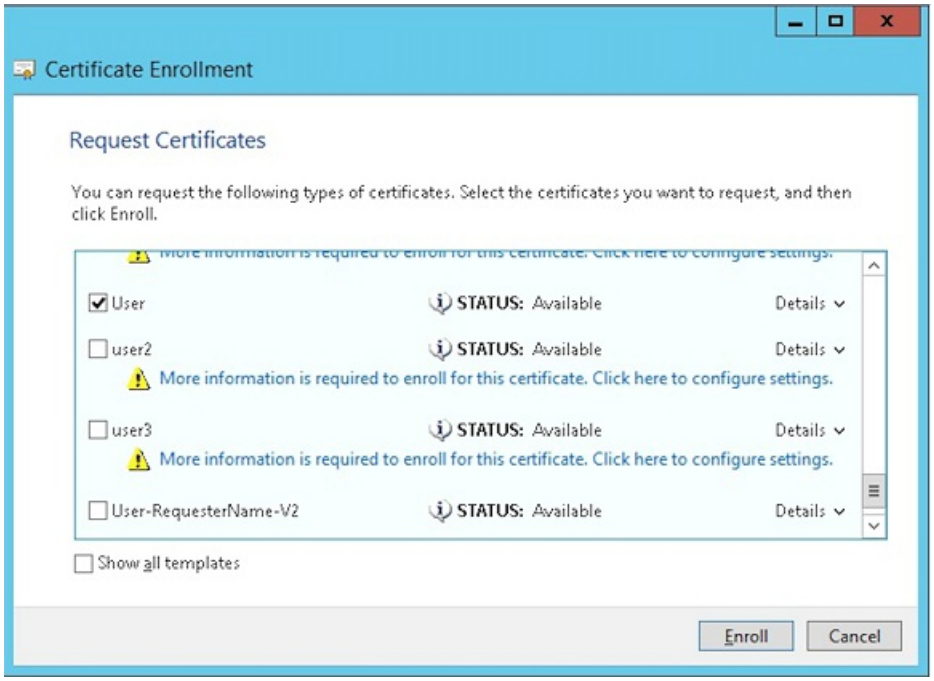
4. Der Bildschirm **Zertifikatregistrierung** wird angezeigt. Klicken Sie auf **Weiter**.



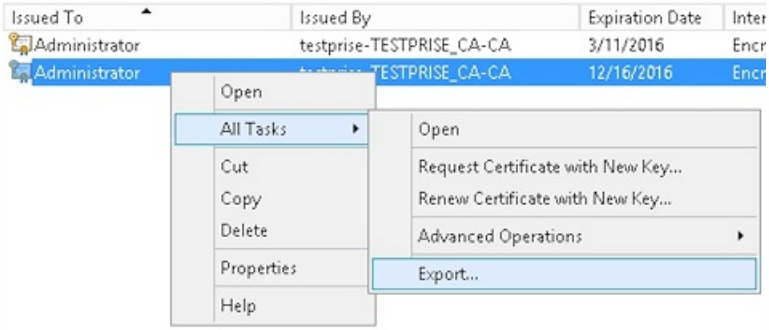
5. Wählen Sie **Active Directory-Registrierungsrichtlinie** und klicken Sie auf **Weiter**.



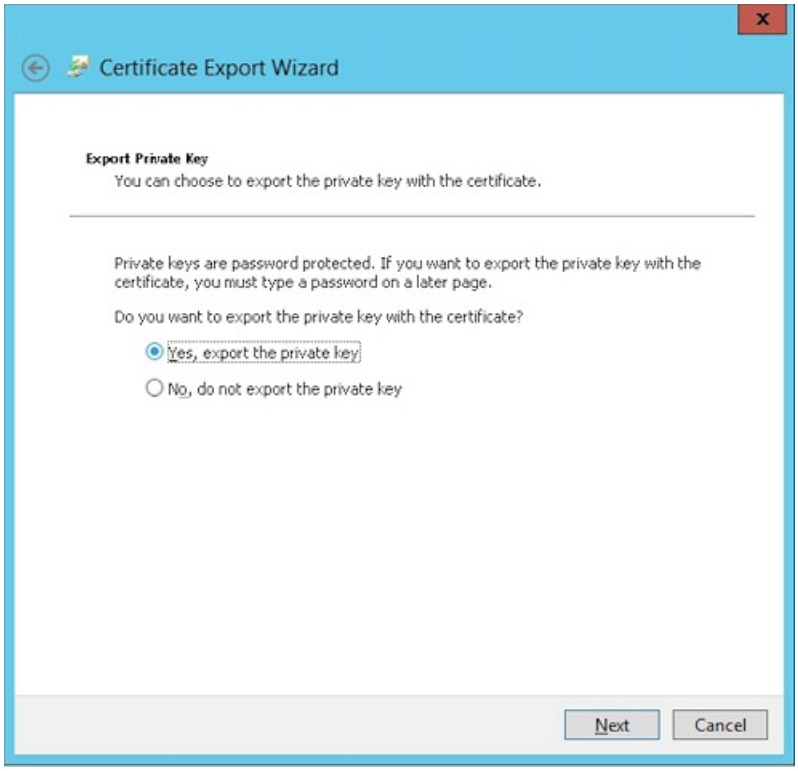
6. Wählen Sie die Vorlage **Benutzer** und klicken Sie auf **Registrieren**.



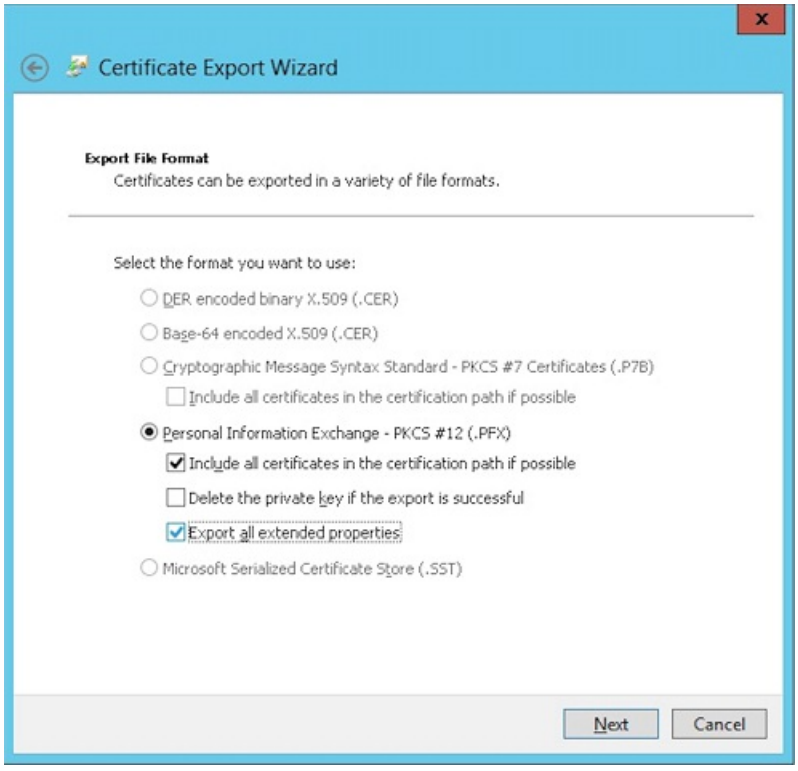
7. Exportieren Sie die PFX-Datei, die Sie im vorherigen Schritt erstellt haben.



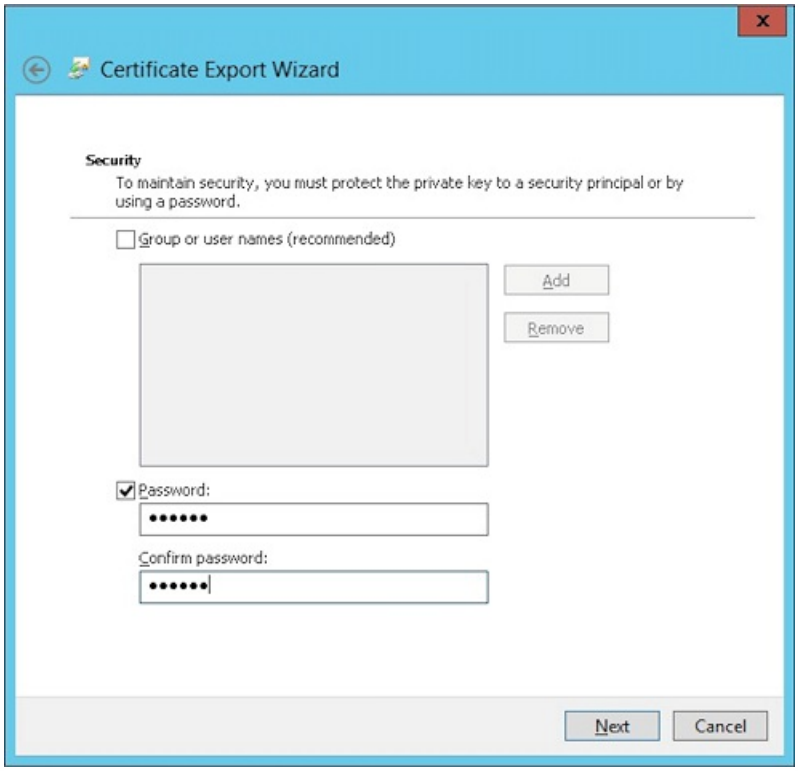
8. Klicken Sie auf **Ja, privaten Schlüssel exportieren**.



9. Aktivieren Sie die Kontrollkästchen **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen** und **Alle erweiterten Eigenschaften exportieren**.



10. Legen Sie ein Kennwort für den Upload des Zertifikats in XenMobile fest.



11. Speichern Sie das Zertifikat auf Ihrer Festplatte.

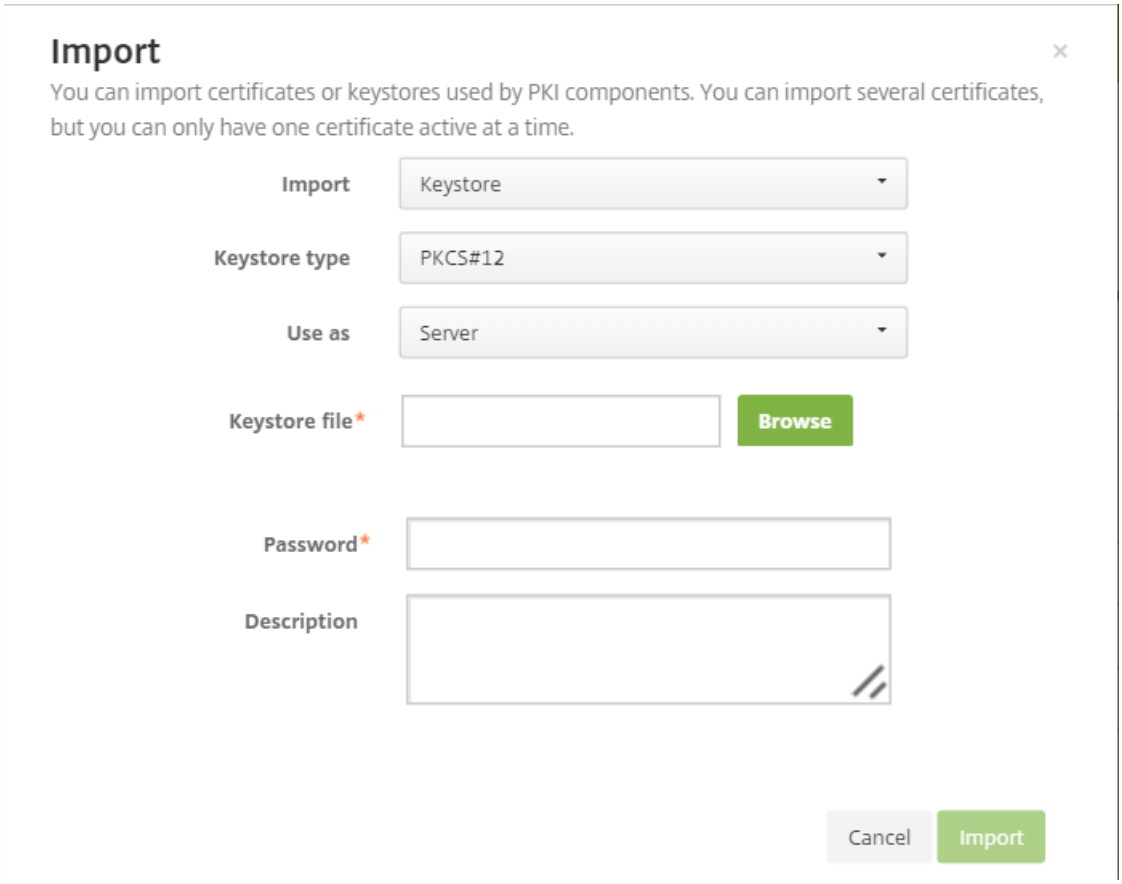
Hochladen des Zertifikats in XenMobile

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Der Bildschirm **Einstellungen** wird angezeigt.

2. Klicken Sie auf **Zertifikate** und dann auf **Importieren**.

3. Geben Sie die folgenden Parameter ein:

- **Importieren**: Schlüsselspeicher
- **Schlüsselspeichertyp**: PKCS#12
- **Verwenden als**: Server
- **Schlüsselspeicherdatei**: Klicken Sie auf **Durchsuchen**, um das erstellte PFX-Zertifikat zu suchen.
- **Kennwort**: Geben Sie das Kennwort ein, das Sie für dieses Zertifikat erstellt haben.



5. Klicken Sie auf **Importieren**.

6. Prüfen Sie, ob das Zertifikat richtig installiert wurde. Es sollte als ein Benutzerzertifikat angezeigt werden.

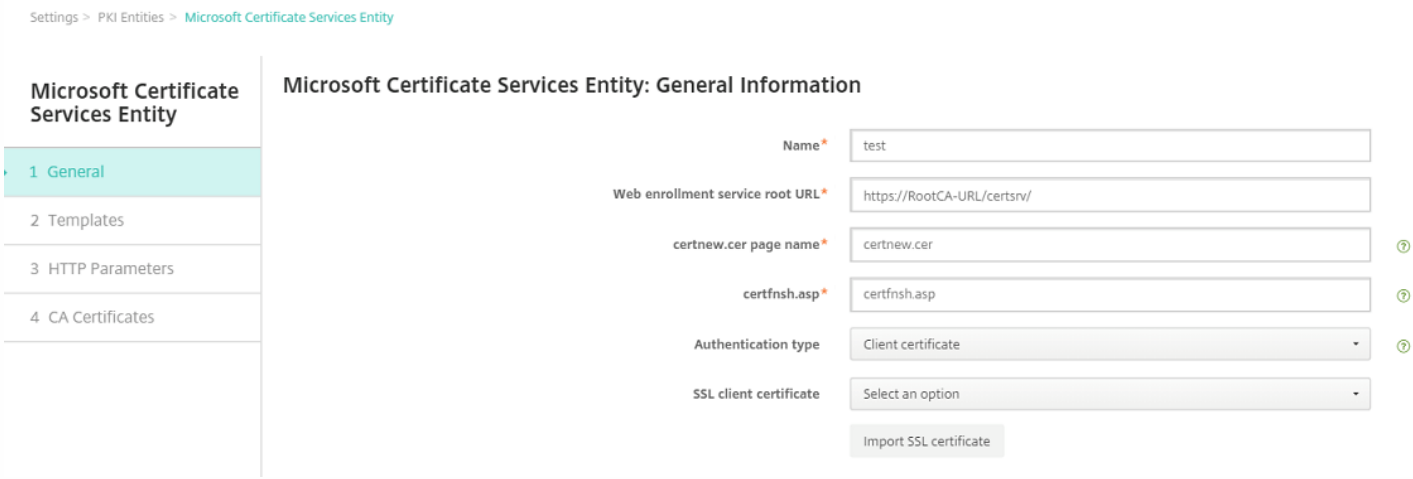
Erstellen der PKI-Entität für zertifikatbasierte Authentifizierung

1. Gehen Sie in **Einstellungen** zu **Mehr > Zertifikatverwaltung > PKI-Entitäten**.

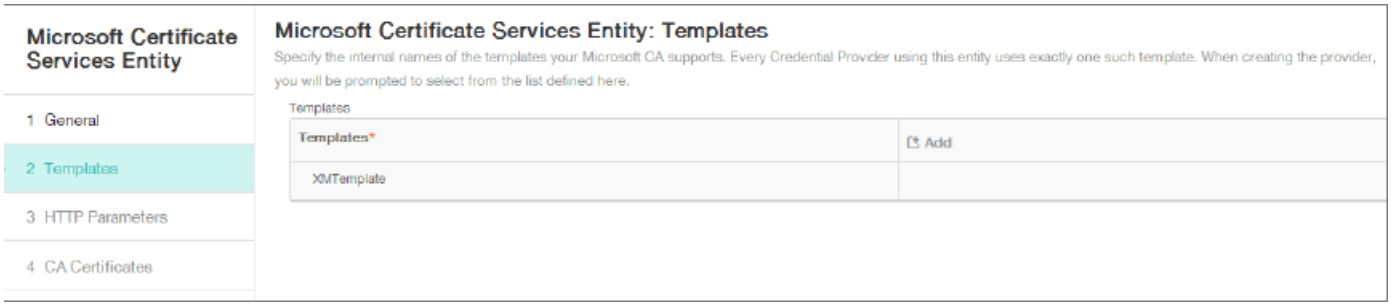
2. Klicken Sie auf **Hinzufügen** und dann auf **Microsoft Zertifikatdiensteentität**. Der Bildschirm "Microsoft Zertifikatdiensteentität: Allgemeine Informationen" wird angezeigt.

3. Geben Sie die folgenden Parameter ein:

- **Name**: Geben Sie einen Namen ein.
- **Stamm-URL des Webregistrierungsdiensts**: https://RootCA-URL/certsrv/
  Hinweis: Geben Sie auf jeden Fall den letzten Schrägstrich (/) im URL-Pfad ein.
- **certnew.cer-Seitenname**: certnew.cer (Standardwert)
- **certfnsh.asp**: certfnsh.asp (Standardwert)
- **Authentifizierungstyp**: Clientzertifikat
- **SSL-Clientzertifikat**: Wählen Sie die Stammzertifizierungsstelle aus, die das XenMobile-Clientzertifikat signiert hat.

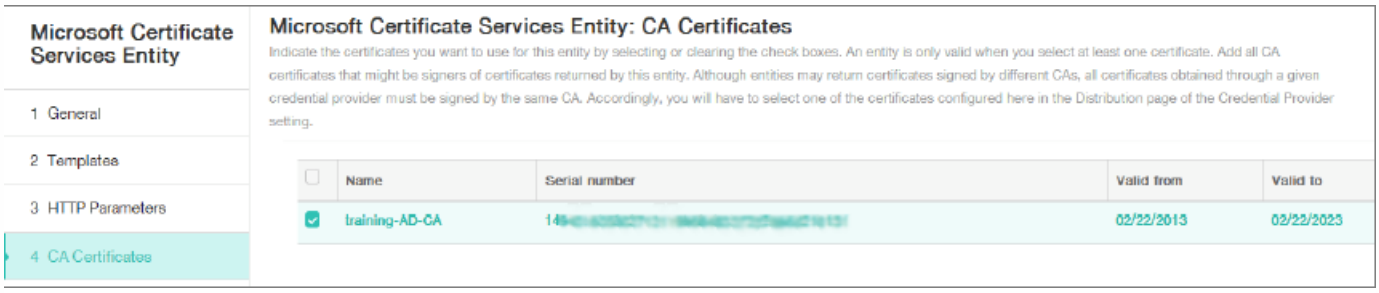


4. Fügen Sie unter **Vorlagen** die Vorlage hinzu, die Sie beim Konfigurieren des Microsoft-Zertifikats erstellt haben. Leerstellen sind nicht zulässig.



5. Überspringen Sie HTTP-Parameter und klicken Sie auf **ZS-Zertifikate**.

6. Wählen Sie das Benutzerzertifikat aus, das für die Ausstellung des XenMobile-Clientzertifikats verwendet werden soll. Die gehört zur Kette, die aus dem XenMobile-Clientzertifikat importiert wurde.



7. Klicken Sie auf **Speichern**.

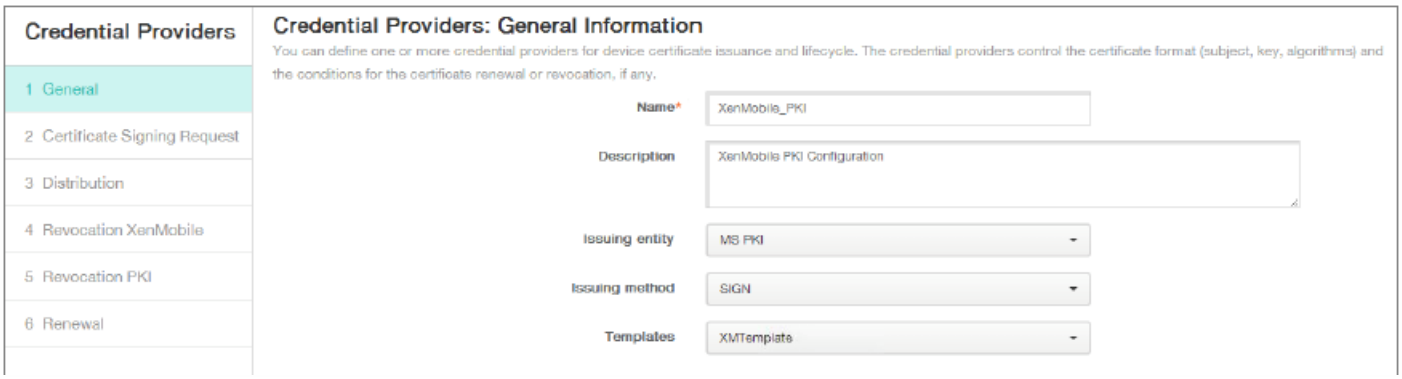
Konfigurieren von Anmeldeinformationsanbietern

1. Navigieren Sie unter "Einstellungen" zu **Mehr > Zertifikatverwaltung > Anbieter für Anmeldeinformationen**.

2. Klicken Sie auf **Hinzufügen**.

3. Geben Sie unter **Allgemein** die folgenden Parameter ein:

- **Name**: Geben Sie einen Namen ein.
- **Beschreibung**: Geben Sie eine Beschreibung ein.
- **Ausstellende Entität**: Wählen Sie die zuvor erstellte PKI-Entität aus.
- **Ausstellungsmethode**: SIGN
- **Vorlagen**: Wählen Sie die unter der PKI-Entität hinzugefügte Vorlage aus.



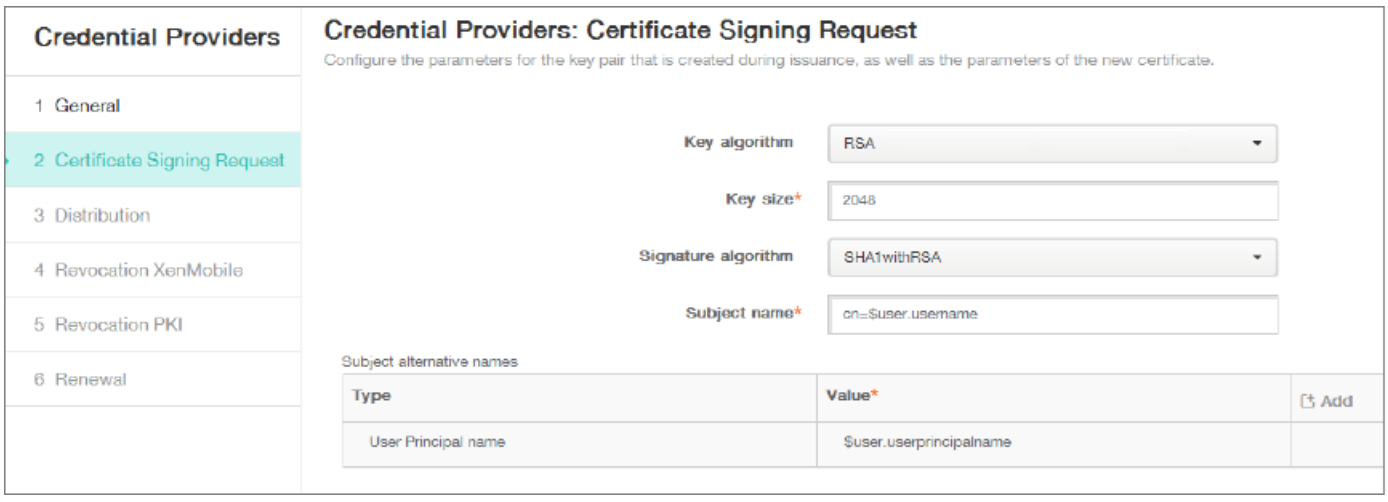
4. Klicken Sie dann auf **Zertifikatsignieranforderung** und geben Sie die folgenden Parameter ein:

- **Schlüsselalgorithmus**: RSA
- **Schlüsselgröße**: 2048
- **Signaturalgorithmus**: SHA1withRSA
- **Antragstellername**: cn=$user.username

  Der Antragstellername verweist auf sAMAccountName. Dadurch kann NetScaler das Benutzernamenfeld für die Authentifizierung verwenden.

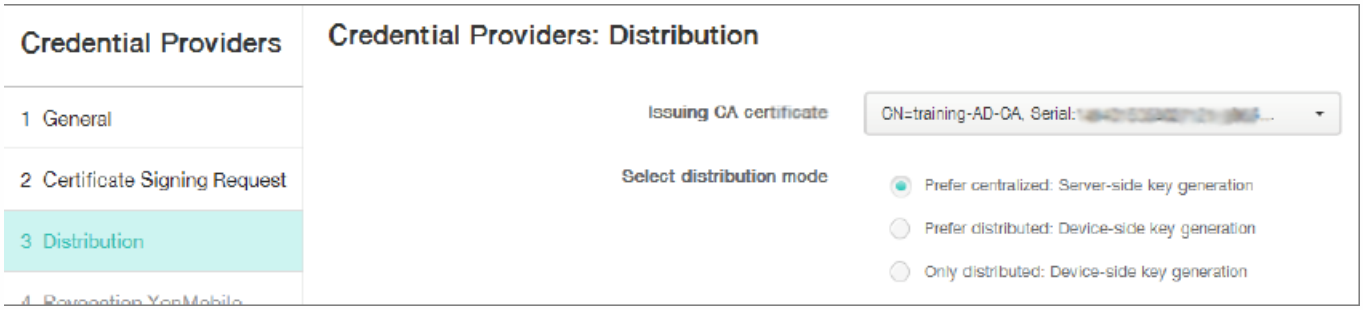
5. Klicken Sie für **Alternative Antragstellernamen** auf **Hinzufügen** und geben Sie die folgenden Parameter ein:

- **Typ**: Benutzerprinzipalname
- **Wert**: $user.userprincipalname



6. Klicken Sie auf **Verteilung** und geben Sie die folgenden Parameter ein:

- **Zertifikat der ausstellenden ZS**: Wählen Sie die ausstellende Zertifizierungsstelle, die das XenMobile-Clientzertifikat signiert hat.
- **Verteilungsmodus wählen**: Wählen Sie **Bevorzugt zentralisiert: Schlüssel serverseitig generieren**.

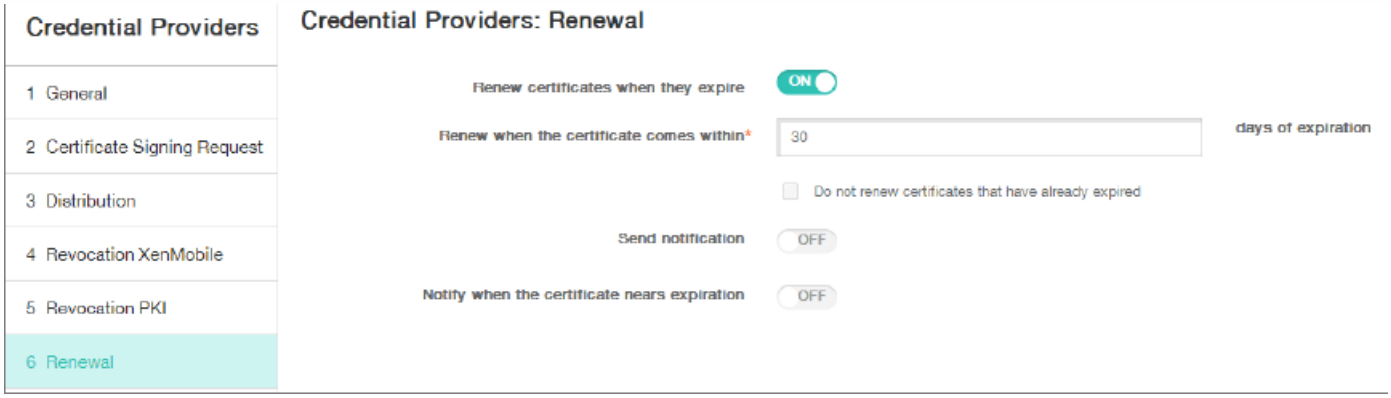


7. Legen Sie für die zwei folgenden Abschnitte **XenMobile-Sperrung** und **PKI-Sperrung** die Parameter nach Bedarf fest. Die beiden Optionen werden in diesem Artikel übersprungen.

8. Klicken Sie auf **Verlängerung**.

9. Wählen Sie für **Zertifikate erneuern, wenn sie ablaufen** die Option **EIN**.

10. Behalten Sie für alle anderen Einstellungen die Standardwerte bei oder ändern Sie sie nach Bedarf.



11. Klicken Sie auf **Speichern**.

Konfigurieren der NetScaler-Zertifikatbereitstellung in XenMobile

1. Melden Sie sich an der XenMobile-Konsole an und klicken Sie auf das Zahnradsymbol rechts oben. Der Bildschirm **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **NetScaler Gateway**.

3. Wenn NetScaler Gateway noch nicht hinzugefügt wurde, klicken Sie auf **Hinzufügen** und legen Sie folgende Einstellungen fest:

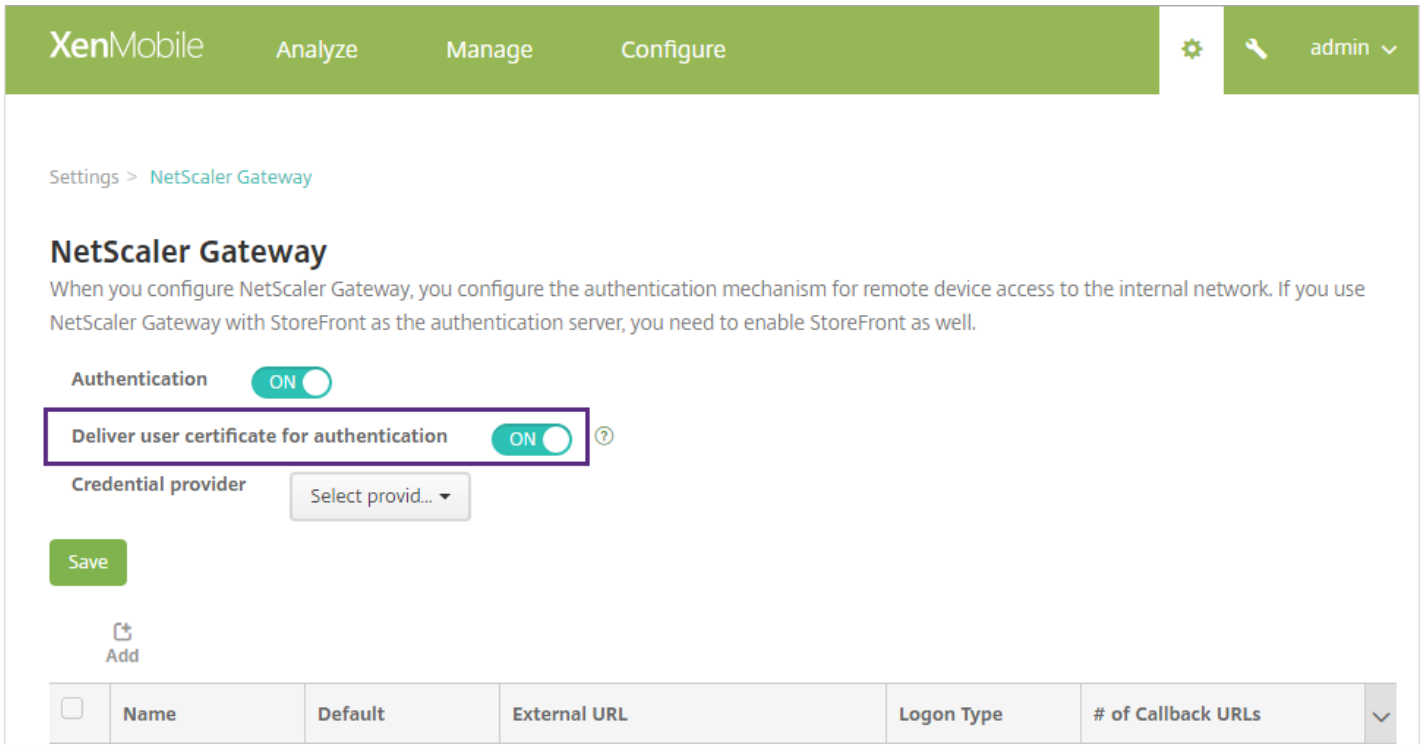
Externe URL: https://URLIhresNetScalerGateways

Anmeldetyp: Zertifikat

Kennwort erforderlich: AUS

Als Standard setzen: EIN

4. Legen Sie **Benutzerzertifikat für Authentifizierung bereitstellen** auf **Ein** fest und klicken Sie auf **Speichern**.



5. Wählen Sie unter **Anmeldeinformationsanbieter** einen Anbieter und klicken Sie auf **Speichern**.

Konfigurieren Sie NetScaler Gateway für die Zertifikatauthentifizierung

Führen Sie die folgenden Schritte auf dem NetScaler Gateway-Gerät aus, um die Clientzertifikatauthentifizierung in XenMobile im ausschließlichen MAM-Modus zu konfigurieren.

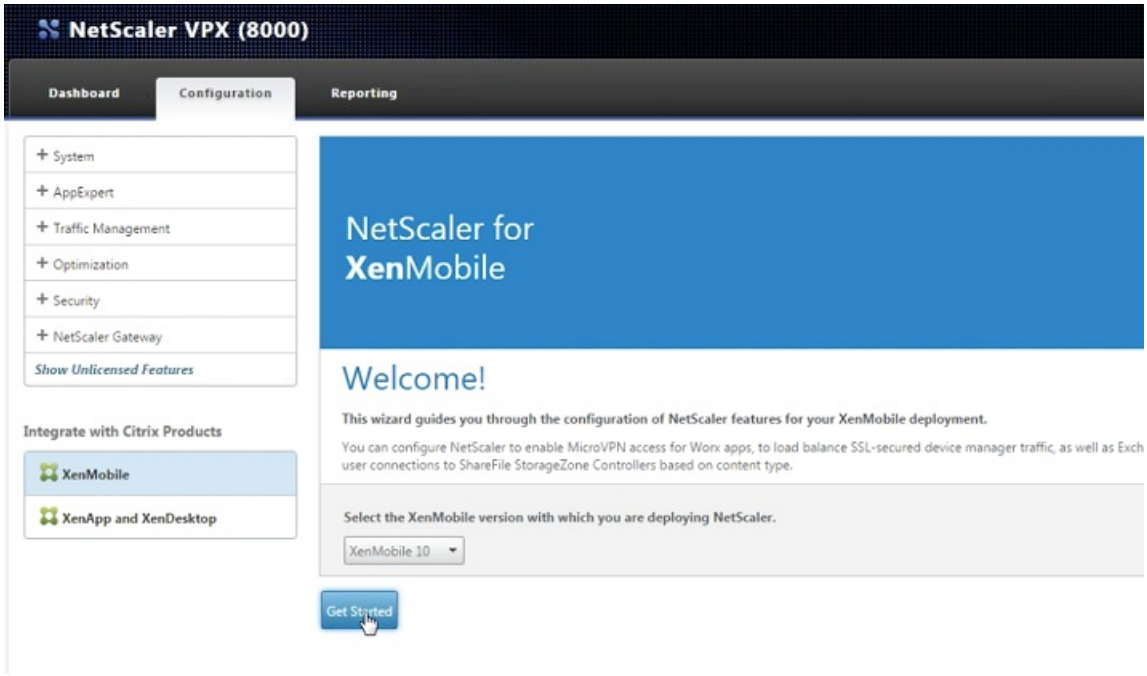
1. Melden Sie sich an NetScaler an.

2. Klicken Sie unter **Configuration** auf **Integrate with Citrix Products** und wählen Sie dann **XenMobile**.

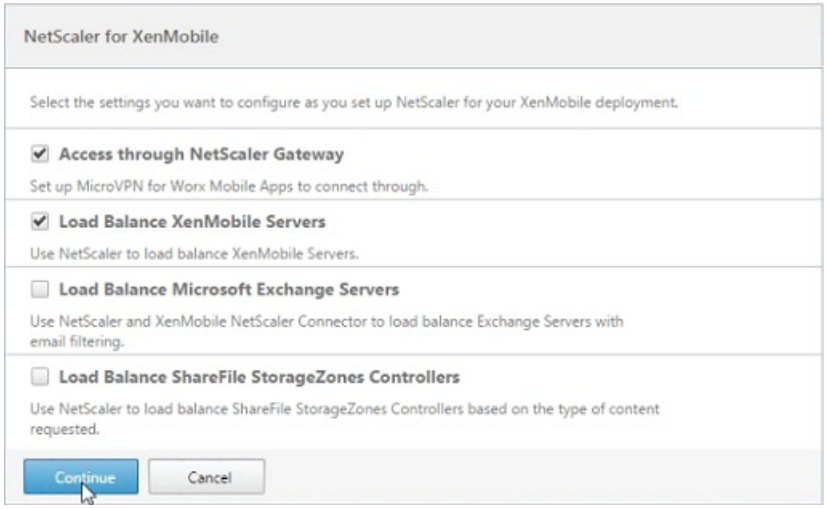
   Daraufhin wird ein Assistent zum Konfigurieren von NetScaler-Features für die XenMobile-Bereitstellung geöffnet.

3. Wählen Sie **XenMobile 10**.

4. Klicken Sie auf **Get Started**.



5. Wählen Sie auf der nächsten Seite **Access through NetScaler Gateway** und **Load Balance XenMobile Servers** und klicken Sie dann auf **Continue**.



6. Geben Sie auf der nächsten Seite die extern ausgerichtete IP-Adresse für NetScaler Gateway ein und klicken Sie auf **Continue**.

   Die Seite für das Serverzertifikat für NetScaler Gateway wird angezeigt.

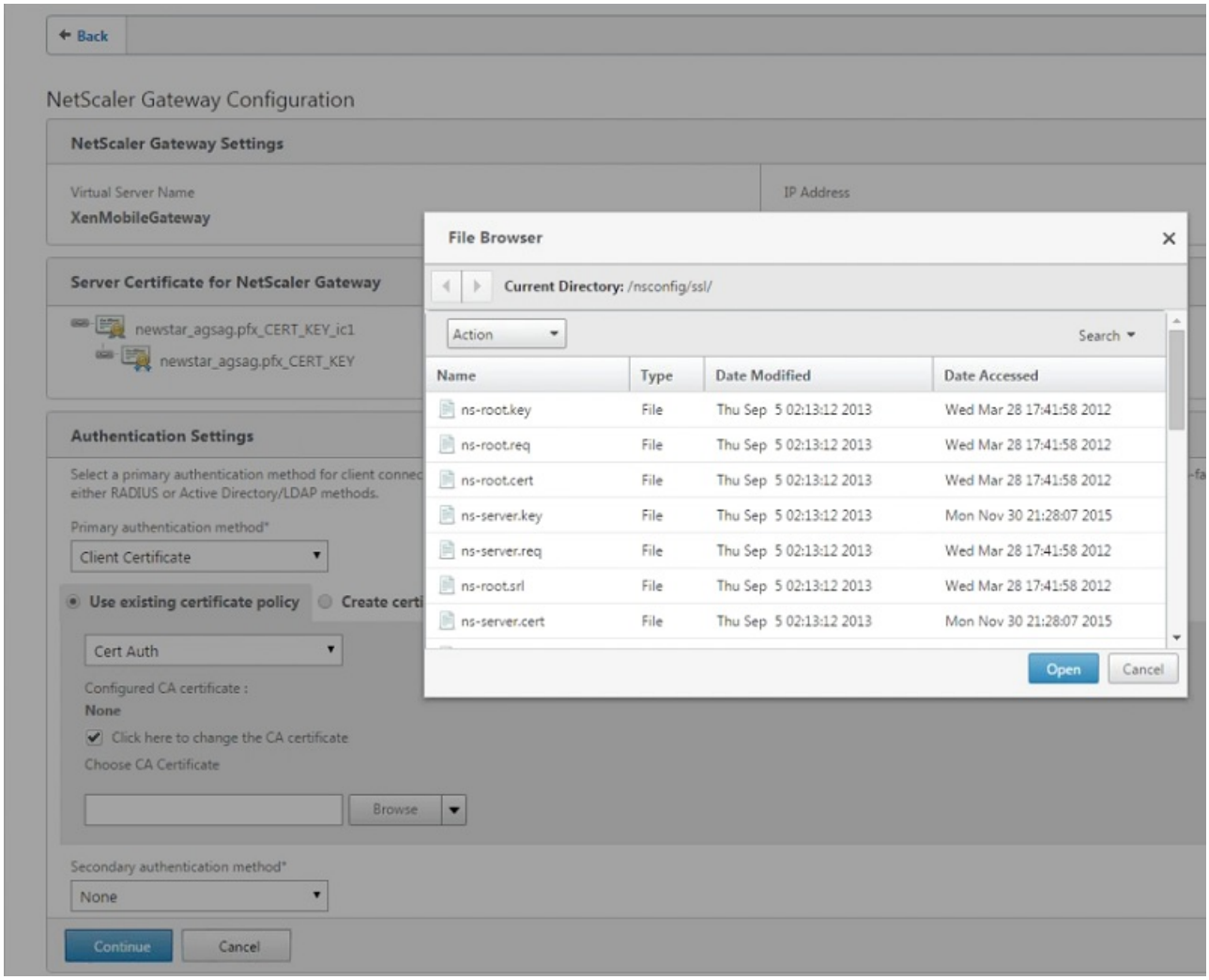
7. Sie verwenden entweder ein vorhandenes Zertifikat oder installieren ein Zertifikat. Klicken Sie auf **Continue**.

   Die Seite **Authentication Settings** wird angezeigt.

8. Wählen Sie im Feld **Primary authentication method** die Option **Client Certificate** aus.

   Auf diese Weise wird automatisch **Use existing certificate policy** und **Cert Auth** in den folgenden beiden Feldern ausgewählt.

9. Wählen Sie **Click here to change the CA certificate** und wählen Sie in der Liste **Browse** das gewünschte Zertifikat aus.



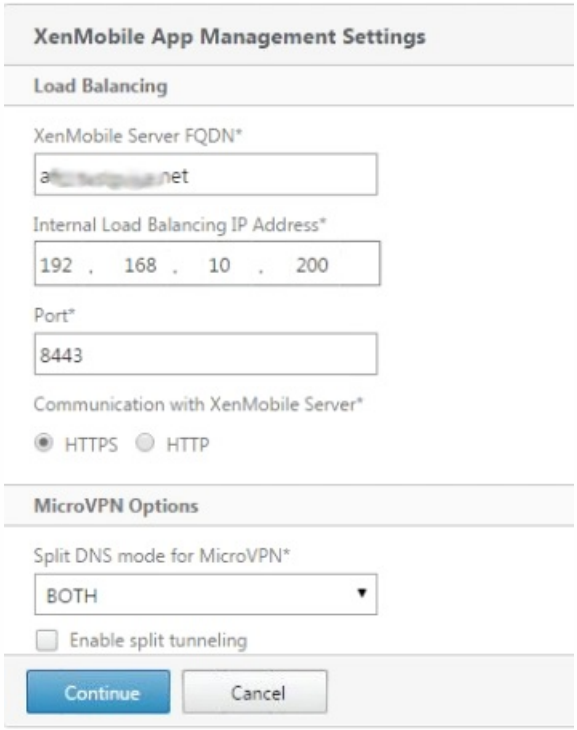
10. Für **Second authentication method** sollte **None** bereits ausgewählt sein. Klicken Sie auf **Continue**.

11. Geben Sie auf der Seite **Load Balancing** den vollqualifizierten Domänennamen (FQDN) für den XenMobile-Server und eine nur für MAM gültige IP-Adresse für internes Load Balancing ein.

12. Da dies eine SSL-Offloadbereitstellung ist, wählen Sie **HTTP** in **Communication with XenMobile Server**.

    Die Einstellung für **Split DNS mode for MicroVPN** ist **BOTH**.

13. Klicken Sie auf **Weiter**.



14. Wählen Sie auf der Seite **XenMobile Server Certificate** ein vorhandenes Serverzertifikat oder installieren Sie ein neues Zertifikat. Wenn Sie mehrere XenMobile-Server ausführen, müssen Sie für jeden Server ein Zertifikat hinzufügen. Klicken Sie auf **Weiter**.

15. Wenn das Zertifikat noch nicht installiert ist, müssen Sie es auf der Seite **Device certificate** über die XenMobile-Konsole exportieren. Vorgehensweise:

a. Klicken Sie in der Konsole auf das Zahnradsymbol oben rechts, um die Seite **Einstellungen** anzuzeigen.

b. Klicken Sie auf **Zertifikat** und wählen Sie das Zertifizierungsstellenzertifikat in der Liste aus.

c. Klicken Sie auf **Exportieren**.

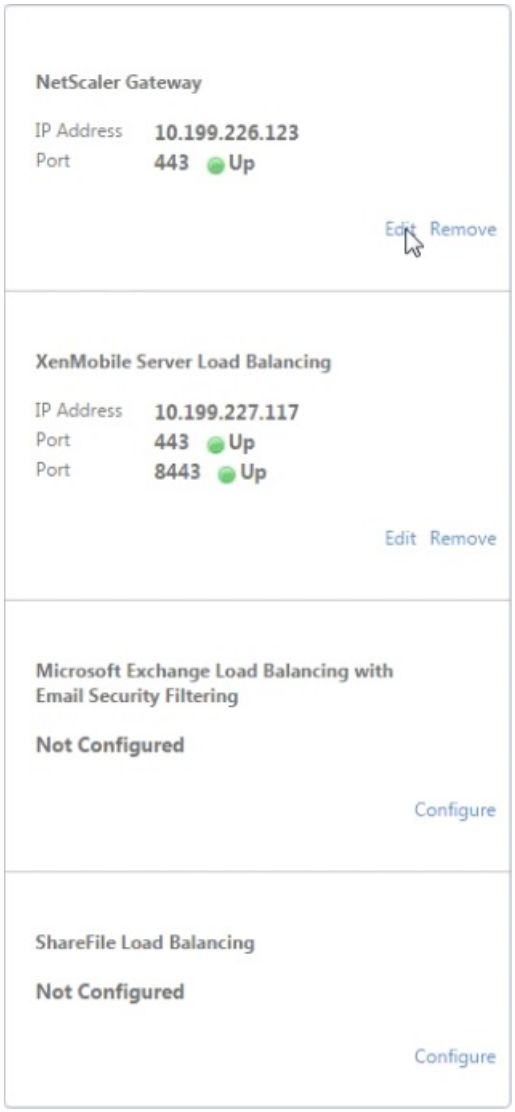
d. Kehren Sie zum NetScaler-Assistenten zurück und wählen Sie das exportierte Zertifikat für die Installation aus.

e. Klicken Sie auf **Weiter**.

Die von Ihnen konfigurierten IP-Adressen für den XenMobile-Server werden angezeigt.

16. Klicken Sie auf **Weiter**.

Bestätigen Sie im NetScaler-Dashboard, dass NetScaler Gateway und XenMobile Load Balancing konfiguriert wurden:



Geräteregistrierungslimit

Jul 28, 2016

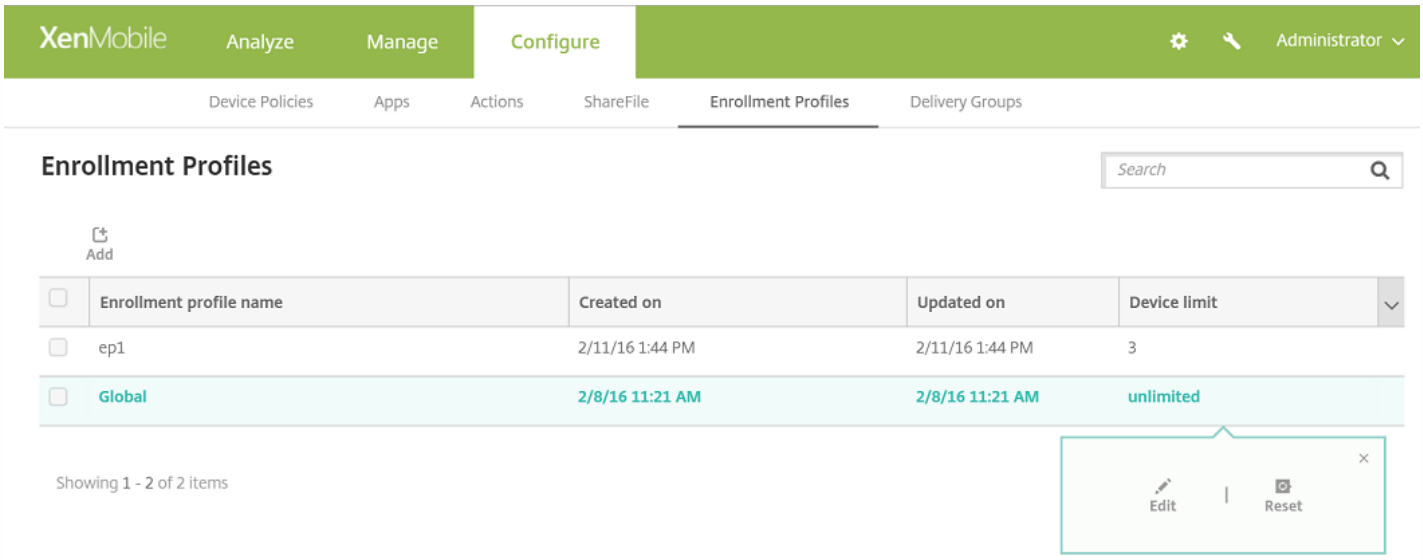
In den ENT-, MDM- und MAM-Servermodi können Sie die Anzahl von Geräten, die ein Benutzer registrieren kann, in der XenMobile-Konsole unter **Konfigurieren > Registrierungsprofile** einschränken. Einschränkungen können global oder pro Bereitstellungsgruppe gelten. Sie können mehrere Registrierungsprofile erstellen und verschiedenen Bereitstellungsgruppen zuweisen.

Wenn Sie kein Limit festlegen, können Benutzer eine unbegrenzte Anzahl von Geräten registrieren. Dieses Feature wird nur für iOS- und Android-Geräte unterstützt. Informationen zur Registrierung von Windows-Geräten finden Sie unterWindows-Geräte.

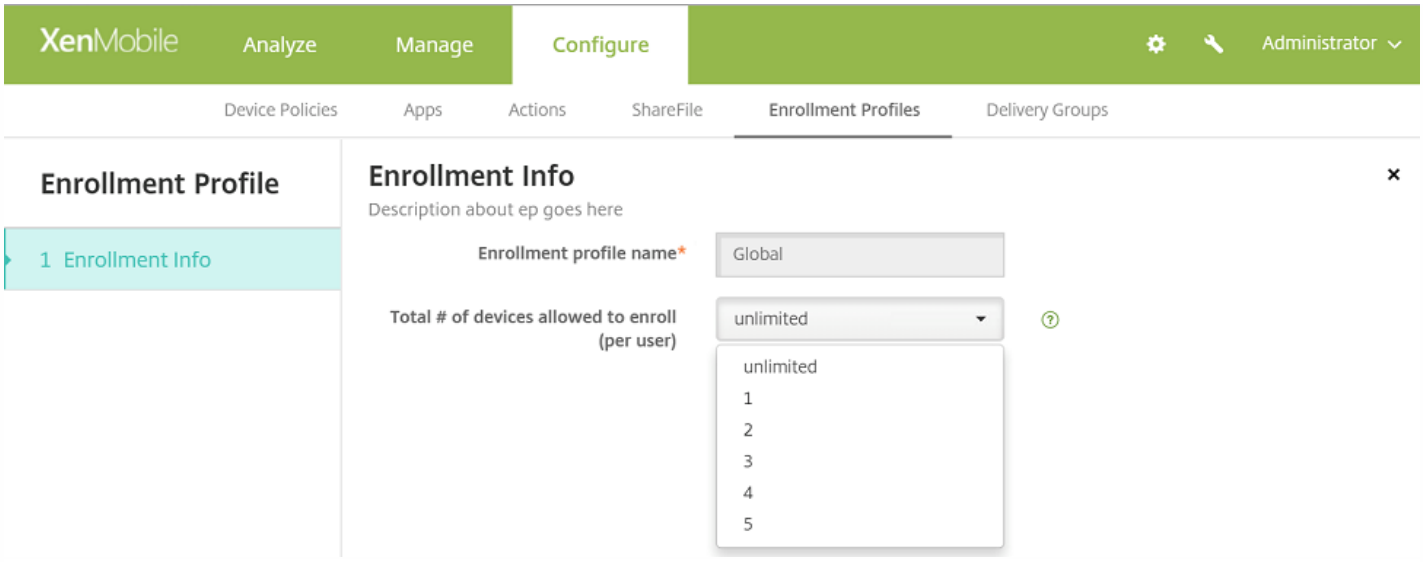
Konfigurieren eines globalen Geräteregistrierungslimits

1. Navigieren Sie zu **Konfigurieren > Registrierungsprofile**.

2. Klicken Sie auf **Global** und wählen Sie **Bearbeiten**.



Die Seite **Registrierungsinfo** wird angezeigt und der Profilname ist automatisch mit **Global** ausgefüllt. Hier können Sie die Anzahl der Geräte festlegen, die Benutzer registrieren können. Diese Einschränkung gilt für alle XenMobile-Benutzer.

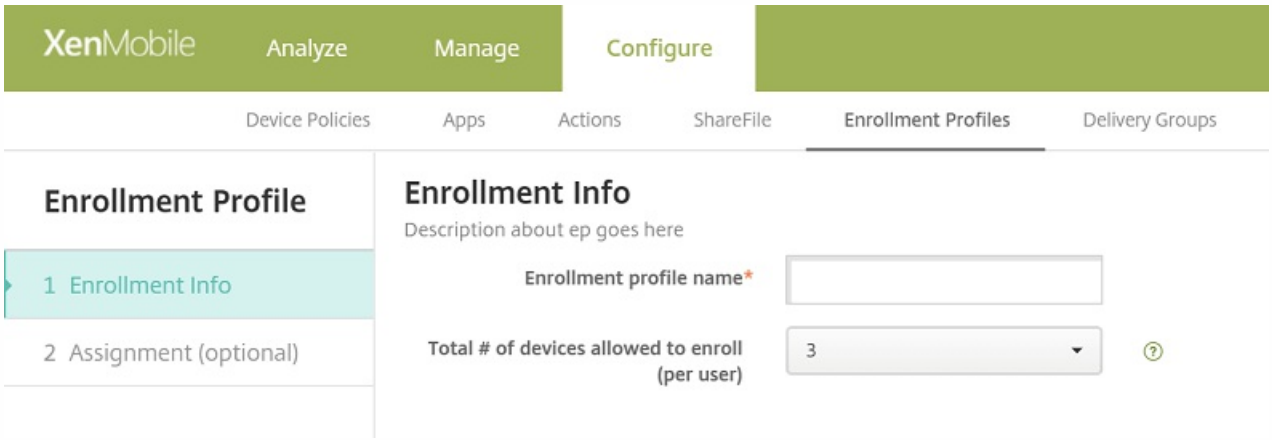


Konfigurieren eines Geräteregistrierungslimits für Bereitstellungsgruppen

1. Navigieren Sie zu **Konfigurieren** > **Registrierungsprofile** > **Hinzufügen**.

   Die Seite **Registrierungsinfo** wird angezeigt.

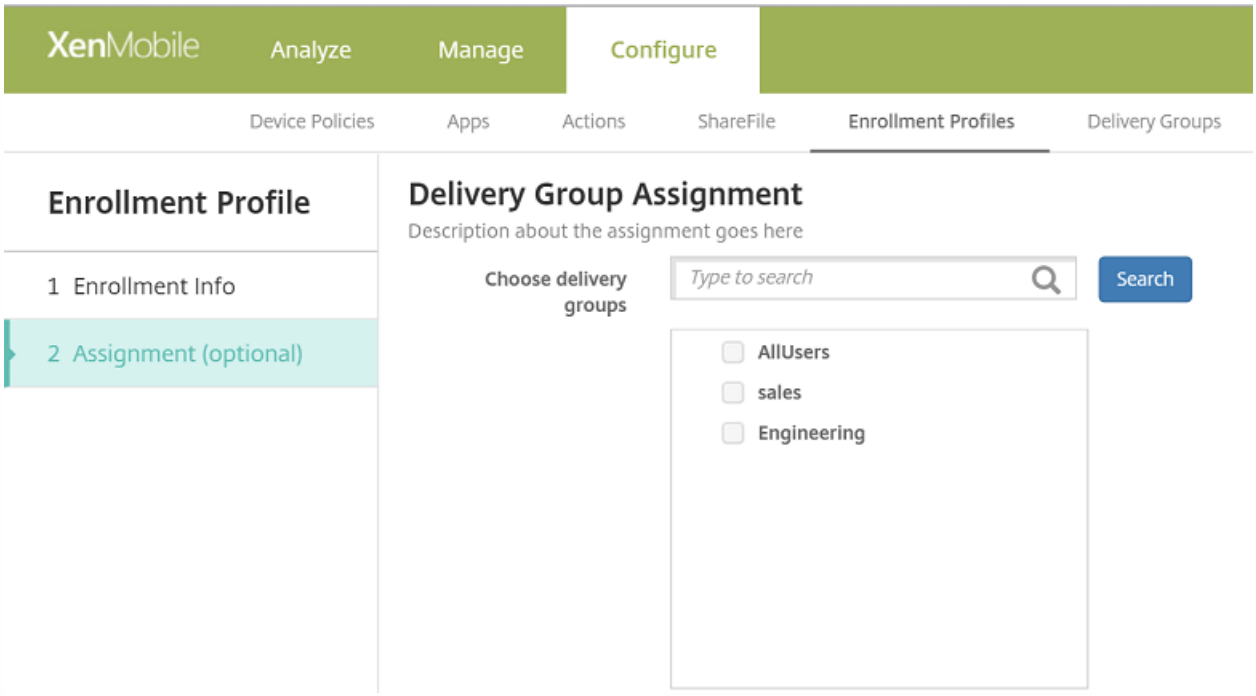
2. Geben Sie einen Namen für das neue Registrierungsprofil an und wählen Sie dann die Anzahl der Geräte aus, die Mitglieder mit diesem Profil registrieren können.



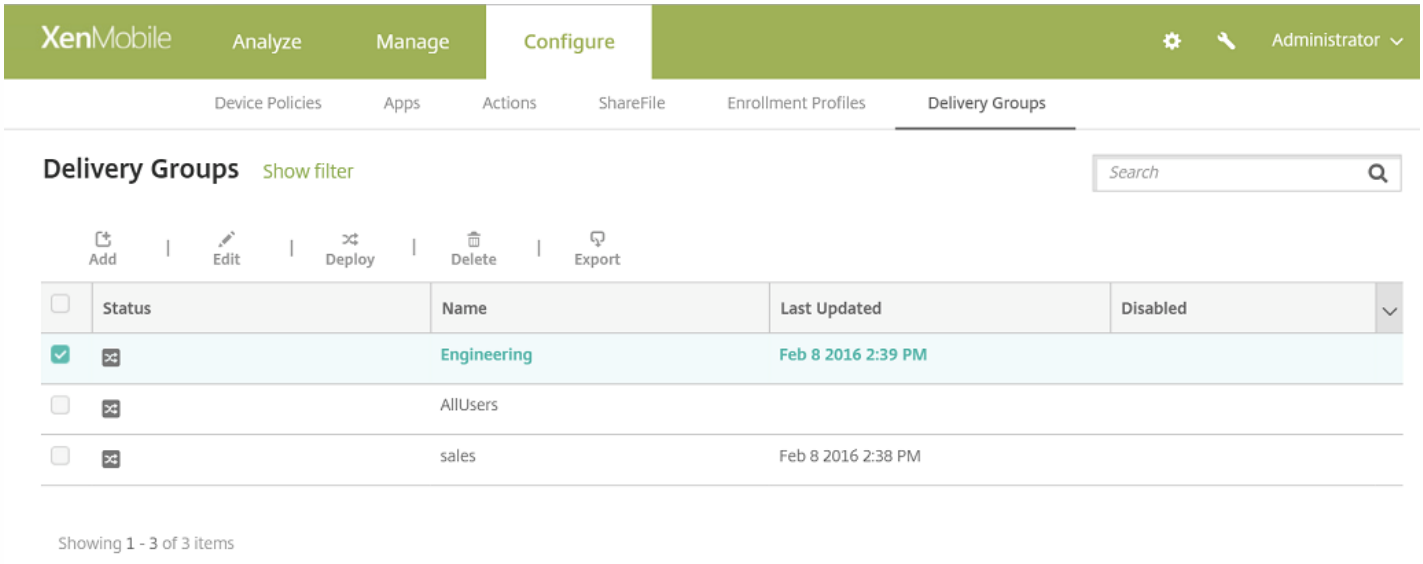
3. Klicken Sie auf **Weiter**.

   Die Seite **Bereitstellungsgruppenzuweisung** wird angezeigt.

4. Wählen Sie die Bereitstellungsgruppen aus, für die das Geräteregistrierungslimit gelten soll, und klicken Sie auf **Speichern**.

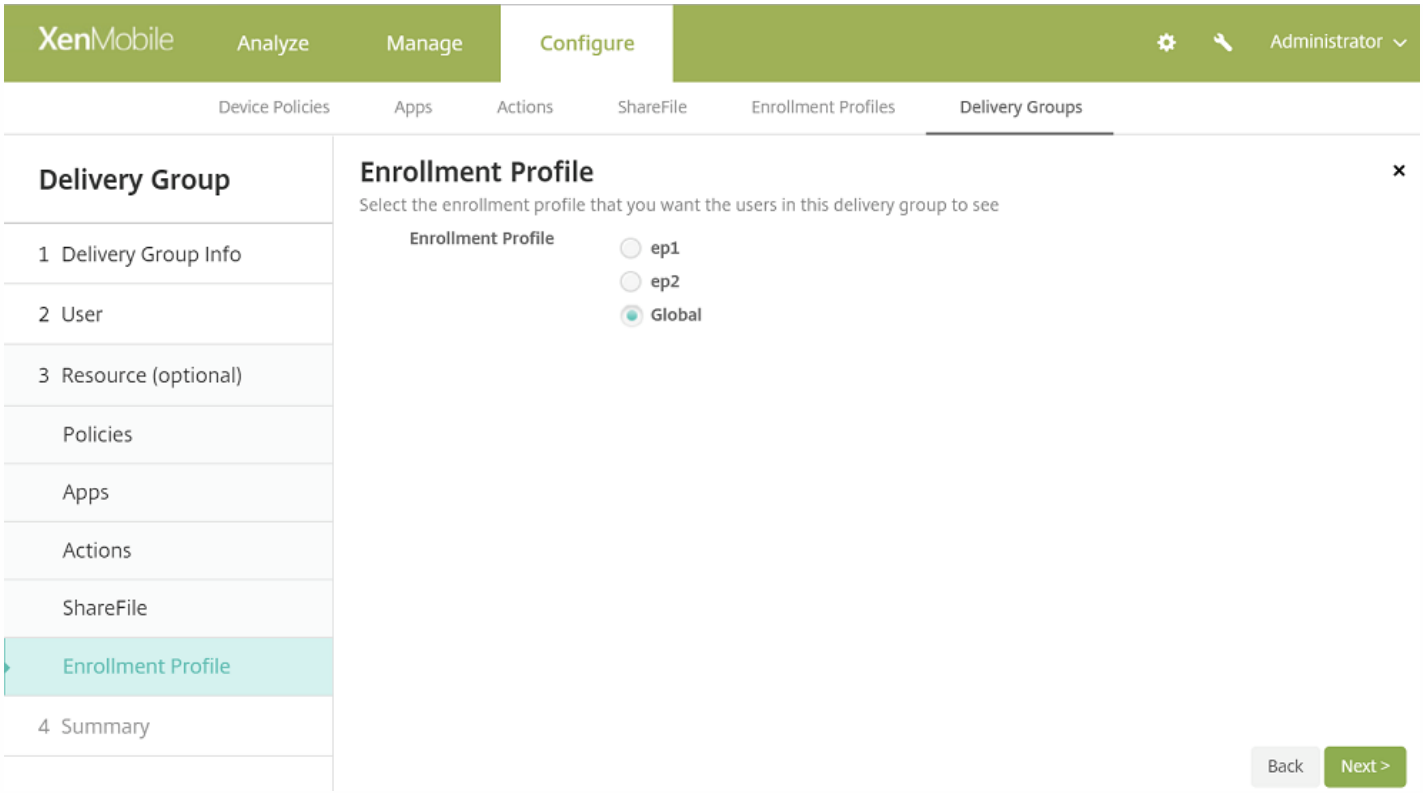


Wenn Sie später das Registrierungsprofil einer Bereitstellungsgruppe ändern möchten, wählen Sie **Konfigurieren** > **Bereitstellungsgruppen**. Wählen Sie die gewünschte Gruppe und klicken Sie auf **Bearbeiten**.



Die Seite **Registrierungsprofil** wird angezeigt.

5. Wählen Sie auf diesem Bildschirm das Registrierungsprofil aus, das Sie auf diese Bereitstellungsgruppe anwenden möchten, und klicken Sie auf **Weiter**, um die Änderungen anzuzeigen und zu speichern.



Benutzererfahrung mit einem Geräteregistrierungslimit

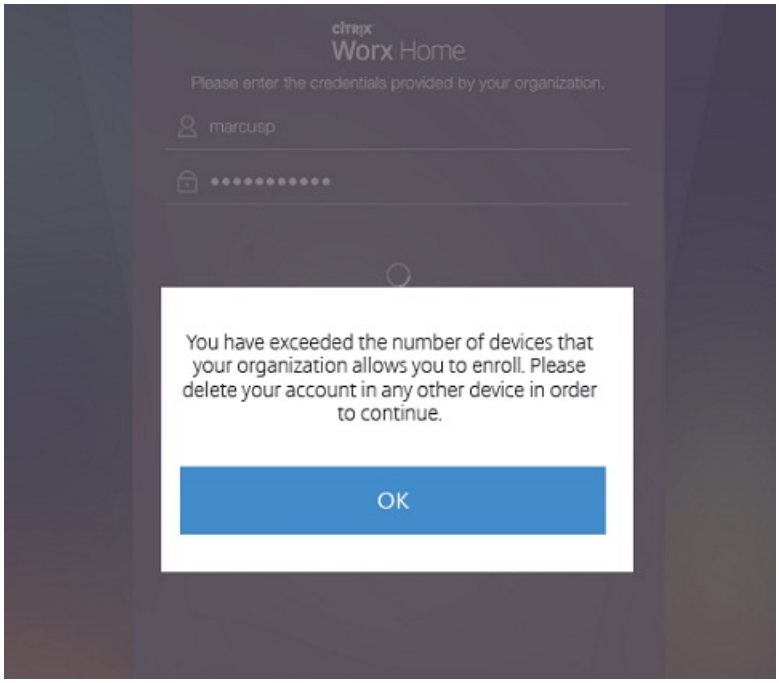
Wenn Sie das Geräteregistrierungslimit festlegen, können Benutzer ein neues Gerät mit den folgenden Schritten registrieren:

1. Melden Sie sich bei Worx Home an.

2. Geben Sie eine Serveradresse für die Registrierung ein.

3. Geben Sie die Anmeldeinformationen ein.

4. Wenn das Gerätelimit erreicht ist, wird eine Fehlermeldung angezeigt, die den Benutzer darüber informiert, dass das Geräteregistrierungslimit erreicht wurde und der Benutzer sich an den Administrator wenden sollte.



Der Worx Home-Registrierungsbildschirm wird wieder angezeigt.

Aktionen für App-Sperre und App löschen im ausschließlichen MAM-Modus

Aug 22, 2016

Durch Aktionen erstellen Sie auf Benutzergeräten automatische Reaktionen auf bestimmte Auslöser, z. B. die Installation einer unzulässigen App oder die Löschung eines Benutzers aus Active Directory. Sie können Benutzern auch Benachrichtigungen senden, um ein Problem zu lösen, bevor ernsthafte Maßnahmen erforderlich sind.

Ab XenMobile 10.3.5 können Sie als Reaktion auf die vier Auslöserkategorien in der XenMobile-Konsole (Ereignis, Geräteeigenschaft, Benutzereigenschaft und Name der installierten App) Apps auf einem Gerät löschen oder sperren. Zuvor hatte nur die Ereigniskategorie diese Funktion.

Konfigurieren der automatischen Löschung oder Sperre von Apps:

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Aktionen**.

2. Klicken Sie auf der Seite **Aktionen** auf **Hinzufügen**.

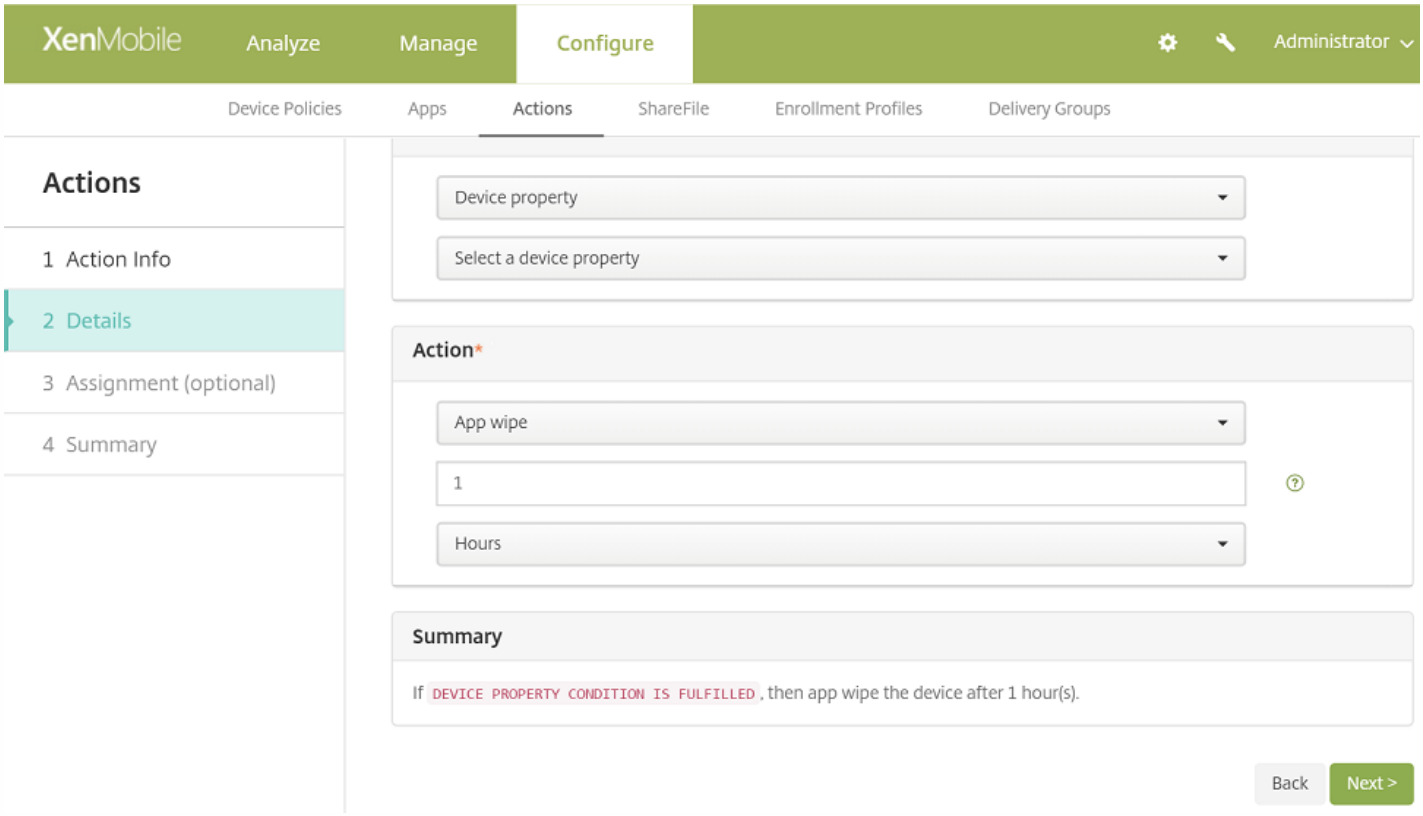
3. Geben Sie auf der Seite **Aktionsinformationen** einen Namen für die Aktion und optional eine Beschreibung ein.

4. Wählen Sie auf der Seite **Aktionsdetails** den gewünschten Auslöser aus.

5. Wählen Sie unter **Aktion** entweder **App löschen** oder **App-Sperre**.

Für jede Option wird automatisch 1 Stunde Verzögerung festgelegt, aber Sie können die Verzögerungszeit auf Minuten, Stunden oder Tagen einstellen. Die Verzögerung gibt Benutzern Zeit, das Problem zu lösen, bevor die Aktion ausgeführt wird. Weitere Informationen über Lösch- und Sperraktionen für Apps finden Sie unter RBAC-Rollen und -Berechtigungen.

> ## Hinweis
>
> Eine zusätzliche Verzögerung von etwa einer Stunde vor der Ausführung der Aktion ist möglich, damit die Active Directory-Datenbank mit XenMobile synchronisiert werden kann.



6. Konfigurieren Sie die Bereitstellungsregeln und klicken Sie auf **Weiter**.

7. Konfigurieren Sie die Zuweisungen für Bereitstellungsgruppen und einen Bereitstellungszeitplan, und klicken Sie auf **Weiter**.

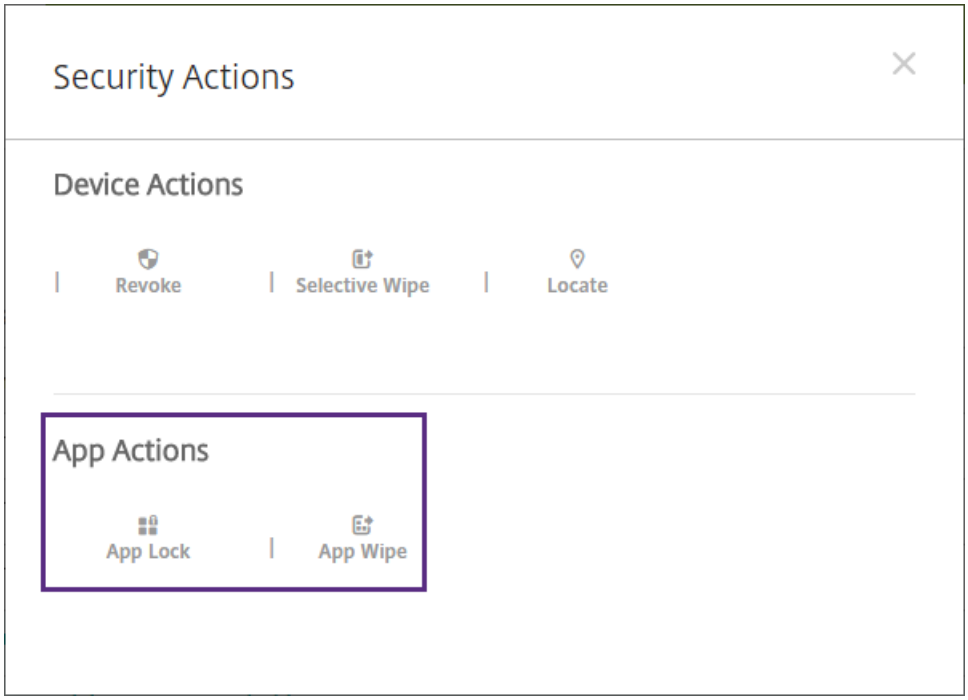
8. Klicken Sie auf **Speichern**.

Sperren, Entsperren, Löschen und Rückgängigmachen des Löschvorgangs:

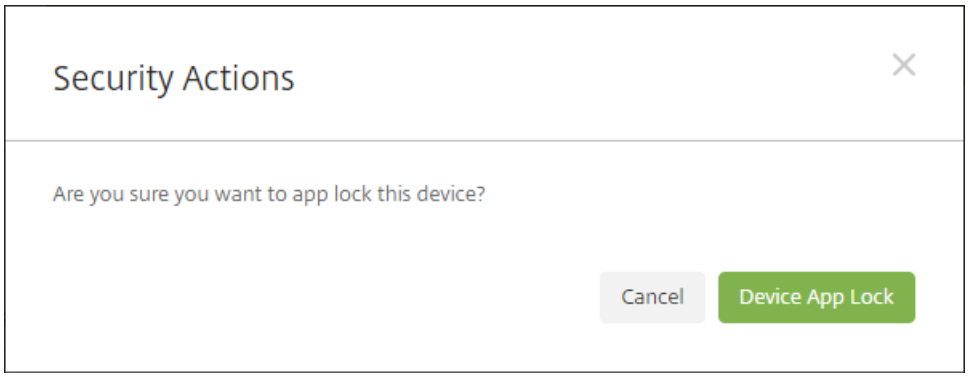
1. Gehen Sie zu **Verwalten > Geräte**, wählen Sie das Gerät aus und klicken Sie auf **Sicherheit**.

2. Klicken Sie im Dialogfeld **Sicherheitsaktionen** auf eine Aktion.

> Hinweis: Sie können in diesem Dialogfeld auch den Status eines Geräts für einen Benutzer überprüfen, der deaktiviert ist oder aus Active Directory gelöscht wurde. Wenn die Aktionen "App-Sperre aufheben" oder "Löschen der Apps rückgängig machen" vorhanden sind, sind die Apps des Benutzers momentan gesperrt oder gelöscht.

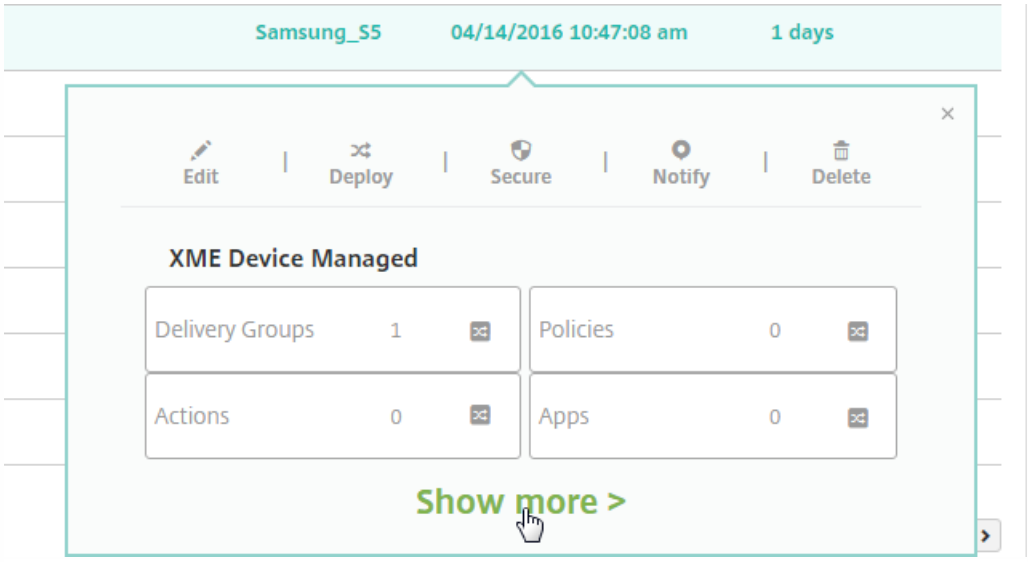


3. Bestätigen Sie die Aktion.

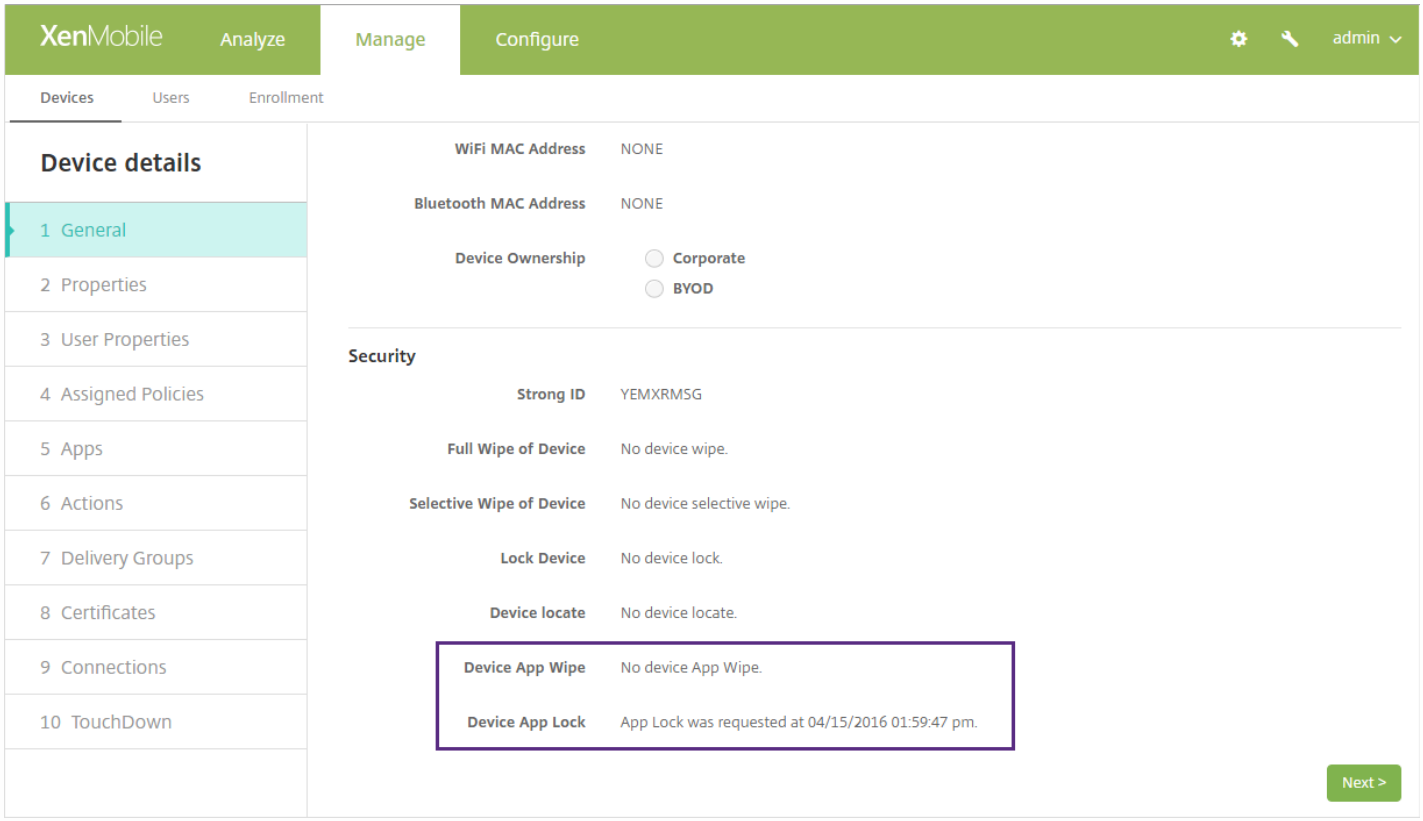


Überprüfen des Status für App-Sperre oder App-Löschen:

1. Gehen Sie zu **Verwalten > Geräte**, wählen Sie ein Gerät aus und klicken Sie auf **Mehr anzeigen**.



2. Führen Sie einen Bildlauf zu **Apps von Gerät löschen** und **App-Sperre für Gerät** durch.



REST-Dienste-APIs für ausschließlichen MAM-Modus

Jul 28, 2016

Für MAM-Geräte können Sie mit einem beliebigen REST-Client und der XenMobile-REST-API REST-Dienste aufrufen, die über die XenMobile-Konsole verfügbar gemacht werden. Die API erfordert zum Aufrufen der in diesem Abschnitt beschriebenen Dienste keine Anmeldung bei der XenMobile-Konsole.

Sie können REST-API-Dienste über den REST-Client aufrufen.

Mit den neuen REST-APIs verfügen Sie über folgende Funktionen:

- **Einladungs-URL und Einmal-PIN senden**

  Mit einer XenMobile-REST-API können Sie Benutzern ermöglichen, BYOD-Zugriff über ein Self-Service-Portal anzufordern. Bei Genehmigung sendet das System dem XenMobile-Server eine Anforderung für Folgendes:

  - Erstellen und Senden einer Registrierungseinladungs-URL an den Benutzer.

  - Erstellen und Senden einer Einmal-PIN an den Benutzer.

  Hinweis: Dieses Feature wird für iOS- und Android-Geräte, jedoch nicht für Windows-Geräte unterstützt.

- **Apps auf Geräten sperren und löschen**

  Sie können mit einer XenMobile-API alle Geräte nach den Geräten eines bestimmten Benutzers durchsuchen, um beispielsweise alle Apps auf einem Gerät zu löschen oder Apps zu sperren.

Nachstehend sind die Geräte-APIs und Einmal-PIN-Registrierungs-APIs aufgeführt, die ab XenMobile 10.3.5 verfügbar sind. Eine umfassende Dokumentation zu den aktuell verfügbaren APIs finden Sie in der PDF-Datei Referenz zur XenMobile REST-API, die heruntergeladen werden kann.

Geräte-APIs

- Get Devices by Filters
- Get Device information by ID
- Get Device applications by device ID
- Get Device actions by device ID
- Get Device delivery groups by device ID
- Get Device managed software inventory by device ID
- Get Device policies by device ID
- Get Device software inventory by device ID
- Get Device GPS Coordinates by device ID
- Send notification to a list of devices/users
- Authorize a list of devices
- Activation lock bypass on a list of devices
- App lock on a list of devices
- App wipe on a list of devices
- Container lock on a list of devices

- Cancel container lock on a list of devices
- Container unlock on a list of devices
- Cancel container unlock on a list of devices
- Reset container password on a list of devices
- Cancel reset container password a list of devices
- Disown a list of devices
- Locate a list of devices
- Cancel locating a list of devices
- GPS tracking a list of devices
- Cancel GPS tracking a list of devices
- Lock a list of devices
- Cancel locking a list of devices
- Unlock a list of devices
- Cancel unlocking a list of devices
- Deploy a list of devices
- Request an Airplay mirroring on a list of devices
- Cancel request for Airplay mirroring a list of devices
- Stop Airplay mirroring on a list of devices
- Cancel stop Airplay mirroring on a list of devices
- Clear the restrictions on a list of devices
- Cancel clear the restrictions on a list of devices
- Revoke a list of devices
- Make ring a list of devices
- Cancel ring on list of devices
- Wipe a list of devices
- Cancel wipe on list of devices
- Selective wipe a list of devices
- Cancel selective wipe on list of devices
- SD card wipe on a list of devices
- Cancel SD card wipe on list of devices
- Get all device known properties
- Get all device used properties
- Retrieve all device properties by device ID
- Update all device properties in bulk by device ID.
- Add or Update a device property by device ID
- Delete a device property by device ID
- Retrieve iOS MDM Status of device by device ID
- Generate pin code

Einmal-PIN-Registrierungs-APIs

- Get Enrollment Modes
- Get Enrollment Information
- Trigger Enrollment Notification
- Create Enrollment Invitation

- Get Enrollment Records by Filter

Bekannte und behobene Probleme in XenMobile 10.3.5

Aug 22, 2016

Die folgenden Probleme sind in XenMobile 10.3.5 bekannt oder wurden behoben:

- Einschränkung: Die Features für den neuen MAM-Only-Modus, z. B. die zertifikatbasierte Authentifizierung, App-Sperre, Apps löschen und MAM-Only-APIs, sind nicht für Windows Phone verfügbar.
- Wenn Benutzer sich mehrmals bei Worx Home registrieren und dann versuchen, eine App aus dem WorxStore zu installieren, besagt eine Fehlermeldung, dass die App entfernt wurde. Als Workaround löschen Sie das Gerät in der XenMobile-Konsole unter **Verwalten > Geräte** und fordern dann die Benutzer auf, sich erneut zu registrieren. [#611172]
- Das SSL-Listenerzertifikat muss ein öffentliches Zertifikat sein, damit Windows-Geräte sich registrieren können. Bei einem selbstsignierten SSL-Zertifikat schlägt die Registrierung fehl. [#618390]
- Wenn die Anzahl der registrierten Geräte das von Ihnen in der XenMobile-Konsole festgelegte Limit erreicht, wird die entsprechende Fehlermeldung nicht auf dem Gerät angezeigt, aber Benutzer können sich nicht registrieren. [#623475]
- Benutzer, die sich bei XenMobile über ein Azure Active Directory-Konto registrieren, können sich auch nach dem Löschen oder Widerrufen des Geräts ohne Autorisierung erneut registrieren. Dies ist ein Drittanbieterproblem. [#628865]
- Nach dem Löschen eines iOS-Geräts von der XenMobile-Konsole schlägt die Registrierung im MAM-Modus gelegentlich fehl, wenn Benutzer das Gerät im XenMobile Enterprise-Modus (MAM und MDM) erneut registrieren. [#629021]
- Wenn Sie die Option zum Verlängern von Zertifikaten auf dem XenMobile-Server deaktivieren, können Benutzer ein abgelaufenes Zertifikat in Worx Home erneuern. [#630894]
- Einige VPP-Lizenzen haben negative IDs, z. B. -123441212. In diesem Fall können Sie die öffentlichen Apps nicht bereitstellen. [#631443]
- Wenn Sie in Google Play-Anmeldeinformationen mit einer ungültigen Geräte-ID konfigurieren und dann für Google Play eine App aus einem öffentlichen App-Store hinzufügen und anschließend im Google Play-Store nach dem Namen der App suchen, schlägt die Suche fehl oder führt zu falschen Suchergebnissen. [#633845]
- Zurzeit können Sie Ihre Android-ID nicht abrufen, indem Sie*#*#8255#*#*auf Ihrem Telefon eingeben, wie unter **Einstellungen > Google Play-Anmeldeinformationen** in der XenMobile-Konsole angewiesen. Verwenden Sie eine Geräte-ID-App aus dem Google Play Store, um die ID Ihres Geräts anzuzeigen. [#633854]
- In der XenMobile-Konsolen gibt es mit **Einstellungen > Rollenbasierte Zugriffssteuerung** die folgenden Probleme im Zusammenhang mit den Standardeinstellungen.
  - In der XenMobile-Konsole für Cloudbereitstellungen ist die Berechtigung **Registrierung für gemeinsam genutzte Geräte** standardmäßig für die Administratorrolle eingestellt. Diese Berechtigung sollte nicht standardmäßig eingestellt sein. [#638069]
  - Die Konsolenfeatureberechtigung **Gerät ausschließen** ist veraltet und sollte nicht angezeigt werden. [#638303]
  - In der XenMobile-Konsole für Cloudbereitstellungen sind die folgenden Features in der Standardeinstellung nicht für die Administratorrolle ausgewählt. Stellen Sie sicher, dass Sie diese Einstellungen für die Standardadministratorrolle wählen, sowie für alle Rollen, die Sie mit der Administratorvorlage erstellt haben. [#638314]

    Container sperren
    Container entsperren
    Containerkennwort zurücksetzen

Aktivierungssperre umgehen
Gerät klingeln lassen

- In der XenMobile-Konsole für lokale und Cloudbereitstellungen sind die folgenden Features in der Standardeinstellung nicht für die Administratorrolle ausgewählt. Stellen Sie sicher, dass Sie diese Einstellungen für die Standardadministratorrolle wählen, sowie für alle Rollen, die Sie mit der Administratorvorlage erstellt haben. [#638322]

  AirPlay-Synchronisierung anfordern
  AirPlay-Synchronisierung beenden

- SSO-Authentifizierung für ShareFile schlägt aufgrund von Zeitsynchronisierungsproblemen zwischen XenMobile und Hyper-V fehl. [#588249]
- Wenn Sie das Verschachteln in den XenMobile LDAP-Einstellungen aktivieren und Bereitstellungsgruppen und RBAC-Einstellungen mit den entsprechenden Domänengruppen konfigurieren, bleiben die Informationen der verschachtelten Gruppen in der Datenbank erhalten, wenn Sie später die Domäne in den LDAP-Einstellungen löschen. [#590363]
- Wenn Sie Benutzer aus Active Directory löschen, können sie trotzdem noch den WorxStore öffnen und Apps abonnieren. [#592825]
- Nachdem Sie nach Updates für Apps im öffentlichen App Store in der XenMobile-Konsole gesucht haben, aktualisiert Worx Home die Apps im öffentlichen App Store mit der aktuellen Version, aber die Apps werden weiterhin in der Liste der ausstehenden Updates auf dem Gerät angezeigt. [#593034]
- Wenn Benutzer Kalendereinladungen vom Exchange-Konto in WorxMail erhalten, kommt die Einladung nicht so schnell an wie erwartet. [#594542]
- Wenn das iOS-Gerät im Device Enrollment Program (DEP) registriert ist, kann Worx Home möglicherweise nicht auf das iOS-Gerät heruntergeladen werden. [#595822]
- Wenn Sie keinen NTP-Client konfigurieren, treten auf dem XenMobile-Server u. U. Probleme aufgrund von Zeitabweichungen auf, z. B. Fehler beim SAML Single Sign-On (SSO) für ShareFile.

  Hinweis: Verwenden Sie die folgende Konfiguration für den Fix:

  1. Melden Sie sich bei der XenMobile-Befehlszeilenschnittstelle auf dem Hypervisor an, auf dem Sie XenMobile installiert haben (Citrix XenServer oder VMware ESXi).

  2. Gehen Sie zu **[2] System**.

  3. Gehen Sie zu **[3] Set NTP Server** und geben Sie die NTP-Serverdetails ein.

  4. Starten Sie den Server neu.

  Wichtig: Wenn das System im Clustermodus konfiguriert ist, führen Sie die oben beschriebene Konfiguration auf jedem Knoten aus. [#597757]

- Wenn Benutzer versuchen, eine App oder einen Weblink in Worx Home zu entfernen, wird die folgende Fehlermeldung angezeigt: Worx Home konnte keine Verbindung herstellen. [#599934]
- PIN-basierte Registrierung kann fehlschlagen, wenn mehrere PINs für Benutzer ausstehen. [#600264]
- Wenn einige Lizenzen von Apple erstattet wurden, werden die Lizenzen beim Import von VPP-Lizenzen in XenMobile fälschlicherweise als gültig angesehen. Daher können Benutzer über den WorxStore keine Apps auf iOS-Geräten installieren. [#601845]
- Wenn Sie eine Aktion erstellen und dann den Namen der Aktion ändern, sodass er mit dem Namen einer der Richtlinien

oder Apps auf Ihrem Gerät übereinstimmt, können Sie die Aktion später nicht löschen. [#602958]

- Wenn Sie mit einem Samsung Galaxy Note 5 auf den WorxStore zugreifen, wird der WorxStore in der Tabletansicht statt wie erwartet in der Telefonansicht angezeigt. Dabei ist nur ein Teil des Bildschirms sichtbar. [#604295]
- Wenn Sie eine Registrierungseinladung mit einer Einmal-PIN-Anforderung für Empfänger der obersten Ebene einer Active Directory-Gruppe erstellen, erhalten verschachtelte Gruppen die Einladung, aber die Registrierung schlägt für die Gruppe auf der dritten Ebene fehl. Dieses Problem tritt auch dann auf, wenn Sie eine Einladung an die Gruppe auf der dritten Ebene senden. [#603434]
- Wenn der Typ Ihrer Lizenz "Advanced" ist und Sie in der XenMobile-Konsole das Kontrollkästchen "Registrierung erforderlich" aktivieren, können Benutzer sich im Nur-MAM-Modus registrieren und auf den WorxStore zugreifen. [#604113]
- Die Eigenschaften **$user.dnsroot** und **$user.netbiosename** werden in Makros zum Bereitstellen von Richtlinien mit Benutzereigenschaften verwendet. Die Benutzereigenschaften **dnsroot** und **netbiosename** sind ab XenMobile 10.1 veraltet. Mit diesem Fix können die Eigenschaften in XenMobile 10.3 wieder aktiviert werden. [#604240]
- 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. [#607143]
- In den Einstellungen für Clientbranding in der XenMobile-Konsole werden für Storenamen nur alphanumerische Zeichen (ASCII-Zeichen) unterstützt. Wenn Sie den Standardnamen durch einen Namen mit Nicht-ASCII-Zeichen ersetzen, können Benutzer sich nicht an Worx Home anmelden. [#609535]
- Wenn LDAP mit verschiedenen Basis-DNs für Benutzer und Gruppen konfiguriert ist und ein Update auf XenMobile 10.3 erfolgt, können Sie Bereitstellungsgruppen keine neuen Gruppen hinzufügen. [#610014]
- Wenn eine WiFi-Geräterichtlinie konfiguriert ist, wird die WiFi-Richtlinie per Push jedes Mal bereitgestellt, wenn ein Gerät eine Verbindung herstellt, selbst wenn der Bereitstellungszeitplan auf **Nur bei Fehler in der vorherigen Bereitstellung** festgelegt ist. [#610325]
- Dieser Fix behebt eine Zero-Day-Schwachstelle in Java für Objektdeserialisierung in Apache Commons Collections. [#610427]
- Wenn Sie eine RBAC-Rolle festlegen, damit Benutzer sich an der XenMobile-Konsole mit einem Benutzernamen im sAMAccountName-Format anmelden können, werden die Benutzer zum Selbsthilfeportal zur weitergeleitet. [#610915]
- Nach der Erstinstallation von XenMobile 10.1 oder nach einem Upgrade von XenMobile 9 im MAM- und MDM-Modus auf XenMobile 10.1 werden in der XenMobile-Konsole unter **Verwalten** > **Gerät** nach dem Aktualisieren der Bereitstellungsgruppen und Richtlinien andere Informationen angezeigt und die Anzahl der Bereitstellungsgruppen und Richtlinien ist falsch. [#611630]
- Wenn mehr als 10 LDAP-Domänen in XenMobile-Versionen vor XenMobile 10.1 konfiguriert sind, werden in XenMobile 10 und nach dem Upgrade auf XenMobile 10.1 nur 10 Domänen in der XenMobile-Konsole angezeigt. [#613502]
- Sie können eine MDX-App nicht hinzufügen oder aktualisieren, wenn Sie keine RBAC-Rolle für Benutzer festlegen, die Berechtigungen für öffentliche Apps enthält. [#614496]
- Wenn Sie den Standardinstanznamen während der Erstkonfiguration von XenMobile ändern, bleibt die Änderung beim Upgrade auf Version 10.3 nicht erhalten. Registrierte Geräte können dann keine Verbindung herstellen. [#614604]
- Wenn Sie LDAP mit einem Sperrlimit konfigurieren und dann ein Upgrade auf XenMobile 10.3 durchführen, reagiert Worx Home nicht mehr und SQL Server fällt aus, wenn ein neuer Benutzer in derselben Domäne in Worx Home ein Gerät mit ungültigen Anmeldeinformationen, z. B. einem falsch geschriebenen Kennwort, registriert. [#615179]
- Nach dem Aktualisieren von XenMobile 10.1 auf XenMobile 10.3 können Sie mit der Option **Einladung hinzufügen** keine Registrierungseinladung an Benutzer senden. [#616584]
- Diese Lösung ermöglicht die Unterstützung für einen LDAP-Multidomänenstamm in einer einzelnen Gesamtstruktur. Diese Unterstützung war in XenMobile 9, jedoch nicht in XenMobile 10.x verfügbar. [#616633, #618899, #620541]
- Wenn Sie eine iOS-Einschränkungsrichtlinie in der XenMobile-Konsole konfigurieren und den Standardwert für die Option **Benutzer darf Richtlinie entfernen** ändern, wird der Wert nicht gespeichert. [#616751]

- Wenn ein Server einen benutzerdefinierten Instanznamen hat, können Benutzer nach dem Update von XenMobile 10.1 auf XenMobile 10.3 ihre Geräte nicht registrieren. [#616954]
- Wenn Benutzer ein DEP-Gerät im XenMobile Enterprise-Modus registrieren, dann ihr eigenes Gerät auf die Werkseinstellungen zurücksetzen (vollständiges Löschen) und dann das Gerät erneut registrieren, wird Worx Home nicht wie erwartet automatisch auf dem Gerät bereitgestellt. [#616986]
- Gelegentlich wird der XenMobile-Server aufgrund eines bekannten Problems in Java Runtime Environment (JRE) nach ungefähr 20 bis 30 Minuten in den Wiederherstellungsmodus versetzt. Nach dem Neustart des Servers tritt das Problem erneut auf. [#616992]
- Auf iOS- und Android-Geräten können Benutzer WorxStore von Worx Home aus nicht öffnen, wenn Sie den **Storenamen** unter **Einstellungen > Clientbranding** entfernen. [#617003]
- Beim Hochladen einer IPA-Datei zur XenMobile-Konsole wird der Fehler "Symbol nicht gefunden" angezeigt. [#617195]
- Wenn Sie eine VPN-Geräterichtlinie bereitstellen, in der die Optionen "Pro-App-VPN aktivieren" und "App-Übereinstimmung bei Bedarf aktiviert" auf **EIN** festgelegt sind, und wenn Sie eine App-Attribute-Richtlinie für eine verwaltete App bereitstellen, auf die die VPN-Richtlinie angewendet wird, wird die VPN-Verbindung nicht wie erwartet automatisch initiiert, wenn Benutzer die verwaltete App öffnen. Benutzer müssen die Einstellung **Connect On Demand** manuell auf ihren Geräten aktivieren. [#617803]
- In der XenMobile-Konsole tritt unter **Verwalten** > **Benutzer** eine Verzögerung bei der Anzeige der vorhandenen Benutzer auf. Daher können Sie keine Vorgänge für lokale Benutzer ausführen. [#618094]
- XenMobile 10.x unterstützt LDAP-Multidomänen in einer einzelnen Active Directory-Gesamtstruktur. [#618375]
- Wenn Sie eine Registrierungseinladung senden und HTML-Code einfügen, erhalten Benutzer die E-Mail als reinen Text ohne den HTML-Link. [#618504]
- Wenn Benutzer eine APPX-Datei als eine Unternehmensapp für Windows 10-Geräte hochladen, wird die App nicht auf den Geräten bereitgestellt. [#628611]
- Benutzer können Windows 10-Geräte nicht in XenMobile im MDM-Modus registrieren, wenn die Benutzer-ID oder das Kennwort Sonderzeichen enthalten. [#618870]
- Auf iPads führt XenMobile 10.3 immer zuerst Lösch- bzw. Entfernungsaktionen aus, unabhängig von der in der XenMobile-Konsole festgelegten Reihenfolge. [#620459]
- Wenn Sie eine vorhandene iOS-Unternehmensapp in der XenMobile-Konsole aktualisieren und die IPA-Datei eine andere Bundle-ID hat, treten beim Bereitstellen der aktualisierten App auf Geräten Probleme auf. [#621009]
- Beim Hinzufügen von Google Play-Anmeldeinformationen in XenMobile-Server wird die Fehlermeldung "Ungültige Geräte-ID" angezeigt und Sie können sich nicht anmelden. [#623182]
- Wenn Sie in XenMobile eine App löschen, die Sie mit VPP importiert haben, wird die App nicht automatisch erneut importiert, bis Sie das Token löschen und erneut hinzufügen. [#623403]
- Wenn Sie ein Gerät löschen, werden diesem Gerät zugeordnete VPP-Lizenzen nicht automatisch freigegeben. Sie müssen die Zuordnung der Lizenz manuell aufheben, um sie auf einem anderen Gerät zu verwenden. [#623716]

Info zu XenMobile Server 10.3

Oct 13, 2016

Sie können ein Upgrade von XenMobile 10.1 auf XenMobile 10.3 mit der XenMobile-Konsole durchführen. Für das Upgrade verwenden Sie xms_10.3.0.824.bin. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben und dann auf **Releasemanagement**. Klicken Sie auf **Upgrade** und laden Sie dann die Datei xms_10.3.0.824.bin hoch. Weitere Informationen über Upgrades der Konsole finden Sie unter Aktualisieren von XenMobile.

Anweisungen für eine neue Installation von XenMobile 10.3 finden Sie unter Installieren von XenMobile.

> ## 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.

XenMobile 10.3 bietet die folgenden neuen Features.

Neues Erscheinungsbild der Konsole

XenMobile 10.3 hat eine neue Optik. Die Konsole hat neue Farben, Schriftarten, Registerkarten und eine verbesserte Funktionalität.

- Die Registerkarte "Dashboard" aus älteren Versionen ist jetzt Teil der neuen Registerkarte "Analysieren". Letztere enthält auch die neue Registerkarte "Berichterstellung". Einzelheiten finden Sie unter Berichte.
- Die Registerkarte "Verwalten" enthält jetzt die neue Registerkarte "Benutzer", auf der Sie lokale Benutzer und Gruppen verwalten können.
- Die Registerkarte "Konfigurieren" enthält eine neue Registerkarte für ShareFile, auf der Einstellungen für die Verbindung mit einem ShareFile-Konto festgelegt werden können.
- Zum Aufrufen der Einstellungen, die zuvor auf der Registerkarte "Konfigurieren" zu finden waren, klicken Sie auf das Zahnradsymbol oben rechts in der Konsole.
- Die Registerkarte "Support" wird jetzt auf der gleichen Registerkarte wie die Konsole anstatt einer neuen Registerkarte geöffnet.

Unterstützung neuer Plattformen

XenMobile 10.3 unterstützt die folgenden Plattformen:

- Mac OS X
- Android HTC
- Android Sony
- Samsung SEAMS
- Windows Mobile/CE
- Windows 10 Phone: Geräteverwaltung im XenMobile MDM- und Enterprise-Modus.

- Windows 10 Desktop/Tablet: Geräteverwaltung im XenMobile MDM- und Enterprise-Modus.

Anweisungen zur Registrierung von Mac OS X-Geräten finden Sie unter Mac OS X-Geräte.

Anweisungen zur Registrierung von Windows 10-Geräten finden Sie unter Windows-Geräte.

> **Hinweis**
>
> Unterstützung für Symbian-Geräte gibt es in XenMobile 10.3 nicht mehr.

Geräterichtlinien

Folgende neue MDM-Richtlinien stehen in XenMobile 10.3 zur Verfügung:

- **App-Sperre**: dient zum Definieren einer Liste von Apps, die auf dem Gerät ausgeführt werden dürfen, oder einer Liste von Apps, die auf einem Gerät blockiert werden. Verfügbar für iOS und Android. Obwohl die Geräterichtlinie auf den meisten Android L- und M-Geräten funktioniert, funktioniert App-Sperre nicht auf Android N oder neueren Geräten, da die erforderliche API von Google eingestellt wurde.
- **App-Netzwerkauslastung**: dient zum Festlegen von Netzwerkauslastungsregeln für die Verwendung von Netzwerken, z. B. mobilen Datennetzwerken, durch verwaltete Apps. Die Regeln gelten nur für verwaltete Apps. Verfügbar für iOS.
- **Verbindungsmanager**: dient zum Konfigurieren der Art und Weise, wie Apps eine Verbindung mit dem Internet oder einem privaten Netzwerk herstellen. Diese Einstellungen funktionieren nur auf Pocket PCs (Touchscreengeräte). Verfügbar für Windows Mobile und Windows CE.
- **Apps in Samsung Container kopieren**: dient zum Erstellen eines SEAMS- oder KNOX-Containers für Apps auf Samsung-Geräten. Verfügbar für Samsung SEAMS und Samsung KNOX.
- **Dateien und Ordner löschen**: dient zum Festlegen der Dateien und Ordner, die gelöscht werden müssen. Verfügbar für Windows Mobile und Windows CE.
- **Device health attestation**: aktiviert Device Health Attestation, ein Windows 10-Feature für Sicherheit und zur Verhinderung von Datenverlust, mit dem Sie die Integrität eines Windows 10-Geräts ermitteln und ggf. Maßnahmen zum Durchsetzen von Unternehmensrichtlinien ergreifen können. Die Nutzlasten werden nur für betreute Geräte unter Windows 10 und höher unterstützt. Verfügbar für Windows Phone und Windows Tablet.
- **Gerätename**: ermöglicht die Festlegung der Namen von iOS- und Mac OS X-Geräten zur einfacheren Identifizierung. Sie können Makros, Text oder eine Kombination daraus verwenden, um Gerätenamen festzulegen.
- **Registrierungsschlüssel und -werte löschen**: dient zum Festlegen der Registrierungsschlüssel und -werte, die gelöscht werden müssen. Ein leerer Wert bedeutet, dass der Eintrag ein Registrierungsschlüssel ist. Verfügbar für Windows Mobile und Windows CE.
- **Unternehmensdatenschutz**: ermöglicht das Festlegen von Apps, die Unternehmensdatenschutz auf einer von ihnen festgelegten Erzwingungsebene erfordern. Die Richtlinie gilt für Windows Phone- und Windows -Tablet-Geräte.
- **iOS- und Mac OS X-Profilimport**: Die Option zum Konfigurieren dieser Richtlinie für Mac OS X ist neu in XenMobile 10.3. Mit dieser Richtlinie können Sie eine XML-Datei für die iOS- oder Mac OS X-Gerätekonfiguration importieren. Die Datei enthält Gerätesicherheitsrichtlinien und -einschränkungen, die Sie mit Apple Configurator vorbereitet haben.
- **Registrierung**: In der Registrierung von Windows Mobile und Windows CE werden Daten zu Apps, Treibern, Benutzereinstellungen und Konfigurationseinstellungen gespeichert. Sie können Registrierungsschlüssel und -werte zum Verwalten von Windows Mobile-/CE-Geräten definieren.
- **Hintergrundbild**: ermöglicht das Hinzufügen einer PNG- oder JPG-Datei, um Hintergrundbilder auf dem Sperr- und Homebildschirm oder auf beiden festzulegen. In iOS 7.1.2 und höher verfügbar. Zum Verwenden verschiedener Bilder auf

iPads und iPhones müssen Sie unterschiedliche Richtlinien erstellen und den entsprechenden Benutzern bereitstellen.
- **Windows CE-Zertifikat**: dient zum Erstellen eines Zertifikats mit einer externen PKI für die Bereitstellung Geräten.

Eine Matrix aller alten und neuen Richtlinien nach Plattform finden Sie unter XenMobile-Geräterichtlinien nach Plattform.

Übersicht über neue Features und Erweiterungen nach Plattform

iOS

- **Neue Geräterichtlinien** App-Netzwerkauslastung, Gerätename und Hintergrundbild
- **Ändern des Zustands einer App von verwaltet in nicht verwaltet**: Option für iOS 9.0 zum Ändern des Zustands einer App von verwaltet in nicht verwaltet. Beim Hinzufügen einer App im öffentlichen App-Store für iOS in der XenMobile-Konsole steht die Option **Verwaltung der App erzwingen** zur Verfügung. Standardmäßig ist diese Option auf **Aus** gesetzt. Wenn Sie die Einstellung **Ein** auswählen und die App als nicht verwaltet installiert wird, werden die Benutzer aufgefordert, die Verwaltung der App auf nicht betreuten Geräten zuzulassen. Einzelheiten finden Sie unter Hinzufügen einer App aus einem öffentlichen App-Store zu XenMobile.
- **Neue Einschränkungen und Richtlinienoptionen für Apple Configurator 1.7.2**: Weitere Informationen finden Sie unter Einschränkungsrichtlinien für Geräte.
- **Unterstützung für Befehle "RequestMirroring" und "StopMirroring"**: Weitere Informationen finden Sie unter Referenz zur XenMobile REST-API.
- **Verbesserungen am Gerätesetupassistenten für DEP**: Weitere Informationen finden Sie unter Massenregistrierung von iOS-Geräten.
- **VPN-Schlüssel "OnDemandRules"**: Weitere Informationen finden Sie unter VPN-Geräterichtlinien.

Android

- **Samsung KNOX Container-Konfiguration**: Weitere Informationen hierzu finden Sie unter Apps in Samsung Container kopieren.
- **Samsung SAFE-APIs**: Weitere Informationen finden Sie unter Referenz zur XenMobile REST-API.
- **ELM-Schlüssel für Samsung-Android-Geräte**:
- **Geräterichtlinie zum Sperren von Apps**: Weitere Informationen finden Sie unter Geräterichtlinie zum Sperren von Apps.

Windows CE

- **Anmeldeinformationsanbieter-Konfiguration**: Weitere Informationen finden Sie unter Anmeldeinformationsrichtlinie.
- **Windows CE-Zertifikatkonfiguration**: Weitere Informationen finden Sie unter Windows CE-Geräterichtlinie für Zertifikate.
- **Registrierungsrichtlinie**: Weitere Informationen finden Sie unter Registrierungsrichtlinie.
- **Verbinden bei SMS-Empfang/Verbinden bei Anruf**:
- **Andere neue Geräterichtlinien**: Verbindungsmanager, Dateien und Ordner löschen, Registrierungsschlüssel und -werte löschen.

Windows Phone 10 und Windows Tablet 10

- Neue Geräterichtlinien: Datenschutz für Unternehmen und Device Health Attestation
- Neue Geräterichtlinienoptionen für Windows Phone und Windows Tablet:

  App-Bestand

Anmeldeinformationen
Benutzerdefinierte XML
Passcode
Einschränkungen
AGB
VPN
WiFI

- Neue Geräterichtlinienoptionen für Windows Tablet:

  App-Deinstallation
  Sideloadingschlüssel
  Signaturzertifikat
  Webclip
  WorxStore

- Neue Geräterichtlinienoptionen für Windows Phone:

  Enterprise Hub
  Speicherverschlüsselung

Mac OS X

- Drahtlose Registrierung. Weitere Informationen finden Sie unter Mac OS X.
- Geräteverwaltungsdaten in der XenMobile-Konsole mit Geräteeigenschaften, Zertifikaten, Berichten und unterstützten Profilen
- Sicherheitsaktionen auf Mac OS X-Geräten: selektives Löschen Sperren, Widerrufen, Löschen
- Neue Geräterichtlinienoptionen:

  Gerätename
  iOS- und Mac OS X-Profilimport
  AirPlay-Spiegelung
  App-Bestand
  Kalender (CalDav)
  Kontakte (CardDAV)
  Anmeldeinformationen
  Exchange
  Schriftart
  LDAP
  E-Mail
  Passcode
  Profilentfernung
  Einschränkungen
  SCEP
  VPN
  Webclip
  WiFI

Neue Features und Verbesserungen für Android for Work

- **Unterstützung für Geräte mit früheren Android-Versionen**:
- **Bereitstellen des Gerätebesitzermodus in Android for Work**

  Sie können nicht nur Android for Work-Apps oder Android-Geräte im BYOD-Modus verwalten, Sie können auch Unternehmensgeräte durch das Bereitstellen des Gerätebesitzermodus verwalten. Verwenden Sie dazu NFC (Near Field Communication) zwischen Geräten. Auf einem Gerät wird das Worx Provisioning Tool ausgeführt und das Gerät überträgt per NFC auf ein neues Gerät oder ein Gerät, das auf die Werkseinstellungen zurückgesetzt wurde. Der Gerätebesitzermodus ist der Unternehmensgerätemodus für die meisten Geräte mit Android 5.x.x.

- **Massenkauf von Android for Work**

  Sie können den Massenkauf von Lizenzen in der XenMobile-Konsole für Apps verwalten, die für Android for Work aktiviert sind. Das Massenkaufabonnement für Android for Work vereinfacht für eine Organisation das Finden, Kaufen und Bereitstellen von Apps und anderer Daten in großer Zahl. Wenn Sie XenMobile einen kostenpflichtigen öffentlichen App-Store für Android for Work hinzufügen, können Sie den Lizenzierungsstatus für Massenkäufe, die Gesamtanzahl verfügbarer Lizenzen, überprüfen. Wenn Sie Benutzern die App bereitstellen, können Sie die Anzahl der zurzeit verwendeten Lizenzen und die E-Mail-Adressen der Benutzer, die eine Lizenz verwenden, überprüfen. Sie können einen Benutzer auswählen und dann auf **Zuweisung aufheben** klicken, um die Lizenzzuweisung zu beenden und eine Lizenz für einen anderen Benutzer freizugeben. Sie können die Zuweisung der Lizenz jedoch nur aufheben, wenn der Benutzer nicht zu einer Bereitstellungsgruppe gehört, die diese App enthält.

Gemeinsam genutzte Geräte

XenMobile ermöglicht die Konfiguration von Geräten, die von mehreren Benutzern verwendet werden. Weitere Informationen finden Sie unter Gemeinsam verwendete Geräte in XenMobile.

Sprachunterstützung

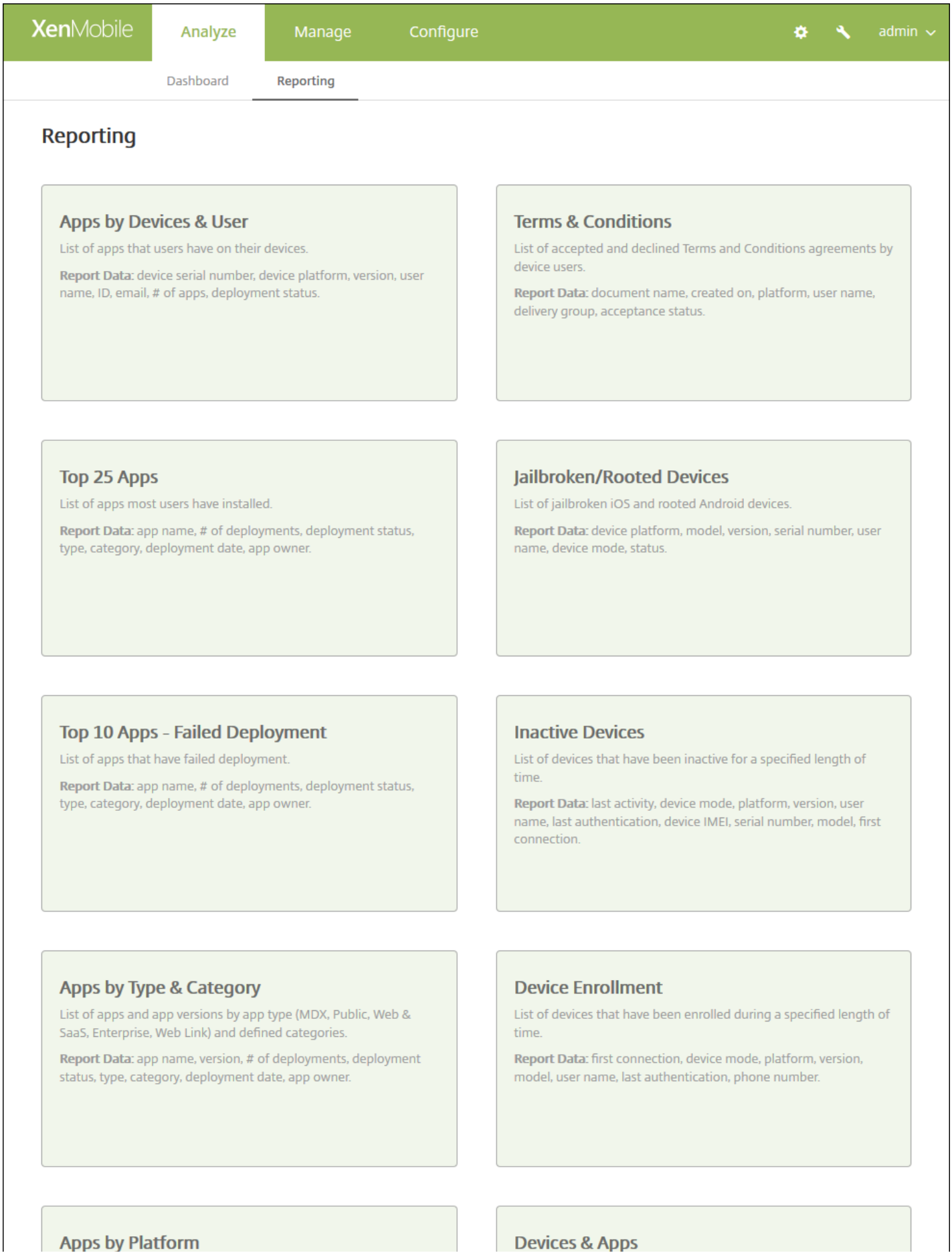
Die XenMobile-Konsole von XenMobile 10.3 steht auf Deutsch, Koreanisch und Portugiesisch zur Verfügung. Die MDX-Richtlinien werden nun in der XenMobile-Konsole lokalisiert angezeigt. Weitere Informationen finden Sie unter Sprachunterstützung für XenMobile.

Berichte

Über die Registerkarte **Berichterstellung** der XenMobile-Konsole können Sie 10 vordefinierte Berichte generieren.

- **Apps nach Geräten & Benutzer**: Liste der Apps, die Benutzer auf ihren Geräten haben
- **AGB**: Benutzerliste mit Informationen dazu, ob die Benutzer die AGB akzeptiert oder abgelehnt haben
- **Top 25 Apps**: Liste der 25 meistinstallierten Apps
- **Geräte mit Jailbreak/Rooting**: Liste der iOS-Geräte mit Jailbreak und der gerooteten Android-Geräte
- **Top 10 Apps - Bereitstellung fehlgeschlagen**: Liste der Apps, deren Bereitstellung fehlgeschlagen ist
- **Inaktive Geräte**: Liste der Geräte, die für eine bestimmte Zeitdauer inaktiv waren
- **Apps nach Typ & Kategorie**: Liste der Apps sortiert nach Version, Typ und Kategorie
- **Geräteregistrierung**: Liste der Geräte, die im angegebenen Zeitraum registriert wurden
- **Apps nach Plattform**: Liste der Apps und App-Versionen sortiert nach Geräteplattform und -version
- **Geräte & Apps**: Liste aller Geräte, Gerätedaten und installierter Apps

Zum Erstellen eines Berichts klicken Sie auf die Registerkarte **Analysieren** in der XenMobile-Konsole und dann auf **Berichterstellung**. Die Berichte haben das CSV-Format und können mit Programmen wie Microsoft Excel geöffnet werden. Weitere Informationen finden Sie unter Berichte in XenMobile.



List of apps and app versions installed on various device platforms and device versions.

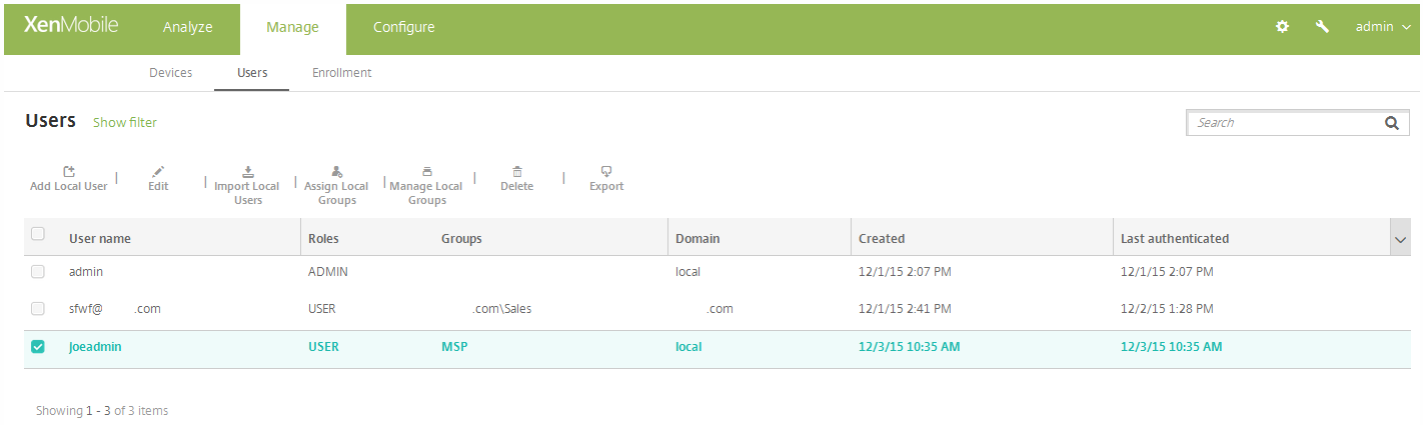
Report Data: app name, version, # of deployments, deployment status, deployment date, app owner, device platform, version, model, model name.

List of all devices, device data, and apps installed.

Report Data: device serial number, user name, ID, email, device platform, version, model, mode, status, last connection, enrollment status, enrollment date, device ownership, location, certificate expiration, app name, version, deployment status, type, category, deployment date, app owner, app ID.

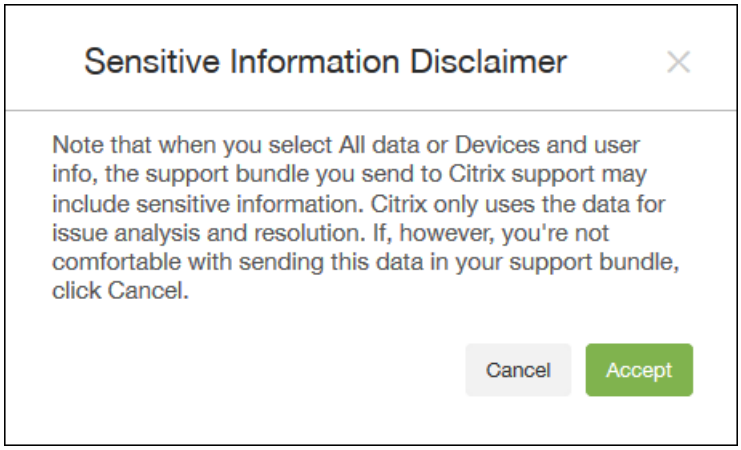
Hinzufügen von LDAP-Mitgliedern (lokale Benutzer) zu Gruppen

In vielen Organisationen werden keine Active Directory-Gruppen konfiguriert, jedoch wird ggf. eine lokale Gruppe für einen bestimmten Zweck (Pilotprojekt o. Ä.) benötigt. In XenMobile 10.3 können Sie lokale LDAP-Benutzer einer lokalen Gruppe hinzufügen. Anschließend können Sie eine Bereitstellungsgruppe definieren, die die lokale Gruppe enthält. Die entsprechenden Benutzer können auf Apps und Richtlinien der Bereitstellungsgruppe zugreifen, ohne ihr Gerät registrieren zu müssen. Weitere Informationen finden Sie unter Erstellen, Bearbeiten oder Löschen lokaler Benutzer in XenMobile.



Rechtliche Vereinbarung für Supportpaket

Wenn Sie das erste Mal ein Supportpaket an Citrix Insight Services (CIS) hochladen, werden Sie aufgefordert, eine rechtliche Vereinbarung zu akzeptieren. Weitere Informationen finden Sie unter Erstellen von Supportpaketen in XenMobile.



Anonymisierung von Daten in Supportpaketen

Beim Erstellen von Supportpaketen in XenMobile werden vertrauliche Benutzer-, Server- und Netzwerkdaten standardmäßig anonymisiert. Sie können dieses Verhalten auf der Seite "Anonymisierung und Deanonymisierung" ändern. Sie können auch eine Zuordnungsdatei herunterladen, die XenMobile beim Anonymisieren von Daten speichert. Der Citrix Support fordert diese Datei u. U. an, um für die Suche nach einem Problem bei einem bestimmten Benutzer oder Gerät die Anonymisierung von Daten rückgängig zu machen. Weitere Informationen finden Sie unter Anonymisierung von Daten in Supportpaketen.

Konnektivitätsprüfungen

Über die Seite "XenMobile-Support" können Sie die Verbindung zwischen XenMobile und NetScaler Gateway sowie anderen Servern und Speicherorten prüfen. Weitere Informationen finden Sie unter Durchführen von Konnektivitätsprüfungen.

Microsoft Azure

Sie können Windows 10-Geräte in Microsoft Azure Active Directory einbinden, um die Registrierung von Geräten mit Azure als föderierter Active Directory-Authentifizierung zu ermöglichen. Weitere Informationen finden Sie unter Microsoft Azure-Einstellungen.

Behobene Probleme bei XenMobile Server 10.3

Jul 28, 2016

Die folgenden Probleme wurden in XenMobile 10.3 behoben Weitere Informationen zu behobenen Problemen in XenMobile 10.3.5 finden Sie unter Bekannte und behobene Probleme in XenMobile 10.3.5.

Ein E-Mail-Sendepräfix wird möglicherweise zweimal einer E-Mail-Adresse hinzugefügt, wenn eine E-Mail von einem SMTP über das SMS-Gateway eines Netzbetreibers gesendet wird. [#492629]

HTTP GET-Anfragen von Cisco Identity Service Engine an XenMobile schlagen u. U. mit einem Fehler 404 fehl. [#555554]

Wenn eine Dateiuploadrichtlinie eine Datei per Push auf Android-Geräten bereitstellt, schlägt das Bereitstellen von Dateien auf dem Gerät möglicherweise fehl. Stattdessen werden u. U. die AGB auf dem Gerät angezeigt. [#564144]

Wenn MDM-Identitätszertifikate per SCEP verteilt und mit der integrierten PKI veröffentlicht werden, sperrt XenMobile bei der Verlängerung der Identitäten das vorherige Zertifikat in bestimmten Fällen nicht richtig. Daher verlieren betroffene Geräte in manchen Fällen ihre MDM-Funktionalität. [#569999]

Nach dem Konfigurieren eines Proxyservers verursachen Konnektivitätsprüfungen Datenverkehr, der nicht über den Proxyserver übertragen wird, und die Verbindung schlägt fehl. [#571467]

Wenn Benutzer Mitglieder einer untergeordneten Domäne sind, schlagen die Verbindungen mit SAML-Apps fehl. [#571851]

Wenn eine iOS MDX-App auf der Liste der ausgeschlossenen Geräte steht, wird die App nicht im WorxStore angezeigt, wenn das Gerät im MAM-Modus (Mobilanwendungsverwaltungsmodus) ist. [#571900]

Nach dem Upgrade auf XenMobile 10 kann die Suche nach einem Gerät bis zu 30 Sekunden dauern und die CPU-Nutzung steigt auf 100 %. [#577010]

Beim Browsen von Intranetsites mit WorxWeb in einer Clusterumgebung mit mehreren Knoten können Benutzer u. U. nicht auf URLs zugreifen und die Meldung "Error Invalid OTT" wird angezeigt. [#577273]

Wenn Sie XenMobile mit einem Proxyserver konfigurieren, schlagen Versuche, Google Play-Anmeldeinformationen hinzuzufügen oder einen öffentlichen Android-Store zu erstellen, möglicherweise fehl. [#578727]

Bei dem Versuch, eine XenMobile-Konsole in einer veröffentlichten Version von Internet Explorer 11 zu öffnen, wird eine leere Seite angezeigt. [#578729]

Dieses Release unterstützt jetzt WPA2 Personal und WPA2 Enterprise für iOS 8. [#579616]

Beim Hinzufügen oder Hochladen einer App in der XenMobile-Konsole kann ein Fehler auftreten, wenn Sie die App mit einem Dateinamen nach XenMobile hochladen, der bereits vorhanden ist. [#580359]

Das Herunterladen von Worx-Apps über den WorxStore schlägt auf Android-Geräten fehl. [#582044]

Wenn Sie ein Makro mit dem Benutzernamen und der Telefonnummer eingeben, wird die Telefonnummer bei der Transformation nicht korrekt übersetzt. [#589130]

Der Befehl "Aktivierungssperre umgehen" funktioniert möglicherweise auf einigen iOS-Geräten nicht. [#589991]

Wenn Eigenschaftswert "memberOf" 255 Zeichen übersteigt, wird die Fehlermeldung "Keine Gruppen gefunden" angezeigt.

Wenn Benutzer versuchen, eine Windows-App über Worx Home zu öffnen, ist die Enumeration erfolgreich, die Anwendung wird jedoch nicht geöffnet. Benutzer erhalten die Fehlermeldung "Could not add account". [#590046]

Wenn Sie eine SCEP-Richtlinie (Simple Certificate Enrollment Protocol) mit einer Kennwortprüfung erstellen, können Sie die Richtlinie nicht speichern. Ab diesem Release ist das Feld "Kennwort überprüfen" optional. [#590798]

Wenn Sie XenMobile für die Verwendung eines Proxyservers konfigurieren, kann Android for Work keine Verbindung zu externen Websites herstellen. [#591707]

Das Hochladen einer IPA-App in App Controller schlägt mit folgender Fehlermeldung fehl: "Invalid package type for selected app". Die Meldung wird angezeigt, wenn ein Fehler in der PNG-Datei vorliegt. [#592748]

Wenn Benutzer versuchen, sich zu registrieren, wird die Fehlermeldung "Benutzer ist nicht vorhanden". Der Fehler tritt auf, wenn der Benutzer sich nach dem Löschen seiner Registrierung erneut registriert. Wenn dies passiert, werden Benutzer in Active Directory neu erstellt. [#593028]

Wenn Sie eine Kalendereinladung von einem Microsoft Outlook- oder Microsoft Exchange-Konto aus erstellen, kann es lange dauern, bis sie in WorxMail angezeigt wird. [#594542]

Wenn Sie einen Workflow konfigurieren und dabei einen anderen Port als 443 (Standardeinstellung) verwenden, können Benutzer den Workflowlink nicht öffnen. [#599441]

Benutzer können eine Android-App auf ihrem Gerät vom XenMobile-Server aus nicht aktualisieren. [#601251]

Benutzer können sich nicht an Worx-Apps anmelden, wenn sie sich über Azure Active Directory registrieren. [#608505]

Ab Dezember 2015 unterstützt Nexmo SMS nur HTTPS-Verbindungen. Die Standardeinstellung in XenMobile ist **EIN**. Wenn Sie den Wert auf **AUS** festlegen, hat das keine Auswirkungen. Nach dem Upgrade wird der Wert immer noch als **AUS** angezeigt, aber die Verbindungen sind sicher. [#609306]

WorxStore benötigt ein Programm für VPP-Benutzer (Volumenlizenzen), obwohl die Lizenz nur für das Gerät gilt. [#610338]

Bekannte Probleme bei XenMobile Server 10.3

Jul 28, 2016

Nachfolgend sind bekannte Probleme in XenMobile 10.3 aufgeführt. Weitere Informationen zu bekannten Problemen in XenMobile 10.3.5 finden Sie unter Bekannte und behobene Probleme in XenMobile 10.3.5.

- Die folgenden Fehler beziehen sich auf die folgenden Versionen von NetScaler bei einer Integration zwischen XenMobile und NetScaler, wenn das Sicherheitsprotokoll TLS 1.2 auf NetScaler konfiguriert ist:
  - NetScaler 11.x-Versionen vor 11.0.64
  - 10.5.59
  - 10.5.58

  Dieses Problem tritt nicht auf, wenn in Ihrer XenMobile MAM-Bereitstellung ein NetScaler Load Balancer zwischen XenMobile und NetScaler Gateway ist.

  Die Kommunikation zwischen NetScaler Gateway und XenMobile im MAM-Modus schlägt aufgrund von Problemen mit einer TLS 1.2-Sitzung auf dem Backend fehl. Daher können Benutzer bei einer Verbindung mit dem internen Netzwerk keine Apps aus dem WorxStore und keine Dateien von ShareFile herunterladen. [#591600#595713#596566#604409]
- App-Push schlägt nach der Deinstallation einer Unternehmensapp fehl. [#591450]
- Nach dem Entfernen der Lizenz von einer App bleibt die App auf dem Benutzergerät. Dies ist ein Drittanbieterproblem. [#596656]
- Wenn Benutzer versuchen, ihre persönlichen Geräte mit einem Microsoft-Unternehmenskonto zu registrieren, schlägt die Registrierung fehl. [#597037]
- Für die AGB Richtlinie wird der Status "installiert" oder "ausstehend" in der XenMobile-Konsole nicht angezeigt, selbst wenn die Richtlinie erfolgreich auf dem Gerät bereitgestellt wurde. [#598407]
- Einschränkungsrichtlinien sind auf Windows 10-Geräten wirksam. Benutzer erhalten jedoch keine Meldung darüber, dass ein blockiertes Feature deaktiviert ist. [#599064#606651]
- Wenn Sie eine Kategorie mit öffentlichen Apps und Unternehmensapps hinzufügen und dann ein Gerät in XenMobile registrieren, wird die Kategorie nicht angezeigt, wenn Benutzer Apps in Worx Home synchronisieren. [#599495]
- Wenn Sie beim Erstellen einer RBAC für gemeinsam genutzte Geräte keine Berechtigung für selektives Löschen hinzufügen, müssen Benutzer das Device Manager-Profil manuell vom Gerät entfernen, wenn sie versuchen, ihr Worx Home-Konto auf einem iOS-Gerät (im XenMobile Enterprise-Modus) zu löschen. [#600705]
- Wenn nach der Bereitstellung von App-Bestands- und Unternehmenshub-Richtlinien für eine App eine öffentliche App mit einem anderen Namen und einer anderen Beschreibung erstellt wird, sind der Name und die Beschreibung der App gleich, wenn Benutzer die App von Worx Home aus öffnen. [#600369]
- Wenn Sie bei der ersten Verwendung Microsoft SQL Server im SSL-Modus konfigurieren und das ZS-Zertifikat nicht dem SQL Server-Zertifikat entspricht, schlägt die Verbindung fehl. Wenn Sie dann mit einem ZS-Zertifikat, das dem SQL Server-Zertifikat entspricht, versuchen die Verbindung herzustellen, schlägt die Verbindung trotzdem fehl. Damit das Zertifikat funktioniert, starten Sie den XenMobile-Server neu, um den Truststore-Cache zu löschen. [#602609]

- Die Benutzernamen auf gemeinsam genutzten Geräten dürfen keine ASCII-Zeichen enthalten. Gemeinsam genutzte Geräte unterstützen keine Benutzernamen mit Nicht-ASCII-Zeichen. [#605544]
- Wenn Benutzer Einladungen mit einem Einmalkennwort für die IMEI-Bindung (Benutzername und Kennwort) und SMTP- und SMS-Benachrichtigungen erhalten, wird das erste Profil erfolgreich installiert, während die zweite Profilinstallation mit folgender Fehlermeldung fehlschlägt: "Profile Installation Fails. A connection to the server could not be established." Auf iPhone 6- und iPhone 6 Plus-Geräten gibt es eine IMEI- und eine MEID-Nummer und das Einmalkennwort bindet die MEID- statt die IMEI-Nummer. Sie können die IMEI-Nummer durch den eindeutigen Gerätebezeichner (Unique Device Identifier, UDID) des iPhones ersetzen oder eine normale Telefonnummer verwenden. [#606162]
- Nach dem Upgrade auf XenMobile 10.3 zeigen die Lizenzierungsinformationen an, dass die Lizenz eine Testversion für 30 Tage ist, und das Flag für "Lizenzserver konfiguriert" ist auf "wahr" festgelegt. Laden Sie nach dem Upgrade des XenMobile-Servers dieselbe Lizenz auf den Server hoch. Dadurch wird der Testzeitraum aufgehoben. [#607939]
- Benutzer können auf Windows 8.1-Tablets erfolgreich Apps vom Gerät entfernen. Unternehmensapps werden weiterhin in der XenMobile-Konsole unter "Geräteeigenschaften" angezeigt. [#608184]
- Die Optionen "App löschen" und "Selektives Löschen" funktionieren in XenMobile Enterprise gleich. [#608715]
- Der XenMobile-Server reagiert nicht mehr, wenn Sie eine Datei im Internet Explorer öffnen oder speichern. Starten Sie den Server neu, um fortzufahren. [#608724]
- Nach dem Upgrade auf XenMobile 10.3 ist Android for Work in der Browserrichtlinie nicht vorhanden, obwohl blockierte Webadressen und Lesezeichen vorhanden sind. [#609002]
- Auf Tablets, auf denen Windows 8.1 und Windows 10 ausgeführt wird, bleiben nach dem manuellen Löschen von Konten vom Gerät einige Richtlinien zurück. [#609201]
- Wenn Benutzer auf Tablets mit Windows 10 die Einstellung für automatische Updates ändern, wird die Änderung nicht in der XenMobile-Konsole unter den Geräteeigenschaften im Bereich "Sicherheitsinformationen" angezeigt. [#609254]
- Für den WorxStore-Namen werden nur ASCII-Zeichen unterstützt. [#609535]
- Versuche, eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) aus Internet Explorer- und Firefox-Webbrowsern herunterzuladen, schlagen mit folgender Fehlermeldung fehl: "The Webpage cannot be displayed". Das Herunterladen der CSR aus dem Chrome-Webbrowser funktioniert. [#609552]
- Wenn Sie bei der Anmeldung an der XenMobile-Konsole zu **Analysieren** > **Berichterstellung** navigieren und dann auf **Inaktive Geräte** klicken, wird eine leere Seite angezeigt statt eine Datei herunterzuladen. [#609649]
- Beim Konfigurieren eines Arbeitsbereichs in Citrix Workspace Cloud werden Bereitstellungsgruppen nicht mit Active Directory-Benutzern oder -Gruppen aktualisiert, die zu einfach oder zweifach untergeordneten Domänen gehören. [#609673]
- Das Registrieren eines Windows 10-Geräts schlägt fehl, wenn mehrere AGB-Richtlinien bereitgestellt wurden und keine der Richtlinien die Standard-AGB ist. [#609694]
- Wenn Sie eine Richtlinie aus einer Bereitstellungsgruppe entfernen, dann auf die Schaltfläche **Zusammenfassung** klicken und die Richtlinie speichern, bleibt die Ressource in der Bereitstellungsgruppe. Klicken Sie auf **Weiter** statt auf **Zusammenfassung**, und die Richtlinie wird aus der Bereitstellungsgruppe entfernt. [#610109]
- Damit die Erweiterung der Originaldatei auf einem Windows CE-Gerät erhalten bleibt, geben Sie nicht den

Zieldateienamen in der Richtlinie an. [#610601]

- Beim Konfigurieren einer VPN-Geräterichtlinie für Mac OS X wird die **VPN**-Option in der Liste **Verbindungstypen** angezeigt. Sie können diese Option jedoch nicht für Mac OS X-Geräte konfigurieren. [#612846]
- Wenn der WorxStore einen benutzerdefinierten Namen hat und XenMobile 10.1 auf Version 10.3 aktualisiert wird, müssen Sie vor dem Update den Namen des Stores auf die Standardeinstellung **Store** ändern und diese Einstellung auf Geräten bereitstellen. Andernfalls verursacht der benutzerdefinierte Storename Probleme bei der XenMobile 10.3-Registrierung, beim Zugriff auf Worx Home und den WorxStore sowie bei der App-Bereitstellung auf iOS-Geräten. [#614049]
- Sie können Android for Work nicht in der XenMobile-Konsole aktivieren. Wenn Sie die Kontoeinstellungen für Android for Work konfigurieren und die von Google erhaltene Dienstkonto-ID (enthält nur Ziffern) eingeben, wird beim Speichern der Einstellungen ein Fehler angezeigt. Wenn Sie die Dienstkonto-ID im früheren Google-Format (Ziffern und Buchstaben) eingeben, tritt derselbe Fehler auf, da das Format nicht der Dienstkonto-ID im XenMobile-Server entspricht. Dies ist ein Drittanbieterproblem.

  Um dieses Problem zu umgehen, aktivieren Sie Android for Work, indem Sie eine Servereigenschaft für die Google Client-ID hinzufügen.

  1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
  2. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Servereigenschaft hinzufügen** wird angezeigt.
  3. Klicken Sie in der Liste **Schlüssel** auf **Benutzerdefinierter Schlüssel**.
  4. Geben Sie unter **Schlüssel** Folgendes ein: **google.aw.enterprise.client.id**
  5. Geben Sie unter **Wert** den numerischen Teil der Client-ID ein, z. B. 3838383838388383.
  6. Geben Sie unter **Anzeigename** einen Anzeigenamen ein, z. B. "Google domain client ID".
  7. Klicken Sie auf **Speichern**.

  [#615118]
- Auf Computern mit Mac OS X und auf iPads führt XenMobile 10.3 immer zuerst Lösch- bzw. Entfernungsaktionen aus, unabhängig von der in der XenMobile-Konsole festgelegten Reihenfolge. [#620459]
- Wenn Sie iOS-Massenregistrierung aktivieren und dann die Stammzertifizierungsstelle (ZS) des XenMobile SSL-Zertifikats aktualisieren, schlägt die Geräteregistrierung oder Neuregistrierung möglicherweise fehl. Das Problem kann auftreten, wenn Sie von einem selbstsignierten Zertifikat zu einem öffentlichen Zertifikat wechseln, ein Zertifikat von einem neuen Anbieter erwerben oder zu einer internen Unternehmenszertifizierungsstelle wechseln. Das Problem wirkt sich nicht auf vorhandene registrierte Geräte aus. Führen Sie als Workaround die folgenden Schritte aus:

  1. Klicken Sie in der XenMobile-Konsole auf **Einstellungen** > **iOS-Massenregistrierung**.
  2. Klicken Sie unter **DEP-Konfiguration** neben **Device Enrollment Program (DEP) zulassen** auf **NEIN** und dann auf **Speichern**. Warten Sie einige Sekunden. Mit diesem Schritt wird das vorherige DEP-Profil von den DEP-Geräten auf dem Apple DEP-Portal entfernt.
  3. Klicken Sie auf **Verwalten** > **Geräte**. Stellen Sie sicher, dass kein DEP-registriertes Gerät in der Spalte **DEP-registriert** angezeigt wird.

4. Klicken Sie erneut auf **Einstellungen** > **iOS-Massenregistrierung**.
5. Klicken Sie unter **DEP-Konfiguration** neben **Device Enrollment Program (DEP) zulassen** auf **JA** und dann auf **Speichern**. Warten Sie einige Sekunden. Mit diesem Schritt wird allen DEP-Geräten ein neues Profil hinzugefügt.
6. Klicken Sie auf **Verbindung testen**, um sicherzustellen, dass die Verbindung zwischen XenMobile und dem Apple DEP-Server weiterhin funktioniert.
7. Klicken Sie erneut auf **Verwalten** > **Geräte**. Stellen Sie sicher, dass alle DEP-registrierten Geräte neu registriert und in der Spalte **DEP-registriert** aufgeführt sind.

Weitere Informationen über das Apple DEP finden Sie unter Massenregistrierung von iOS-Geräten.
[#635699]

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.
- Geräteregistrierung: 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. Weitere Informationen finden Sie unter Informationen zum MDX Toolkit.
- 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.

XenMobile unterstützt eine integrierte Lösung, die die Verwaltung von Geräten und Apps über die XenMobile-Konsole gestattet. In diesem Abschnitt wird die Referenzarchitektur für die XenMobile-Bereitstellung erläutert.

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.

Weitere Informationen zum Konfigurieren von XenMobile 10 Enterprise Edition für eine Notfallwiederherstellung und ein Architekturdiagramm finden Sie unter Disaster Recovery Guide für XenMobile.

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.

Mobilgeräteverwaltungsmodus (MDM-Modus)

XenMobile MDM Edition ermöglicht die Verwaltung mobiler iOS-, Android-, Amazon- und Windows Phone-Geräte (siehe Unterstützte Geräteplattformen in XenMobile). Sie stellen XenMobile im MDM-Modus bereit, wenn Sie nur seine MDM-Features verwenden möchten. 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, jedoch keine Windows Phones (siehe Unterstützte Geräteplattformen in XenMobile). Sie stellen XenMobile im MAM-Modus (auch MAM-Only-Modus genannt) bereit, wenn Sie nur die MAM-Features ohne Registrierung der Geräte für MDM verwenden möchten. 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

Im kombinierten MDM- und MAM-Modus können mobile Apps und Daten sowie mobile iOS-, Android- und Windows Phone-Geräte verwaltet werden (siehe Unterstützte Geräteplattformen in XenMobile). Sie stellen XenMobile im ENT-Modus (= Enterprise) bereit, wenn Sie MDM- und MAM-Features verwenden möchten. 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.

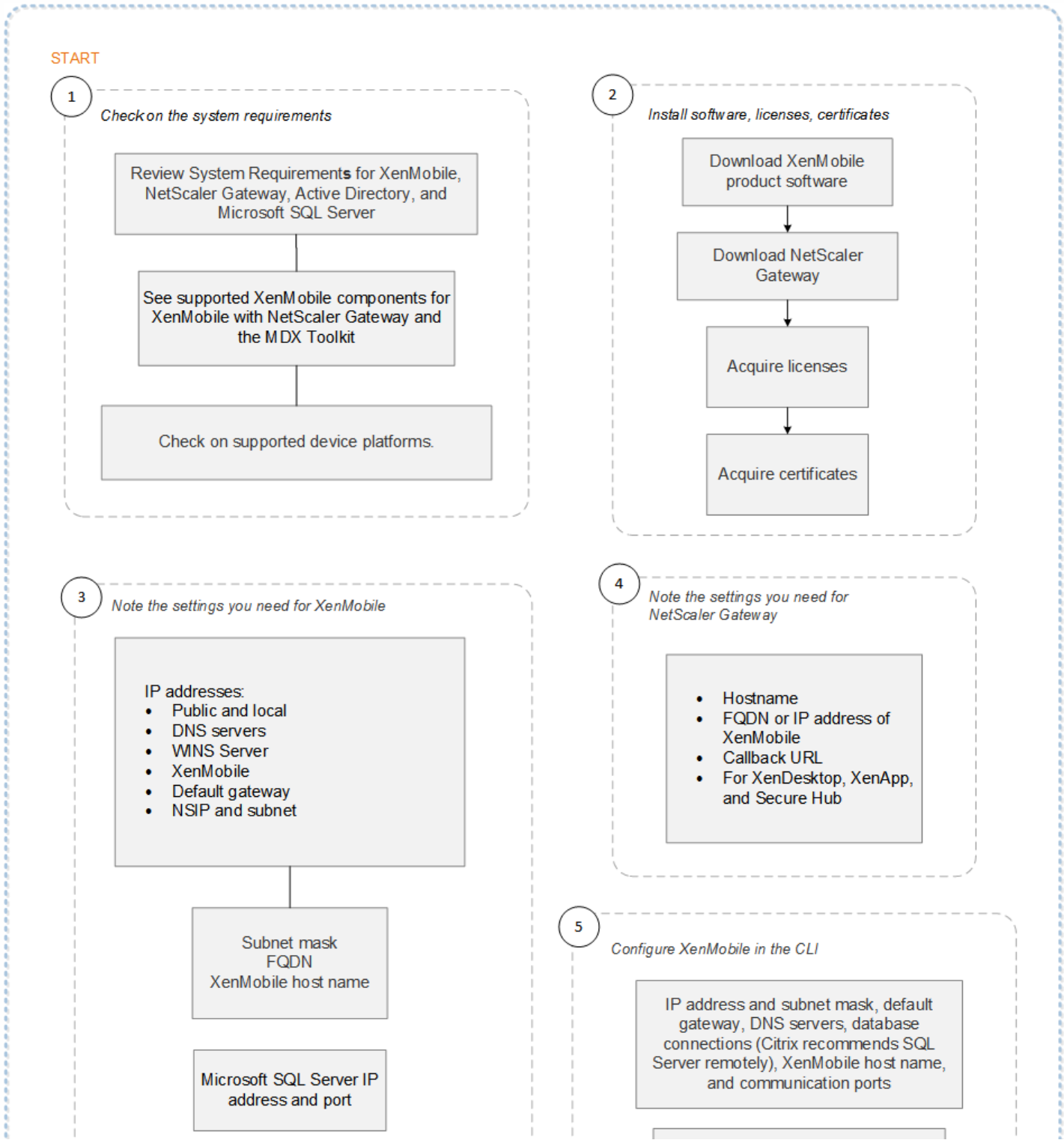
XenMobile im internen Netzwerk: Eine andere Bereitstellungsoption ist, den XenMobile-Server im internen Netzwerk

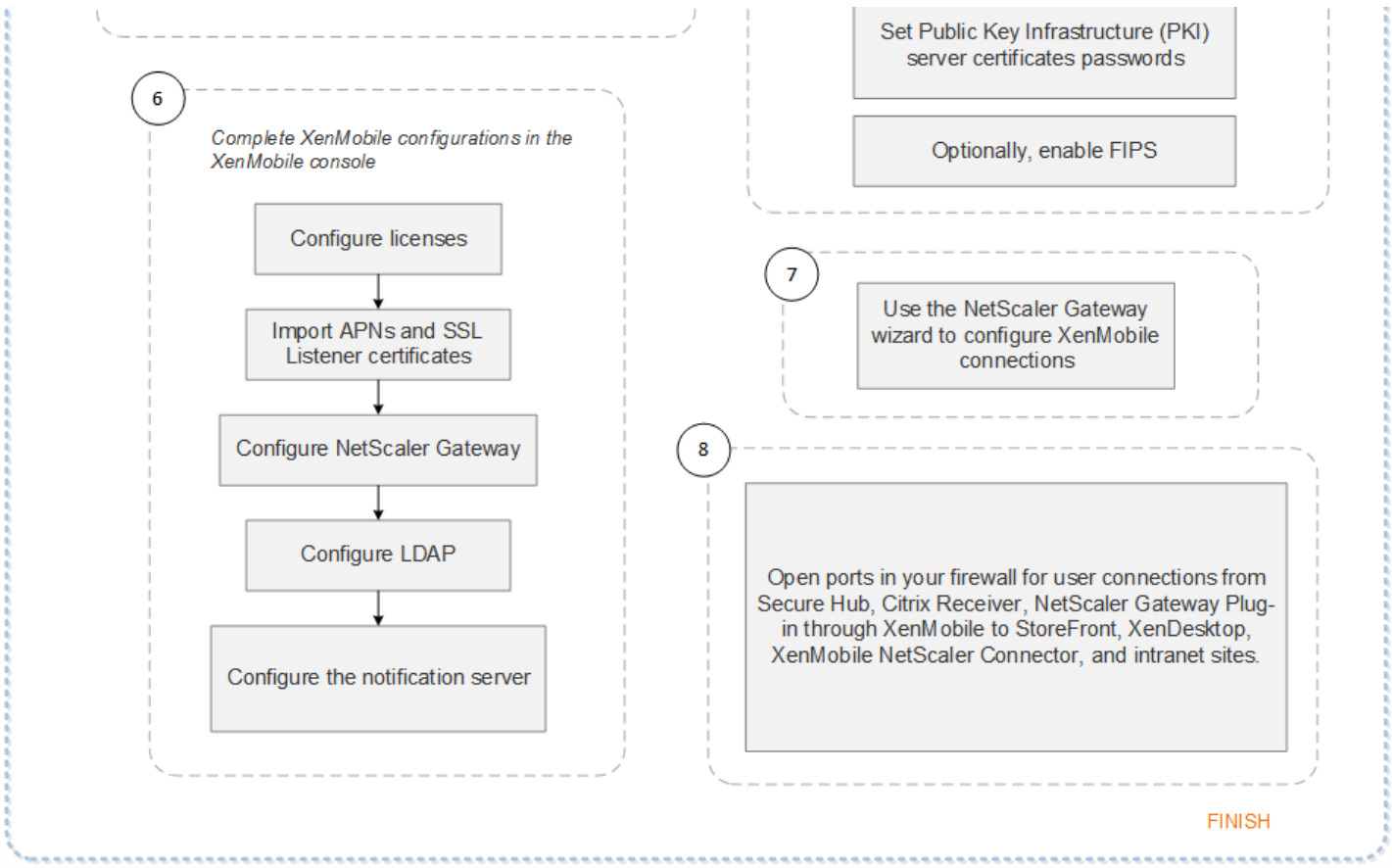
statt in der DMZ zu haben. Diese Bereitstellungsoption wird verwendet, wenn Sicherheitsrichtlinien vorschreiben, dass nur Netzwerkgeräte in der DMZ sein dürfen. Da der XenMobile-Server in dieser Bereitstellung nicht in der DMZ ist, müssen Sie keine Ports in der internen Firewall öffnen, um Zugriff auf den SQL Server und PKI-Server von der DMZ zu geben.

Flussdiagramm der Bereitstellung von XenMobile mit NetScaler Gateway

Oct 13, 2016

Dieses Flussdiagramm führt Sie durch die Hauptschritte zur Bereitstellung von XenMobile 10.3 mit NetScaler Gateway. Im Anschluss an die Abbildung folgen Links zu Abschnitten zu jedem Schritt.





1

- Systemanforderungen für XenMobile 10,3
- XenMobile-Kompatibilität
- Unterstützte Geräteplattformen in XenMobile 10,3

2

- Installieren von XenMobile
- Zertifikate in XenMobile
- Lizenzierung von XenMobile

3

- Installationscheckliste für XenMobile

4

- Installationscheckliste für XenMobile

5

- Konfigurieren von XenMobile im Eingabeaufforderungsfenster

6

- Konfigurieren von XenMobile in einem Webbrowser

7

- Konfigurieren von Einstellungen für die XenMobile-Umgebung

8

- Portanforderungen für XenMobile

Das Flussdiagramm ist auch im PDF-Format verfügbar.

Flussdiagramm für die Bereitstellung von XenMobile

Skalierung von XenMobile

Oct 13, 2016

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.

Die Angaben in diesem Artikel dienen als Richtlinie zur Bestimmung von Leistung und Skalierbarkeit einer XenMobile 10.3-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.

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

> **Important**
>
> Die Automatisierungsanforderung für diesen Bericht ist 1.000 bis 100.000 Geräte. Anforderungen, die 100.000 Geräte übersteigen, gehen über diesen Bericht hinaus.

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.

- Die Verbindungsanzahl pro Benutzersitzung auf NetScaler ist ein wichtiger Gesichtspunkt.
- 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.

Die folgende Tabelle 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.

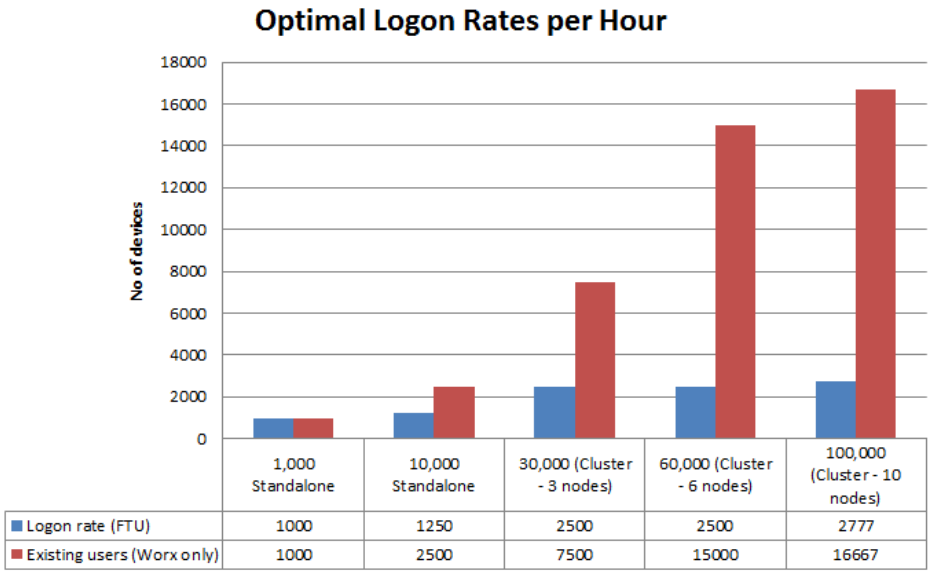
Erwartete Gerätezahl	1.000	10.000	30.000	60.000	100.000
Tatsächliche Gerätezahl	1.000	9.997	29.976	59.831	99.645
Anmelderate					
Onboarding (Erstverwendung)	125	1.250	2.500	2.500	2.777
Vorhandene Benutzer (nur Worx)	1.000	2.500	7.500	15.000	16.667
Konfiguration					
Referenzumgebung	VPX-XenMobile, eigenständig	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	Extern	Extern: Microsoft SQL Server	Extern: Microsoft SQL Server	Extern: Microsoft SQL Server	Extern: Microsoft SQL Server

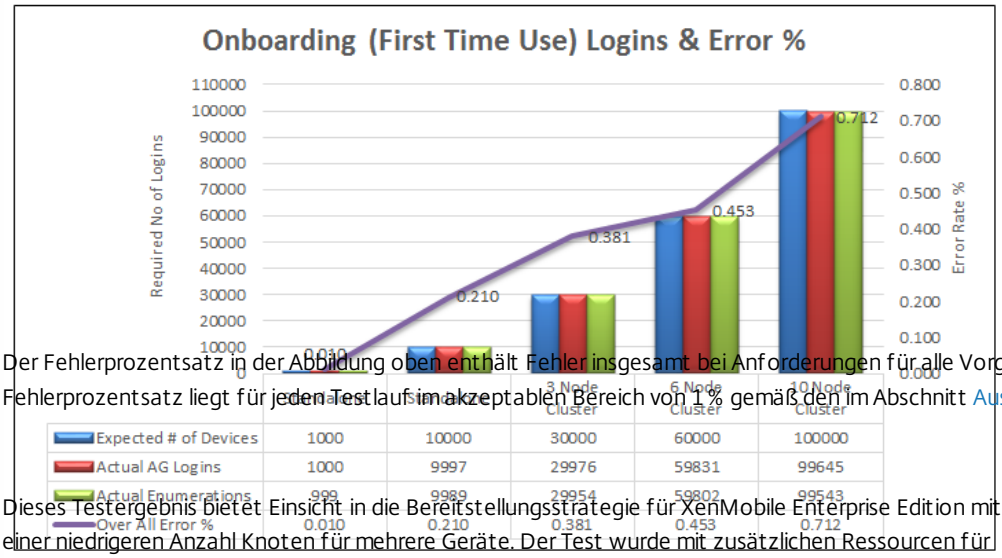
		Speicher: 16 GB vCPUs: 12	Speicher: 16 GB vCPUs: 12	Speicher: 32 GB vCPUs: 12	Speicher: 32 GB vCPUs: 16

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

Die folgenden Informationen bieten zusätzliche aufgezeichnete Datenpunkte, die die Ergebnisse in der Tabelle oben beeinflussen.

- Registrierungs- bzw. Anmeldelatenz (Roundtripzeit)
  - Durchschnittliche Latenz insgesamt: 0,5 bis 1,5 Sekunden
  - Durchschnittliche Latenz bei NetScaler Gateway-Anmeldungen: > 120 bis 440 ms
  - Durchschnittliche Latenz bei Worx Store-Anforderungen: 2 bis 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
  - Langsame Reaktionszeit der XenMobile-Konsole bei hohen Lasten



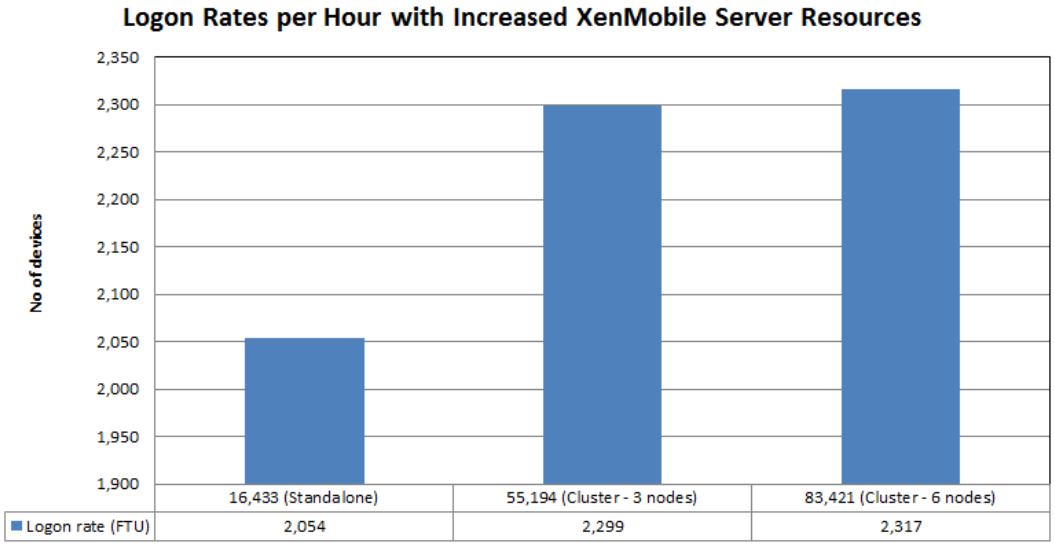


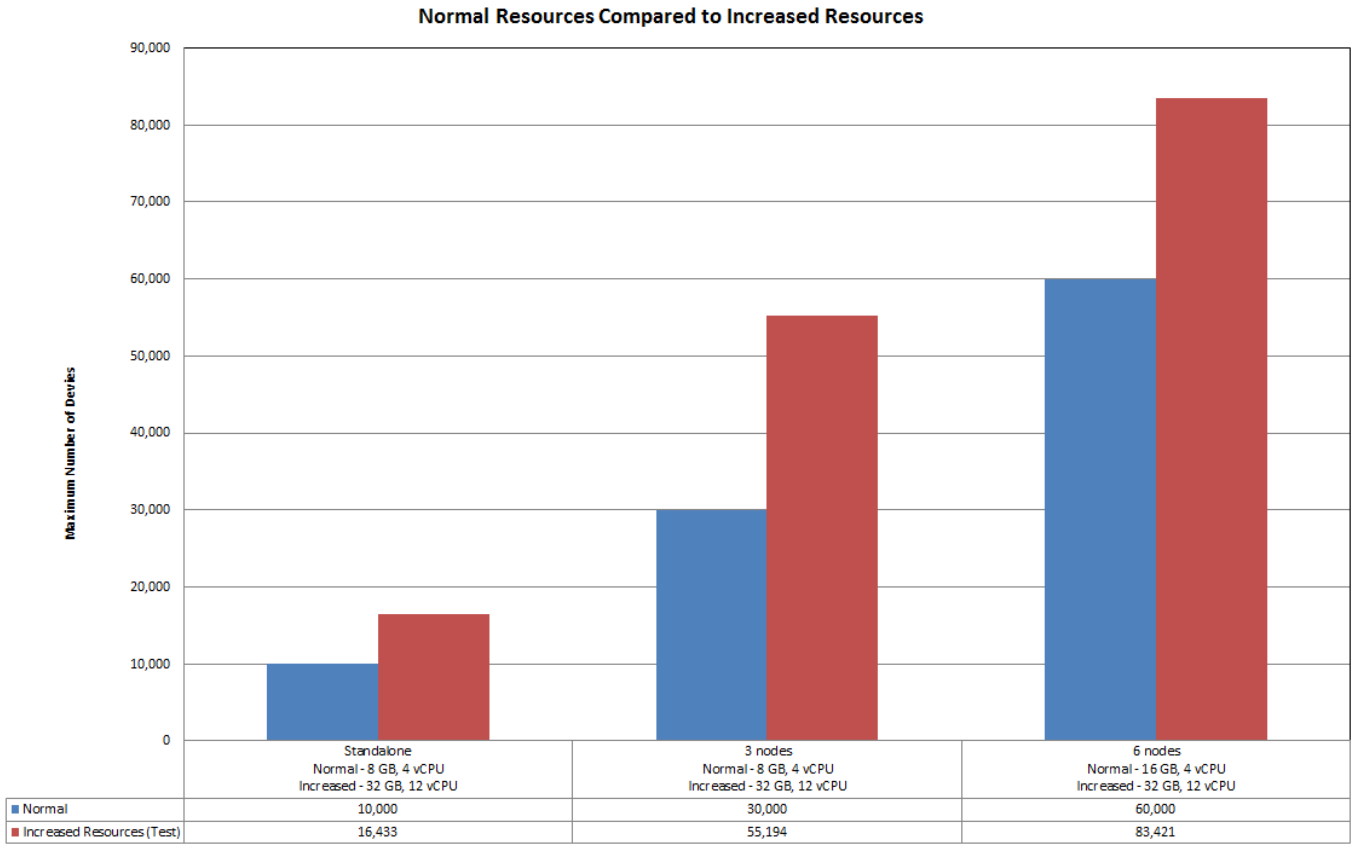
Der Fehlerprozentsatz in der Abbildung oben enthält Fehler insgesamt bei Anforderungen für alle Vorgänge und nicht nur für Anmeldungen. Der Fehlerprozentsatz liegt für jeden Testlauf im akzeptablen Bereich von 1% gemäß den im Abschnitt Ausgangskriterien aufgeführten Kriterien.

Dieses Testergebnis bietet Einsicht in die Bereitstellungsstrategie für XenMobile Enterprise Edition mit einer niedrigeren Anzahl Knoten für mehrere Geräte. Der Test wurde mit zusätzlichen Ressourcen für die Hardwarekomponenten (CPU und Speicher) der XenMobile-Server ausgeführt, um die Skalierbarkeit zu messen. Dies führte zu einem Anstieg der von den XenMobile-Serverknoten unterstützten maximalen Anzahl an Sitzungen/Geräten im Vergleich zum Test mit normalen Ressourcen und der gleichen Anzahl Knoten.

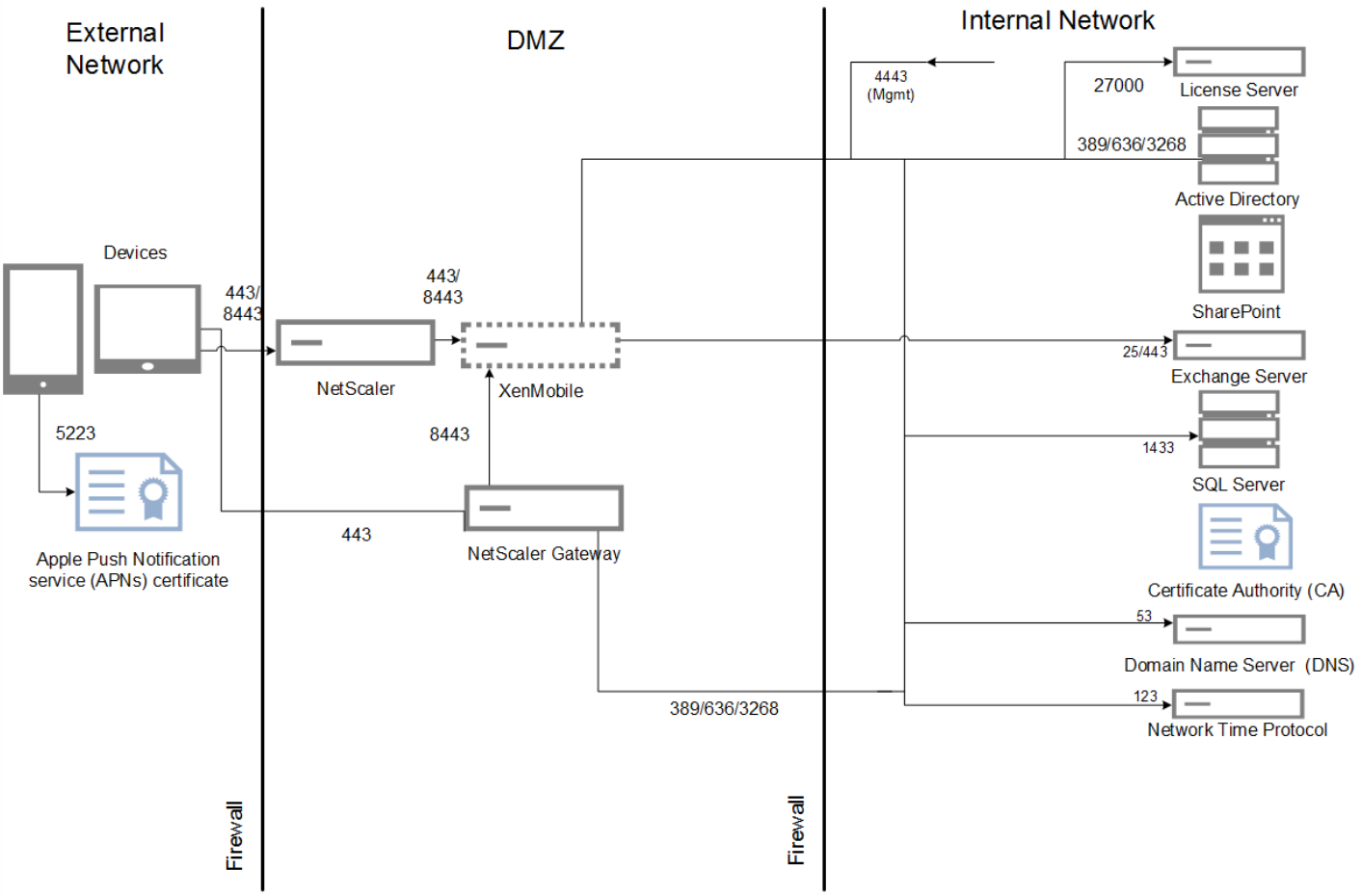
Skalierbarkeit			
Maximale Anzahl tatsächlicher Geräte	16.433	55.194	83.421
Anmelderate			
Onboarding für Erstverwendung - Hinzufügen neuer Benutzer	2.054	2.299	2.317
Konfiguration			
Referenzumgebung	VPX-XenMobile, eigenständig	MPX-XenMobile, 3 Cluster	MPX-XenMobile, 6 Cluster
NetScaler Gateway	MPX-10500	MPX-10500	MPX-20500
XenMobile-Modus	Eigenständig	Cluster	Cluster
XenMobile-Cluster	nicht zutreffend	3	6
XenMobile – virtuelles Gerät	Speicher: 32 GB vCPUs: 12	Speicher: 32 GB vCPUs: 12	Speicher: 32 GB vCPUs: 12
Device Manager-Datenbank	Extern: SQL Server Speicher: 16 GB vCPUs: 12	Extern: SQL Server Speicher: 32 GB vCPUs: 12	Extern: SQL Server Speicher: 32 GB vCPUs: 16

Active Directory	Speicher: 8 GB vCPUs: 4	Speicher: 16 GB vCPUs: 4	Speicher: 16 GB vCPUs: 4

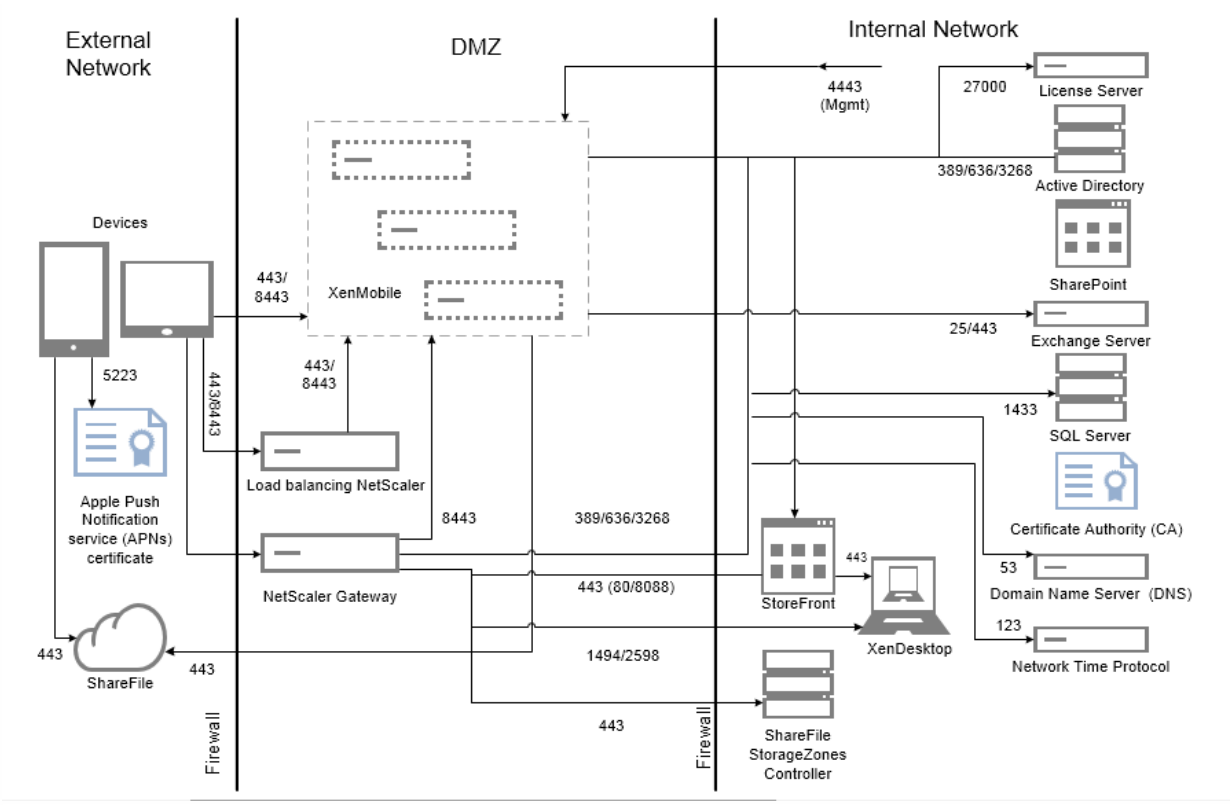




Die folgende Abbildung zeigt die Referenzarchitektur für eine kleine Bereitstellung. Es ist eine eigenständige Architektur für bis zu 10.000 Geräte.



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



Die Tests wurden an XenMobile Enterprise zur Benchmarkerstellung ausgeführt. Zum Testen sowohl kleiner und als auch großer Bereitstellungen wurden 1000 bis 100.000 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.

Benutzerarbeitslasten werden wie folgt definiert:

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.

Anmerkungen und Annahmen

Zur Einrichtung von XenMobile für über 30.000 Geräte müssen Sie folgende Serverparameter einstellen:

Config File - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/push_services.xml

-

Config File - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/ew-config.properties

- ios.mdm.apns.connectionPoolSize=15
- hibernate.c3p0.max_size=1000

Nehmen Sie diese Änderungen auf allen XenMobile-Knoten vor und starten Sie dann den Server neu.

Die folgenden Szenarios sind nicht Teil der Skalierbarkeitstests. Diese Szenarios werden ggf. für zukünftige Verbesserungen bei Skalierbarkeitstests einbezogen:

- Über Android verbundene Geräte werden nicht getestet.
- Die Paketbereitstellung wird nicht getestet.
- Die Windows-Plattform wird nicht getestet.

Jedes XenMobile unterstützt maximal 10.000 gleichzeitige Verbindungen.

Die Tests wurden unter idealen Bedingungen in einem LAN durchgeführt, um Netzwerklatenzprobleme außen vor zu halten. In einer Produktionsumgebung hängt die Skalierbarkeit auch von der für die Benutzer verfügbaren Bandbreite ab, insbesondere bei App-Downloads.

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) einschließlich Gerätestatusprüfungen
- Richtlinienbereitstellung per Push (iOS)
- Minimale WorxMail- und WorxWeb-Verbindungen (VPN-Tunnel): zwei Verbindungen
- Installation erforderlicher Apps über XenMobile

Die Arbeitslastparameter werden in der folgenden Tabelle definiert:

Geräte	Registrierte Geräte	Enumerationen	Enumerierte Apps pro Gerät	WorxStore-Starts pro Gerät	Web-/SaaS-SSO pro Gerät	MDX-App-Downloads pro Gerät	Erforderliche App-Downloads, ausgelöst über XenMobile-Server	Per Push bereitgestellte Richtlinien pro Gerät (iOS)
1000	1000	1000	14	4	4	2	2	2
10000	10000	10000	14	4	4	2	2	2

30000	30000	30000	14	4	4	2	2	2
60000	60000	60000	14	4	4	2	2	2
100000	100000	100000	14	4	4	2	2	2

Arbeitslast für vorhandene Benutzer mit ausschließlich Worx-Verbindungen

Die folgende Tabelle zeigt die Arbeitslast vorhandener Benutzer (mit ausschließlich Worx-Verbindungen). Diese Arbeitslast simulierte einen Benutzer mit WorxMail- und WorxWeb-Apps. Diese Simulation wurde zum Messen der NetScaler Gateway-Skalierbarkeit innerhalb der XenMobile-Konfiguration verwendet. Da nur die beiden Worx-Apps verwendet werden, ist die Last des Netzwerks minimal. Bei der WorxWeb-App greifen Benutzer auf interne Websites zu, die keinen XenMobile-Server-SSO auslösen. Dieser Modus umfasste folgende Vorgänge:

- Authentifizierung (NetScaler Gateway und XenMobile)
- WorxMail- und WorxWeb-Verbindungen (VPN-Tunnel): vier Verbindungen

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

Geräte	Enumerationen	Enumerierte Apps pro Gerät	VPN-Tunnel pro Gerät[1]
1000	1000	14	4
10000	10000	14	4
30000	30000	14	4
60000	60000	14	4
100000	100000	14	4

1. Die Anzahl der VPN-Tunnel entspricht WorxMail- und WorxWeb-Verbindungen.

Die Verbindungsprofile für WorxMail und WorxWeb werden in der folgenden Tabelle aufgeführt:

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)

Diese Empfehlungen basieren auf den WorxMail- und WorxWeb-Profilen, mit denen eine
mittlere Arbeitslast automatisiert wird. 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 für die Apps verwendeten Profile sollen eine "sehr hohe" Arbeitslast automatisieren. In den folgenden Tabellen sind die WorxMail- und WorxWeb-Profildetails dargestellt.

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

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.

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.

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

Komponente	Version
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0,824
Externe Datenbank	Microsoft SQL Server 2014

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

Anbieter	Genuine Intel
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).

Info über XenMobile Cloud

Jul 28, 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.

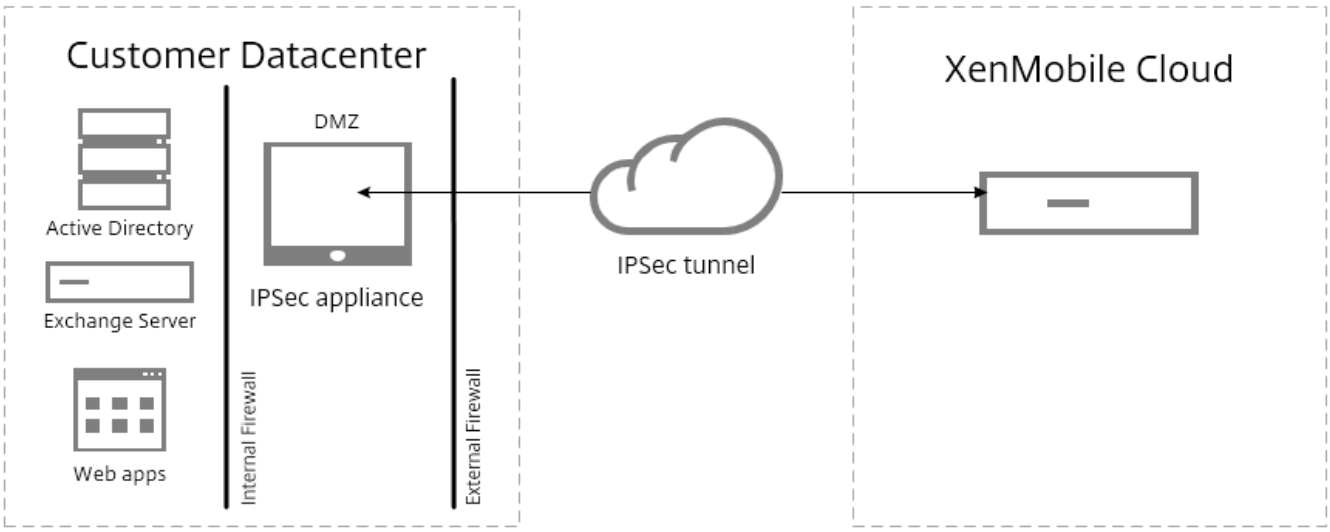
Cloud Operations-Administratoren kümmern sich um die Pflege und Konfiguration der Netzwerkkonnektivität und um die Integration von Citrix Produkten wie NetScaler, XenApp, XenDesktop, StoreFront und ShareFile. Die Cloud-Umgebung wird in weltweit verteilten Amazon-Datencentern gehostet, wodurch eine hohe 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 **Alle herunterladen**. Weitere Informationen finden Sie unter Anzeigen und Analysieren von Protokolldateien in XenMobile.

Die Abbildung unten zeigt die grundlegende Architektur von XenMobile Cloud. Detaillierte Architekturdiagramme finden Sie im Abschnitt "Reference Architecture for Cloud Deployments" des XenMobile-Bereitstellungshandbuchs.



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	ALLE	ALLE	IT-Verwaltung
Verwaltung	Geräte	ALL	IT-Verwaltung
Verwaltung	Registrierung	ALLE	IT-Verwaltung
Konfigurieren	Geräterichtlinien	ALLE	IT-Verwaltung
Konfigurieren	Apps	ALLE	IT-Verwaltung
Konfigurieren	Aktionen	ALLE	IT-Verwaltung
Konfigurieren	Bereitstellungsgruppen	ALLE	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	Network Access Control	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

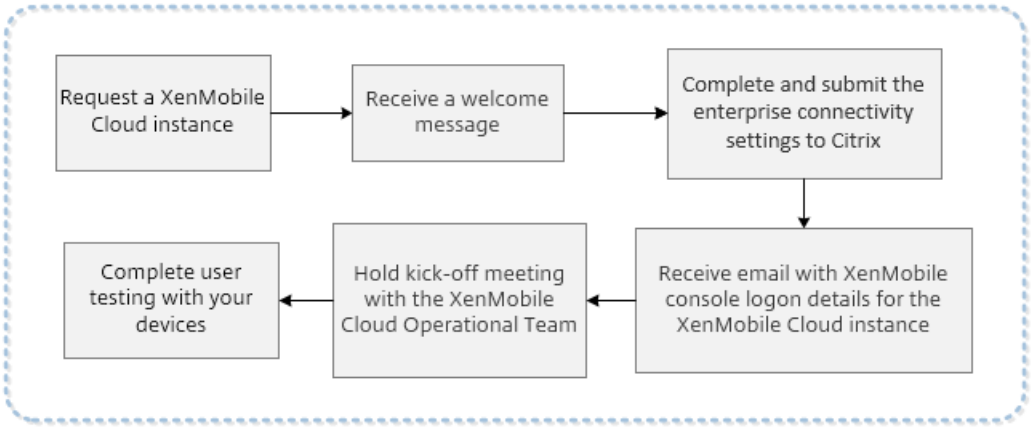
Schrittweise Anweisungen zum Anpassen von Rollen finden Sie unter Konfigurieren von Rollen mit RBAC.

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

Jul 28, 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 (AWS)-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.

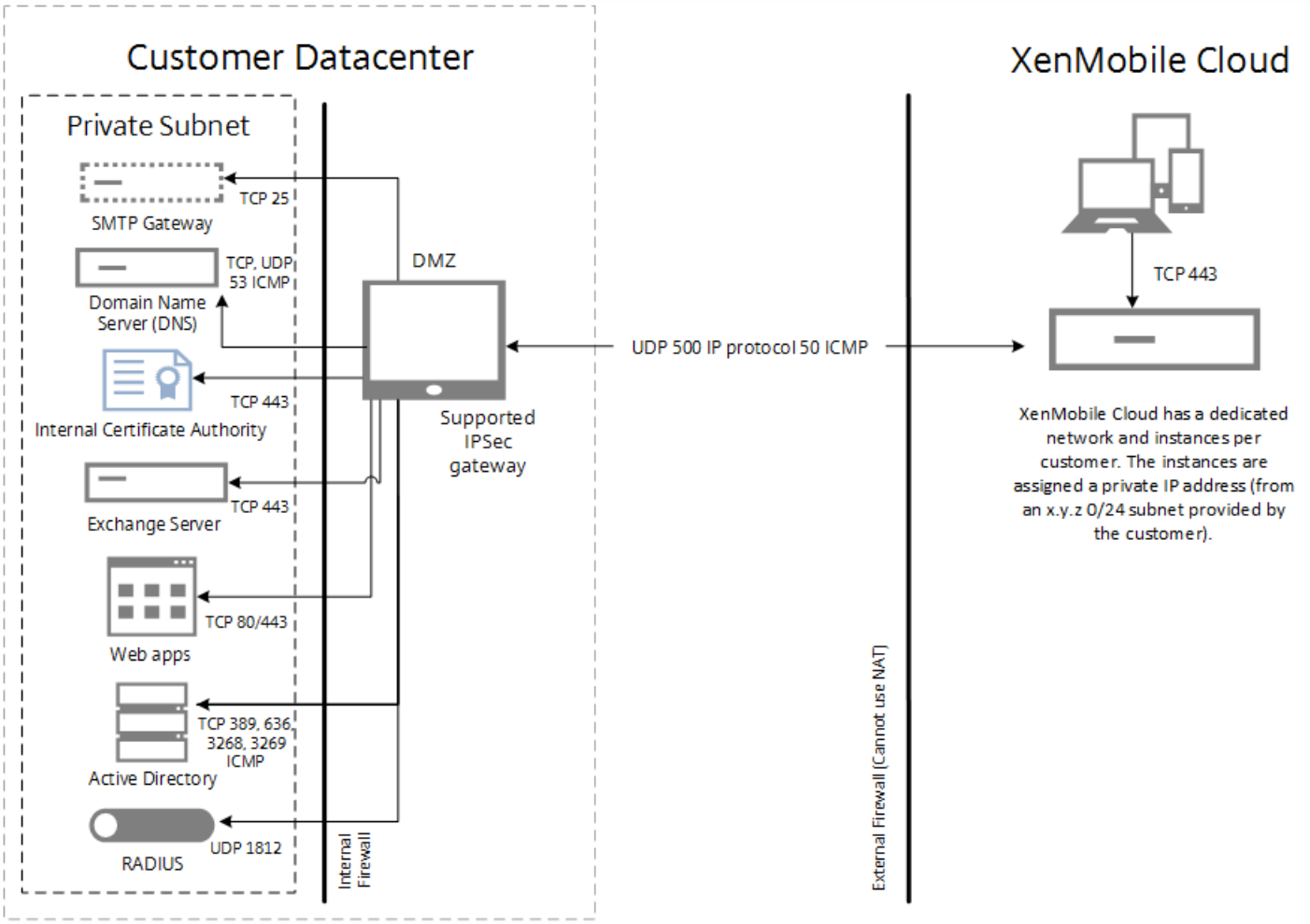
Ihr IPsec-Gateway benötigt eine direkt zugewiesene öffentliche IP-Adresse, für die keine Netzwerkadressübersetzung

(NAT) verwendet werden darf.

Ihre AWS-VPN-Verbindung erfordert permanentes Keep-Alive, das von der Kundenseite initiiert wird. Konfigurieren Sie einen permanenten Ping von Ihrer Umgebung zum Amazon VPC-Subnetz, um die Dienstkontinuität sicherzustellen.

Mehrere auf dem IPsec-Gateway konfigurierte Sicherheitszuordnungen werden von Ihrer AWS-VPN-Verbindung nicht unterstützt. Nur ein eindeutiges Sicherheitszuordnungspaar (ein eingehendes und ein ausgehendes) ist pro Tunnel zulässig. Konsolidieren Sie die Regeln und Filter, damit unerwünschter Datenverkehr nicht zugelassen wird.

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-	IPSec-Gerät des Kunden	UPD	500	IPSec-IKE-Konfiguration

Adressen von XenMobile Cloud (AWS) IPSec-VPN [1]				
Öffentliche IP-Adressen von XenMobile Cloud (AWS) IPSec-VPN [1]	IPSec-Gerät des Kunden	IP-Protokoll-ID	50	IPSec-ESP-Protokoll
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-	RADIUS-Server	UDP	1812	Optional (nicht in XenMobile-POCs verwendet):

Kundensubnetz [2]				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. Einzelheiten 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

Jul 28, 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.

- 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.

- 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.

- 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 10.3 gelten die folgenden Mindestanforderungen:

- Eines der Folgenden:
  - XenServer (unterstützte Versionen: 6.5.x und 6.2.x); weitere Details finden Sie unter XenServer
  - VMware (unterstützte Versionen: ESXi 5.1, ESXi 5.5 oder ESXi 6.0); weitere Informationen finden Sie unter VMware. ESXi 6.0 wird nur unter XenMobile 10.3.x unterstützt.
  - 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
- 4 virtuelle CPUs
- 8 GB RAM
- 50 GB Speicherplatz auf der Festplatte

Empfohlene Konfiguration für 10.000+ Geräte:

- Vierkernprozessor mit 8 GB RAM für jeden Knoten

XenMobile Version 10.3.x erfordert den Citrix Lizenzserver 11.12.1 oder höher.

Systemanforderungen für NetScaler Gateway

Für die Ausführung von NetScaler Gateway mit XenMobile 10.3 gelten die folgenden Mindestanforderungen:

- Eines der Folgenden:
  - XenServer (unterstützte Versionen: 6.2.x, 6.1.x oder 6.0.x)
  - VMWare (unterstützte Versionen: ESXi 4.1, ESXi 5.1, ESXi 5.5, ESXi 6.0)
  - Hyper-V (unterstützte Versionen: Windows Server 2008 R2, Windows Server 2012 und Windows Server 2012 R2)
- 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 10.3-Datenbankanforderungen

Für XenMobile ist eine der folgenden Datenbanken erforderlich:

- Microsoft SQL Server

  Das XenMobile-Repository unterstützt eine Microsoft SQL Server-Datenbank mit einer der folgenden unterstützten Versionen (weitere Informationen zu Microsoft SQL Server-Datenbanken finden Sie unter Microsoft SQL Server):

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

XenMobile 10.1 unterstützt SQL Server AlwaysOn-Verfügbarkeitsgruppen.

Citrix empfiehlt die Remote-Verwendung von Microsoft SQL.

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 Liste **Andere Versionen** aus):

Serverkonfiguration – Dienstkonten

Konfigurieren von Windows-Dienstkonten und -Berechtigungen

Rollen auf Serverebene

- PostgreSQL

  PostgreSQL wird mit XenMobile ausgeliefert. Sie können es lokal oder remote verwenden.

  Hinweis: Alle XenMobile-Editionen unterstützen Remote PostgreSQL 9.3.11 für Windows mit den folgenden Einschränkungen:

  - Unterstützung für bis zu 300 Geräte

    Verwenden Sie einen lokalen SQL Server für mehr als 300 Geräte.

  - Keine Unterstützung für Clustering

StoreFront-Kompatibilität

StoreFront 3.6
StoreFront 3.5
StoreFront 3.0
StoreFront 2.6
Webinterface 5.4
XenApp und XenDesktop 7.9
XenApp und XenDesktop 7.8
XenApp und XenDesktop 7.7
XenApp und XenDesktop 7.6
XenApp und XenDesktop 7.5
XenApp 6.5

XenMobile 10.3 – E-Mail-Serveranforderungen

XenMobile 10.3 unterstützt die folgenden E-Mail-Server:

- Exchange 2016
- Exchange 2013
- Exchange 2010

XenMobile-Kompatibilität

Jul 28, 2016

Eine Zusammenfassung integrierbarer XenMobile-Komponenten finden Sie unter XenMobile-Kompatibilität.

Unterstützte Geräteplattformen

Jul 28, 2016

Sie finden die vollständige Liste der Geräte, die XenMobile 10.x für Enterprise Mobility Management unterstützt, in Unterstützte Geräteplattformen in XenMobile.

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
389	Wird für unsichere LDAP-Verbindungen verwendet.	XenMobile	LDAP-Authentifizierungsserver oder Active Directory

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 Android- und Windows-Geräte, die XenMobile-Webkonsole und den MDM-Client für Remotesupport verwendet.	Internes 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)
8081	Wird für die App-Tunnel des optionalen MDM-Remotesupportclients verwendet. Standardwert: 8081.	Remotesupportclient	Internet, für App-Tunnel zu Benutzergeräten (nur Android und Windows)
8443	Für die Registrierung von iOS- und Windows Phone-Geräten.	Internet LAN und WiFi	XenMobile

Portanforderungen für die Verbindung mit Auto Discovery Service

Diese Portkonfiguration gewährleistet, dass auf Android-Geräten mit Worx Home für Android 10.2 und 10.3 über das interne Netzwerk auf den 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-Konformität

Jul 28, 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

Oct 13, 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. Weitere Informationen zum Globalisierungssupport für alle Citrix Produkte finden Sie in http://support.citrix.com/article/CTX119253.

Sprachunterstützung für mobile Worx-Apps

Ein X bedeutet, dass die App in der Sprache verfügbar ist. Secure Forms ist derzeit nur in Englisch verfügbar.

iOS						
	Worx Home	**WorxMail**	**WorxWeb**	**WorxNotes**	**WorxTasks**	**QuickEdit**
Japanisch	X	X	X	X	X	X
Vereinfachtes Chinesisch	X	X	X	X	X	X
Traditionelles Chinesisch	X	X	X	X	X	X
Französisch	X	X	X	X	X	X
Deutsch	X	X	X	X	X	X
Spanisch	X	X	X	X	X	X
Koreanisch	X	X	X	X	X	X
Portugiesisch	X	X	X	X	X	X
Niederländisch	X	X	X	X	X	X
Italienisch	X	X	X	X	X	X
Dänisch	X	X	X	X	X	X

Schwedisch	X	X	X	X	X	X
Hebräisch	X	X	X	X	X	X
Arabisch	X	X	X	X	X	X

Android						
	Worx Home	**WorxMail**	**WorxWeb**	**WorxNotes**	**WorxTasks**	**QuickEdit**
Japanisch	X	X	X	X	X	X
Vereinfachtes Chinesisch	X	X	X	X	X	X
Traditionelles Chinesisch	X	X	X	X	X	
Französisch	X	X	X	X	X	X
Deutsch	X	X	X	X	X	X
Spanisch	X	X	X	X	X	X
Koreanisch	X	X	X	X	X	X
Portugiesisch	X	X	X	X	X	X
Niederländisch	X	X	X	X	X	X
Italienisch	X	X	X	X	X	X
Dänisch	X	X	X	X	X	X
Schwedisch	X	X	X	X	X	X

Hebräisch	X	X	X	X	X	
Arabisch	X	X	X	X	X	

Windows			
	Worx Home	**WorxMail**	**WorxWeb**
Französisch	X	X	X
Deutsch	X	X	X
Spanisch	X	X	X
Italienisch	X	X	X
Dänisch	X	X	X
Schwedisch	X	X	X

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

Sprachunterstützung für die XenMobile-Konsole

Die XenMobile-Konsole ist in vereinfachtem Chinesisch, Deutsch, Französisch, Koreanisch und Portugiesisch verfügbar.

Unterstützung für Right-to-Left

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

Jul 28, 2016

Diese Checkliste enthält die Voraussetzungen und Einstellungen für die Installation von XenMobile. 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 Ein 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 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	

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 10.3 und Installationscheckliste für XenMobile.

> ## Hinweis
>
> Stellen Sie sicher, dass der Hypervisor mit der richtigen Uhrzeit konfiguriert ist, da diese von XenMobile verwendet wird. Verwenden Sie hierfür einen NTP-Server oder eine manuelle Konfiguration.

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.
- - Löschen Sie die Datei Virtual Machines/.xml.
  - Verschieben Sie die Datei Legacy/.exp in "Virtual Machines".

Wenn Sie Windows Server 2008 R2 oder Windows Server 2012 installieren, führen Sie folgende Schritte aus:

Diese Schritte sind erforderlich, da es zwei Versionen der Hyper-V-Manifestdatei für die VM-Konfiguration gibt (.exp und .xml). Windows Server 2008 R2 und Windows Server 2012 unterstützen nur .exp. Für diese Releases müssen Sie vor der Installation sicherstellen, dass nur die nur die EXP-Manifestdatei vorliegt.

Windows Server 2012 R2 erfordert die zusätzlichen Schritte nicht.

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.

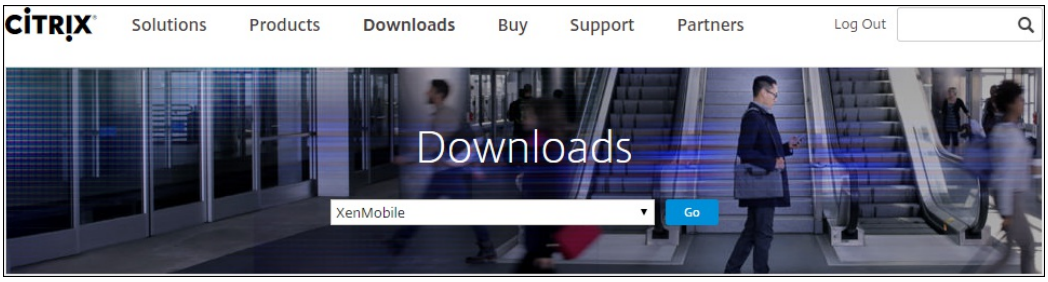
Download der XenMobile-Produktsoftware

Sie können Produktsoftware von der Citrix Website herunterladen. Melden Sie sich an der Site an und navigieren Sie über

den Link Downloads auf der Citrix Webseite zu der Seite mit der Software, die Sie herunterladen möchten.

Herunterladen der Software für XenMobile

1. Gehen Sie zur Citrix Website.
2. Klicken Sie neben dem Suchfeld auf Log On und melden Sie sich mit Ihrem Konto an.
3. Klicken Sie auf die Registerkarte Downloads.
4. Klicken Sie auf der Seite Downloads in der Liste für die Produktauswahl auf XenMobile.



5. Klicken Sie auf Go. Die Seite XenMobile wird angezeigt.
6. Erweitern Sie XenMobile 10.
7. Klicken Sie auf XenMobile 10.0 Server.
8. Klicken Sie auf der Seite XenMobile 10.0 Server für das gewünschte virtuelle Image (XenServer, VMware oder Hyper-V) auf Download, um XenMobile zu installieren.
9. Folgen Sie den Anweisungen auf dem Bildschirm, um die Software herunterzuladen.

Herunterladen der Software für NetScaler Gateway

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. Wenn Sie nicht bereits bei der Citrix Website angemeldet sind,klicken Sie neben dem Feld zum Suchen auf Anmelden und melden Sie sich mit Ihrem Konto an.
3. Klicken Sie auf die Registerkarte Downloads.
4. Klicken Sie auf der Seite Downloads in der Liste für die Produktauswahl auf NetScaler Gateway.
5. Klicken Sie auf Go. Die Seite NetScaler Gateway wird angezeigt.
6. Erweitern Sie auf der Seite NetScaler Gateway die Version von NetScaler Gateway, die Sie ausführen.
7. Klicken Sie unter Firmware auf die Gerätesoftwareversion, die Sie herunterladen möchten.
   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.
8. Klicken Sie auf die Gerätesoftwareversion, die Sie herunterladen möchten.
9. Klicken Sie auf der Gerätesoftwareseite für die Version, die Sie herunterladen möchten, auf Download für das gewünschte virtuelle Gerät.
10. Folgen Sie den Anweisungen auf dem Bildschirm, um die Software herunterzuladen.

Konfigurieren von XenMobile für die Erstverwendung

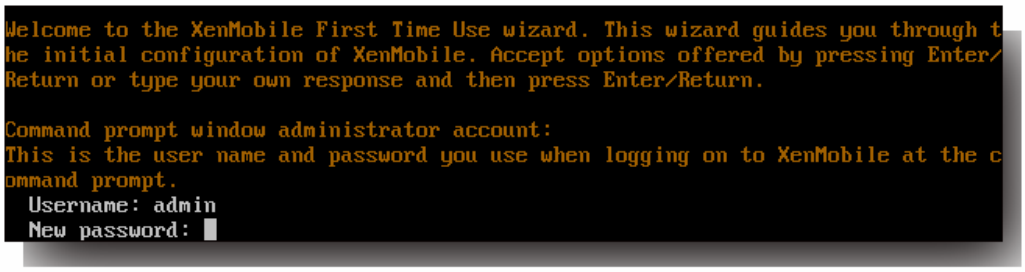
Die anfängliche Konfiguration von XenMobile ist ein zweiteiliger Prozess.

1. Konfigurieren von IP-Adresse, Subnetzmaske, Standardgateway, DNS-Server usw. für XenMobile über die XenCenter- oder vSphere-Befehlszeilenkonsole
2. Anmelden bei der XenMobile-Verwaltungskonsole an und befolgen der 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. Geben Sie dazu den Administratorbenutzernamen und das Administratorkennwort ein.
   Wichtig:
   Wenn Sie Kennwörter für das Administratorkonto an der Eingabeaufforderung, für Public Key-Infrastruktur-Serverzertifikate und FIPS erstellen oder ändern, erzwingt XenMobile die folgenden Regeln für alle Benutzer außer Active Directory-Benutzer, deren Kennwörter außerhalb von XenMobile verwaltet werden:
   - Das Kennwort muss mindestens 8 Zeichen lang sein und es muss mindestens drei der folgenden Komplexitätskriterien erfüllen:
     - Großbuchstaben (A bis Z)
     - Kleinbuchstaben (a bis z)
     - Ziffern (0 bis 9)
     - Sonderzeichen (z. B. !, #, $, %)

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

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

5. Sekundärer DNS-Server (optional)

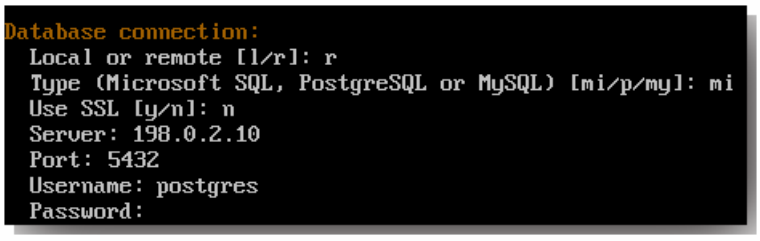
Hinweis: Die abgebildeten Adressen sind nicht funktionsfähig und dienen nur als Beispiel.

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

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

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

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



1. Sie können eine lokale oder remote Datenbank verwenden. Eingabel für lokal oderr für remote ein.
2. Wählen Sie den Datenbanktyp. Eingabemi für Microsoft SQL oderp für PostgreSQL ein.
   Wichtig:
   - Citrix empfiehlt die Remote-Verwendung von Microsoft SQL. PostgreSQL ist Teil von XenMobile und sollte lokal

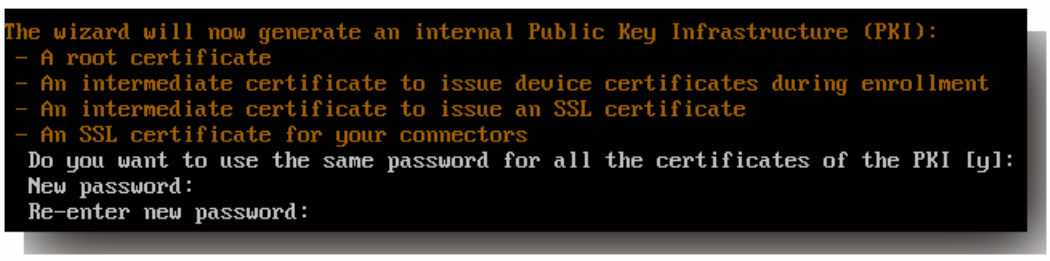
oder remote nur in Testumgebungen verwendet werden.
- Eine Datenbankmigration wird nicht unterstützt. In einer Testumgebung erstellte Datenbanken können nicht in eine Produktionsumgebung übertragen werden.

3. Optional können Siey eingeben, damit SSL-Authentifizierung für die Datenbank verwendet wird.
4. Geben Sie den vollqualifizierten Domänennamen (FQDN) des Servers ein, auf dem XenMobile gehostet wird. Dieser Hostserver wird sowohl für die Geräteverwaltung als auch für die App-Verwaltung verwendet.
5. Geben Sie Ihre Datenbankportnummer ein, wenn sie sich von der Standardportnummer unterscheidet. Der Standardport für Microsoft SQL ist 1433 und der Standardport für PostgreSQL ist 5432.
6. Geben Sie den Benutzernamen für den Datenbankadministrator ein.
7. Geben Sie das Kennwort des Datenbankadministrators ein.
8. Geben Sie den Namen der Datenbank ein.
9. Drücken Sie die Eingabetaste, um die Datenbankeinstellungen zu übernehmen.

8. Optional können Siey eingeben, um das Clustering von XenMobile-Knoten oder Instanzen zu aktivieren.
   Wichtig: Wenn Sie einen XenMobile-Cluster aktivieren, öffnen Sie nach der Systemkonfiguration Port 80, um die Echtzeitkommunikation zwischen Clustermitgliedern zu aktivieren. Dieser Vorgang muss auf allen Clusterknoten ausgeführt werden.
9. Geben Sie den vollqualifizierten Domänennamen (FQDN) des XenMobile-Servers ein.

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

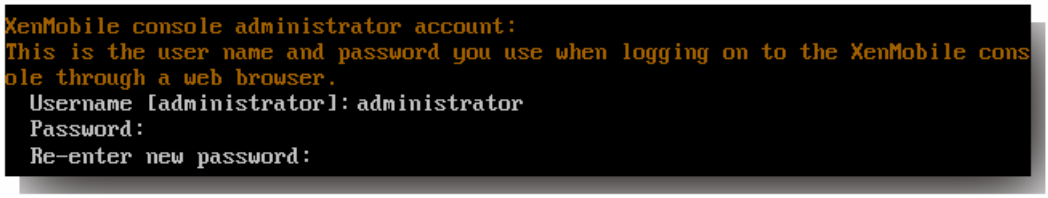
12. Überspringen Sie die nächste Frage zum Upgrade von einem vorherigen XenMobile-Release, da Sie XenMobile zum ersten Mal installieren.
13. Eingabey ein, wenn Sie dasselbe Kennwort für alle Public Key-Infrastruktur-Zertifikate verwenden möchten. Informationen zum XenMobile PKI-Feature finden Sie unter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



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

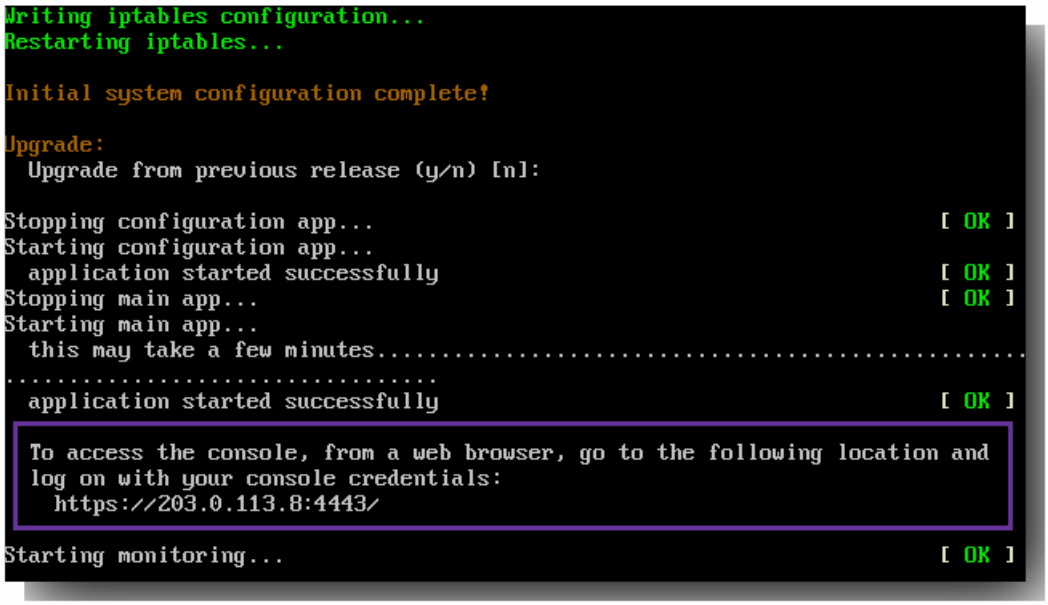
14. Geben Sie das neue Kennwort ein und geben Sie dann das neue Kennwort zur Bestätigung erneut ein.
    Hinweis: Bei der Eingabe des neuen Kennworts werden keine Zeichen (Sternchen o. Ä.) angezeigt. Es wird nichts angezeigt.

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



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

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

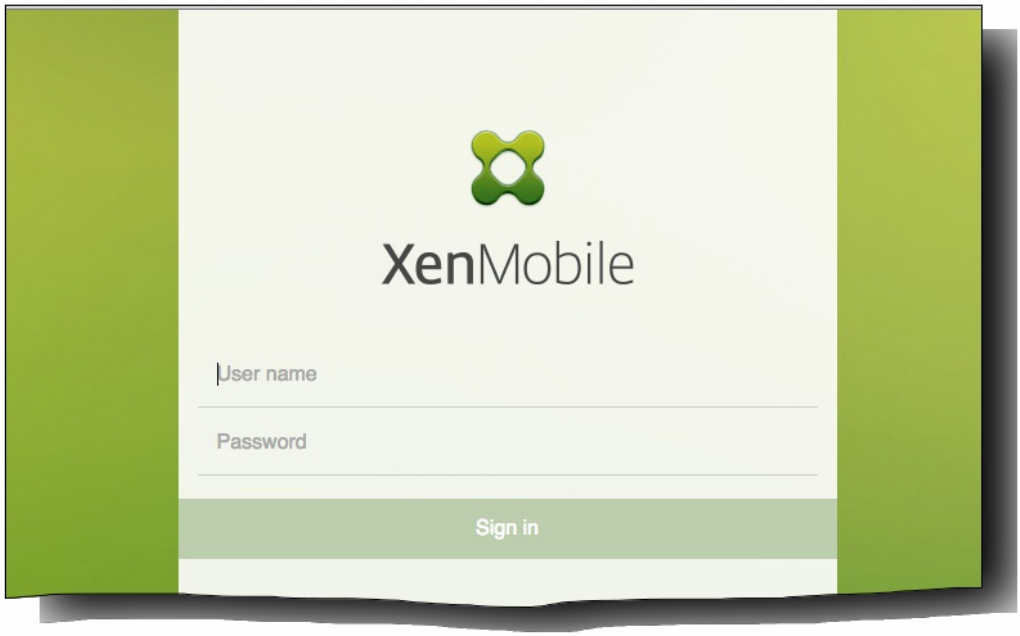


Konfigurieren von XenMobile in einem Webbrowser

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 mithilfe von XenMobile-Clustering 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: Dieser Schritt erfordert den Neustart des Servers.
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.
   - 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

Jul 28, 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.

Aktualisieren von XenMobile

Oct 13, 2016

Sobald eine neue Version oder ein wichtiges Update für XenMobile verfügbar wird, wird sie bzw. es auf Citrix.com veröffentlicht und eine Meldung an die als Kontaktperson verzeichnete Person bei den Kunden gesendet. Es gibt drei Optionen für das Upgrade von XenMobile, die davon abhängen, welche Version Sie zurzeit verwenden:

- **Upgrade von XenMobile 9.0** MDM Edition, App Edition und Enterprise Edition
  Sie müssen zunächst mit dem Upgrade Tool ein Upgrade auf XenMobile 10.1 durchführen. Sie können das Tool unter Citrix.com von der Seite "Downloads" herunterladen. Weitere Informationen zum Upgrade Tool finden Sie unter Aktualisieren von XenMobile.

  Mit der aktuellen Version des Upgrade Tools können Sie jetzt die Daten der folgenden Gerätetypen migrieren, wenn Sie ein Upgrade von XenMobile 9 auf XenMobile 10.1 durchführen und dann ein Update auf XenMobile 10.3.x installieren:

  Windows CE
  Windows 10 Phone
  Windows 10 Tablet

  Wenn in der aktuellen Version des Upgrade Tools die Multi-Tenant Console (MTC) unter XenMobile 9.0 aktiviert ist, können Sie mit der MTC verwaltete XenMobile 9-Instanzen zu eigenständigen XenMobile 10-Instanzen migrieren. XenMobile 10 unterstützt die Multi-Tenant Console nicht, daher müssen Sie die aktualisierten Instanzen individuell verwalten. Weitere Informationen finden Sie unter Aktualisieren des MTC-Mandantenservers auf XenMobile 10.1.

- **Upgrade von XenMobile 10.1 auf XenMobile 10.3.x**
  Verwenden Sie die Seite **Releasemanagement** in der XenMobile-Konsole wie in diesem Artikel beschrieben. Das Upgrade Tool wird zum Installieren von XenMobile 10.3.x nicht verwendet.

- **Installieren neuer Versionen von Software, Service Packs und Systempatches für XenMobile 10.3.x**
  Verwenden Sie die Seite **Releasemanagement** in der XenMobile-Konsole wie in diesem Artikel beschrieben.

Important

- Wenn der WorxStore einen benutzerdefinierten Namen hat und XenMobile 10.1 auf Version 10.3.x aktualisiert wird, müssen Sie vor dem Update den Namen des Stores auf die Standardeinstellung **Store** ändern und diese Einstellung auf Geräten bereitstellen. Andernfalls verursacht der benutzerdefinierte Storename Probleme bei der XenMobile 10.3-Registrierung, beim Zugriff auf Worx Home und den WorxStore sowie bei der App-Bereitstellung auf iOS-Geräten. Weitere Informationen zur Konfiguration von WorxStore-Branding finden Sie unter Erstellen von angepasstem Worx Store-Branding für iOS-Geräte.
- Wenn Sie nach dem Upgrade auf XenMobile 10.3.x die mobilen Worx-Apps in XenMobile 10.3.x aktualisieren, die Sie in einer früheren Version konfiguriert haben, werden die App-Einstellungen nicht mehr in der XenMobile-Konsole angezeigt. Sie müssen die Einstellungen für diese Apps erneut bearbeiten und konfigurieren. Die Apps müssen nicht neu installiert werden. Diesen Schritt brauchen Sie nur einmal auszuführen. Die Werte bleiben bei zukünftigen Updates erhalten, wenn Sie die App oder den Server aktualisieren.

Upgradepfad - Zusammenfassung

XenMobile Server-Version	Releasenummer	Upgrade auf	Releasenummer	Upgradepfad	Speicherort
XenMobile Server 9 mit App Controller Patch 5	9.0.0.97582	XenMobile Server 10.1	10.1.0.63030	XenMobile Server 9 auf XenMobile Server 10.1	Download (App Controller Patch 5 und Upgrade Tool)
XenMobile Server 10 oder 10.1	10.1.0.63030	XenMobile Server 10.3	10.3.0.824	XenMobile Server 10 oder 10.1 Upgrade auf 10.3	Download
XenMobile Server 10.3	10.3.0.10004, 10.3.0.10008, 10.3.0.10010, 10.3.0.10014, 10.3.0.10016, 10.3.0.10032, 10.3.0.10036	XenMobile Server 10.3 Rollup Patch 3	10.3.0.10048	XenMobile Server 10.3 Upgrade auf 10.3 Rolling Patch 3	Download
XenMobile Server 10.3	10.3.0.x	XenMobile Server 10.3.5	10.3.5.354	XenMobile Server 10.3 Upgrade auf 10.3.5	Download
XenMobile Server 10.3.5	10.3.5.354	XenMobile Server 10.3.6 (Service Pack)	10.3.6.310	XenMobile Server 10.3.5 Upgrade auf 10.3.6	Download

Upgrade von XenMobile 10.1 oder von XenMobile 10.3.x

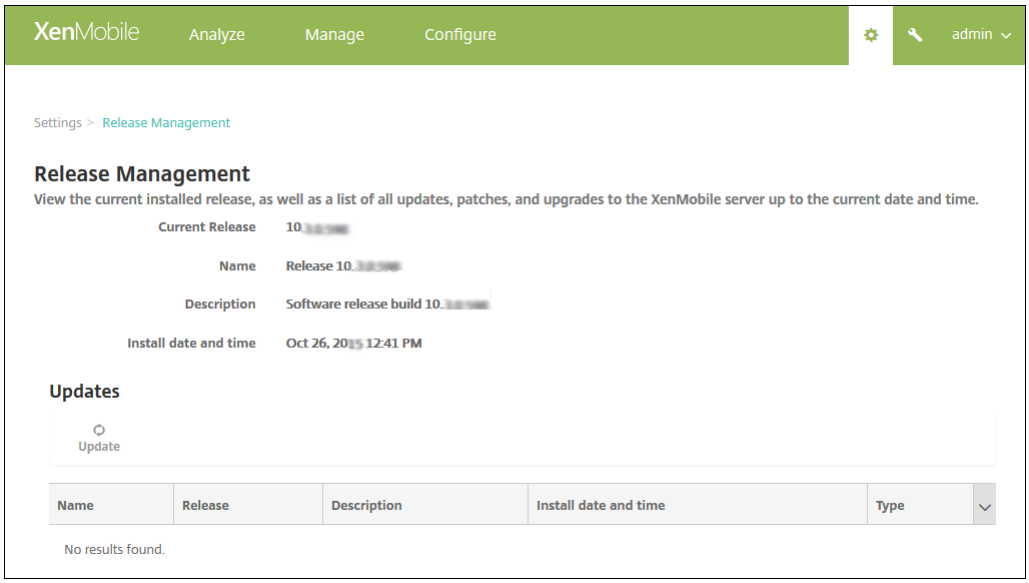
Voraussetzungen:

- Vor der Installation eines XenMobile-Updates verwenden Sie die Funktionen der virtuellen Maschine (VM) zum Erstellen eines Systemsnapshots.
- Sichern Sie die Konfigurationsdatenbank des Systems.
- Überprüfen Sie die Systemanforderungen für die Version, auf die Sie aktualisieren. Informationen für XenMobile 10.3 finden Sie unter Systemanforderungen.

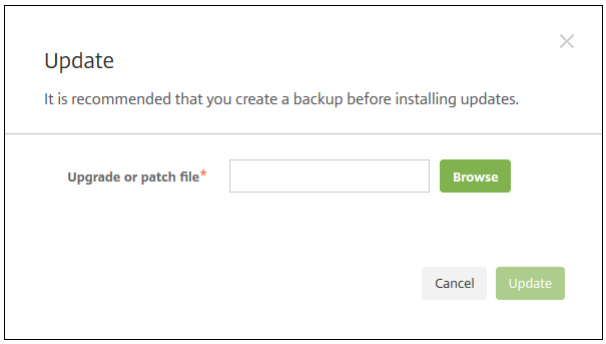
1. Melden Sie sich mit Ihrem Konto auf der Citrix Website an und laden Sie die XenMobile-Upgradedatei (.bin) an einen geeigneten Speicherort herunter.

2. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

3. Klicken Sie auf **Releasemanagement**. Die Seite **Releasemanagement** wird angezeigt.



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



4. Klicken Sie auf **Durchsuchen**, navigieren Sie zum Speicherort der von Citrix.com heruntergeladenen XenMobile-Upgradedatei und wählen Sie sie 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. Leeren Sie den Browsercache nach dem Neustart des Systems.

Wichtig: Wenn das System im Clustermodus konfiguriert ist, führen Sie die folgenden Schritte aus, um jeden Knoten zu aktualisieren:

1. Laden Sie die BIN-Datei von **Einstellungen** > **Releasemanagement** auf allen Knoten hoch.

2. Fahren Sie alle Knoten über **Einstellungen** in der Befehlszeilenschnittstelle herunter.

3. Starten Sie einen Knoten und prüfen Sie, ob der Dienst ausgeführt wird.

4. Starten Sie die anderen Knoten einen nach dem anderen.

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.

4. Klicken Sie auf "Durchsuchen", 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 e

Wichtig: Wenn das System im Clustermodus konfiguriert ist, führen Sie die folgenden Schritte aus, um jeden Knoten zu aktualisieren:

1. Fahren Sie alle Knoten bis auf einen herunter.
2. Aktualisieren Sie den Knoten.
3. 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.

4. Klicken Sie auf "Durchsuchen", 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 e

Wichtig: Wenn das System im Clustermodus konfiguriert ist, führen Sie die folgenden Schritte aus, um jeden Knoten zu aktualisieren:

1. Fahren Sie alle Knoten bis auf einen herunter.
2. Aktualisieren Sie den Knoten.
3. 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.

Unterstützung für benannte SQL-Instanzen

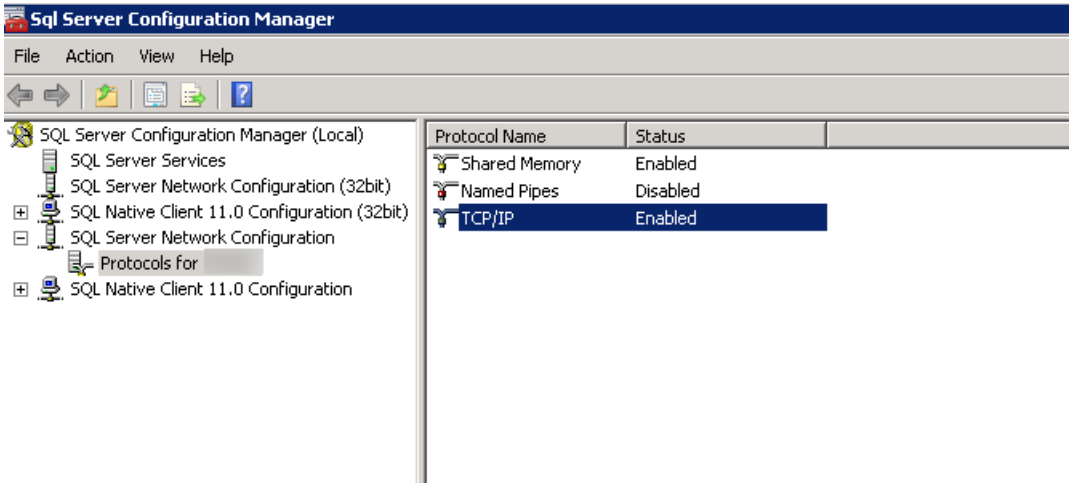
Jul 28, 2016

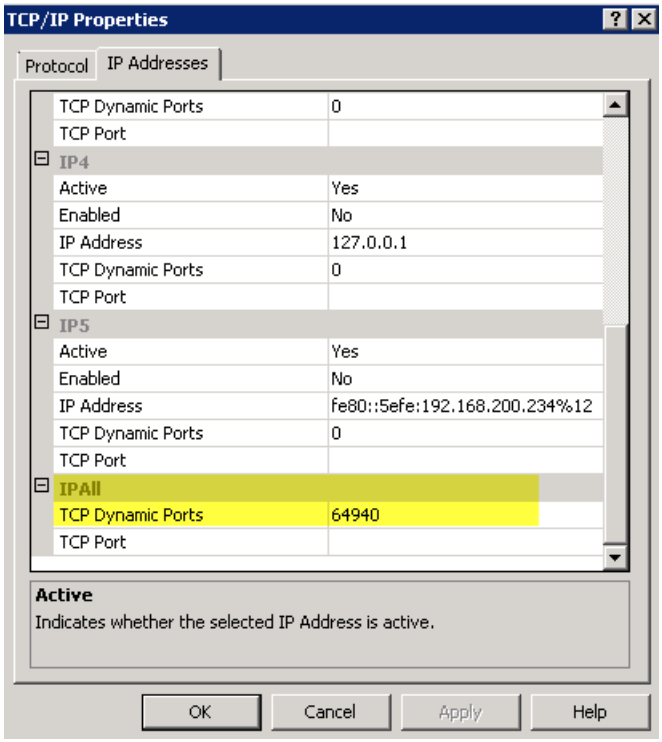
Mit dem Upgrade Tool können Sie Upgrades von XenMobile 9 auf XenMobile 10 und von XenMobile 9 auf XenMobile 10.1 durchführen. Wenn Ihr XenMobile 9-Setup auf benannten SQL-Instanzen basiert, müssen Sie bestimmten Schritten folgen. Wenn Ihre XenMobile 9-Umgebung die folgenden Voraussetzungen erfüllt, folgen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

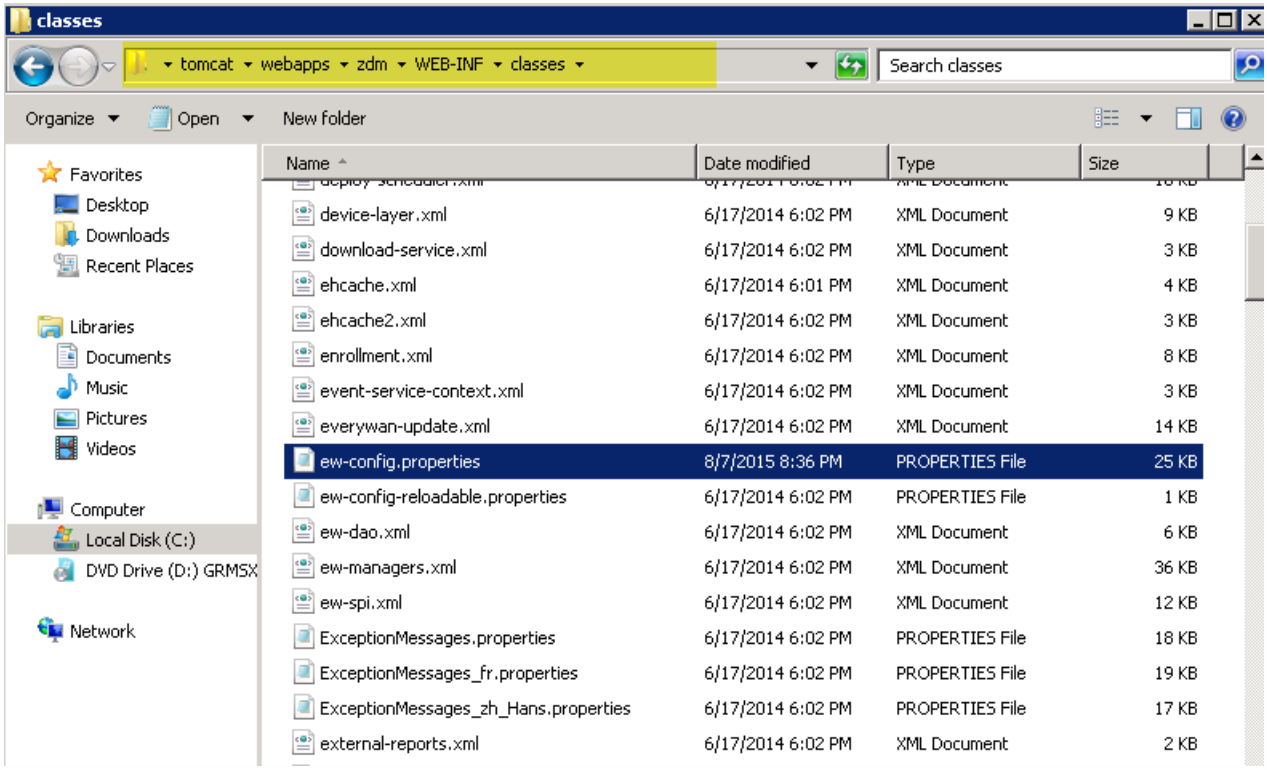
Citrix empfiehlt, die SQL Server-Datenbankinstanz immer auf einem statischen Port auszuführen, weil der XenMobile-Server kontinuierlichen Zugriff auf die Datenbank benötigt. Diese Verbindung erfolgt im Allgemeinen durch eine Firewall. Sie müssen daher den entsprechenden Port in der Firewall öffnen und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

ew-config.properties

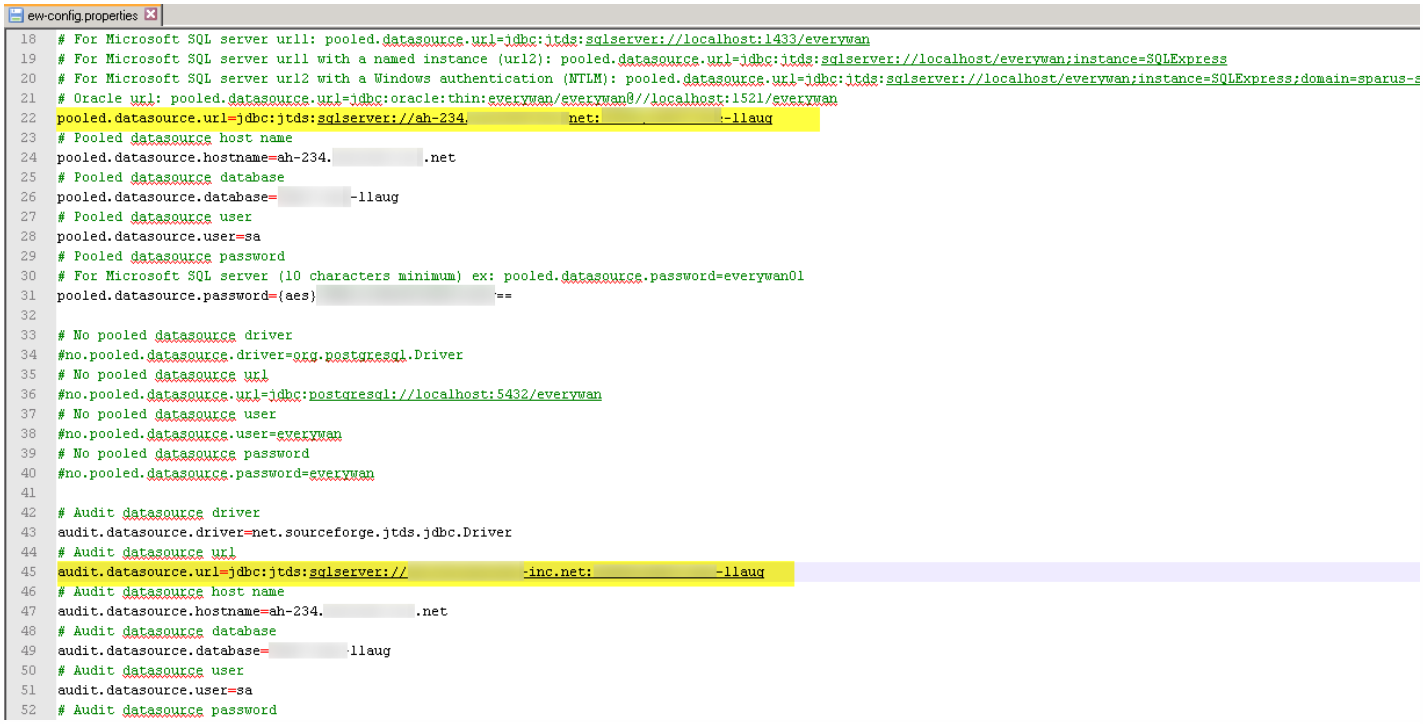
```
# For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
# For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
# For Microsoft SQL server url2 with a Windows authentication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

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

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

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.

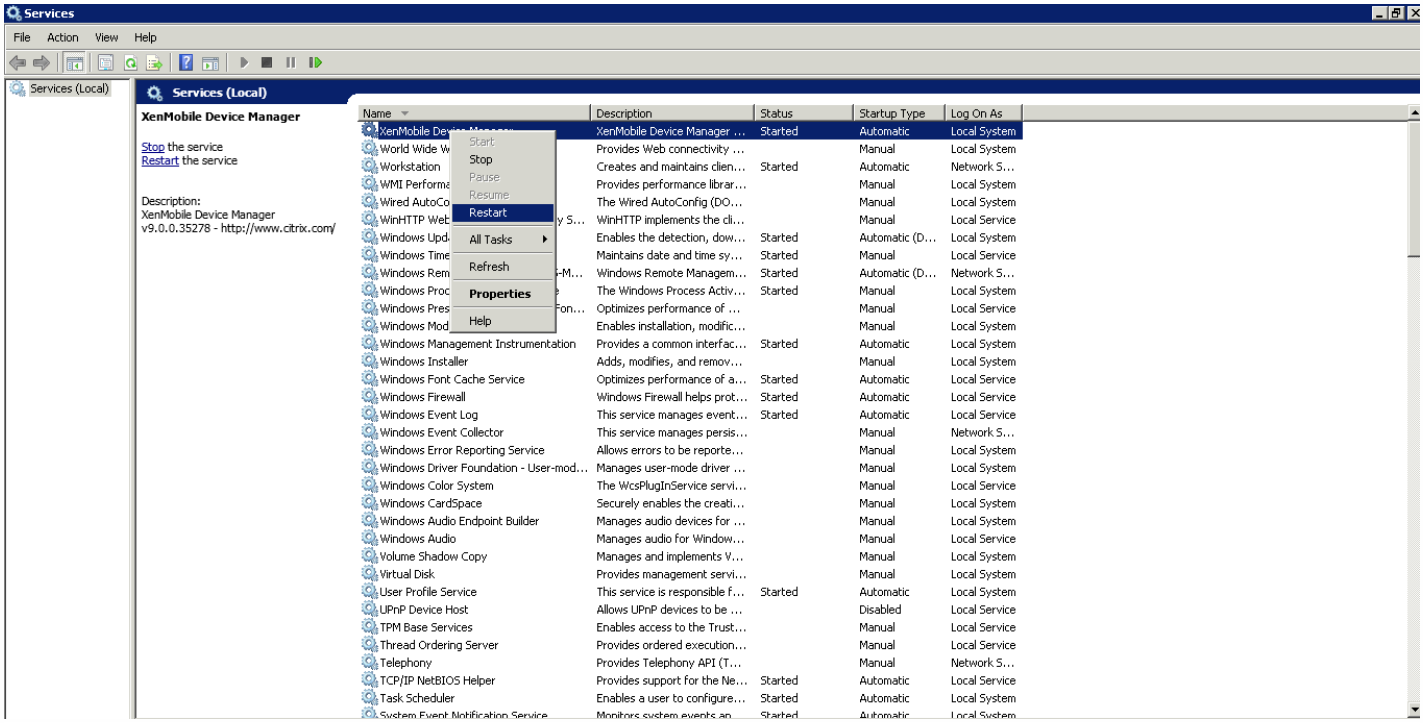
pooled.datasource.url=jdbc:jtds:sqlserver:// :64940/

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

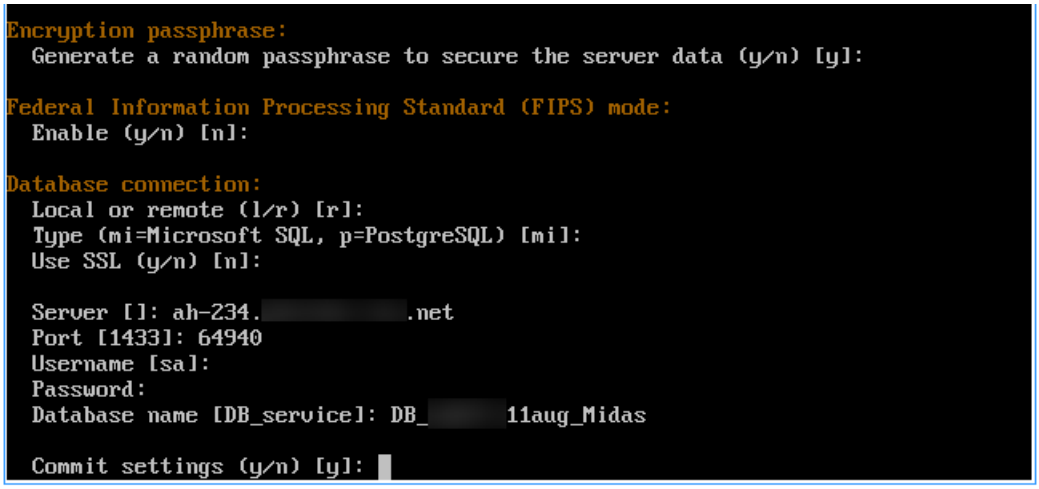
> ## Hinweis
>
> Citrix empfiehlt, eine Datensicherung durchzuführen, eine Kopie zu erstellen oder genau aufzuschreiben, welche Änderungen Sie in der Datei ew-config.properties vornehmen. Diese Informationen sind nützlich, falls ein Fehler bei der Migration auftritt.



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. Führen Sie für weitere Upgrades Ihrer XenMobile-Umgebung die folgenden Schritte aus:

Für das Upgrade von XenMobile 9.0 (MDM Edition, App Edition und Enterprise Edition) auf XenMobile 10.1 verwenden Sie das Upgrade Tool. Das Upgrade Tool können Sie von der Seite Citrix.com downloads herunterladen. Weitere Informationen finden Sie unter Aktualisieren von XenMobile.

Konfigurieren von Clustering für XenMobile 10

Jul 28, 2016

In XenMobile-Versionen vor 10 wurden Device Manager als Cluster und App Controller als hochverfügbares Paar konfiguriert. In XenMobile 10 wurden Device Manager und App Controller aus XenMobile 9 integriert. Ab Version 10 ist hohe Verfügbarkeit in XenMobile kein Thema mehr. Um Clustering 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.
- Eine öffentliche IP-Adresse für MDM L-Band und eine private IP-Adresse für MAM.
- Serverzertifikate
- Sie haben eine freie IP für die virtuelle IP-Adresse von NetScaler.

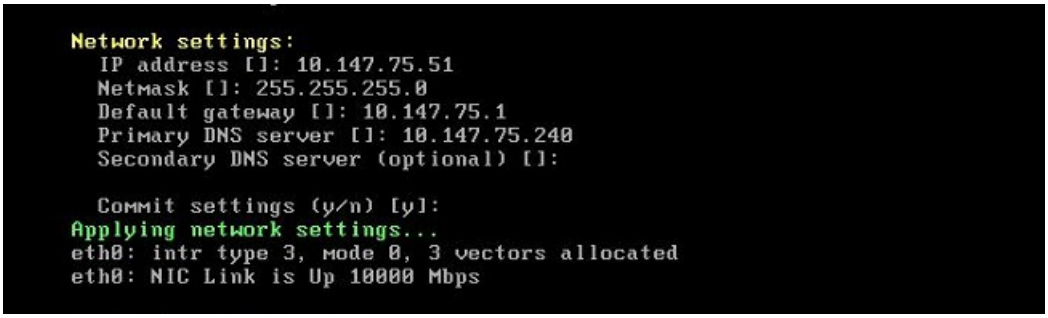
Referenzarchitekturdiagramme für XenMobile 10.x in Clusterkonfigurationen finden Sie unter Architektur im Überblick.

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.

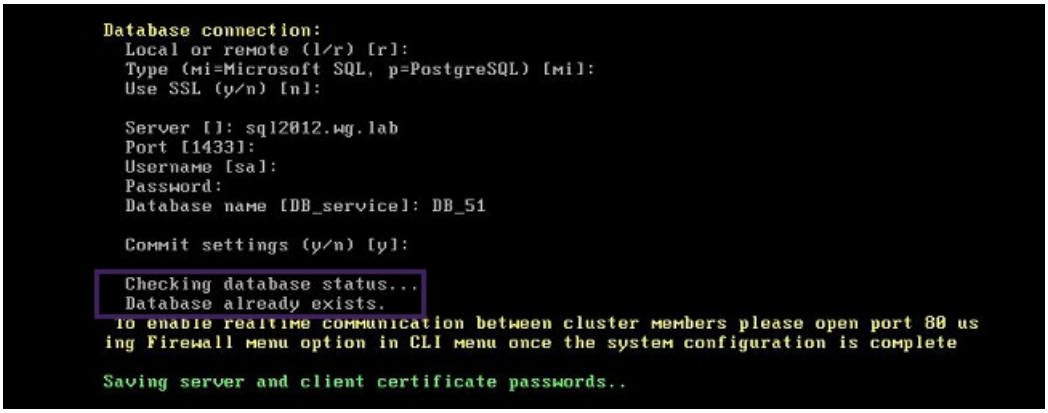
2. Geben Sie die Details der Netzwerkkonfiguration wie in der folgenden Abbildung dargestellt an.



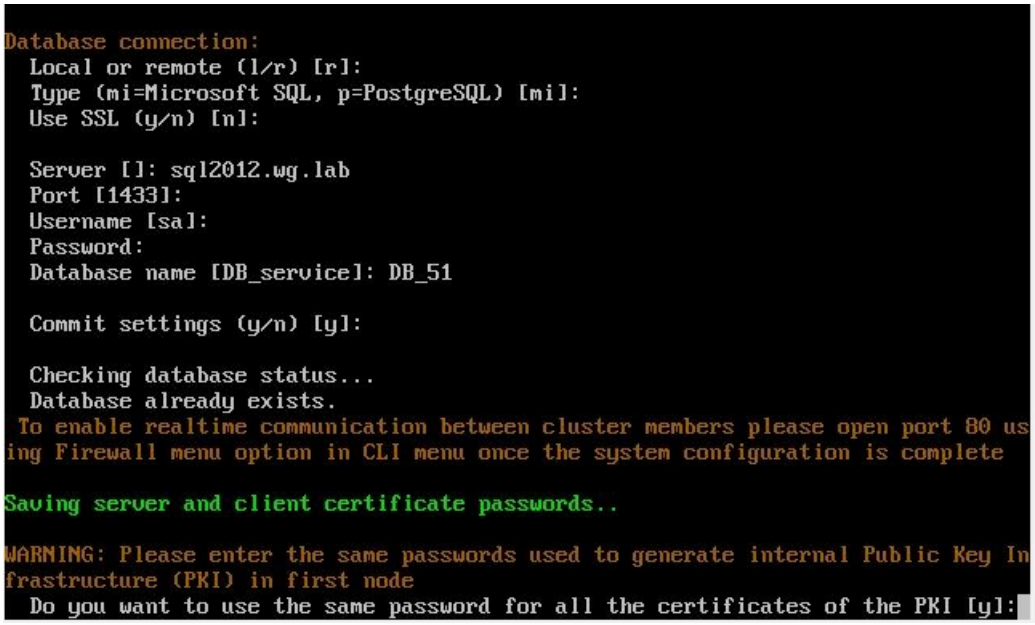
3. Wenn Sie das Standardkennwort für den Schutz von Daten verwenden möchten, geben Sieyein, andernfallsn und ein neues Kennwort ein.

4. Wenn Sie FIPS verwenden möchten, geben Sieyein, andernfallsn.

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.

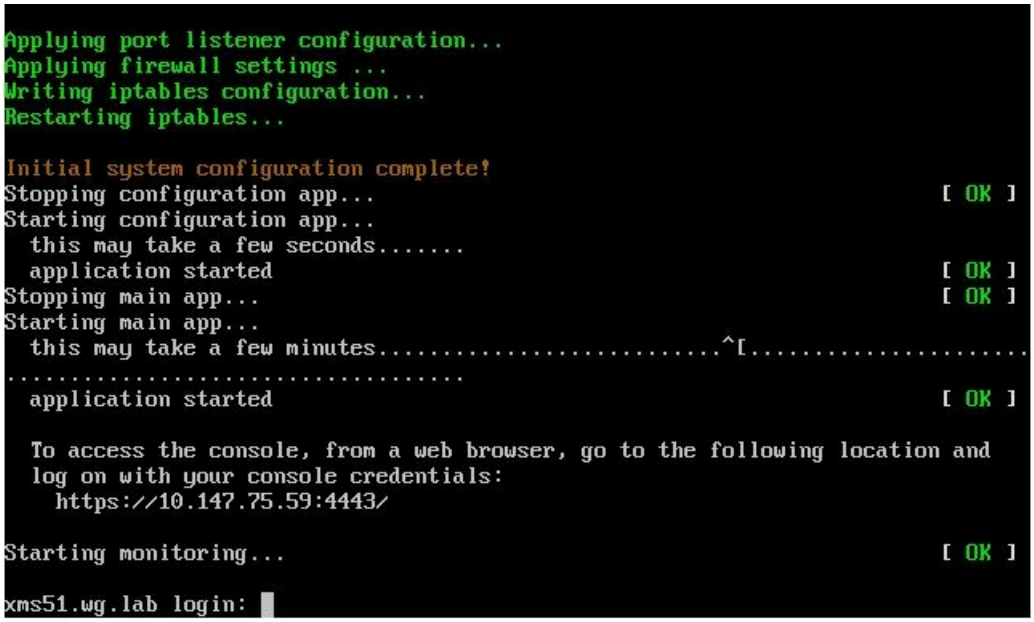


6. Geben Sie die gleichen Kennwörter für die Zertifikate an, wie für die erste VM.



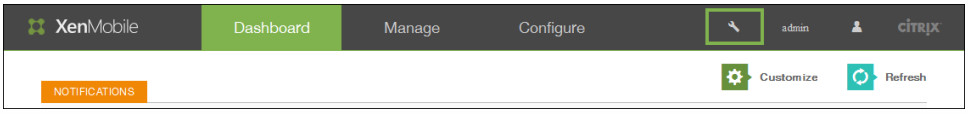
Nachdem Sie das Kennwort eingegeben haben, wird die anfängliche Konfiguration auf dem zweiten Knoten abgeschlossen.

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

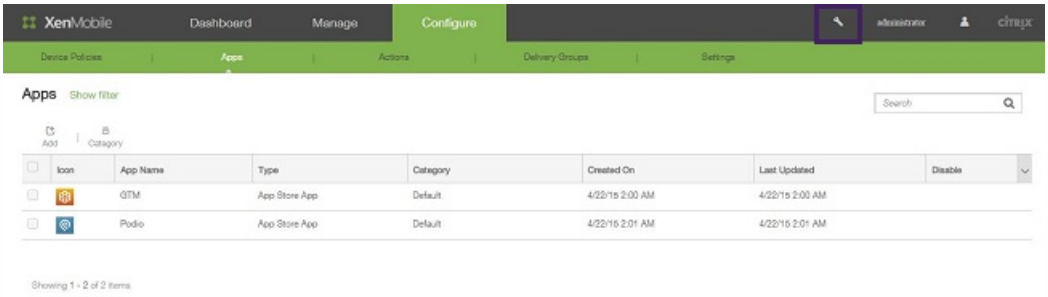


Hinweis: Das Anmeldedialogfeld ist das gleiche wie für die erste VM. Die Übereinstimmung zeigt Ihnen, dass beide VMs den gleichen Datenbankserver verwenden.

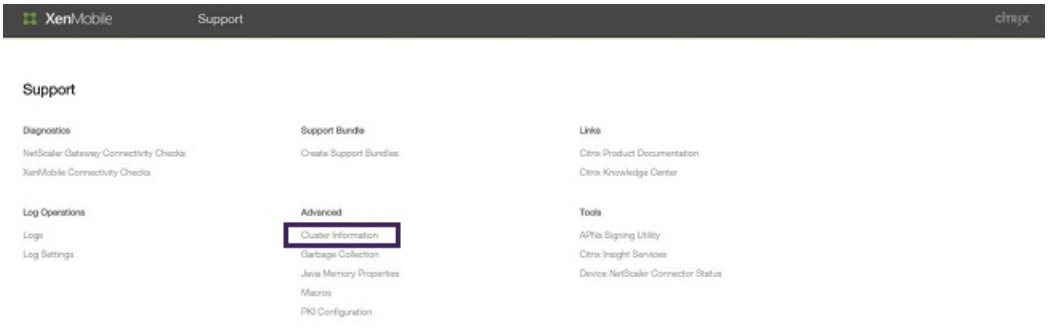
8. Verwenden Sie den vollqualifizierten Domänennamen (FQDN) von XenMobile, um die XenMobile-Konsole in einem Webbrowser zu öffnen.
9. Klicken Sie im Dashboard auf das Toolsymbol oben rechts auf dem Bildschirm.



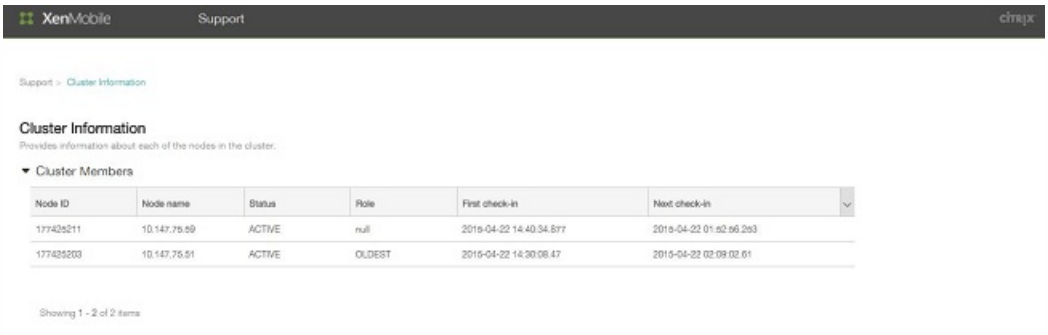
Die Seite "Support" wird geöffnet.



10. Klicken sie unter Advanced auf Cluster Information.



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



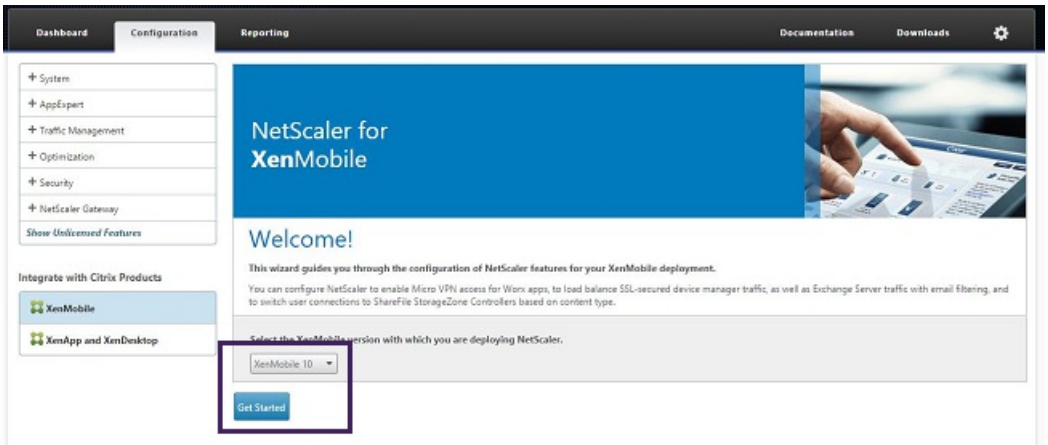
Der neue Knoten gehört nun zu dem Cluster. Sie können auf die gleiche Weise noch weitere Knoten hinzufügen.

Konfigurieren von Lastausgleich für den XenMobile-Cluster in NetScaler

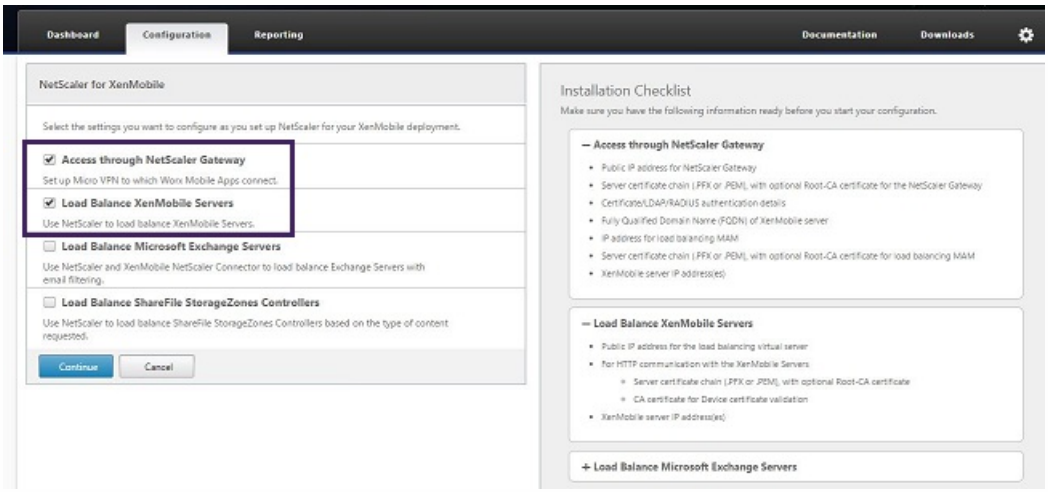
Nachdem Sie die erforderlichen Knoten als Mitglieder des XenMobile-Clusters hinzugefügt haben, müssen Sie für die Knoten den Lastausgleich durchführen, um auf die Cluster zuzugreifen. Der Lastausgleich geschieht, indem Sie den XenMobile-Assistent in NetScaler 10.5.x ausführen. Folgen Sie diesen Schritten,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

1. Melden Sie sich an NetScaler an.

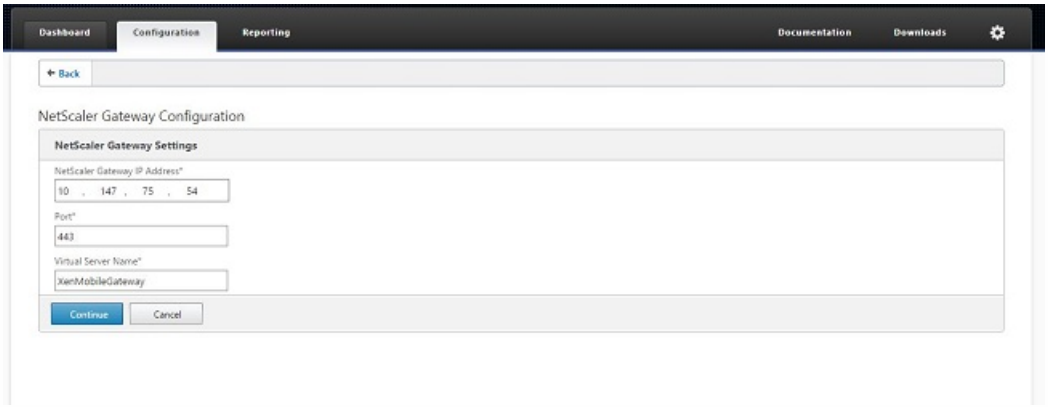
2. Klicken Sie auf der Registerkarte Configuration auf XenMobile und dann auf Get Started.



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

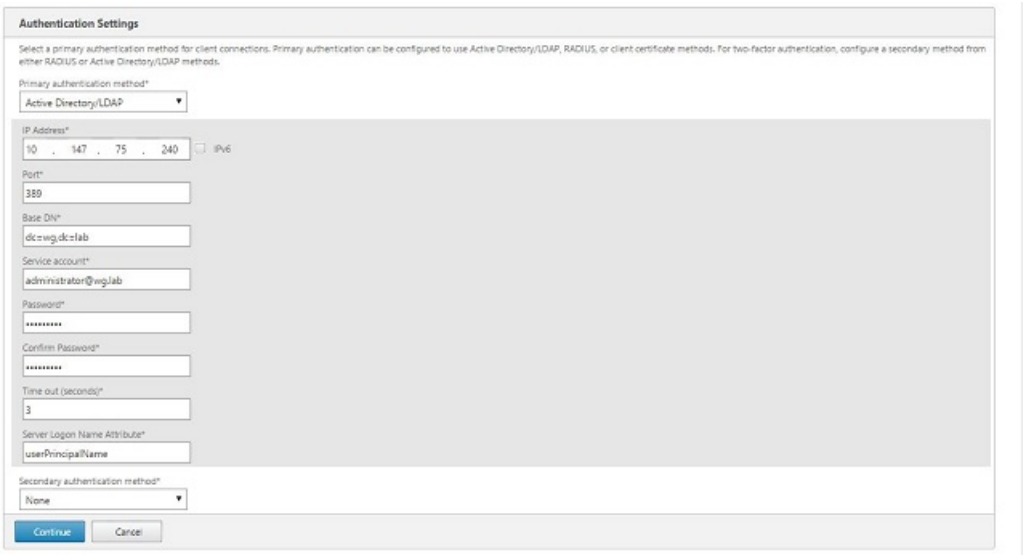


4. Geben Sie die IP-Adresse für NetScaler Gateway ein und klicken Sie auf Continue.



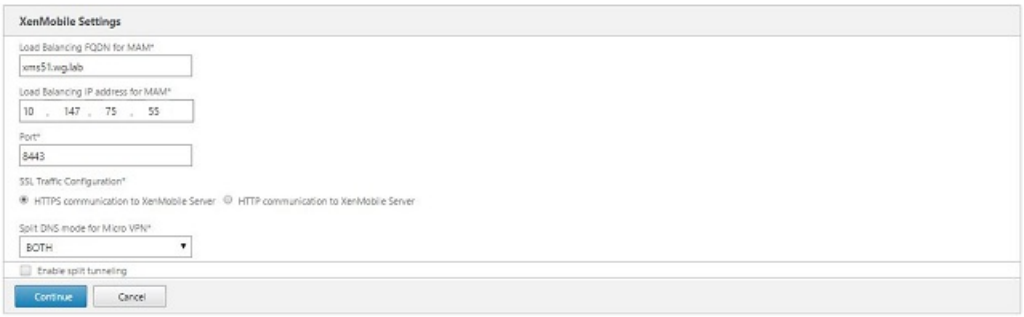
5. Binden Sie mit einer der folgenden Methoden das Serverzertifikat an die virtuelle IP-Adresse von NetScaler Gateway und klicken Sie dann auf Continue.
   - Wählen Sie unter Use existing certificate das Serverzertifikat aus der Liste.
   - Klicken Sie auf die Registerkarte Install Certificate, um ein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

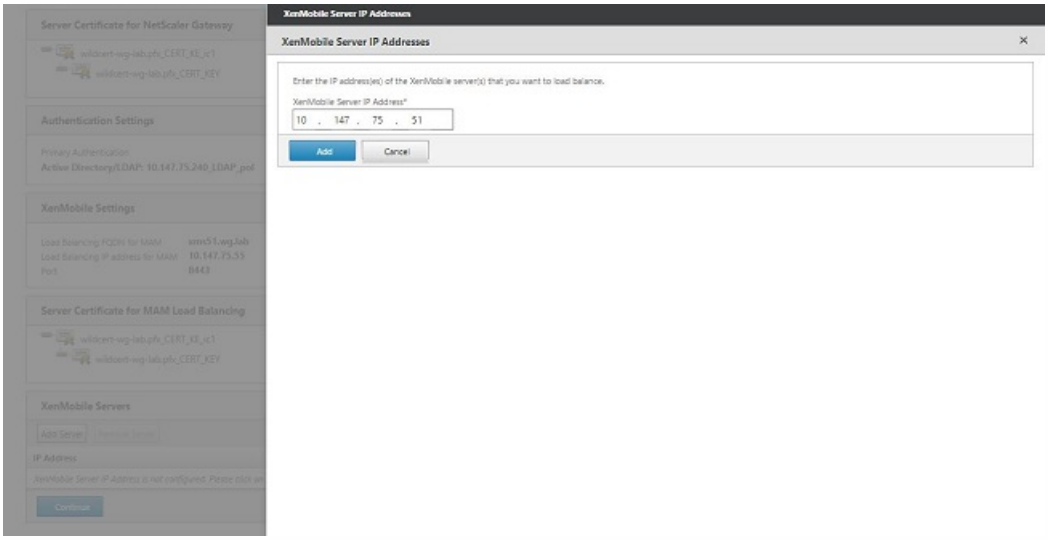


Hinweis: Stellen Sie sicher, dass der vollqualifizierte Domänenname (FQDN) der virtuellen IP-Adresse für den MAM-Lastausgleich und der FQDN von XenMobile gleich sind.

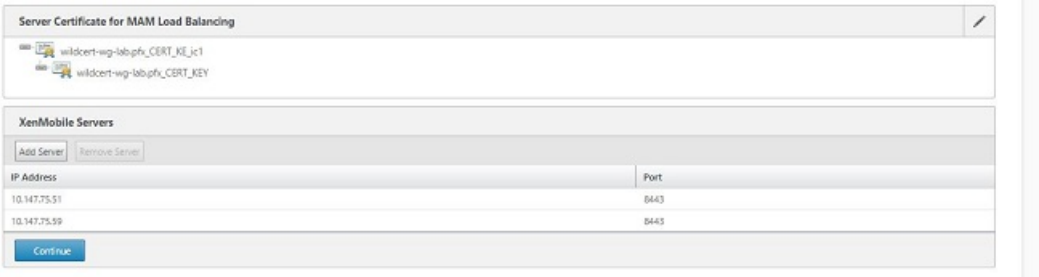
8. Wenn Sie den SSL-Brückenmodus (HTTPS) verwenden möchten, wählen Sie HTTPS communication to XenMobile Server. Wenn Sie aber SSL-Offload verwenden möchten, wählen Sie HTTP communication to XenMobile Server, wie in der voranstehenden Abbildung dargestellt. Für die Zwecke dieses Artikels nehmen wir SSL-Brückenmodus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

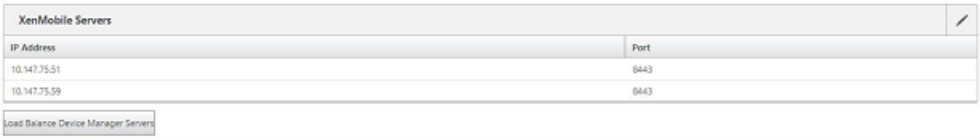
11. Geben Sie die IP-Adresse des XenMobile-Knotens ein und klicken Sie auf Add.



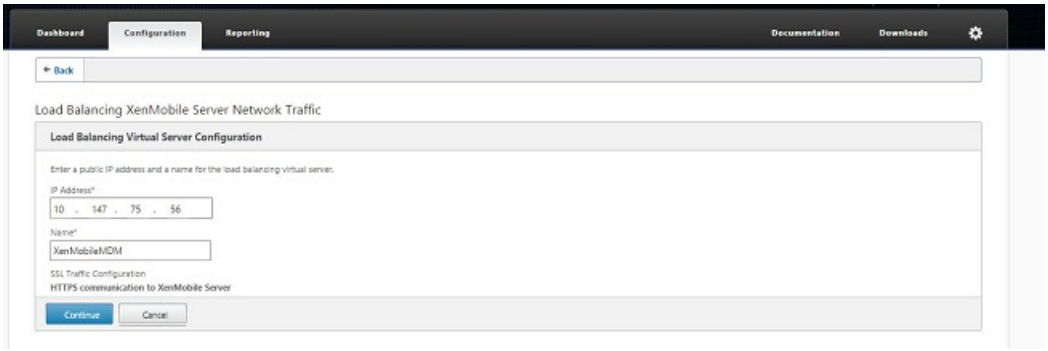
12. Wiederholen die Schritte 10 und 11, um weitere XenMobile-Knoten hinzuzufügen, die Teil des XenMobile-Clusters sind. Sie sehen dann alle XenMobile-Knoten, die Sie hinzugefügt haben. Klicken Sie auf Continue.



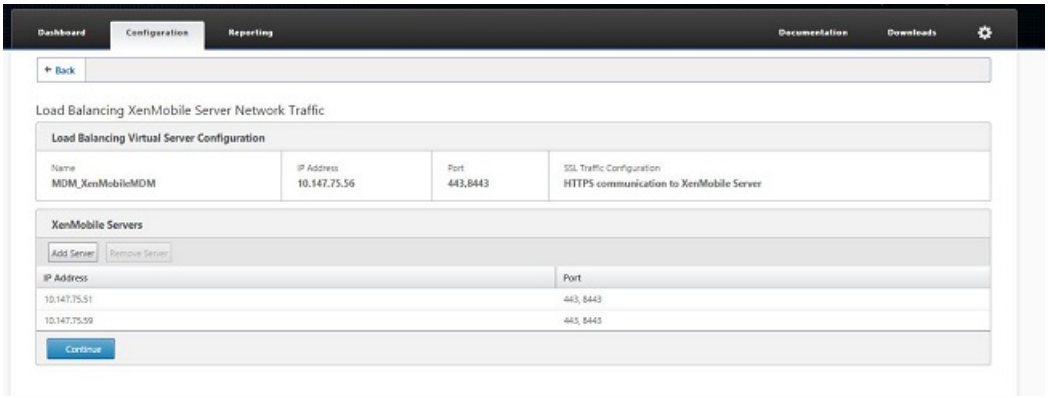
13. Klicken Sie auf Load Balance Device Manager Servers, um mit der Konfiguration des MDM-Lastausgleichs fortzufahren.



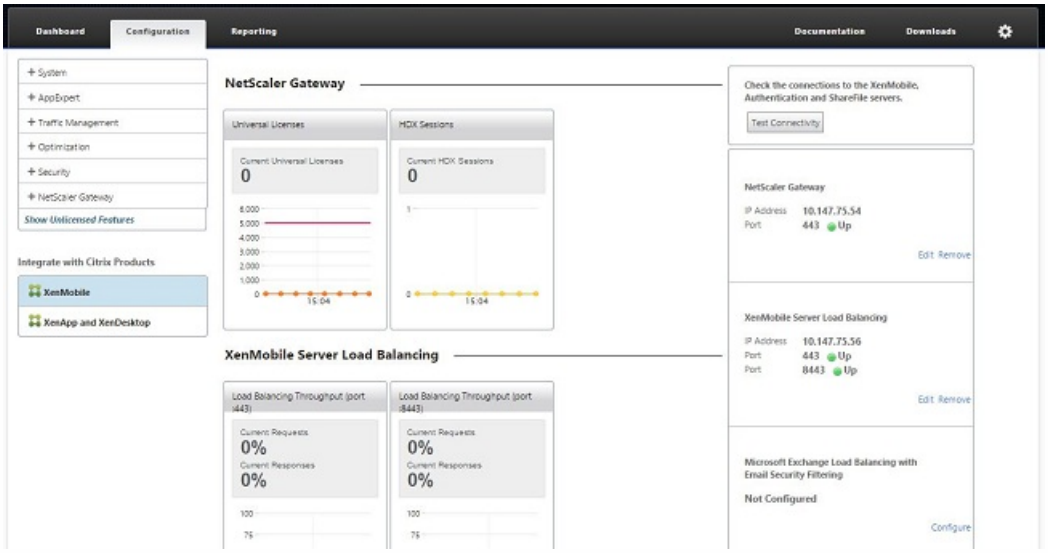
14. Geben Sie die IP-Adresse ein, die für den MDM-Lastausgleich verwendet werden soll und klicken Sie auf Continue.



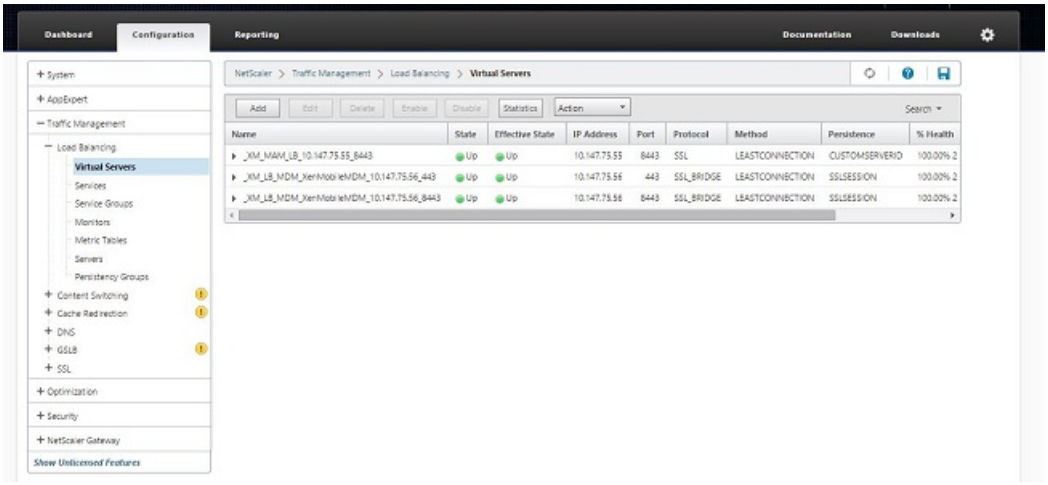
15. Sobald Sie die XenMobile-Knoten in der Liste sehen, klicken Sie auf Continue und dann auf click Done, um den Vorgang abzuschließen.



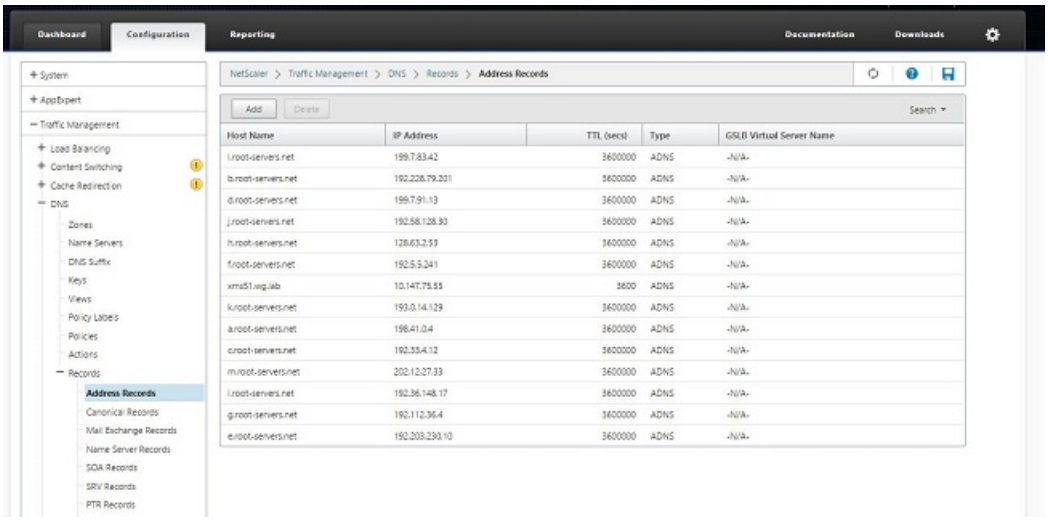
Sie sehen den Status der virtuellen IP-Adresse auf der Seite XenMobile.



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.

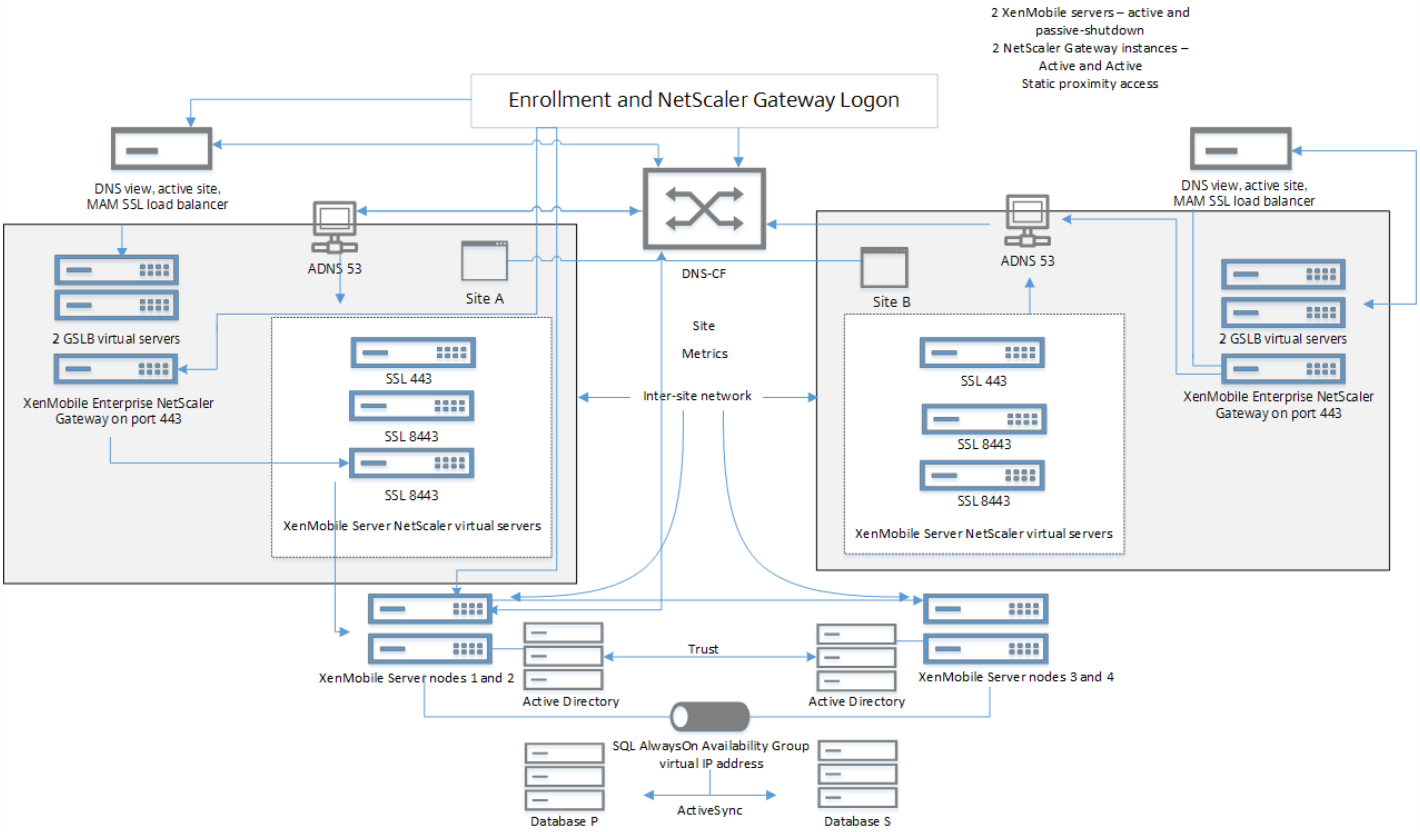


Disaster Recovery Guide für XenMobile

Jul 28, 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

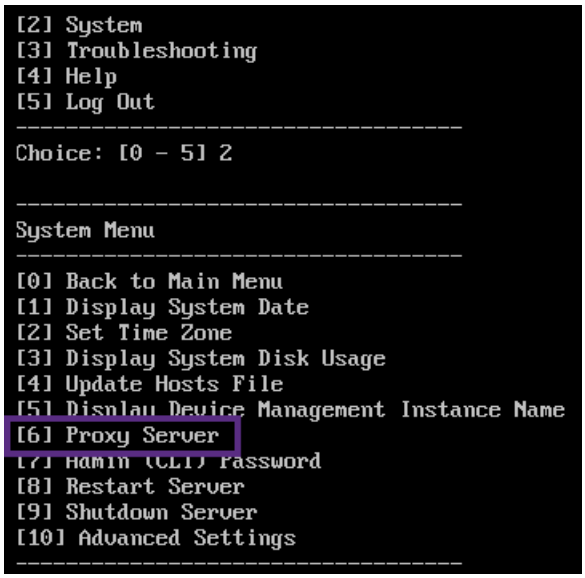
Aktivieren von Proxyservern in XenMobile

Jul 28, 2016

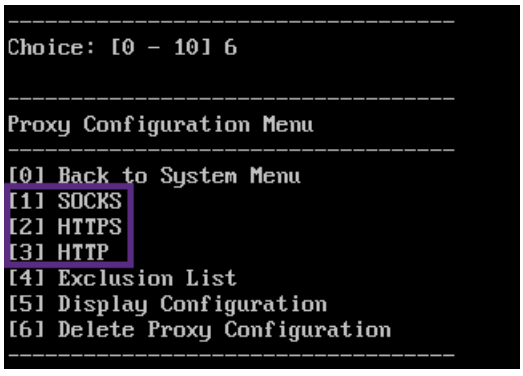
Zum Steuern von ausgehendem Internetverkehr können Sie in XenMobile einen Proxyserver für den Verkehr einrichten. Dazu müssen Sie den Proxyserver über die Befehlszeilenschnittstelle (CLI) einrichten. Zum Einrichten des Proxyservers müssen Sie das System neu starten.

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.



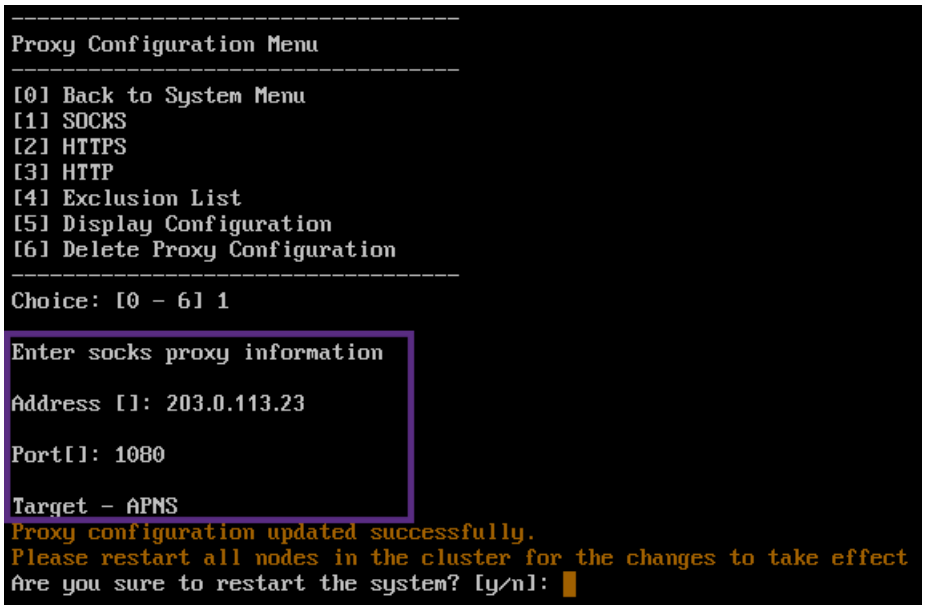
3. Geben Sie im Menü für die Proxykonfiguration **1** für die Auswahl von SOCKS ein, **2** für die Auswahl von HTTPS oder **3** für die Auswahl von HTTP.



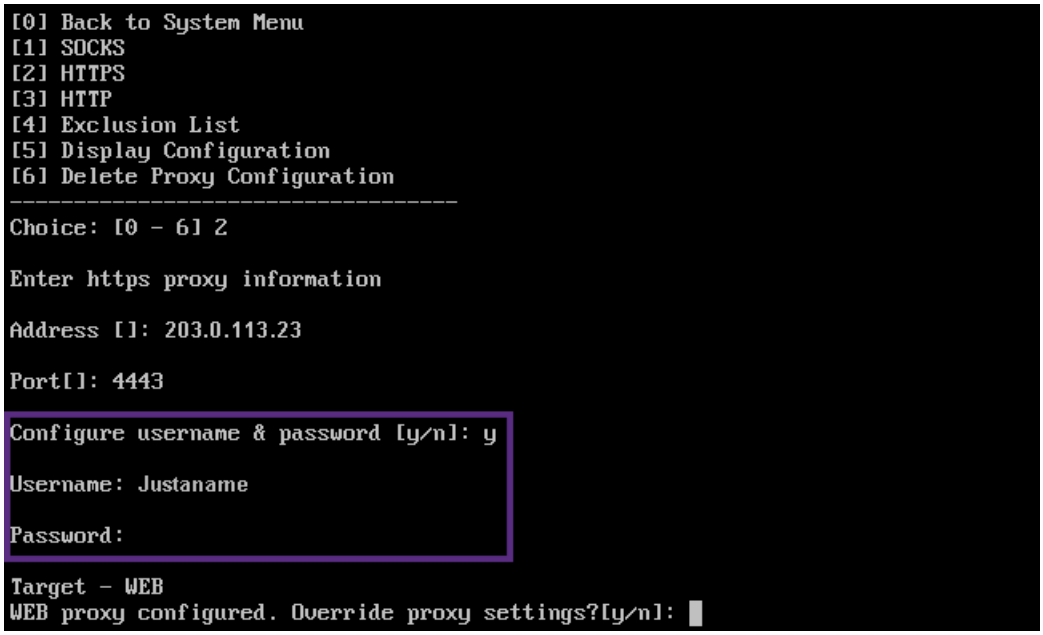
4. Geben Sie IP-Adresse, Portnummer und Ziel des Proxyservers ein. In der folgenden Tabelle sind die für die Proxyservertypen unterstützten Zieltypen aufgeführt.

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

Oct 13, 2016

XenMobile und NetScaler Gateway erfordern eine Lizenz. Diese PDF enthält ein Datenblatt zu den in jeder Edition verfügbaren XenMobile-Features.

Weitere Informationen zu Lizenzen für NetScaler Gateway finden Sie unter NetScaler Gateway Licenses. Die Lizenzverwaltung in XenMobile erfolgt über die Citrix Lizenzierung. Informationen über die Citrix Lizenzierung finden Sie unter Das Lizenzierungssystem von Citrix.

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 10.3.x erfordert den Citrix Lizenzserver 11.12.1 oder höher, ältere Versionen funktionieren nicht mit XenMobile 10.3.x.

> ## Important
>
> 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 von XenMobile. Der Zugriff auf die XenMobile-Webkonsole ist nie gesperrt, unabhängig davon, ob eine gültige XenMobile-Lizenz verfügbar ist. In der XenMobile-Konsole können Sie sehen, wie viele Tage Ihres Testzeitraums verbleiben.

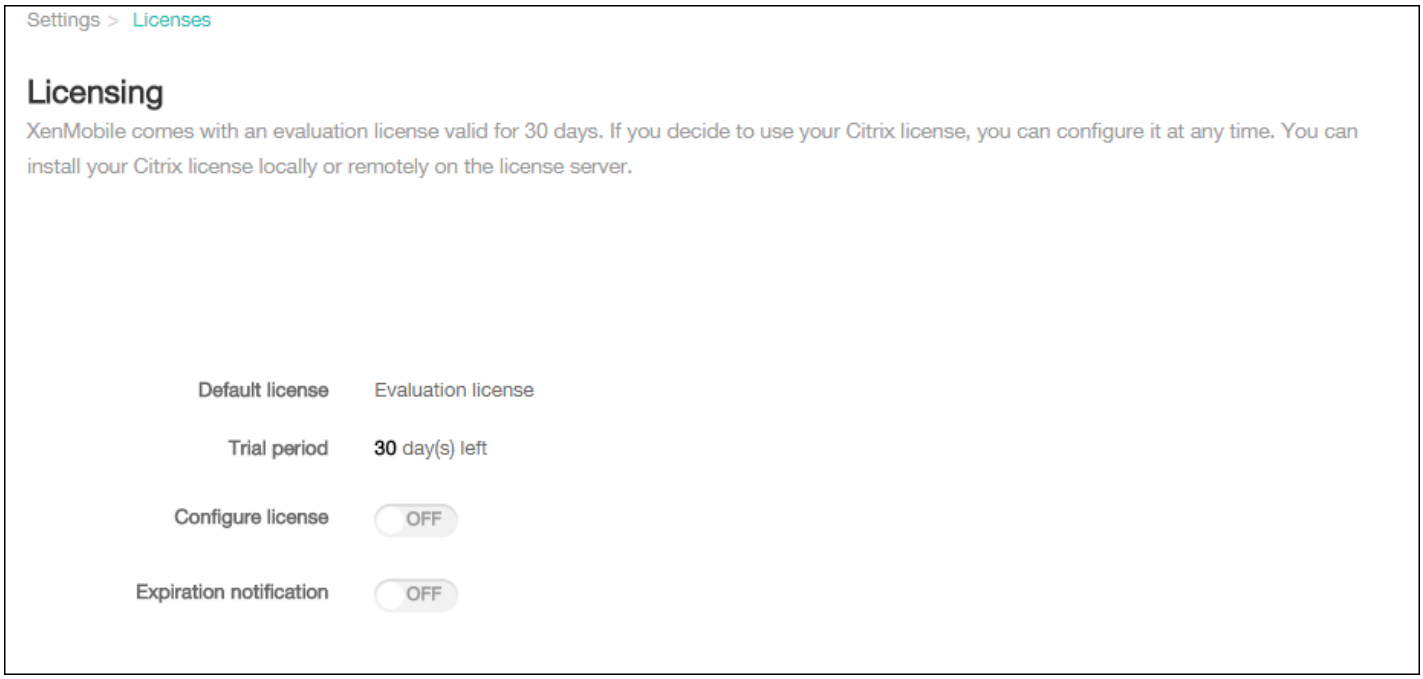
In XenMobile können zwar mehrere Lizenzen hochgeladen werden, es kann aber nur eine Lizenz aktiviert werden.

Wenn eine XenMobile-Lizenz abläuft, können Sie keine Geräteverwaltung mehr durchführen. Neue Benutzer oder Geräte können dann beispielsweise nicht registriert werden und auf registrierten Geräten bereitgestellte Apps und Konfigurationen können nicht aktualisiert werden. Weitere Informationen über XenMobile-Lizenzierungsmodelle und -Programme finden Sie

unter XenMobile-Lizenzierung.

So finden Sie die Lizenzierungsseite in der XenMobile-Konsole

Wenn die Seite **Lizenzierung** 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 das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie auf **Lizenzierung**. Die Seite **Lizenzierung** wird angezeigt.

Hinzufügen einer lokalen Lizenz

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 **Gesamtanzahl Lizenzen** und **Anzahl verwendet** in ihrer Kombination als Gesamtzahl der Lizenzen. Das Datum unter **Ablauf am** ist das Ablaufdatum der aktuellsten Lizenz.

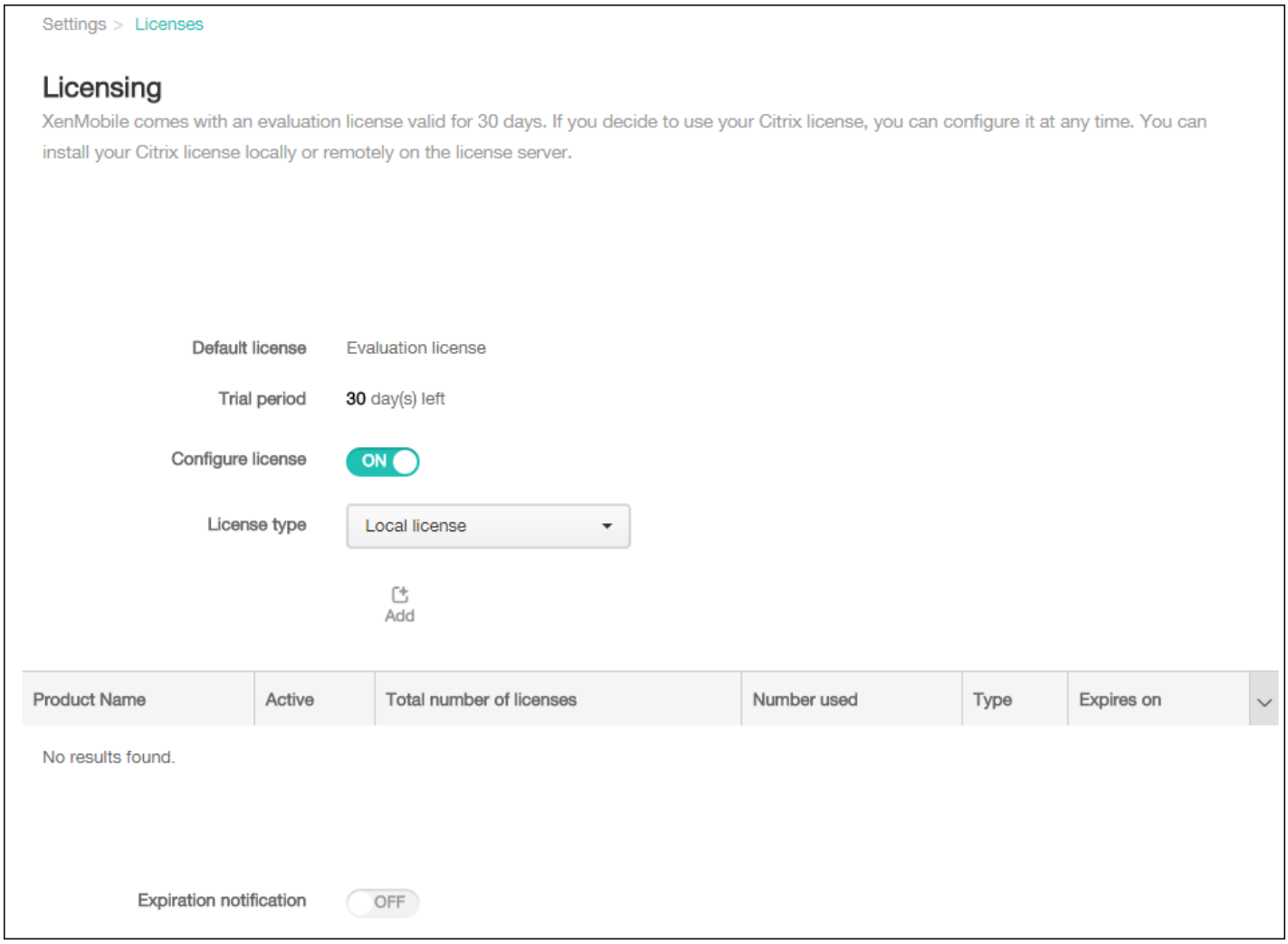
Sie können alle lokalen Lizenzen über die XenMobile-Konsole verwalten.

1. Beziehen Sie eine Lizenzdatei 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.

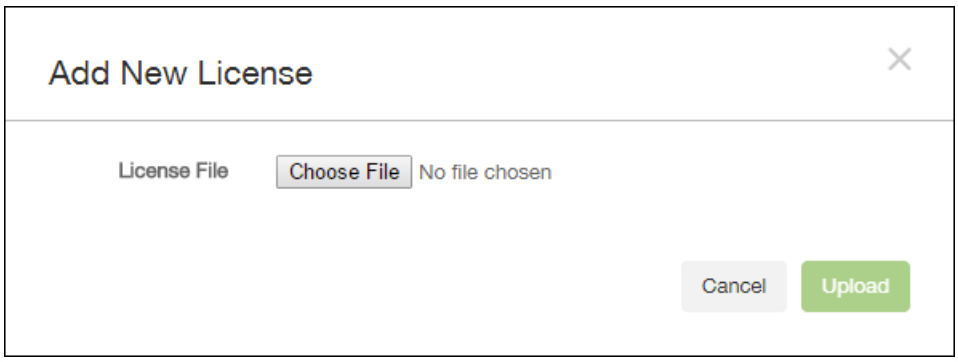
2. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

3. Klicken Sie auf **Lizenzierung**. Die Seite **Lizenzierung** wird angezeigt.

4. Legen Sie für **Lizenz konfigurieren** den Wert **Ein** fest. Es werden die Liste **Lizenztyp**, die Schaltfläche **Hinzufügen** 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.

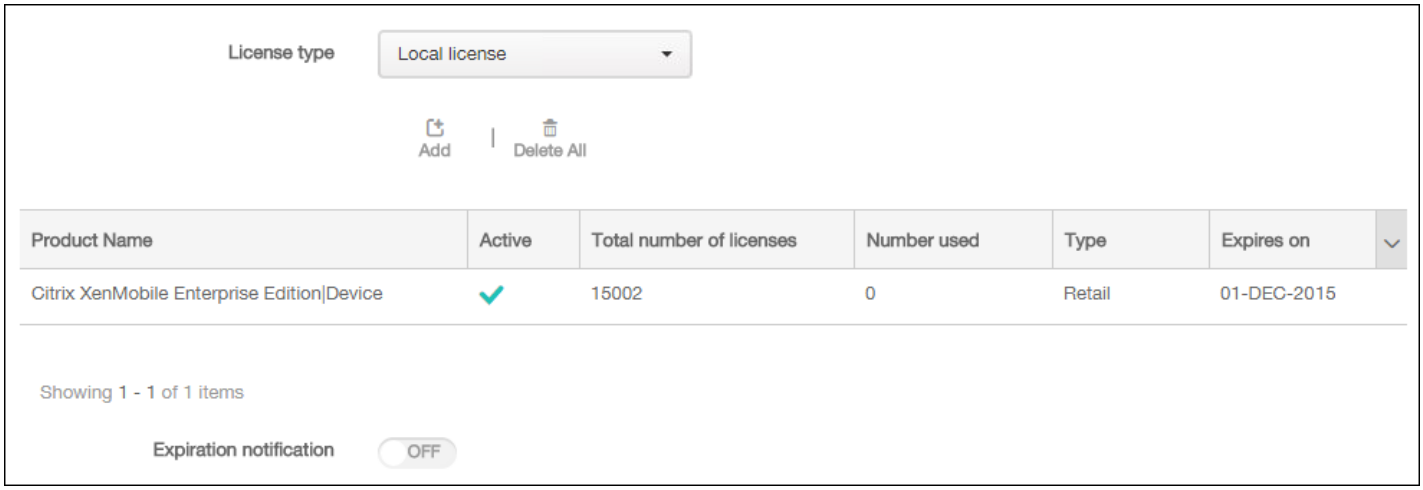


5. Stellen Sie sicher, dass **Lizenztyp** auf **Lokale Lizenz** festgelegt ist, und klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Lizenz hinzufügen** wird angezeigt.



6. Klicken Sie im Dialogfeld **Neue Lizenz hinzufügen** auf **Datei auswählen** und navigieren Sie zu der Lizenz.

7. Klicken Sie auf **Upload**. Die Lizenz wird lokal hochgeladen und in der Tabelle angezeigt.



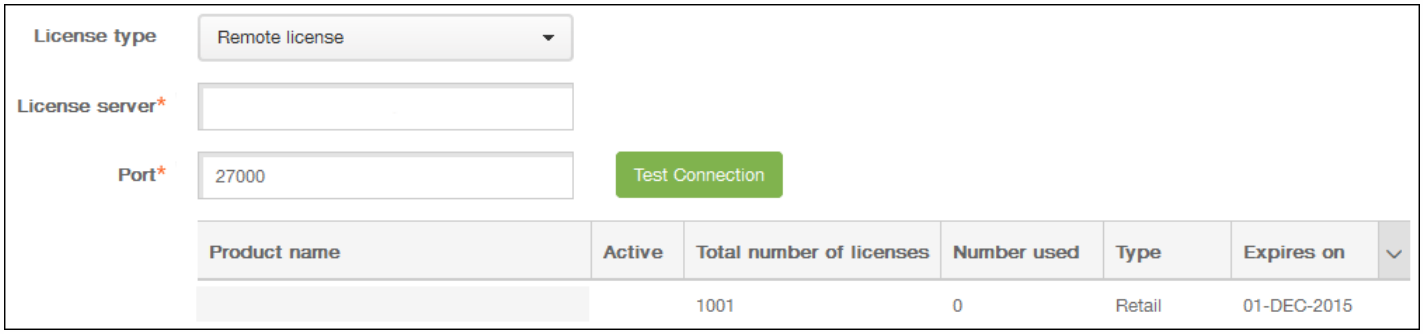
8. Wenn die Lizenz in der Tabelle auf der Seite **Lizenzierung** angezeigt wird, aktivieren Sie sie. Wenn dies die erste Lizenz in der Tabelle ist, wird sie automatisch aktiviert.

Hinzufügen einer Remote-Lizenz

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 **Lizenzierung** den Wert für **Lizenz konfigurieren** auf **Ein** fest. Es werden die Liste **Lizenztyp**, die Schaltfläche **Hinzufügen** 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.

3. Legen Sie für **Lizenztyp** den Wert **Remotelizenz** fest. Die Schaltfläche **Hinzufügen** wird durch die Felder **Lizenzserver** und **Port** und die Schaltfläche **Verbindung testen** ersetzt.



4. Konfigurieren Sie die folgenden Einstellungen:

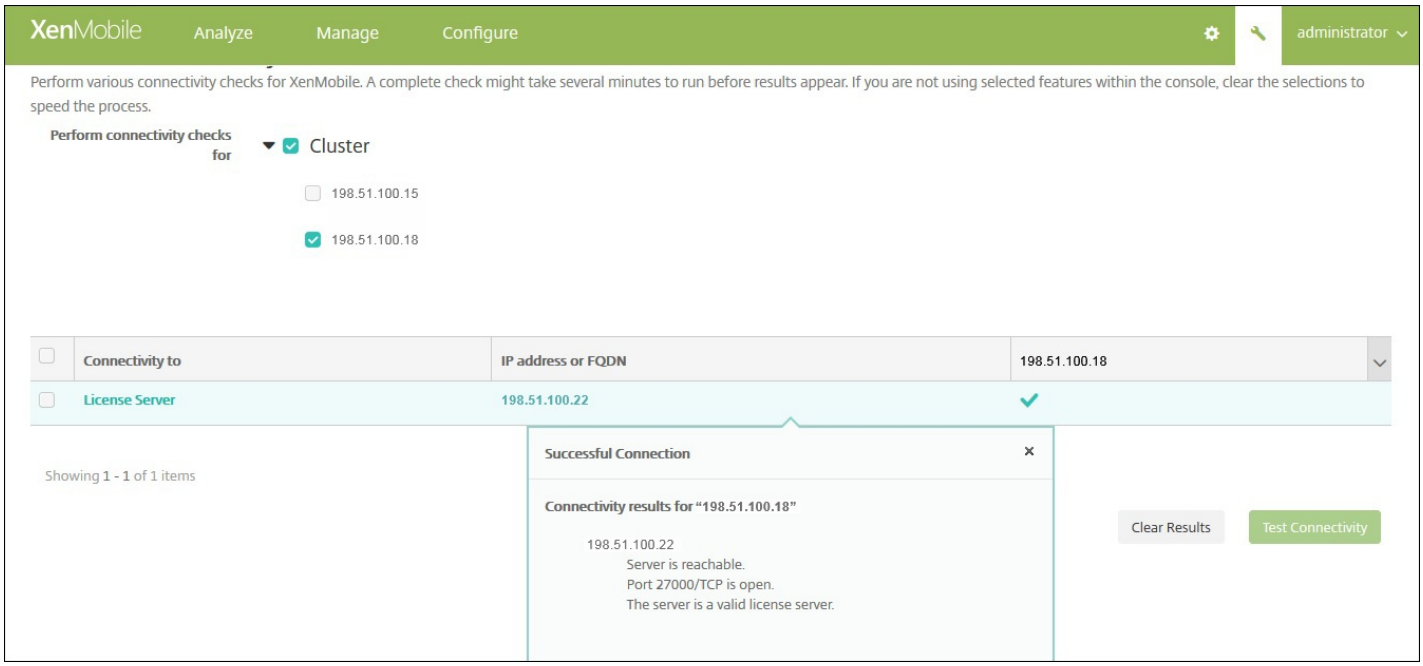
- **Lizenzserver**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des Remoteservers für die Lizenzierung ein.
- **Port**: Übernehmen Sie den Standardport oder geben Sie die Portnummer für die Kommunikation mit dem Lizenzserver ein.

5. Klicken Sie auf **Verbindung testen**. Wenn die Verbindung erfolgreich hergestellt wird, stellt XenMobile eine Verbindung mit dem Lizenzserver her und die Lizenztabelle wird mit den verfügbaren Lizenzen aufgefüllt. Gibt es nur eine Lizenz, wird diese automatisch aktiviert.

Wenn Sie auf **Verbindung testen** klicken, wird Folgendes geprüft:

- XenMobile kann mit dem Lizenzserver kommunizieren.
- Die Lizenzen auf dem Lizenzserver sind gültig.
- Der Lizenzserver ist mit XenMobile kompatibel.

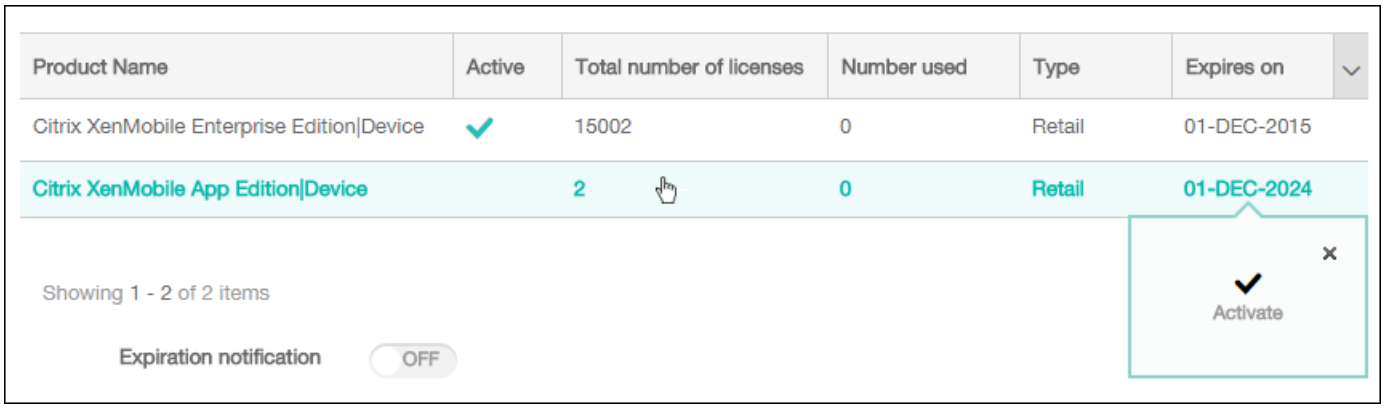
Wenn der Verbindungstest nicht bestanden wird, lesen Sie die angezeigte Fehlermeldung, nehmen Sie die erforderlichen Korrekturen vor und klicken Sie erneut auf **Verbindung testen**.



Aktivieren einer anderen 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 **Lizenzierung** in der Lizenztabelle auf die Zeile der Lizenz, die Sie aktivieren möchten. Neben der Zeile wird zur Bestätigung das Feld **Aktivieren** eingeblendet.



2. Klicken Sie auf **Aktivieren**. Das Dialogfeld **Aktivieren** wird angezeigt.

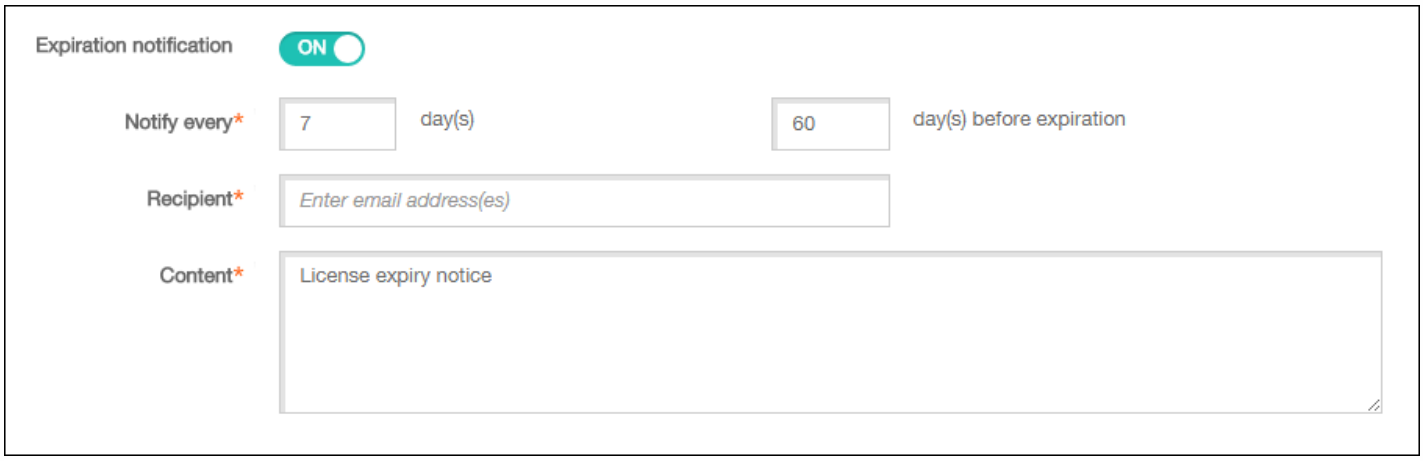
3. Klicken Sie auf **Aktivieren**. Die ausgewählte Lizenz wird aktiviert.

> **Important**
>
> Wenn Sie die ausgewählte Lizenz aktivieren, wird die bisher aktive Lizenz deaktiviert.

Einrichten einer automatischen Ablaufbenachrichtigung

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 **Lizenzierung** den Wert für **Ablaufbenachrichtigung** auf **Ein** fest. Es werden Felder für die Benachrichtigung eingeblendet.



2. Konfigurieren Sie die folgenden Einstellungen:

- **Benachrichtigung alle**: Geben Sie 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.
- **Empfänger**: Geben Sie Ihre E-Mail-Adresse oder die der für die Lizenzierung zuständigen Person ein.
- **Inhalt**: Geben Sie den Text der Ablaufbenachrichtigung ein.

3. Klicken Sie auf **Speichern**. Zu dem festgelegten Zeitraum vor dem Ablauf der Lizenz beginnt XenMobile mit dem Versand von E-Mail-Nachrichten mit dem von Ihnen für **Inhalt** angegebenen Text an den von Ihnen im Feld **Empfänger** festgelegten Empfänger. Der Versand der Benachrichtigungen wird mit der von Ihnen vorgegebenen Häufigkeit wiederholt.

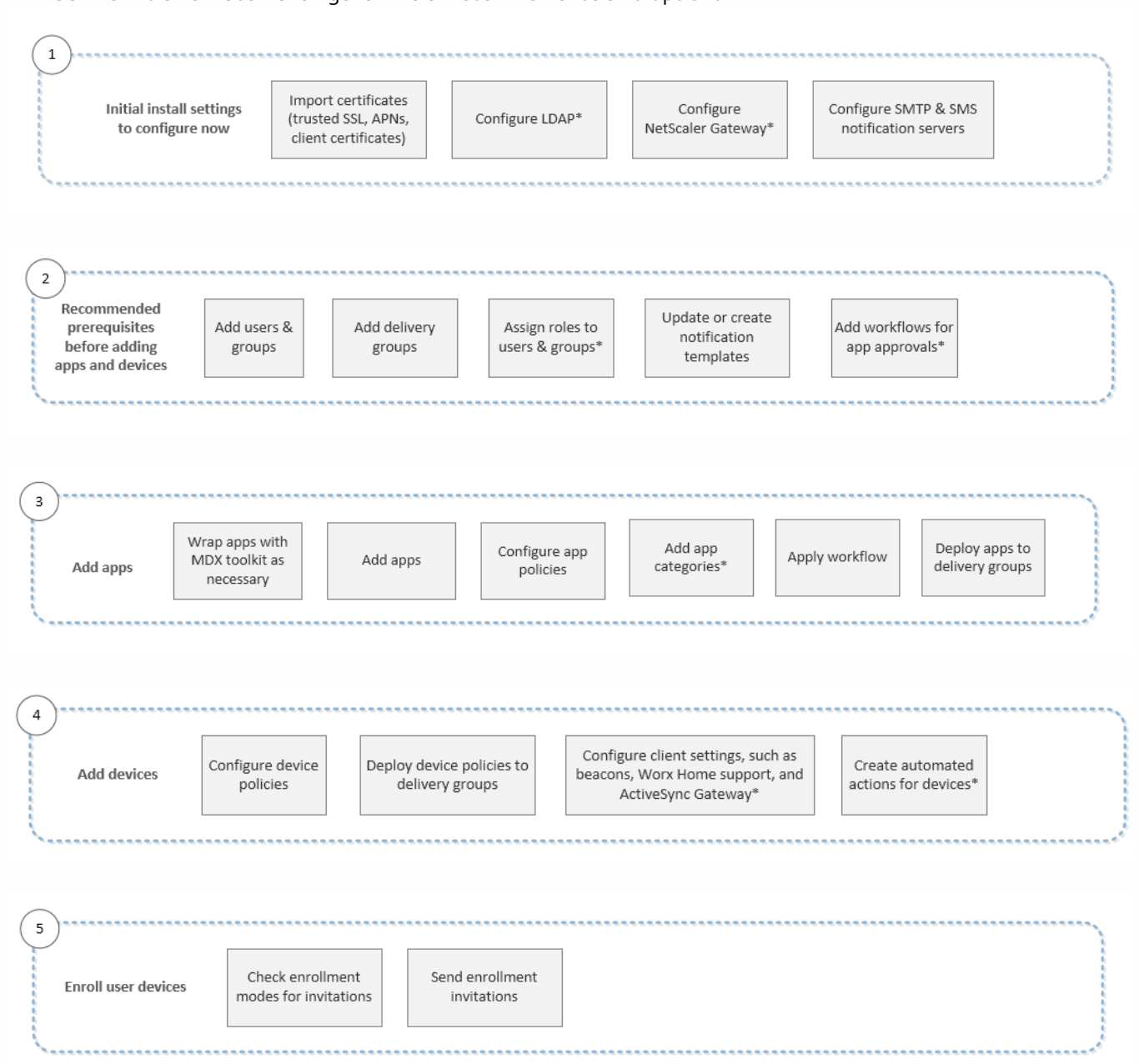
Erste Schritte mit der XenMobile-Konsole

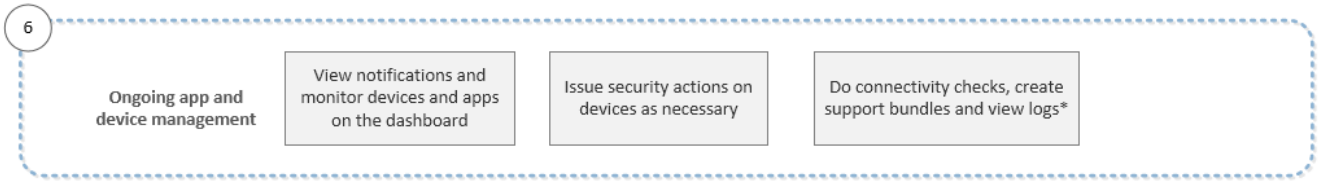
Jul 28, 2016

Die XenMobile-Konsole ist das zentrale Verwaltungstool in XenMobile. 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. Weitere Informationen zur Browserunterstützung für die XenMobile-Konsole finden Sie unter Browserunterstützung im Artikel zur XenMobile-Kompatibilität.

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.

Hinweis: Die mit einem Sternchen gekennzeichneten Elemente sind optional.



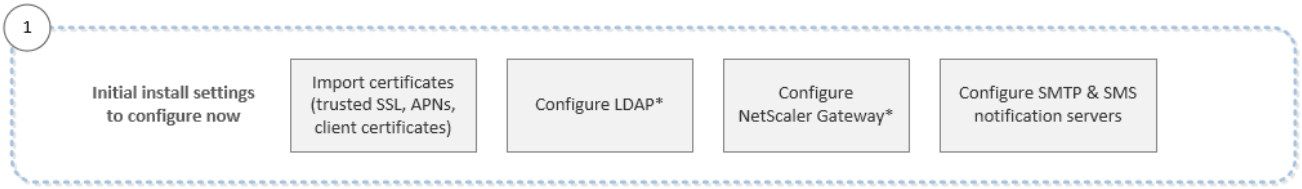


Workflow für erste Einstellungen

Jul 28, 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 in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. 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 Artikeln der Citrix Produktdokumentation:

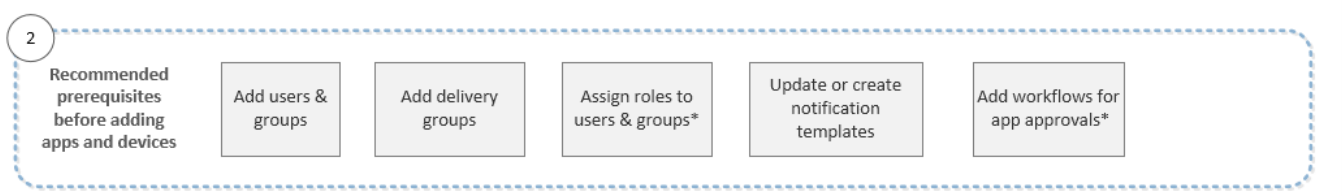
- Zertifikate in XenMobile
- Konfigurieren von LDAP
- NetScaler Gateway und XenMobile
- Benachrichtigungen in XenMobile

Workflow für Konsolenvoraussetzungen

Oct 13, 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 Artikeln der Citrix Produktdokumentation:

- Konfigurieren von Benutzerkonten, Rollen und Registrierungseinstellungen
- Verwalten von Bereitstellungsgruppen in XenMobile
- Konfigurieren von Rollen mit RBAC
- Erstellen und Aktualisieren von Benachrichtigungsvorlagen in XenMobile
- Konfigurieren von Registrierungsmodi und Aktivieren des Selbsthilfeportals
- Erstellen und Verwalten von Workflows

Workflow beim Hinzufügen von Apps

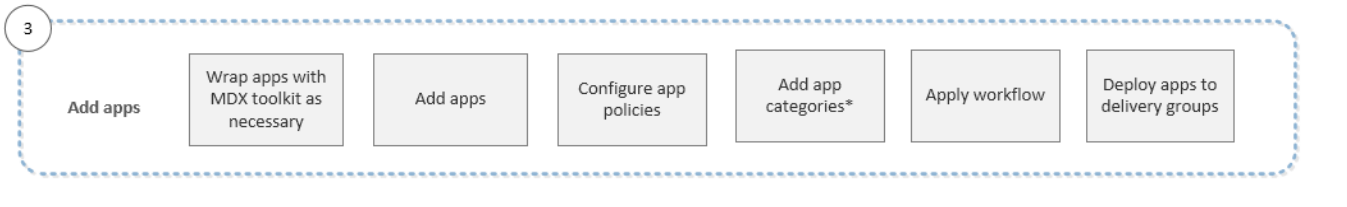
Oct 13, 2016

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 Artikeln der Citrix Produktdokumentation:

- Info über das MDX Toolkit
- Hinzufügen von Apps in XenMobile
- MDX-Richtlinien
- Hinzufügen von App-Kategorien
- Erstellen und Verwalten von Workflows
- Verwalten von Bereitstellungsgruppen in XenMobile

Workflow beim Hinzufügen von Geräten

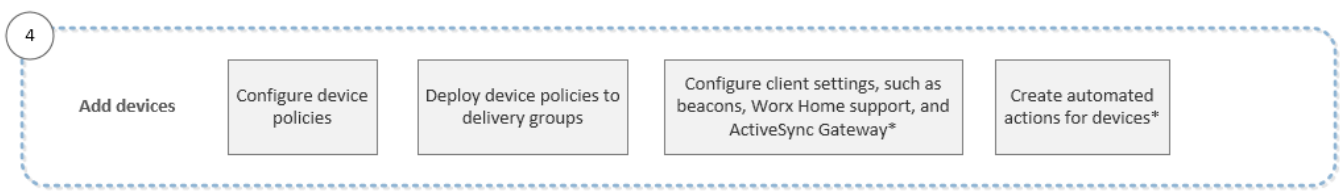
Jul 28, 2016

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 Artikeln der Citrix Produktdokumentation:

- 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

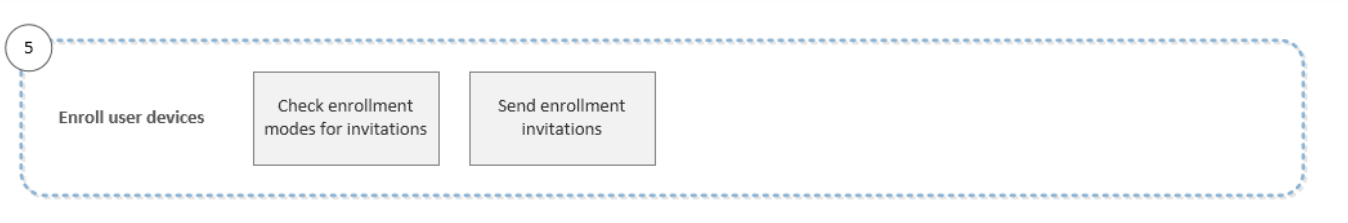
Workflow beim Registrieren von Benutzergeräten

Jul 28, 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 Artikeln der Citrix Produktdokumentation:

- Konfigurieren von Benutzerkonten, Rollen und Registrierungseinstellungen
- Konfigurieren von Registrierungsmodi und Aktivieren des Selbsthilfeportals

Workflow bei der Verwaltung von Apps und Geräten

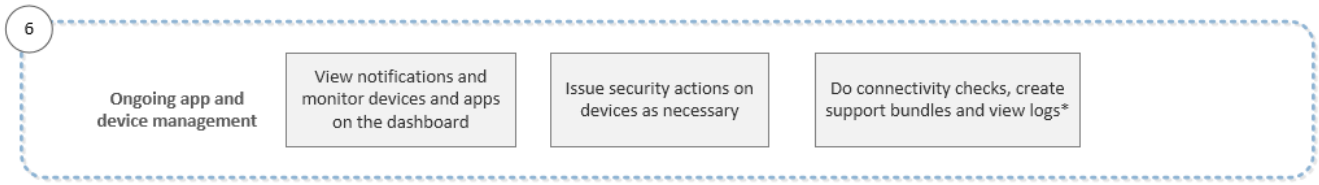
Jul 28, 2016

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

Jul 28, 2016

In der XenMobile-Konsole sind die überall Filter und Tabellen verfügbar. Sie finden sie auf den Registerkarten für Geräte, Registrierung, Geräterichtlinien, Apps, Aktionen und Bereitstellungsgruppen sowie auf vielen Seiten der Registerkarte "Einstellungen". Mit Filtern können Sie die Informationen in all diesen Bereichen auf die von Ihnen gesuchten einschränken und dann anzeigen oder damit verbundene Aktionen ausführen. Innerhalb von Tabellen können Sie auf ein Objekt oder mehrere Objekte klicken und die damit verbundenen Aktionen anzeigen. Die Optionen sind möglicherweise je nach Anzahl der ausgewählten Elemente unterschiedlich.

In der folgenden Tabelle werden einige der allgemeinen Optionen aufgelistet und wo Sie sie finden.

Menüoption	Aktion	Tabelle, in der die Option angezeigt wird
Fügen Sie dem DNS-Server	Hinzufügen eines neuen Elements zur Tabelle.	Alle
Kategorie	Hinzufügen und Verwalten von Kategorien für Anwendungen.	Apps
URL kopieren	Kopieren einer URL in die Zwischenablage.	Registrierung
Löschen oder Alles löschen	Endgültiges Entfernen der ausgewählten Elemente.	Alle
Bereitstellen	Bereitstellen von Ressourcen für Benutzer und Geräte.	Geräte und Bereitstellungsgruppen
Automatische	Deaktivieren einer App oder der Bereitstellungsgruppe "AllUsers".	Apps und Bereitstellungsgruppen
Bearbeiten	Vornehmen von Änderungen an einem vorhandenen Element.	Alle außer Registrierung
Exportieren	Senden von Tabelleninhalt an eine CSV-Datei.	Alle
Importieren	Hinzufügen von Geräten aus einer Provisioningdatei.	Geräte
	Hinzufügen lokaler Benutzer und Gruppen aus einer Datei.	Lokale Benutzer und Gruppen
Lokale Gruppen verwalten	Hinzufügen einer lokalen Gruppe für die Verwaltung.	Lokale Benutzer und Gruppen
Benachrichtigen	Senden einer Nachricht an die ausgewählten Benutzer und Geräte.	Registrierung und Geräte

Menüoption	Aktion	Tabelle, in der die Option angezeigt wird
Aktualisieren	Aktualisieren der Tabelle.	Geräte
Sicherung	Aufrufen von Sicherheitsaktionen für das ausgewählte Gerät.	Geräte
Selbsthilfeportal	Aktivieren des Selbsthilfeportals als Registrierungsmodus.	Registrierung
Update	Aktualisieren der Werte in einer Tabelle.	Releasemanagement

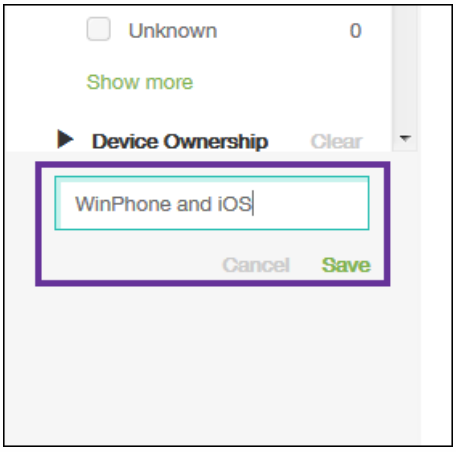
Sie können die Optionen zum Ausführen von Aktionen für Informationen in den Tabellen der Konsole auf verschiedene Weise anzeigen:

- Sie können das Kontrollkästchen neben einem Element aktivieren, um das Menü der Optionen oberhalb der Liste anzuzeigen.
- Sie können die Kontrollkästchen mehrerer Elemente auswählen, um eine Aktion für alle Elemente gleichzeitig auszuführen. Die für mehrere Elemente verfügbaren Aktionen hängen von der Tabelle ab, die Sie anzeigen.
- Sie können auf ein Element in der Liste klicken, um das Menü mit den Optionen rechts daneben anzuzeigen. Wenn Sie auf Mehr anzeigen klicken, werden Details zu dem Element angezeigt. Die Details sind je nach Tabelle unterschiedlich.
- Sie können einen Namen vollständig oder teilweise in das Feld Suchen eingeben, um die Anzahl der angezeigten Elemente zu beschränken.

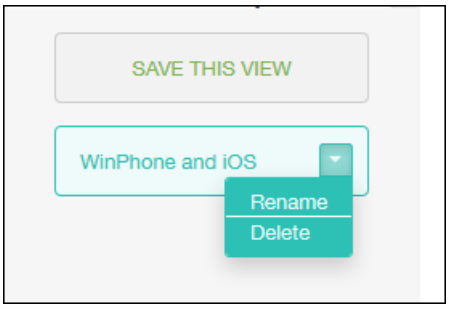
Im Bereich "Geräterichtlinien" der Konsole werden nur 10 Objekte pro Seite aufgeführt. Klicken Sie auf die Dreiecke in der unteren rechten Ecke, um durch die Seiten zu blättern.

Wenn Sie einen bestimmten Teil der Informationen in einem Konsolenbereich wie "Geräte", "Registrierung", "Geräterichtlinien", "Apps", "Aktionen", "Bereitstellungsgruppen" oder "Lokale Benutzer und Gruppen" anzeigen möchten, können Sie die Liste nach Ihren Kriterien filtern. Hier wird die Seite "Geräte" als Beispiel verwendet, die Schritte zum Filtern sind jedoch in der gesamten Konsole gleich.

1. Klicken Sie auf der Seite Geräte auf Filter anzeigen.
   Der Bereich "Filter" mit den Kriterien, anhand derer Sie die Liste Geräte filtern können, wird angezeigt. Wenn Sie den Filter zum ersten Mal anzeigen, sind alle Kriterien ausgeblendet.
2. Klicken Sie auf das Dreieck links neben einem Filter, um die Kriterien für den Filter anzuzeigen. Die Zahlen rechts neben jedem Kriterium repräsentieren die Zahl der Geräte, die dem Kriterium entsprechen.
3. Wählen Sie die gewünschten Filterkriterien aus. Die Liste Geräte enthält nun nur die Geräte, die den ausgewählten Kriterien entsprechen.
4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf Filter ausblenden, um die Arbeit mit der gefilterten Liste fortzusetzen.
   - Klicken Sie auf Auswahl aufheben, um die vollständige Liste wiederherzustellen.
   - Klicken Sie neben einem bestimmten Kriterium auf Löschen, um den Filter zu löschen und die Elemente aus der gefilterten Liste zu entfernen.
5. Zum Speichern der ausgewählten Kriterien in einem benutzerdefinierten Filter geben Sie im Feld Diese Ansicht speichern unten im Bereich Filter einen aussagekräftigen Namen ein und klicken Sie auf Speichern. Wenn Sie den Filter nicht speichern möchten, klicken Sie auf Abbrechen.



6. Nach dem Speichern des Filters können Sie ihn unten im Bereich Filter auswählen, um Informationen in der Tabelle zu filtern.
   Hinweis: Wenn Sie auf das Dreieck rechts neben dem Filternamen klicken, können Sie den Filter umbenennen oder löschen.



Berichte in XenMobile

Jul 28, 2016

XenMobile 10 bietet vordefinierte Berichte für die Analyse von App- und Gerätebereitstellungen:

- **Apps nach Geräten & Benutzer**: Liste der Apps, die Benutzer auf ihren Geräten haben
- **AGB**: Benutzerliste mit Informationen dazu, ob die Benutzer die AGB akzeptiert oder abgelehnt haben
- **Top 25 Apps**: Liste der 25 meistinstallierten Apps
- **Geräte mit Jailbreak/Rooting**: Liste der iOS-Geräte mit Jailbreak und der gerooteten Android-Geräte
- **Top 10 Apps - Bereitstellung fehlgeschlagen**: Liste der Apps, deren Bereitstellung fehlgeschlagen ist
- **Inaktive Geräte**: Liste der Geräte, die für eine bestimmte Zeitdauer inaktiv waren
- **Apps nach Typ & Kategorie**: Liste der Apps sortiert nach Version, Typ und Kategorie
- **Geräteregistrierung**: Liste der Geräte, die im angegebenen Zeitraum registriert wurden
- **Apps nach Plattform**: Liste der Apps und App-Versionen sortiert nach Geräteplattform und -version
- **Geräte & Apps**: Liste aller installierten Geräte, Gerätedaten und verwalteter Apps

Die Berichte haben das CSV-Format und können mit Programmen wie Microsoft Excel geöffnet werden. Die folgende Tabelle enthält die Spaltenüberschriften und Informationen dazu, in welchen Berichten sie verwendet werden.

Überschrift	Beschreibung	Verwendet in
ACCEPTANCE_STATUS	Status der Annahme der AGB	AGB
APP_CATEGORY	Kategorie, unter der die App auf Geräten angezeigt wird (z. B. öffentlicher App-Store oder Unternehmensapps)	Top 10 Apps - Bereitstellung fehlgeschlagen, Apps nach Typ & Kategorie, Geräte & Apps
APP_ID	Eindeutige App-ID	Geräte & Apps
APP_NAME	App-Name	Top 25 Apps, Top 10 Apps - Bereitstellung fehlgeschlagen, Apps nach Typ & Kategorie, Geräte & Apps
APP_OWNER	App-Besitzer (z. B. Citrix.com bei Worx-Apps)	Top 25 Apps, Top 10 Apps - Bereitstellung fehlgeschlagen, Apps nach Typ & Kategorie, Apps nach Plattform, Geräte & Apps
APP_TYPE	App-Typ (z. B. öffentlicher App-Store oder Unternehmen)	Top 25 Apps, Top 10 Apps - Bereitstellung fehlgeschlagen, Apps nach Typ & Kategorie, Geräte & Apps

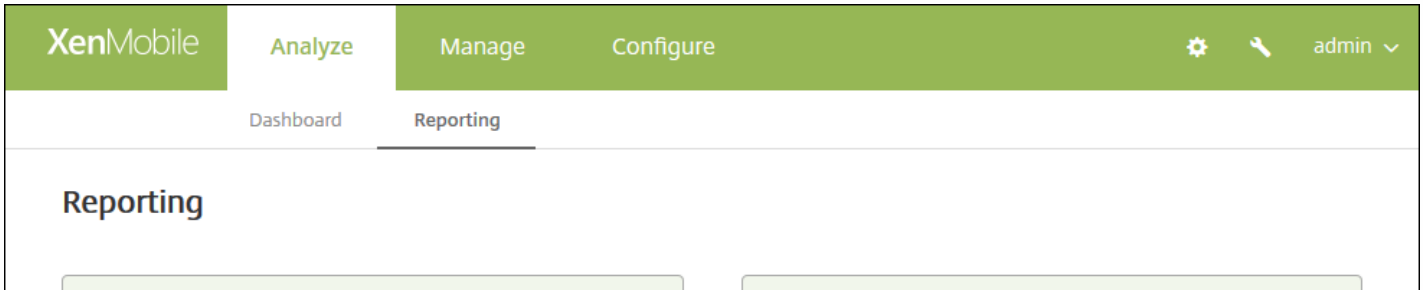
APP_VERSION	App-Version	Top 25 Apps, Top 10 Apps - Bereitstellung fehlgeschlagen, Apps nach Typ & Kategorie, Apps nach Plattform, Geräte & Apps
APPS_ON_DEVICE	Anzahl der auf dem Gerät installierten Apps	Apps nach Geräten & Benutzer
CERTIFICATE_EXPIRATION	Datum, an dem das Gerätezertifikat abläuft	Geräte & Apps
CREATION_DATE	Datum, an dem die AGB-Datei erstellt wurde	AGB
DELIVERY_GROUP	Der bereitgestellten Ressource zugewiesene Bereitstellungsgruppe	AGB
DEPLOYMENT_DATE	Datum, an dem die Ressource bereitgestellt wurde	Top 25 Apps, Top 10 Apps - Bereitstellung fehlgeschlagen, Apps nach Typ & Kategorie, Geräte & Apps
DEPLOYMENT_SUCCESS, DEPLOYMENT_FAILED, DEPLOYMENT_PENDING	Bereitstellungsstatus	Apps nach Gerät & Benutzer, Top 25 Apps, Top 10 Apps - Bereitstellung fehlgeschlagen, Apps nach Typ & Kategorie, Apps nach Plattform, Geräte & Apps
DEPLOYMENT_TOTAL	Gesamtzahl der versuchten Bereitstellungen	Top 25 Apps, Top 10 Apps - Bereitstellung fehlgeschlagen, Apps nach Typ & Kategorie, Apps nach Plattform, Geräte & Apps
DEVICE_MODE	Gerätemodus (verwaltet oder nicht verwaltet)	Geräte mit Jailbreak/Rooting, Inaktive Geräte, Geräteregistrierung, Geräte & Apps
DEVICE_OWNERSHIP	Kategorie des Gerätebesitzes (BYOD, Unternehmen oder Unbekannt)	Geräte & Apps

DEVICE_PLATFORM	Geräteplattform	Apps nach Plattform
DEVICE_STATUS	Status der Richtlinientreue	Geräte & Apps
DEVICE_VERSION	Versionsnummer des Gerätebetriebssystems	Apps nach Plattform
DOCUMENT_NAME	Name der AGB-Datei	AGB
E-Mail	E-Mail-Adresse des Benutzers	Geräte & Apps
ENROLLMENT_DATE	Datum, an dem das Gerät bei XenMobile registriert wurde	Geräte & Apps
ENROLLMENT_STATUS	Registrierungsstatus des Geräts (registriert oder nicht registriert)	Geräte & Apps
FIRST_CONNECTION_DATE	Datum, an dem das Gerät die erste Verbindung mit XenMobile hergestellt hat	Inaktive Geräte, Geräteregistrierung
IMEI	Device International Mobile Station Equipment Identity-Nummer	Inaktive Geräte
LAST_ACTIVITY	Datum der letzten Geräteaktivität	Inaktive Geräte
LAST_AUTH_DATE	Datum, an dem das Gerät zum letzten Mal bei XenMobile authentifiziert wurde	Inaktive Geräte, Geräteregistrierung, Geräte & Apps
LAST_USERNAME	Dem Gerät zugewiesener Nachname	Geräte mit Jailbreak/Rooting, Inaktive Geräte, Geräteregistrierung
LOCATION	Geografischer Standort des Geräts	Geräte & Apps
MANAGED	Gibt an, ob das Gerät verwaltet wird oder nicht	Geräte mit Jailbreak/Rooting
Modell	Gerätemodell	Geräte mit Jailbreak/Rooting, Inaktive Geräte,

		Geräteregistrierung, Apps nach Plattform
MODEL_NAME	Gerätemodell	Geräte & Apps
OS_VERSION	Version des Betriebssystems auf dem Gerät	Apps nach Geräten und Benutzer, Inaktive Geräte, Geräteregistrierung, Geräte & Apps
PHONE_NUMBER	Telefonnummer des Benutzers	Geräteregistrierung
PLATFORM	Geräteplattform	Apps nach Geräten und Benutzer, AGB, Geräte mit Jailbreak/Rooting, Inaktive Geräte, Geräteregistrierung, Geräte & Apps
SERIAL_NUMBER	Geräteseriennummer	Apps nach Geräten & Benutzer Geräte mit Jailbreak/Rooting, Inaktive Geräte, Geräte & Apps
USER EMAIL	E-Mail-Adresse des Benutzers	Apps nach Geräten & Benutzer
USER_ID	Eindeutige Benutzer-ID	Geräte & Apps
USER_NAME	Benutzername	Apps nach Geräten & Benutzer, AGB, Geräte & Apps
USERID	Benutzer-ID	Apps nach Geräten & Benutzer

Führen Sie die folgenden Schritte zur Erstellung eines Berichts aus:

1. Klicken Sie in der XenMobile-Konsole auf die Registerkarte **Analysieren** und dann auf **Berichterstellung**. Die Seite **Berichterstellung** wird angezeigt.



Apps by Devices & User

List of apps that users have on their devices.

Report Data: device serial number, device platform, version, user name, ID, email, # of apps, deployment status.

Terms & Conditions

List of accepted and declined Terms and Conditions agreements by device users.

Report Data: document name, created on, platform, user name, delivery group, acceptance status.

Top 25 Apps

List of apps most users have installed.

Report Data: app name, # of deployments, deployment status, type, category, deployment date, app owner.

Jailbroken/Rooted Devices

List of jailbroken iOS and rooted Android devices.

Report Data: device platform, model, version, serial number, user name, device mode, status.

Top 10 Apps - Failed Deployment

List of apps that have failed deployment.

Report Data: app name, # of deployments, deployment status, type, category, deployment date, app owner.

Inactive Devices

List of devices that have been inactive for a specified length of time.

Report Data: last activity, device mode, platform, version, user name, last authentication, device IMEI, serial number, model, first connection.

Apps by Type & Category

List of apps and app versions by app type (MDX, Public, Web & SaaS, Enterprise, Web Link) and defined categories.

Report Data: app name, version, # of deployments, deployment status, type, category, deployment date, app owner.

Device Enrollment

List of devices that have been enrolled during a specified length of time.

Report Data: first connection, device mode, platform, version, model, user name, last authentication, phone number.

Apps by Platform

List of apps and app versions installed on various device platforms and device versions.

Report Data: app name, version, # of deployments, deployment status, deployment date, app owner, device platform, version, model, model name.

Devices & Apps

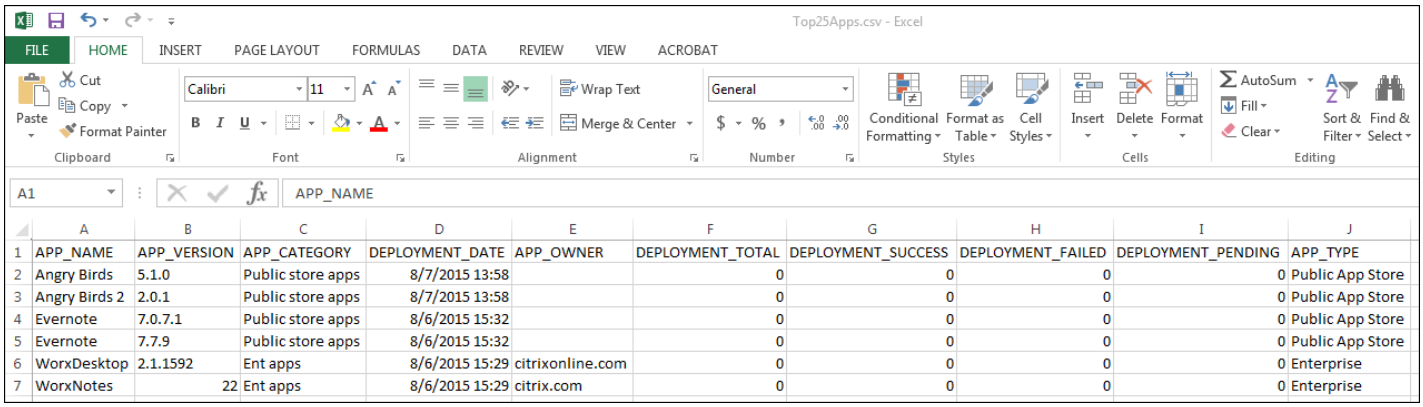
List of all devices, device data, and apps installed.

Report Data: device serial number, user name, ID, email, device platform, version, model, mode, status, last connection, enrollment status, enrollment date, device ownership, location, certificate expiration, app name, version, deployment status, type, category, deployment date, app owner, app ID.

2. Klicken Sie auf den gewünschten Bericht. Abhängig vom verwendeten Browser wird die Datei automatisch heruntergeladen oder Sie werden aufgefordert, die Datei zu speichern.

3. Wiederholen Sie Schritt 2 für jeden Bericht, den Sie erstellen möchten.

Nachfolgend wird das Beispiel des Berichts "Top 25 Apps" in Microsoft Excel gezeigt:



	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORY	DEPLOYMENT_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	Angry Birds	5.1.0	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
3	Angry Birds 2	2.0.1	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
4	Evernote	7.0.7.1	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
5	Evernote	7.7.9	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
6	WorxDesktop	2.1.1592	Ent apps	8/6/2015 15:29	citrixonline.com	0	0	0	0	Enterprise
7	WorxNotes	22	Ent apps	8/6/2015 15:29	citrix.com	0	0	0	0	Enterprise

Benachrichtigungen

Jul 28, 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 Automatisierte Aktionen.

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 Kommunikationssystemenfür Textnachrichten. Sie verwendet standardisierte Kommunikationsprotokolle für den Austausch kurzer Textnachrichten zwischen Festnetz- oder Mobiltelefonen.

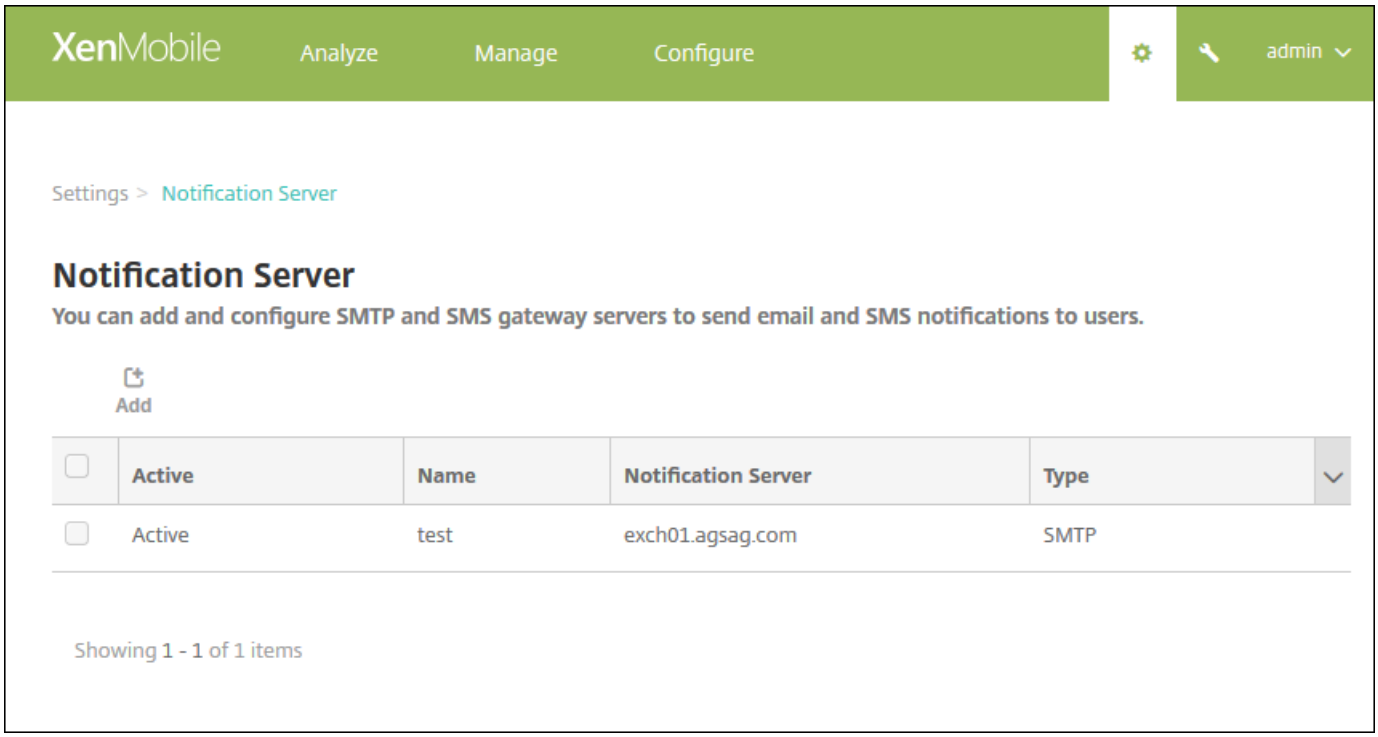
Sie können auch ein Netzbetreiber-SMS-Gateway in XenMobile einrichten, um Benachrichtigungen zu konfigurieren, die über das SMS-Gateway eines Netzbetreibers gesendet werden. Netzbetreiber nutzen SMS-Gateways für den Versand oder Empfang von Textnachrichten an bzw. von einem Telekommunikationsnetz. Standardisierte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

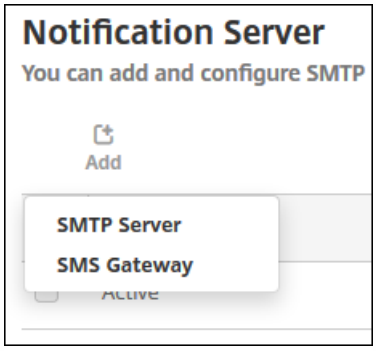
- Bringen Sie vor der Konfiguration des SMS-Gateways beim zuständigen Systemadministrator die Serverinformationen in Erfahrung. Wichtig ist, ob der SMS-Server auf einem internen Unternehmensserver gehostet wird oder Teil eines gehosteten E-Mail-Diensts ist. Im letzteren Fall benötigen Sie Informationen 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 das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

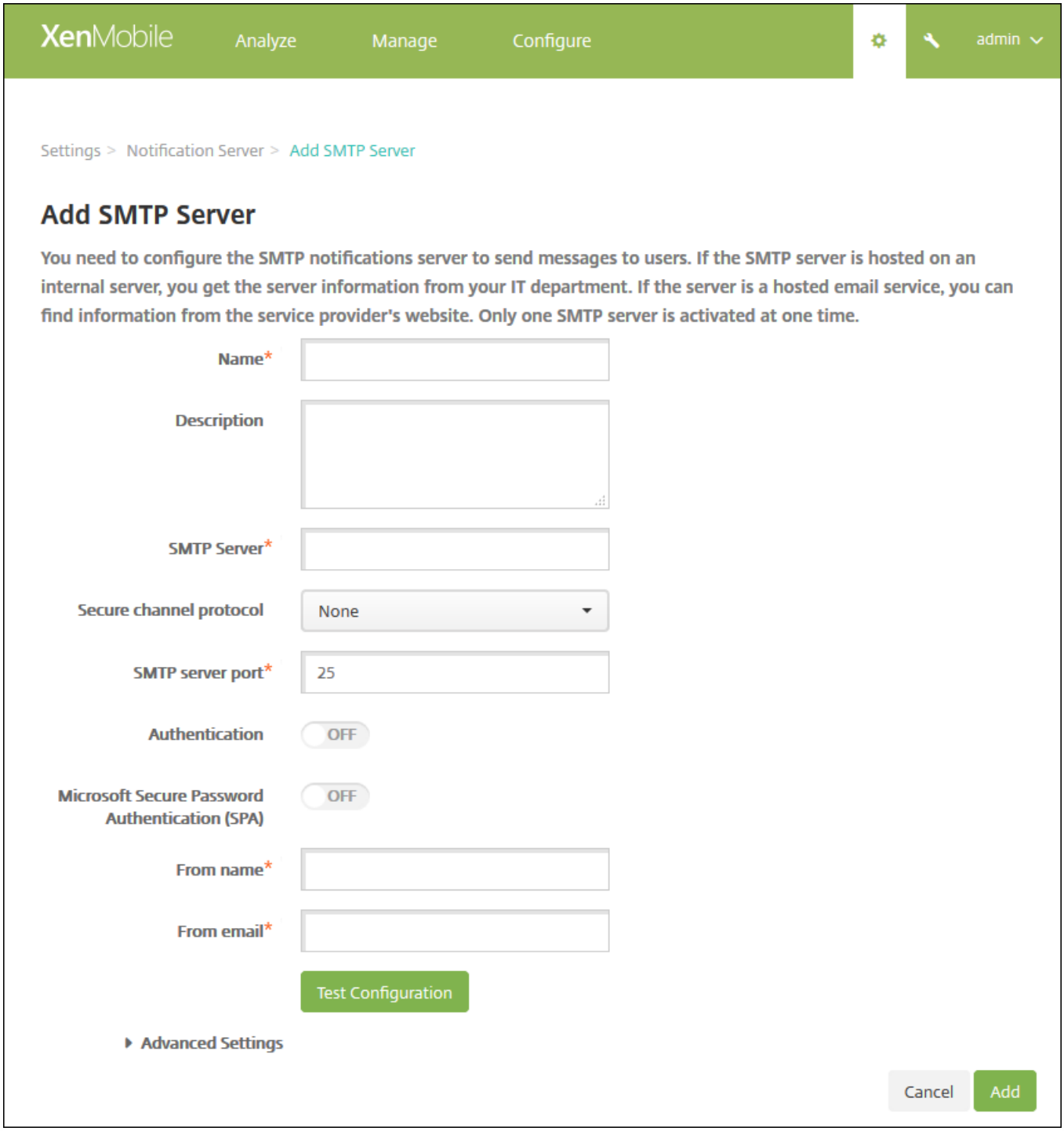
2. Klicken Sie unter **Benachrichtigungen** auf **Benachrichtigungsserver**. Die Seite **Benachrichtigungsserver** wird angezeigt.



2. Klicken Sie auf **Hinzufügen**. Ein Menü mit den Optionen zum Konfigurieren eines SMTP-Servers oder eines SMS-Gateways wird angezeigt.



- Zum Hinzufügen eines SMTP-Servers klicken Sie auf **SMTP-Server** und führen Sie die unter Hinzufügen eines SMTP-Servers aufgeführten Schritte aus, um diese Einstellung zu konfigurieren.
- Zum Hinzufügen eines SMS-Gateways klicken Sie auf **SMS-Gateway** und führen Sie die unter Hinzufügen eines SMS-Gateways aufgeführten Schritte aus, um diese Einstellung zu konfigurieren.



1. Konfigurieren Sie die folgenden Einstellungen:

- **Name**: Geben Sie den Namen des SMTP-Serverkontos ein.
- **Beschreibung**: 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-Protokoll**: Klicken Sie in der Liste auf **SSL**, **TLS** oder **Ohne**, um das von dem Server verwendete Protokoll (sofern dieser für die sichere Authentifizierung konfiguriert ist) anzugeben. Der Standardwert ist **Ohne**.
- **SMTP-Serverport**: 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.

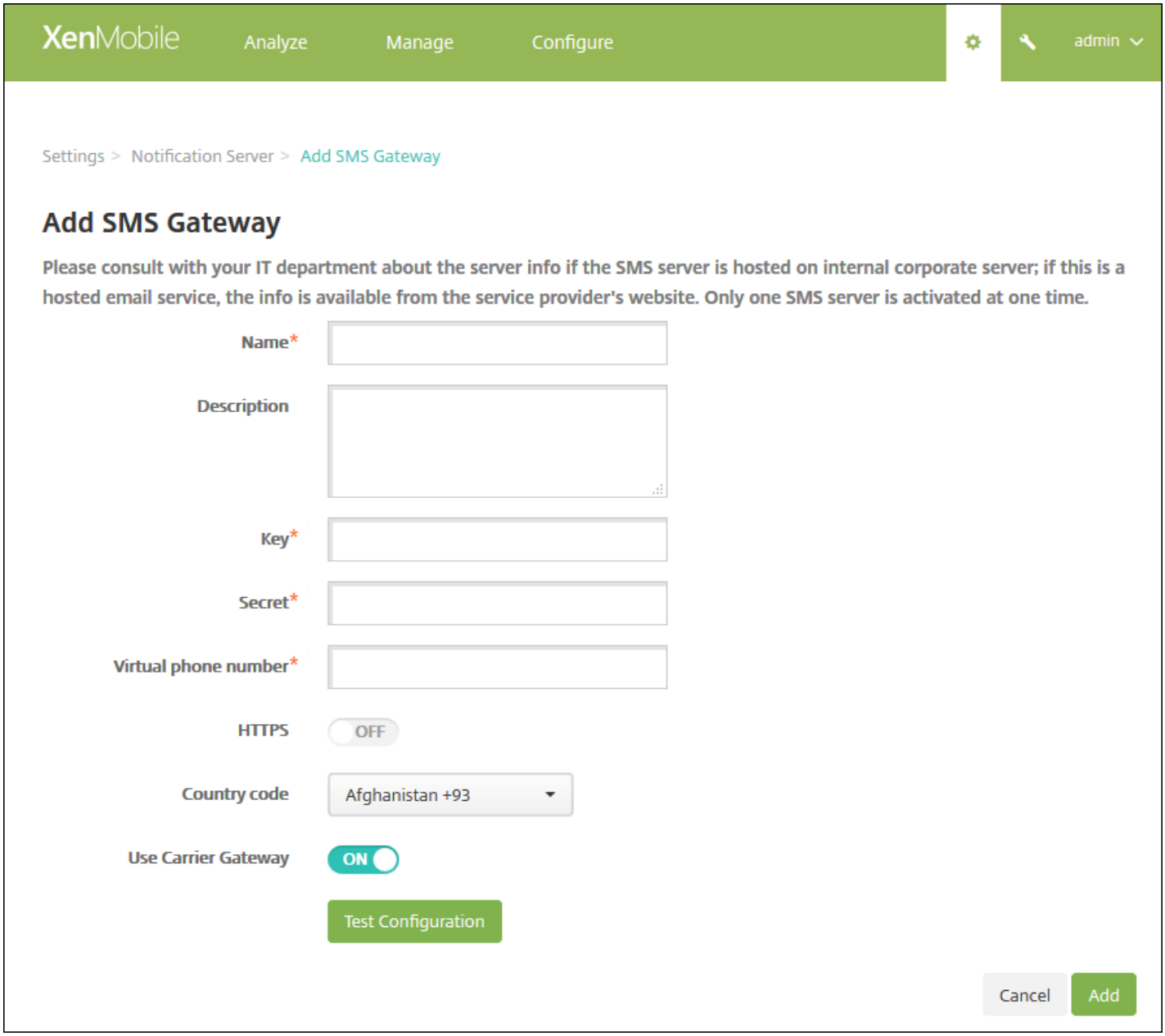
- **Authentifizierung**: Wählen Sie **EIN** oder **AUS**. Der Standardwert ist **AUS**.
- Wenn Sie **Authentifizierung** aktivieren, konfigurieren Sie die folgenden Einstellungen:
  - **Benutzername**: Geben Sie den Benutzernamen für die Authentifizierung ein.
  - **Kennwort**: Geben Sie das Kennwort des Benutzers für die Authentifizierung ein.
- **Microsoft Gesicherte Kennwortauthentifizierung (SPA)**: Wenn für den SMTP-Server SPA verwendet wird, klicken Sie auf **EIN**. Der Standardwert ist **AUS**.
- **Von (Name)**: Geben Sie den Namen ein, der in Benachrichtigungs-E-Mails von diesem Server im Absenderfeld angezeigt werden soll. Beispiel: IT-Abteilung.
- **Von (E-Mail)**: Geben Sie die E-Mail-Adresse ein, die verwendet werden soll, wenn eine E-Mail Empfänger auf eine Benachrichtigung vom SMTP-Server antwortet.

2. Klicken Sie auf **Konfiguration testen**, um eine Test-E-Mail zu senden.

3. Erweitern Sie **Erweiterte Einstellungen** und konfigurieren Sie folgende Einstellungen:

- **Anzahl SMTP-Versuche**: Geben Sie die Anzahl wiederholter Sendeversuche für fehlgeschlagene Nachrichten vom SMTP-Server ein. Der Standardwert 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. Der Standardwert ist 30 Sekunden.
- **Anzahl SMTP-Empfänger maximal**: Geben Sie die maximale Anzahl Empfänger pro E-Mail-Nachricht vom SMTP-Server ein. Der Standardwert ist 100.

4. Klicken Sie auf **Hinzufügen**.



Hinweis

XenMobile unterstützt für Textnachrichten nur Nexmo. Wenn Sie noch kein Konto für Nexmo Messaging haben, erstellen Sie eines auf der Nexmo-Website.

1. Konfigurieren Sie die folgenden Einstellungen:

- **Name**: Geben Sie einen eindeutigen Namen für die SMS-Gateway-Konfiguration ein. Diese Angabe ist erforderlich.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Konfiguration ein.
- **Schlüssel**: Geben Sie den numerischen Bezeichner ein, der vom Systemadministrator bereitgestellt wird, wenn das Konto aktiviert wird. Diese Angabe ist erforderlich.
- **Geheimnis**: Geben Sie den vom Systemadministrator bereitgestellten Schlüssel ein, mit dem Sie im Fall eines Verlusts oder

Diebstahls des Kennworts auf das Konto zugreifen können. Diese Angabe ist erforderlich.

- **Virtuelle Telefonnummer**: 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 aus, ob für die Übermittlung von SMS-Anforderungen an Nexmo HTTPS verwendet werden soll. Der Standardwert ist **AUS**.
- **Ländercode**: Klicken Sie in der Liste auf die Standard-SMS-Ländervorwahl für Empfänger in Ihrem Unternehmen. Dieses Feld beginnt immer mit +. Der Standardwert ist **Afghanistan +93**.

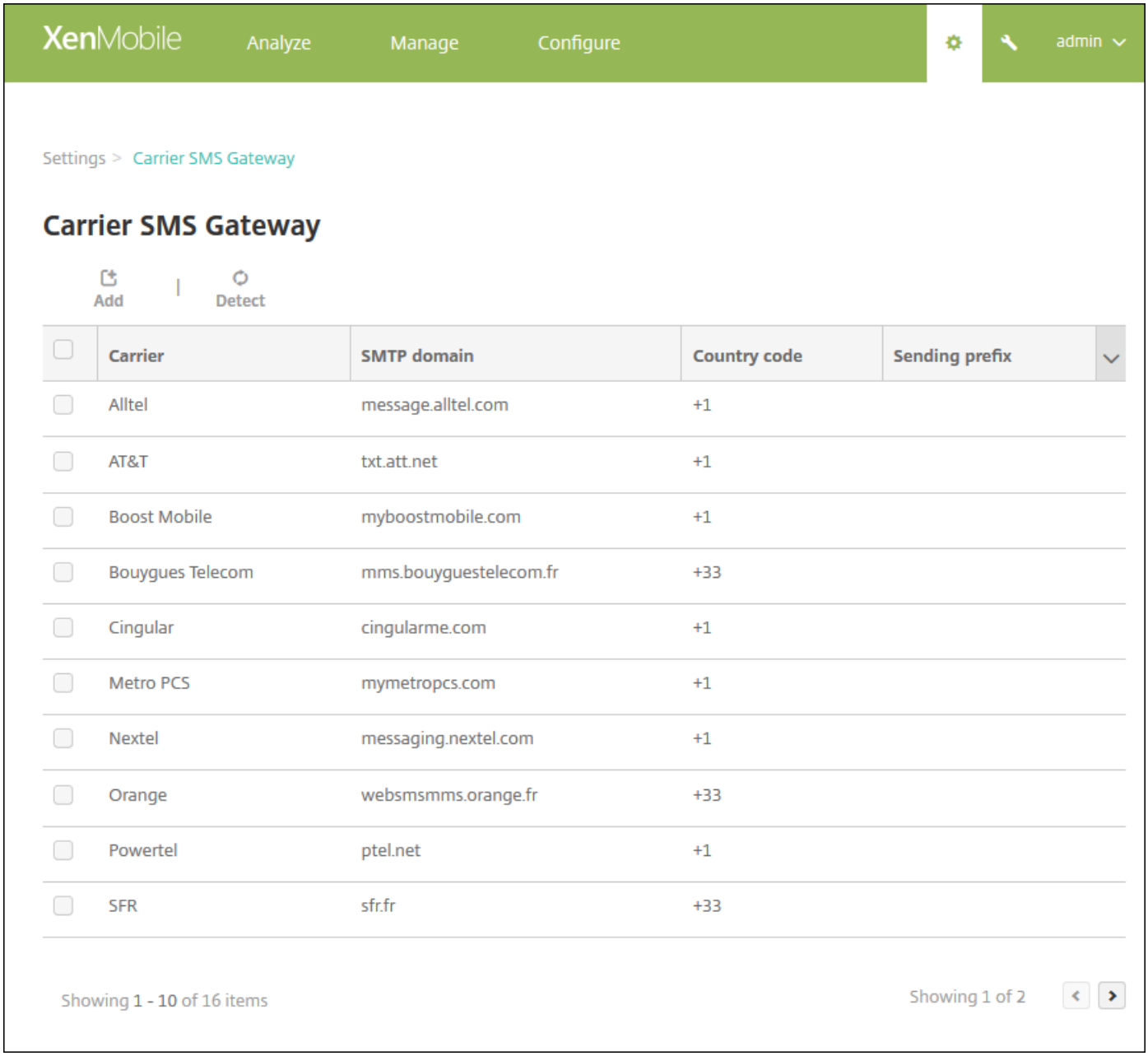
2. Klicken Sie auf **Konfiguration testen**, um eine E-Mail zum Testen der neuen Konfiguration zu senden. Authentifizierungsfehler, Fehler bei der virtuellen Telefonnummer und andere Verbindungsfehler, werden sofort erkannt und gemeldet. Die Übermittlung von Nachrichten dauert ungefähr so lange wie bei Mobiltelefonen.

2. Klicken Sie auf **Hinzufügen**.

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.

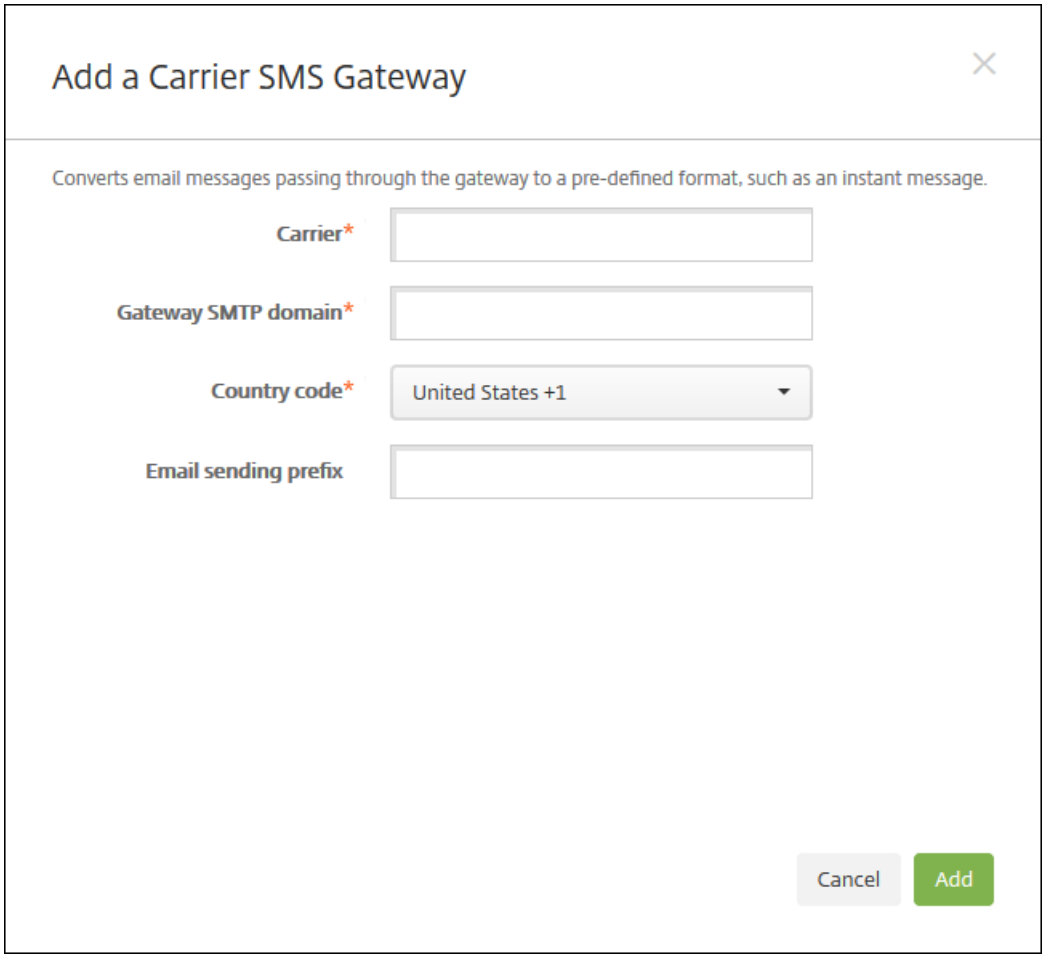
1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Benachrichtigungen** auf **Netzbetreiber-SMS-Gateway**. Die Seite **Netzbetreiber-SMS-Gateway** wird geöffnet.



3. Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf **Ermitteln**, um automatisch ein Gateway zu ermitteln. Ein Dialogfeld wird angezeigt, in dem die bei den registrierten Geräten gefundenen neuen Netzbetreiber aufgelistet werden. Wurden keine Netzbetreiber gefunden, enthält das Dialogfeld eine entsprechende Meldung.
- Klicken Sie auf **Hinzufügen**. Das Dialogfeld **SMS-Gateway des Netzbetreibers hinzufügen** 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.

4. Konfigurieren Sie die folgenden Einstellungen:

- **Netzbetreiber**: Geben Sie den Namen des Netzbetreibers ein.
- **Gateway-SMTP-Domäne**: Geben Sie die dem SMTP-Gateway zugeordnete Domäne an.
- **Ländercode**: Klicken Sie in der Liste auf die Landeskennzahl des Netzbetreibers.
- **E-Mail-Sendepräfix**: Geben Sie optional ein Präfix für den E-Mail-Versand ein.

5. Klicken Sie auf **Hinzufügen**, um den neuen Netzbetreiber hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

NetScaler Gateway und XenMobile

Oct 13, 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 über für XenMobile unterstützte Versionen von NetScaler Gateway finden Sie unter XenMobile Compatibilty. Weitere Informationen zum Einrichten von NetScaler Gateway für XenMobile auf NetScaler finden Sie unter Configuring Settings for Your XenMobile Environment.

Authentifizierung

Bei der Authentifizierung in XenMobile spielen verschiedene Komponenten eine Rolle:

- **XenMobile-Server**: Auf dem XenMobile-Server definieren Sie die Sicherheit für die Registrierung und die Registrierungserfahrung. Optionen zum Onboarding von Benutzern umfassen den Umfang der Registrierung, d. h. ob sie für alle offen ist oder nur bei Einladung und ob zwei- oder dreistufige Authentifizierung erforderlich ist. Sie können in den Clienteigenschaften in XenMobile die Authentifizierung mit Worx-PIN aktivieren und die Komplexität sowie das Ablaufdatum der PIN konfigurieren.
- **NetScaler**: NetScaler bietet Beendigung für SSL-Sitzungen mit Micro VPN, In-Transit-Netzwerksicherheit und ermöglicht das Definieren der Authentifizierungserfahrung für den Benutzerzugriff auf Apps.
- **Worx Home**: Worx Home wird vom XenMobile-Server für Registrierungsvorgänge verwendet. Worx Home ist auf einem Gerät die Entität, die mit NetScaler kommuniziert: Wenn eine Sitzung abläuft, erhält Worx Home ein Authentifizierungsticket von NetScaler und gibt das Ticket an die MDX-Apps weiter. Citrix empfiehlt, Zertifikatpinning zu verwenden, um Man-in-the-middle-Angriffe zu verhindern. Weitere Informationen finden Sie im Abschnitt über Zertifikatpinning im Artikel über Worx Home.

  Worx Home unterstützt zudem den MDX-Sicherheitscontainer: Worx Home stellt Richtlinien per Push bereit, erstellt eine neue Sitzung mit NetScaler, wenn ein Timeout für eine App auftritt, und definiert die Benutzererfahrung für MDX-Timeout und -Authentifizierung. Worx Home ist zudem verantwortlich für die Erkennung von Jailbreaks, Geolocation-Prüfungen und angewendeten Richtlinien.

- **MDX-Richtlinien**: MDX-Richtlinien erstellen einen Datentresor auf dem Gerät. MDX-Richtlinien leiten Micro VPN-Verbindungen zurück zu NetScaler, erzwingen Offlinemoduseinschränkungen und Clientrichtlinien, wie Timeouts.

Weitere Informationen zur Authentifizierung, einschließlich einstufige und zweistufige Authentifizierungsmethoden, mit der Authentifizierung verbundene Richtlinien, Einstellungen und Clienteigenschaften sowie Beispiele für drei XenMobile-Konfigurationen mit verschiedenen Sicherheitsstufen finden Sie unter Authentifizierung.

Weitere Informationen zur Konfiguration finden Sie in den folgenden Artikeln:

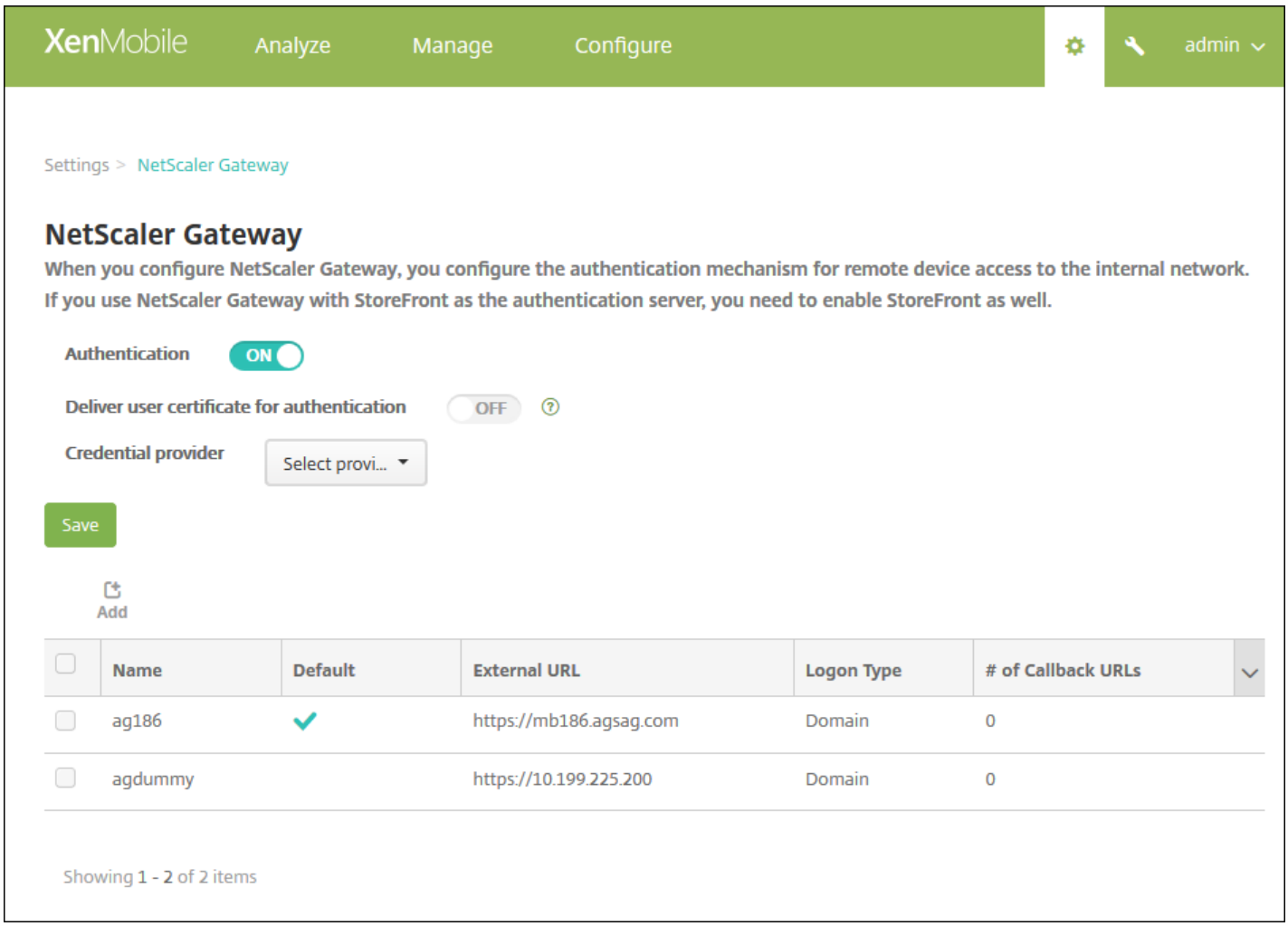
Konfigurieren von Authentifizierung mit Domäne und Sicherheitstoken

Konfigurieren der Clientzertifikatauthentifizierung

Configuring XenMobile for Certificate and Security Token Authentication

1. Klicken Sie in der XenMobile-Webkonsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **NetScaler Gateway**. Die Seite **NetScaler Gateway** wird angezeigt.



Konfigurieren Sie folgende Einstellungen:

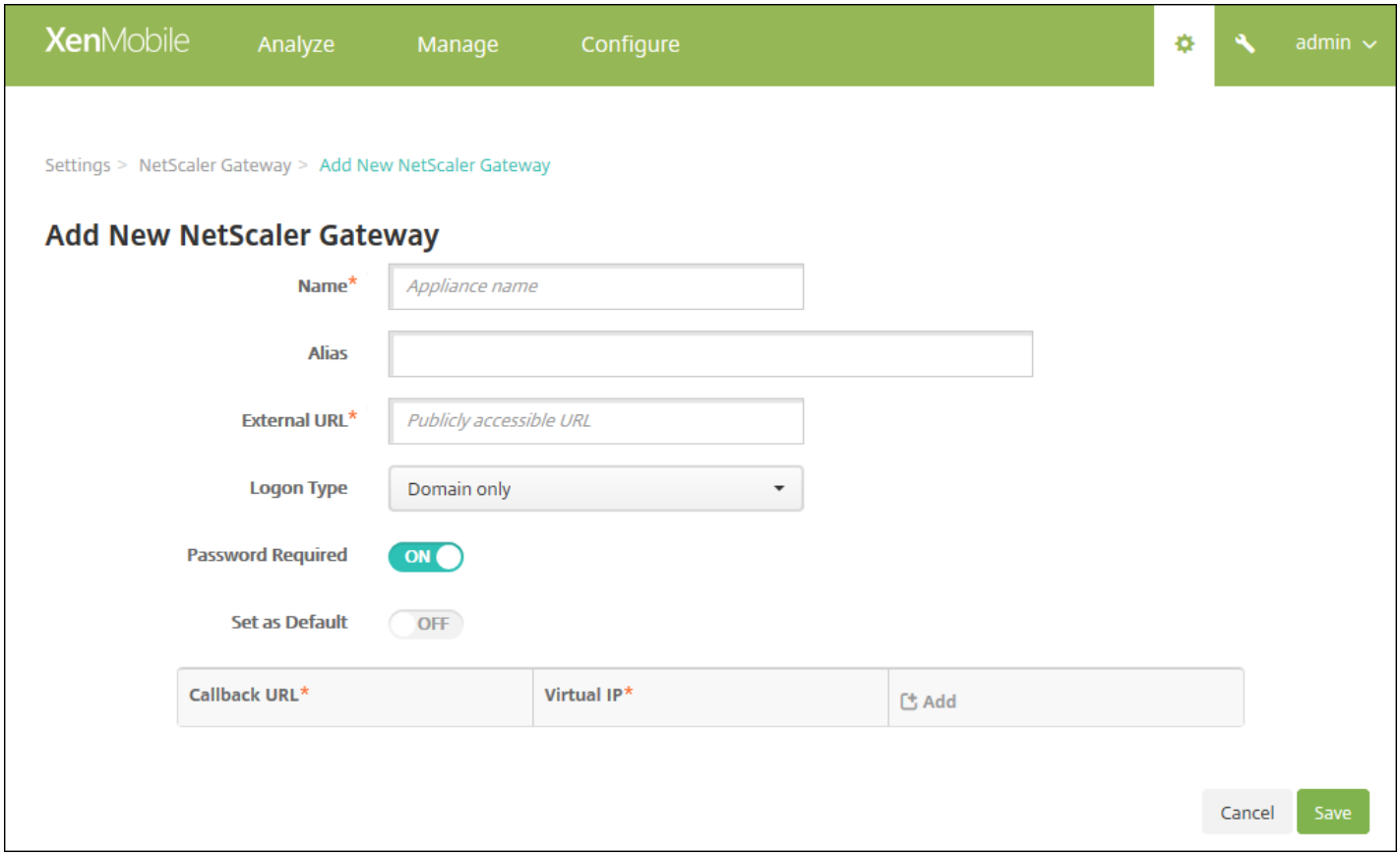
- **Authentifizierung**: Wählen Sie aus, ob die Authentifizierung aktiviert werden soll. Der Standardwert ist **EIN**.
- **Benutzerzertifikat für Authentifizierung bereitstellen**: Wählen Sie aus, ob XenMobile das Authentifizierungszertifikat zusammen mit Worx Home verwenden soll, sodass NetScaler Gateway die Clientzertifikatauthentifizierung abwickelt. Der Standardwert ist **AUS**.
- **Anmeldeinformationsanbieter**: Klicken Sie in der Liste auf den gewünschten Anmeldeinformationsanbieter. Weitere Informationen finden Sie unter Anmeldeinformationsanbieter.

3. Klicken Sie auf **Speichern**.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **NetScaler Gateway**. Die Seite **NetScaler Gateway** wird angezeigt.

3. Klicken Sie auf **Hinzufügen**. Die Seite **Neues NetScaler Gateway hinzufügen** wird angezeigt.



4. Konfigurieren Sie die folgenden Einstellungen:

- **Name**: Geben Sie einen Namen für die NetScaler Gateway-Instanz ein.
- **Alias**: Geben Sie optional ein Alias ein.
- Externe URL: Geben Sie die öffentlich zugängliche URL für NetScaler Gateway ein. Beispiel: https://receiver.com.
- **Anmeldetyp**: Klicken Sie in der Liste auf einen Anmeldetyp. Zur Auswahl stehen **Nur Domäne**, **Nur Sicherheitstoken**, **Domäne und Sicherheitstoken**, **Zertifikat**, **Zertifikat und Domäne** und **Zertifikat und Sicherheitstoken**. Der Standardwert ist **Nur Domäne**.

  Wenn Sie mehrere Domänen haben, funktioniert **Nur Domäne** nicht, sondern Sie müssen **Zertifikat und Domäne** verwenden. Bei einigen Optionen, z. B. **Nur Domäne**, können Sie das Feld **Kennwort** nicht ändern.

  Bei diesem Anmeldetyp gilt für das Feld immer die Einstellung **EIN**. Außerdem ändern sich die Standardwerte des Felds **Kennwort erforderlich** je nach der Auswahl unter **Anmeldetyp**.

  Wenn Sie **Zertifikat und Sicherheitstoken** verwenden, müssen Sie zur Unterstützung von Worx Home einige zusätzliche Konfigurationen auf dem NetScaler Gateway ausführen. Weitere Informationen finden Sie unter Configuring XenMobile for Certificate and Security Token Authentication.
- **Kennwort erforderlich**: Wählen Sie aus, ob die Kennwortauthentifizierung erzwungen werden soll. Der Standardwert ist **EIN**.

- **Als Standard setzen**: Wählen Sie aus, ob die NetScaler Gateway-Instanz als Standard verwendet werden soll. Der Standardwert ist **AUS**.

5. 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 **Hinzufügen**. Die Seite **Neues NetScaler Gateway hinzufügen** wird angezeigt.

2. Klicken Sie in der Tabelle mit den Callback-URLs auf **Hinzufügen**.

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

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

Konfigurieren von LDAP

Aug 22, 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.

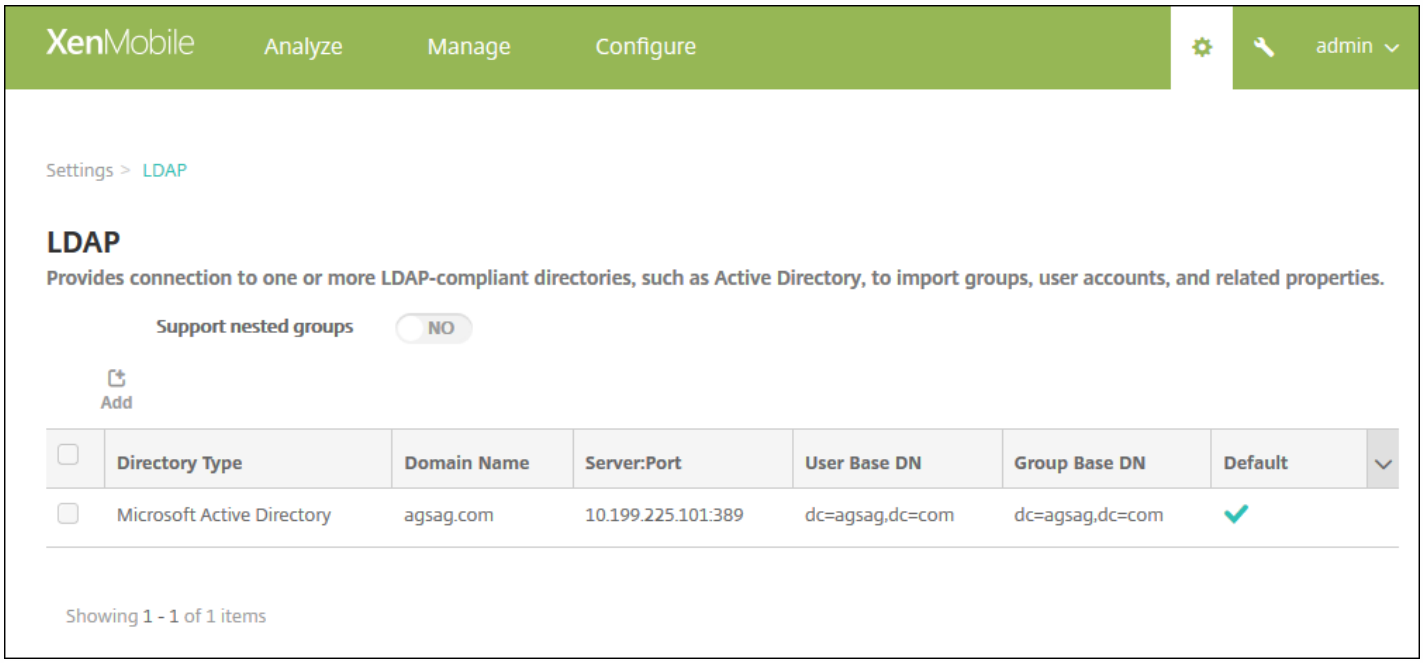
Funktionsweise von LDAP

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.

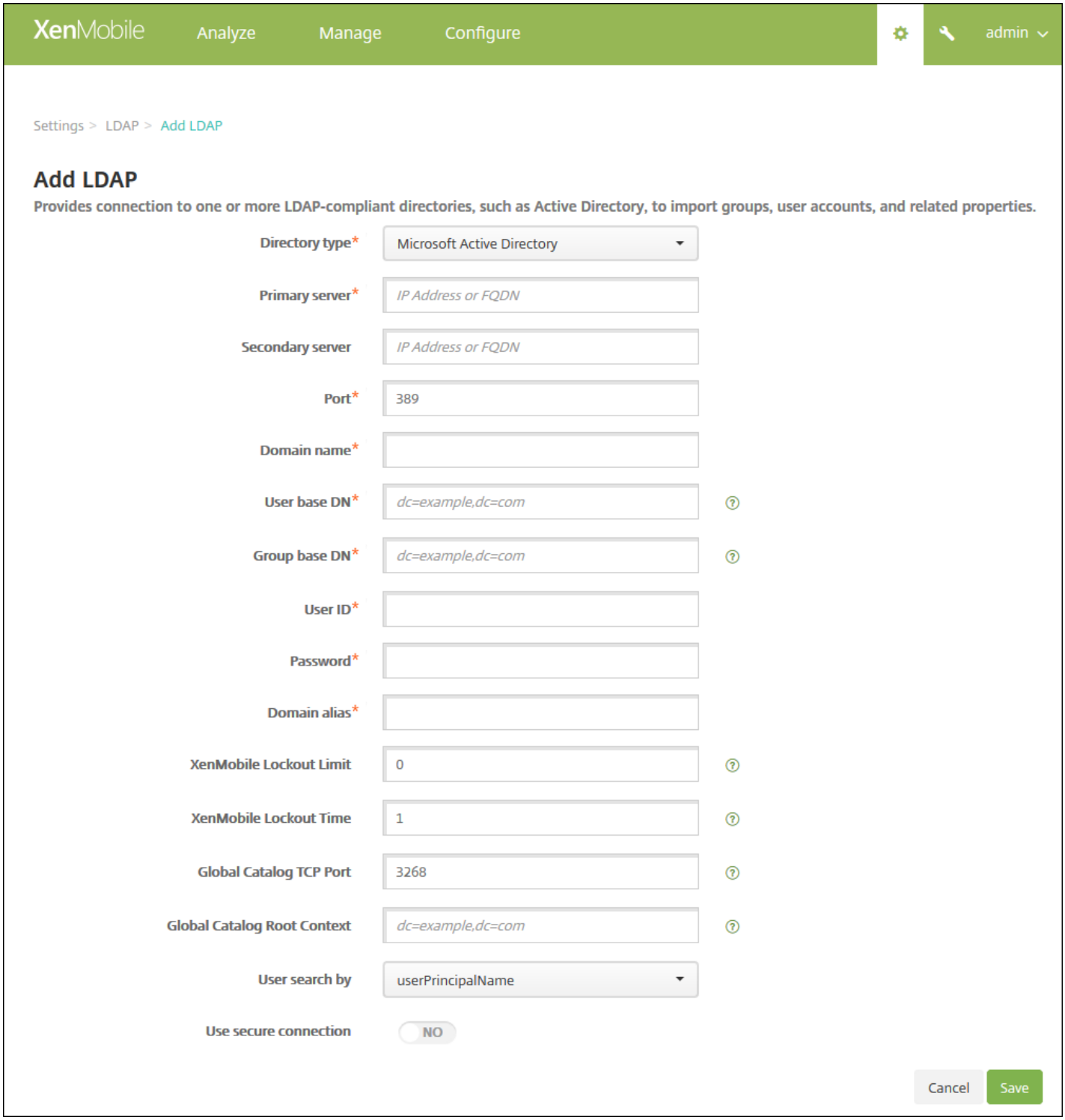
Konfigurieren von LDAP-Verbindungen in XenMobile

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **LDAP**. Die Seite **LDAP** wird angezeigt. Auf dieser Seite können Sie LDAP-konforme Verzeichnisse hinzufügen, bearbeiten und löschen.



1. Klicken Sie auf der Seite **LDAP** auf **Hinzufügen**. Die Seite **LDAP hinzufügen** wird angezeigt.



2. Konfigurieren Sie die folgenden Einstellungen:

- **Verbindungstyp**: Klicken Sie in der Liste auf den Verbindungstyp. Der Standardwert ist **Microsoft Active Directory**.
- **Primärer Server**: Geben Sie den für LDAP verwendeten primären Server an. Sie können die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) eingeben.
- **Sekundärer 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.

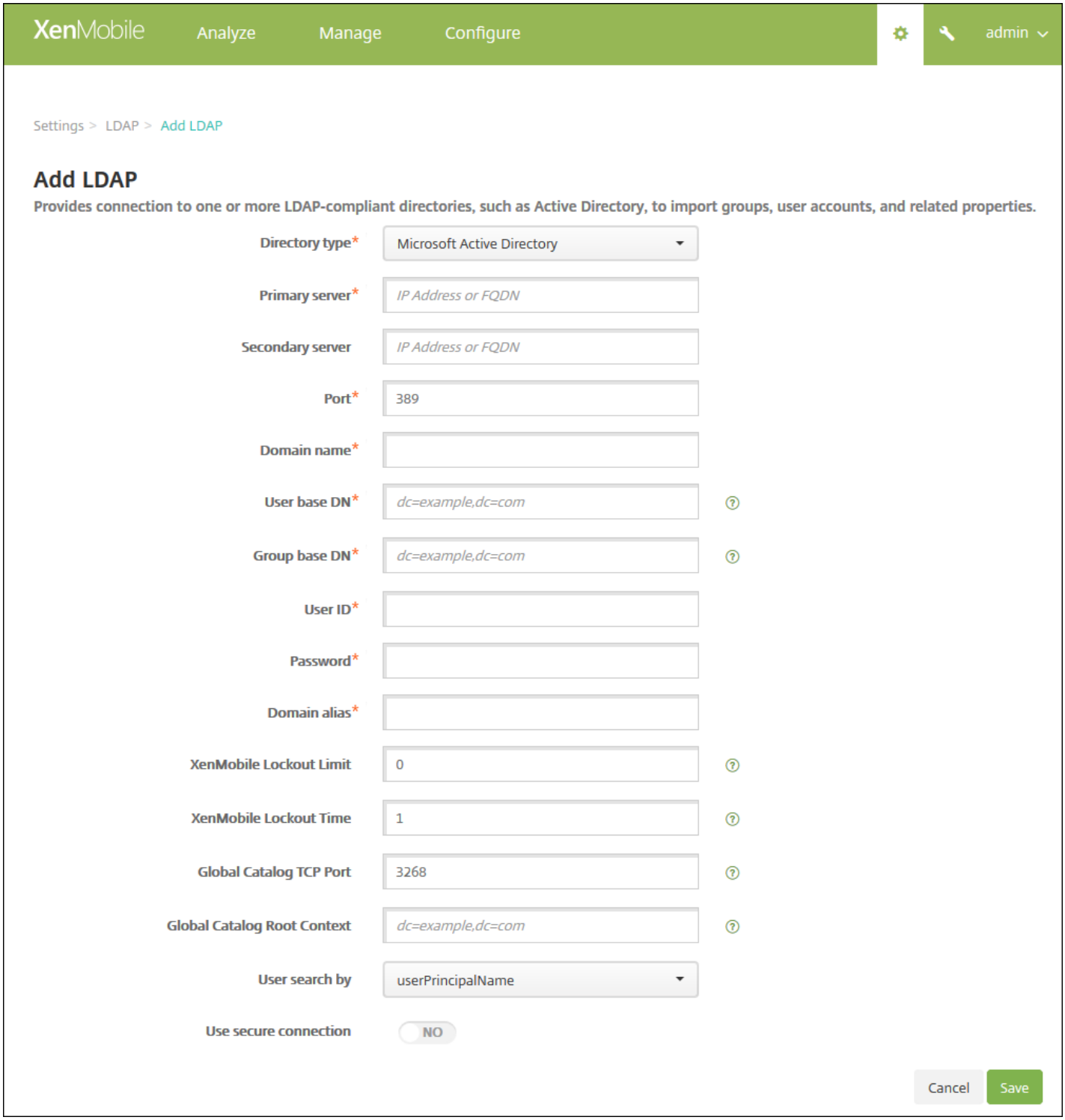
- **Domänenname**: Geben Sie den Domänennamen ein.
- **Basis-DN für Benutzer**: Geben Sie den Speicherort von Benutzern in Active Directory über einen eindeutigen Bezeichner ein. Syntaxbeispiele: ou=users, dc=example oder dc=com.
- **Basis-DN für Gruppen**: Geben Sie den Gruppen-Basis-DN-Namen gemäß 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.
- **Benutzer-ID**: Geben Sie die dem Active Directory-Konto zugeordnete Benutzer-ID ein.
- **Kennwort**: Geben Sie das dem Benutzer zugeordnete Kennwort ein.
- **Domänenalias**: Geben Sie ein Alias für den Domänennamen ein.
- **XenMobile-Sperrlimit**: 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-Sperrzeitraum**: 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.
- **TCP-Port für globalen Katalog**: 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.
- **Stammkontext für globalen Katalog**: 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.
- **Benutzersuche nach**: Klicken Sie in der Liste auf **userprincipalname** oder **sAMAccountName**. Der Standardwert ist **userprincipalname**.
- **Sichere Verbindung verwenden**: Wählen Sie aus, ob sichere Verbindungen verwendet werden sollen. Die Standardeinstellung ist **NEIN**.

3. Klicken Sie auf **Speichern**.

1. Wählen Sie in der Tabelle **LDAP** das gewünschte Verzeichnis aus.

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

2. Klicken Sie auf **Bearbeiten**. Die Seite **LDAP hinzufügen** wird angezeigt.



3. Ändern Sie nach Bedarf die folgenden Informationen:

- **Verbindungstyp**: Klicken Sie in der Liste auf den Verbindungstyp .
- **Primärer Server**: Geben Sie den für LDAP verwendeten primären Server an. Sie können die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) eingeben.
- **Sekundärer 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.

- **Domänenname**: Sie können dieses Feld nicht ändern.
- **Basis-DN für Benutzer**: Geben Sie den Speicherort von Benutzern in Active Directory über einen eindeutigen Bezeichner ein. Syntaxbeispiele: ou=users, dc=example oder dc=com.
- **Basis-DN für Gruppen**: 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.
- **Benutzer-ID**: Geben Sie die dem Active Directory-Konto zugeordnete Benutzer-ID ein.
- **Kennwort**: Geben Sie das dem Benutzer zugeordnete Kennwort ein.
- **Domänenalias**: Geben Sie ein Alias für den Domänennamen ein.
- **XenMobile-Sperrlimit**: 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-Sperrzeitraum**: 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.
- **TCP-Port für globalen Katalog**: 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.
- **Stammkontext für globalen Katalog**: 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.
- **Benutzersuche nach**: Klicken Sie in der Liste auf **userprincipalname** oder **sAMAccountName**.
- **Sichere Verbindung verwenden**: Wählen Sie aus, ob sichere Verbindungen verwendet werden sollen.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um die Eigenschaft unverändert zu lassen.

1. Wählen Sie in der Tabelle **LDAP** das gewünschte Verzeichnis aus.

Hinweis: Sie können mehrere Eigenschaften auswählen, indem Sie die Kontrollkästchen daneben aktivieren.

2. Klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie noch einmal auf **Löschen**.

Konfigurieren von Authentifizierung mit Domäne und Sicherheitstoken

Oct 13, 2016

Sie können XenMobile konfigurieren, sodass Benutzer sich mit ihren LDAP-Anmeldeinformationen und einem Einmalkennwort authentifizieren müssen. Dabei wird das RADIUS-Protokoll verwendet.

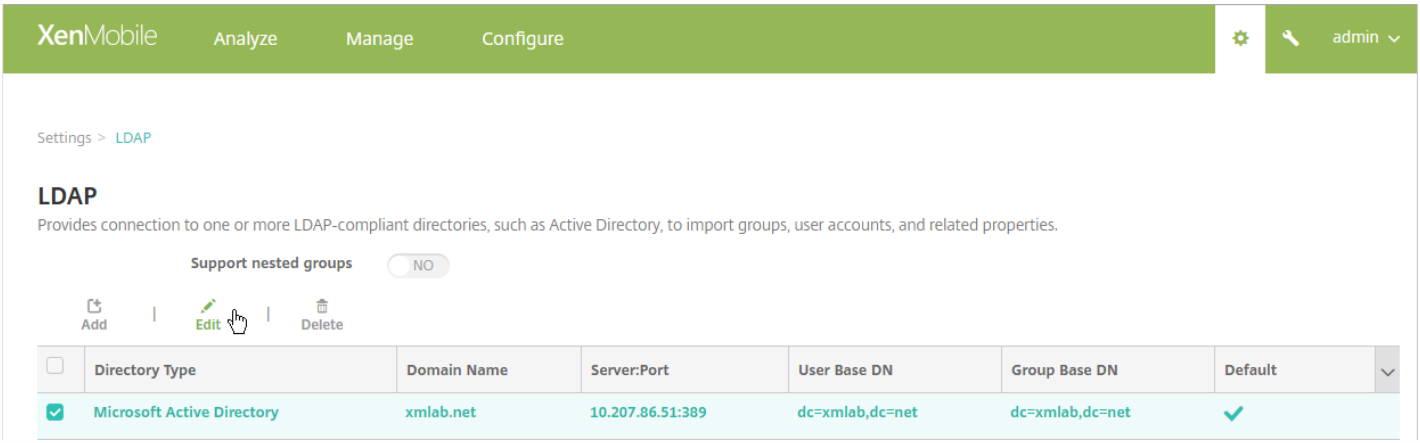
Für optimale Benutzerfreundlichkeit können Sie diese Konfiguration mit der Worx-PIN und der Active Directory-Kennwortzwischenspeicherung kombinieren, damit Benutzer ihre Active Directory-Benutzernamen und -Kennwörter nicht wiederholt eingeben müssen. Benutzer müssen Benutzernamen und Kennwörter für die Registrierung sowie bei Kennwortablauf und Kontosperrung eingeben.

Konfigurieren von LDAP-Einstellungen

Die Verwendung von LDAP zur Authentifizierung erfordert die Installation eines SSL-Zertifikats von einer Zertifizierungsstelle in XenMobile. Weitere Informationen finden Sie unter Hochladen von Zertifikaten in XenMobile.

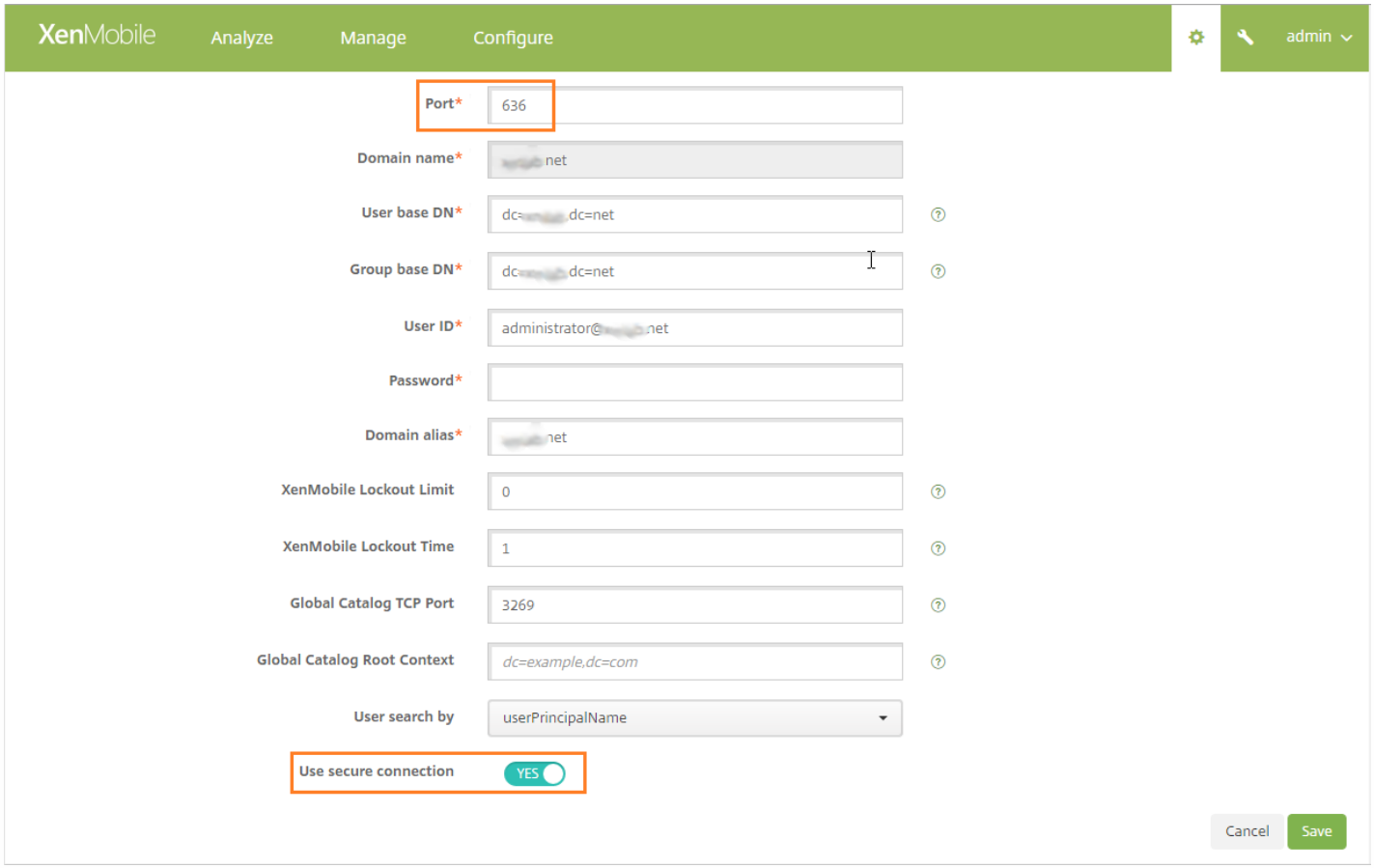
1. Klicken Sie in **Einstellungen** auf **LDAP**.

2. Wählen Sie **Microsoft Active Directory** und klicken Sie auf **Bearbeiten**.



3. Überprüfen Sie, ob der **Port** auf **636** für sichere LDAP-Verbindungen oder auf **3269** für sichere Microsoft LDAP-Verbindungen festgelegt ist.

4. Legen Sie **Sichere Verbindung verwenden** auf **Ja** fest.



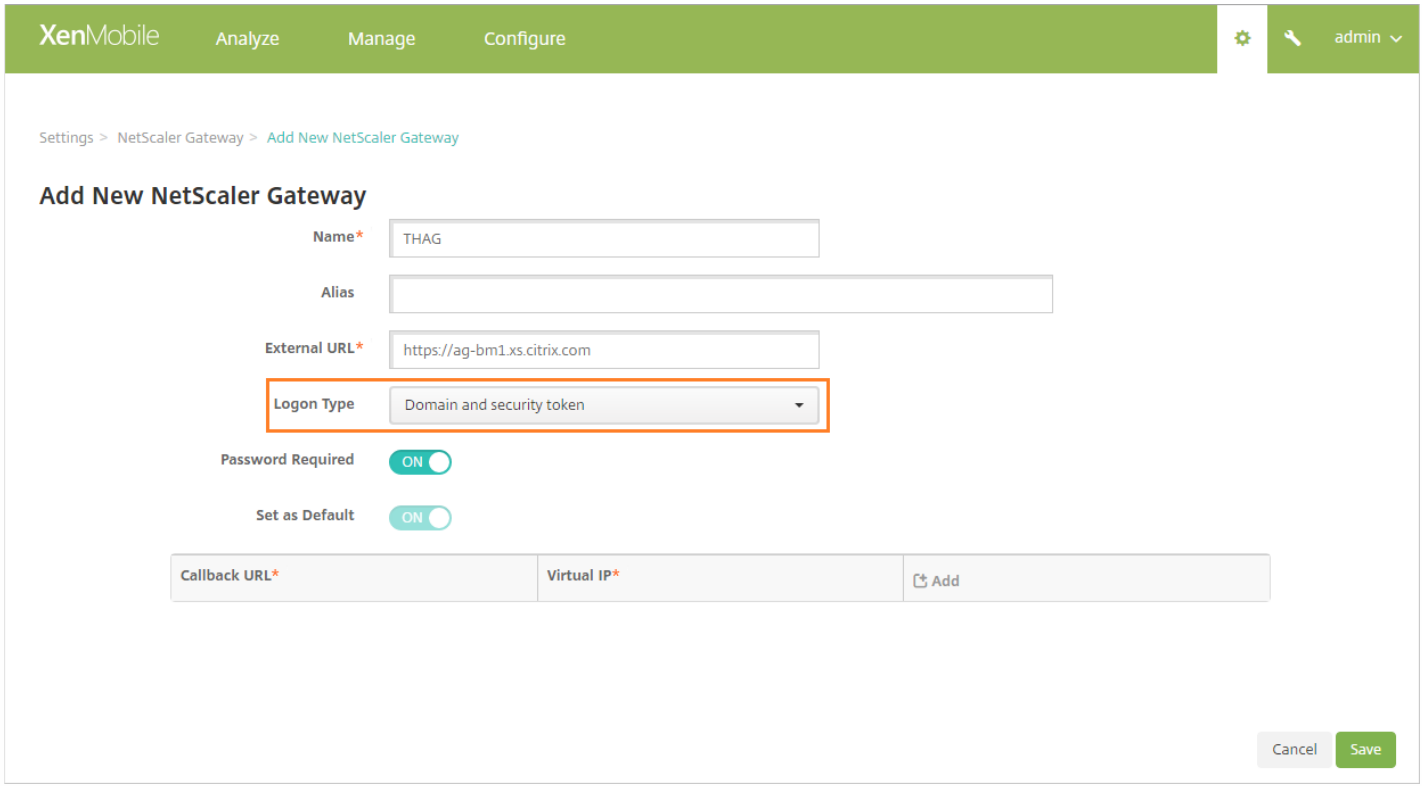
Konfigurieren der NetScaler Gateway-Einstellungen

Für die folgenden Schritte wird angenommen, dass Sie XenMobile bereits eine NetScaler Gateway-Instanz hinzugefügt haben. Anweisungen zum Hinzufügen einer NetScaler Gateway-Instanz finden Sie unter NetScaler Gateway und XenMobile.

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

2. Wählen Sie den NetScaler Gateway und klicken Sie auf **Bearbeiten**.

3. Wählen Sie unter **Anmeldetyp** die Option **Domäne und Sicherheitstoken**.



Aktivieren von Worx-PIN und Active Directory-Kennwortzwischenspeicherung

Um Worx-PIN und Active Directory-Kennwortzwischenspeicherung zu aktivieren, gehen Sie zu **Einstellungen** > **Clienteigenschaften** und aktivieren Sie die Kontrollkästchen **Enable Worx PIN Authentication** und **Enable User Password Caching**. Weitere Informationen finden Sie unter Referenz der Clienteigenschaften.

Konfigurieren von NetScaler Gateway für die Authentifizierung mit Domäne und Sicherheitstoken

Konfigurieren Sie NetScaler Gateway-Sitzungsprofile und Richtlinien für die virtuellen Server, die mit XenMobile verwendet werden. Weitere Informationen finden Sie in der NetScaler Gateway-Dokumentation unter Configuring Domain and Security Token Authentication for XenMobile.

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.

Die Clientzertifikatauthentifizierung bietet zusätzliche Sicherheit für mobile Apps und ermöglicht den Benutzern den direkten Zugriff auf HDX-Apps. Wenn die Clientzertifikatauthentifizierung konfiguriert ist, geben die Benutzer ihre Worx-PIN für den Single Sign-On-Zugriff auf Worx-aktivierte Apps ein. Worx-PIN vereinfacht zudem die Benutzerauthentifizierung. Mit Worx-PIN können Clientzertifikate gesichert oder Active Directory-Anmeldeinformationen lokal auf einem Gerät gespeichert werden.

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. Mit dem folgenden openssl-Befehl erstellen Sie eine PFX-Datei aus einer PEM-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.

In der XenMobile-Umgebung ist eine Kombination aus Clientzertifikat- und LDAP- Authentifizierung die beste Lösung für Sicherheit und Benutzererfahrung, da sie die besten SSO-Möglichkeiten mit der zweistufigen Authentifizierung über NetScaler vereint. Die Verwendung von Clientzertifikat und LDAP bietet Sicherheit durch etwas, das Benutzer wissen (Active Directory-Kennwort) und etwas, das sie haben (Clientzertifikat auf ihrem Gerät). In WorxMail (und einigen anderen Worx-Apps) kann eine nahtlose Benutzererfahrung bei der Erstverwendung mit Clientzertifikatauthentifizierung und einer ordnungsgemäß konfigurierten Exchange-Clientzugriffsserverumgebung automatisch konfiguriert und bereitgestellt werden. Die optimale Benutzerfreundlichkeit erreichen Sie, wenn Sie diese Option mit der Worx-PIN und der Active Directory-Kennwortzwischenspeicherung kombinieren.

Die Clientzertifikatauthentifizierung basiert auf den Attributen des Clientzertifikats, das dem virtuellen Server präsentiert wird. Sie müssen ein Stammzertifikat an den virtuellen Server von NetScaler Gateway binden. Wenn sich Benutzer bei NetScaler Gateway anmelden, wird der Benutzername 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.

Hinweise:

- Die Clientzertifikatauthentifizierung kann zusammen mit einem anderen Authentifizierungstyp wie etwa RADIUS verwendet werden.
- 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.
- In WorxMail (und einigen anderen Worx-Apps) kann eine nahtlose Benutzererfahrung bei der Erstverwendung mit Clientzertifikatauthentifizierung und einer ordnungsgemäß konfigurierten Exchange-Clientzugriffsserverumgebung automatisch konfiguriert und bereitgestellt werden. Die optimale Benutzerfreundlichkeit erreichen Sie, wenn Sie diese Option mit der Worx-PIN und der Active Directory-Kennwortzwischenspeicherung kombinieren.
- Geräteauthentifizierung mit NetScaler Gateway wird nicht für Zertifikate unterstützt, die über eine eigenverwaltete Zertifizierungsstelle abgerufen wurden.
- XenMobile unterstützt keine Clientzertifikatauthentifizierung für gemeinsam genutzte Geräte.

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 vom XenMobile-Server 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

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.

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.

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"

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.

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.

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.

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

Oct 13, 2016

Zertifikate werden funktional vom XenMobile-Server verwendet. Zertifikate werden in XenMobile über den Bereich **Zertifikate** der XenMobile-Konsole hochgeladen. Zu den Zertifikaten gehören Zertifizierungsstellenzertifikate (ZS-Zertifikate), Registrierungsstellenzertifikate (RA-Zertifikate) und Zertifikate für die Clientauthentifizierung bei anderen Komponenten der Infrastruktur. Außerdem können Sie den Bereich "Zertifikate" als Speicherort 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.

In diesem Abschnitt finden Sie allgemeine Anleitungen zum Hochladen von Zertifikaten. Einzelheiten zum Erstellen, Hochladen und Konfigurieren von Clientzertifikaten finden Sie unter Konfigurieren der Clientzertifikatauthentifizierung.

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.

Sie können das ZS-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 ZS-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)

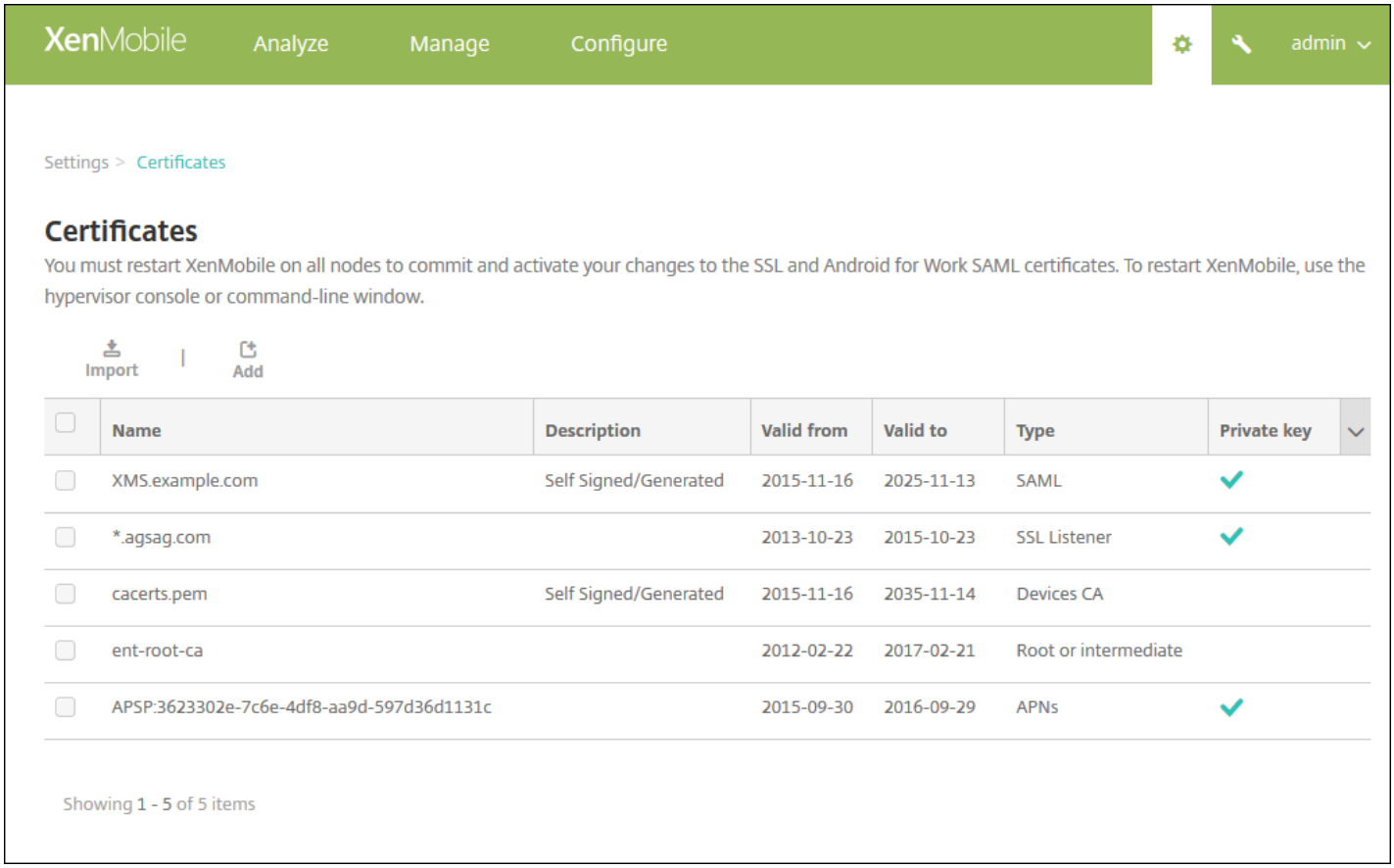
Wichtig: XenMobile-Server unterstützt keine Zertifikate mit der Erweiterung .pem. Mit dem folgenden openssl-Befehl erstellen Sie aus einer PEM-Datei eine PFX-Datei:

```
openssl pkcs12 -export -out certificate.pfx  -in certificate.pem
```

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 das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

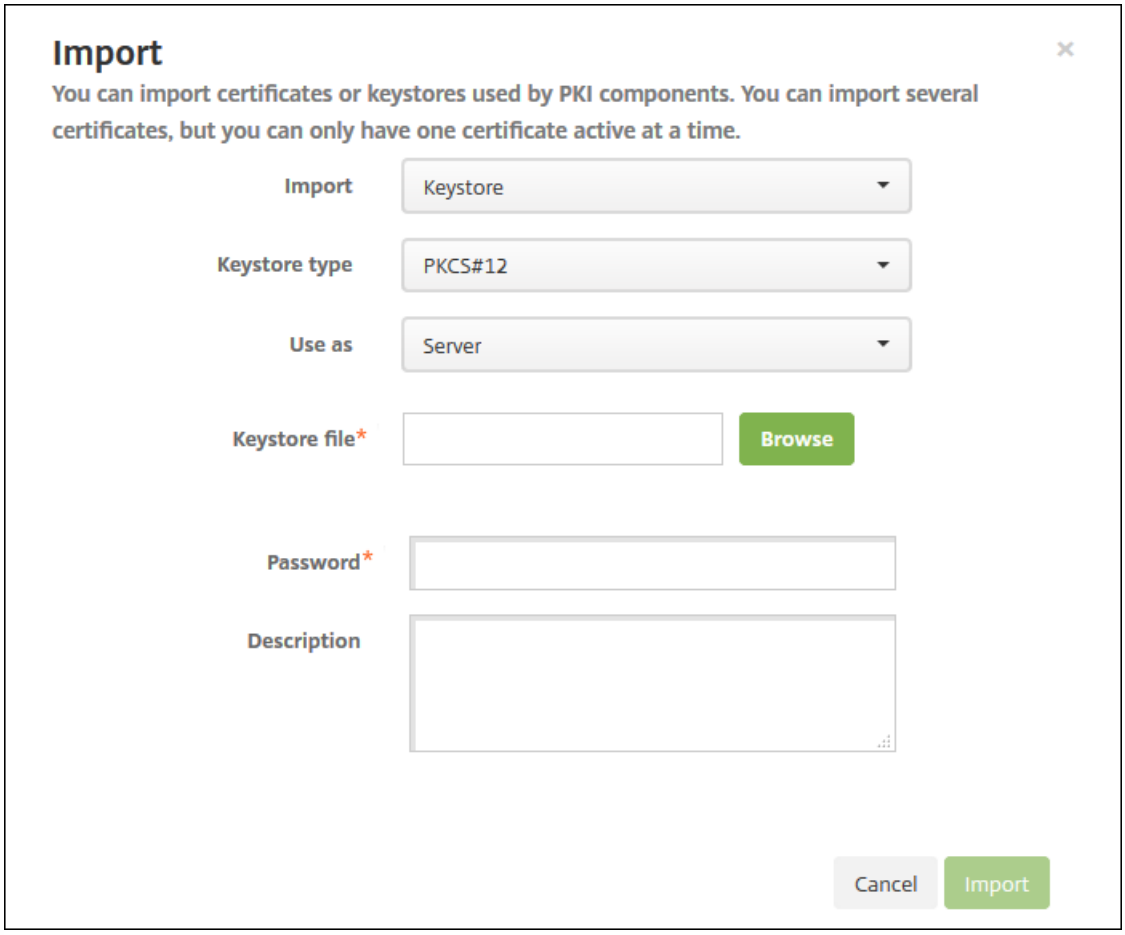
2. Klicken Sie auf **Zertifikate**. Die Seite **Zertifikate** wird angezeigt.



3. Klicken Sie auf **Importieren**. Das Dialogfeld **Importieren** wird angezeigt.

4. Konfigurieren Sie die folgenden Einstellungen:

- **Importieren**: Klicken Sie in der Liste auf **Schlüsselspeicher**. Das Dialogfeld **Importieren** ändert sich und enthält nun die verfügbaren Schlüsselspeicheroptionen.



- **Schlüsselspeichertyp**: Klicken Sie in der Liste auf **PKCS#12**.
- Wählen Sie unter **Verwenden als** 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 ZS-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.
- **Schlüsselspeicherdatei**: Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort der Schlüsselspeicherdatei, um diese auszuwählen.
- Geben Sie unter **Kennwort** das Kennwort für das Zertifikat ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung für den Schlüsselspeicher ein, anhand derer Sie diesen von anderen Schlüsselspeichern unterscheiden können.

5. Klicken Sie auf **Importieren**. Der Schlüsselspeicher wird der Zertifikattabelle hinzugefügt.

Beim Importieren eines Zertifikats aus einer Datei oder einem Schlüsselspeichereintrag versucht XenMobile die Erstellung

einer Zertifikatskette 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 das Zahnradsymbol rechts oben und dann auf **Zertifikate**.

2. Klicken Sie auf der Seite **Zertifikate** auf **Importieren**. Das Dialogfeld **Importieren** wird angezeigt.

3. Aktivieren Sie im Dialogfeld **Importieren** unter **Importieren** die Option **Zertifikat**, sofern sie noch nicht aktiviert ist.

4. Das Dialogfeld **Importieren** ändert sich und enthält nun die verfügbaren Zertifikatoptionen. Wählen Sie unter **Verwenden als** aus, wie Sie den Schlüsselspeicherverwenden 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 ZS-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 **Importieren**. Das Zertifikat wird der Zertifikattabelle hinzugefügt.

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.

Zur Verwendung des optimalen Verfahrens zum Aktualisieren der Zertifikate klicken Sie auf das Zahnradsymbol in der oberen rechten Ecke der Konsole zum Öffnen die Seite Einstellungen und klicken Sie dann auf Zertifikate. Importieren Sie das neue Zertifikat über das Dialogfeld Importieren. 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.

Konfigurieren der Clientzertifikatauthentifizierung

Jul 28, 2016

Zum Verwenden von Clientzertifikatauthentifizierung im Enterprise- oder MAM-Modus müssen Sie den Microsoft-Server, den XenMobile-Server und dann NetScaler Gateway konfigurieren. Die folgenden allgemeinen Schritte werden in diesem Artikel ausführlich erläutert.

Auf dem Microsoft-Server:

1. Fügen Sie der Microsoft Management Console ein Zertifikat-Snap-In hinzu.
2. Fügen Sie der Zertifizierungsstelle (ZS) eine Vorlage hinzu.
3. Erstellen Sie ein PFX-Zertifikat vom ZS-Server.

Auf dem XenMobile-Server:

1. Laden Sie das Zertifikat in XenMobile hoch.
2. Erstellen Sie die PKI-Entität für zertifikatbasierte Authentifizierung.
3. Konfigurieren Sie Anmeldeinformationsanbieter.
4. Konfigurieren Sie NetScaler Gateway, um ein Benutzerzertifikat für die Authentifizierung bereitzustellen.

In NetScaler Gateway:

1. Konfigurieren Sie NetScaler Gateway für die Zertifikatauthentifizierung im XenMobile-MAM-Modus.

Voraussetzungen

- Für Windows Phone 8.1-Geräte mit Clientzertifikatauthentifizierung und SSL-Offload müssen Sie die Wiederverwendung von SSL-Sitzungen für Port 443 auf beiden virtuellen Lastausgleichsservern in NetScaler deaktivieren. Führen Sie hierfür auf diesen virtuellen Servern den folgenden Befehl für Port 443 aus:

  set ssl vserver sessReuse DISABLE

  Hinweis: Mit der SSL-Sitzungswiederverwendung werden einige Optimierungen von NetScaler deaktiviert, was zu einer Leistungsminderung bei NetScaler führen kann.

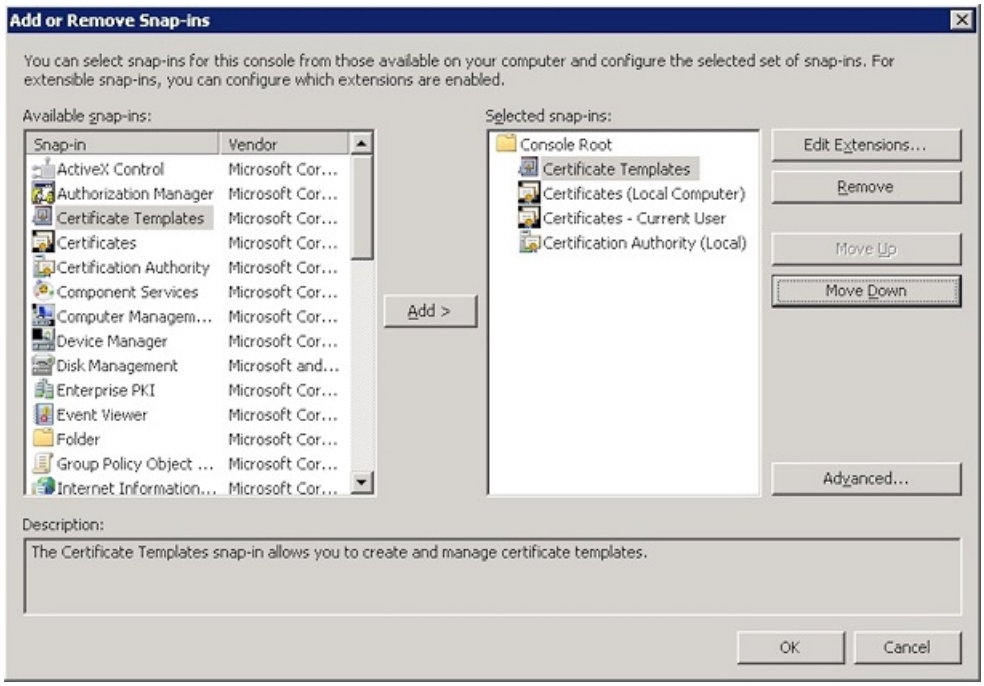
- Informationen zum Konfigurieren der zertifikatbasierten Authentifizierung für Exchange ActiveSync finden Sie in diesem Microsoft-Blog.
- Wenn Sie private Serverzertifikate zum Schützen des ActiveSync-Datenverkehrs an Exchange Server verwenden, müssen die mobilen Geräte alle Stamm- und Zwischenzertifikate haben. Ansonsten schlägt die zertifikatbasierte Authentifizierung beim Einrichten des Postfachs in WorxMail fehl. In der Exchange-IIS-Konsole müssen Sie folgende Schritte ausführen:
  - Website für die Verwendung durch XenMobile mit Exchange hinzufügen und das Webserverzertifikat binden
  - Port 9443 verwenden
  - Für die Website zwei Anwendungen hinzufügen, eine für "Microsoft-Server-ActiveSync" und eine für "EWS". Für beide Anwendungen müssen Sie unter **SSL-Einstellungen** die Option **SSL erforderlich** wählen.
- Stellen Sie sicher, dass WorxMail für iOS, Android und Windows Phone mit der aktuellen MDX-Toolkitversion umschlossen wird.

Hinzufügen eines Zertifikat-Snap-Ins zu Microsoft Management Console

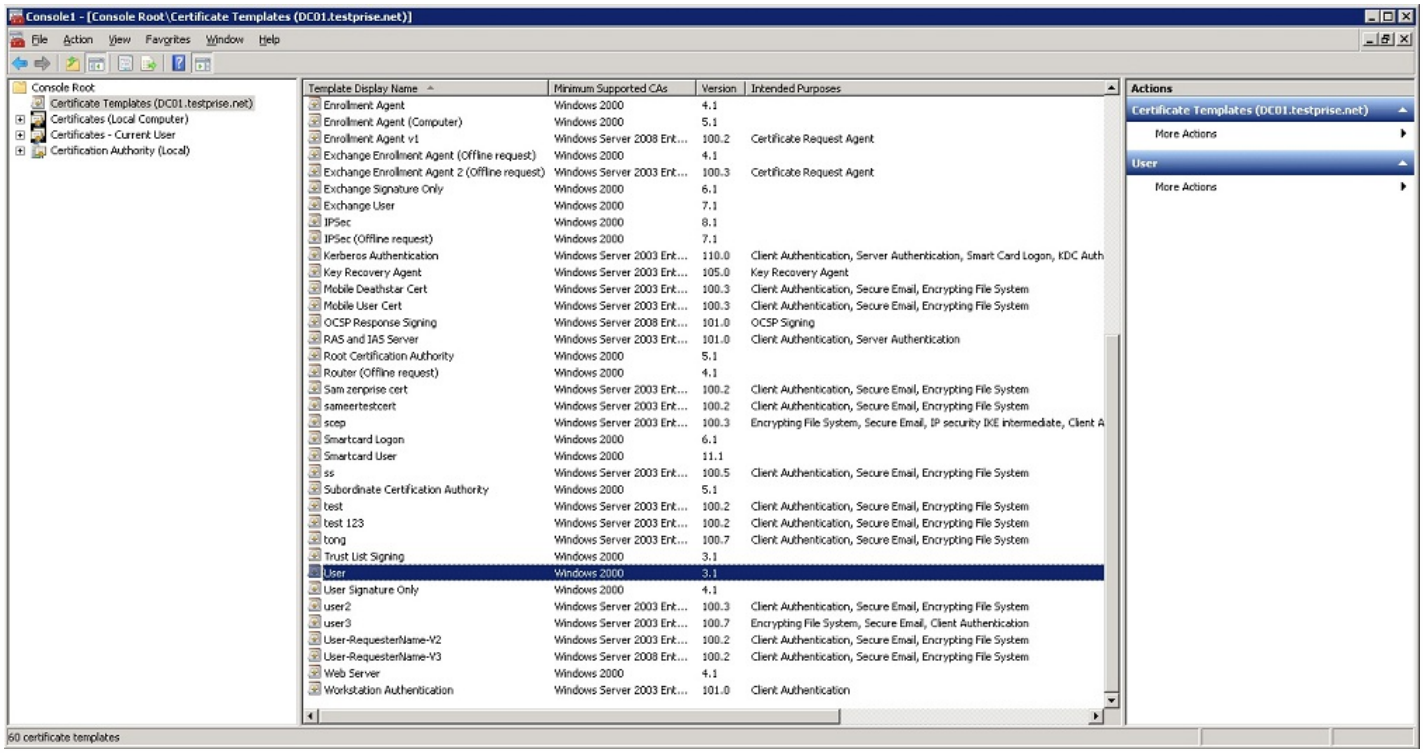
1. Öffnen Sie die Konsole und klicken Sie auf **Snap-In hinzufügen/entfernen**.

2. Fügen Sie die folgenden Snap-Ins hinzu:

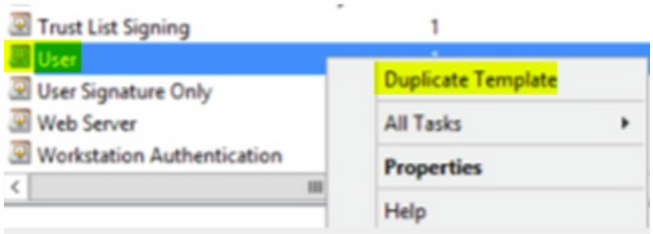
    Zertifikatvorlagen
    Zertifikate (Lokaler Computer)
    Zertifikate – aktueller Benutzer
    Zertifizierungsstelle (Lokal)



3. Erweitern Sie **Zertifikatvorlagen**.



4. Wählen Sie die Vorlage **Benutzer** und dann **Doppelte Vorlage**.

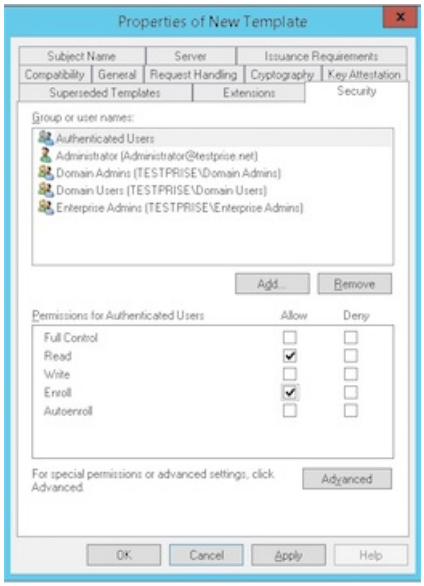


5. Geben Sie den Anzeigenamen der Vorlage an.

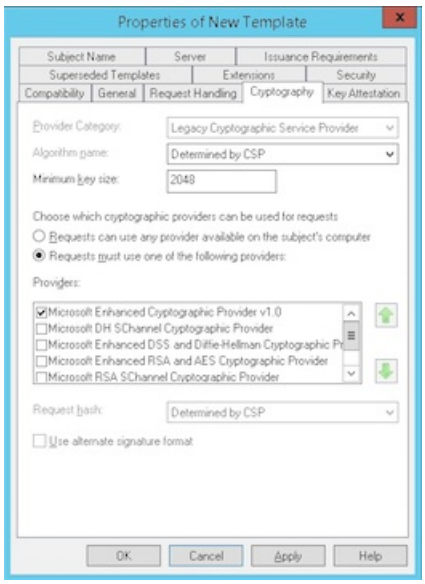
> **Wichtig:** Aktivieren Sie das Kontrollkästchen **Zertifikat in Active Directory veröffentlichen** nur bei Bedarf. Wenn diese Option aktiviert ist, werden alle Benutzer-Clientzertifikate in Active Directory erstellt/bereitgestellt, wodurch Ihre Active Directory-Datenbank überladen werden kann.

6. Wählen Sie als Vorlagentyp **Windows 2003 Server**. In Windows 2012 R2 Server wählen Sie unter **Kompatibilität** die Option **Zertifizierungsstelle** und als Empfänger **Windows 2003**.

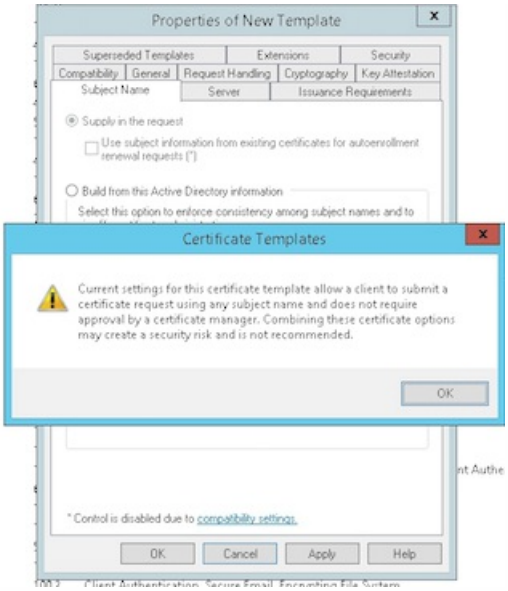
7. Wählen Sie unter **Sicherheit** in der Spalte **Zulassen** die Option **Registrieren** für die authentifizierten Benutzer aus.



8. Geben Sie unter **Kryptografie** die Schlüsselgröße an, die Sie während der Konfiguration von XenMobile eingeben müssen.



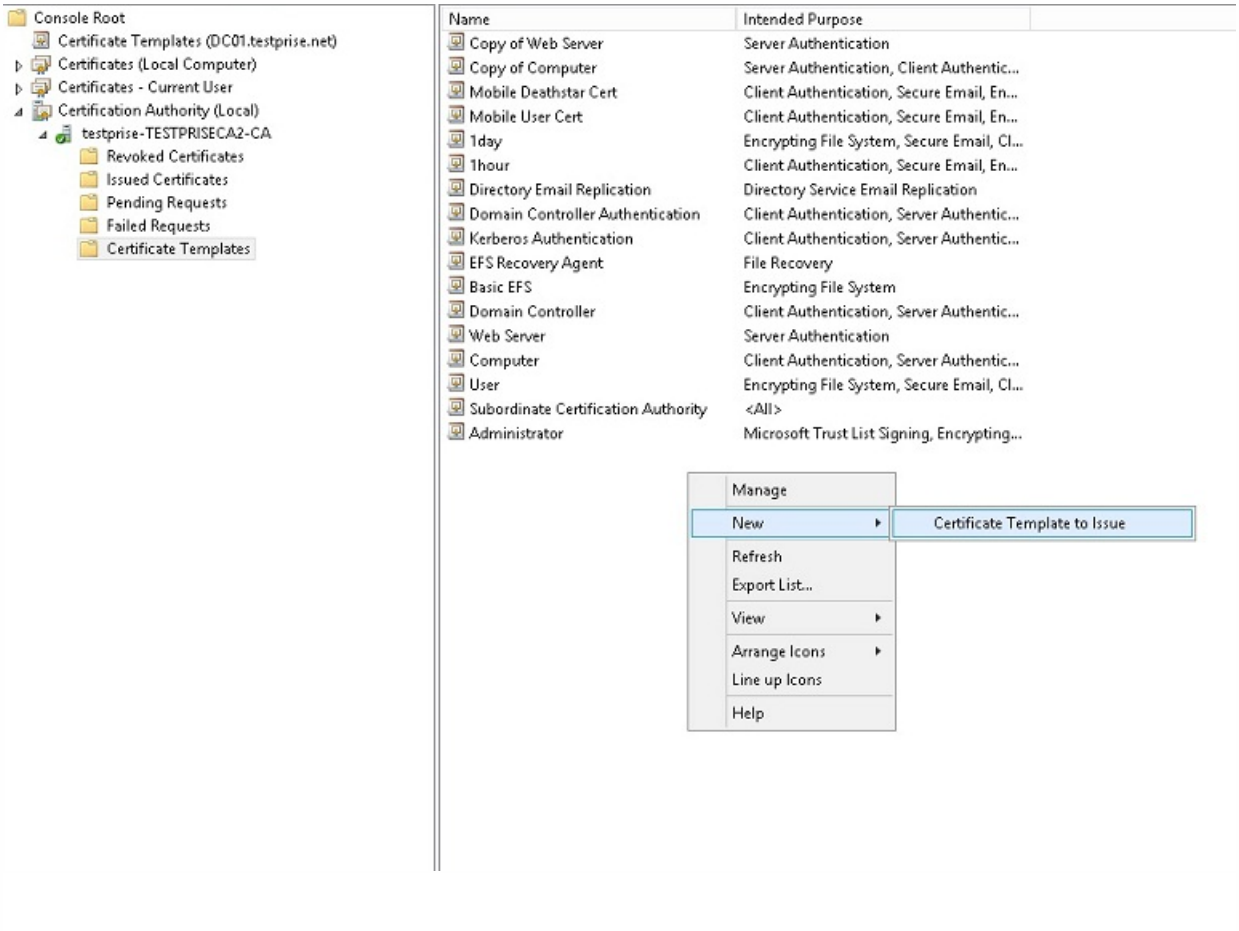
9. Wählen Sie unter **Antragstellername** die Option **Informationen werden in der Anforderung angegeben** aus. Wenden Sie die Änderungen an und speichern Sie.



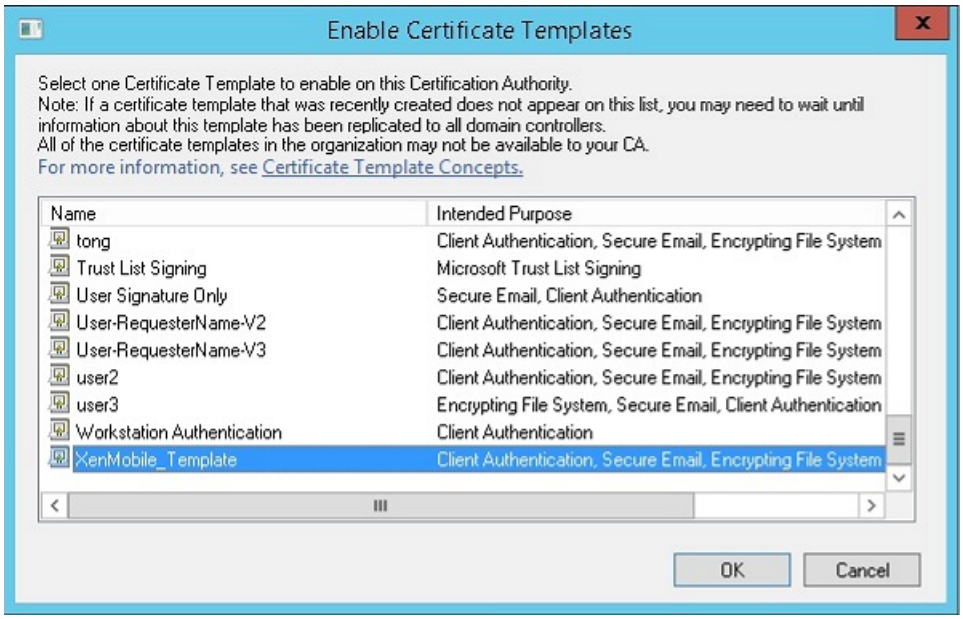
Hinzufügen der Vorlage zur Zertifizierungsstelle

1. Navigieren Sie zu **Zertifizierungsstelle** und wählen Sie **Zertifikatvorlagen**.

2. Klicken Sie mit der rechten Maustaste in den rechten Bereich und wählen Sie **Neu > Auszustellende Zertifikatvorlage**.



3. Wählen Sie die im vorherigen Schritt erstellte Vorlage und klicken Sie auf **OK**, um sie der Zertifizierungsstelle hinzuzufügen.

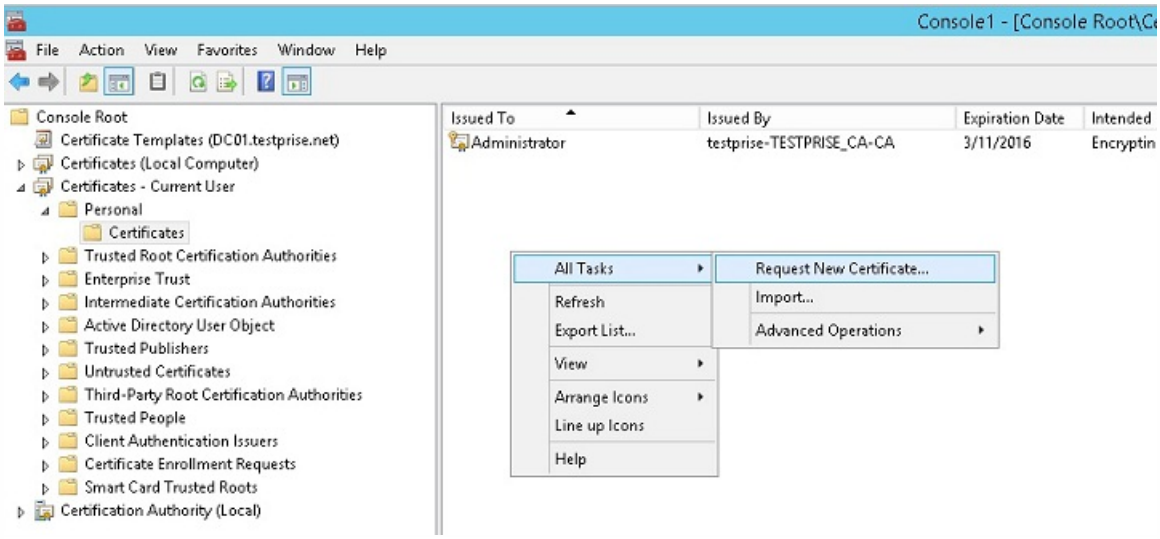


Erstellen eines PFX-Zertifikats vom ZS-Server

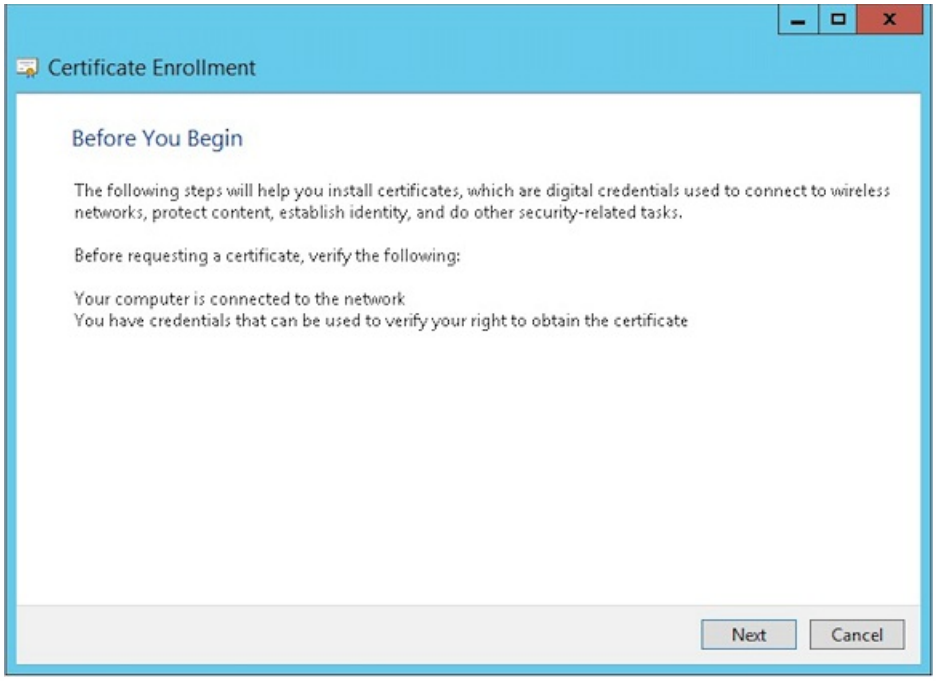
1. Erstellen Sie mit dem Dienstkonto, mit dem Sie sich angemeldet haben, ein PFX-Benutzerzertifikat. Diese PFX-Datei wird in XenMobile hochgeladen, um ein Benutzerzertifikat im Namen der Benutzer anzufordern, die ihre Geräte registrieren.

2. Erweitern Sie **Zertifikate** unter **Aktueller Benutzer**.

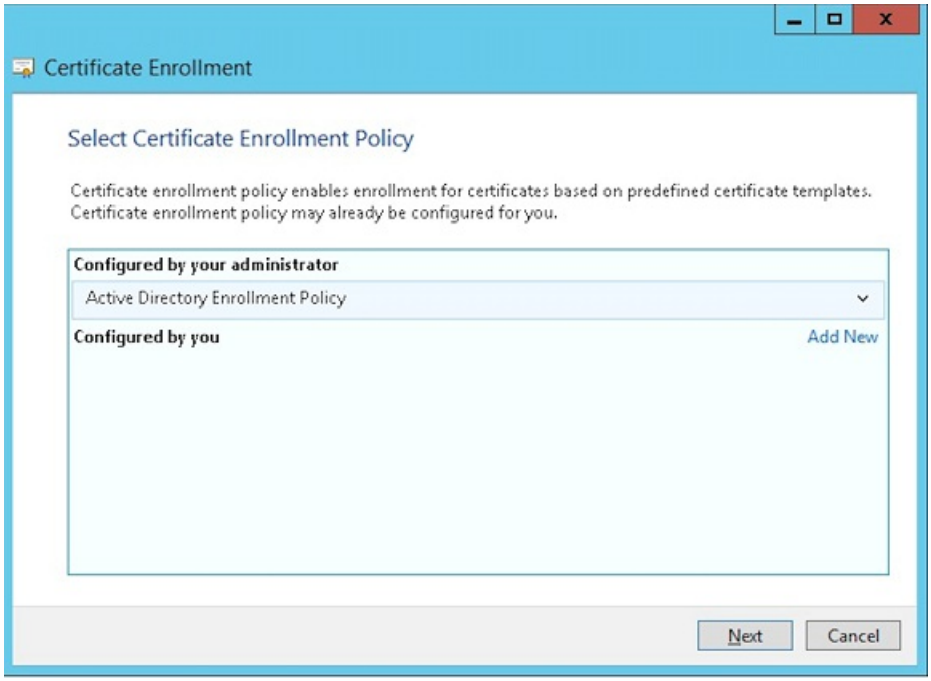
3. Klicken Sie mit der rechten Maustaste in den rechten Bereich und klicken Sie auf **Neues Zertifikat anfordern**.



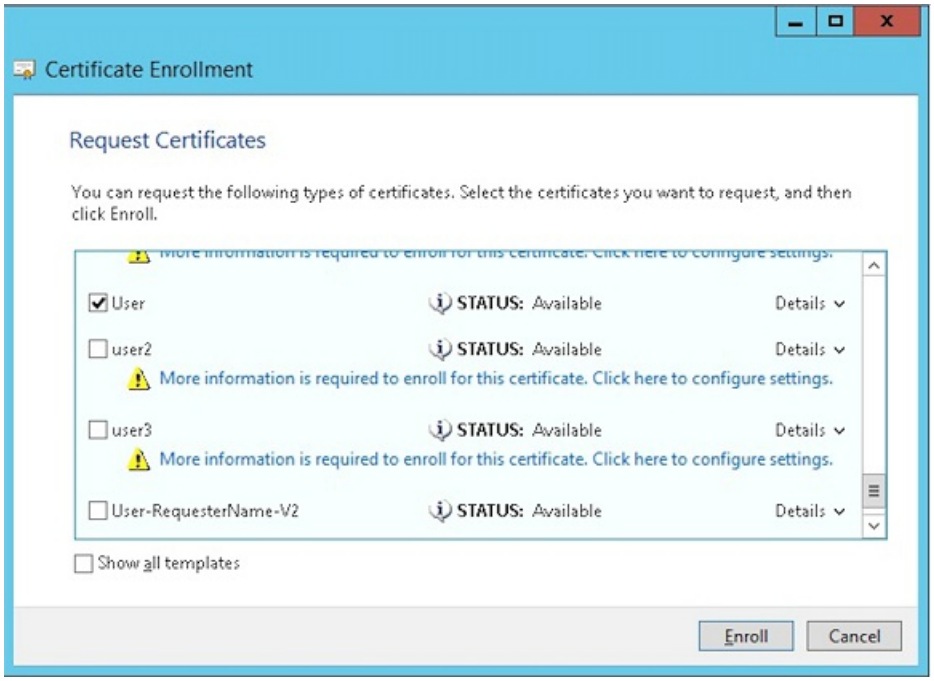
4. Der Bildschirm **Zertifikatregistrierung** wird angezeigt. Klicken Sie auf **Next**.



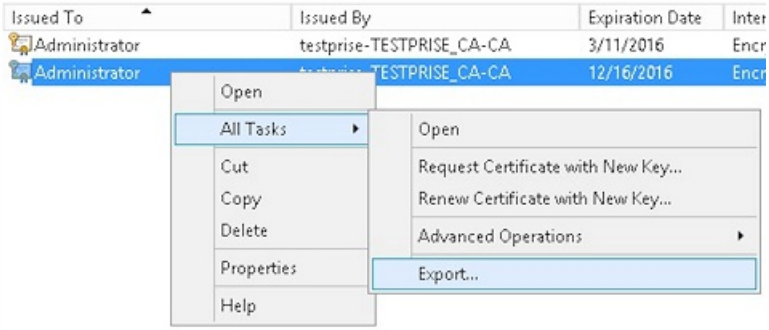
5. Wählen Sie **Active Directory-Registrierungsrichtlinie** und klicken Sie auf **Weiter**.



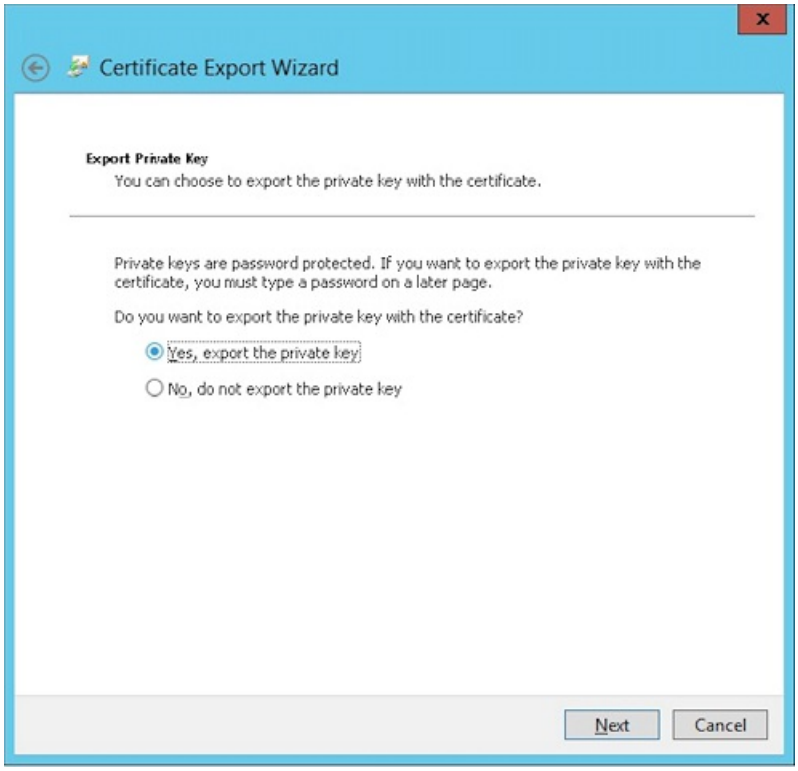
6. Wählen Sie die Vorlage **Benutzer** und klicken Sie auf **Registrieren**.



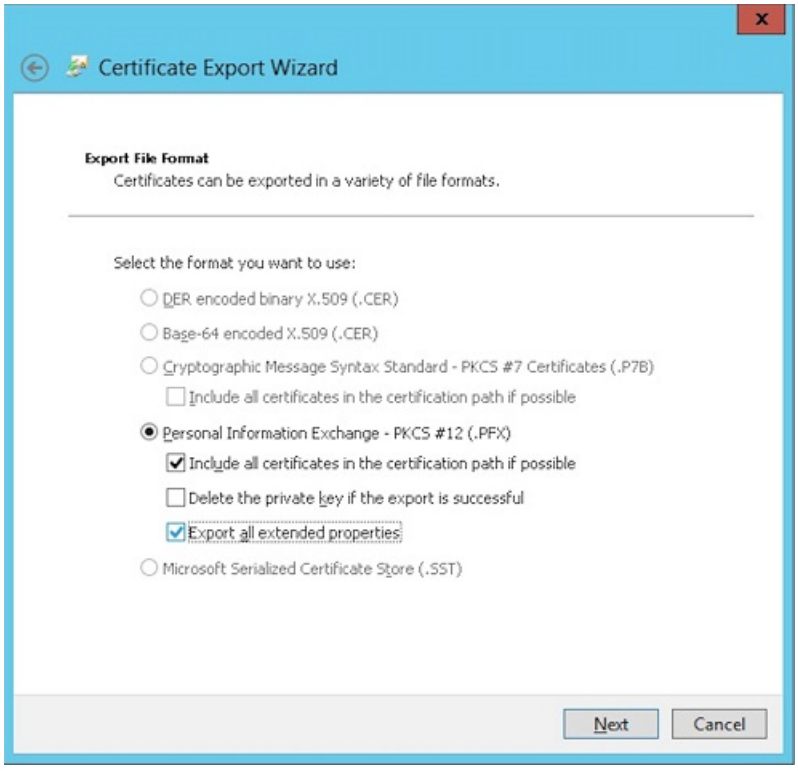
7. Exportieren Sie die PFX-Datei, die Sie im vorherigen Schritt erstellt haben.



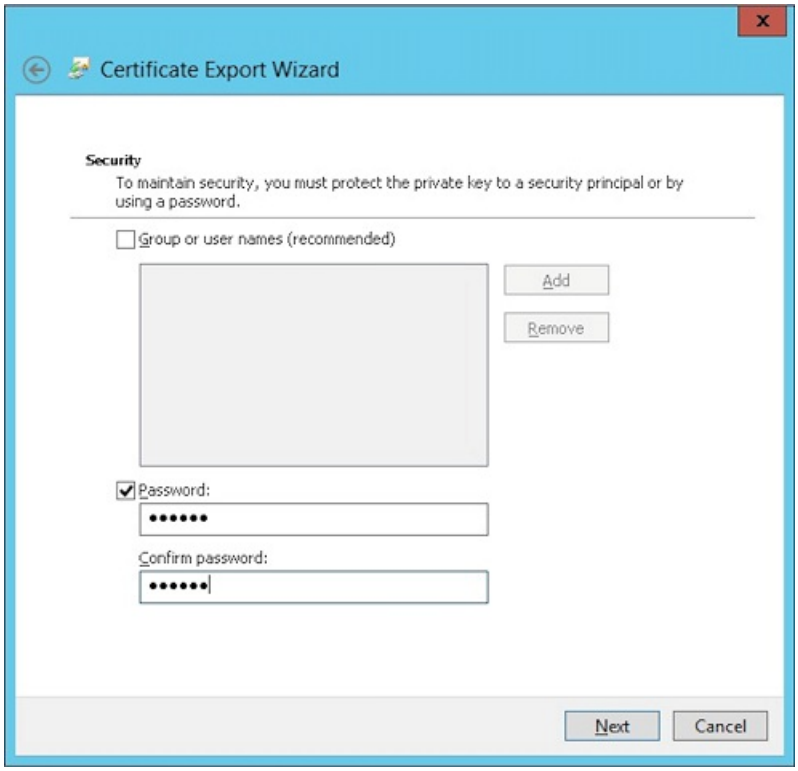
8. Klicken Sie auf **Ja, privaten Schlüssel exportieren**.



9. Aktivieren Sie die Kontrollkästchen **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen** und **Alle erweiterten Eigenschaften exportieren**.



10. Legen Sie ein Kennwort für den Upload des Zertifikats in XenMobile fest.



11. Speichern Sie das Zertifikat auf Ihrer Festplatte.

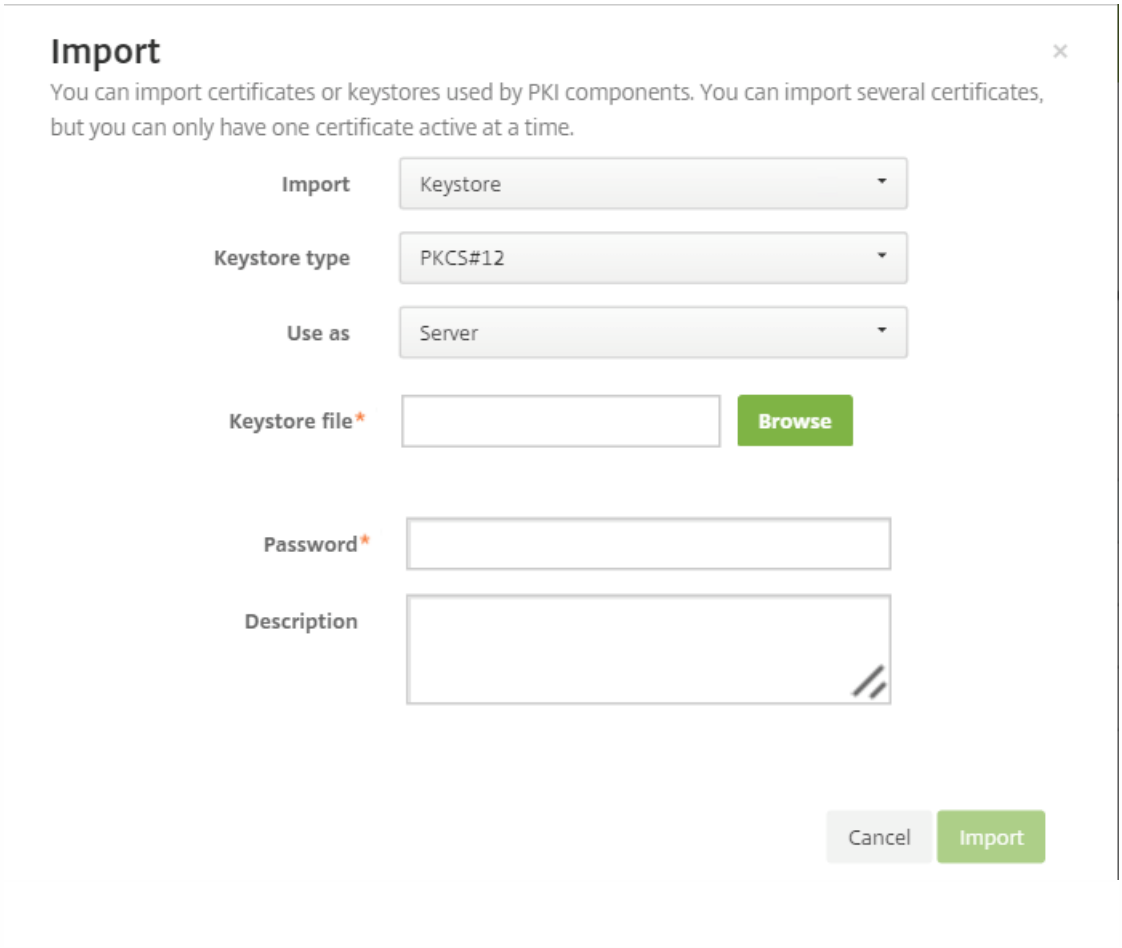
Hochladen des Zertifikats in XenMobile

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Der Bildschirm **Einstellungen** wird angezeigt.

2. Klicken Sie auf **Zertifikate** und dann auf **Importieren**.

3. Geben Sie die folgenden Parameter ein:

- **Importieren**: Schlüsselspeicher
- **Schlüsselspeichertyp**: PKCS#12
- **Verwenden als**: Server
- **Schlüsselspeicherdatei**: Klicken Sie auf Durchsuchen, um das erstellte PFX-Zertifikat zu suchen.
- **Kennwort**: Geben Sie das Kennwort ein, das Sie für dieses Zertifikat erstellt haben.



4. Klicken Sie auf **Importieren**.

5. Prüfen Sie, ob das Zertifikat richtig installiert wurde. Es sollte als ein Benutzerzertifikat angezeigt werden.

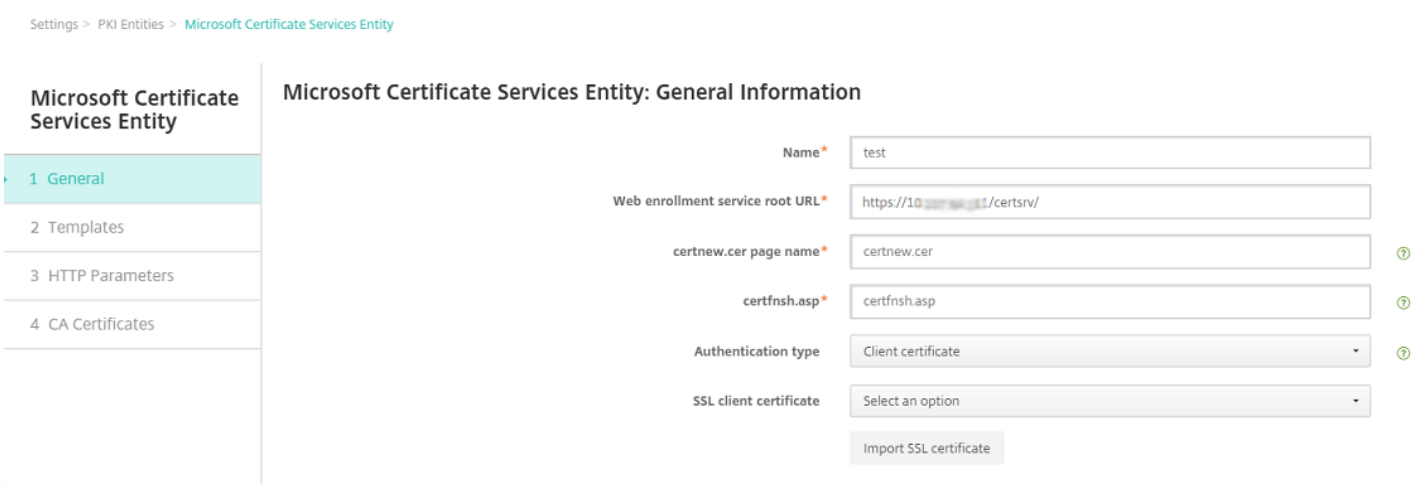
Erstellen der PKI-Entität für die zertifikatbasierte Authentifizierung

1. Gehen Sie in **Einstellungen** zu **Mehr > Zertifikatverwaltung > PKI-Entitäten**.

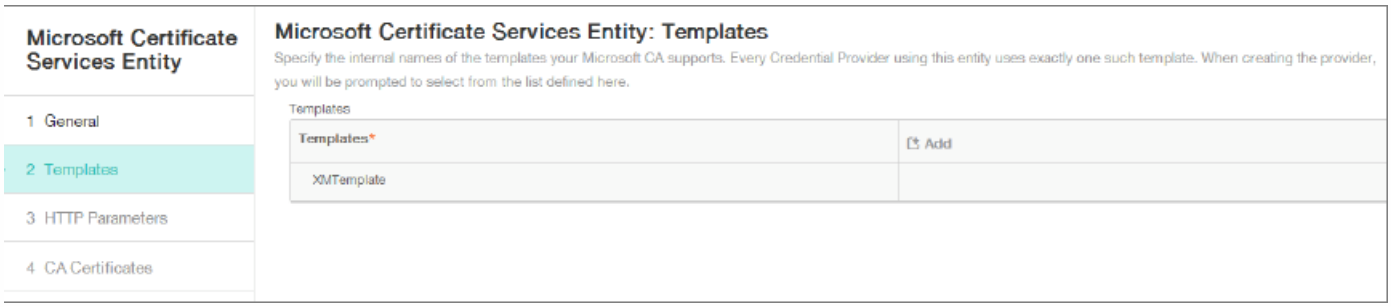
2. Klicken Sie auf **Hinzufügen** und dann auf **Microsoft Zertifikatdiensteentität**. Der Bildschirm **Microsoft Zertifikatdiensteentität: Allgemeine Informationen** wird angezeigt.

3. Geben Sie die folgenden Parameter ein:

- **Name**: Geben Sie einen Namen ein.
- **Stamm-URL des Webregistrierungsdiensts**: https://RootCA-URL/certsrv/
  Geben Sie auf jeden Fall den letzten Schrägstrich (/) im URL-Pfad ein.
- **certnew.cer-Seitenname**: certnew.cer (Standardwert)
- **certfnsh.asp**: certfnsh.asp (Standardwert)
- **Authentifizierungstyp**: Clientzertifikat
- **SSL-Clientzertifikat**: Wählen Sie das Benutzerzertifikat aus, das für die Ausstellung des XenMobile-Clientzertifikats verwendet werden soll.

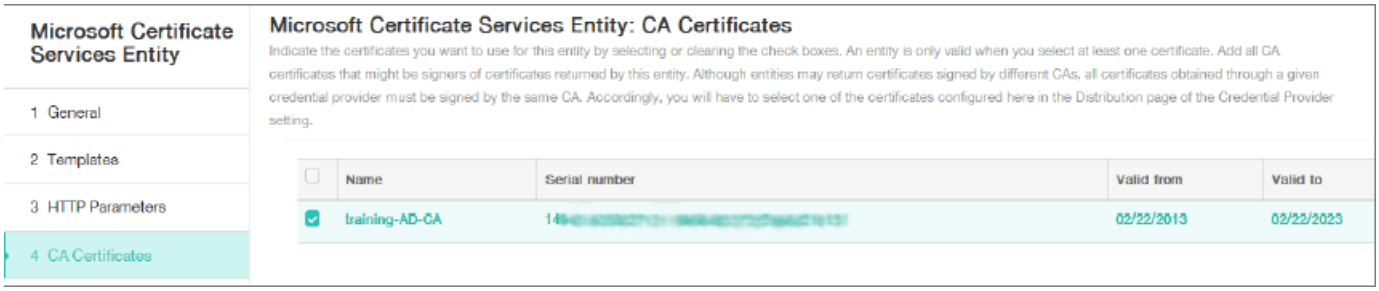


4. Fügen Sie unter **Vorlagen** die Vorlage hinzu, die Sie beim Konfigurieren des Microsoft-Zertifikats erstellt haben. Leerstellen sind nicht zulässig.



5. Überspringen Sie HTTP-Parameter und klicken Sie auf **ZS-Zertifikate**.

6. Wählen Sie den Namen der Stammzertifizierungsstelle, der mit Ihrer Umgebung übereinstimmt. Diese Stammzertifizierungsstelle gehört zur Kette, die aus dem XenMobile-Clientzertifikat importiert wurde.



7. Klicken Sie auf **Speichern**.

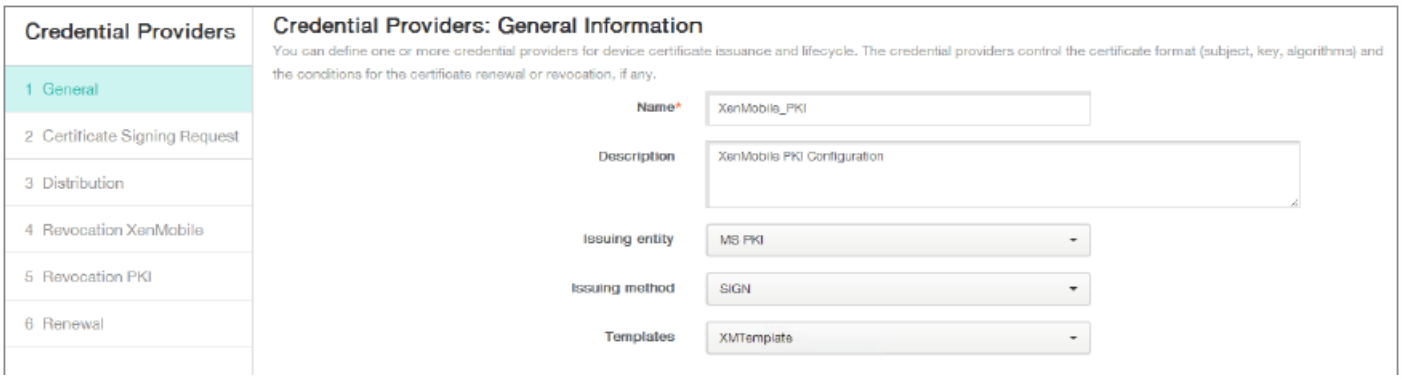
Konfigurieren der Anmeldeinformationsanbieter

1. Navigieren Sie unter **Einstellungen** zu **Mehr > Zertifikatverwaltung > Anbieter für Anmeldeinformationen**.

2. Klicken Sie auf **Hinzufügen**.

3. Geben Sie unter **Allgemein** die folgenden Parameter ein:

- **Name**: Geben Sie einen Namen ein.
- **Beschreibung**: Geben Sie eine Beschreibung ein.
- **Ausstellende Entität**: Wählen Sie die zuvor erstellte PKI-Entität aus.
- **Ausstellungsmethode**: SIGN
- **Vorlagen**: Wählen Sie die unter der PKI-Entität hinzugefügte Vorlage aus.

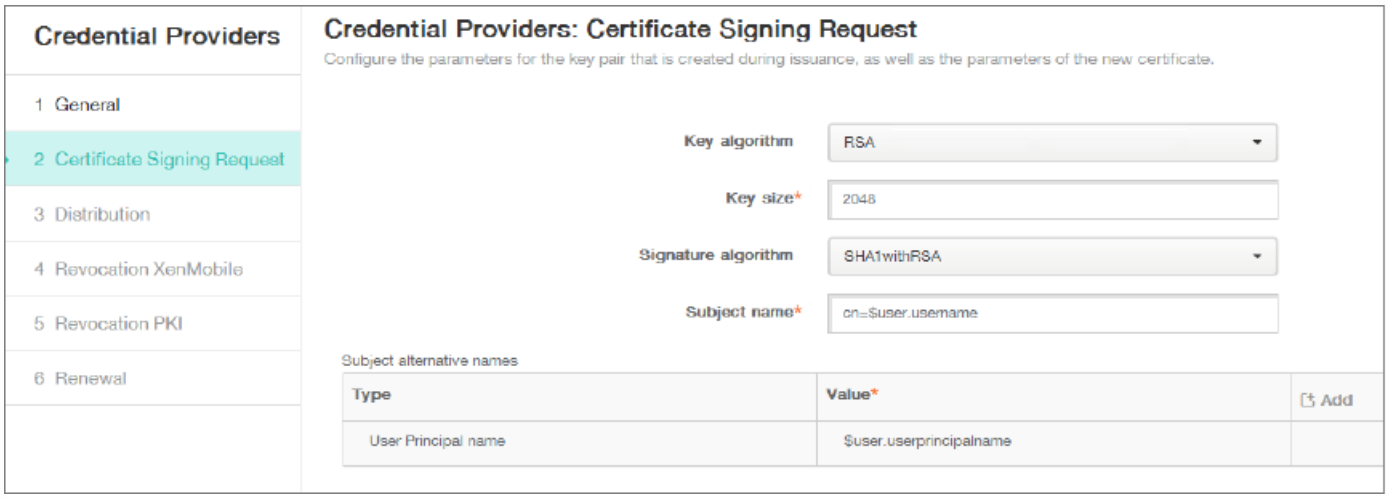


4. Klicken Sie auf **Zertifikatsignieranforderung** und geben Sie die folgenden Parameter ein:

- **Schlüsselalgorithmus**: RSA
- **Schlüsselgröße**: 2048
- **Signaturalgorithmus**: SHA1withRSA
- **Antragstellername**: cn=$user.username

Klicken Sie für **Alternative Antragstellernamen** auf **Hinzufügen** und geben Sie die folgenden Parameter ein:

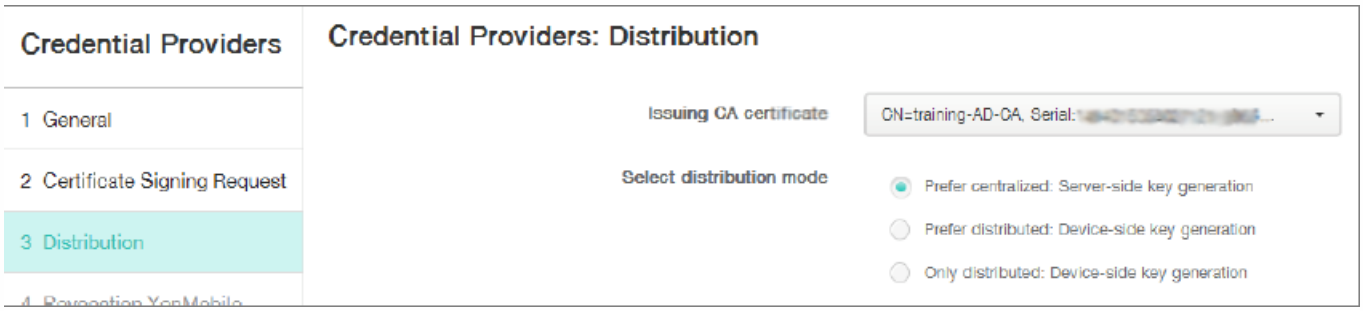
- **Typ**: Benutzerprinzipalname
- **Wert**: $user.userprincipalname



5. Klicken Sie auf **Verteilung** und geben Sie die folgenden Parameter ein:

- **Zertifikat der austellenden ZS**: Wählen Sie die ausstellende Zertifizierungsstelle, die das XenMobile-Clientzertifikat signiert hat.

- **Verteilungsmodus wählen**: Wählen Sie **Bevorzugt zentralisiert: Schlüssel serverseitig generieren**.

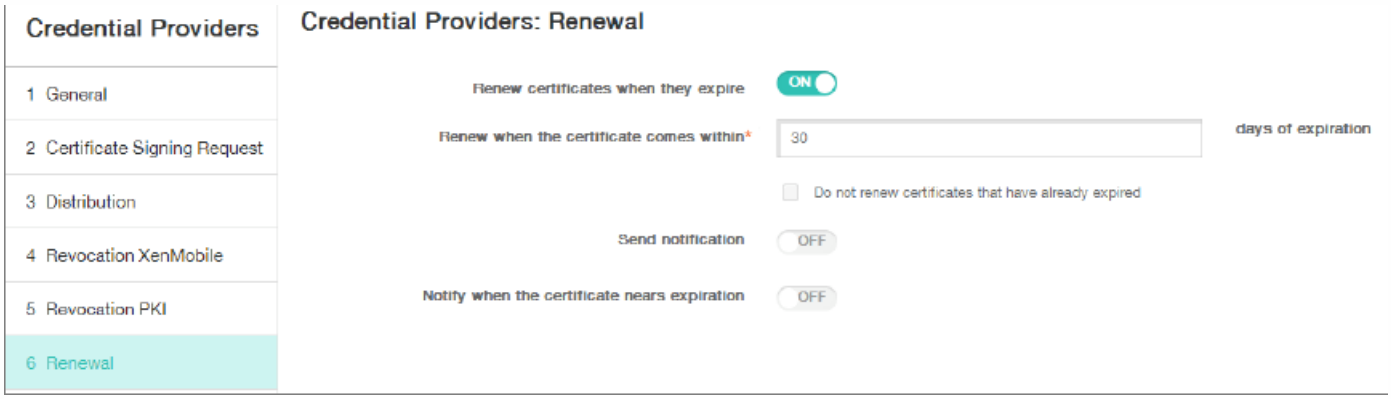


6. Legen Sie für die zwei folgenden Abschnitte **XenMobile-Sperrung** und **PKI-Sperrung** die Parameter nach Bedarf fest. Die beiden Optionen werden in diesem Artikel übersprungen.

7. Klicken Sie auf **Verlängerung**.

8. Wählen Sie für **Zertifikate erneuern, wenn sie ablaufen** die Option **EIN**.

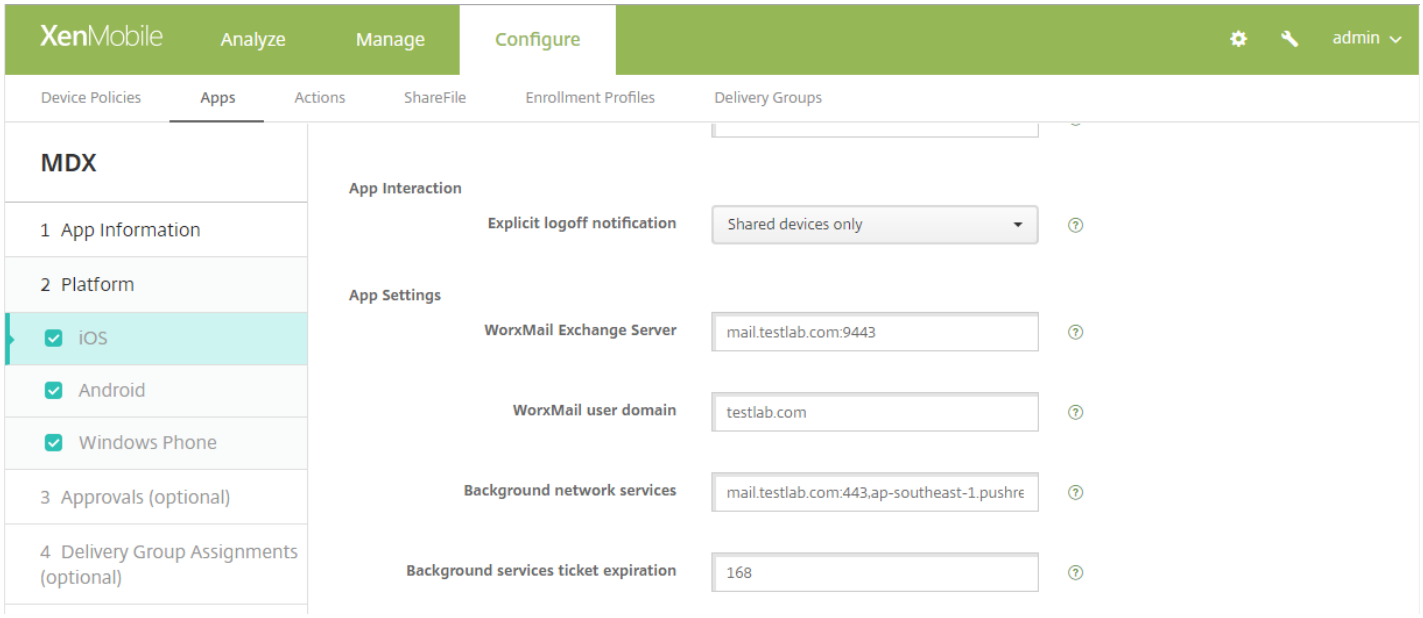
9. Behalten Sie für alle anderen Einstellungen die Standardwerte bei oder ändern Sie sie nach Bedarf.



10. Klicken Sie auf **Speichern**.

Konfigurieren von WorxMail für die zertifikatbasierte Authentifizierung

Beim Hinzufügen von WorxMail zu XenMobile müssen Sie die Exchange-Einstellungen unter **App-Einstellungen** konfigurieren.



Konfigurieren der NetScaler-Zertifikatbereitstellung in XenMobile

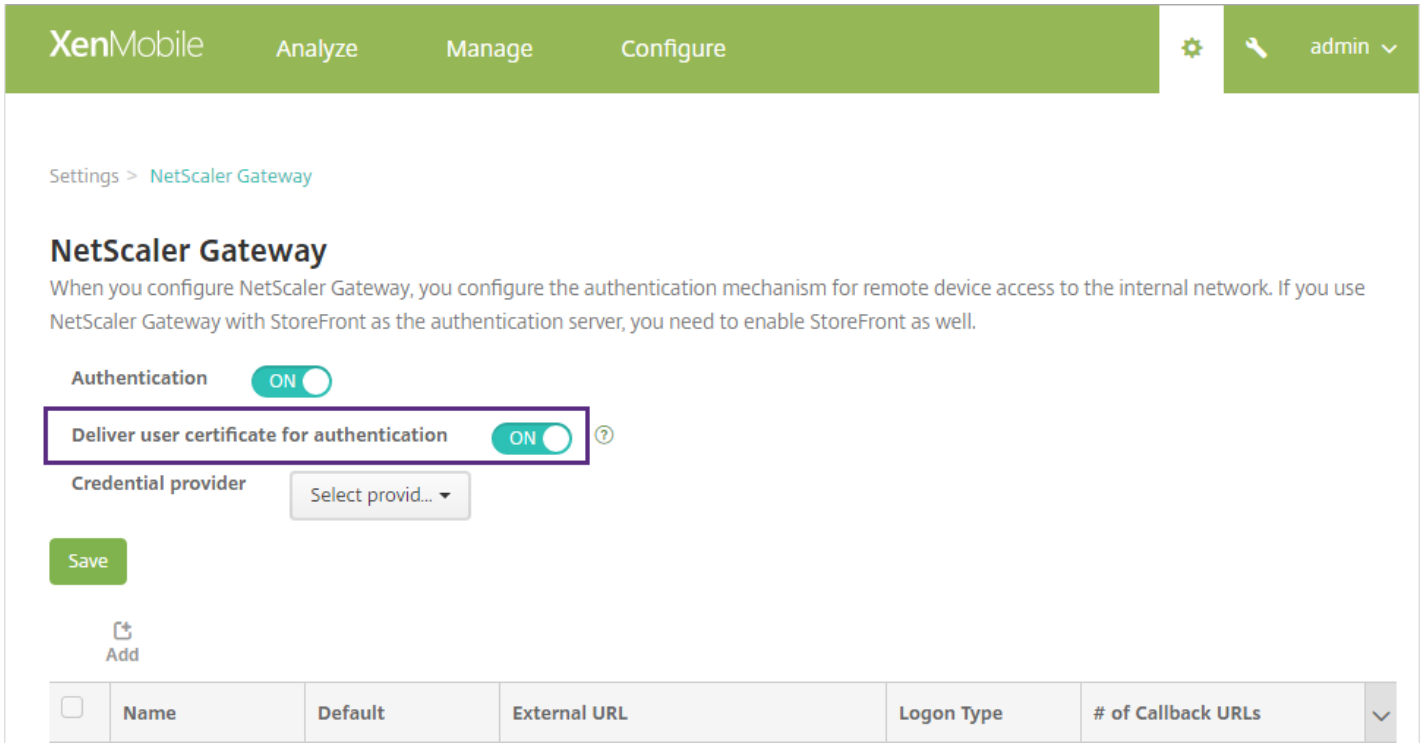
1. Melden Sie sich an der XenMobile-Konsole an und klicken Sie auf das Zahnradsymbol rechts oben. Der Bildschirm **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **NetScaler Gateway**.

3. Wenn NetScaler Gateway noch nicht hinzugefügt wurde, klicken Sie auf **Hinzufügen** und legen Sie folgende Einstellungen fest:

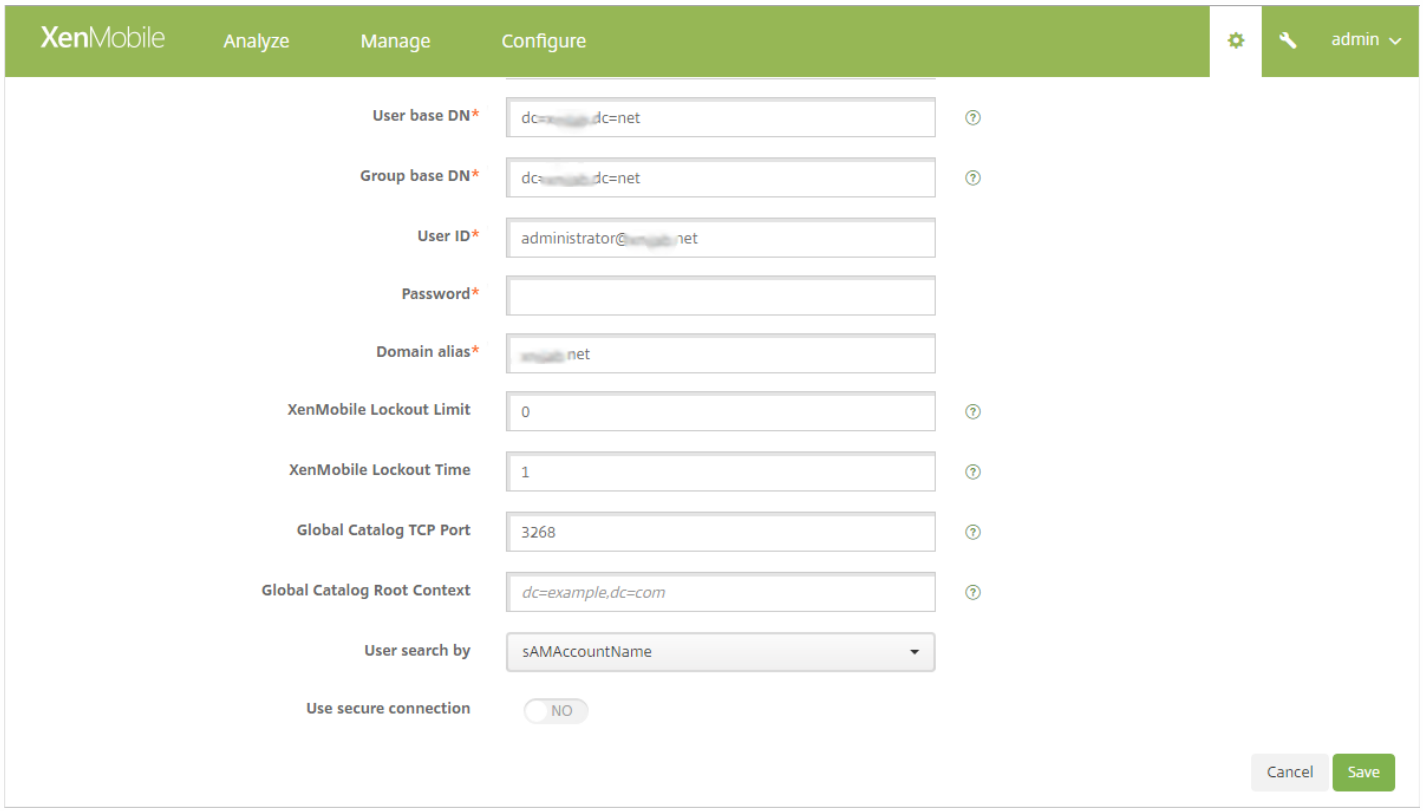
- **Externe URL**: https://URLIhresNetScalerGateways
- **Anmeldetyp**: Zertifikat
- **Kennwort erforderlich**: AUS
- **Als Standard setzen**: EIN

4. Legen Sie **Benutzerzertifikat für Authentifizierung bereitstellen** auf **Ein** fest.



5. Wählen Sie unter **Anmeldeinformationsanbieter** einen Anbieter und klicken Sie auf **Speichern**.

6. Wenn Sie in den Benutzerzertifikaten sAMAccount-Attribute anstelle des UPN (Benutzerprinzipalname) verwenden, konfigurieren Sie den LDAP-Connector in XenMobile folgendermaßen: Navigieren Sie zu **Einstellungen > LDAP**, wählen Sie das Verzeichnis, klicken Sie auf **Bearbeiten** und wählen Sie für **Benutzersuche nach** die Option **sAMAccountName**.



Erstellen einer Enterprise Hub-Richtlinie für Windows Phone 8.1

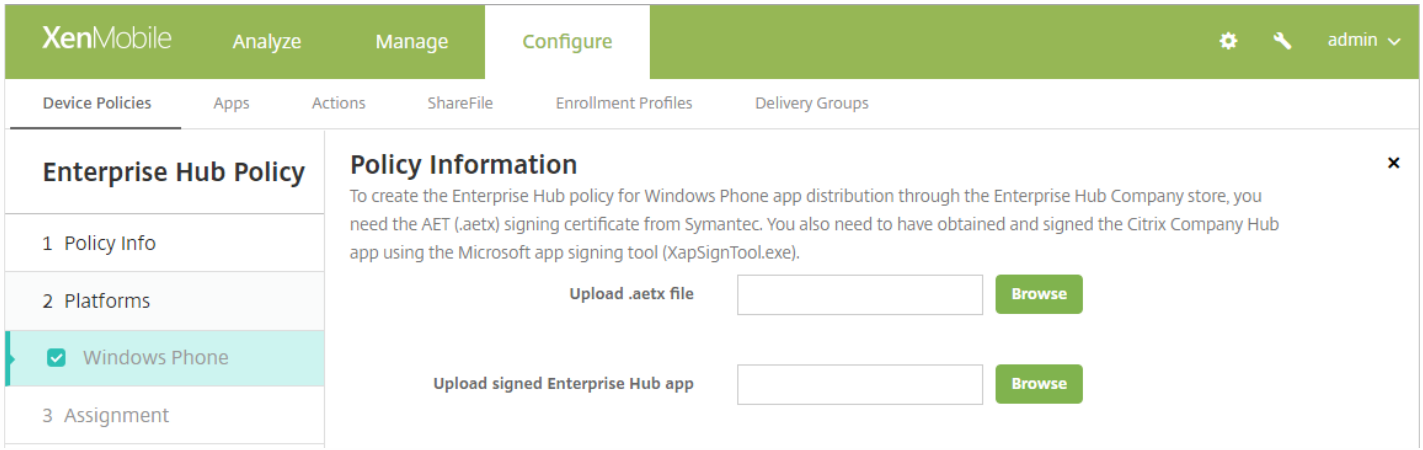
Für Windows Phone 8.1-Geräte müssen Sie eine Enterprise Hub-Richtlinie zum Bereitstellen der AETX-Datei und des Worx Home-Clients erstellen.

> **Hinweis**
>
> Vergewissern Sie sich, dass für die AETX- und die Worx Home-Dateien das gleiche Enterprise- Zertifikat des Zertifikatsanbieters und die gleiche Aussteller-ID des Windows Store-Entwicklerkontos verwendet wurden.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Geräterichtlinien**.

2. Klicken Sie auf **Hinzufügen** und dann unter **Mehr > XenMobile-Agent** auf **Enterprise Hub**.

3. Nach Eingabe eines Namens für die Richtlinie wählen Sie die richtige AETX-Datei und signierte Worx Home-App für den Enterprise Hub aus.



4. Weisen Sie die Richtlinie Bereitstellungsgruppen zu und speichern Sie sie.

Konfigurieren von NetScaler Gateway mit dem NetScaler für XenMobile-Assistenten für die Clientzertifikat-Authentifizierung

> **Hinweis**
>
> Sie können den NetScaler für XenMobile-Assistenten nur einmal ausführen. Wenn Sie den Assistenten bereits verwendet haben,

folgen Sie den Anweisungen "Manuelles Konfigurieren von NetScaler Gateway für die Zertifikatauthentifizierung" weiter unten.

Führen Sie die folgenden Schritte auf dem NetScaler-Gerät zum Konfigurieren der Zertifikatauthentifizierung in XenMobile durch.

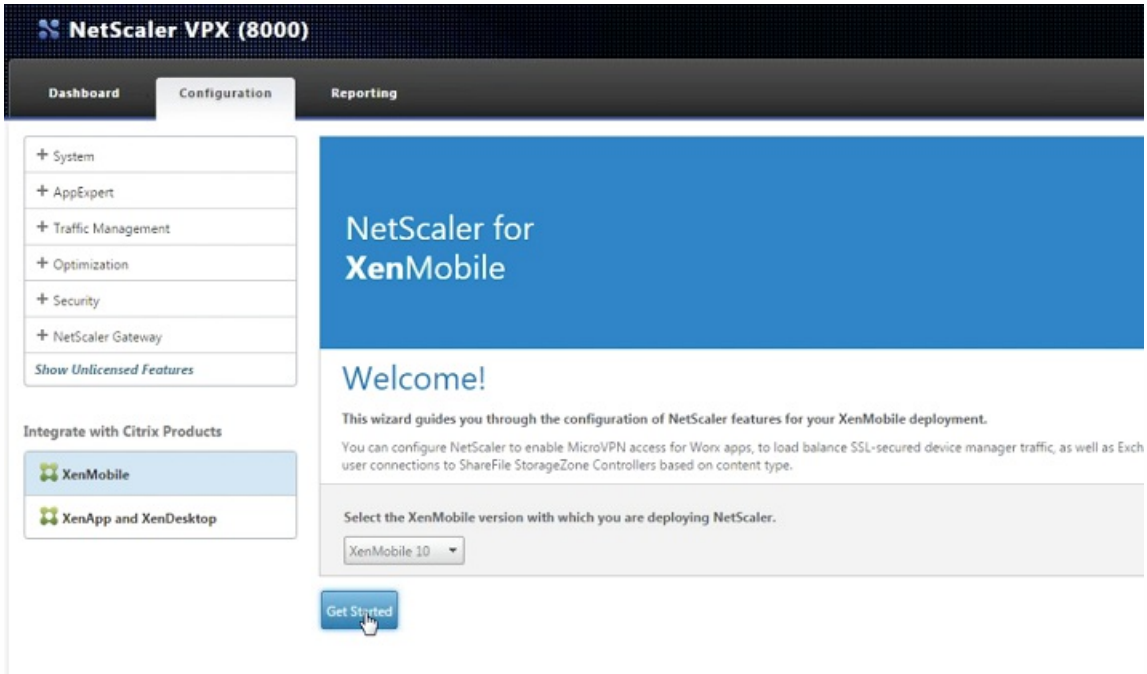
1. Melden Sie sich an NetScaler an.

2. Klicken Sie unter **Configuration** auf **Integrate with Citrix Products** und wählen Sie dann **XenMobile**.

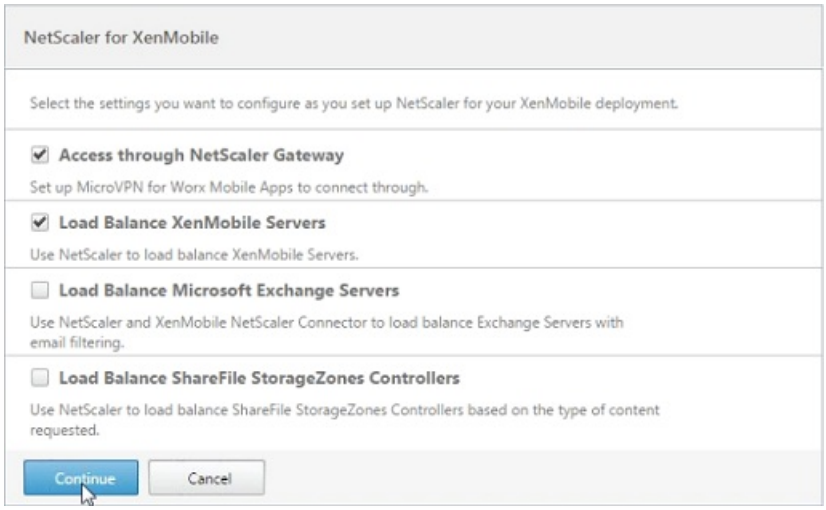
Daraufhin wird ein Assistent zum Konfigurieren von NetScaler-Features für die XenMobile-Bereitstellung geöffnet.

3. Wählen Sie **XenMobile 10**.

4. Klicken Sie auf **Get Started**.



5. Wählen Sie auf der nächsten Seite **Access through NetScaler Gateway** (für Enterprise- und MAM-Modus) und **Load Balance XenMobile Servers** und klicken Sie dann auf **Continue**.



6. Geben Sie auf der nächsten Seite die extern ausgerichtete IP-Adresse für NetScaler Gateway ein und klicken Sie auf **Continue**.

Die Seite für das Serverzertifikat für NetScaler Gateway wird angezeigt.

7. Sie verwenden entweder ein vorhandenes Zertifikat oder installieren ein Zertifikat. Klicken Sie auf **Continue**.

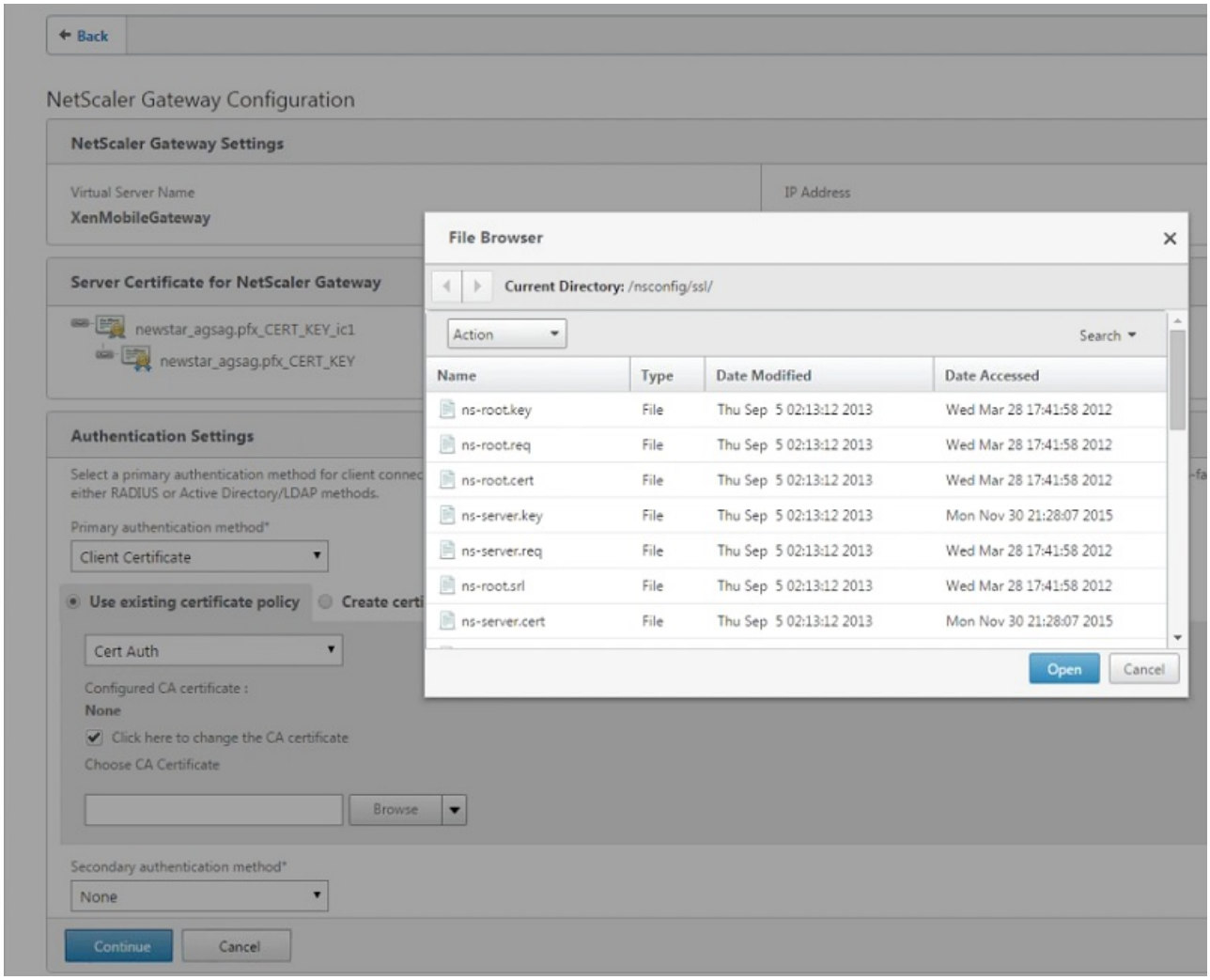
Die Seite **Authentication Settings** wird angezeigt.

8. Wählen Sie im Feld **Primary authentication method** die Option **Client Certificate** aus.

Auf diese Weise wird automatisch **Use existing certificate policy** und **Cert Auth** in den folgenden beiden Feldern ausgewählt. Bei den folgenden Schritten wird davon ausgegangen, dass Sie bereits eine Zertifikatrichtlinie haben.

Wenn Sie eine Zertifikatrichtlinie erstellen müssen, klicken Sie auf **Create certificate policy** und legen Sie die Einstellungen fest. Wählen Sie auf der Seite **XenMobile Server Certificate** ein vorhandenes Serverzertifikat oder installieren Sie ein neues Zertifikat. Wenn Sie mehrere XenMobile-Server ausführen, müssen Sie für jeden Server ein Zertifikat hinzufügen. Legen Sie **Server Logon Name Attribute** auf **userPrincipalName** oder **samAccountName** fest.

9. Wählen Sie **Click here to change the CA certificate** und wählen Sie in der Liste **Browse** das gewünschte Zertifikat aus.



10. Für **Second authentication method** sollte **None** bereits ausgewählt sein. Klicken Sie auf **Continue**.

11. Exportieren Sie auf der Seite **Device certificate** das Zertifikat, wenn es noch nicht installiert ist, aus der XenMobile-Konsole. Vorgehensweise:

a. Klicken Sie in der Konsole auf das Zahnradsymbol oben rechts, um die Seite **Einstellungen** anzuzeigen.

b. Klicken Sie auf **Zertifikat** und wählen Sie das Zertifizierungsstellenzertifikat in der Liste aus.

c. Klicken Sie auf **Exportieren**.

d. Kehren Sie zum NetScaler-Assistenten zurück und wählen Sie das exportierte Zertifikat für die Installation aus.

e. Klicken Sie auf **Continue**.

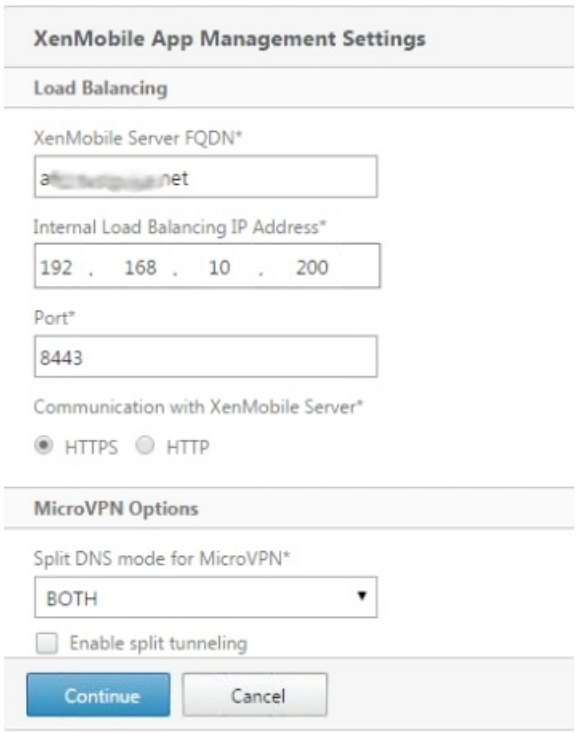
Die von Ihnen konfigurierten IP-Adressen für den XenMobile-Server werden angezeigt.

12. Geben Sie auf der Seite **Load Balancing** den vollqualifizierten Domänennamen (FQDN) für den XenMobile-Server und eine nur für MAM gültige IP-Adresse für internes Load Balancing ein.

13. Da dies eine SSL-Offloadbereitstellung ist, wählen Sie **HTTP** in **Communication with XenMobile Server**.

Die Einstellung für **Split DNS mode for MicroVPN** ist **BOTH**.

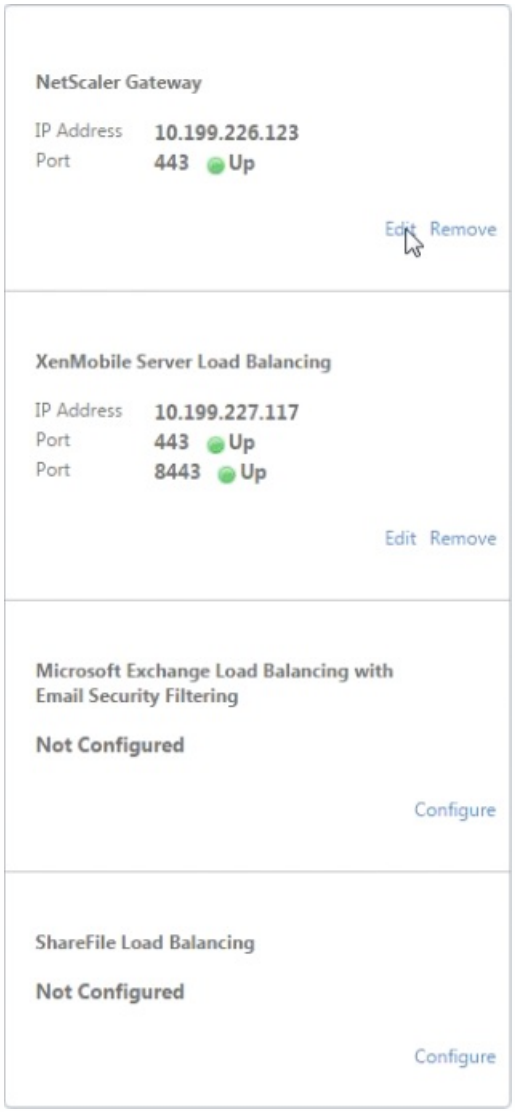
14. Klicken Sie auf **Weiter**.



Die von Ihnen konfigurierten IP-Adressen für den XenMobile-Server werden angezeigt.

15. Klicken Sie auf **Weiter**.

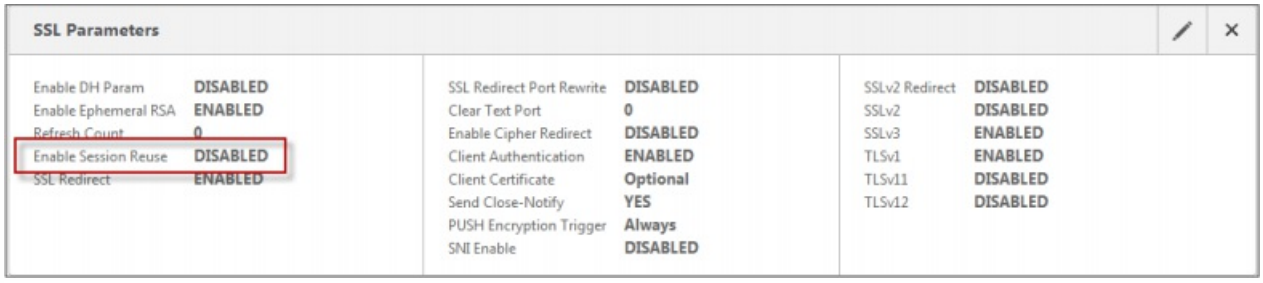
Vergewissern Sie sich im NetScaler-Dashboard, dass NetScaler Gateway und XenMobile Load Balancing folgendermaßen konfiguriert wurden:



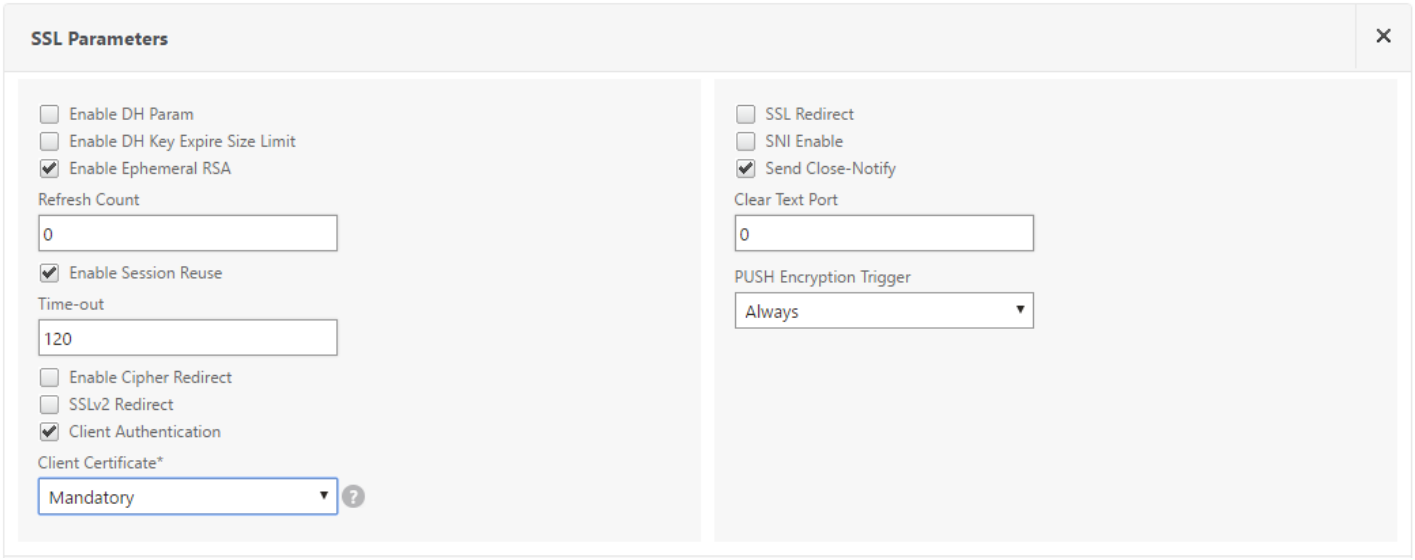
16. Wenn Sie in den Benutzerzertifikaten sAMAccount-Attribute anstelle des UPN (Benutzerprinzipalname) verwenden, konfigurieren Sie das Zertifikatprofil gemäß den Anweisungen im nächsten Abschnitt.

Manuelles Konfigurieren von NetScaler Gateway für die Zertifikatauthentifizierung

1. Aktualisieren Sie unter **Traffic Management > Load Balancing > Virtual Servers** für jeden virtuellen Server (443 und 8443) die Einstellung für **SSL Parameters**, indem Sie **Enable Session Reuse** auf **DISABLED** festlegen.



2. Wählen Sie auf dem virtuellen NetScaler Gateway-Server unter **Enable Client Authentication -> Client Certificate** die Option **Client Authentication** und für **Client Certificate** die Option **Mandatory**.



3. Erstellen Sie eine neue Authentifizierungszertifikatrichtlinie, damit XenMobile den Parameter **userPrincipalName** bzw. **sAMAccount** aus dem von Worx Home für NetScaler Gateway bereitgestellten Clientzertifikat extrahieren kann.

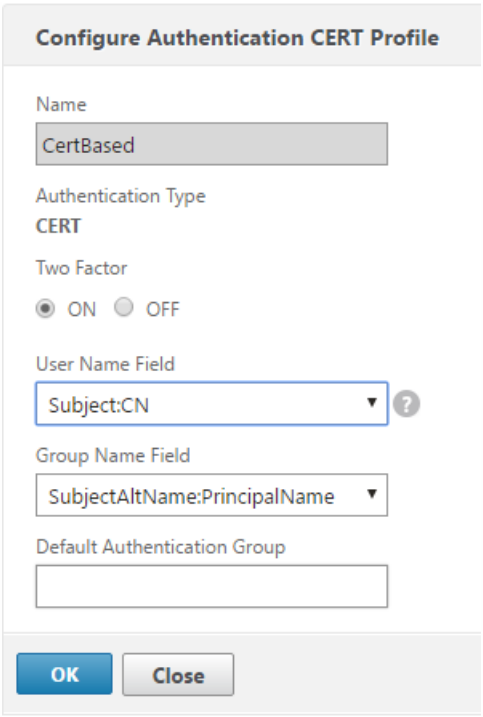
4. Legen Sie die folgenden Parameter für das Zertifikatprofil fest:

Authentication Type: **CERT**

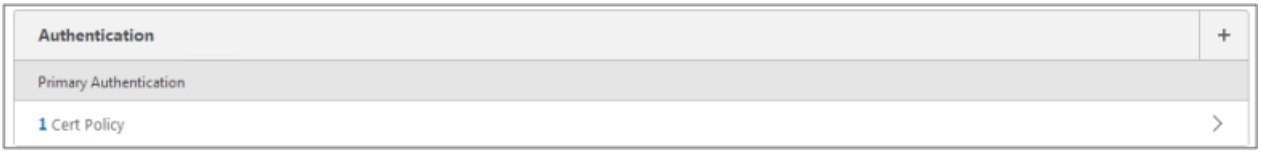
Two Factor: **ON** oder **OFF**

User Name Field: **Subject:CN**

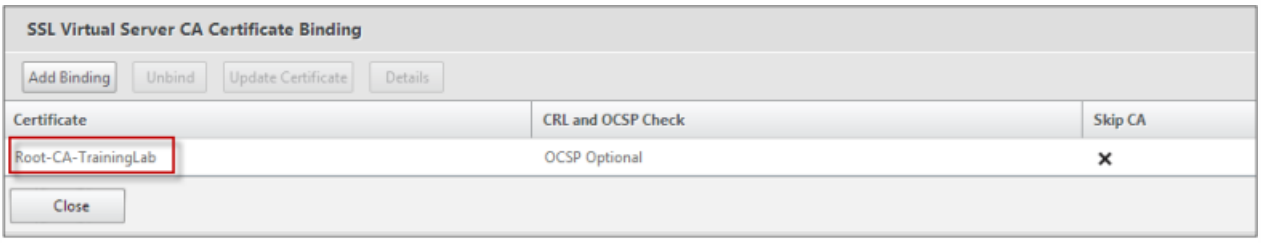
Group Name Field: **SubjectAltName:PrincipalName**

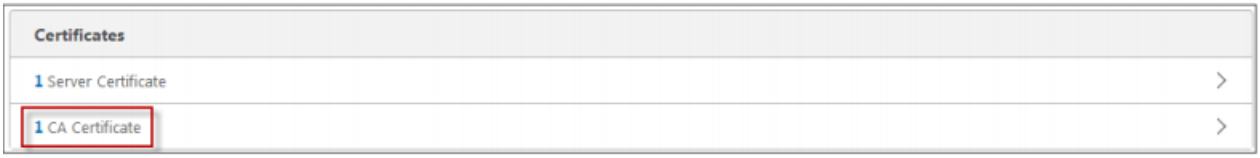


5. Binden Sie ausschließlich die Zertifikatauthentifizierungsrichtlinie unter **Primary Authentication** auf dem virtuellen NetScaler Gateway-Server.



6. Binden Sie das Stammzertifizierungsstellenzertifikat für die Prüfung der Vertrauensstellung des an NetScaler Gateway übergebenen Clientzertifikats.





Problembehandlung bei der

Clientzertifikatkonfiguration

Nach einer erfolgreichen Konfiguration ist der Workflow für Benutzer wie folgt:

1. Der Benutzer registriert sein mobiles Gerät.

2. XenMobile fordert den Benutzer auf, eine Worx-PIN zu erstellen.

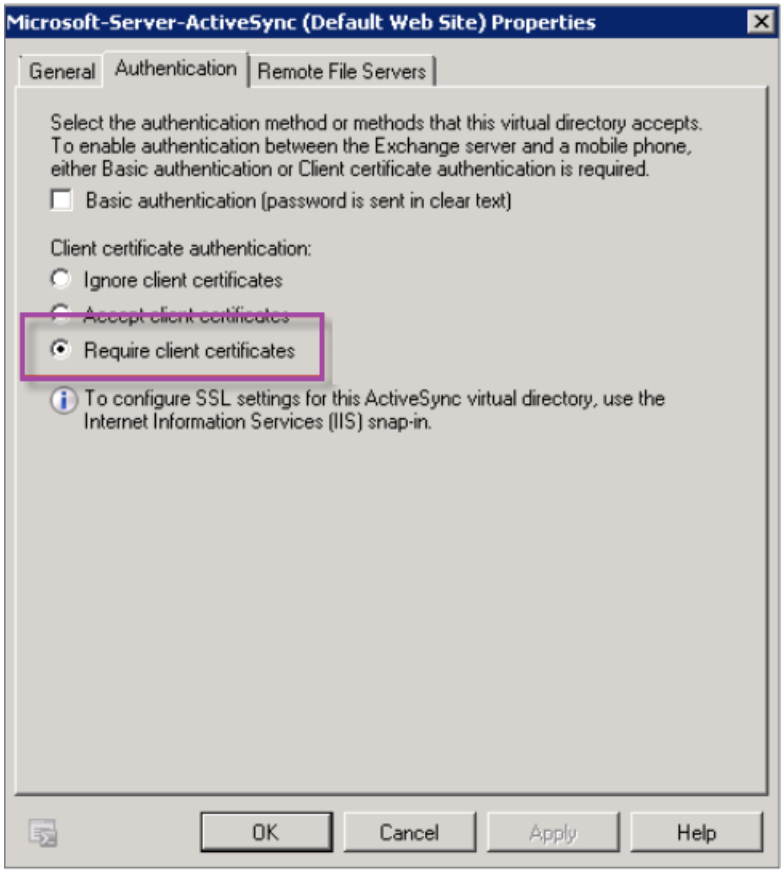
3. Der Benutzer wird an den WorxStore weitergeleitet.

4. Wenn der Benutzer WorxMail für iOS, Android oder Windows Phone 8.1 startet, wird er nicht zur Eingabe von Anmeldeinformationen zum Konfigurieren des Postfachs aufgefordert. Stattdessen fordert WorxMail das Clientzertifikat aus Worx Home an und sendet es zur Authentifizierung an Microsoft Exchange Server. Wenn XenMobile beim Starten von WorxMail durch die Benutzer die Eingabe von Anmeldeinformationen anfordert, prüfen Sie die Konfiguration.

Wenn die Benutzer WorxMail herunterladen und installieren können, die Postfachkonfiguration jedoch nicht abgeschlossen werden kann, führen Sie folgende Schritte aus:

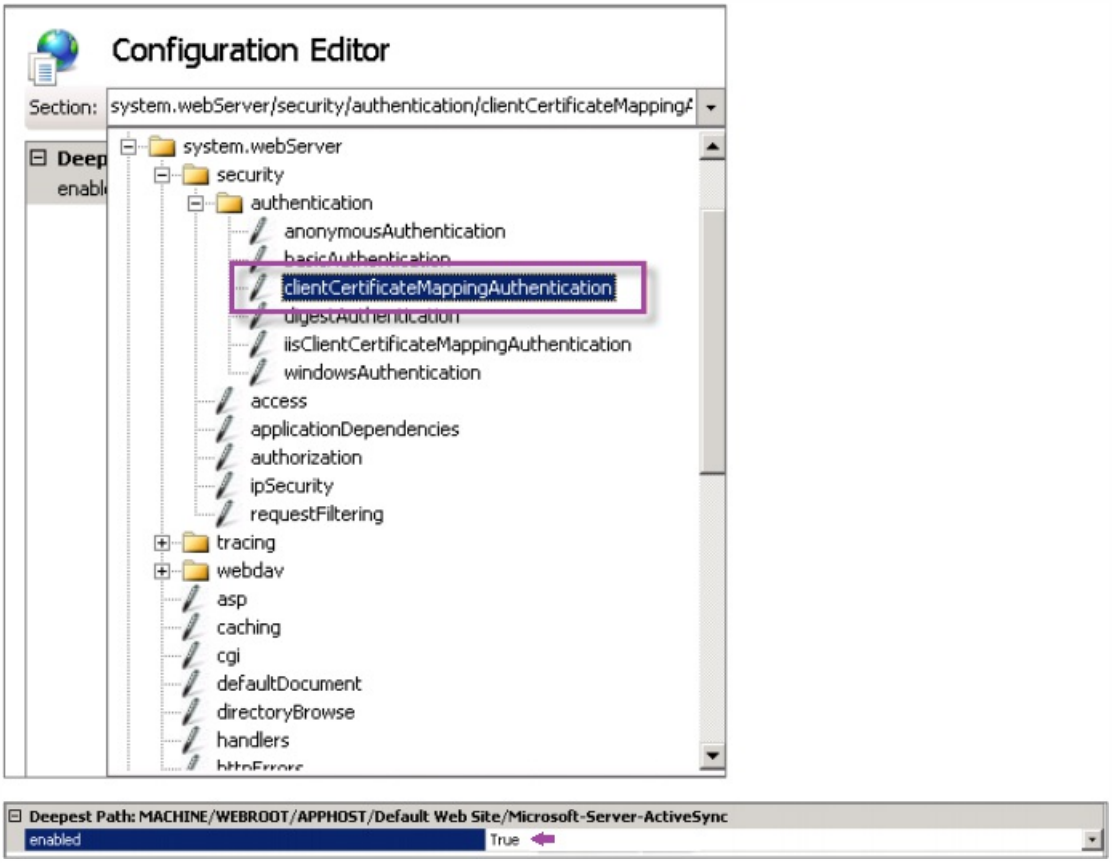
1. Wenn Microsoft Exchange Server ActiveSync private SSL-Serverzertifikate zum Schützen des Datenverkehrs verwendet, vergewissern Sie sich, dass das Stamm- und Zwischenzertifikat auf dem Mobilgerät installiert sind.

2. Vergewissern Sie sich, dass für ActiveSync der Authentifizierungstyp **Clientzertifikate anfordern** festgelegt ist.



3. Vergewissern Sie sich, dass in Microsoft Exchange Server für die Site **Microsoft-Server-ActiveSync** die

Authentifizierung über Clientzertifikatzuordnung aktiviert ist (sie ist standardmäßig deaktiviert). Die Option ist im Konfigurationseditor unter **Sicherheit > Authentifizierung**.



Hinweis: Klicken Sie nach der Auswahl von **True** auf **Anwenden**, damit die Änderungen wirksam werden.

4. Überprüfen Sie die NetScaler Gateway-Einstellungen in der XenMobile-Konsole: Vergewissern Sie sich, dass **Benutzerzertifikat für Authentifizierung bereitstellen** auf **EIN** festgelegt ist und für **Anmeldeinformationsanbieter** das richtige Profil ausgewählt wurde (siehe "Konfigurieren der NetScaler-Zertifikatbereitstellung in XenMobile" oben).

Ermitteln, ob das Clientzertifikat auf einem Mobilgerät bereitgestellt wurde:

1. Navigieren Sie in der XenMobile-Konsole zu **Verwalten > Geräte** und wählen Sie das Gerät.

2. Klicken Sie auf **Bearbeiten** oder **Mehr anzeigen**.

3. Navigieren Sie zum Bereich **Bereitstellungsgruppen** und suchen Sie folgenden Eintrag:

    NetScaler Gateway-Anmeldeinformationen: Requested credential, CertId=

Überprüfen, ob die Clientzertifikataushandlung aktiviert wurde:

1. Führen Sie folgenden netsh-Befehl aus, um die auf der IIS-Website gebundene SSL-Zertifikatkonfiguration anzuzeigen:

    netsh http show sslcert

2. Wenn der Wert für **Negotiate Client Certificate** mit **Disabled** angegeben ist, aktivieren Sie die Aushandlung mit folgendem Befehl:

netsh http delete sslcert ipport=0.0.0.0:443

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

Beispiel:

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

Wenn Sie über XenMobile keine Stamm-/Zwischenzertifikate auf einem Windows Phone 8.1-Gerät bereitstellen können, gehen Sie folgendermaßen vor:

- Senden Sie Stamm-/Zwischenzertifikate (CER-Dateien) per E-Mail an das Windows Phone 8.1-Gerät und installieren Sie sie direkt.

Wenn WorxMail nicht unter Windows Phone 8.1 installiert werden kann, gehen Sie folgendermaßen vor:

- Vergewissern Sie sich, dass das Anwendungsregistrierungstoken (.AETX) mit XenMobile über die Enterprise Hub-Richtlinie bereitgestellt wird.
- Vergewissern Sie sich, dass das Anwendungsregistrierungstoken mit dem gleichen Enterprise-Zertifikat des Zertifikatanbieters erstellt wurde, das zum Umschließen von Apps und zum Signieren von Worx Home-Apps verwendet wird.
- Vergewissern Sie sich, dass zum Signieren und Umschließen von Worx Home, WorxMail und Anwendungsregistrierungstoken die gleiche Aussteller-ID verwendet wird.

PKI-Entitäten

Oct 13, 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

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 ZS-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.

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.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren** > **Einstellungen** > **Mehr** > **PKI-Entitäten**.

2. Klicken Sie auf der Seite **PKI-Entitäten** auf **Hinzufügen**.

Eine Liste mit den Typen der PKI-Entitäten, die Sie hinzufügen können, wird angezeigt.

3. Klicken Sie auf **Generic PKI-Entität**.

Die Seite "Generic PKI-Entität: Allgemeine Informationen" wird angezeigt.

4. Führen Sie auf der Seite **Generic PKI-Entität: Allgemeine Informationen** folgende Schritte aus:

- **Name**: Geben Sie einen aussagekräftigen Namen für die PKI-Entität ein.
- **WSDL URL**: Geben Sie den Speicherort der WSDL mit der Beschreibung des Adapters ein.
- **Authentifizierungstyp**: Klicken Sie auf die Authentifizierungsmethode, die Sie verwenden möchten.
- **Ohne**
- **HTTP Basic**: Geben Sie Benutzername und Kennwort für die Verbindung mit dem Adapter ein.
- **Clientzertifikat**: Wählen Sie das richtige SSL-Clientzertifikat aus.

5. Klicken Sie auf **Weiter**.

Die Seite "Generic PKI-Entität: Adapterfunktionen" wird angezeigt.

6. Prüfen Sie auf der Seite **Generic PKI-Entität: Adapterfunktionen** die Funktionen und Parameter des Adapters und klicken Sie dann auf **Weiter**.

Die Seite **Generic PKI-Entität: Ausstellen von ZS-Zertifikaten** wird angezeigt.

7. Wählen Sie auf der Seite "Generic PKI-Entität: Ausstellen von ZS-Zertifikaten" die Zertifikate aus, die Sie für die Entität verwenden möchten.

Hinweis: Obwohl Entitäten 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 der Einstellung **Anmeldeinformationsanbieter** auf der Seite **Verteilung** eines der hier konfigurierten Zertifikate aus.

8. Klicken Sie auf **Speichern**.

Die Entität wird in der Tabelle der PKI-Entitäten angezeigt.

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.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben und dann auf **Mehr** > **PKI-Entitäten**.

2. Klicken Sie auf der Seite **PKI-Entitäten** auf **Hinzufügen**.

Eine Liste mit den Typen der PKI-Entitäten, die Sie hinzufügen können, wird angezeigt.

3. Klicken Sie auf **Microsoft Zertifikatdiensteentität**.

Die Seite **Microsoft Zertifikatdiensteentität: Allgemeine Informationen** wird angezeigt.

4. Führen Sie auf der Seite Microsoft Zertifikatdiensteentität: Allgemeine Informationen folgende Schritte aus:

- Name: Geben Sie einen Namen für die neue Entität ein. Der Name von Entitäten muss eindeutig sein.
- Stamm-URL des Webregistrierungsdiensts: 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.
- certnew.cer page name: Name der certnew.cer-Seite. Verwenden Sie den Standardnamen, es sei denn, Sie haben die Seite aus irgendeinem Grund umbenannt.
- certfnsh.asp: Name der certfnsh.asp-Seite. Verwenden Sie den Standardnamen, es sei denn, Sie haben die Seite aus irgendeinem Grund umbenannt.
- Authentifizierungstyp: Klicken Sie auf die Authentifizierungsmethode, die Sie verwenden möchten.
- Keine
- HTTP Basic: Geben Sie den Benutzernamen und das Kennwort für die Verbindung ein.
- Clientzertifikat: Wählen Sie das richtige SSL-Clientzertifikat aus.

5. Klicken Sie auf **Weiter**.

Die Seite **Microsoft Zertifikatdiensteentität: Vorlagen** 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.

Informationen zu Voraussetzungen für Microsoft-Zertifikatdienstvorlagen finden Sie in der Microsoft-Dokumentation auf Ihrer Version des Microsoft-Servers. Außer den unter Zertifikate aufgeführten Zertifikatformaten gibt es in XenMobile keine weiteren Voraussetzungen für verteilte Zertifikate.

6. Klicken Sie auf der Seite **Microsoft Zertifikatdiensteentität: Vorlagen** auf **Hinzufügen**, geben Sie den Namen der Vorlage ein und klicken Sie auf **Speichern**. Wiederholen Sie diesen Schritt für jede Vorlage, die Sie hinzufügen möchten.

7. Klicken Sie auf **Weiter**.

Die Seite **Microsoft Zertifikatdiensteentität: HTTP-Parameter** 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.

8. Klicken Sie auf der Seite **Microsoft Zertifikatdiensteentität: HTTP-Parameter** auf **Hinzufügen**, geben Sie Namen und Wert der gewünschten HTTP-Parameter ein und klicken Sie auf **Weiter**.

Die Seite **Microsoft Zertifikatdiensteentität: ZS-Zertifikate** 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.

9. Wählen Sie auf der Seite **Microsoft Zertifikatdiensteentität: ZS-Zertifikate** die Zertifikate aus, die Sie für die Entität verwenden möchten.

10. Klicken Sie auf **Speichern**.

Die Entität wird in der Tabelle der PKI-Entitäten angezeigt.

XenMobile unterstützt Zertifikatsperrlisten nur für Drittanbieterzertifizierungsstellen. Wenn Sie eine Microsoft-Zertifizierungsstelle konfiguriert haben, wird in XenMobile zum Verwalten der Zertifikatsperre NetScaler verwendet. Bedenken Sie beim Konfigurieren der Clientzertifikatauthentifizierung, ob Sie die NetScaler-Einstellung für Zertifikatsperrlisten **Enable CRL Auto Refresh** konfigurieren müssen. Dadurch wird verhindert, dass Benutzer von Geräten im MAM-Only-Modus sich mit einem auf dem Gerät vorhandenen Zertifikat authentifizieren. XenMobile stellt ein neues Zertifikat aus, da die Generierung von Zertifikaten durch Benutzer nach Zertifikatsperre nicht unterbunden wird. Diese Einstellung erhöht die Sicherheit von PKI-Entitäten, wenn über die Zertifikatsperrliste auf abgelaufene PKI-Entitäten geprüft wird.

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.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben und dann auf **Mehr** > **PKI-Entitäten**.

2. Klicken Sie auf der Seite **PKI-Entitäten** auf **Hinzufügen**.

Eine Liste mit den Typen der PKI-Entitäten, die Sie hinzufügen können, wird angezeigt.

3. Klicken Sie auf **Eigenverwaltete ZS**.

Die Seite **Eigenverwaltete ZS: Allgemeine Informationen** wird angezeigt.

4. Führen Sie auf der Seite **Eigenverwaltete ZS** folgende Schritte aus:

- **Name**: Geben Sie einen aussagekräftigen Namen für die eigenverwaltete ZS ein.
- **ZS-Zertifikate zum Signieren von Zertifikatanforderungen**: Klicken Sie auf das Zertifikat, das von der eigenverwalteten ZS zum Signieren von Zertifikatanforderungen verwendet werden soll. Die Liste der Zertifikate wird aus den von Ihnen über **Konfigurieren** > **Einstellungen** > **Zertifikate** hochgeladenen Zertifizierungsstellenzertifikaten mit privatem Schlüssel generiert.

5. Klicken Sie auf **Weiter**.

Die Seite **Eigenverwaltete ZS: Parameter** wird angezeigt.

6. Führen Sie auf der Seite **Eigenverwaltete ZS: Parameter** folgende Schritte aus:
- **Seriennummergenerator**: Die eigenverwaltete ZS generiert Seriennummern für die von ihr herausgegebenen Zertifikate. Klicken Sie in dieser Liste auf **Sequenziell** oder **Nichtsequenziell**, um zu bestimmen, wie die Nummern generiert werden sollen.
- **Nächste Seriennummer**: Geben Sie einen Wert für die nächste Seriennummer ein.
- **Zertifikat gültig für**: Geben Sie die Anzahl der Tage ein, für die das Zertifikat gültig sein soll.
- **Schlüsselverwendung**: Legen Sie den Zweck der von der eigenverwalteten ZS herausgegebenen Zertifikate fest, indem Sie die entsprechenden Schlüssel auf **Ein** setzen. Im Anschluss an diese Einstellung ist die Zertifizierungsstelle auf die Ausstellung von Zertifikaten für diese Zwecke beschränkt.
- **Erweiterte Schlüsselverwendung**: Zum Hinzufügen weiterer Parameter klicken Sie auf **Hinzufügen**, geben Sie den Schlüsselnamen ein und klicken Sie auf **Speichern**.

7. Klicken Sie auf **Weiter**.

Die Seite **Eigenverwaltete ZS: Verteilung** wird angezeigt.

8. Wählen Sie auf der Seite **Eigenverwaltete ZS: Verteilung** einen Verteilungsmodus aus:

- **Zentralisiert: Schlüssel serverseitig generieren**: Citrix empfiehlt diese zentrale Verteilung. Die privaten Schlüssel werden auf dem Server generiert und gespeichert und auf die Benutzergeräte verteilt.

- **Verteilt: Schlüssel geräteseitig generieren**: Die privaten Schlüssel werden auf den Benutzergeräten generiert. Beim verteilten Modus wird SCEP verwendet und es ist ein RA-Verschlüsselungszertifikat mit KeyUsage "keyEncryption" sowie ein RA-Signaturzertifikat mit KeyUsage "digitalSignature" erforderlich. Das gleiche Zertifikat kann für Verschlüsselung und Signieren verwendet werden.

9. Klicken Sie auf **Weiter**.

Die Seite **Eigenverwaltete ZS: Online Certificate Status Protocol (OCSP)** wird angezeigt.

Führen Sie auf der Seite **Eigenverwaltete ZS: Online Certificate Status Protocol (OCSP)** folgende Schritte aus:

- Wenn Sie den von dieser Zertifizierungsstelle signierten Zertifikaten eine AuthorityInfoAccess-Erweiterung (RFC2459) hinzufügen möchten, legen Sie **OCSP-Unterstützung für diese ZS aktivieren** auf **Ein** fest. Diese Erweiterung verweist auf den OCSP-Responder der Zertifizierungsstelle unter https://server/instance/ocsp.
- Wenn Sie OCSP-Unterstützung aktiviert haben, wählen Sie ein OSCP-Zertifizierungsstellenzertifikat aus. Die Liste der Zertifikate wird aus den von Ihnen in XenMobile hochgeladenen Zertifizierungsstellenzertifikaten generiert.

10. Klicken Sie auf **Speichern**.

Die eigenverwaltete ZS wird in der Tabelle der PKI-Entitäten angezeigt.

Anmeldeinformationsanbieter

Jul 28, 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.

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").

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

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.

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.

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 ZS-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-Konsole auf das Zahnradsymbol rechts oben und dann auf **Mehr** > **Anbieter für Anmeldeinformationen**.

2. Klicken Sie auf der Seite **Anbieter für Anmeldeinfo** auf **Hinzufügen**.

Es wird die Seite **Anbieter für Anmeldeinformationen: Allgemeine Informationen** angezeigt.

3. Führen Sie auf der Seite **Anbieter für Anmeldeinformationen: Allgemeine Informationen** folgende Schritte aus:

- **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.
- **Beschreibung**: 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.
- **Ausstellende Entität**: Klicken Sie auf die ausstellende Entität.
- **Ausstellungsmethode**: Klicken Sie auf **Zertifikat signieren** oder **Zertifikat abrufen** zu Festlegen der Methode für den Bezug von Zertifikaten von der konfigurierten Entität. Verwenden Sie für die Clientzertifikatauthentifizierung **Signieren**.
- Wenn die Vorlagenliste verfügbar ist, wählen Sie eine Vorlage für den Anmeldeinformationsanbieter aus.

4. Klicken Sie auf **Weiter**.

Hinweis: Die Vorlagen werden verfügbar, wenn Microsoft-Zertifikatdienste-Entitäten über **Einstellungen** > **Mehr** > **PKI-Entitäten** hinzugefügt werden.

Es wird die Seite **Anbieter für Anmeldeinformationen: Zertifikatsignieranforderung** angezeigt.

5. Führen Sie auf der Seite **Anbieter für Anmeldeinformationen: Zertifikatsignieranforderung** folgende Schritte aus:

- **Schlüsselalgorithmus**: Klicken Sie auf den Schlüsselalgorithmus für das neue Schlüsselpaar. Verfügbare Werte sind **RSA**, **DSA** und **ECDSA**.
- **Schlüsselgröße**: 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.

- **Signaturalgorithmus**: Klicken Sie auf einen Wert für das neue Zertifikat. Welche Werte zulässig sind, hängt vom Schlüsselalgorithmus ab.
- **Antragstellername**: 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.

  Verwenden Sie für die Clientzertifikatauthentifizierung beispielsweise die folgenden Einstellungen:

  Schlüsselalgorithmus: RSA
  Schlüsselgröße: 2048
  Signaturalgorithmus: SHA1withRSA
  Antragstellername: cn=$user.username

6. Zum Hinzufügen eines neuen Eintrags zur Tabelle **Alternative Antragstellernamen** klicken Sie auf **Hinzufügen**. Wählen Sie den Typ des alternativen Namens aus und geben Sie einen Wert in der zweiten Spalte ein.

Geben Sie für die Clientzertifikatauthentifizierung Folgendes an:

  Typ: Benutzerprinzipalname
  Wert: $user.userprincipalname

Hinweis: Wie beim Antragstellernamen können Sie in dem Wertefeld XenMobile-Makros verwenden.

7. Klicken Sie auf **Weiter**.

Es wird die Seite **Anbieter für Anmeldeinformationen: Verteilung** angezeigt.

8. Führen Sie auf der Seite **Anbieter für Anmeldeinformationen: Verteilung** folgende Schritte aus:

- Klicken Sie in der Liste **Zertifikat der austellenden ZS** auf das angebotene ZS-Zertifikat. Da der Anmeldeinformationsanbieter eine eigenverwaltete Zertifizierungsstelle verwendet, erhält er immer das für die Entität selbst konfigurierte ZS-Zertifikat. Die Aufführung hier erfolgt aus Gründen der Konsistenz mit Konfigurationen, in denen externe Entitäten verwendet werden.
- Wählen Sie für **Verteilungsmodus wählen** eine der folgenden Methoden zum Generieren und Verteilen von Schlüsseln:
  - **Bevorzugt zentralisiert: Schlüssel serverseitig generieren**: 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.
  - **Bevorzugt verteilt: Schlüssel geräteseitig generieren**: 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.
  - **Nur verteilt: Schlüssel geräteseitig generieren**: Diese Option funktioniert wie "Bevorzugt verteilt: Schlüssel geräteseitig generieren", doch da sie anstelle einer Bevorzugung eine Ausschließlichkeit definiert, steht keine Option zur Verfügung, wenn die geräteseitige Schlüsselgenerierung fehlschlägt oder nicht verfügbar ist.

Wenn Sie **Bevorzugt verteilt: Schlüssel geräteseitig generieren** oder **Nur verteilt: Schlüssel geräteseitig generieren** ausgewählt haben, klicken Sie auf das gewünschte RA-Signaturzertifikat und das RA-Verschlüsselungszertifikat. Das gleiche Zertifikat kann für beides verwendet werden. Es werden neue Felder für diese Zertifikate eingeblendet.

9. Klicken Sie auf **Weiter**.

Es wird die Seite **Anbieter für Anmeldeinformationen: XenMobile-Sperrung** angezeigt. Auf dieser Seite konfigurieren Sie die Bedingungen, unter denen XenMobile Zertifikate, die über diese Anbieterkonfiguration ausgestellt wurden, intern als gesperrt kennzeichnet.

12. Führen Sie auf der Seite **Anbieter für Anmeldeinformationen: XenMobile-Sperrung** folgende Schritte aus:

- Wählen Sie für **Ausgestellte Zertifikate widerrufen** aus, wann Zertifikate gesperrt werden sollen.
- Wenn XenMobile eine Benachrichtigung bei Sperrung des Zertifikats senden soll, legen Sie für **Benachrichtigung senden** die Einstellung **Ein** fest und wählen Sie eine Benachrichtigungsvorlage aus.

- Wenn das Zertifikat bei Sperrung durch XenMobile in der PKI gesperrt werden soll, legen Sie für **Zertifikat in PKI widerrufen** die Option **Ein** fest und klicken Sie in der Liste **Entität** auf eine Vorlage. Die Liste "Entität" enthält alle verfügbaren GPKI-Entitäten mit Sperrfunktion. Wenn das Zertifikat von XenMobile gesperrt wird, wird ein Sperraufruf an die in der Liste "Entität" ausgewählte PKI gesendet.

13. Klicken Sie auf **Weiter**.

Es wird die Seite **Anbieter für Anmeldeinformationen: PKI-Sperrung** 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.

14. Führen Sie auf der Seite **Anbieter für Anmeldeinformationen: PKI-Sperrung** folgende Schritte aus, wenn Sie Zertifikate über die PKI sperren möchten:

- Ändern Sie die Einstellung für **Prüfen der externen Zertifikatsperre aktivieren** in **Ein**. Zusätzliche Felder für die Sperrung werden angezeigt.
- Klicken Sie in der Liste **OCSP-Responder für ZS-Zertifikat** auf den Distinguished Name (DN) des Antragstellers des Zertifikats. **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
- Klicken Sie in der Liste **Wenn Zertifikat widerrufen wird** auf eine der folgenden Optionen zum Festzulegen der in der PKI bei Sperrung des Zertifikats auszuführenden Aktionen:

  Nichts tun

  Zertifikat erneuern

  Gerät widerrufen und löschen

- Wenn XenMobile eine Benachrichtigung bei Sperrung des Zertifikats senden soll, legen Sie für **Benachrichtigung senden** die Einstellung **Ein** fest.

Sie können eine von zwei Benachrichtigungsoptionen auswählen:

- Mit **Benachrichtigungsvorlage wählen** können Sie einen vorhandenen Benachrichtigungstext auswählen und ggf. anpassen. Die entsprechenden Vorlagen sind in der Liste der Benachrichtigungsvorlagen aufgeführt.
- Mit **Geben Sie die Benachrichtigungsdetails ein** 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.

15. Klicken Sie auf **Weiter**.

Es wird die Seite **Anbieter für Anmeldeinformationen: Verlängerung** 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

16. Führen Sie auf der Seite **Anbieter für Anmeldeinformationen: Verlängerung** folgende Schritte aus, wenn Zertifikate bei Ablauf verlängert werden sollen: Legen Sie für **Zertifikate erneuern, wenn sie ablaufen** auf **Ein** fest.

Zusätzliche Felder werden eingeblendet.

- Geben Sie im Feld **Benachrichtigung bei Zertifikatablauf in** die Zeit vor Ablauf des Zertifikats in Tagen ein, zu der die Verlängerung erfolgen soll.
- Wählen Sie optional **Bereits abgelaufene Zertifikate nicht erneuern** aus. **Hinweis:** In diesem Zusammenhang bedeutet "bereits abgelaufen", dass das NotAfter-Datum des Zertifikats in der Vergangenheit liegt, und nicht, dass das Zertifikat gesperrt wurde. XenMobile verlängert keine intern gesperrten Zertifikate.

17. Wenn XenMobile eine Benachrichtigung bei Verlängerung des Zertifikats senden soll, legen Sie **Benachrichtigung senden** auf **Ein** fest. Sie können eine von zwei Benachrichtigungsoptionen auswählen:

- Mit **Benachrichtigungsvorlage wählen** können Sie einen vorhandenen Benachrichtigungstext auswählen und ggf. anpassen. Die entsprechenden Vorlagen sind in der Liste Benachrichtigungsvorlage.

- Mit **Geben Sie die Benachrichtigungsdetails ein** 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.

18. Wenn XenMobile eine Benachrichtigung bei anstehendem Ablauf des Zertifikats senden soll, legen Sie **Benachrichtigen, wenn Zertifikat bald abläuft** auf **Ein** fest. Sie können eine von zwei Benachrichtigungsoptionen auswählen:

- Mit **Benachrichtigungsvorlage wählen** können Sie einen vorhandenen Benachrichtigungstext auswählen und ggf. anpassen. Die entsprechenden Vorlagen sind in der Liste **Benachrichtigungsvorlage**.
- Mit **Geben Sie die Benachrichtigungsdetails ein** 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.

19. Geben Sie im Feld **Benachrichtigung bei Zertifikatablauf in** die Zeit vor Ablauf des Zertifikats in Tagen ein, zu der die Benachrichtigung gesendet werden soll.

20. Klicken Sie auf **Speichern**.

Der neue Anbieter wird der Tabelle der Anmeldeinformationsanbieter hinzugefügt.

Anfordern eines APNs-Zertifikats

Jul 28, 2016

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

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

Hinweis:

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

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

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

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

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 an der XenMobile-Konsole als Administrator an.
9. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
10. Klicken Sie auf **Zertifikate**. Die Seite **Zertifikate** wird angezeigt.
11. Klicken Sie auf **Importieren**. Das Dialogfeld **Importieren** wird angezeigt.
12. Klicken Sie im Menü **Importieren** auf **Keystore**.
13. Wählen Sie unter **Verwenden als** die Option **APNs**.
14. Klicken Sie zum Auswählen der **Schlüsselspeicherdatei** auf **Durchsuchen** und navigieren Sie zum Speicherort der Schlüsselspeicherdatei.
15. Geben Sie unter **Kennwort** das Kennwort für das Zertifikat ein.
16. Klicken Sie auf **Importieren**.

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. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie auf **Zertifikate**. Die Seite **Zertifikate** wird angezeigt.
3. Klicken Sie auf **Importieren**. Das Dialogfeld **Importieren** wird angezeigt.
4. Klicken Sie im Menü **Importieren** auf **Keystore**.
5. Wählen Sie unter **Verwenden als** die Option **APNs**.
6. Navigieren Sie zu der P12-Datei auf Ihrem Computer.
7. Geben Sie ein Kennwort ein und klicken Sie auf **Import**.

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 **Configure** > **Settings** > **Certificates**. Ist das Zertifikat abgelaufen, müssen Sie es nicht widerrufen.

1. Generieren Sie eine Zertifikatsignieranforderung mit Microsoft Internetinformationsdienste (IIS).
2. Laden Sie die neue CSR auf die XenMobile APNs CSR Signing-Website hoch und klicken Sie dann auf **Sign**.
3. Senden Sie die signierte Zertifikatsignieranforderung im Apple Push Certificate Portal an Apple.
4. Klicken Sie auf **Renew**.
5. Generieren Sie ein PCKS#12-APNs-Zertifikat (PFX-Datei) mit Microsoft IIS.
6. Aktualisieren Sie das neue APNs-Zertifikat in der XenMobile-Konsole. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
7. Klicken Sie auf **Zertifikate**. Die Seite **Zertifikate** wird angezeigt.
8. Klicken Sie auf **Importieren**. Das Dialogfeld **Importieren** wird angezeigt.
9. Klicken Sie im Menü **Importieren** auf **Keystore**.
10. Wählen Sie unter **Verwenden als** die Option **APNs**.
11. Navigieren Sie zu der P12-Datei auf Ihrem Computer.
12. Geben Sie ein Kennwort ein und klicken Sie auf **Import**.

Benutzerkonten, Rollen und Registrierungseinstellungen

Jul 28, 2016

In XenMobile konfigurieren Sie Benutzer und Gruppen, Rollen für Benutzer und Gruppen sowie den Registrierungsmodus und Einladungen auf der Seite Einstellungen der XenMobile-Konsole. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben, um die Seite **Einstellungen** zu öffnen.

Auf der Seite **Einstellungen** können Sie folgende Einstellungen ändern:

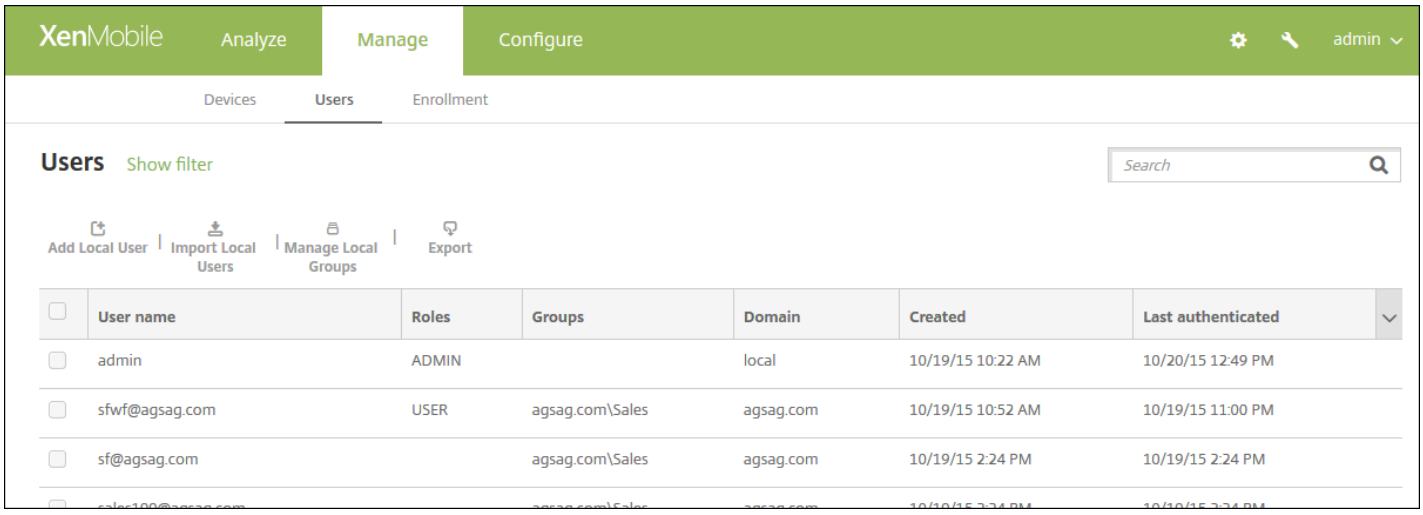
- Klicken Sie auf **Lokale Benutzer und Gruppen**, um Benutzerkonten manuell oder unter Verwendung einer CSV-Provisioningdatei für den Import hinzuzufügen und lokale Gruppen zu verwalten. Einzelheiten finden Sie in den folgenden Abschnitten:
  - Erstellen, Bearbeiten oder Löschen von lokalen Benutzern in XenMobile
  - Importieren von Benutzerkonten über eine CSV-Provisioningdatei und Provisioningdateiformate.
  - Hinzufügen oder Entfernen von Gruppen in XenMobile
- Klicken Sie auf **Registrierung** zum Konfigurieren von bis zu sieben Registrierungsmodi mit jeweils eigener Sicherheitsstufe und eigenem Verfahren und zum Senden von Registrierungseinladungen. Einzelheiten finden Sie in den folgenden Abschnitten:
  - Konfigurieren von Registrierungsmodi und Aktivieren des Selbsthilfeportals
  - Aktivieren von Autodiscovery für die Benutzerregistrierung in XenMobile
- Klicken Sie auf **Rollenbasierte Zugriffssteuerung**, um Benutzern und Gruppen vordefinierte Rollen bzw. Berechtigungssätze zuzuweisen. Diese Berechtigungen steuern den Zugriff der Benutzer auf Systemfunktionen. Einzelheiten finden Sie in den folgenden Abschnitten:
  - Konfigurieren von Rollen mit RBAC und RBAC-Rollen und -Berechtigungen
- Klicken Sie auf **Benachrichtigungsvorlagen**, 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. Einzelheiten finden Sie in den folgenden Abschnitten:
  - Erstellen und Aktualisieren von Benachrichtigungsvorlagen

Erstellen, Bearbeiten oder Löschen von lokalen Benutzern in XenMobile

Jul 28, 2016

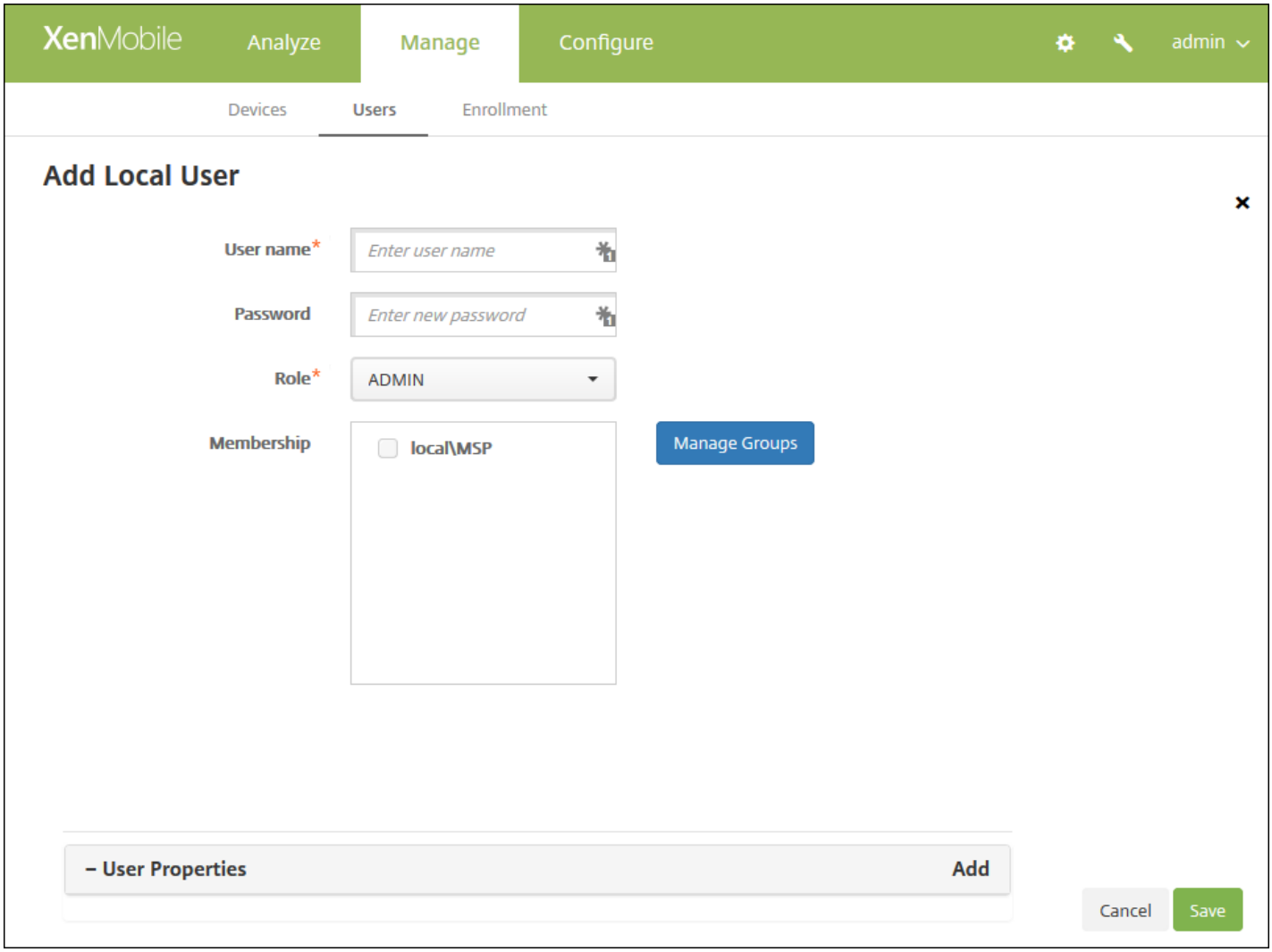
Sie können lokale Benutzerkonten in XenMobile manuell hinzufügen oder mit einer Provisioningdatei importieren. Eine Anleitung zum Importieren von Benutzern aus einer Provisioningdatei finden Sie unter Importieren von Benutzerkonten über eine CSV-Provisioningdatei.

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



Mit diesem Verfahren werden XenMobile Benutzer einzeln hinzugefügt. Zum Hinzufügen mehrerer Benutzer siehe Importieren von Benutzerkonten über eine CSV-Provisioningdatei.

1. Klicken Sie auf der Seite **Benutzer** auf **Lokalen Benutzer hinzufügen**. Die Seite **Lokalen Benutzer hinzufügen** wird angezeigt.



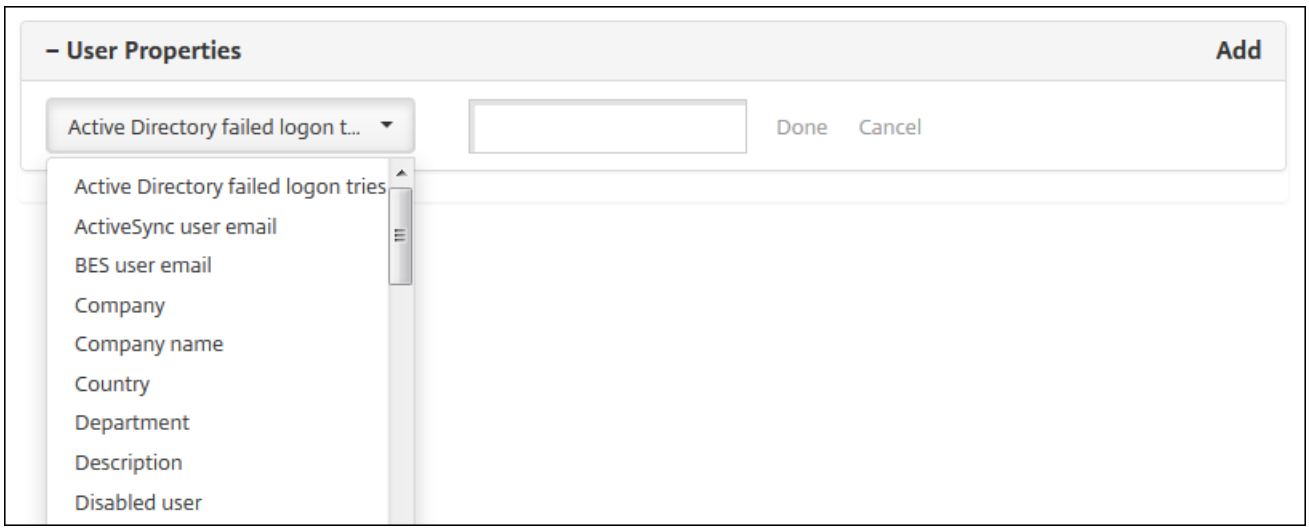
2. Konfigurieren Sie die folgenden Einstellungen:

- Benutzername: **Geben** Sie den Benutzernamen ein. Dies ist ein Pflichtfeld. Namen dürfen Leerstellen sowie Groß- und Kleinbuchstaben enthalten.
- **Kennwort**: Geben Sie ein optionales Benutzerkennwort ein.
- **Rolle**: Klicken Sie auf die Rolle des Benutzers. Weitere Informationen über Rollen finden Sie unter Konfigurieren von Rollen mit RBAC und RBAC-Rollen und -Berechtigungen. Mögliche Optionen:
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- **Mitgliedschaft**: Klicken Sie in der Liste auf die Gruppen, zu denen der Benutzer gehören soll.
- **Benutzereigenschaften**: Fügen Sie optional Benutzereigenschaften hinzu. Für jede Eigenschaft, die Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Benutzereigenschaften**: Klicken Sie in der Liste auf eine Eigenschaft und geben Sie das zugehörige Attribut im Feld daneben ein.
  - Klicken Sie auf **Fertig**, um die Benutzereigenschaft zu speichern oder auf **Abbrechen**, um sie nicht zu speichern.

    Hinweis: Zum Löschen einer vorhandenen Benutzereigenschaft zeigen Sie auf deren Zeile und klicken Sie auf das

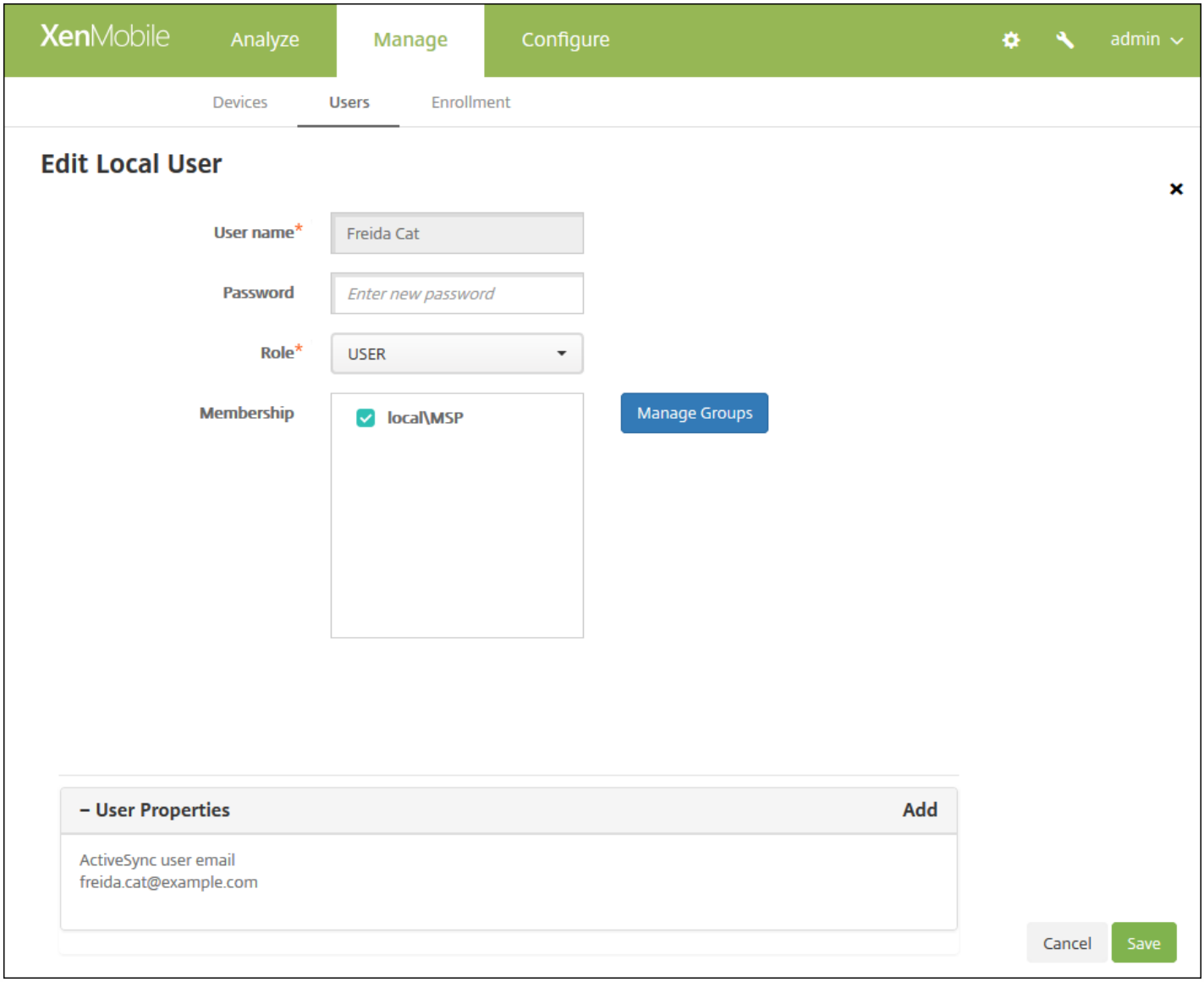
Papierkorbsymbol auf der rechten Seite. Die Eigenschaft wird sofort gelöscht.

Zum Bearbeiten einer Benutzereigenschaft klicken darauf und nehmen Sie die Änderungen vor. Klicken Sie auf **Fertig**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Eintrag unverändert zu lassen.



3. Klicken Sie auf **Speichern**.

1. Wählen Sie auf der Seite **Benutzer** den Benutzer in der Liste aus und klicken Sie auf **Bearbeiten**. Die Seite **Lokalen Benutzer bearbeiten** wird angezeigt. Weitere Informationen zum Auswählen von Elementen in Tabellen finden Sie unter Filter und Tabellen in der XenMobile-Konsole.



2. Ändern Sie nach Bedarf die folgenden Informationen:

- **Benutzername**: Sie können den Benutzernamen nicht ändern.
- **Kennwort**: Geben Sie ein Kennwort ein bzw. ändern Sie das vorhandene.
- **Rolle**: Klicken Sie auf die Rolle des Benutzers.
- **Mitgliedschaft**: Klicken Sie in der Liste auf die Gruppen, zu denen der Benutzer gehören soll. Zum Entfernen eines Benutzers aus einer Gruppe deaktivieren Sie das Kontrollkästchen neben dem Gruppennamen.
- **Benutzereigenschaften**: Führen Sie einen der folgenden Schritte aus:
  - Klicken Sie auf jede Eigenschaft, die Sie ändern möchten, und nehmen Sie die Änderungen vor. Klicken Sie auf **Fertig**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Eintrag unverändert zu lassen.
  - Für jede Eigenschaft, die Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
    - **Benutzereigenschaften**: Klicken Sie in der Liste auf eine Eigenschaft und geben Sie das zugehörige Attribut im Feld daneben ein.
    - Klicken Sie auf **Fertig**, um die Benutzereigenschaft zu speichern oder auf **Abbrechen**, um sie nicht zu speichern.
  - Zum Löschen einer Benutzereigenschaft zeigen Sie auf deren Zeile und klicken Sie auf das X auf der rechten Seite. Die Eigenschaft wird sofort gelöscht.

3. Klicken Sie auf **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Benutzer unverändert zu lassen.

1. Wählen Sie auf der Seite **Benutzer** in der Liste den Benutzer aus.

    Hinweis: Sie können mehrere Benutzer auswählen, indem Sie die Kontrollkästchen daneben aktivieren.

2. Klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt.

3. Klicken Sie auf **Löschen** zum Löschen des Benutzers oder auf **Abbrechen**, um ihn beizubehalten.

Importieren von Benutzerkonten

Oct 13, 2016

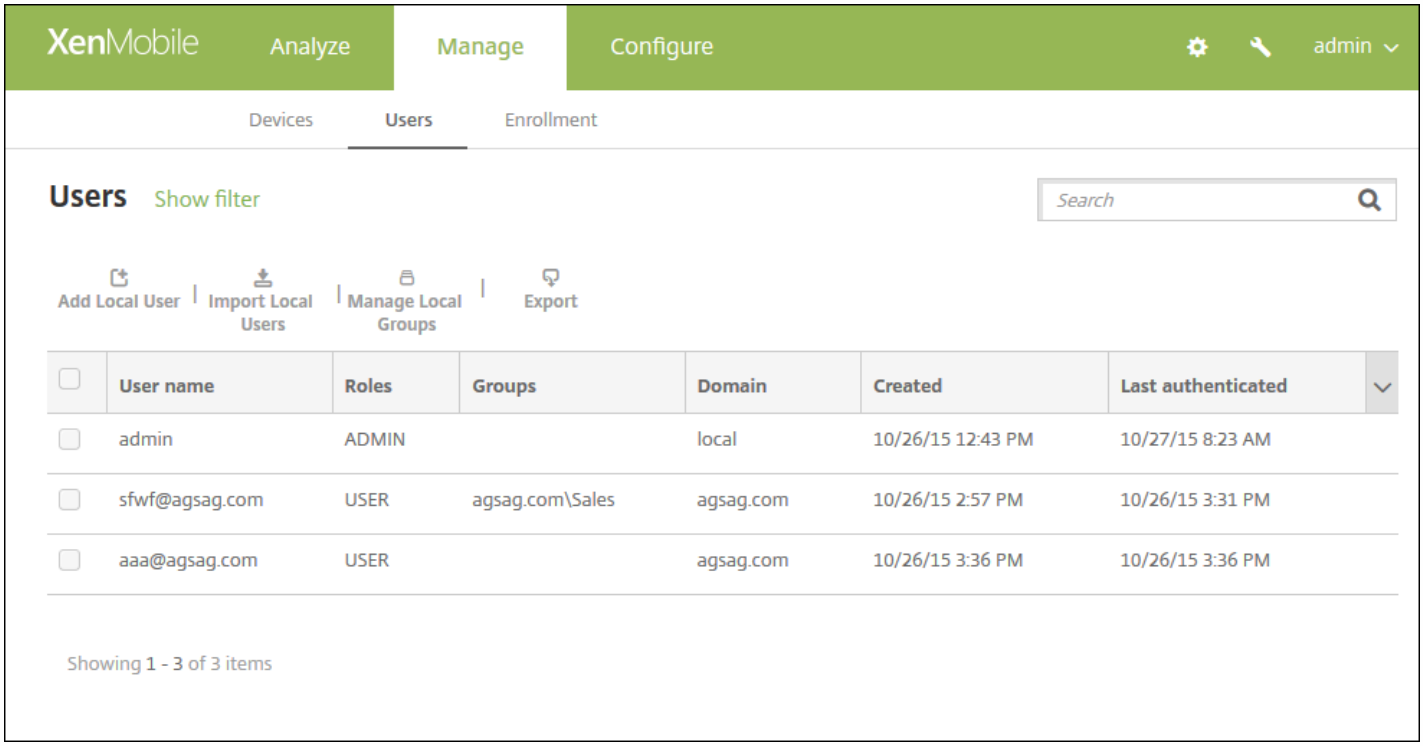
Sie können Benutzerkonten und Eigenschaften aus einer CSV-Datei, einer so genannten Provisioningdatei importieren, die Sie manuell erstellen können. Informationen zur Formatierung von Provisioningdateien finden Sie unter Provisioningdateiformate.

Hinweis:

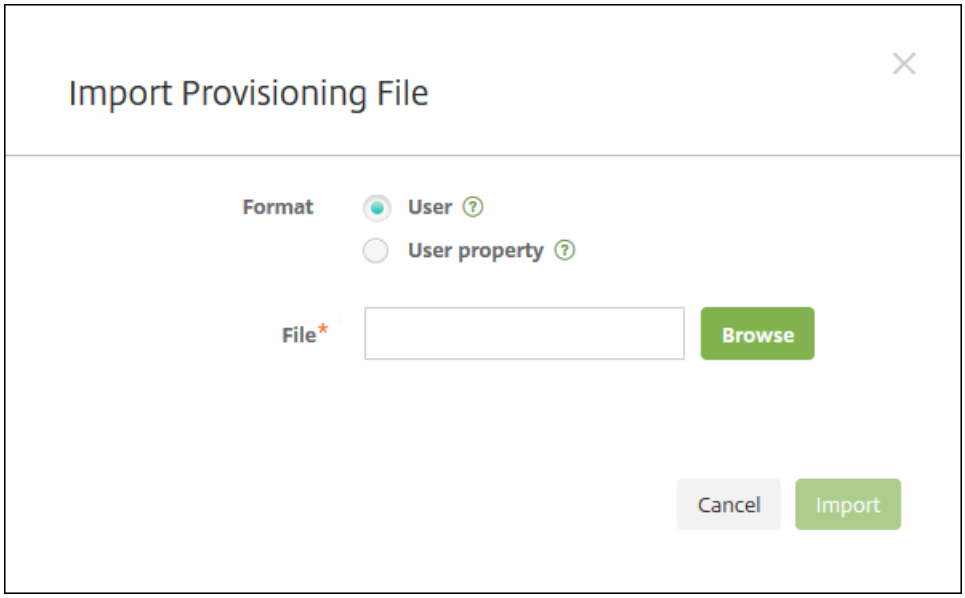
- Wenn Sie Benutzer aus einem LDAP-Verzeichnis importieren, verwenden Sie den Domänennamen zusammen mit dem Benutzernamen in der Importdatei. Beispiel: username@domain.com. Diese Syntax vermeidet zusätzliche Nachschlagevorgänge, die den Import verlangsamen.
- Beim Importieren von Benutzerkonten in das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



2. Klicken Sie auf **Lokale Benutzer importieren**. Das Dialogfeld **Provisioningdatei importieren** wird angezeigt.



3. Wählen Sie als Format für die Provisioningdatei **Benutzer** oder **Eigenschaft** aus.

4. Klicken Sie zur Auswahl der zu importierenden Provisioningdatei auf **Durchsuchen** und navigieren Sie zum Speicherort der Datei.

5. Klicken Sie auf **Importieren**.

Provisioningdateiformate

Aug 22, 2016

Eine manuell erstellte Provisioningdatei zum Importieren von Benutzerkonten und -eigenschaften in XenMobile muss eines der folgenden Formate haben:

- Felder der Provisioningdatei: userpassword;role;group1;group2
- Felder der Provisioningdatei für Benutzerattribute: 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: Die Eigenschaft "propertyV;test;1;2" würde als "propertyV\;test\;1\;2" in der Provisioningdatei eingegeben werden.
- 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\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01" bedeutet Folgendes:

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

Der Eintrag AUser0;1.password;USER;ActiveDirectory.test.net bedeutet Folgendes:

- Benutzer: AUser0
- Kennwort: 1.password
- Rolle: USER
- Gruppe: ActiveDirectory.test.net

Der Eintrag user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value, bedeutet:

- User: user01
- Eigenschaft 1
  - Name: propertyN
  - Wert: propertyV;test;1;2
- Eigenschaft 2:
  - Name: prop 2
  - Wert: prop2 value

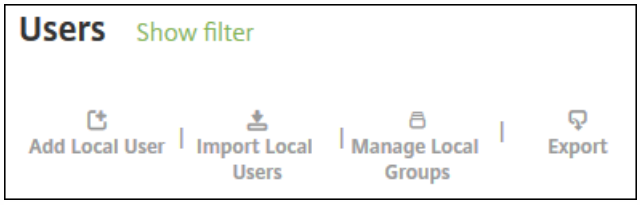
Hinzufügen oder Entfernen von Gruppen

Jul 28, 2016

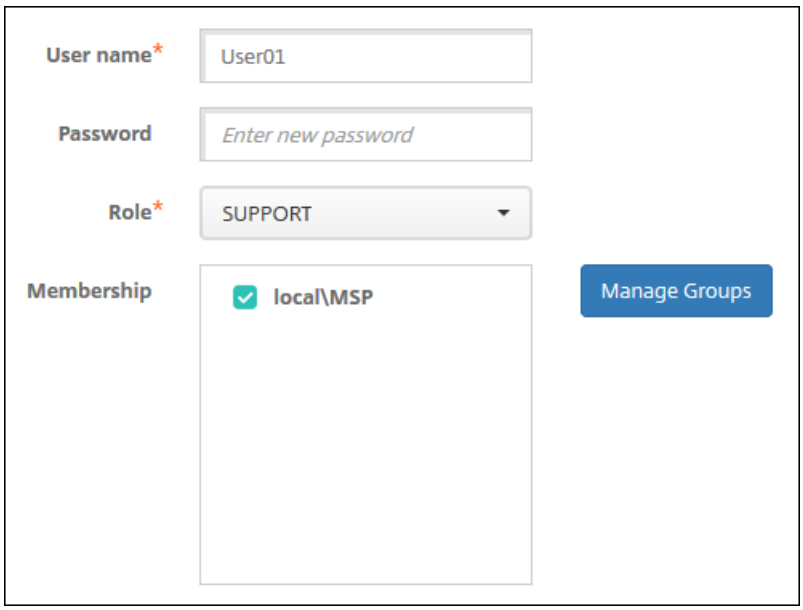
Gruppen werden im Dialogfeld Gruppen verwalten in der XenMobile-Konsole verwaltet. Dieses kann über die Seite **Benutzer**, **Lokalen Benutzer hinzufügen** oder **Lokalen Benutzer bearbeiten** aufgerufen werden. Es gibt keinen spezifischen Befehl zum Bearbeiten von Gruppen. Das Entfernen einer Gruppe 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:

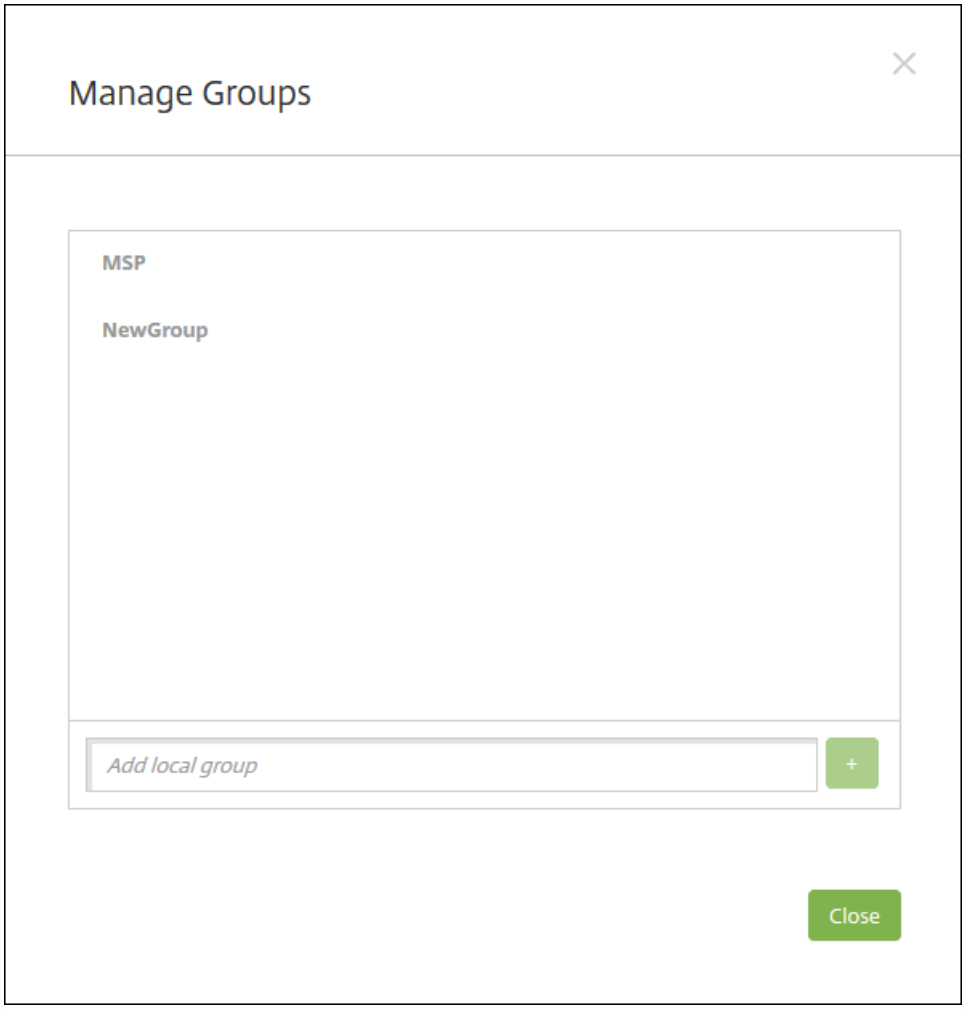
- Klicken Sie auf der Seite **Benutzer** auf **Lokale Gruppen verwalten**.



- Klicken Sie auf der Seite **Lokalen Benutzer hinzufügen** oder **Lokalen Benutzer bearbeiten** auf **Gruppen verwalten**.



Das Dialogfeld **Gruppen verwalten** wird angezeigt.



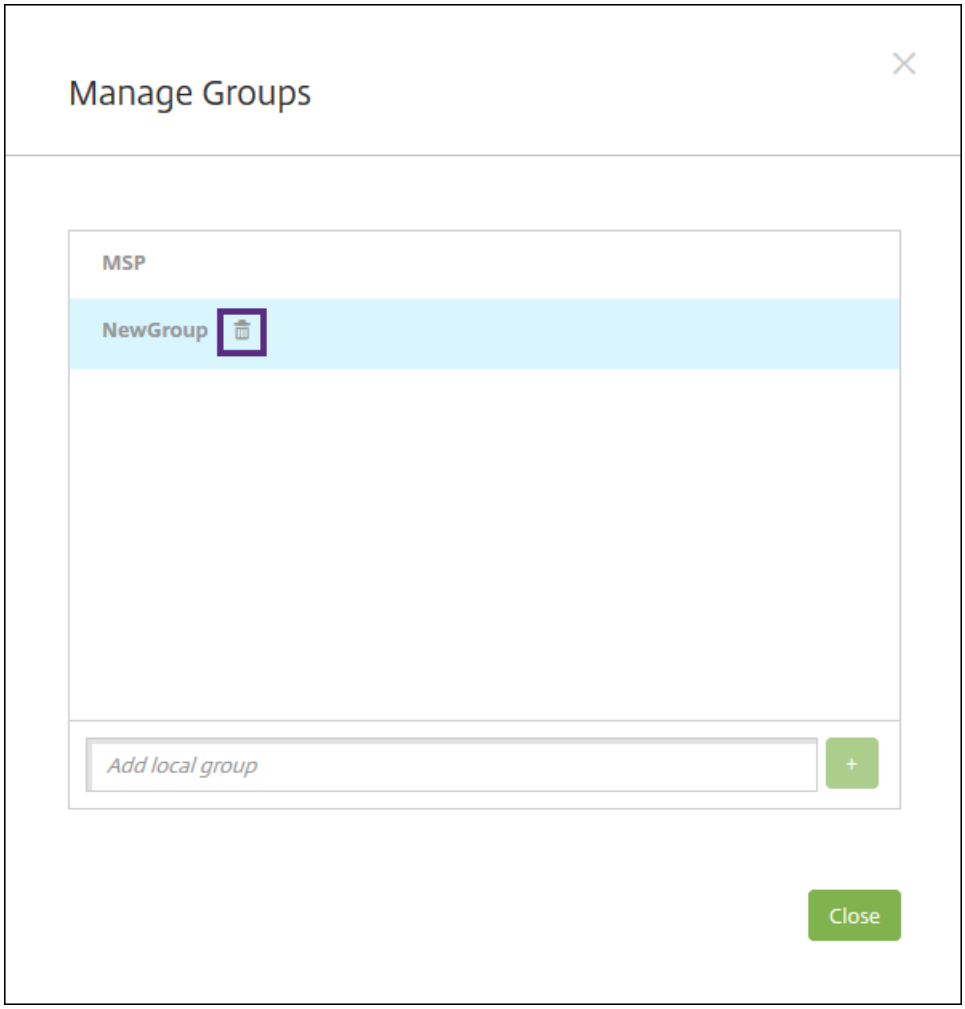
2. Geben Sie unterhalb der Gruppenliste einen Namen für die neue Gruppe ein und klicken Sie auf das Pluszeichen (+). Die Benutzergruppe wird der Liste hinzugefügt.

3. Klicken Sie auf **Schließen**.

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 Benutzer auf **Lokale Gruppen verwalten**.
- Klicken Sie auf der Seite **Lokalen Benutzer hinzufügen** oder **Lokalen Benutzer bearbeiten** auf **Gruppen verwalten**.

Das Dialogfeld **Gruppen verwalten** wird angezeigt.



2. Klicken Sie im Dialogfeld **Gruppen verwalten** 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 **Löschen**, um den Vorgang zu bestätigen und die Gruppe zu entfernen.

   Wichtig: Sie können diesen Vorgang nicht rückgängig machen.

5. Klicken Sie im Dialogfeld **Gruppen verwalten** auf **Schließen**.

Konfigurieren von Rollen mit RBAC

Oct 13, 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**: Gibt Vollzugriff auf das System.
- **Geräteprovisioning**: Gibt den Zugriff auf Grundfunktionen der Geräteverwaltung für Windows CE-Geräte.
- **Support**: Gibt Zugriff auf Remotesupport.
- **Benutzer**: Von Benutzern verwendete Rolle für die Registrierung von Geräten und den Zugriff auf das Selbsthilfeportal.

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.

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.

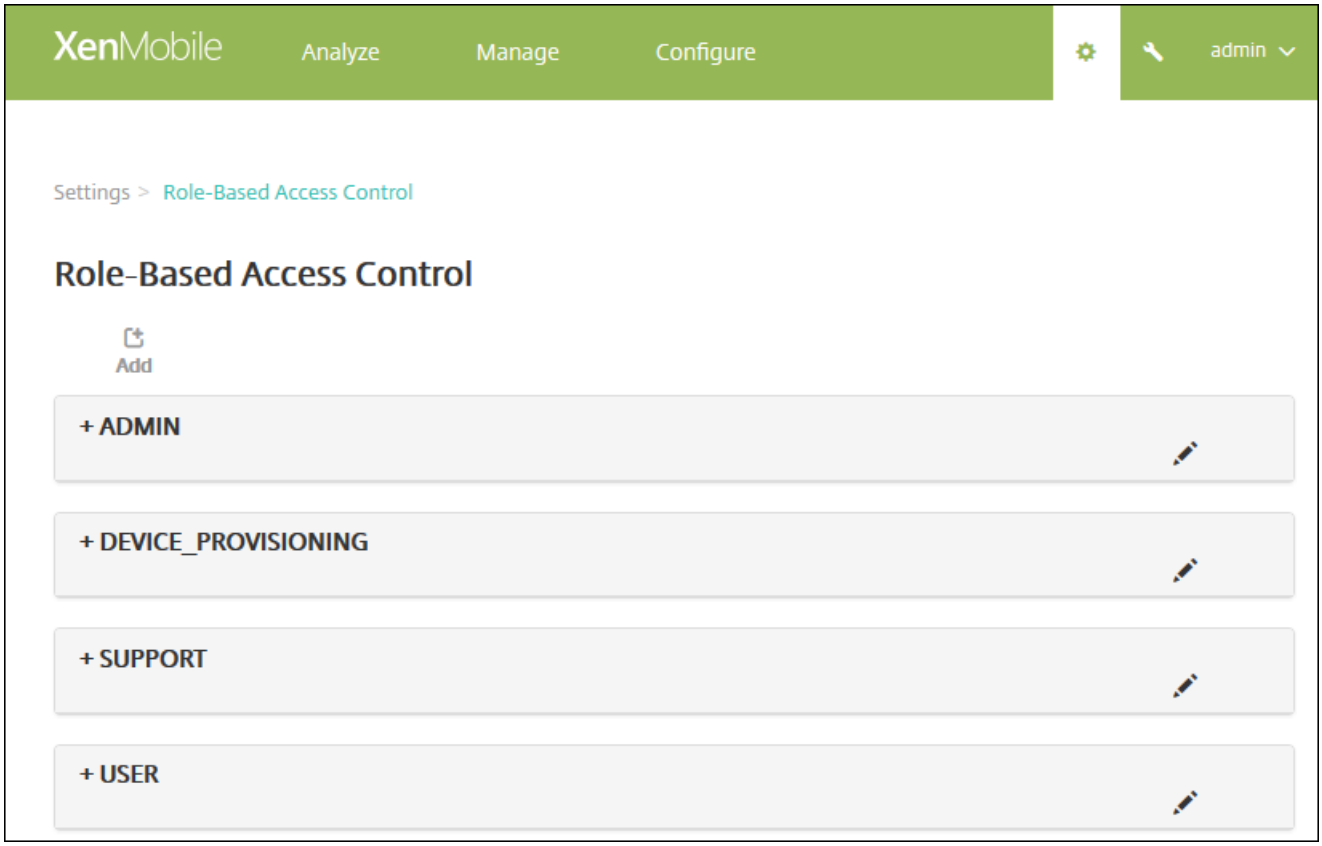
Hinweis: Lokalen Benutzern kann bei Bedarf nur eine Rolle zugewiesen werden.

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 das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie auf **Rollenbasierte Zugriffssteuerung (RBAC)**. Die Seite **Rollenbasierte Zugriffssteuerung** mit den vier Standardbenutzerrollen und allen von Ihnen zuvor hinzugefügten Rollen wird angezeigt.



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

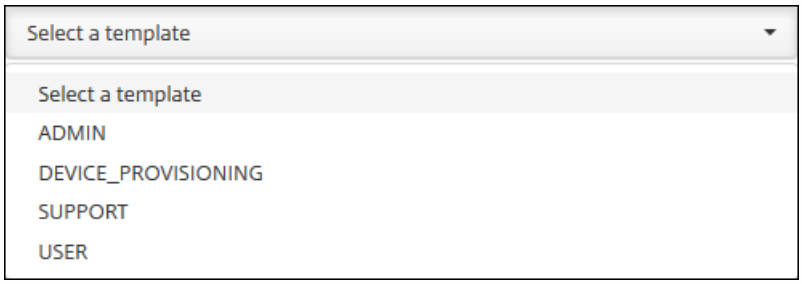
3. Klicken Sie auf **Hinzufügen**, um eine neue Benutzerrolle hinzuzufügen, klicken Sie auf das Stiftsymbol rechts neben einer vorhandenen Rolle, um diese zu bearbeiten, oder klicken Sie auf das Papierkorbsymbol rechts neben einer von Ihnen hinzugefügten Rolle, um sie zu löschen. Sie können die Standardbenutzerrollen nicht löschen.

- Wenn Sie auf **Hinzufügen** oder das Stiftsymbol klicken, wird die Seite **Rolle hinzufügen** bzw. **Rolle bearbeiten** angezeigt.
- Wenn Sie auf das Papierkorbsymbol klicken, wird ein Bestätigungsdialogfeld angezeigt. Klicken Sie auf **Löschen**, um die ausgewählte Rolle zu entfernen.

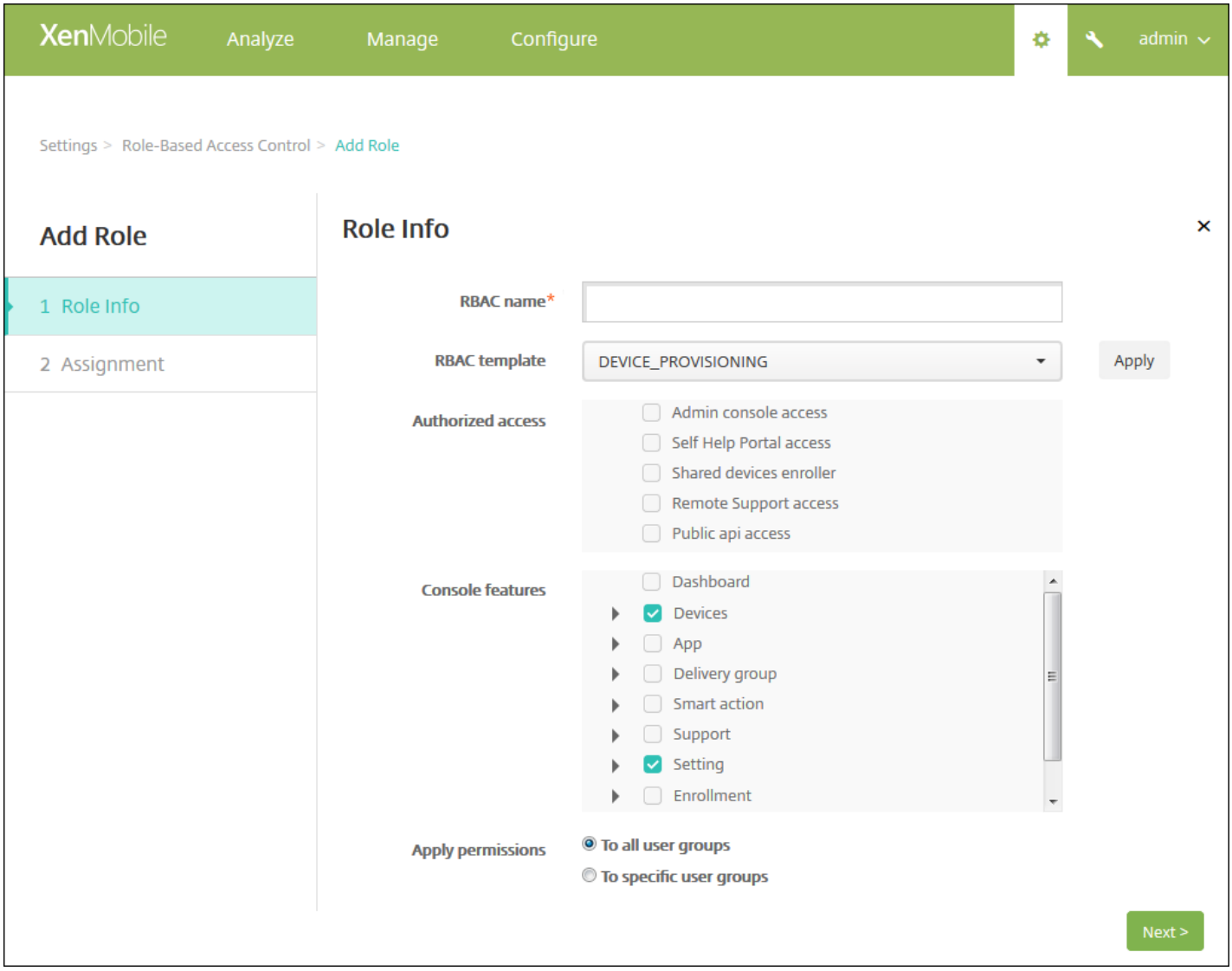
4. Geben Sie die folgenden Informationen zum Erstellen einer neuen Benutzerrolle bzw. zum Bearbeiten einer vorhandenen Benutzerrolle ein:

- **RBAC-Name**: Geben Sie einen aussagekräftigen Namen für die neue Benutzerrolle ein. Sie können den Namen vorhandener Rollen nicht ändern.
- **RBAC-Vorlage**: Klicken Sie optional auf eine Vorlage als Ausgangsbasis für die neue Rolle. Sie können keine Vorlage auswählen, wenn Sie eine vorhandene Rolle bearbeiten.

  RBAC-Vorlagen sind die Standardbenutzerrollen. Sie definieren den Zugriff auf Systemfunktionen für Benutzer, denen die jeweiligen Rolle zugewiesen ist. Nach der Auswahl einer RBAC-Vorlage werden alle zu der Rolle gehörenden Berechtigungen in den Feldern **Autorisierter Zugriff** und **Konsolenfeatures** angezeigt. Die Verwendung von Vorlagen ist optional. Sie können die Berechtigungen auch direkt in den Feldern **Autorisierter Zugriff** und **Konsolenfeatures** auswählen.

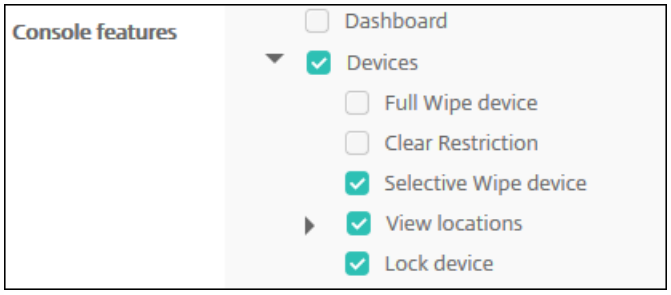


5. Klicken Sie auf rechts neben dem Feld **RBAC-Vorlage** auf **Anwenden**, um die Kontrollkästchen für **Autorisierter Zugriff** und **Konsolenfeatures** gemäß den Berechtigungen der ausgewählten Vorlage einzustellen.

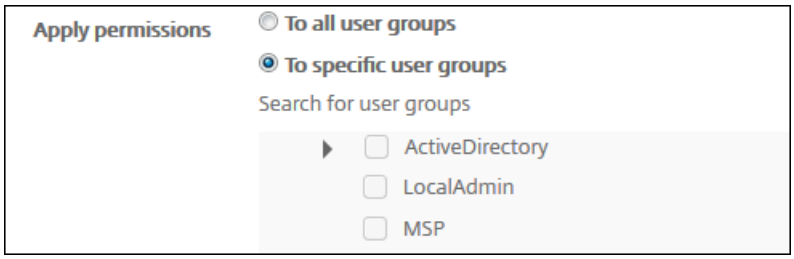


6. Aktivieren bzw. deaktivieren Sie die Kontrollkästchen für **Autorisierter Zugriff** und **Konsolenfeatures**, um die Rolle anzupassen.

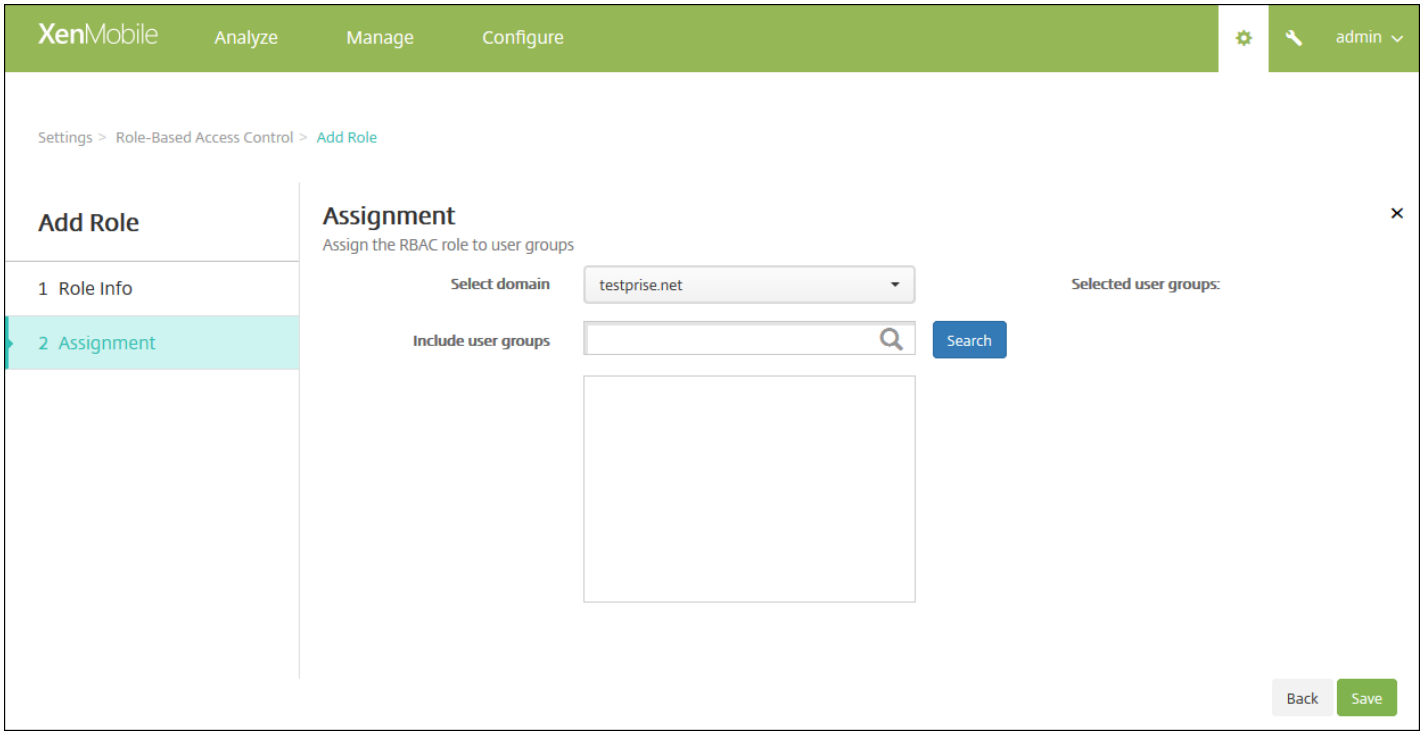
Wenn Sie auf das Dreieck neben einem Konsolenfeature klicken, werden featurespezifische Berechtigungen angezeigt, die Sie aktivieren und deaktivieren können. Wenn Sie auf das oberste Kontrollkästchen eines Konsolenbereichs klicken, wird der Zugriff auf den Konsolenbereich verweigert. Zum Aktivieren des Zugriffs auf spezifische Optionen müssen Sie jeweils das zugehörige Kontrollkästchen aktivieren. Beispiel: In der folgenden Abbildung werden die Optionen **Gerät vollständig löschen** und **Einschränkungen deaktivieren** für Benutzer, denen die Rolle zugewiesen ist, nicht in der Konsole angezeigt, während die aktivierten Optionen angezeigt werden.



7. **Berechtigungen anwenden**: Wählen Sie die Gruppen aus, denen Sie die ausgewählten Berechtigungen erteilen möchten. Wenn Sie auf **Auf bestimmte Benutzergruppen** klicken, wird eine Liste mit Gruppen angezeigt, in der Sie eine oder mehrere Gruppen auswählen können.

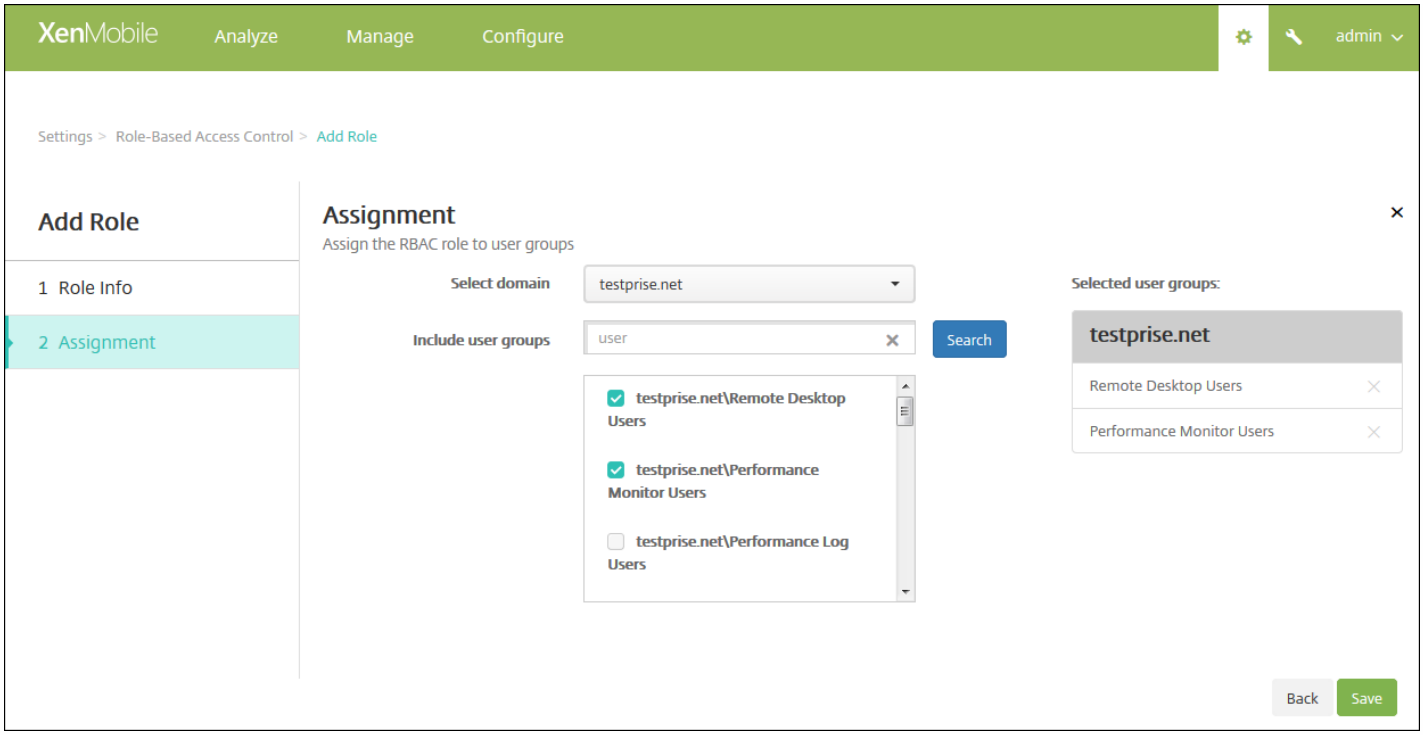


8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** wird angezeigt.



9. Geben Sie die folgenden Informationen zum Zuweisen der Rolle zu Gruppen ein.

- **Domäne auswählen**: Klicken Sie in der Liste auf eine Domäne.
- **Benutzergruppe einschließen**: Klicken Sie auf **Suchen**, 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.
- Wählen Sie in der nun angezeigten Liste die Benutzergruppen aus, denen Sie die Rolle zuweisen möchten. Wenn Sie eine Benutzergruppe auswählen, wird die Gruppe in der Liste **Ausgewählte Benutzergruppen** angezeigt.



Hinweis: Zum Entfernen einer Benutzergruppe aus der Liste **Ausgewählte Benutzergruppen** klicken Sie auf das X neben ihrem Namen.

10. Klicken Sie auf **Speichern**.

RBAC-Rollen und -Berechtigungen

Aug 22, 2016

Jeder vordefinierten Rolle für die rollenbasierte Zugriffssteuerung (RBAC) sind bestimmte Zugriffs- und Featureberechtigungen zugewiesen. In diesem Artikel werden die einzelnen Berechtigungen erläutert. Eine vollständige Liste der Standardberechtigungen für jede integrierte Rolle finden Sie unter Role-Based Access Control Defaults.

Weitere Informationen über das Konfigurieren von RBAC-Rollen finden Sie unter Konfigurieren von Rollen mit RBAC.

- Administratorrolle
- Rolle für das Geräteprovisioning
- Supportrolle
- Benutzerrolle

Konfigurieren von Registrierungsmodi und Aktivieren des Selbsthilfeportals

Jul 28, 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 **Einstellungen > Registrierung**. Zum Senden von Registrierungseinladungen verwenden Sie in der XenMobile-Konsole die Seite **Verwalten > Registrierung** (siehe Registrieren von Benutzern und Geräten in XenMobile).

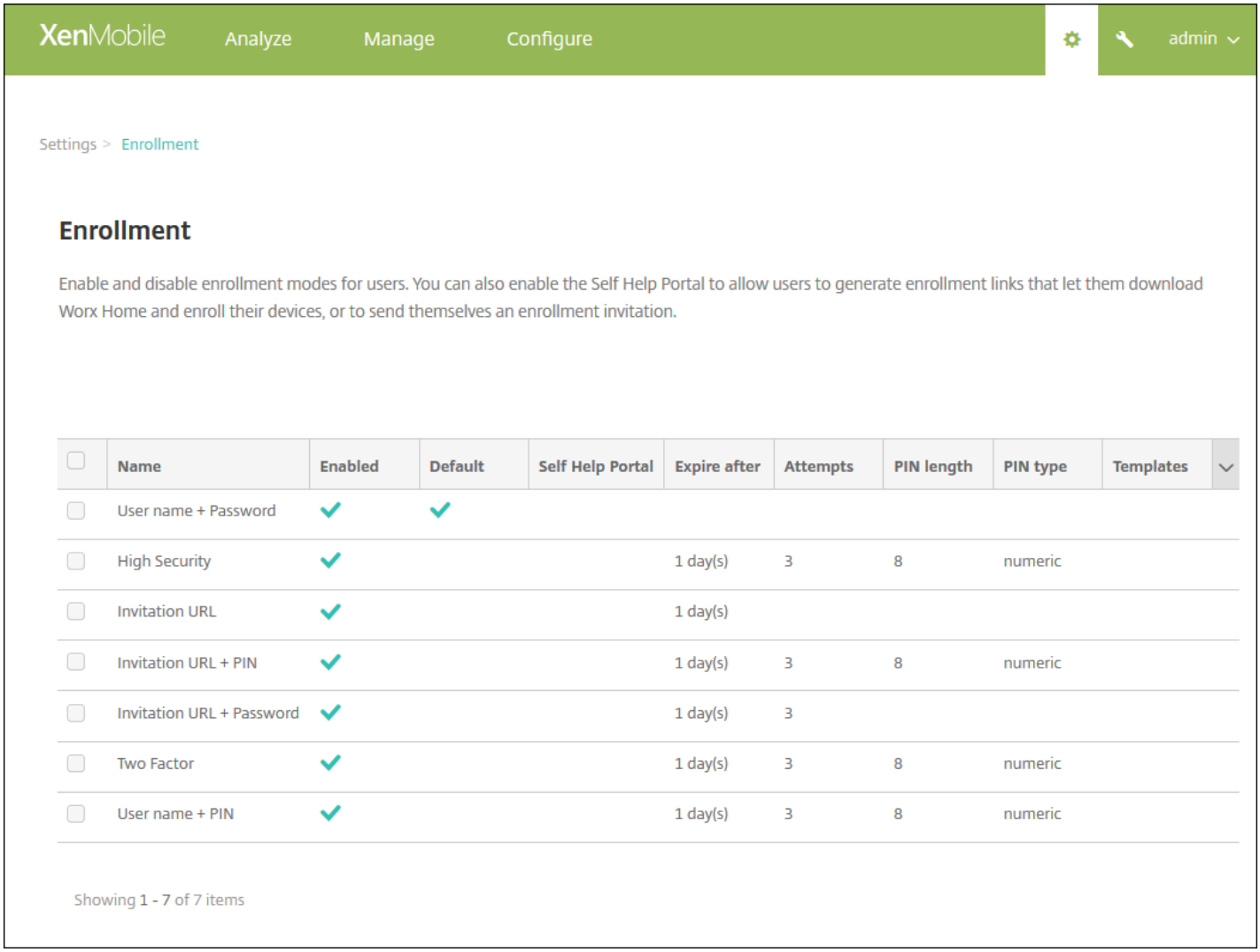
Hinweis: Wenn Sie benutzerdefinierte Benachrichtigungsvorlagen verwenden möchten, müssen Sie diese vor dem Konfigurieren der Registrierungsmodi erstellen. Weitere Informationen über Benachrichtigungsvorlagen finden Sie unter Erstellen oder Aktualisieren von Benachrichtigungsvorlagen.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie auf **Registrierung**. Die Seite **Registrierung** wird angezeigt. Sie enthält eine Tabelle aller verfügbaren Registrierungsmodi. Standardmäßig sind alle Registrierungsmodi aktiviert.

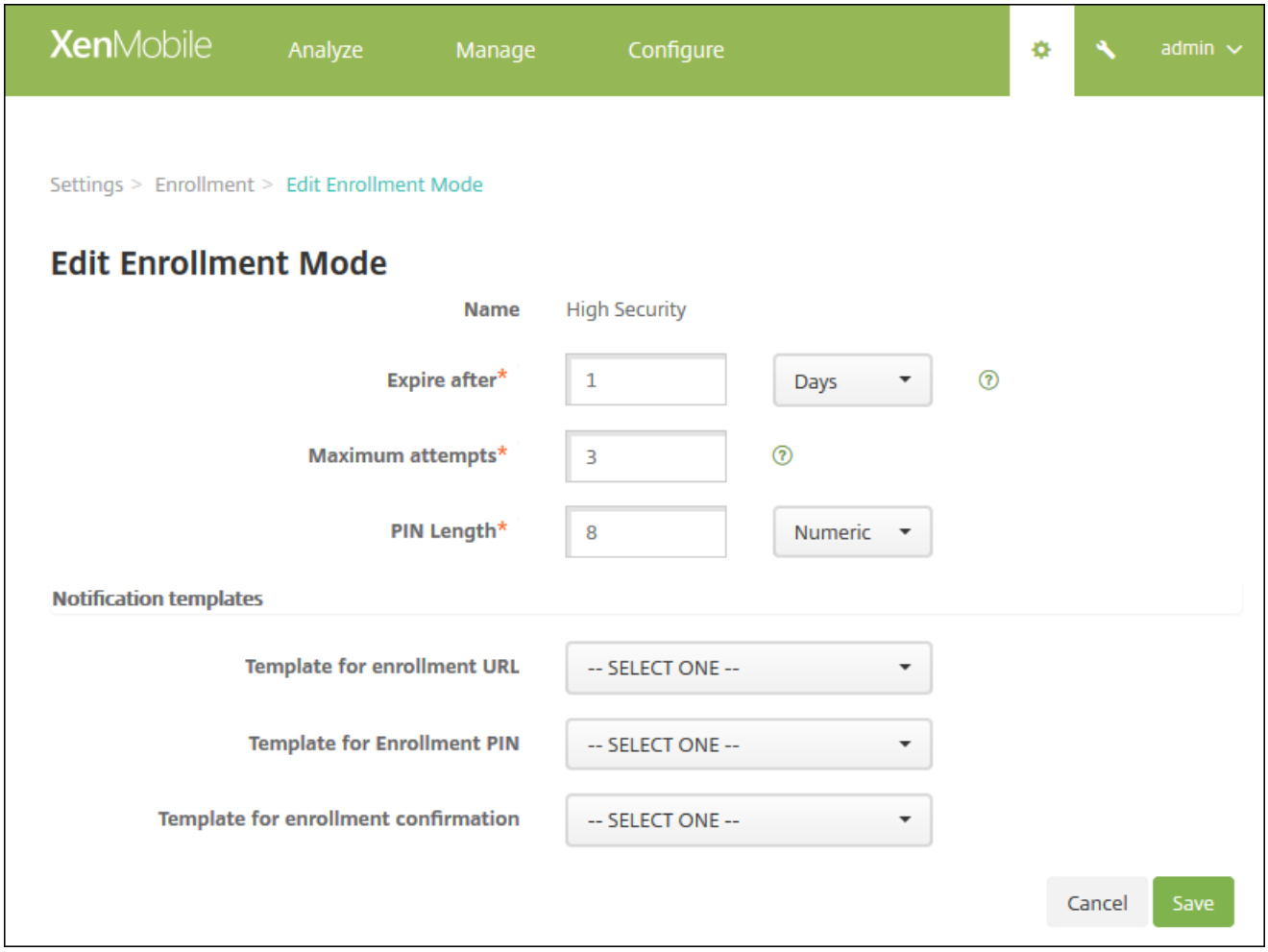
3. Wählen Sie einen Registrierungsmodus in der Liste zur Bearbeitung aus und legen Sie diesen als Standard fest, löschen Sie ihn oder erteilen Sie Benutzern Zugriff darauf über das Selbsthilfeportal.

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.



Bearbeiten eines Registrierungsmodus

1. Wählen Sie in der Liste **Registrierung** einen Registrierungsmodus aus und klicken Sie dann auf Bearbeiten. Die Seite **Registrierungsmodus bearbeiten** wird angezeigt. Abhängig von dem ausgewählten Modus werden ggf. andere Optionen angezeigt.



2. Ändern Sie nach Bedarf die folgenden Informationen:

- **Ablauf nach**: Geben Sie einen Zeitraum ein, nach dem die Benutzer ihre Geräte nicht mehr registrieren können. Dieser Wert wird auf den Seiten zur Konfiguration der Registrierungseinladung für Benutzer und Gruppen angezeigt.
  Hinweis: Geben Sie 0 ein, wenn die Einladung nicht ablaufen soll.

- **Tage**: Klicken Sie in der Liste auf **Tage** oder **Stunden** zur Bestimmung der Maßeinheit für den unter **Ablauf nach** eingegebenen Zeitraum.
- **Versuche maximal**: Geben Sie die Anzahl der Registrierungsversuche ein, die ein Benutzer machen darf, bevor die Registrierung für ihn gesperrt wird. Dieser Wert wird auf den Seiten zur Konfiguration der Registrierungseinladung für Benutzer und Gruppen angezeigt.
  Hinweis: Geben Sie 0 ein, um eine unbegrenzte Anzahl von Versuchen zuzulassen.

- **PIN-Länge**: Geben Sie eine Zahl für die Länge der generierten PIN in Ziffern/Zeichen ein.
- **Numerisch**: Klicken Sie in der Liste auf **Numerisch** oder **Alphanumerisch**, um die Art der PIN festzulegen.
- **Benachrichtigungsvorlagen**:
  - **Vorlage für Registrierungs-URL**: Wählen Sie in der Liste 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 Benachrichtigungsvorlagen finden Sie unter Erstellen oder Aktualisieren von Benachrichtigungsvorlagen.
  - **Vorlage für Registrierungs-PIN**: Wählen Sie in der Liste eine Vorlage für die Registrierungs-PIN aus.

- **Vorlage für Registrierungsbestätigung**: Wählen Sie in der Liste eine Vorlage für die Benachrichtigung der Benutzer über eine erfolgreiche Registrierung aus.

3. Klicken Sie auf **Speichern**.

Festlegen eines Registrierungsmodus als Standard

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 **Benutzername + Kennwort**, **Zweifaktor** oder **Benutzername + PIN** können als Standardregistrierungsmodus festgelegt werden.
1. Wählen Sie **Benutzername + Kennwort**, **Zweifaktor** oder **Benutzername + PIN** als Standardregistrierungsmodus aus.

Hinweis: Der ausgewählte Modus muss aktiviert sein, um als Standard festgelegt werden zu können.
2. Klicken Sie auf **Standard**. Der ausgewählte Modus ist jetzt der Standardmodus. War zuvor ein anderer Registrierungsmodus als Standard eingestellt, ist dieser Modus nun nicht mehr Standardmodus.

Deaktivieren eines Registrierungsmodus

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

1. Wählen Sie einen Registrierungsmodus aus.

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

Aktivieren eines Registrierungsmodus auf dem Selbsthilfeportal

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

Hinweis:

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

1. Wählen Sie einen Registrierungsmodus aus.

2. Klicken Sie auf **Selbsthilfeportal**. Der ausgewählte Registrierungsmodus steht Benutzern jetzt auf dem Selbsthilfeportal zur Verfügung. Andere für das Selbsthilfeportal aktivierte Modi sind nicht mehr für Benutzer verfügbar.

Aktivieren von Autodiscovery für die Benutzerregistrierung in XenMobile

Jul 28, 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.

Sie können Autodiscovery über das Autodiscovery-Dienstportal unter https://xenmobiletools.citrix.com aktivieren. 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 nicht über das Autodiscovery-Dienstportal unter https://xenmobiletools.citrix.com aktivieren können, öffnen Sie über das Citrix Support-Portal einen Supportfall und geben Sie die folgenden Informationen an:

- Die Domäne mit den Konten, mit denen Benutzer Geräte registrieren.
- Vollqualifizierter Domänenname (FQDN) des XenMobile-Servers.
- XenMobile-Instanzname. Standardmäßig lautet der Instanzname"zdm" (Groß-/Kleinschreibung beachten).
- 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:

- 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.
- Erstellen Sie einen Datensatz mit einem kanonischen Namen (CNAME) im DNS und weisen Sie die Adresse des SSL-Zertifikats (enterpriseenrollment.mycompany.com) der Adresse autodisc.zc.zenprise.com zu. Wenn ein Benutzer ein Windows-Gerät unter Angabe des UPNs und der Details des XenMobile-Servers registriert, weist der Citrix Registrierungsserver das Gerät an, ein gültiges Zertifikat vom XenMobile-Server anzufordern.

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

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

- SubjectDN mit einem CN, der die primäre Domäne für das Zertifikat angibt (z. B. enterpriseenrollment.mycompany1.com)

- SANs der restlichen Domänen (z. B. enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com usw.)

Erstellen und Aktualisieren von Benachrichtigungsvorlagen

Jul 28, 2016

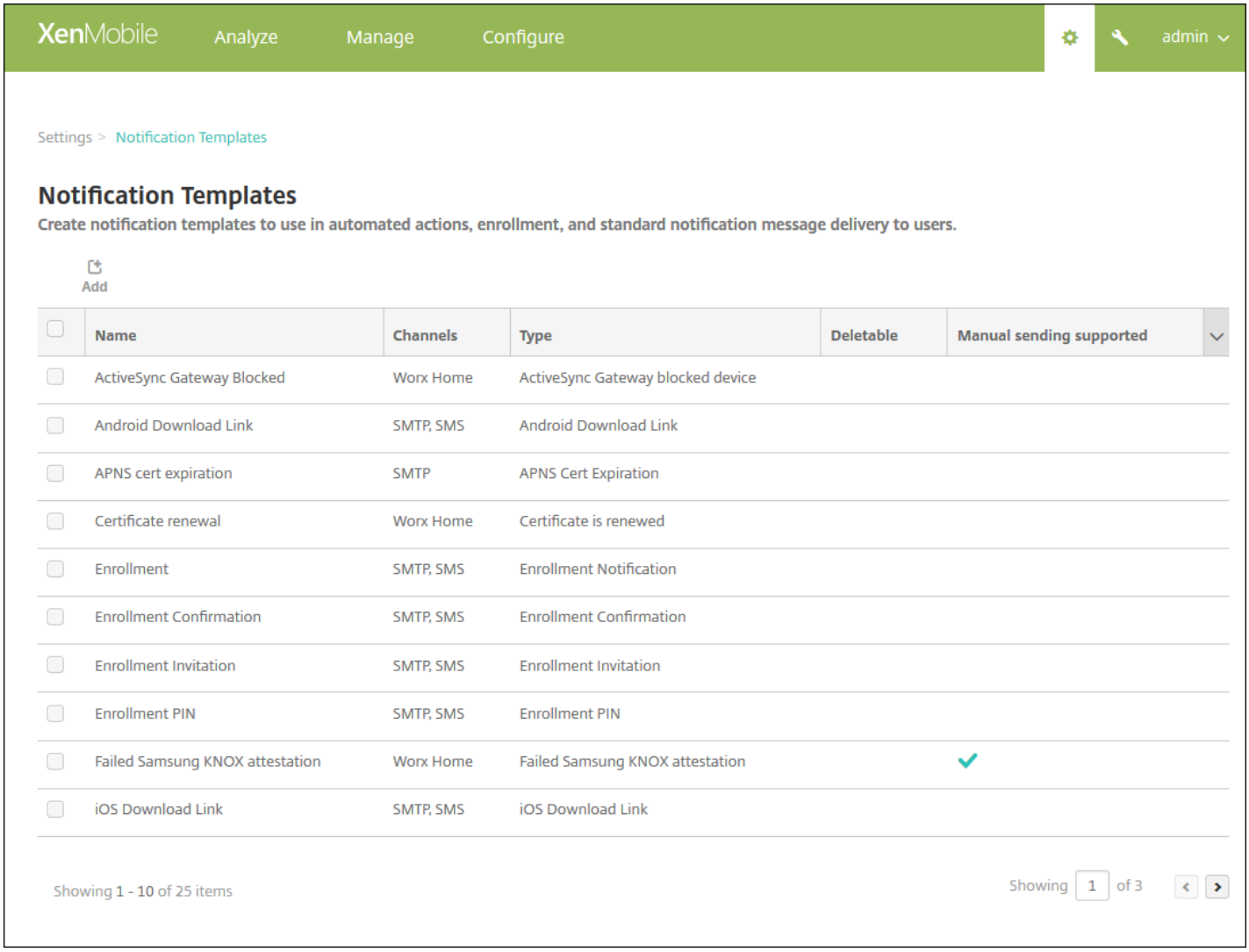
Sie können Benachrichtigungsvorlagen zur Verwendung in automatisierten Aktionen, bei der Registrierung und für Standardbenachrichtigungen an Benutzer erstellen und aktualisieren. Sie können Benachrichtigungsvorlagen zum Senden von Nachrichten über drei verschiedene Kanäle konfigurieren: Worx Home, SMTP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

XenMobile umfasst viele vordefinierte Vorlagen für die diversen Ereignisse, auf die XenMobile automatisch für jedes Gerät im System reagiert.

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 das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie auf **Benachrichtigungsvorlagen**. Die Seite **Benachrichtigungsvorlagen** wird angezeigt.



Hinzufügen einer Benachrichtigungsvorlage

1. Klicken Sie auf **Hinzufügen**. 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. Die Seite **Benachrichtigungsvorlage hinzufügen** wird angezeigt.

Wenn Sie sich für eine sofortige Einrichtung des SMS- bzw. SMTP-Servers entscheiden, werden Sie zu der Seite **Benachrichtigungsserver** unter **Einstellung** geleitet. Nach der Einrichtung der gewünschten Kanäle können Sie zur Seite **Benachrichtigungsvorlage** zurückkehren, um mit dem Hinzufügen bzw. Ändern von Benachrichtigungsvorlagen fortzufahren.

Important

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.

2. Konfigurieren Sie die folgenden Einstellungen:

- **Name**: Geben Sie einen aussagekräftigen Namen für die Vorlage ein.
- **Beschreibung:** Geben Sie eine Beschreibung für die Vorlage ein.
- **Typ**: Klicken Sie in der Liste auf den Benachrichtigungstyp. Es werden nur für den ausgewählten Typ unterstützte Kanäle angezeigt. Es ist nur eine APNS Cert Expiration-Vorlage zulässig und zwar die vordefinierte Vorlage. Sie können also keine Vorlage dieses Typs hinzufügen.

Hinweis: Unterhalb einiger Vorlagentypen wird *Manuelles Senden wird unterstützt* angezeigt. Solche Vorlagen sind in der Liste **Benachrichtigungen** im Dashboard und auf der Seite **Geräte** 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)}

3. Konfigurieren Sie unter **Kanäle** 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 **SMTP** auswählen, sollten die meisten Benutzer Benachrichtigungen empfangen, da sie sich mit ihrer E-Mail-Adresse registriert haben.
- Wenn Sie **SMS** auswählen, empfangen nur Geräte mit einer SIM-Karte Benachrichtigungen.

Worx Home:

- **Aktivieren**: Klicken Sie hier zum Aktivieren dieses Benachrichtigungskanals.
- **Nachricht**: Geben Sie die Nachricht ein, die an die Benutzer gesendet werden soll. Dieses Feld ist erforderlich, wenn Sie Worx Home verwenden.
- **Audiodatei**: Wählen Sie den Benachrichtigungston aus, der bei Empfang einer Benachrichtigung ausgegeben werden soll.

SMTP:

- **Aktivieren**: Klicken Sie hier zum Aktivieren dieses Benachrichtigungskanals.

  Wichtig: Sie können den SMTP-Kanal nur aktivieren, wenn Sie bereits den SMTP-Server eingerichtet haben.

- **Absender**: Geben Sie optional einen Absender für die Benachrichtigung an (Name, E-Mail-Adresse oder beides).
- **Empfänger**: 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 **Verwalten** > **Geräte** auswählen und die Benachrichtigungen von dort aus senden. Weitere Informationen finden Sie unter Hinzufügen von Geräten und Anzeigen von Gerätedetails in XenMobile
- **Betreff**: Geben Sie einen aussagekräftigen Betreff für die Benachrichtigung ein. Diese Angabe ist erforderlich.
- **Nachricht**: Geben Sie die Nachricht ein, die an die Benutzer gesendet werden soll.

SMS:

- **Aktivieren**: Klicken Sie hier zum Aktivieren dieses Benachrichtigungskanals.

  Wichtig: Sie können den SMS-Kanal nur aktivieren, wenn Sie bereits das SMS-Gateway eingerichtet haben.
- **Empfänger**: 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 **Verwalten** > **Geräte** auswählen.
- **Nachricht**: Geben Sie die Nachricht ein, die an die Benutzer gesendet werden soll. Diese Angabe ist erforderlich.

5. Klicken Sie auf **Hinzufügen**. Wenn alle Kanäle richtig konfiguriert sind, werden sie in dieser Reihenfolge auf der Seite **Benachrichtigungsvorlagen** angezeigt: SMTP, SMS und Worx Home. Falsch konfigurierte Kanäle werden nach den richtig konfigurierten Kanälen angezeigt.

Bearbeiten einer Benachrichtigungsvorlage

1. Wählen Sie die Benachrichtigungsvorlage aus. Die Seite zum Bearbeiten der ausgewählten Vorlage wird angezeigt. Sie können alle Felder mit Ausnahme von **Typ** ändern und Kanäle aktivieren oder deaktivieren.

2. Klicken Sie auf **Speichern**.

Löschen einer Benachrichtigungsvorlage

Hinweis: Sie können nur Benachrichtigungsvorlagen löschen, die Sie selbst hinzugefügt haben, nicht aber vordefinierte Vorlagen.

1. Wählen Sie die Benachrichtigungsvorlage aus.

2. Klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt.

3. Klicken Sie auf **Löschen** zum Löschen der Benachrichtigungsvorlage oder auf **Abbrechen**, um den Vorgang abzubrechen.

Verwalten von Bereitstellungsgruppen

Jul 28, 2016

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

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

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

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

Bereitstellungsreihenfolge

Die Bereitstellungsreihenfolge ist die Reihenfolge, in der XenMobile Ressourcen per Push auf den Geräten bereitstellt. Die Bereitstellungsreihenfolge wird nur für den MDM-Modus unterstützt.

Beim Ermitteln der Bereitstellungsreihenfolge wendet XenMobile Filter- und Steuerungskriterien für Richtlinien, Apps, Aktionen und Bereitstellungsgruppen an, z. B. Bereitstellungsregeln und Bereitstellungszeitpläne. Vor dem Hinzufügen von Bereitstellungsgruppen, beachten Sie, wie sich die Informationen in diesem Abschnitt mit Ihren Bereitstellungszielsetzungen zusammenhängen.

Hier ist eine Zusammenfassung der grundlegende Konzepte für die Bereitstellungsreihenfolge:

- **Bereitstellungsreihenfolge:** Die Reihenfolge, in der XenMobile Ressourcen (Richtlinien und Apps) und Aktionen per Push auf einem Gerät bereitstellt Die Bereitstellungsreihenfolge einiger Richtlinien, wie AGB und Softwareinventar, hat keine Auswirkung auf andere Ressourcen. Die Reihenfolge, in der Aktionen bereitgestellt werden, hat keine Auswirkung auf andere Ressourcen, daher wird ihre Position ignoriert, wenn XenMobile die Ressourcen bereitstellt.
- **Bereitstellungsregeln:** XenMobile verwendet die Bereitstellungsregeln, die Sie für Geräteigenschaften angeben, zum Filtern von Richtlinien, Apps, Aktionen und Bereitstellungsgruppen. Beispiel: Eine Bereitstellungsregel könnte angeben, dass eine Bereitstellungspaket per Push bereitgestellt wird, wenn ein Domänenname einen bestimmten Wert hat.

- **Bereitstellungszeitplan:** XenMobile verwendet den Bereitstellungszeitplan, den Sie für Aktionen, Apps und Gerätерichtlinien angeben, um die Bereitstellung dieser Elemente zu steuern. Sie können festlegen, dass eine Bereitstellung sofort, zu einem bestimmten Datum und einer bestimmten Uhrzeit oder basierend auf Bereitstellungsbedingungen stattfindet.

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

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

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

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

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

Berechnungsschritte:

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

Bereitstellungszeitplan gelten. Der Sortieralgorithmus ist wie folgt:

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

b. Bei einem Gleichstand zwischen Bereitstellungsgruppen werden Ressourcen von Bereitstellungsgruppen nach dem Bereitstellungsgruppennamen sortiert. Beispiel: Ressourcen von Bereitstellung Gruppe A werden vor denen aus Bereitstellungsgruppe B einsortiert.

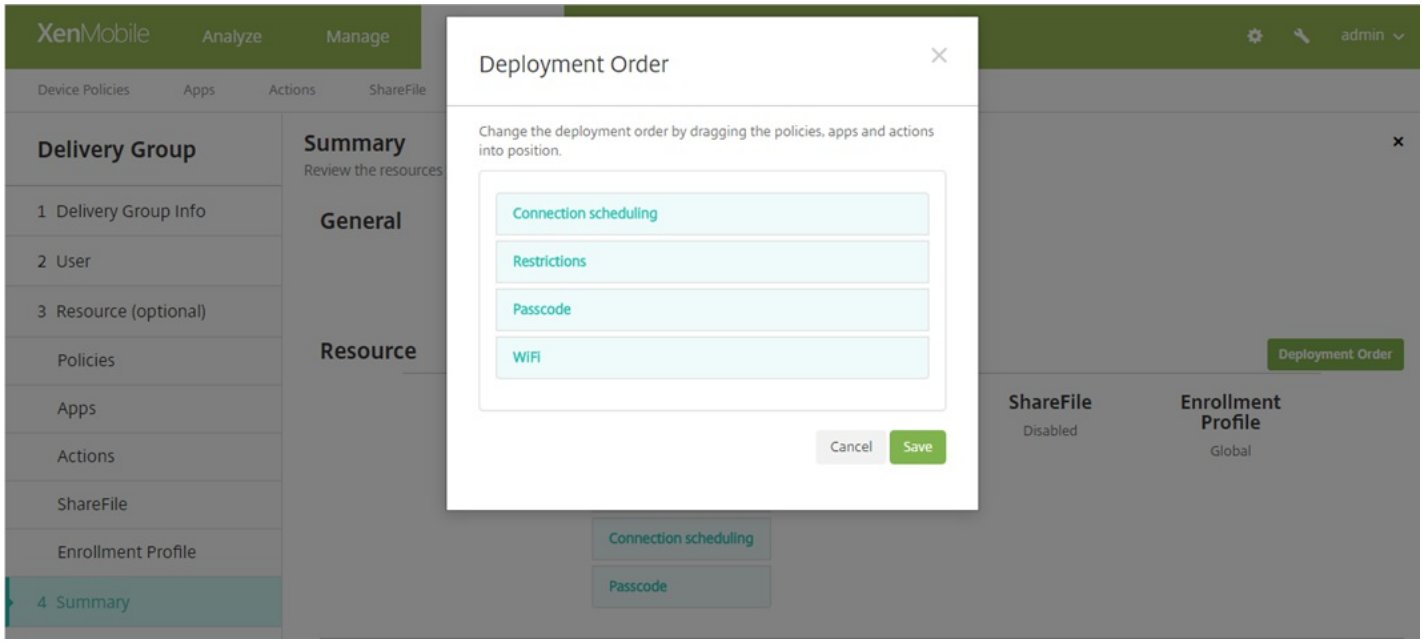
c. Wurde eine benutzerdefinierte Bereitstellungsreihenfolge für Ressourcen in einer Bereitstellungsgruppe angegeben, muss sie beim Sortieren erhalten bleiben. Sonst die Ressourcen in der Bereitstellungsuppe nach Ressourcenname sortieren.

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

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

Beispiel: Angenommen, Sie haben zwei Bereitstellungsgruppen:

- Bereitstellungsgruppe Kontomanager 1: **nicht angegebene** Ressourcenreihenfolge, enthält die Richtlinien **WiFi** und **Passcode**
- Bereitstellungsgruppe Kontomanager 2: **angegebene** Ressourcenreihenfolge, enthält die Richtlinien **Verbindungszeitplan**, **Einschränkungen**, **WiFi** und **Passcode** In diesem Fall müssen Sie die Passcoderichtlinie vor der WiFi- Richtlinie bereitstellen.



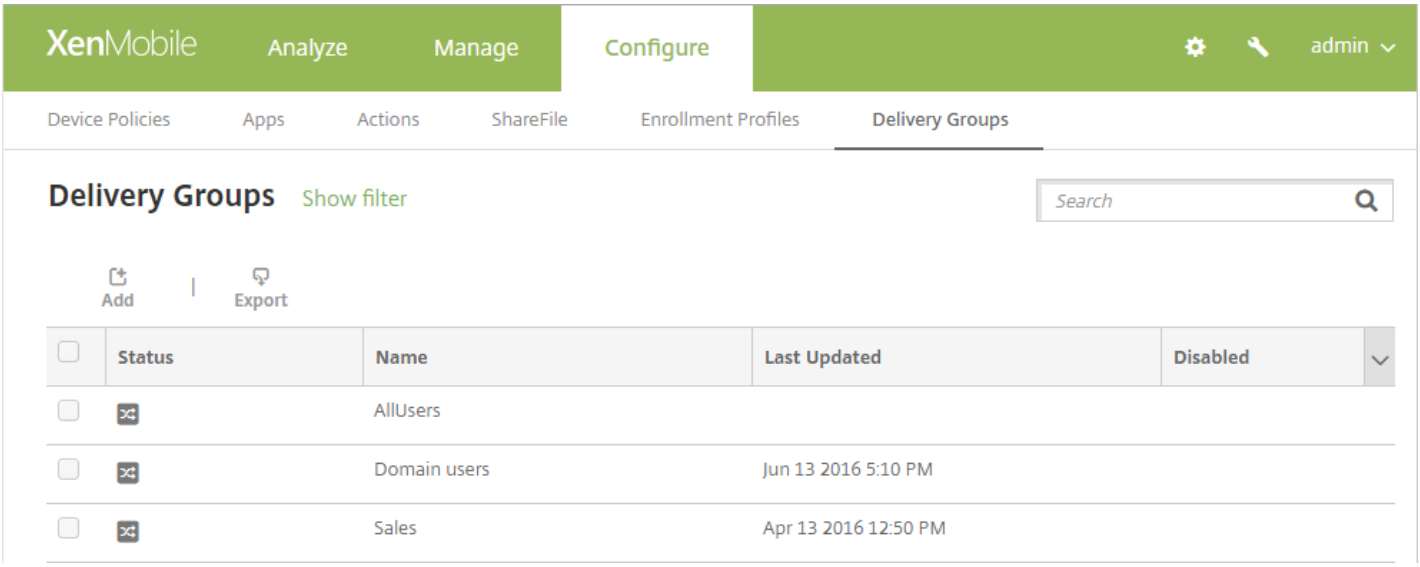
Würden Bereitstellungsgruppen durch den Algorithmus nur nach Namen sortiert, dann würde die Bereitstellung beginnend mit der Bereitstellungsgruppe "Kontomanager 1" in der Reihenfolge **WiFi**, **Passcode**, **Verbindungszeitplan**,

Einschränkungen erfolgen. Die Richtlinien **Passcode** und **WiFi** für die Bereitstellungsgruppe "Kontomanager 2" würden als Duplikate ignoriert.

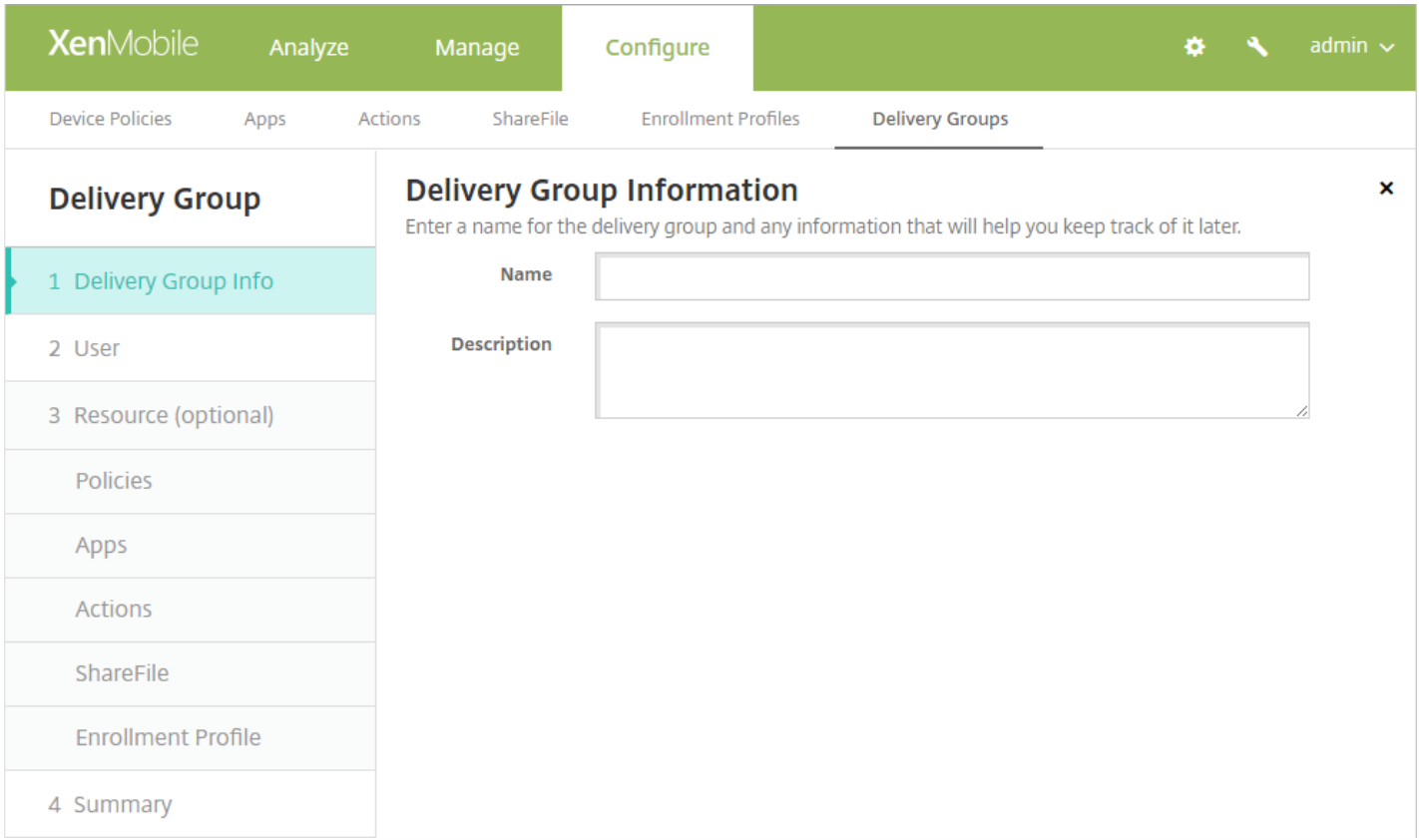
Da jedoch für die Bereitstellungsgruppe "Kontomanager 2" vom Administrator eine Bereitstellungsreihenfolge festgelegt wurde, werden Ressourcen aus dieser Bereitstellungsgruppe in der Liste über denen der Bereitstellungsgruppe "Kontomanager 1" eingeordnet. Die Richtlinien werden daher in der Reihenfolge **Verbindungszeitplan**, **Einschränkungen**, **Passcode**, **WiFi** bereitgestellt. Die Richtlinien **WiFi** und **Passcode** für die Bereitstellungsgruppe "Kontomanager 1" werden als Duplikate ignoriert. Dieser Algorithmus wendet daher die vom XenMobile-Administrator festgelegte Reihenfolge an.

Hinzufügen einer Bereitstellungsgruppe

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



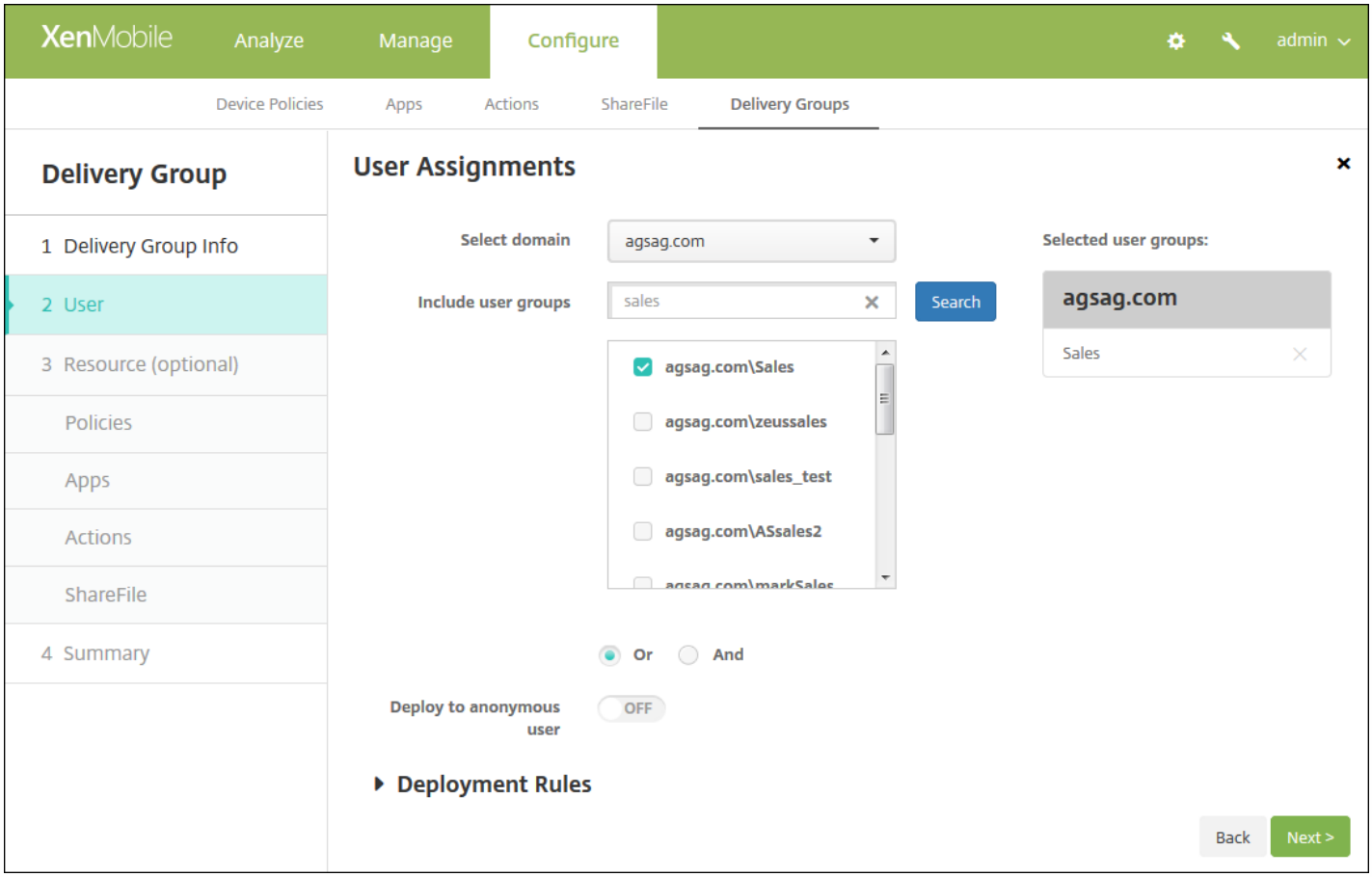
2. Klicken Sie auf der Seite **Bereitstellungsgruppen** auf **Hinzufügen**. Die Seite **Bereitstellungsgruppeninformationen** wird angezeigt.



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

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

4. Klicken Sie auf **Weiter**. Die Seite **Benutzerzuweisungen** wird angezeigt.



5. Konfigurieren Sie die folgenden Einstellungen:

- **Domäne auswählen**: Wählen Sie in der Liste die Domäne aus, in der Sie Benutzer auswählen möchten.
- **Benutzergruppen einschließen**: Führen Sie einen der folgenden Schritte aus:
  - Klicken Sie in der Liste der Benutzergruppen auf die Gruppen, die Sie hinzufügen möchten. Die ausgewählten Gruppen werden in der Liste **Ausgewählte Benutzergruppen** angezeigt.
  - Klicken Sie auf **Suchen**, um eine Liste aller Benutzergruppen in der ausgewählten Domäne anzuzeigen.
  - Geben Sie den Gruppennamen vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf **Suchen**, um die Liste der Benutzergruppen einzuschränken.
    - Zum Entfernen einer Benutzergruppe aus der Liste **Ausgewählte Benutzergruppen** führen Sie einen der folgenden Schritte aus:
      - Klicken Sie in der Liste **Ausgewählte Benutzergruppen** auf das **X** neben den Gruppen, die Sie entfernen möchten.
      - Klicken Sie auf **Suchen**, um eine Liste aller Benutzergruppen in der ausgewählten Domäne zu sehen. Navigieren Sie durch die Liste und deaktivieren Sie die Kontrollkästchen aller Gruppen, die Sie entfernen möchten.
      - Geben Sie den Gruppennamen vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf **Suchen**, um die Liste der Benutzergruppen einzuschränken. Navigieren Sie durch die Liste und deaktivieren Sie die Kontrollkästchen aller Gruppen, die Sie entfernen möchten.
- **Oder/Und**: Wählen Sie aus, ob Benutzer für die bereitzustellende Ressource nur einer Gruppe angehören dürfen (Oder) oder ob sie allen Gruppen angehören müssen (Und).
- **Für anonyme Benutzer bereitstellen:** Wählen Sie aus, ob die Bereitstellung auch für nicht authentifizierte Benutzer in der Bereitstellungsgruppe erfolgen soll.

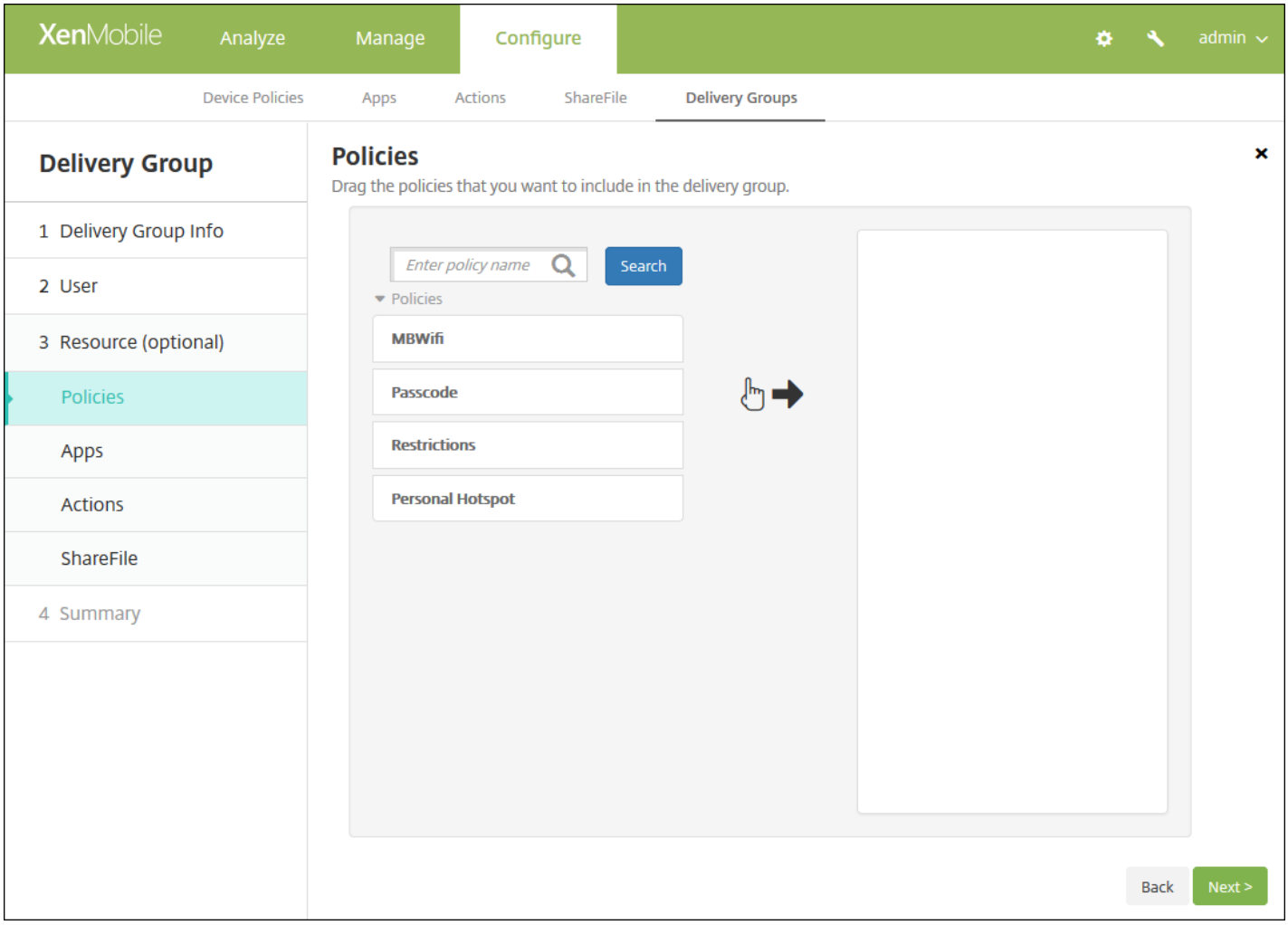
Hinweis: Nicht authentifizierte Benutzer sind Benutzer, bei denen keine Authentifizierung erfolgen konnte, denen jedoch dennoch eine Verbindung mit XenMobile gestattet wurde.

6. Konfigurieren der Bereitstellungsregeln

Hinzufügen optionaler Ressourcen zu Bereitstellungsgruppen

Sie können Bereitstellungsgruppen optional spezifische Richtlinien, erforderliche und optionale Apps oder automatische Aktionen hinzufügen und ShareFile für das Single Sign-On für Inhalte und Daten aktivieren. In den folgenden Abschnitten wird beschrieben, wie Sie Richtlinien, Apps und Aktionen hinzufügen und ShareFile aktivieren. Sie können Bereitstellungsgruppen einige oder alle dieser Ressourcen nach Bedarf hinzufügen, müssen dies jedoch nicht tun. Klicken Sie auf die Ressource, die Sie hinzufügen möchten, oder auf **Zusammenfassung**, wenn Sie keine Ressource hinzufügen möchten.

Hinzufügen von Richtlinien



1. Führen für jede Richtlinie, die Sie hinzufügen möchten, folgende Schritte aus:

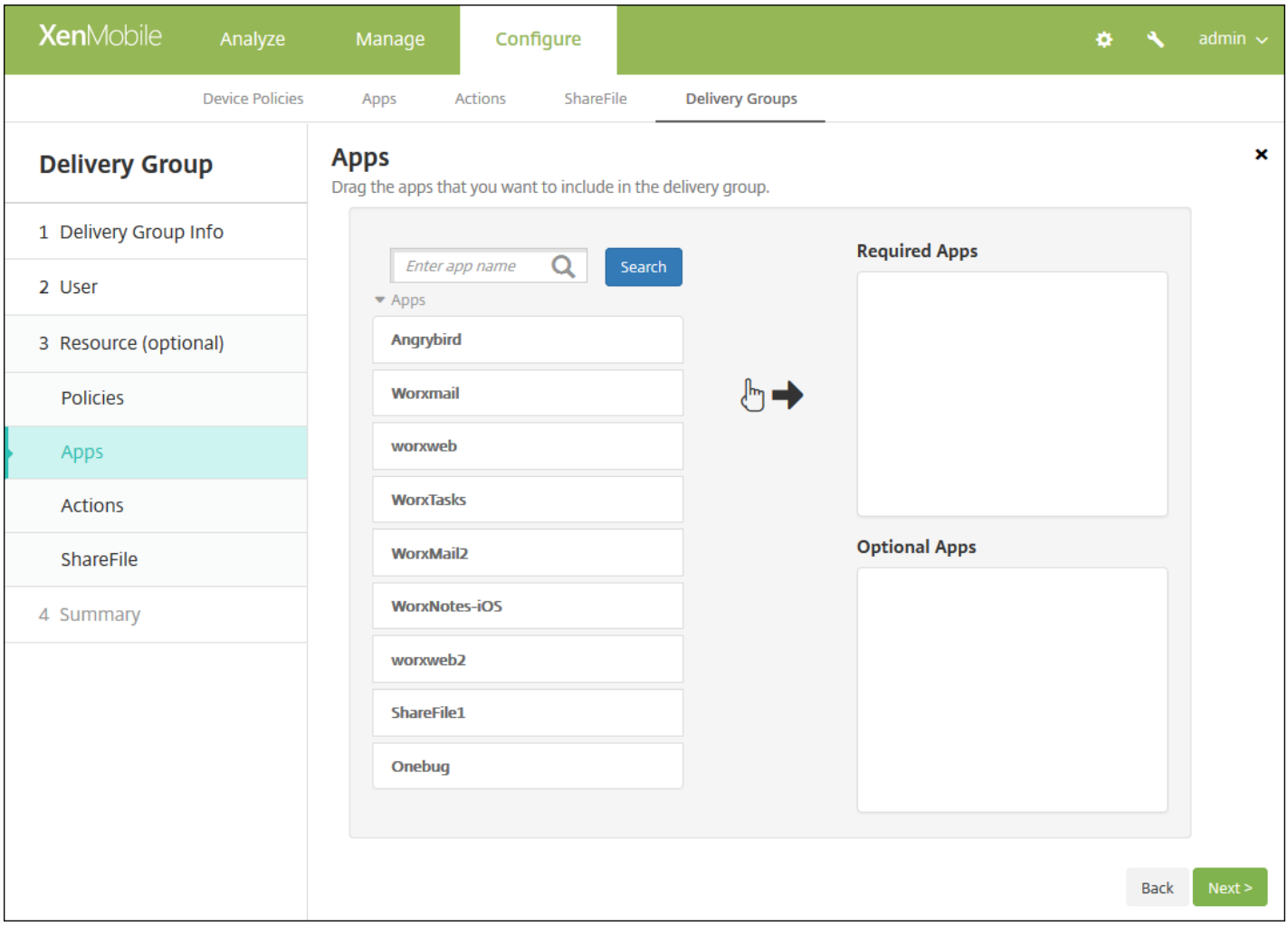
- Suchen Sie die gewünschte Richtlinie in der Liste der verfügbaren Richtlinien.
- Alternative: Um die Liste der Richtlinien einzuschränken, geben Sie den Richtliniennamen vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf **Suchen**.

- Klicken Sie auf die Richtlinie und ziehen Sie sie in das Feld auf der rechten Seite.

Hinweis: Zum Entfernen einer Richtlinie klicken Sie im rechten Feld auf das **X** neben deren Namen.

2. Klicken Sie auf **Weiter**. Die Seite **Apps** wird angezeigt.

Hinzufügen von Apps



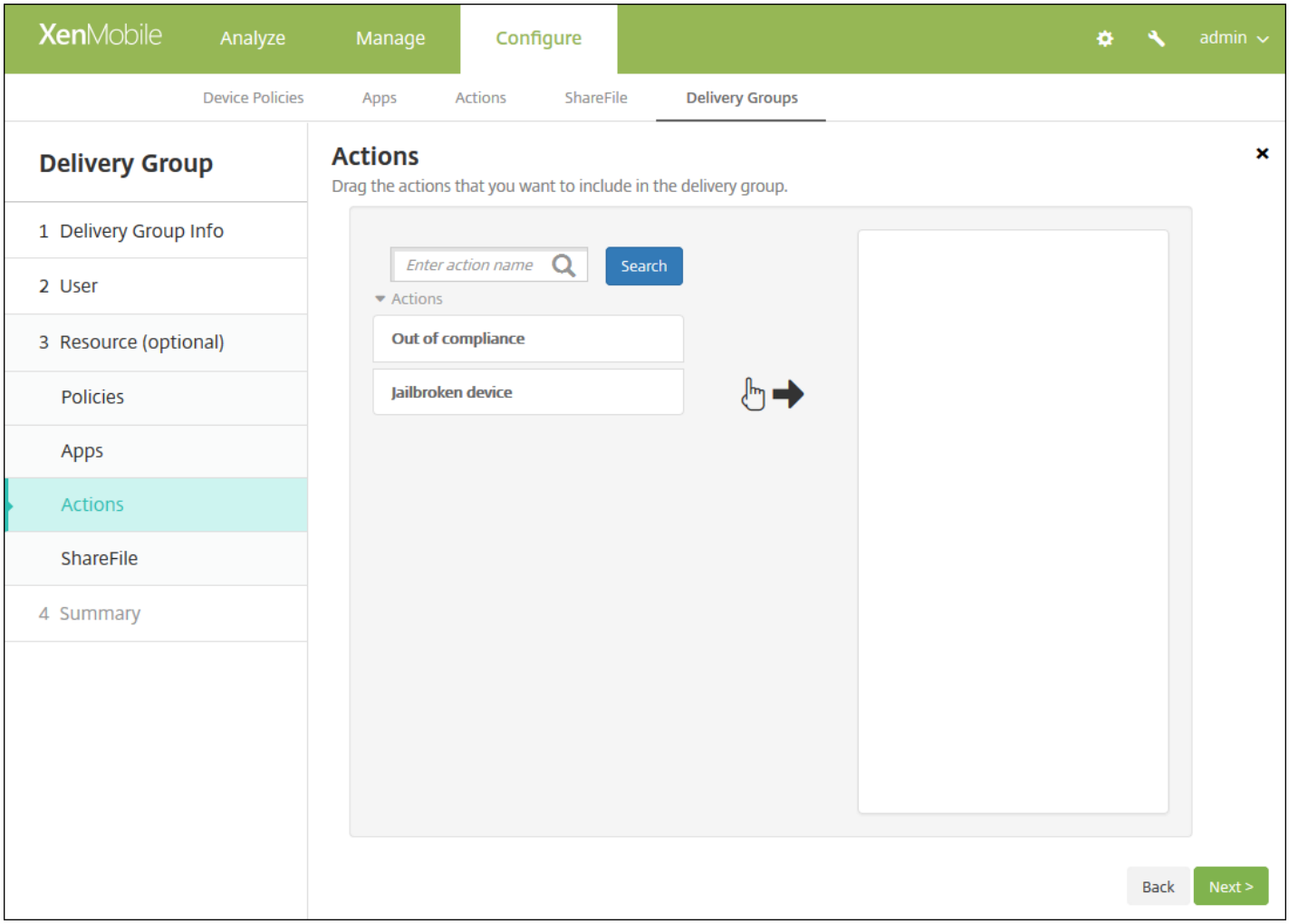
1. Führen für jede App, die Sie hinzufügen möchten, folgende Schritte aus:

- Suchen Sie die gewünschte App in der Liste der verfügbaren Apps.
- Alternative: Um die Liste der Apps einzuschränken, geben Sie den App-Namen vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf **Suchen**.
- Klicken Sie auf die App und ziehen Sie sie entweder in das Feld **Erforderliche Apps** oder in das Feld **Optionale Apps**.

Hinweis: Zum Entfernen einer App klicken Sie im rechten Feld auf das **X** neben deren Namen.

2. Klicken Sie auf **Weiter**. Die Seite **Aktionen** wird angezeigt.

Hinzufügen von Aktionen



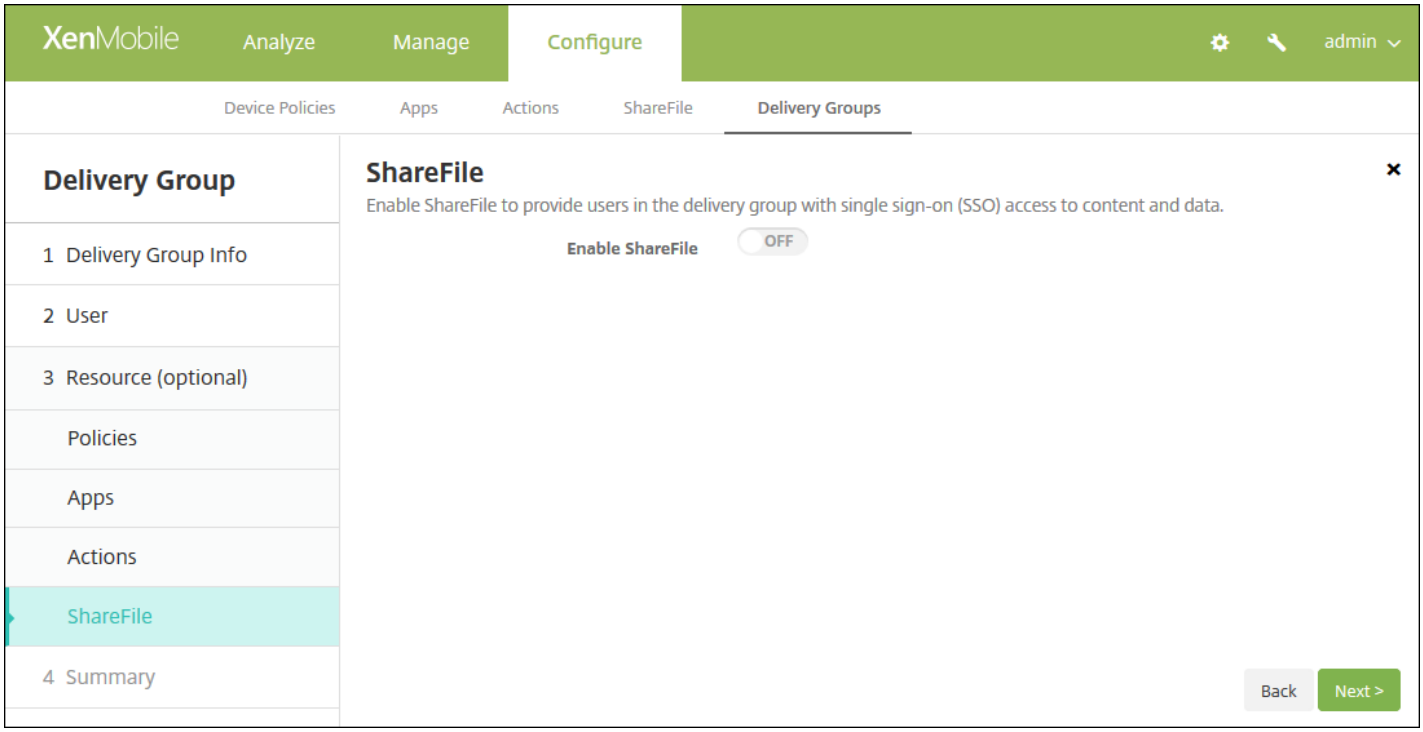
1. Führen für jede Aktion, die Sie hinzufügen möchten, folgende Schritte aus:

- Suchen Sie die gewünschte Aktion in der Liste der verfügbaren Aktionen.
- Alternative: Um die Liste der Aktionen einzuschränken, geben Sie den Namen der Aktion vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf **Suchen**.
- Klicken Sie auf die Aktion und ziehen Sie sie in das Feld auf der rechten Seite.

Hinweis: Zum Entfernen einer Aktion klicken Sie im rechten Feld auf das **X** neben deren Namen.

2. Klicken Sie auf **Weiter**. Die Seite **ShareFile** wird angezeigt.

ShareFile aktivieren

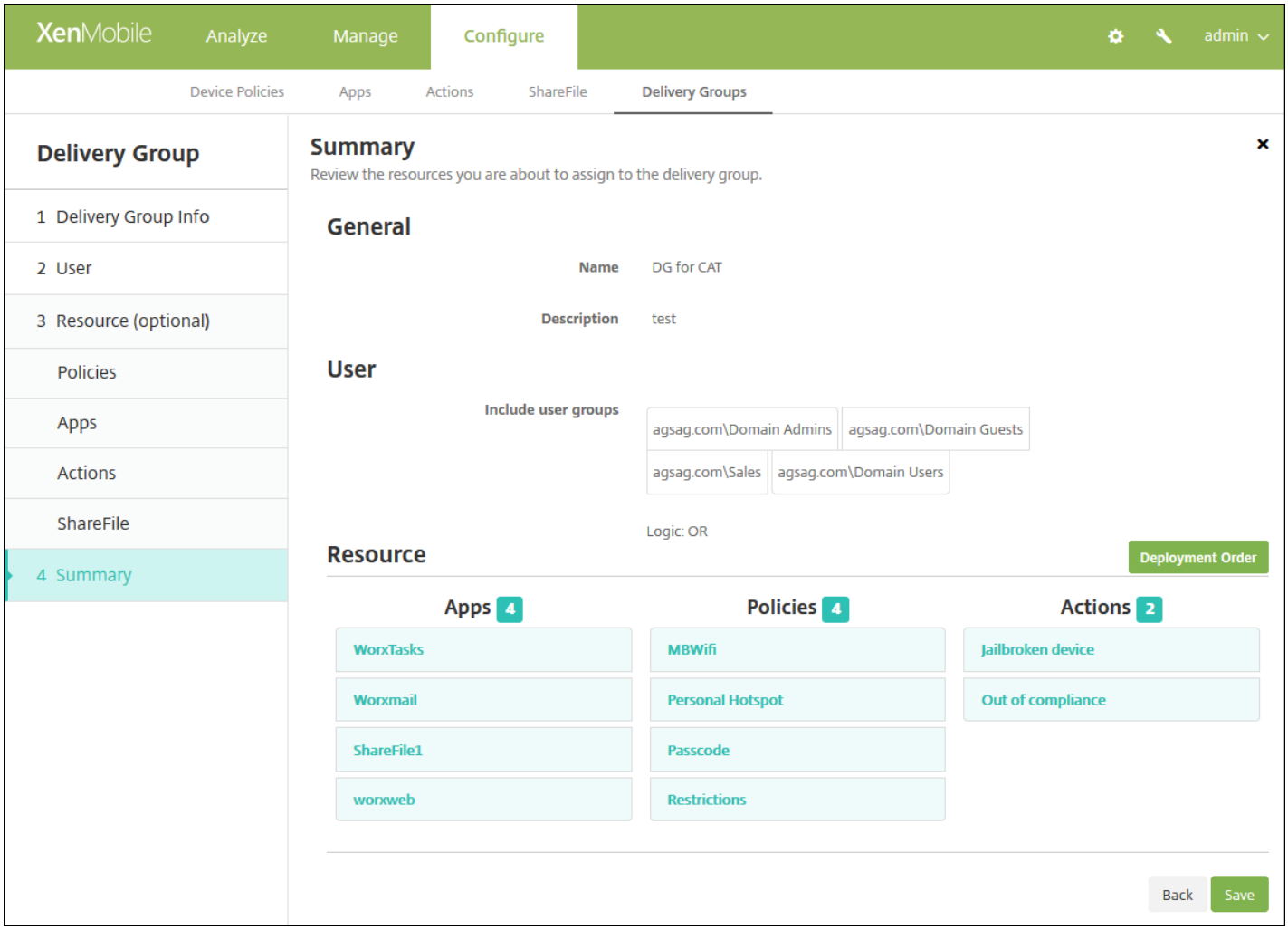


1. Konfigurieren Sie folgende Einstellung:

- **ShareFile aktivieren**: Klicken Sie auf **Ein**, um Single Sign-On über ShareFile für den Zugriff auf Inhalt und Daten zu aktivieren.

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

Überprüfen der konfigurierten Optionen und Ändern der Bereitstellungsreihenfolge



Auf der Seite **Zusammenfassung** können Sie die Optionen überprüfen, die Sie für die Bereitstellungsgruppe konfiguriert haben, und die Bereitstellungsreihenfolge der Ressourcen ändern. Auf der Seite "Zusammenfassung" werden die Ressourcen nach Kategorie angezeigt. Die Bereitstellungsreihenfolge ist hier nicht ersichtlich.

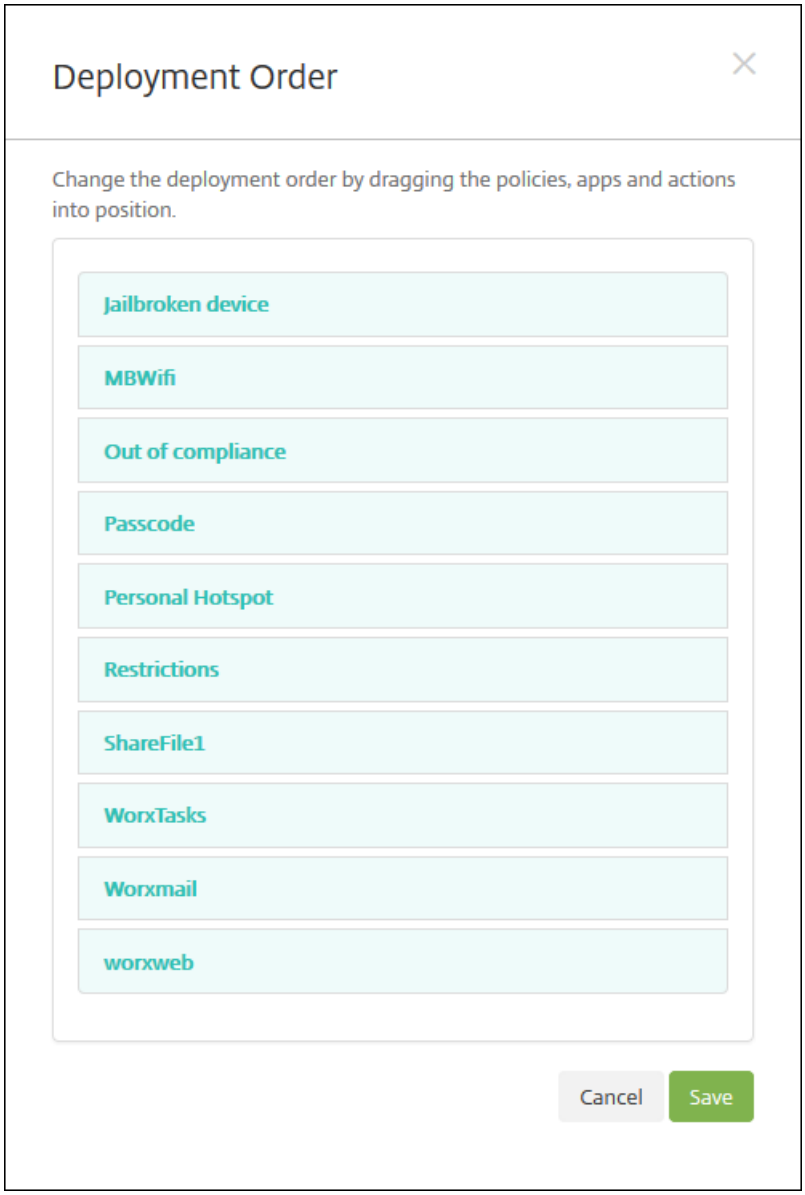
1. Klicken Sie auf **Zurück**, um zu vorherigen Seiten zurückzukehren und notwendige Änderungen an der Konfiguration zu machen.

2. Klicken Sie auf **Bereitstellungsreihenfolge**, um die Reihenfolge anzuzeigen und ggf. zu ändern.

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

Ändern der Bereitstellungsreihenfolge

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



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

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

Bearbeiten einer Bereitstellungsgruppe

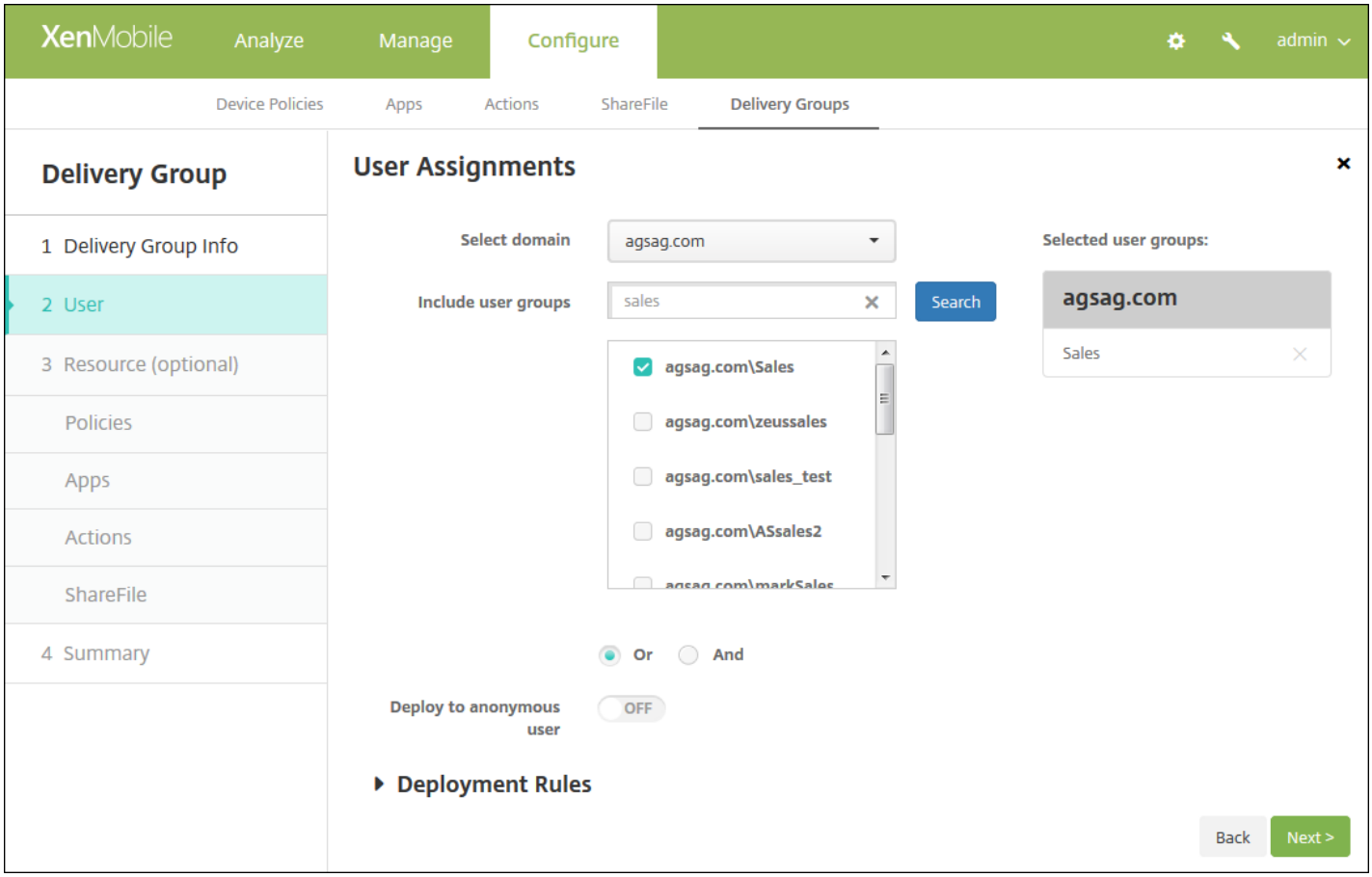
1. Wählen Sie auf der Seite **Bereitstellungsgruppen** die gewünschte Bereitstellungsgruppe aus, indem Sie auf das Kontrollkästchen neben ihrem Namen oder auf die Zeile mit ihrem Namen klicken, und klicken Sie auf **Bearbeiten**. Die Seite **Bereitstellungsgruppeninformationen** wird zur Bearbeitung angezeigt.

> **Hinweis**
>
> Der Befehl **Bearbeiten** wird, je nachdem wie Sie die Bereitstellungsgruppe ausgewählt haben, oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.

2. Ändern Sie unter **Beschreibung** die Beschreibung, bzw. fügen Sie eine Beschreibung hinzu.

Hinweis: Sie können den Namen einer vorhandenen Gruppe nicht ändern.

3. Klicken Sie auf **Weiter**. Die Seite **Benutzerzuweisungen** wird angezeigt.



4. Geben Sie im Bereich **Benutzergruppen auswählen** die folgenden Informationen ein, bzw. ändern Sie sie:

- **Domäne auswählen**: Wählen Sie in der Liste die Domäne aus, in der Sie Benutzer auswählen möchten.
- **Benutzergruppen einschließen**: Führen Sie einen der folgenden Schritte aus:
  - Klicken Sie in der Liste der Benutzergruppen auf die Gruppen, die Sie hinzufügen möchten. Die ausgewählten Gruppen werden in der Liste **Ausgewählte Benutzergruppen** angezeigt.
  - Klicken Sie auf **Suchen**, um eine Liste aller Benutzergruppen in der ausgewählten Domäne anzuzeigen.
  - Geben Sie den Gruppennamen vollständig oder teilweise in das Suchfeld ein und klicken Sie dann auf **Suchen**, um die Liste der Benutzergruppen einzuschränken.

    Hinweis: Zum Entfernen von Benutzergruppen klicken Sie auf **Suchen** 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 **Suchen** klicken, um die Liste der Benutzergruppen einzuschränken.

- **Oder/Und**: Wählen Sie aus, ob Benutzer für die Bereitstellung nur einer Gruppe angehören dürfen (Oder) oder ob sie allen Gruppen angehören müssen (Und).
- **Für anonyme Benutzer bereitstellen**: Wählen Sie aus, ob die Bereitstellung auch für nicht authentifizierte Benutzer in

der Bereitstellungsgruppe erfolgen soll.

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

5. Erweitern Sie **Bereitstellungsregeln** und konfigurieren Sie die Einstellungen wie zuvor in Schritt 5 dieses Verfahrens.

6. Klicken Sie auf **Weiter**. Die Seite **Ressourcen** für die Bereitstellungsgruppe wird angezeigt. Hier können Sie Richtlinien, Apps oder Aktionen hinzufügen oder löschen. Zum Überspringen dieses Schritts klicken Sie unter **Bereitstellungsgruppe** auf **Zusammenfassung**, um eine Zusammenfassung der Bereitstellungsgruppenkonfiguration anzuzeigen.

7. Wenn Sie eine Ressource modifiziert haben, klicken Sie auf **Weiter** oder unter **Bereitstellungsgruppe** auf **Zusammenfassung**.

8. Auf der Seite **Zusammenfassung** können Sie die Optionen überprüfen, die Sie für die Bereitstellungsgruppe konfiguriert haben, und die Bereitstellungsreihenfolge der Ressourcen ändern.

9. Klicken Sie auf **Zurück**, um auf vorherige Seiten aufzurufen, wenn Sie Änderungen vornehmen müssen.

10. Klicken Sie auf **Bereitstellungsreihenfolge**, um die Bereitstellungsreihenfolge der Ressourcen zu ändern. Weitere Informationen zum Ändern der Bereitstellungsreihenfolge finden Sie unter Ändern der Bereitstellungsreihenfolge.

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

Aktivieren oder Deaktivieren der Bereitstellungsgruppe "AllUsers"

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

1. Wählen Sie auf der Seite **Bereitstellungsgruppen** 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 **Aktivieren** bzw. **Deaktivieren** wird, je nachdem wie Sie die Bereitstellungsgruppe "AllUsers" ausgewählt haben, oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.

- Klicken Sie auf **Deaktivieren**, um die Bereitstellungsgruppe "AllUsers" zu deaktivieren. Dieser Befehl ist nur verfügbar, wenn "AllUsers" aktiviert ist (= Standardeinstellung). **Deaktiviert** wird unter der gleichnamigen Spaltenüberschrift in der Tabelle angezeigt.
- Klicken Sie auf **Aktivieren**, um die Bereitstellungsgruppe "AllUsers" zu aktivieren. Dieser Befehl ist nur verfügbar, wenn "AllUsers" deaktiviert ist. **Deaktiviert** wird unter der gleichnamigen Spaltenüberschrift in der Tabelle ausgeblendet.

Bereitstellen in Bereitstellungsgruppen

Das Bereitstellen in einer Bereitstellungsgruppe bedeutet, dass eine Pushbenachrichtigung an alle Benutzer mit iOS-, Windows Phone- und Windows Tablet-Geräte in der Bereitstellungsgruppe gesendet wird, dass sie sich mit XenMobile verbinden. Auf diese Weise können Sie die Geräte neu auswerten und Apps, Richtlinien und Aktionen bereitstellen. Benutzer mit Geräten auf anderen Plattformen 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 **Bereitstellungsgruppen** einen der folgenden Schritte aus:

- Zur Bereitstellung für mehrere Bereitstellungsgruppen aktivieren Sie die Kontrollkästchen neben den gewünschten Gruppen.
- Zum Bereitstellen einer einzelnen Bereitstellungsgruppe klicken Sie auf das Kontrollkästchen neben dem Namen oder auf die Zeile mit dem Namen.

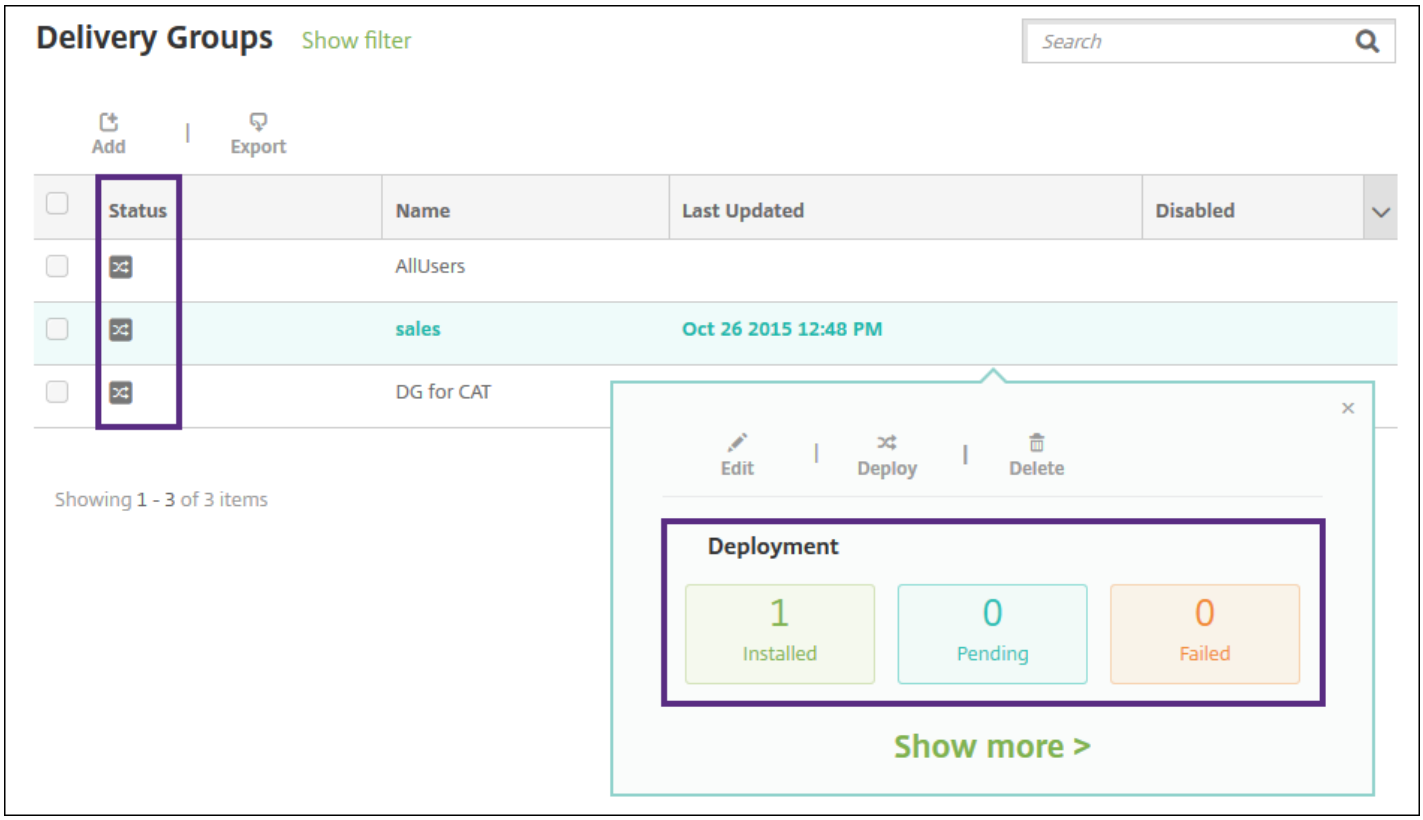
2. Klicken Sie auf **Bereitstellen**.

Hinweis: Der Befehl **Bereitstellen** wird, je nachdem wie Sie die einzelne Bereitstellungsgruppe ausgewählt haben, oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.

Stellen Sie sicher, dass die Gruppen, in denen Sie Apps, Richtlinien und Aktionen bereitstellen möchten, aufgelistet werden und klicken Sie dann auf **Bereitstellen**. Die Apps, Richtlinien und Aktionen werden in den ausgewählten Gruppen bereitgestellt, basierend auf Geräteplattform und Planungsrichtlinie.

Sie können den Bereitstellungsstatus auf der Seite **Bereitstellungsgruppen** 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 **Installiert**, **Ausstehend** oder **Fehlgeschlagen** angezeigt wird.



Löschen von Bereitstellungsgruppen

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

1. Führen Sie auf der Seite **Bereitstellungsgruppen** 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 **Löschen**. Das Dialogfeld **Löschen** wird angezeigt.

Hinweis: Der Befehl **Löschen** wird, je nachdem wie Sie die einzelne Bereitstellungsgruppe ausgewählt haben, oberhalb der Bereitstellungsgruppe oder rechts daneben angezeigt.

3. Klicken Sie auf **Löschen**.

> **Important**
>
> Sie können diese Aktion nicht rückgängig machen.

Exportieren der Bereitstellungsgruppentabelle

1. Klicken Sie auf die Schaltfläche **Exportieren** oberhalb der Tabelle **Bereitstellungsgruppen**. Die Informationen in der Tabelle **Bereitstellungsgruppen** werden extrahiert und in eine CSV-Datei konvertiert.

2. Öffnen oder speichern Sie die CSV-Datei. Ihre Vorgehensweise hängt von dem verwendeten Browser ab. Sie können den Vorgang auch abbrechen.

Registrieren von Benutzern und Geräten

Aug 22, 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.

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 **Verwalten > Registrierung**:

Android-Geräte

Jul 28, 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. Sie müssen die Worx-PIN zweimal eingeben. Geben Sie im Bildschirm Worx-PIN erstellen eine PIN aus sechs beliebigen Zahlen ein.
8. Geben Sie die PIN erneut ein. Worx Home wird geöffnet. Sie können nun auf den Worx Store zugreifen und Apps für die Installation auf dem Android-Gerät anzeigen.
9. Wenn Sie XenMobile so konfiguriert haben, dass Apps nach der Registrierung automatisch per Push auf Benutzergeräten bereitgestellt werden, werden Meldungen angezeigt, durch die die Benutzer zur Installation der Apps aufgefordert werden. Tippen Sie auf Installieren, um die Apps zu installieren.

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

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 Erneut registrieren. Eine Meldung wird zur Bestätigung, dass Sie das Gerät erneut registrieren möchten, angezeigt.
4. Tippen Sie auf OK. Die Registrierung des Geräts wird aufgehoben.
5. Folgen Sie dann den Anweisungen auf dem Bildschirm, um das Gerät erneut zu registrieren.

iOS-Geräte

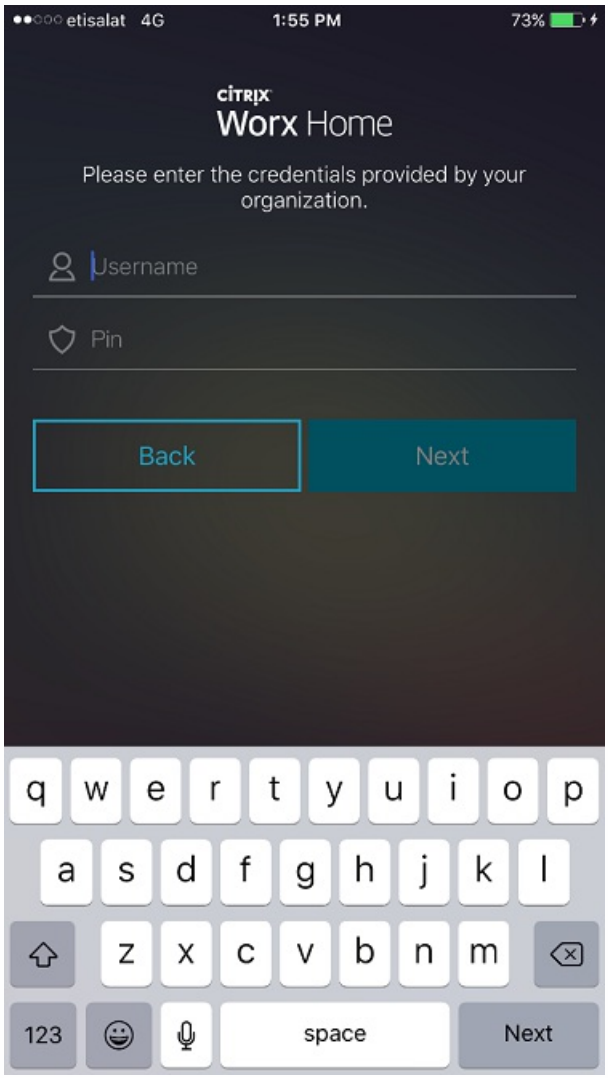
Jul 28, 2016

1. Laden Sie die Worx Home-App aus dem Apple iTunes-App Store auf das Gerät herunter und installieren Sie sie auf dem Gerät.

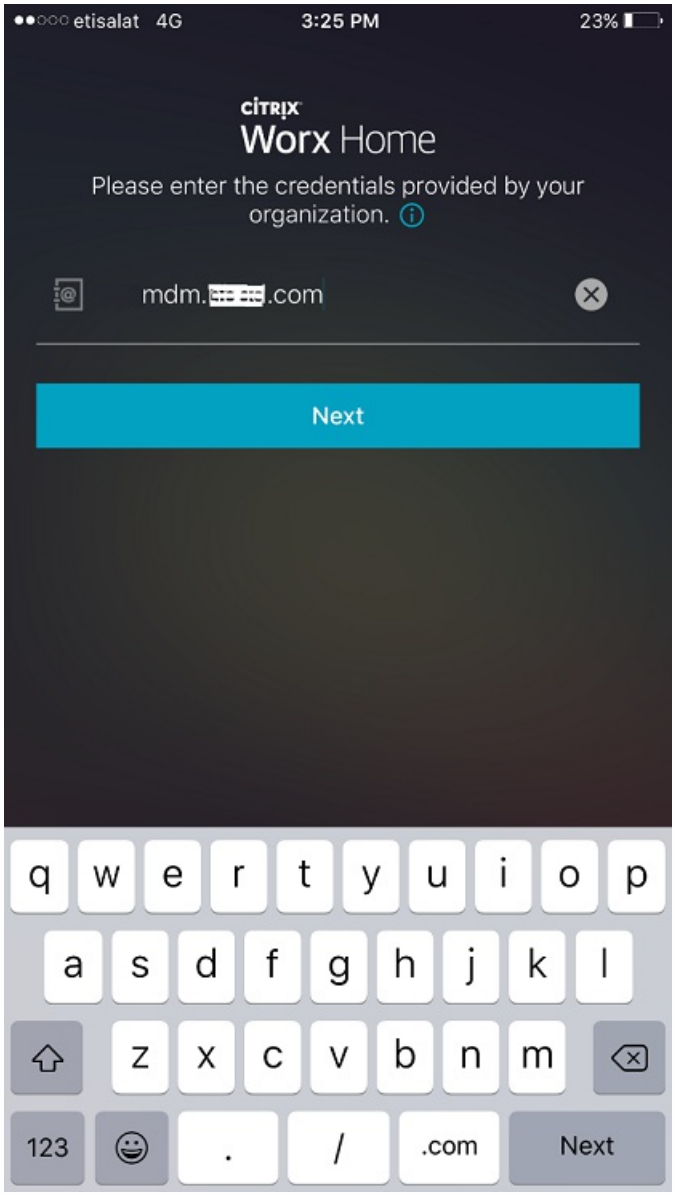
2. Tippen Sie auf dem Homebildschirm des iOS-Geräts auf die Worx Home-App.

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**.

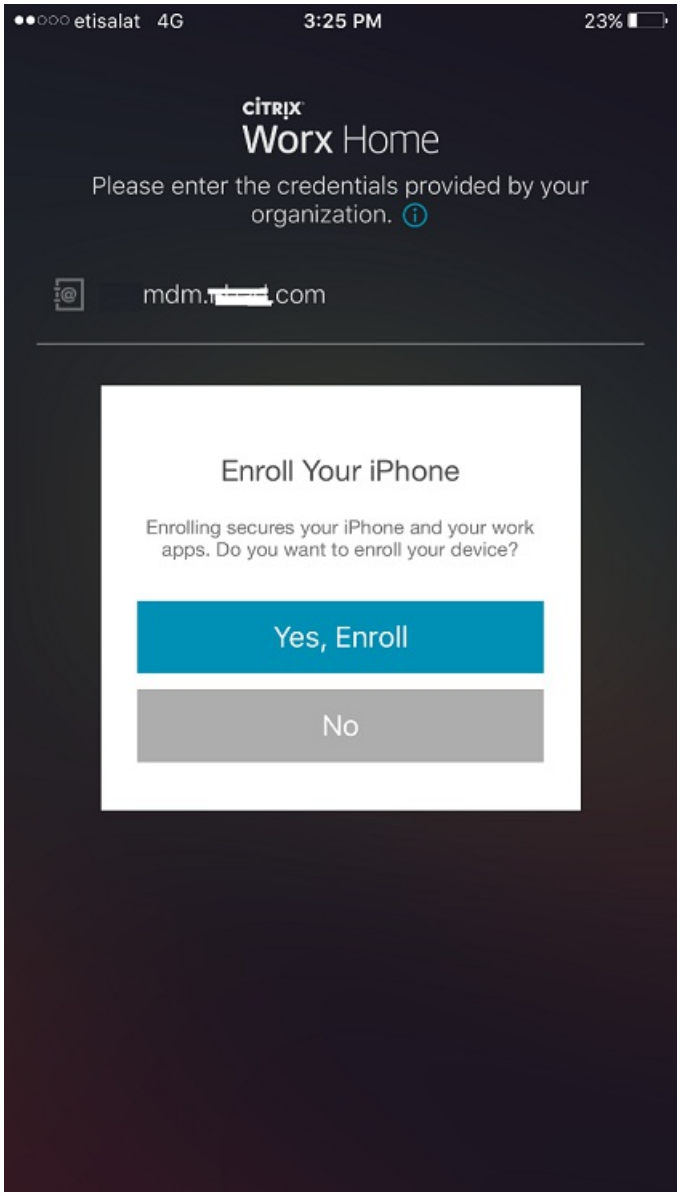
Die angezeigten Seiten unterscheiden sich je nach XenMobile-Konfiguration u. U. von den folgenden Beispielen.

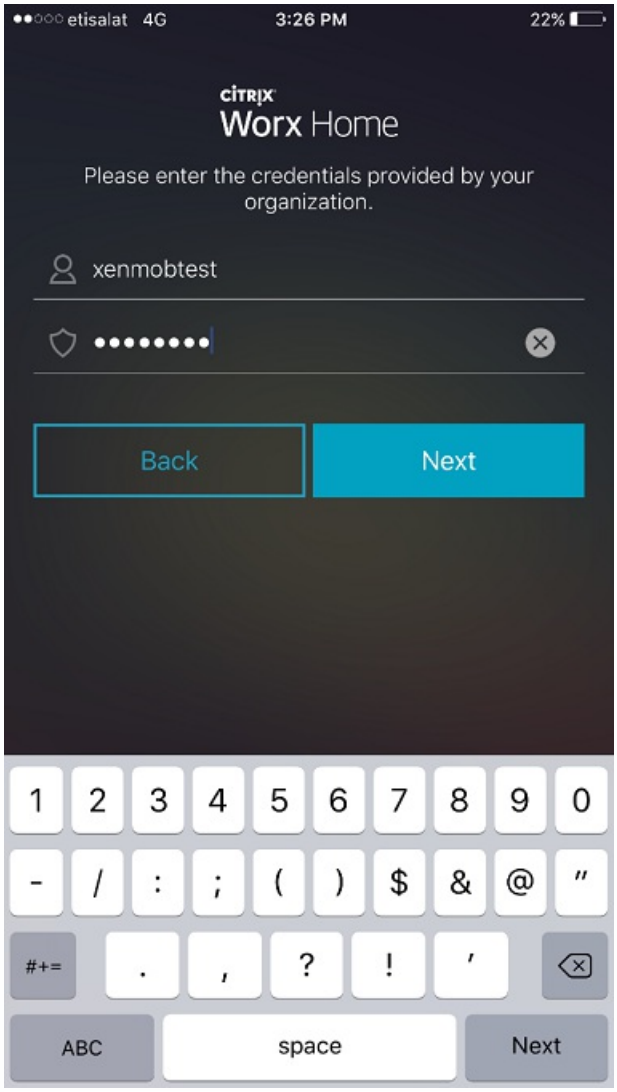


4. Geben Sie die von Ihrem Helpdesk erhaltene Adresse ein.



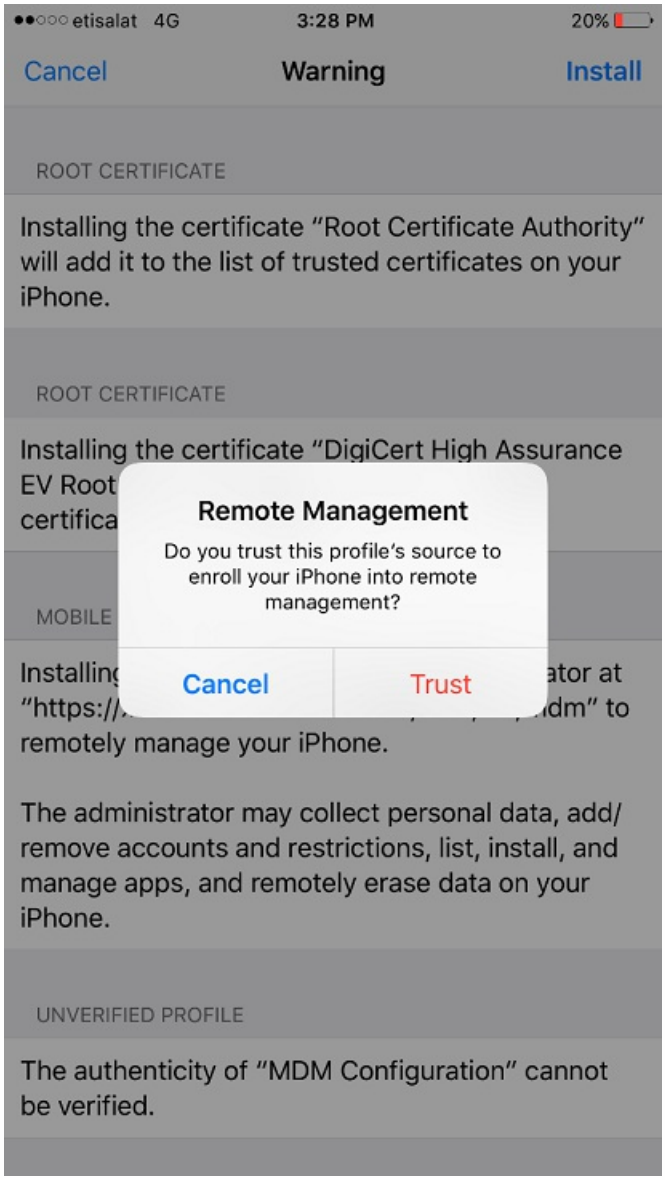
5. Wenn Sie zur Registrierung aufgefordert werden, klicken Sie auf **Ja, registrieren** und geben Sie Ihre Anmeldeinformationen ein, wenn Sie dazu aufgefordert werden.



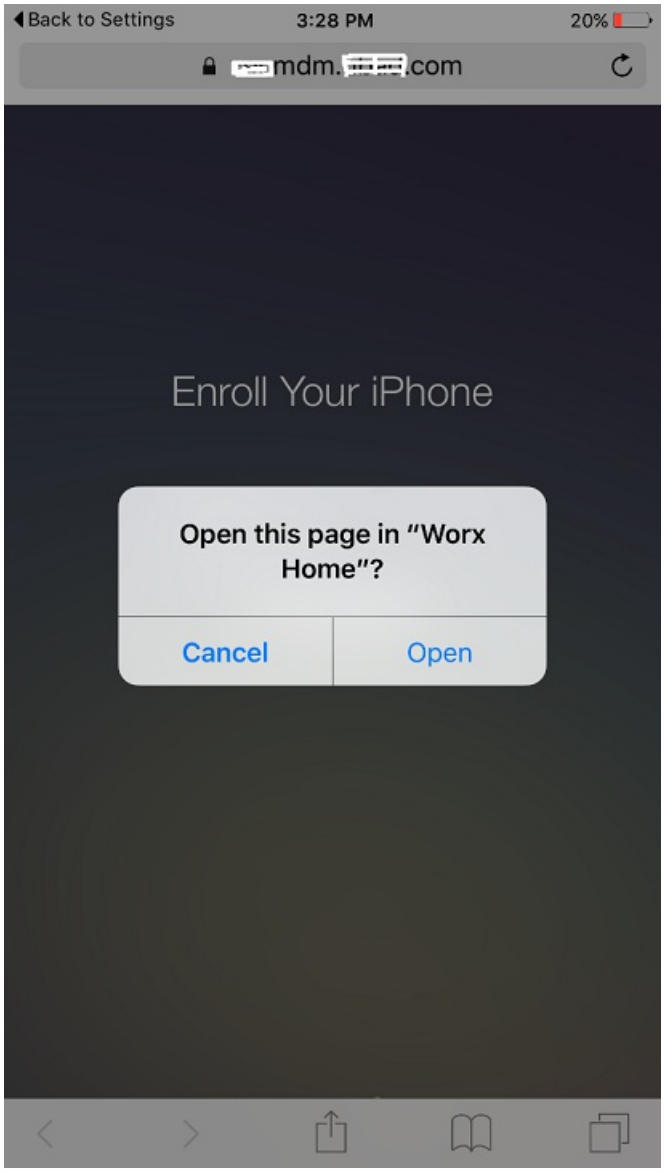


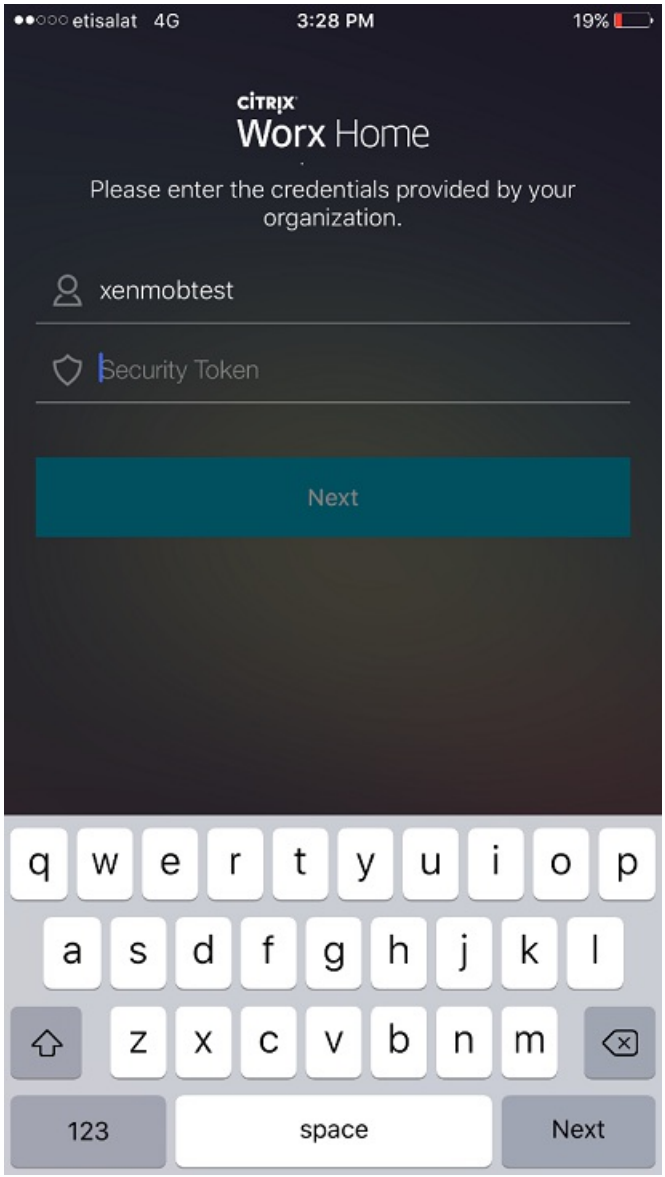
6. Tippen Sie auf **Installieren**, um den Citrix Profildienst zu installieren.

7. Tippen Sie auf **Vertrauensstellung**.



8. Tippen Sie auf **Öffnen** und geben Sie Ihre Anmeldeinformationen ein.





Mac OS X-Geräte

Jul 28, 2016

Sie können Mac-Geräte, auf denen Mac OS X ausgeführt wird, in XenMobile registrieren. Mac-Benutzer führen die Registrierung direkt über das Gerät aus.

Das Verfahren zur Registrierung von Macs ist folgendes:

1. Richten Sie optional Mac-Geräterichtlinien in der XenMobile-Konsole ein. Weitere Informationen finden Sie unter Geräterichtlinien. Der Abschnitt XenMobile-Geräterichtlinien nach Plattform enthält Informationen dazu, welche Geräterichtlinien Sie für Macs konfigurieren können.

2. Senden Sie den Registrierungslink https://serverFQDN:8443/zdm/macos/otae. Diesen öffnen die Benutzer in Safari. Dabei ist

- serverFQDN der vollqualifizierte Domänenname (FQDN) des Servers, auf dem XenMobile ausgeführt wird.
- Port 8443 ist der standardmäßige sichere Port. Wenn Sie einen anderen Port konfiguriert haben, verwenden Sie diesen Port anstelle von 8443.
- zdm ist der Instanzname, der bei der Serverinstallation verwendet wird.

Weitere Informationen zum Senden von Installationslinks finden Sie unter Senden von Installationslinks.

3. Die Benutzer installieren die benötigten Zertifikate. Ob Benutzer zur Installation von Zertifikaten aufgefordert werden, hängt davon ab, ob Sie ein öffentlich vertrauenswürdiges SSL-Zertifikat und ein öffentlich vertrauenswürdiges digitales Signaturzertifikat für iOS und Mac OS konfiguriert haben. Weitere Informationen über Zertifikate finden Sie unter Zertifikate.

4: Die Benutzer melden sich bei ihren Macs an.

5. Die Mac-Geräterichtlinien werden installiert.

Sie können Macs nun mit XenMobile genauso verwalten wie Mobilgeräte.

Windows-Geräte

Jul 28, 2016

Sie können in XenMobile Geräte mit folgenden Windows-Betriebssystemen registrieren:

- Windows 8.1 und 10
- Windows Phone 8.1 und 10

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

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

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

Registrieren von Windows-Geräten mit Autodiscovery

Benutzer können Geräte mit Windows RT 8.1, Windows 8.1 Pro (32-Bit- und 64-Bit-Version), Windows 8.1 Enterprise und Windows 10 registrieren. Um die Verwaltung von Windows-Geräten zu ermöglichen, empfiehlt Citrix, dass Sie Autodiscovery und den Windows-Ermittlungsdienst konfigurieren. Weitere Informationen finden Sie unter Aktivieren von Autodiscovery für die Benutzerregistrierung in XenMobile.

1. Prüfen Sie auf dem Gerät auf Updates und installieren Sie alle verfügbaren Windows-Updates. Dieser Schritt ist besonders beim Upgrade von Windows 8 auf Windows 8.1 wichtig, da die Benutzer möglicherweise nicht automatisch über alle verfügbaren Updates benachrichtigt werden.

2. Tippen Sie im Charms-Menü auf **Einstellungen** und dann auf Folgendes:

- Für Windows 8.1 tippen Sie auf **Netzwerk** > **Arbeitsbereich**.
- Für Windows 10 tippen Sie auf **Konten** > **Arbeitsplatzzugriff** > **Für MDM-Verwaltungsdienst registrieren**.

3. Geben Sie Ihre geschäftliche E-Mail-Adresse ein und tippen Sie dann auf **Einschalten** in Windows 8.1 oder auf **Weiter** in Windows 10. 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, wobei die Registrierung von Windows integrierter Geräteverwaltung vorgenommen wird. 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. In Windows 8.1 stimmen Sie im Dialogfeld **Apps und Dienste des IT-Administrators zulassen** zu, dass Ihr Gerät verwaltet wird und tippen auf **Einschalten**. In Windows 10 stimmen Sie im Dialogfeld **Nutzungsbedingungen** zu, dass Ihr Gerät verwaltet wird und tippen auf **Akzeptieren**.

Registrieren von Windows-Geräten ohne Autodiscovery

Windows-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 beim Upgrade von Windows 8 auf Windows 8.1 wichtig, da die Benutzer möglicherweise nicht automatisch über alle verfügbaren Updates benachrichtigt werden.

2. Tippen Sie im Charms-Menü auf **Einstellungen** und dann auf Folgendes:

- In Windows 8.1 tippen Sie auf **Netzwerk** > **Arbeitsbereich**.
- In Windows 10 tippen Sie auf **Konten** > **Arbeitsplatzzugriff** > **Für MDM-Verwaltungsdienst registrieren**.

3. Geben Sie Ihre geschäftliche E-Mail-Adresse ein.

4. Unter Windows 10 wird, wenn Autodiscovery nicht konfiguriert ist, eine Option zur Eingabe der Serverinformationen (s. Schritt 5) angezeigt. Wenn unter Windows 8.1 die Option zum automatischen Erkennen der Serveradresse aktiviert ist, deaktivieren Sie die Option.

5. Machen Sie im Feld zur Eingabe der Adresse des Servers folgende Eingabe:

- Geben Sie unter Windows 8.1 die Serveradresse in folgendem Format ein: https://*serverfqdn:8443/serverinstanz*/Discovery.svc. Wenn für SSL-Verbindungen ohne Authentifizierung eine andere Portnummer als *8443* verwendet wird, geben Sie die verwendete Portnummer mit der Adresse ein.
- Verwenden Sie unter Windows 10 folgende Adresse: https://beta.managedm.com:8443/zdm/wpe. 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. In Windows 8.1 stimmen Sie im Dialogfeld **Apps und Dienste des IT-Administrators zulassen** zu, dass Ihr Gerät verwaltet wird und tippen auf **Einschalten**. In Windows 10 stimmen Sie im Dialogfeld **Nutzungsbedingungen** zu, dass Ihr Gerät verwaltet wird und tippen auf **Akzeptieren**.

Registrieren von Windows Phone-Geräten in XenMobile

Für die Registrierung von Windows Phone-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-App für Citrix Worx Home für jede unterstützte Plattform).
1. Tippen Sie auf der Hauptseite des Windows Phone-Geräts auf das Symbol **Einstellungen**.

2. Tippen Sie unter Windows Phone 8.1 auf **System** > **Arbeitsbereich** und dann auf **Konto hinzufügen**. Bei einem Windows 10 Phone tippen Sie auf **Konten** > **Arbeitsplatzzugriff** > **Für MDM-Verwaltungsdienst registrieren**.

3. 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.

4. 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.

5. Geben Sie den Benutzernamen und die Domäne ein, sofern die Authentifizierung über einen Benutzernamen und eine Domäne erfolgt und tippen Sie auf **Anmelden**.

6. 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**.

7. Wenn das Konto unter Windows Phone 8.1 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.

8. Tippen Sie unter Windows Phone 8.1 im Bildschirm **Konto hinzugefügt** auf **Fertig**.

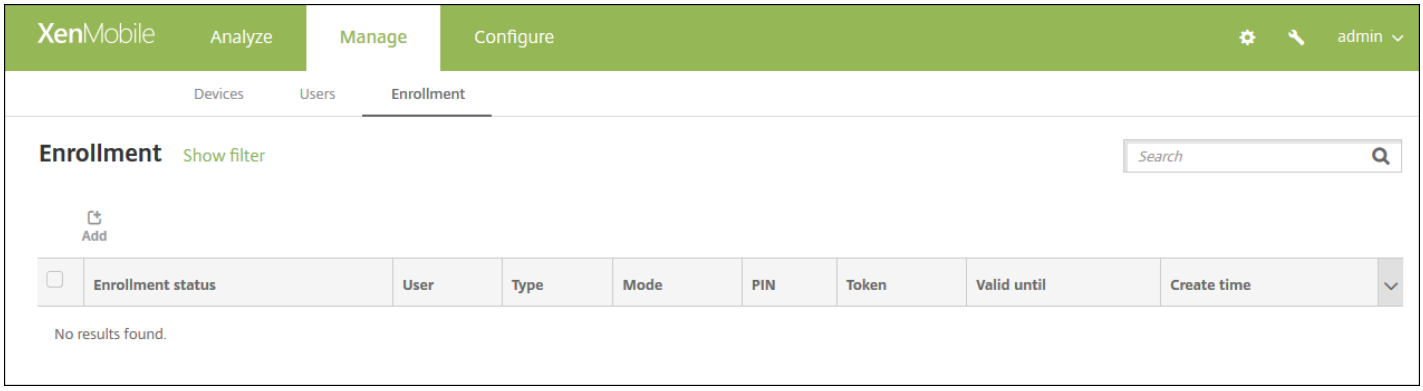
9. Zum Erzwingen einer Verbindung mit dem Server tippen Sie auf das Symbol zum Aktualisieren. Wenn das Gerät nicht manuell eine Verbindung mit Server herstellt, versucht XenMobile, die Verbindung wiederherzustellen. XenMobile versucht 5 Mal alle 3 Minuten eine Verbindung herzustellen, anschließend alle 2 Stunden. Sie können diese Verbindungsrate unter **Servereigenschaften** über die Option Windows **WNS-Taktintervall** ändern. Nachdem die Registrierung abgeschlossen ist, wird Worx Home im Hintergrund registriert. Der Abschluss der Installation wird nicht angezeigt. Öffnen Sie Worx Home über den Bildschirm **Alle Apps**.

Senden einer Registrierungseinladung in XenMobile

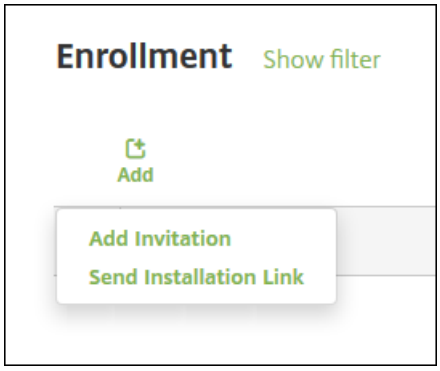
Oct 13, 2016

In der XenMobile-Konsole können Sie Registrierungseinladungen an Benutzer mit iOS- oder Android-Geräten senden. Sie können auch einen Installationslink an Benutzer mit iOS-, Android-, Windows- oder Mac-Geräten senden.

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



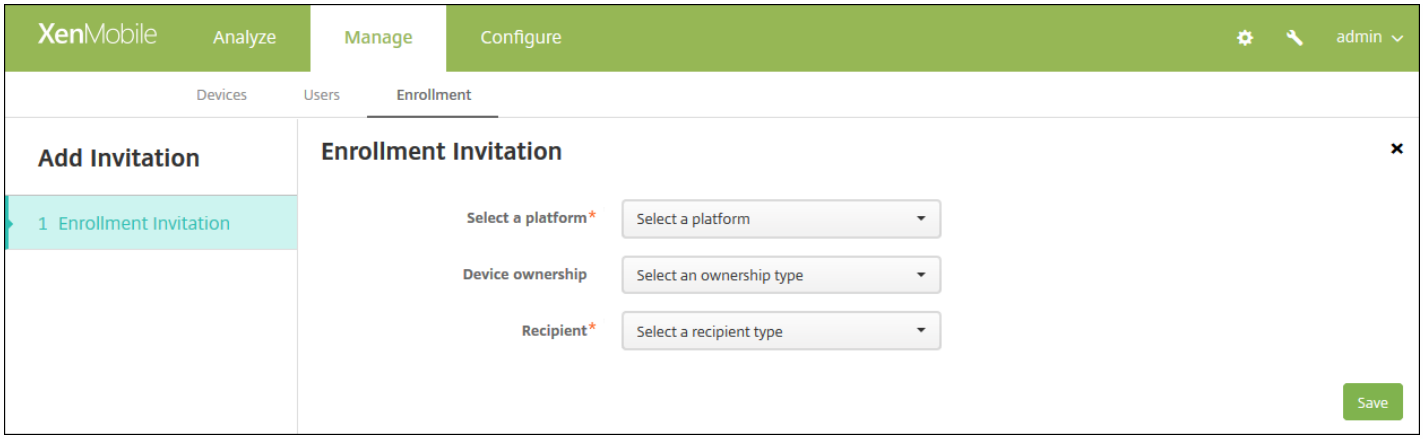
2. Klicken Sie auf **Hinzufügen**. Ein Menü mit den Registrierungsoptionen wird eingeblendet.



- Zum Senden einer Registrierungseinladung an einen Benutzer oder eine Gruppe klicken Sie auf **Einladung hinzufügen** und konfigurieren Sie diese Einstellung gemäß den Anweisungen unter Senden von Einladungen.
- Zum Senden eines Installationslinks an eine Reihe von Benutzern über SMTP oder per SMS klicken Sie auf **Installationslink senden** und konfigurieren Sie diese Einstellung gemäß den Anweisungen unter Senden von Installationslinks.

Senden von Einladungen

1. Klicken Sie auf **Einladung hinzufügen**. Die Seite **Registrierungseinladung** wird angezeigt.

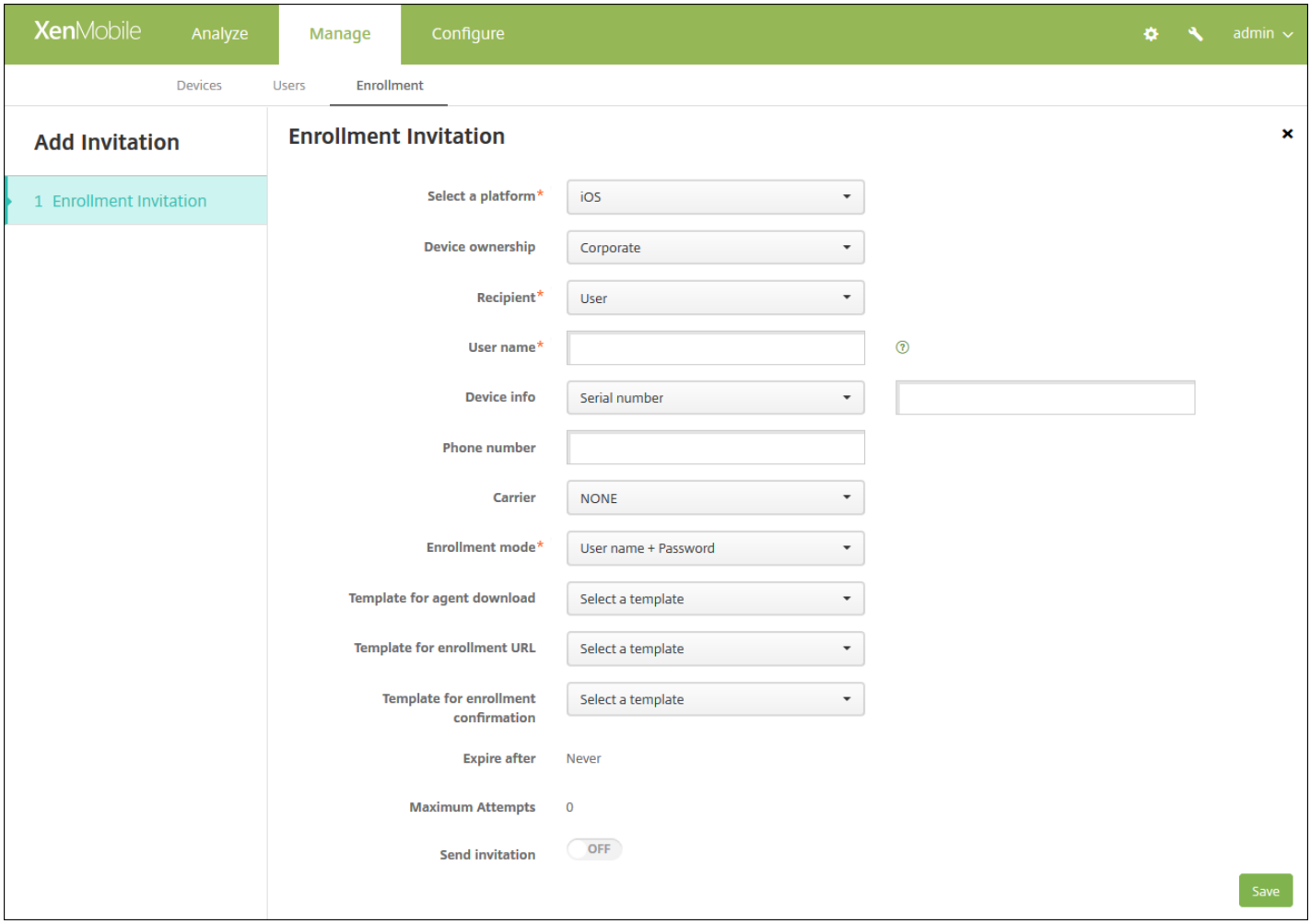


2. Konfigurieren Sie die folgenden Einstellungen:

- **Plattform wählen** Klicken Sie in der Liste auf **iOS** oder **Android**.
- **Gerätebesitz**: Klicken Sie in der Liste auf **Unternehmen** oder **Mitarbeiter**.
- **Empfänger**: Klicken Sie in der Liste auf **Benutzer** oder **Gruppe**.

Abhängig vom ausgewählten Empfänger werden ggf. weitere Einstellungen zum Konfigurieren angezeigt. Informationen zum Festlegen von Einstellungen für Benutzer finden Sie unter Senden von Registrierungseinladungen an Benutzer, die Einstellungen für Gruppen werden unter Senden von Registrierungseinladungen an Gruppen erläutert.

Senden einer Registrierungseinladung an einen Benutzer



1. Konfigurieren Sie folgende Einstellungen für **Benutzer**:

- **Benutzername**: Geben Sie 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 an sie gesendet werden können. Bei Active Directory-Benutzern muss LDAP konfiguriert sein.
- **Geräteinfo**: Klicken Sie in der Liste auf **Seriennummer** , **UDID** oder **IMEI**. Wenn Sie eine Option auswählen, wird ein Feld angezeigt, in das Sie den entsprechenden Wert für das Gerät eingeben können.
- **Telefonnummer**: Geben Sie optional die Telefonnummer des Benutzers ein.
- **Netzbetreiber**: Wählen Sie in der Liste den Netzbetreiber aus, der der Telefonnummer zugeordnet werden soll.
- **Registrierungsmodus**: Klicken Sie in der Liste auf die gewünschte Registrierungsmethode. Der Standard ist **Benutzername Kennwort**. Mögliche Optionen:
  - Hohe Sicherheit
  - Einladungs-URL
  - Einladungs-URL + PIN
  - Einladungs-URL + Kennwort
  - Zweifaktor
  - Benutzername + PIN

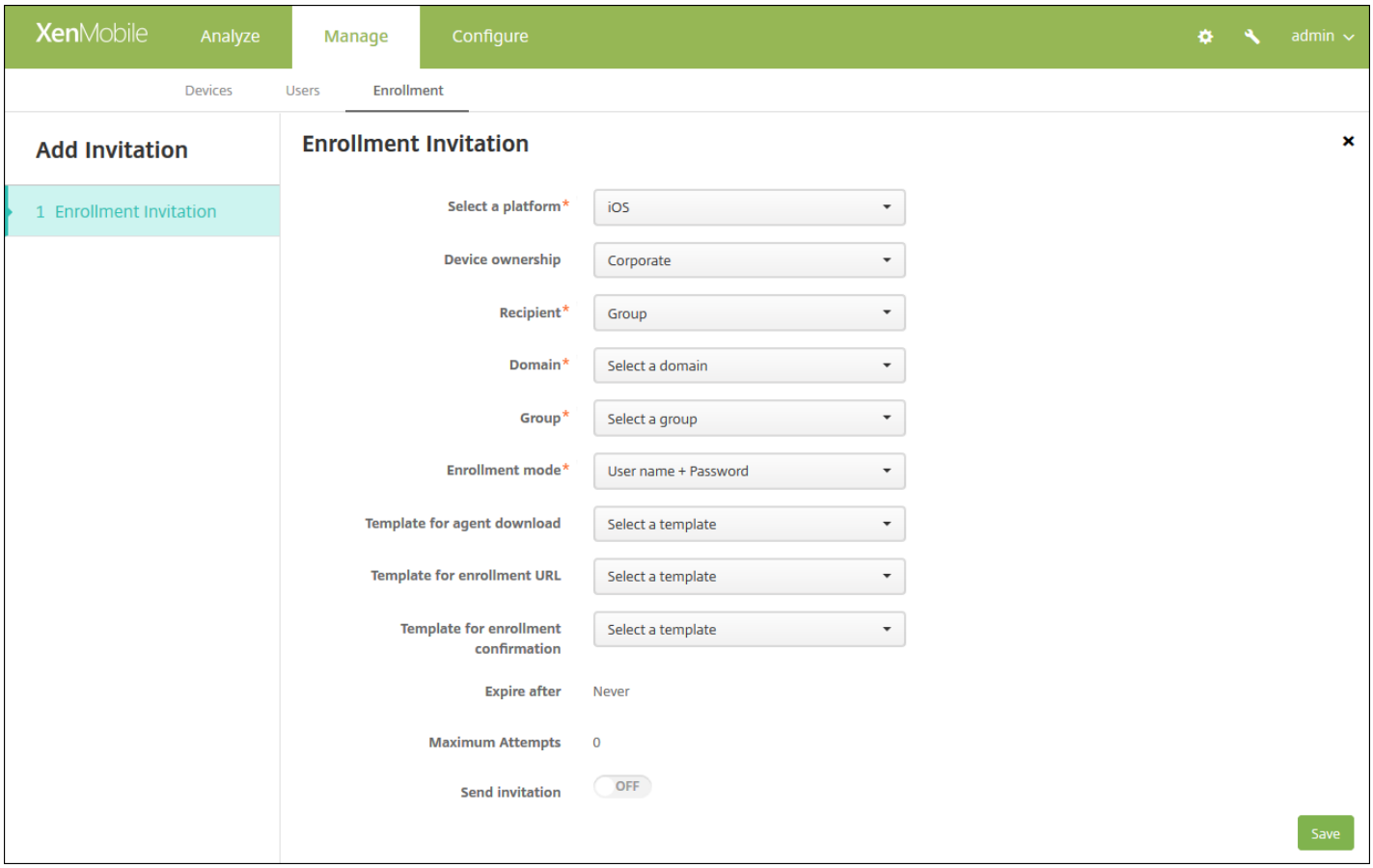
  Hinweis: Wenn Sie einen Registrierungsmodus mit PIN auswählen, wird das Feld **Vorlage für Registrierungs-PIN**

eingeblendet, in dem Sie auf **Registrierungs-PIN** klicken.

- **Vorlage für Agentdownload**: Klicken Sie in der Liste auf die Vorlage, die für die Registrierungseinladung verwendet werden soll. Die angebotenen Optionen hängen vom Plattformtyp ab. Beispielsweise wird **iOS Download Link** angezeigt, wenn Sie als Plattform **iOS** ausgewählt haben.
- **Vorlage für Registrierungs-URL**: Klicken Sie in der Liste auf **Registrierungseinladung**.
- **Vorlage für Registrierungsbestätigung**: Klicken Sie in der Liste auf **Registrierungsbestätigung**.
- **Ablauf nach**: Dieses Feld wird ausgefüllt, wenn Sie den Registrierungsmodus konfigurieren, es gibt an, wann die Registrierung abläuft. Weitere Informationen zum Konfigurieren von Registrierungsmodi finden Sie unter Konfigurieren von Registrierungsmodi.
- **Versuche maximal**: Dieses Feld wird ausgefüllt, wenn Sie den Registrierungsmodus konfigurieren, es gibt die maximale Anzahl Registrierungsversuche an. Weitere Informationen zum Konfigurieren von Registrierungsmodi finden Sie unter Konfigurieren von Registrierungsmodi.
- **Einladung senden**: Wählen Sie **Ein**, wenn die Einladung sofort gesendet werden soll, oder **Aus**, wenn lediglich die Einladung in die Tabelle auf der Seite **Registrierung** eingefügt werden soll.

2. Klicken Sie auf **Speichern und senden**, wenn Sie **Einladung senden** ausgewählt haben, andernfalls klicken Sie auf **Speichern**. Die Einladung wird in der Tabelle auf der Seite **Registrierung** aufgeführt.

Senden einer Registrierungseinladung an eine Gruppe



1. Konfigurieren Sie die folgenden Einstellungen:

- **Domäne**: Klicken Sie in der Liste auf die Domäne, in der Sie die Gruppe auswählen möchten.

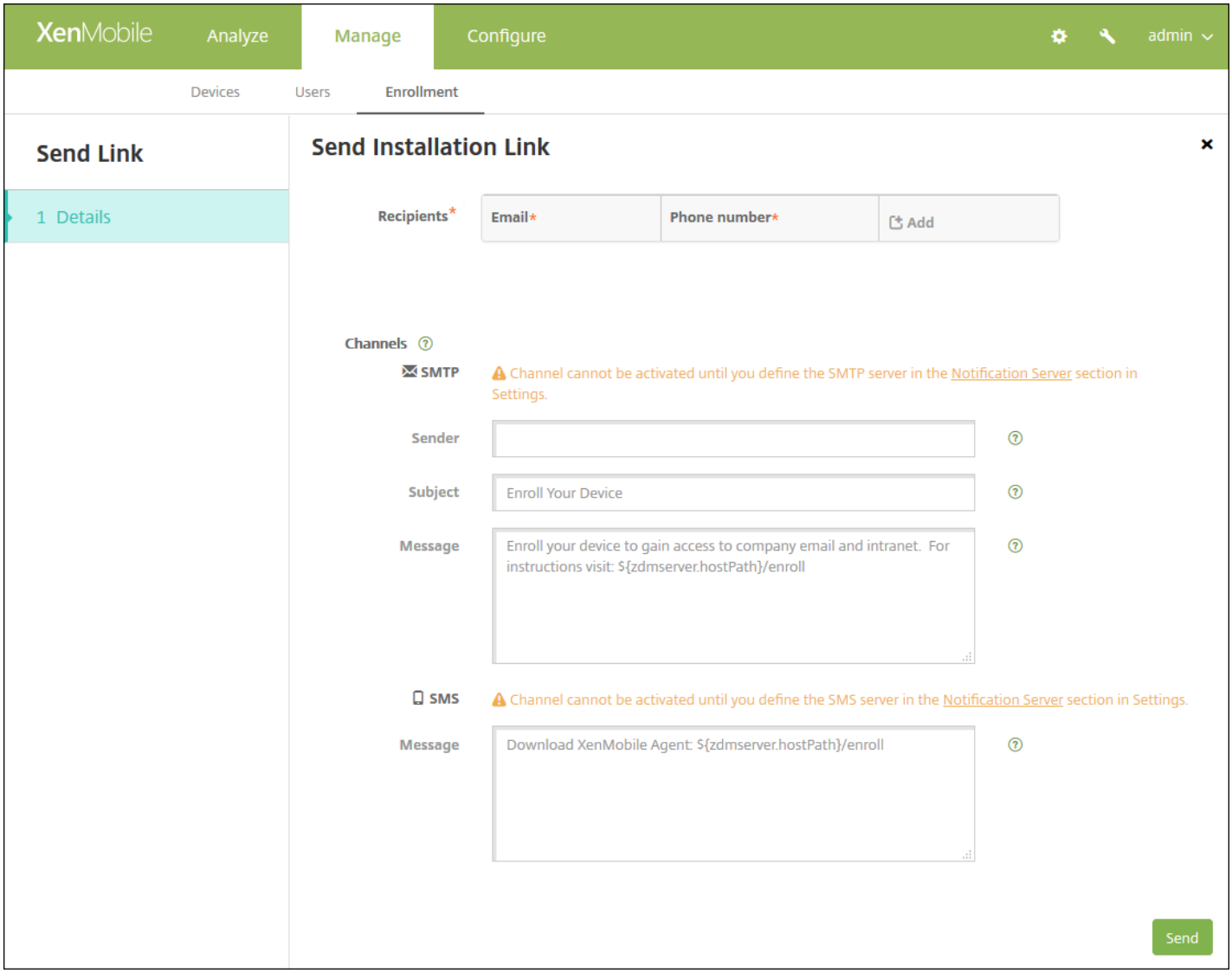
- **Gruppe**: Klicken Sie in der Liste auf die Gruppe, die die Einladung erhalten soll.
- **Registrierungsmodus**: Klicken Sie in der Liste auf die gewünschte Registrierungsmethode. Der Standard ist **Benutzername Kennwort**. Mögliche Optionen:
  - Hohe Sicherheit
  - Einladungs-URL
  - Einladungs-URL + PIN
  - Einladungs-URL + Kennwort
  - Zweifaktor
  - Benutzername + PIN

  Hinweis: Wenn Sie einen Registrierungsmodus mit PIN auswählen, wird das Feld **Vorlage für Registrierungs-PIN** eingeblendet, in dem Sie auf **Registrierungs-PIN** klicken.

- **Vorlage für Agentdownload**: Klicken Sie in der Liste auf die Vorlage, die für die Registrierungseinladung verwendet werden soll. Die angebotenen Optionen hängen vom Plattformtyp ab. Beispielsweise wird **iOS Download Link** angezeigt, wenn Sie als Plattform **iOS** ausgewählt haben.
- **Vorlage für Registrierungs-URL**: Klicken Sie in der Liste auf **Registrierungseinladung**.
- **Vorlage für Registrierungsbestätigung**: Klicken Sie in der Liste auf **Registrierungsbestätigung**.
- **Ablauf nach**: Dieses Feld wird ausgefüllt, wenn Sie den Registrierungsmodus konfigurieren, es gibt an, wann die Registrierung abläuft. Weitere Informationen zum Konfigurieren von Registrierungsmodi finden Sie unter Konfigurieren von Registrierungsmodi.
- **Versuche maximal**: Dieses Feld wird ausgefüllt, wenn Sie den Registrierungsmodus konfigurieren, es gibt die maximale Anzahl Registrierungsversuche an. Weitere Informationen zum Konfigurieren von Registrierungsmodi finden Sie unter Konfigurieren von Registrierungsmodi.
- **Einladung senden**: Wählen Sie **Ein**, wenn die Einladung sofort gesendet werden soll, oder **Aus**, wenn lediglich die Einladung in die Tabelle auf der Seite **Registrierung** eingefügt werden soll.

2. Klicken Sie auf **Speichern und senden**, wenn Sie **Einladung senden** ausgewählt haben, andernfalls klicken Sie auf **Speichern**. Die Einladung wird in der Tabelle auf der Seite **Registrierung** aufgeführt.

Senden von Installationslinks



Zum Senden von Installationslinks für die Registrierung müssen Sie Kanäle (SMTP oder SMS) auf dem Benachrichtigungsserver über die Seite **Einstellungen** konfigurieren. Details finden Sie unter Benachrichtigungen.

1. Konfigurieren Sie die folgenden Einstellungen:

- **Empfänger**: Für jeden Empfänger, den Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **E-Mail**: Geben Sie die E-Mail-Adresse des Empfängers ein. Diese Angabe ist erforderlich.
  - **Telefonnummer**: Geben Sie die Telefonnummer des Empfängers ein. Diese Angabe ist erforderlich.
  - Klicken Sie auf **Speichern**.

    Hinweis: Zum Löschen eines vorhandenen Empfängers zeigen Sie auf dessen Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, um ihn beizubehalten.

    Zum Bearbeiten eines Empfängers 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

- **Kanäle**: Wählen Sie den Kanal zum Senden des Installationslinks aus. Sie können Benachrichtigungen über SMTP oder SMS senden. Diese Kanäle werden erst aktiviert, wenn Sie die Servereinstellungen unter **Benachrichtigungsserver** auf der Seite **Einstellungen** konfiguriert haben. Details finden Sie unter Benachrichtigungen.
  - **SMTP**: Konfigurieren Sie folgende optionalen Einstellungen. Wenn Sie diese Felder nicht ausfüllen, werden die Standardwerte der Benachrichtigungsvorlage für die ausgewählte Plattform verwendet:
    - **Absender**: Geben Sie optional einen Absender ein.
    - **Betreff**: Geben Sie optional einen Betreff für die Benachrichtigung ein. Beispiel: "Registrieren Sie Ihr Gerät".
    - **Nachricht**: Geben Sie optional eine Nachricht ein, die an Empfänger gesendet werden soll. Beispiel: "Registrieren Sie Ihr Gerät für den Zugriff auf Unternehmens-Apps und -E-Mail".
  - **SMS**: Konfigurieren Sie diese Einstellung. Wenn Sie dieses Feld nicht ausfüllen, wird der Standardwert der Benachrichtigungsvorlage für die ausgewählte Plattform verwendet:
    - **Nachricht**: Geben Sie eine Nachricht ein, die an Empfänger gesendet werden soll. Dieses Feld ist für die Benachrichtigung per SMS erforderlich.

      Hinweis: In Nordamerika werden SMS-Nachrichten mit mehr als 160 Zeichen in mehrere Nachrichten aufgeteilt.

2. Klicken Sie auf **Senden**.

Hinweis

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

Gemeinsam genutzte Geräte in XenMobile

Jul 28, 2016

XenMobile ermöglicht die Konfiguration von Geräten, die von mehreren Benutzern verwendet werden. Ärzte in Krankenhäusern können so beispielsweise das jeweils nächstgelegene Gerät für den Zugriff auf Apps und Daten nutzen, anstatt ein bestimmtes Gerät mit sich herumtragen zu müssen. Die gemeinsame Gerätenutzung kann auch für Personal im Außendienst eingeführt werden, um Ausrüstungskosten zu senken.

Wichtige Hinweise zur gemeinsamen Gerätenutzung

MDM-Modus

- Auf iOS- und Android-Tablets und -Telefonen verfügbar. Die einfache Registrierung per Device Enrollment Program (DEP) wird für gemeinsam genutzte Geräte unter XenMobile Enterprise nicht unterstützt. In diesem Modus ist für gemeinsam genutzte Geräte ein autorisiertes DEP erforderlich.
- Clientzertifikatauthentifizierung, Worx-PIN, Touch ID und Benutzerentropie werden nicht unterstützt.

MDM+MAM-Modus

- Nur auf iOS- und Android-Tablets verfügbar.
- Wird nur auf XenMobile 10.3.x-Server und -Client unterstützt.
- Der MAM-Only-Modus wird nicht unterstützt. Die Geräte müssen in MDM registriert werden.
- Nur WorxMail, WorxWeb, und die mobile ShareFile-App (Version 4.4) werden unterstützt. HDX-Apps werden nicht unterstützt.
- Es werden nur Active Directory-Benutzer unterstützt, keine lokalen Benutzer und Gruppen.
- Eine erneute Registrierung vorhandener und nur per MDM verwalteter gemeinsam genutzter Geräte ist erforderlich, um ein Update auf den MDM+MAM-Modus durchzuführen
- Benutzer können nur Worx-Apps und mit MDX umschlossene Apps gemeinsam nutzen. Native Apps können nicht gemeinsam genutzt werden.
- Nach dem Download während der Erstregistrierung werden Worx Apps nicht jedes Mal neu heruntergeladen, wenn sich ein neuer Benutzer am Gerät anmeldet. Ein neuer Benutzer kann sich einfach am Gerät anmelden und loslegen.
- Damit Sie unter Android die Daten der einzelnen Benutzer für Sicherheitszwecke isolieren können, muss die Richtlinie für die Unzulässigkeit von Geräten mit Rooting in der XenMobile-Konsole auf **Ein** festgelegt sein.

Voraussetzungen für die Registrierung gemeinsam genutzter Geräte

Vor dem Registrieren gemeinsam genutzter Geräte müssen Sie die folgenden Schritte ausführen:

- Benutzerrolle für gemeinsam genutzte Geräte erstellen: siehe Konfigurieren von Rollen mit RBAC
- Benutzer für gemeinsam genutzte Geräte erstellen: siehe Erstellen, Bearbeiten und Löschen lokaler Benutzer in XenMobile
- Bereitstellungsgruppe mit Basisrichtlinien, Apps und Aktionen erstellen, die auf den Benutzer für die Registrierung

gemeinsam genutzter Geräte angewendet werden sollen: siehe Verwalten von Bereitstellungsgruppen

Voraussetzungen für MDM+MAM-Modus

1. Erstellen Sie eine Active Directory-Gruppe mit einem aussagekräftigen Namen. In diesem Beispiel wird **Shared Device Enrollers** verwendet.
2. Fügen Sie der Gruppe Active Directory-Benutzer hinzu, die gemeinsam genutzte Geräte registrieren. Wenn Sie für diesen Zweck ein neues Konto verwenden möchten, erstellen Sie einen neuen Active Directory-Benutzer (z. B. **sdenroll**) und fügen Sie den Benutzer der Active Directory-Gruppe hinzu.

Anforderungen für gemeinsam genutzte Geräte

Zur Gewährleistung einer optimalen Benutzererfahrung, einschließlich automatischer Installation und Deinstallation von Apps, empfiehlt Citrix, gemeinsam genutzte Geräte auf den folgenden Plattformen zu konfigurieren:

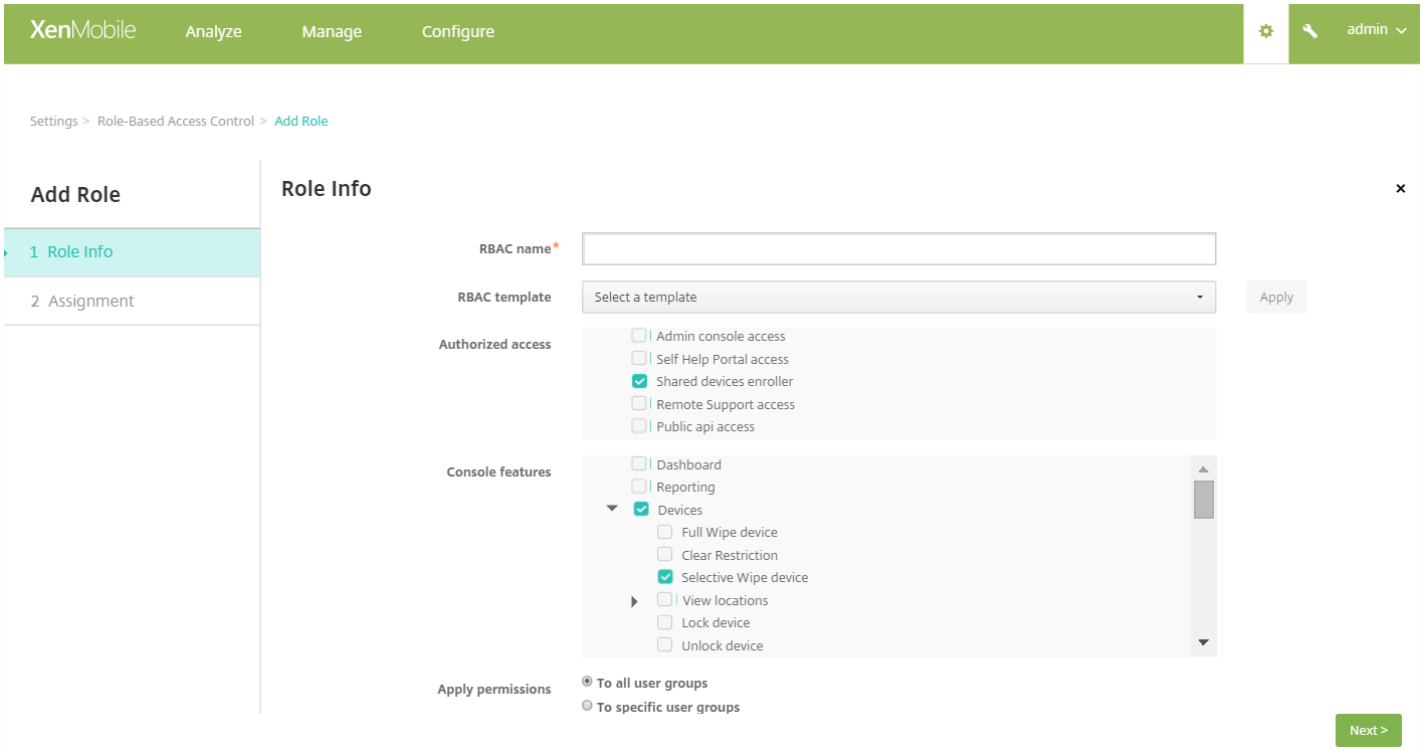
- iOS 9
- iOS 8
- Android M
- Android 5.x
- Android 4.4.x
- Android 4.0.x (ausschließlicher MDM-Modus)

Konfigurieren eines gemeinsam genutzten Geräts

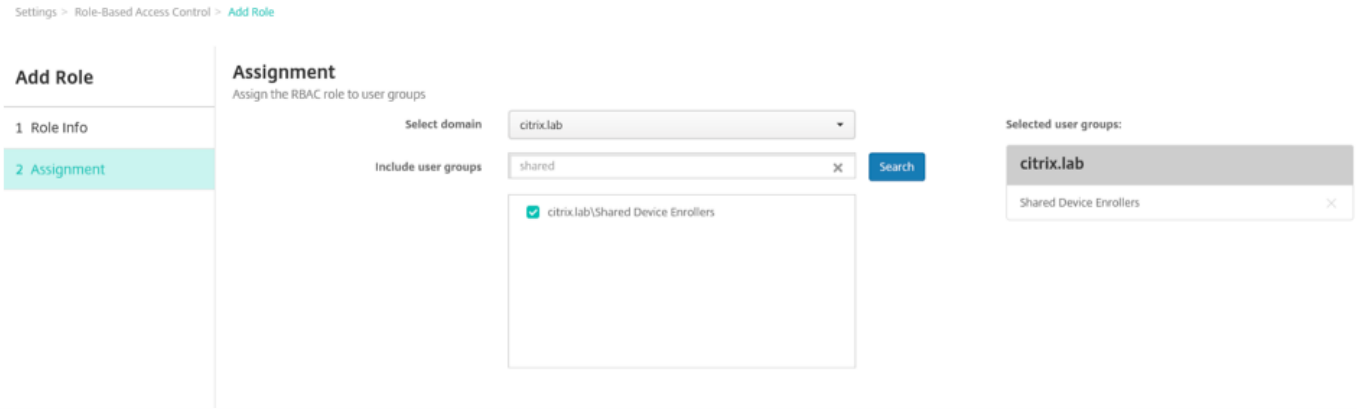
Mit den folgenden Schritten konfigurieren Sie ein gemeinsam genutztes Gerät.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite "Einstellungen" wird angezeigt.
2. Klicken Sie auf **Rollenbasierte Zugriffssteuerung** und dann auf **Hinzufügen**. Der Bildschirm **Rolle hinzufügen** wird angezeigt.
3. Erstellen Sie eine Benutzerrolle für die Registrierung gemeinsam genutzter Geräte namens **Registrierungsbenutzer für gemeinsam genutzte Geräte** mit den Berechtigungen **Registrierung für gemeinsam genutzte Geräte** unter **Autorisierter Zugriff**. Erweitern Sie **Geräte** unter **Konsolenfeatures** und wählen Sie **Gerät selektiv löschen** aus. Mit dieser Einstellung wird sichergestellt, dass die über das Konto "Registrierungsbenutzer für gemeinsam genutzte Geräte" bereitgestellten Apps und Richtlinien von Worx Home gelöscht werden, wenn die Registrierung des Geräts aufgehoben wird.

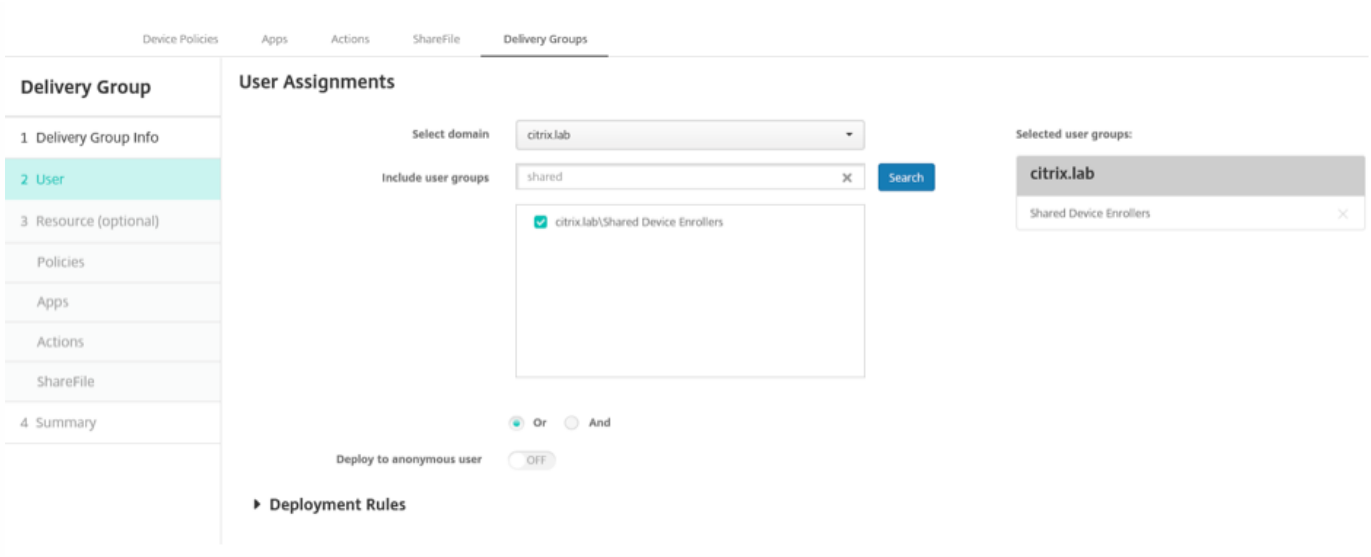
   Behalten Sie die Standardeinstellung **Auf alle Benutzergruppen** für **Berechtigungen anwenden** bei oder weisen Sie bestimmten Active Directory-Benutzergruppen Berechtigungen mit der Option **Auf bestimmte Benutzergruppen** zu.



Klicken Sie auf **Weiter**, um den Bildschirm **Zuweisung** anzuzeigen. Weisen Sie die Registrierungsrolle für gemeinsam genutzte Geräte, die Sie gerade erstellt haben, der Active Directory-Gruppe zu, die Sie für Registrierungsbenutzer für gemeinsam genutzte Geräte in Schritt 1 unter "Voraussetzungen" erstellt haben. In der Abbildung unten ist **citrix.lab** die Active Directory-Domäne und **Shared Device Enrollers** ist die Active Directory-Gruppe.



4. Erstellen Sie eine Bereitstellungsgruppe mit den grundlegenden Richtlinien, Apps und Aktionen, die für das Gerät gelten sollen, wenn kein Benutzer angemeldet ist, und weisen Sie die Bereitstellungsgruppe der Active Directory-Gruppe für die Registrierung des gemeinsam genutzten Geräts zu.



5. Installieren Sie Worx Home auf dem gemeinsam genutzten Gerät und registrieren Sie es in XenMobile mit dem Benutzerkonto für die Registrierung des gemeinsam genutzten Geräts. Sie können das Gerät nun über die XenMobile-Konsole anzeigen und verwalten. Weitere Informationen finden Sie unter Registrieren von Geräten.

6. Zum Anwenden unterschiedlicher Richtlinien oder zum Bereitstellen zusätzlicher Apps für authentifizierte Benutzer müssen Sie eine diesen Benutzern zugewiesene Bereitstellungsgruppe erstellen und sie nur auf gemeinsam genutzten Geräten bereitstellen. Konfigurieren Sie beim Erstellen der Bereitstellungsgruppen Bereitstellungsregeln, um sicherzustellen, dass sie für gemeinsam genutzte Geräte bereitgestellt werden. Weitere Informationen finden Sie unter Konfigurieren von Bereitstellungsregeln.

7. Zum Beenden der gemeinsamen Gerätenutzung führen Sie einen selektiven Löschvorgang durch, um das Benutzerkonto für die Registrierung des gemeinsam genutzten Geräts zusammen mit jeglichen bereitgestellten Apps und Richtlinien von dem Gerät zu löschen.

Benutzererfahrung bei gemeinsam genutzten Geräten

MDM-Modus

Jedem Benutzer werden nur die ihm verfügbaren Ressourcen angezeigt und seine Benutzererfahrung ist auf jedem gemeinsam genutzten Gerät gleich. Die Richtlinien und Apps für gemeinsam genutzte Geräte bleiben immer auf dem Gerät. Wenn ein Benutzer, der nicht für gemeinsam genutzte Geräte registriert ist, sich an Worx Home anmeldet, werden die Richtlinien und Apps dieser Person auf dem Gerät bereitgestellt. Wenn sich der Benutzer abmeldet, werden die Richtlinien und Apps entfernt, die sich von denen unterscheiden, die bei der Registrierung als gemeinsam genutztes Gerät bereitgestellt werden, während die Ressourcen des gemeinsam genutzten Geräts intakt bleiben.

MDM+MAM-Modus

WorxMail und WorxWeb werden auf dem Gerät bereitgestellt, wenn der Registrierungsbenutzer des gemeinsam genutzten Geräts es registriert. Die Benutzerdaten werden sicher auf dem Gerät gespeichert. Die Daten werden keinem anderen Benutzer offengelegt, wenn dieser sich an WorxMail oder WorxWeb anmeldet.

Nur jeweils ein Benutzer kann sich bei Worx Home anmelden. Der vorherige Benutzer muss sich abmelden, bevor der nächste

Benutzer sich anmelden kann. Aus Sicherheitsgründen speichert Worx Home keine Anmeldeinformationen auf gemeinsam genutzten Geräten, sodass Benutzer ihre Anmeldeinformationen bei jeder Anmeldung eingeben müssen. Damit ein neuer Benutzer nicht auf die Ressourcen des vorherigen zugreifen kann, lässt Worx Home nicht zu, dass neue Benutzer sich während des Entfernens von Richtlinien, Apps und Daten des vorherigen Benutzers anmelden.

Der Upgradevorgang für Apps ändert sich bei gemeinsam genutzten Geräten nicht. Sie können Upgrades wie gewohnt Benutzern gemeinsam genutzter Geräte per Push bereitstellen und Benutzer können Upgrades von Apps direkt auf ihren Geräten durchführen.

Empfohlene WorxMail-Richtlinien

- Für die optimale Leistung von WorxMail legen Sie denmaximalen Synchronisierungszeitraum basierend auf der Anzahl der Benutzer fest, die das Gerät gemeinsam verwenden. Das Zulassen unbegrenzter Synchronisierungen wird nicht empfohlen.

Anzahl Benutzer, die Gerät gemeinsam verwenden	**Empfohlener maximaler Synchronisierungszeitraum**
21 bis 25	1 Woche oder weniger
6 bis 20	2 Wochen oder weniger
5 oder weniger	1 Monat oder weniger

- Blockieren Sie das Exportieren von Kontakten, damit Benutzer, die das Gerät gemeinsam verwenden, nicht auf die Kontakte der anderen Benutzer zugreifen können.

- Auf iOS können nur die folgenden Einstellungen pro Benutzer festgelegt werden. Alle anderen Einstellungen gelten für alle Benutzer, die das Gerät gemeinsam verwenden:

  Benachrichtigungen
  Signatur
  Abwesend
  E-Mail-Synchronisierungszeitraum
  S/MIME
  Rechtschreibprüfung

Verwalten von Geräten mit Android for Work in XenMobile

Oct 13, 2016

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

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

Sie verwenden Google Play for Work zum Hinzufügen, Erwerben und Genehmigen von Apps für die Bereitstellung in dem Android for Work-Arbeitsbereich von Geräten. Über Google Play for Work können Sie private Android-Apps sowie öffentliche Apps und solche von Drittanbietern bereitstellen. Wenn Sie XenMobile einen kostenpflichtigen öffentlichen App-Store für Android for Work hinzufügen, können Sie den Lizenzierungsstatus für Massenkäufe überprüfen: die Gesamtanzahl verfügbarer Lizenzen, die derzeit verwendeten Lizenzen und die E-Mail-Adressen der Benutzer, die eine Lizenz verwenden. Einzelheiten finden Sie unter Hinzufügen einer App aus einem öffentlichen App-Store zu XenMobile.

Anforderungen für Android for Work:

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

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

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

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

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

Voraussetzungen für Android for Work

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

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

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

> **Warnung**
>
> Ein bekanntes Drittanbieterproblem ist, dass Sie über die XenMobile-Konsole Android for Work nicht aktivieren können. Weitere Informationen zu diesem Problem und zum Konfigurieren einer Servereigenschaft als Workaround finden Sie unter Problem #615118 im Abschnitt Bekannte Probleme bei XenMobile Server 10.3.

Erstellen eines Android for Work-Kontos

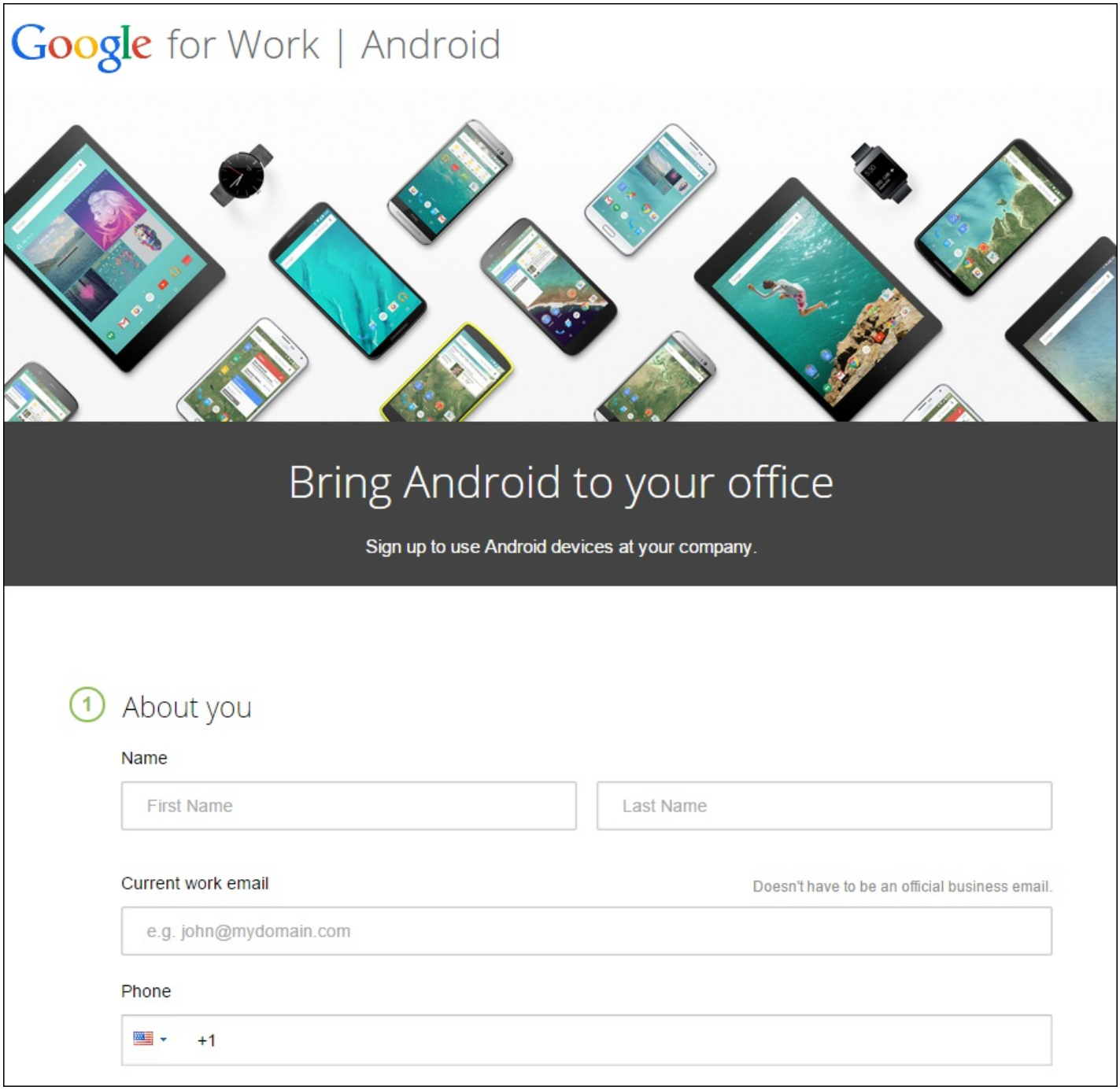
Die folgenden Voraussetzungen müssen erfüllt sein, damit Sie ein Android for Work-Konto erstellen können:

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

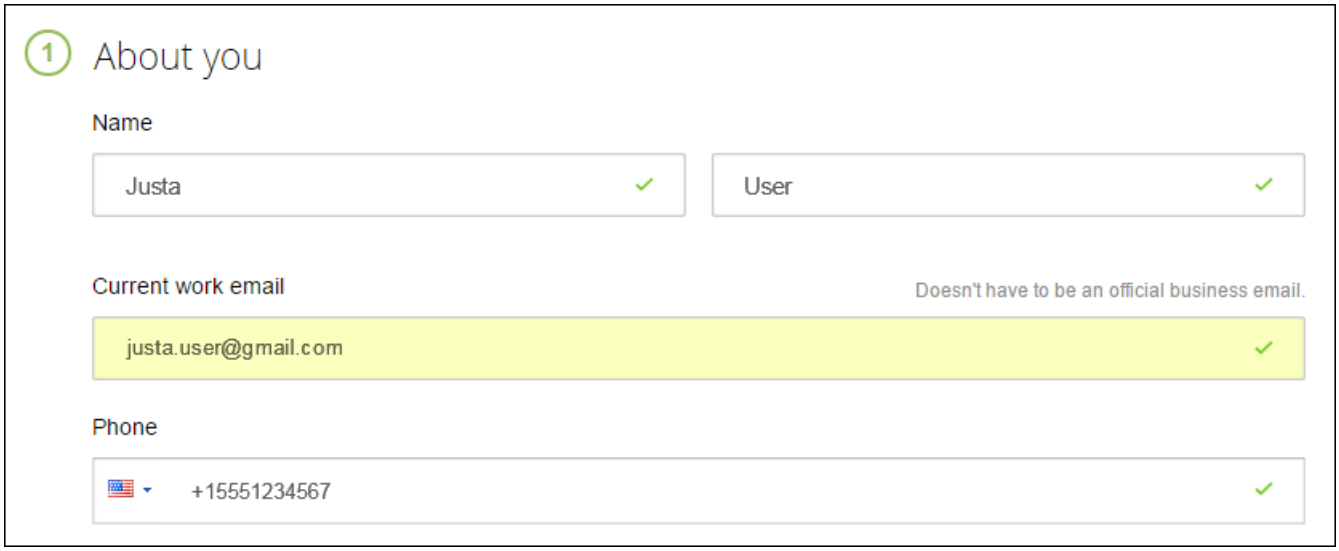
Wenn Ihr Domänenname bei Google bereits verifiziert wurde, können Sie mit dem Schritt Einrichten eines Android for Work-Dienstkontos und Download eines Android for Work-Zertifikats fortfahren.

1. Navigieren Sie zu https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

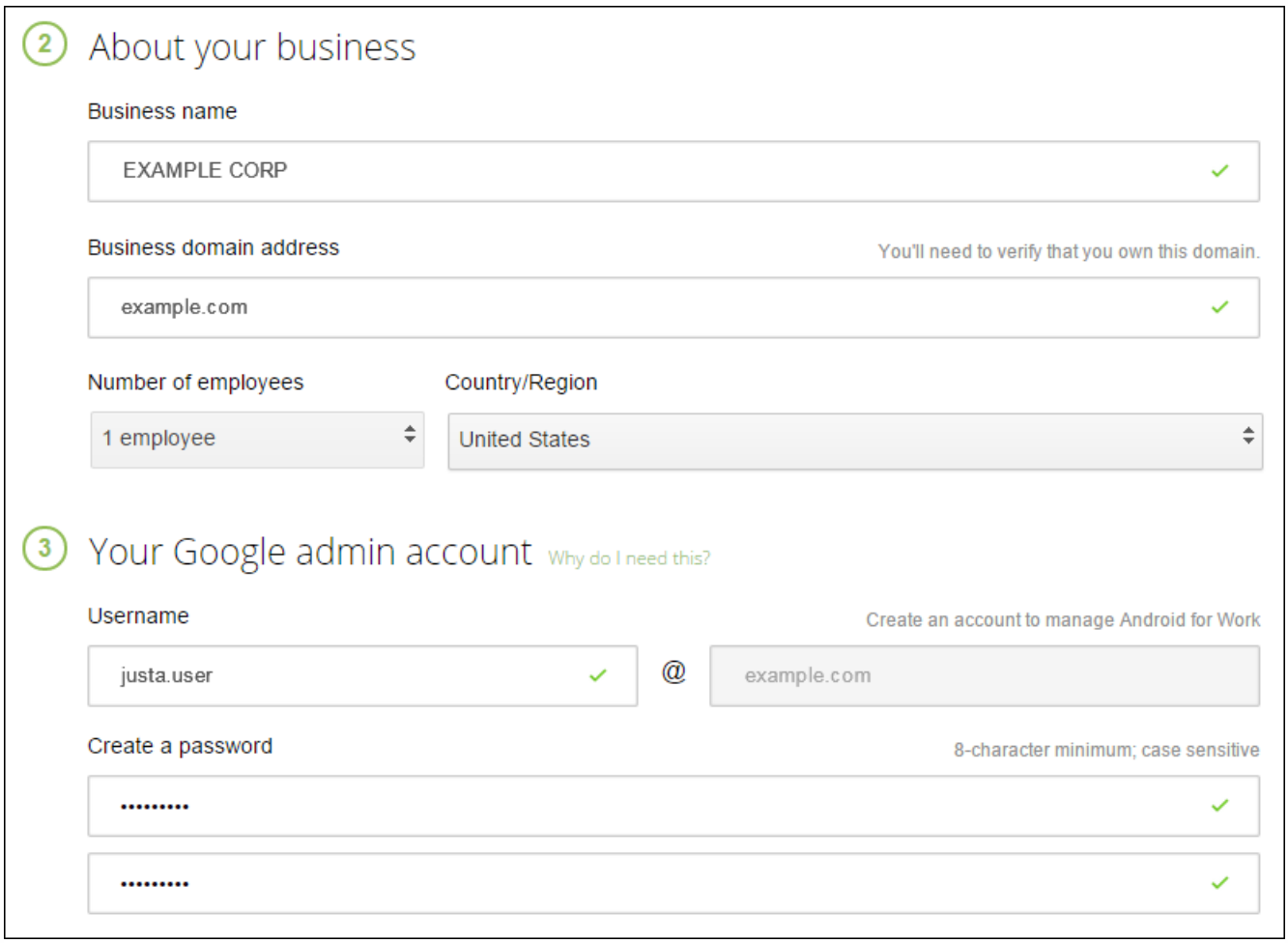
Die folgende Seite wird angezeigt, auf der Sie die Administrator- und Unternehmensinformationen eingeben müssen.



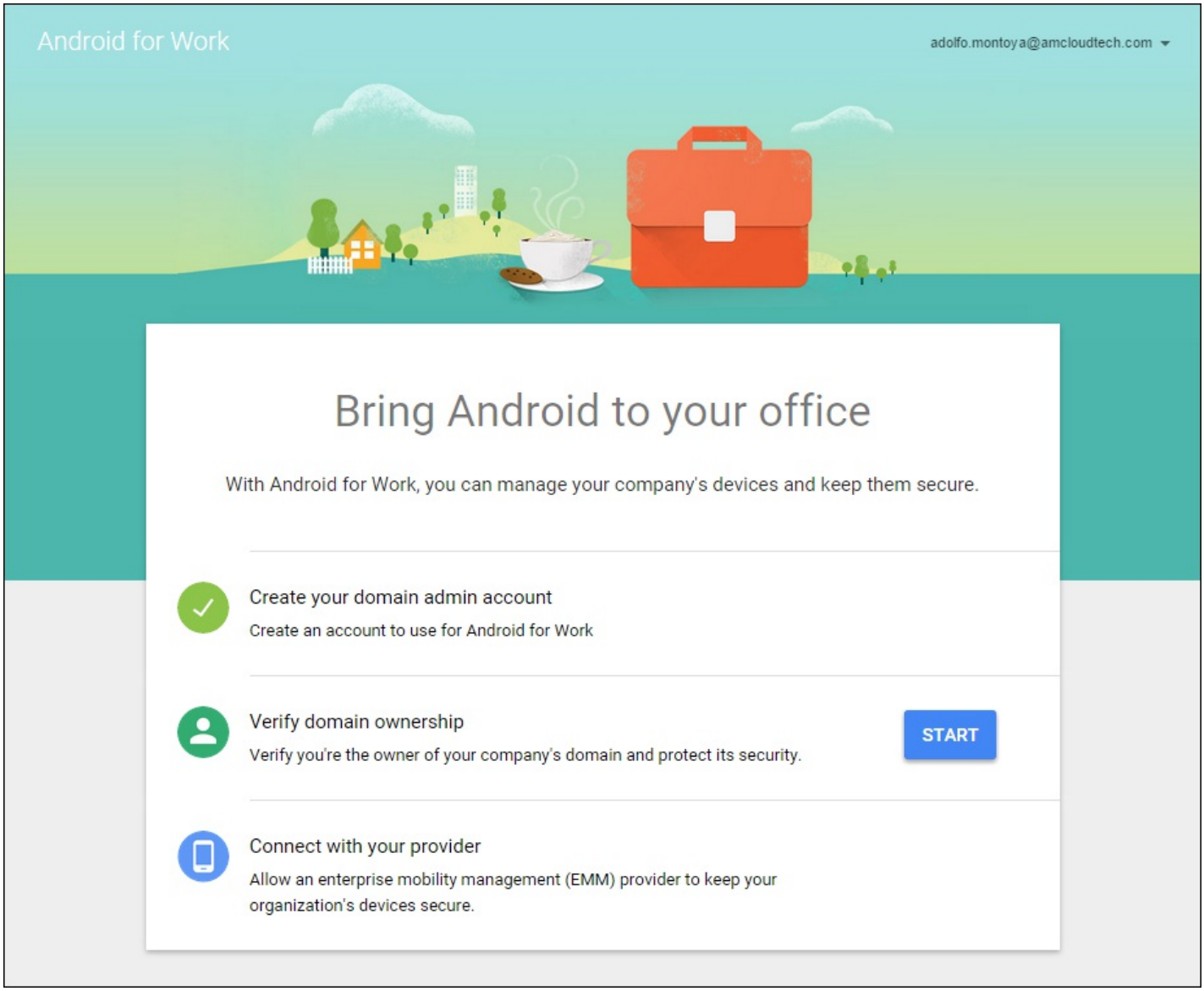
2. Geben Sie die Administratorinformationen ein.



3. Geben Sie Ihre Unternehmensinformationen sowie die Administratorkonteninformationen ein.



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

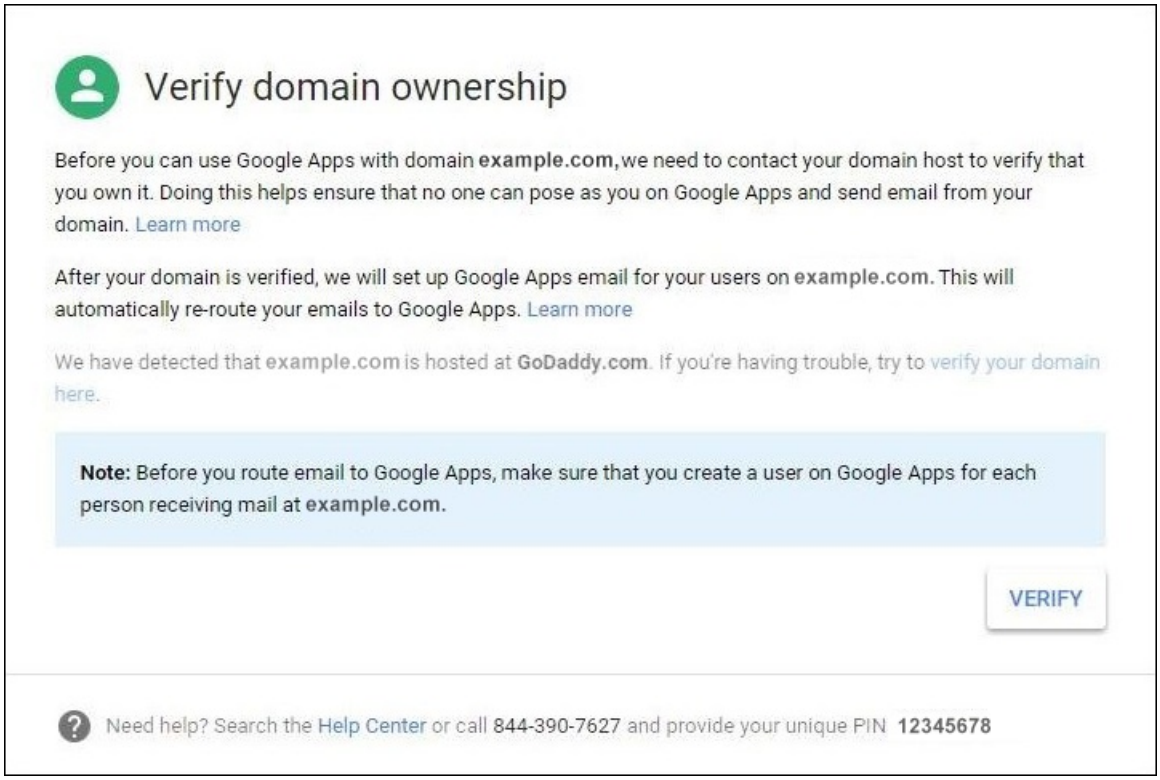


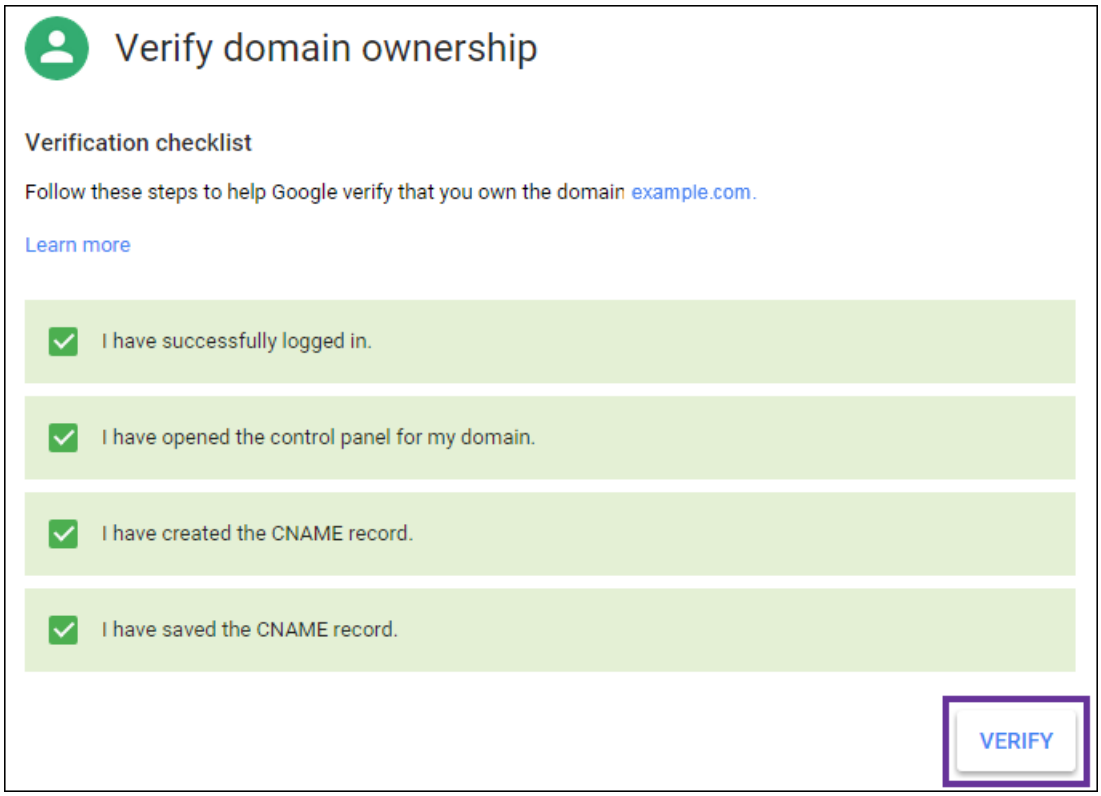
Überprüfen der Domäneneigentümerschaft

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

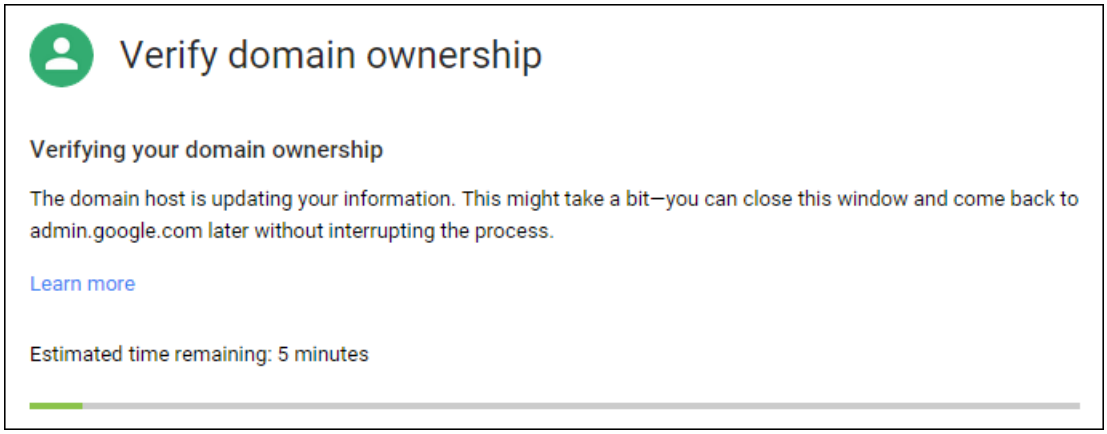
1. Klicken Sie auf **Start**, um die Domänenüberprüfung zu beginnen. Die Seite **Verify domain ownership** wird angezeigt. Folgen Sie den angezeigten Anweisungen zum Überprüfen Ihrer Domäne.

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

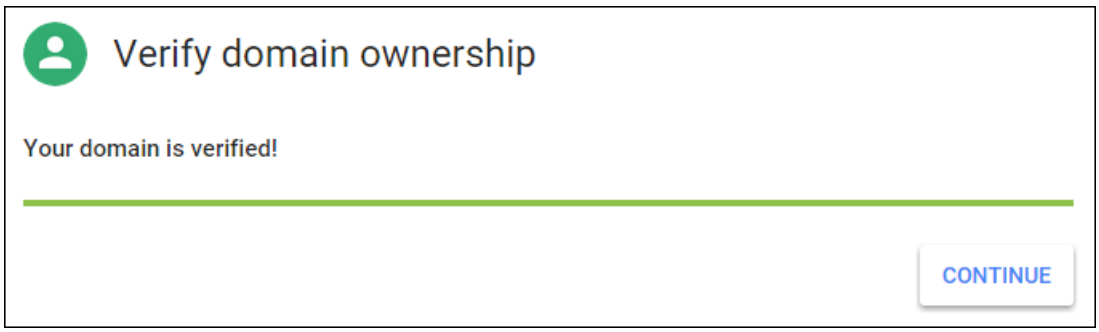




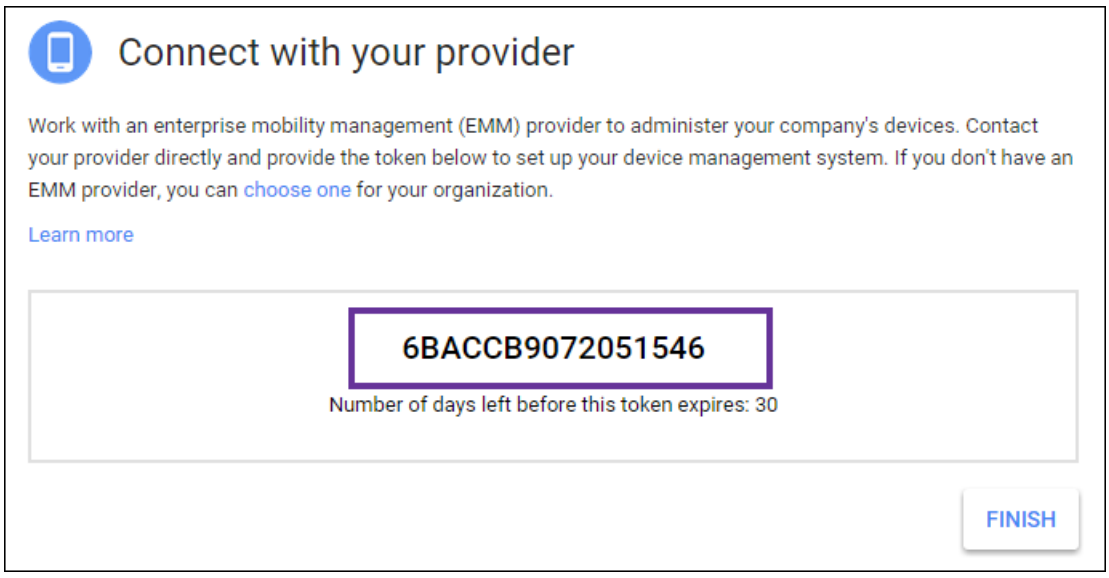
3. Google überprüft die Eigentümerschaft der Domäne.



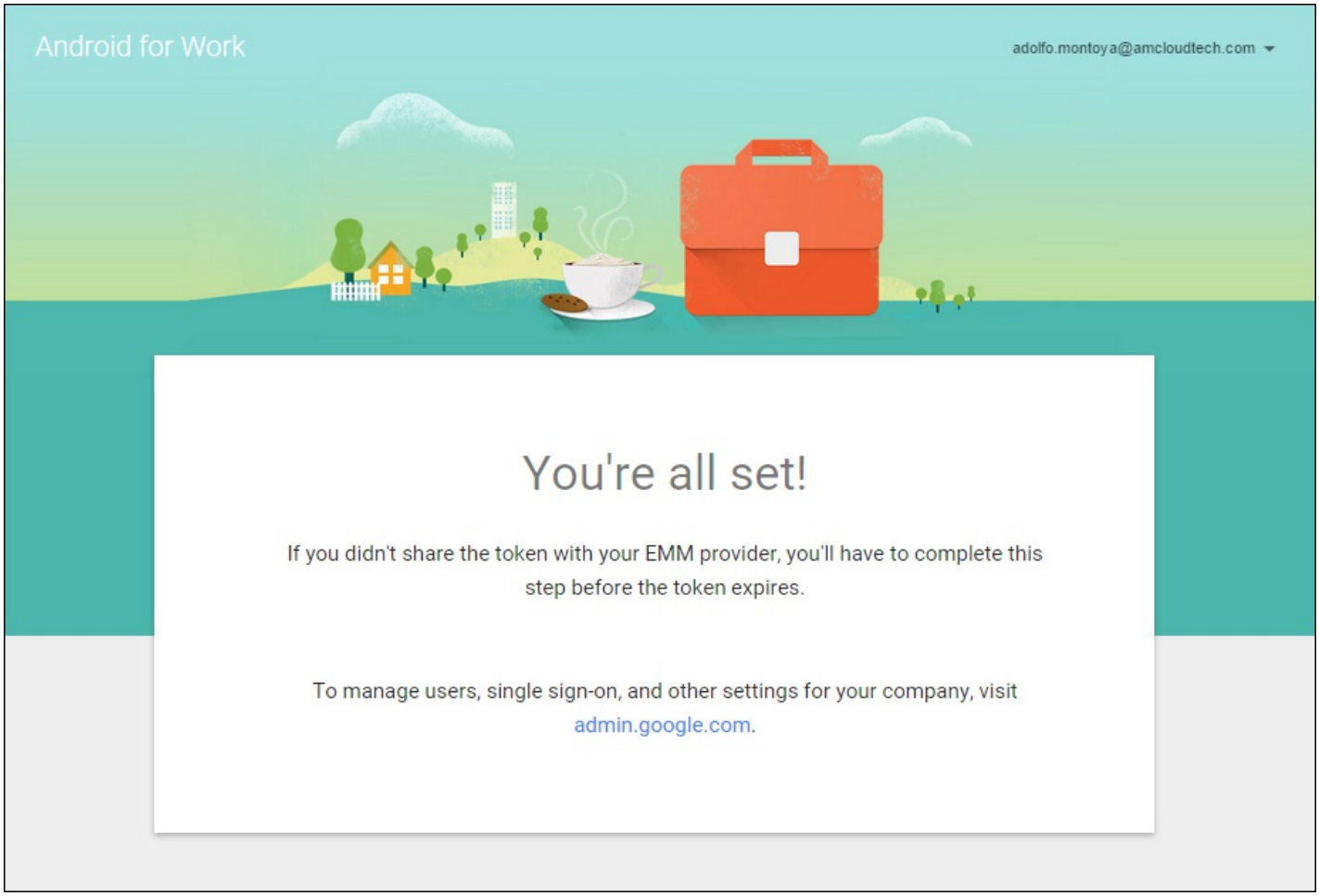
4. Nach Bestehen der Prüfung wird die folgende Seite angezeigt. Klicken Sie auf **Continue**.



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



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



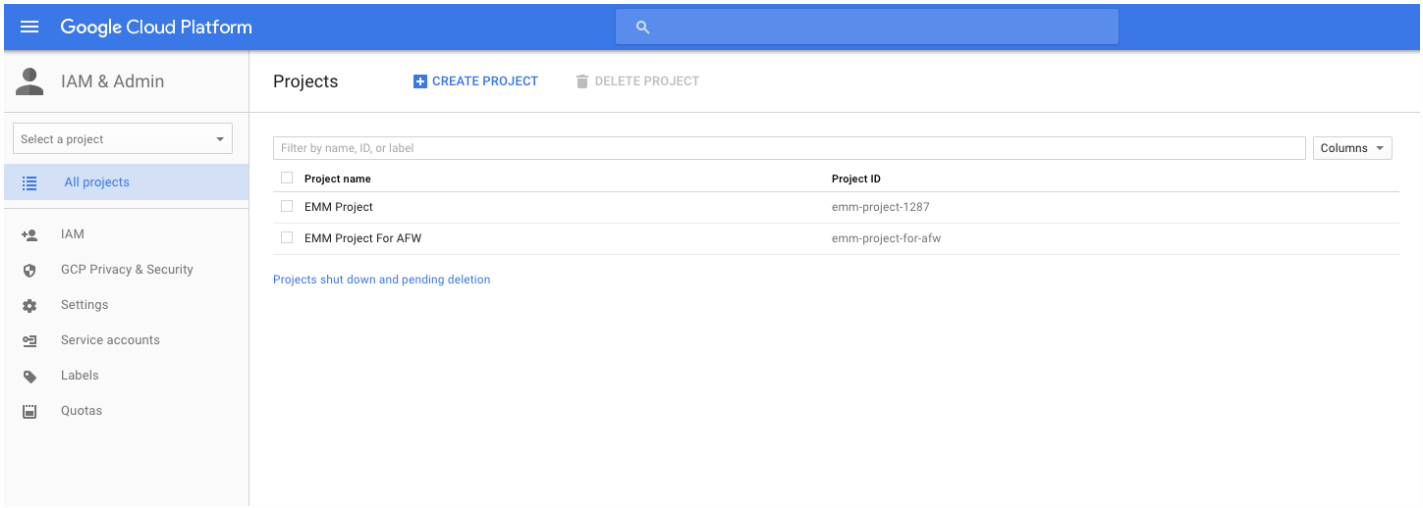
Nach dem Erstellen eines Android for Work-Dienstkontos können Sie sich bei der Google-Verwaltungskonsole zum Verwalten der Android for Work-Mobility Management-Einstellungen anmelden.

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

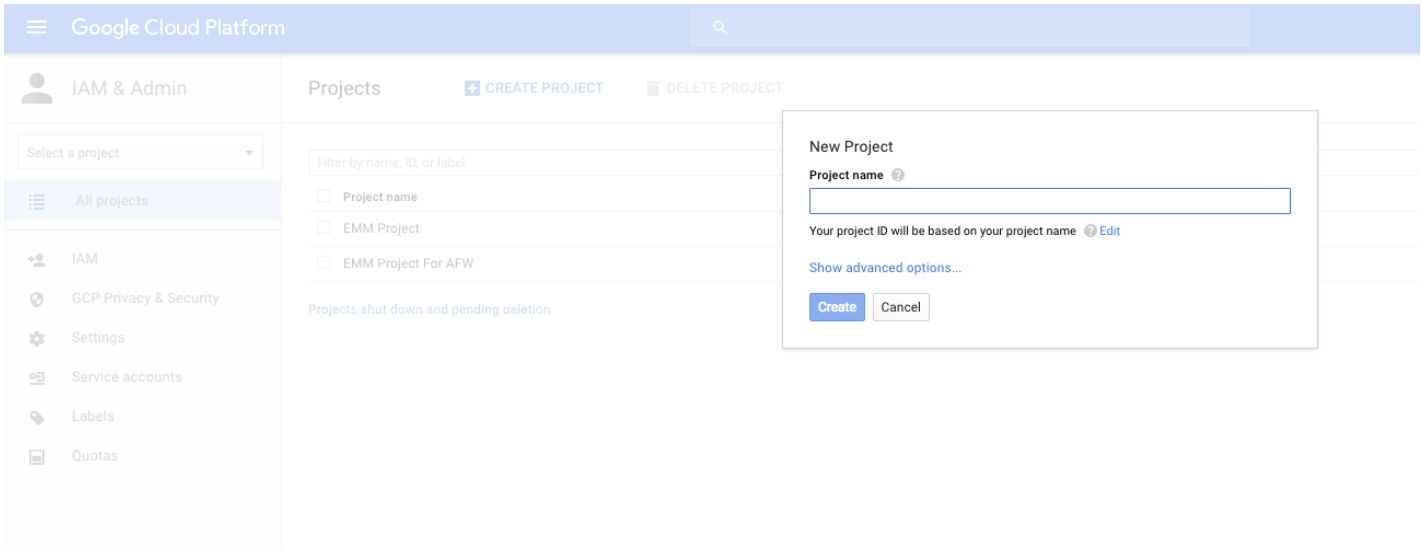
Damit XenMobile Google Play und Verzeichnisdienste kontaktieren kann, müssen Sie ein neues Dienstkonto mit dem Projektportal für Entwickler von Google erstellen. Das Dienstkonto wird für die Server-Kommunikation zwischen XenMobile und den Google-Diensten für Android for Work verwendet. Weitere Informationen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

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

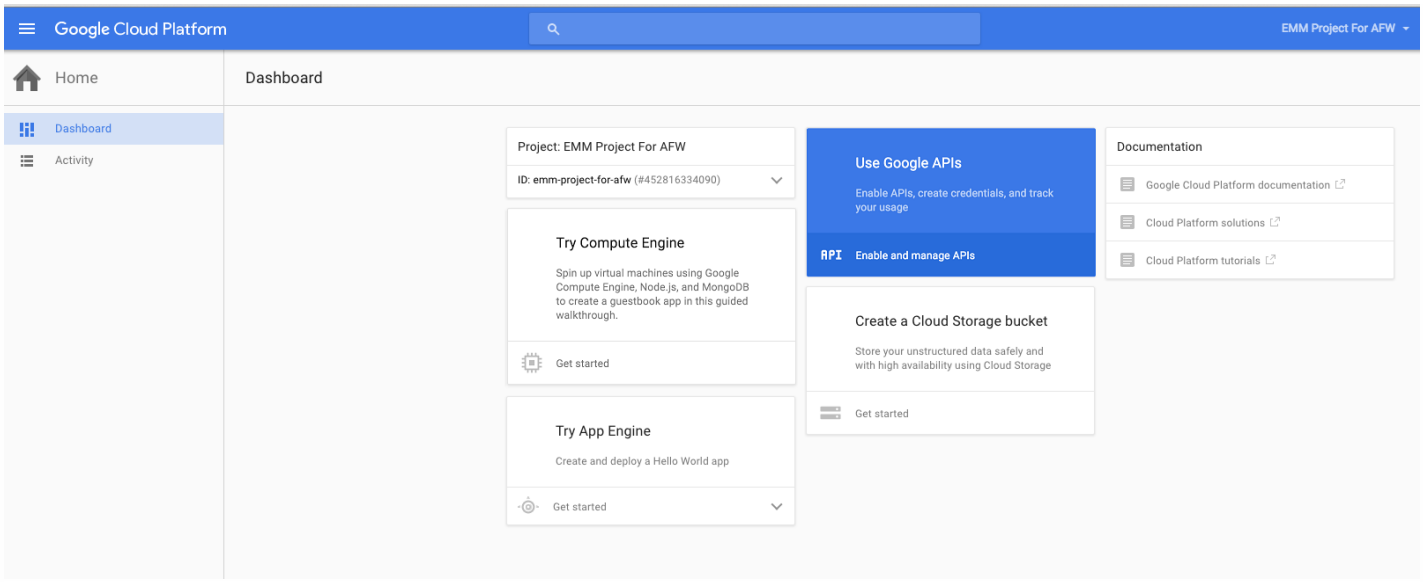
2. Klicken Sie in der Liste **Projects** auf **Create project**.



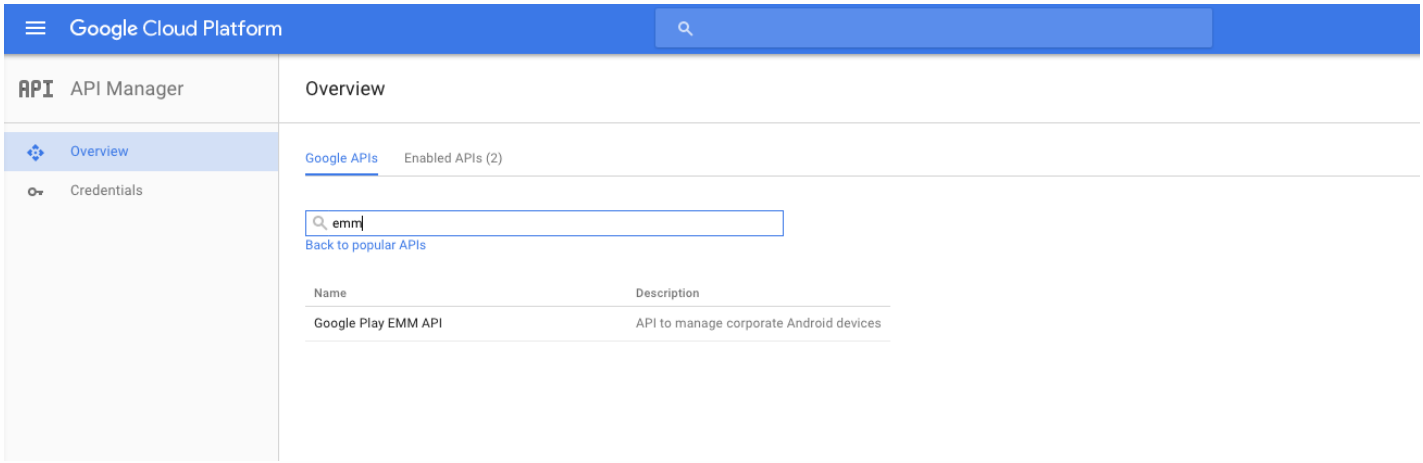
3. Geben Sie unter **Project name** einen Namen für das Projekt ein.



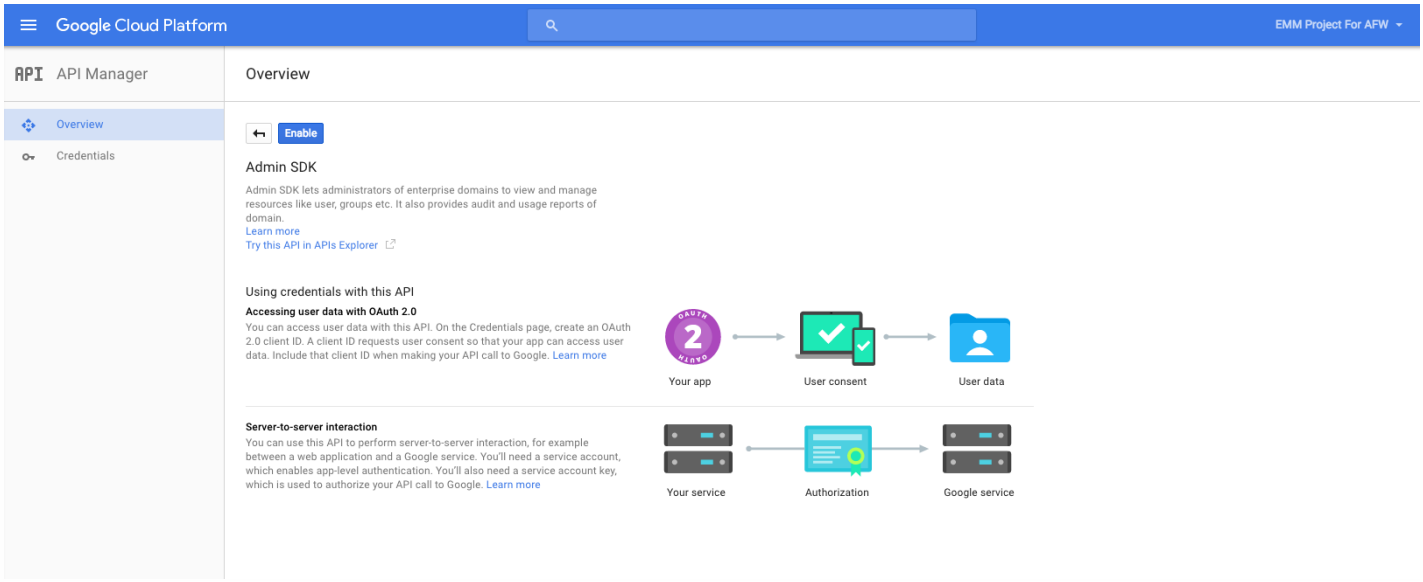
4. Klicken Sie im Dashboard auf **Use Google APIs**.



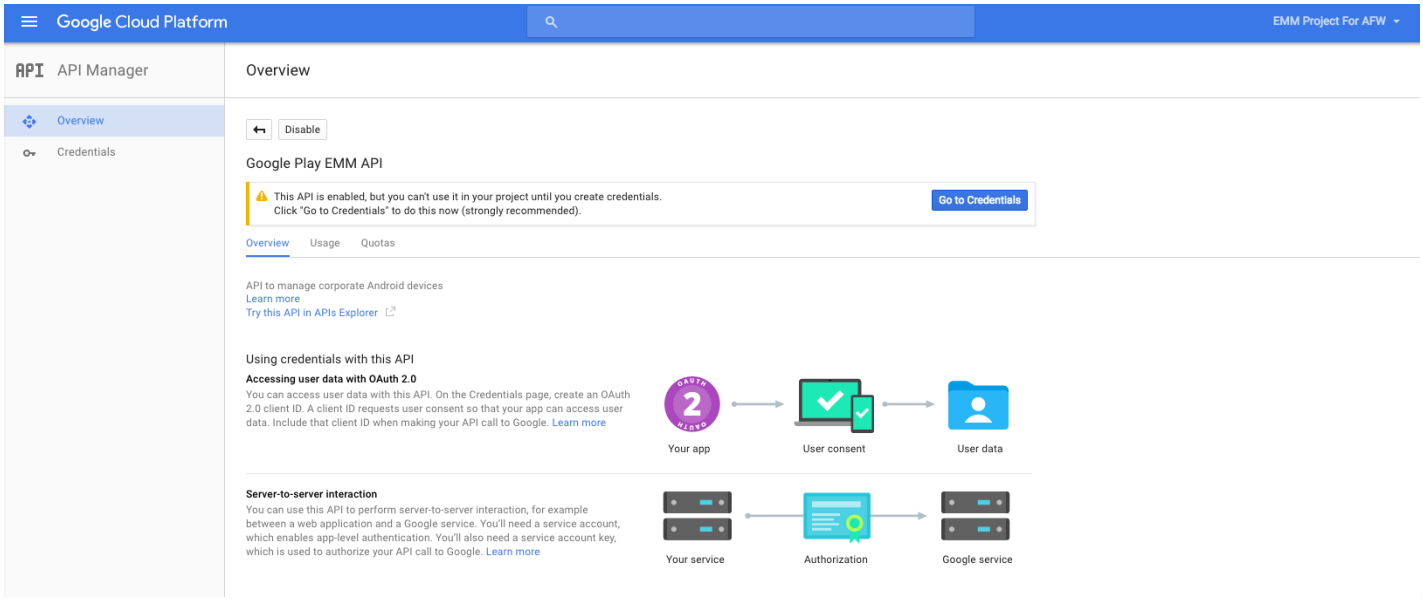
5. Geben Sie auf der Seite "Google APIs" **EMM** im Feld **Search** ein und klicken Sie dann auf das Suchergebnis.



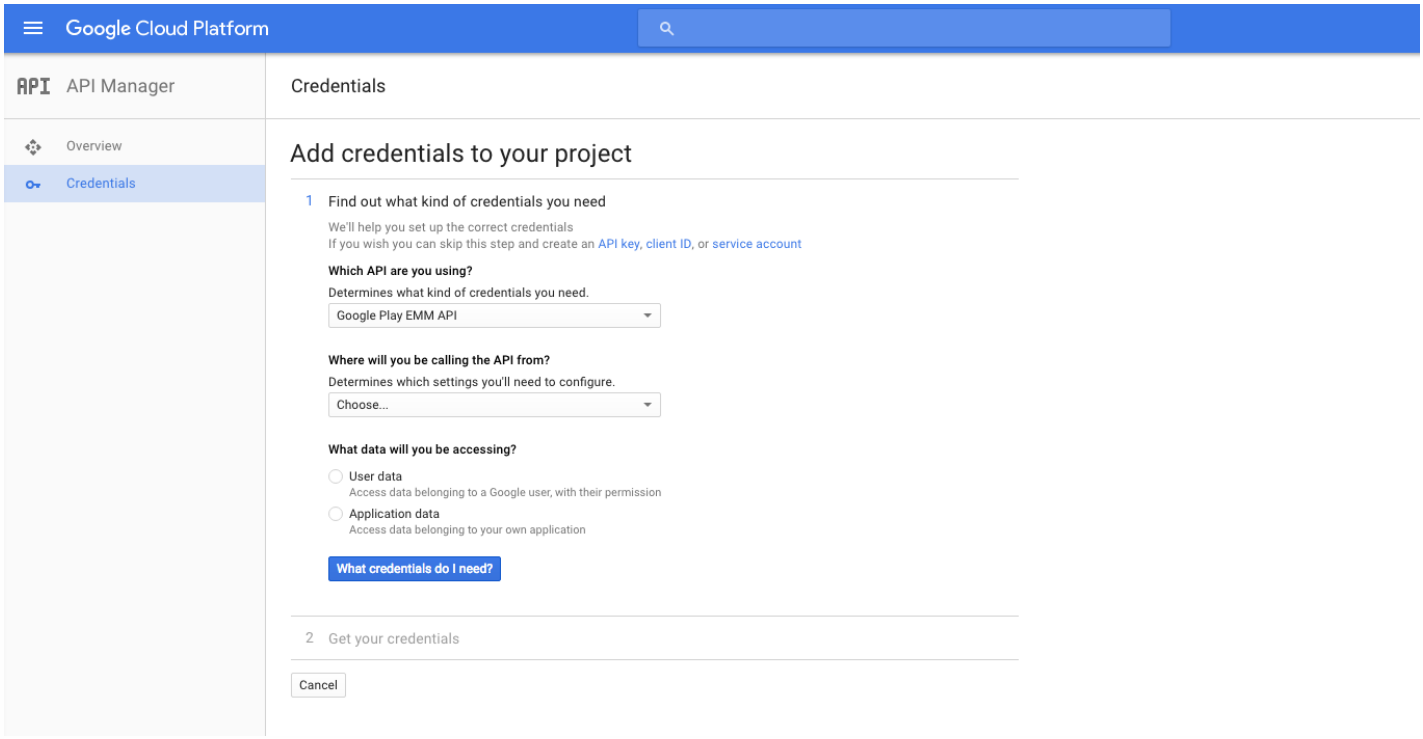
6. Klicken Sie auf der Seite "Overview" auf **Enable**.



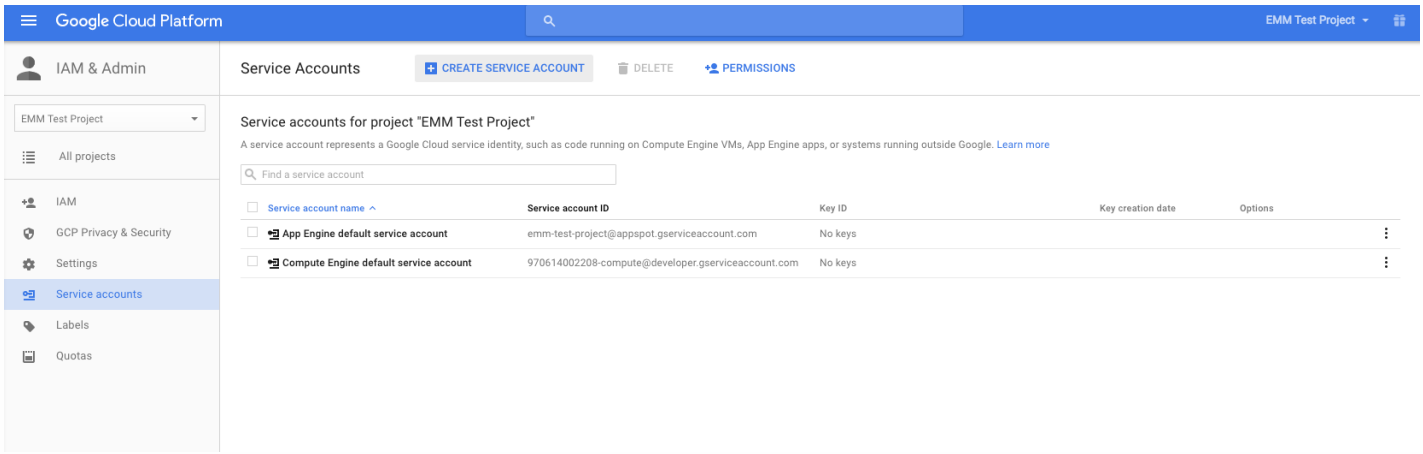
7. Klicken Sie neben **Google Play EMM API** auf **Go to Credentials**.



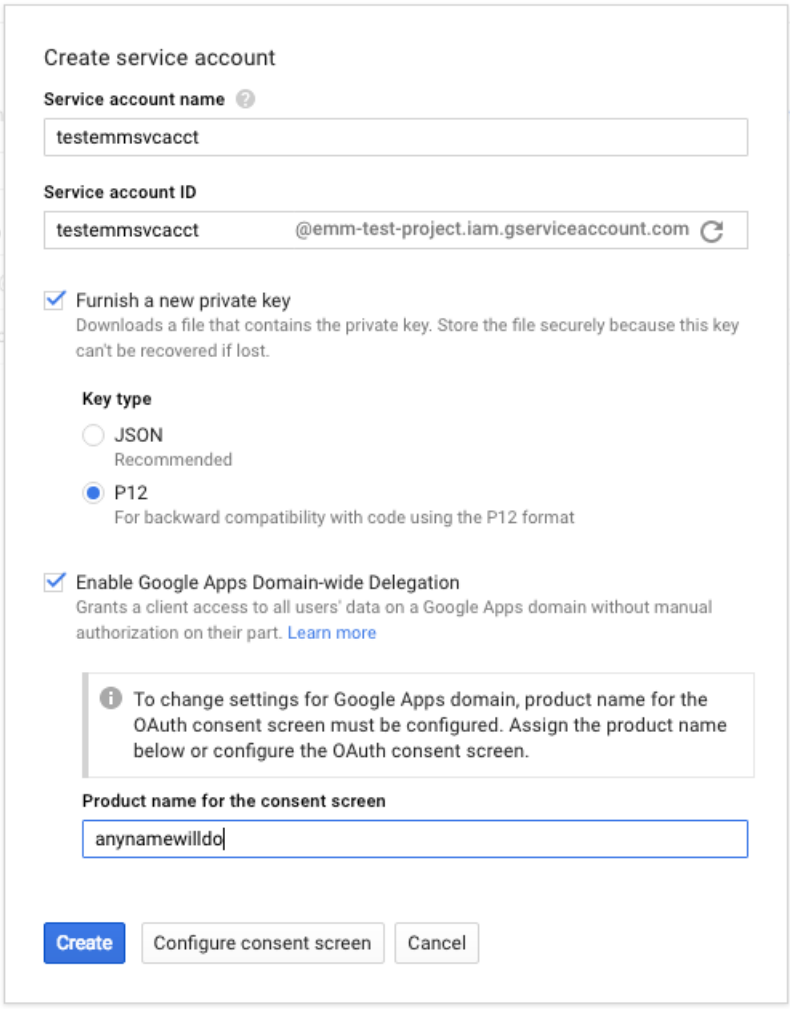
8: Klicken Sie in der Liste **Add credentials to our project** unter Schritt 1 auf **service account**.



9. Klicken Sie auf der Seite **Service Accounts** auf **Create Service Account**.

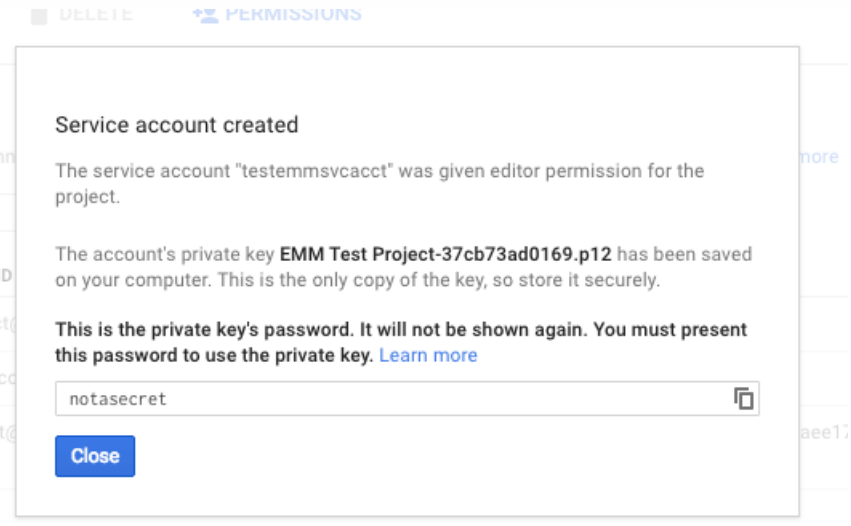


10. Geben Sie im Dialogfeld **Create service account key** einen Namen für das Konto ein, aktivieren das Kontrollkästchen **Furnish a new private key**, klicken Sie auf **P12**, aktivieren Sie das Kontrollkästchen **Enable Google Apps Domain-wide Delegation** und klicken Sie auf **Create.**

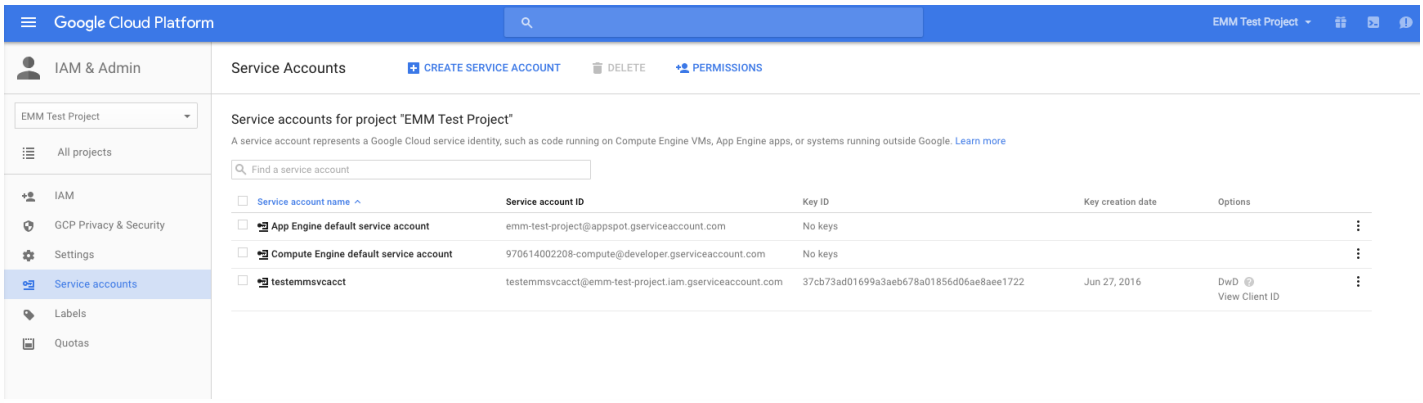


Die Zertifikatdatei (P12-Datei) wird auf Ihren Computer heruntergeladen. Speichern Sie das Zertifikat an einem sicheren Ort.

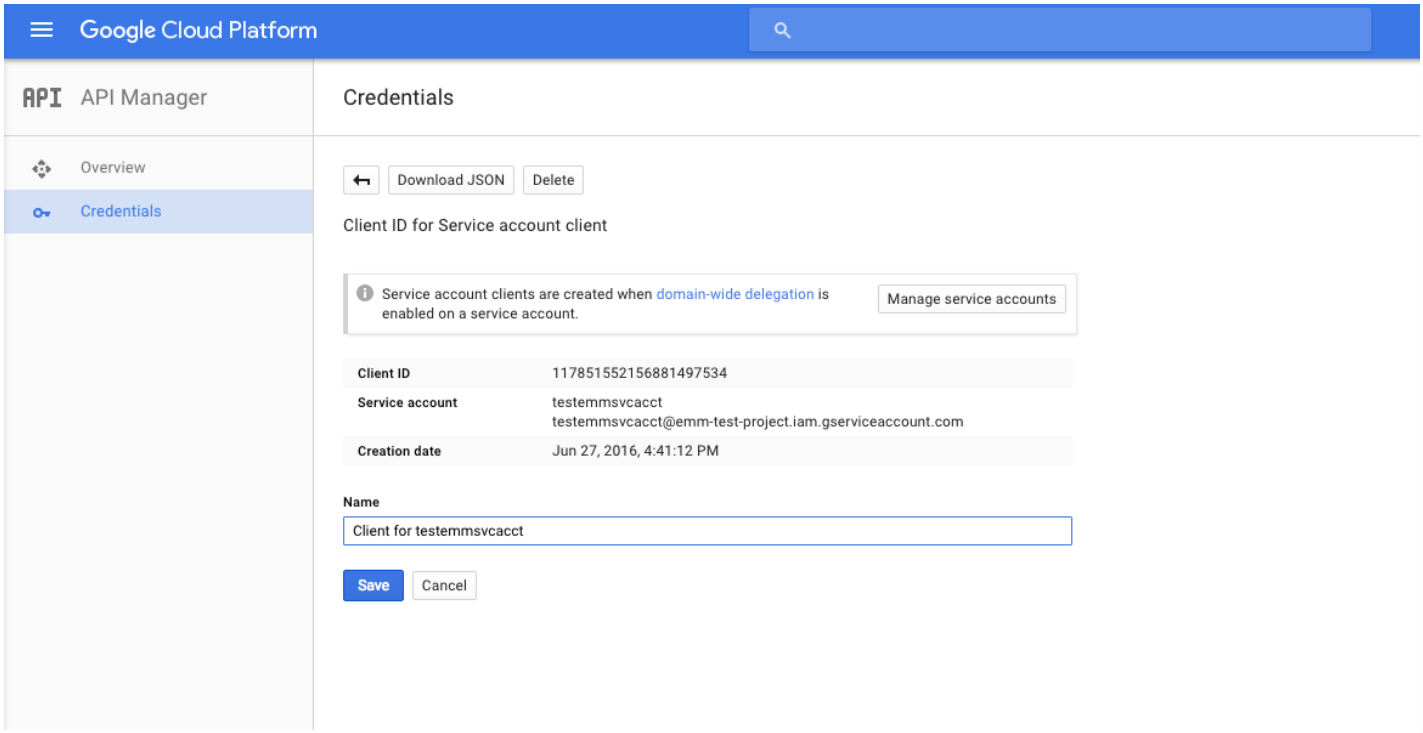
11. Klicken Sie im Bestätigungsbildschirm **Service account created** auf **Close**.



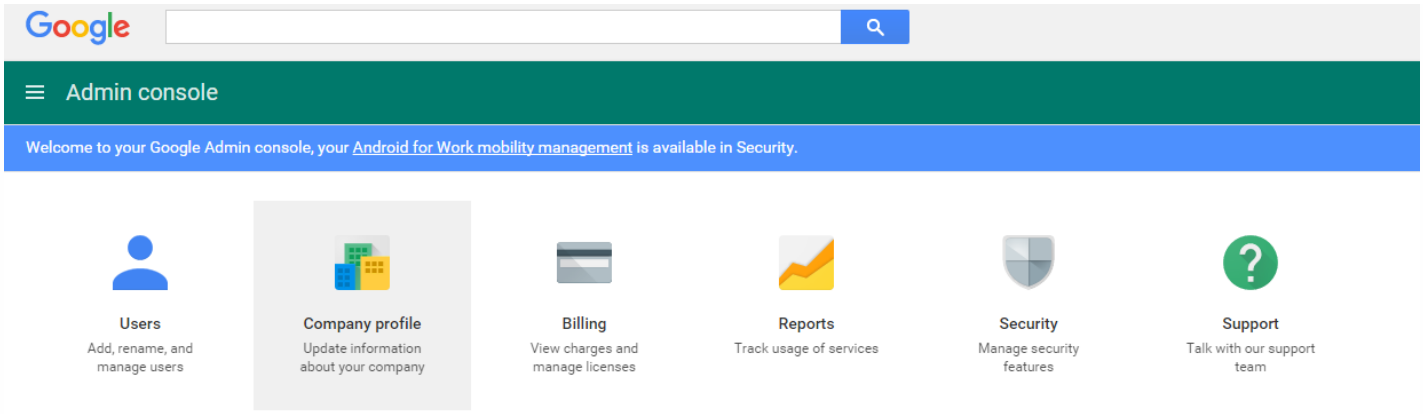
12. Klicken Sie auf der Seite **Permissions** auf **Service accounts** und dann unter **Options** auf **View Client ID**.



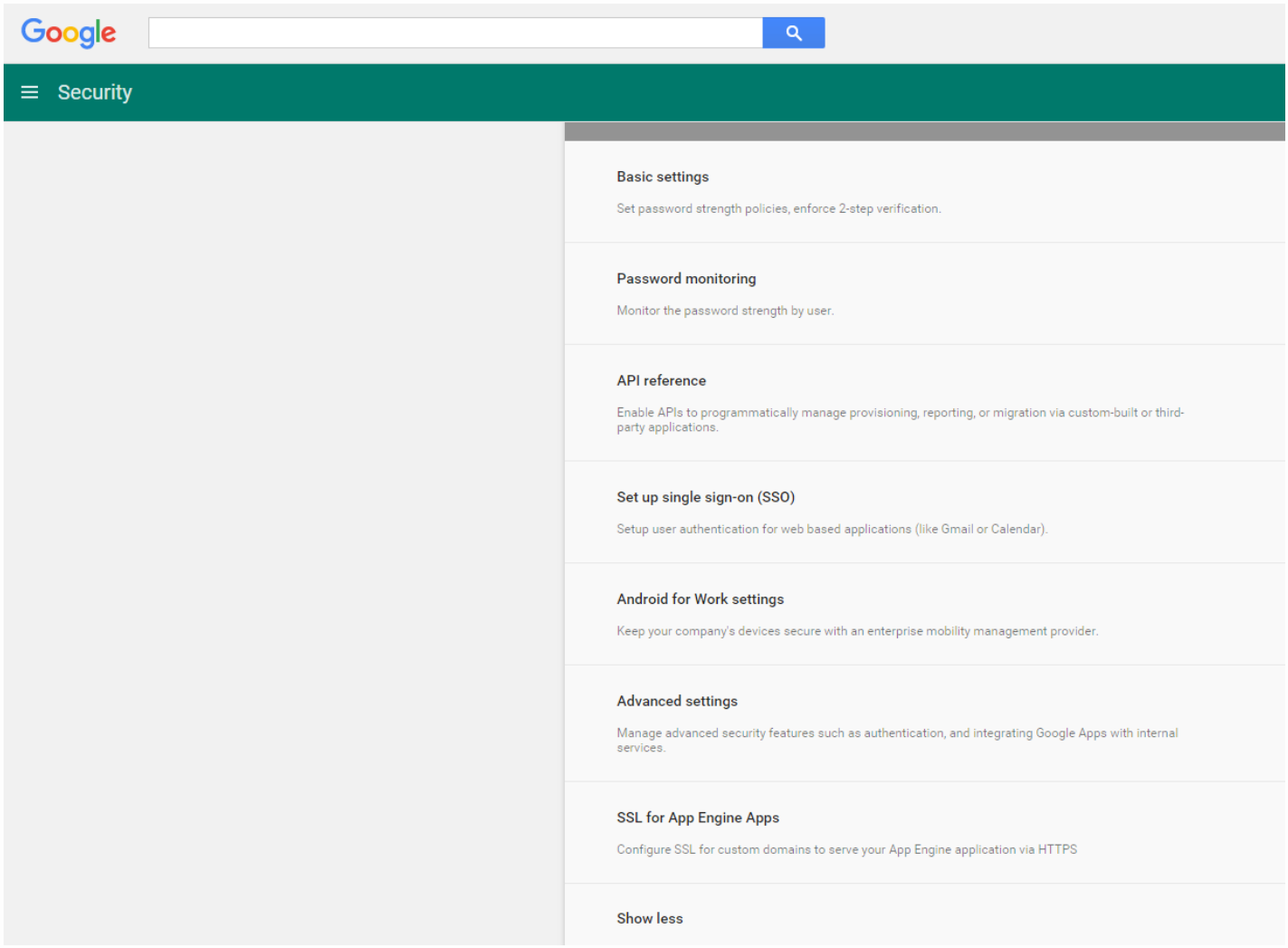
13. Die für die Kontoautorisierung auf der Google Admin console erforderlichen Informationen werden angezeigt. Kopieren Sie die **Client ID** und **Service account ID** in einen Speicherort, um sie später von dort abzurufen. Sie müssen diese Informationen mit dem Domänennamen an den Citrix Support senden, damit sie auf eine Positivliste gesetzt werden.



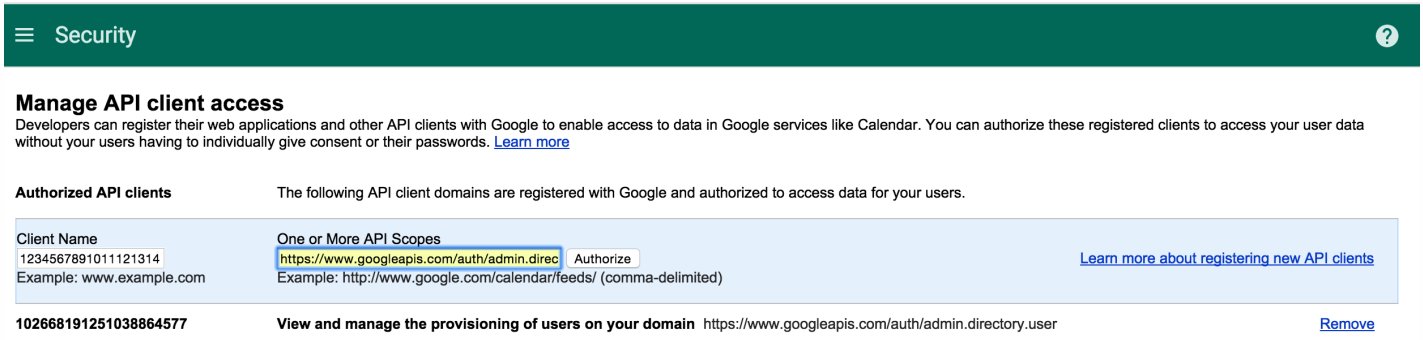
14. Öffnen Sie die Google Admin console für Ihre Domäne und klicken Sie auf **Security**.



15. Klicken Sie auf **Android for Work settings**.



16. Geben Sie unter **Client Name** die Client-ID ein, die Sie zuvor gespeichert haben, geben Sie unter **One or More API Scopes** https://www.googleapis.com/auth/admin.directory.user ein und klicken Sie auf **Authorize**.

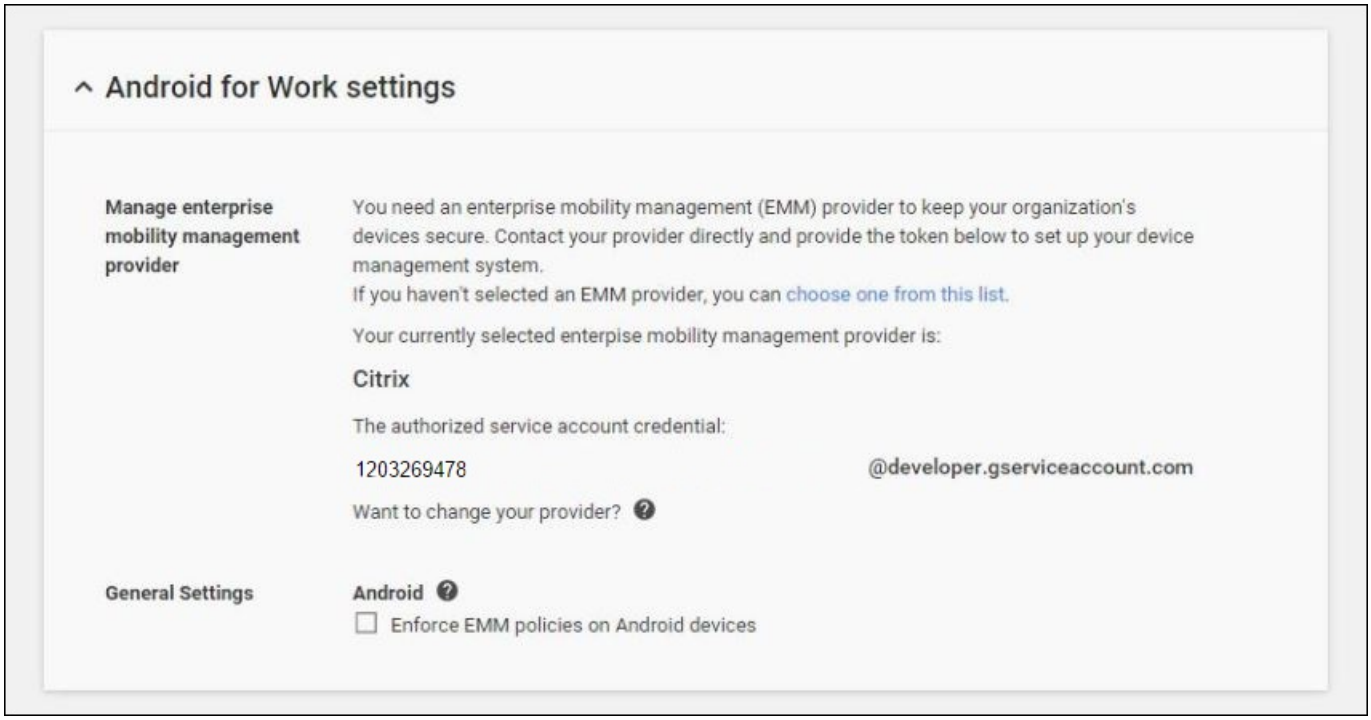


Binden an EMM

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

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

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



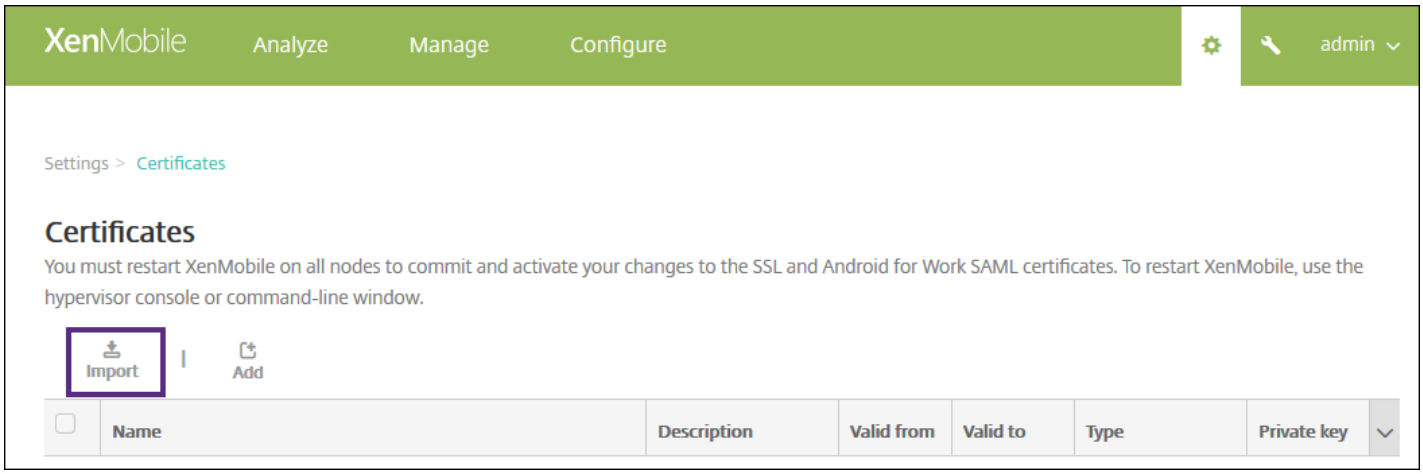
Nach der Prüfung der Tokenbindung können Sie XenMobile zum Verwalten der Android for Work-Geräte verwenden. Sie müssen das in Schritt 14 generierte P12-Zertifikat importieren, den Android for Work-Server einrichten, das SAML-basierte Single Sign-On aktivieren und mindestens eine Android for Work-Richtlinie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

Importieren des P12-Zertifikats

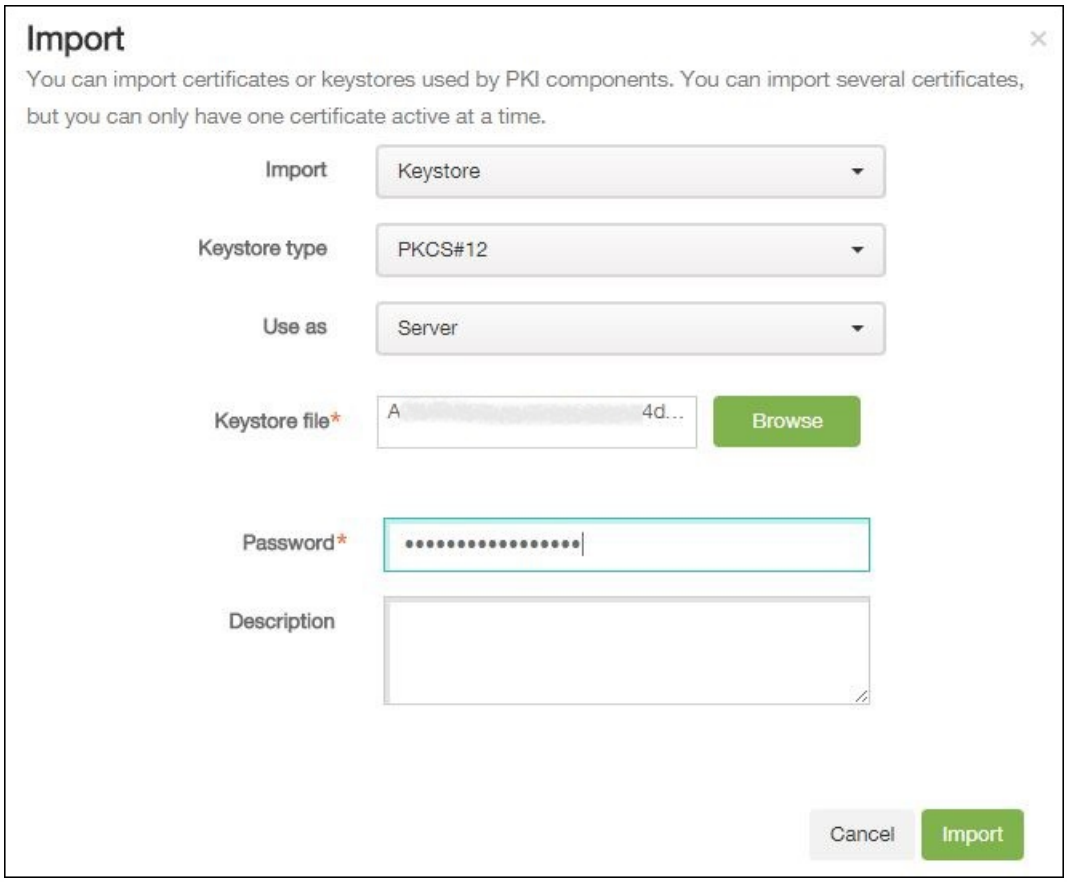
Führen Sie die folgenden Schritte zum Importieren des Android for Work-P12-Zertifikats aus:

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

2. Klicken Sie auf das Zahnradsymbol in der oberen rechten Ecke der Konsole zum Öffnen die Seite **Einstellungen** und klicken Sie dann auf **Zertifikate**. Die Seite **Zertifikate** wird angezeigt.



3. Klicken Sie auf **Importieren**. Das Dialogfeld **Import** wird angezeigt.



Konfigurieren Sie die folgenden Einstellungen:

- **Importieren**: Klicken Sie in der Liste auf **Schlüsselspeicher**.
- **Schlüsselspeichertyp**: Klicken Sie in der Liste auf **PKCS#12**.

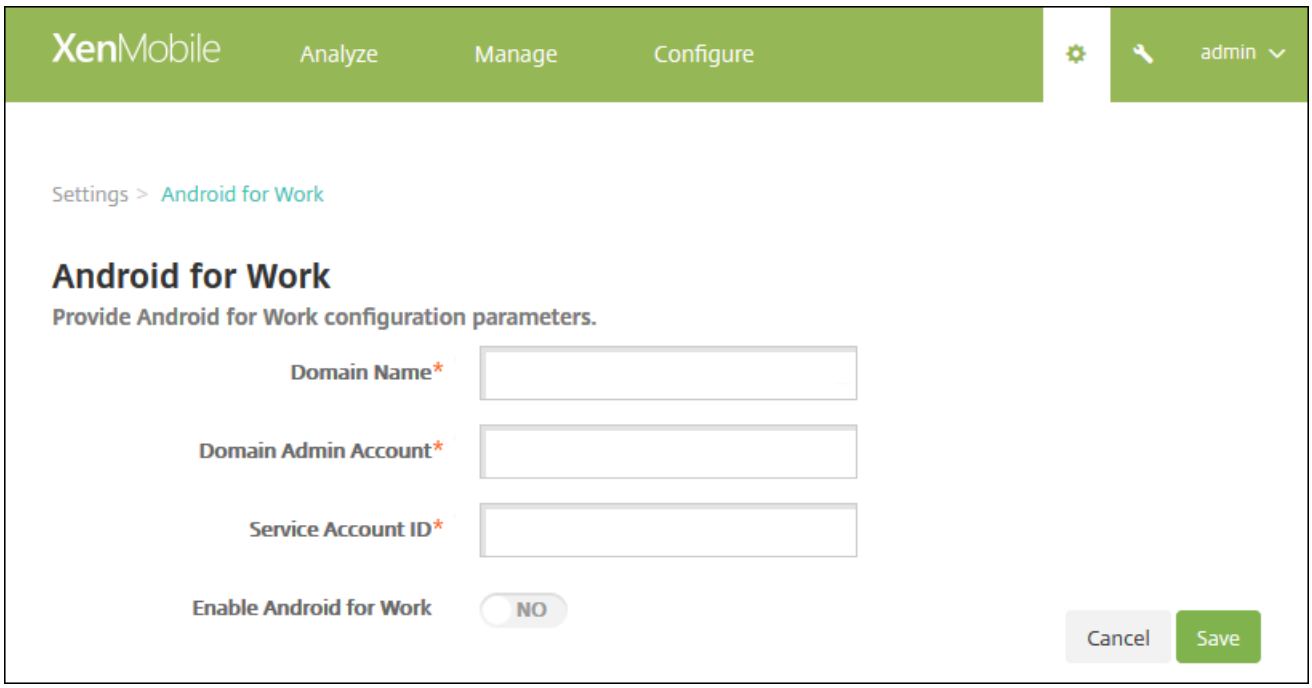
- **Verwenden als**: Klicken Sie in der Liste auf **Server**.
- **Schlüsselspeicherdatei**: Klicken Sie auf **Durchsuchen** und navigieren Sie zu dem P12-Zertifikat.
- **Kennwort**: Geben Sie das Schlüsselspeicherkennwort für die Anmeldeinformationen ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung des Zertifikats ein.

4. Klicken Sie auf **Importieren**.

Einrichten des Android for Work-Servers

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **Android for Work**. Die Seite **Android for Work** wird angezeigt.



Konfigurieren Sie die folgenden Einstellungen:

- **Domänenname**: Geben Sie den Namen der Android for Work-Domäne ein, z. B. domain.com.
- **Domänenadministratorkonto**: Geben Sie Ihren Domänenadministrator-Benutzernamen ein, z. B. das für das Google Developer Portal verwendete E-Mail-Konto.
- **Dienstkonto-ID**: Geben Sie die ID Ihres Dienstkontos ein, z. B. die dem Google-Dienstkonto zugeordnete E-Mail-Adresse (serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com).
- **Android for Work aktivieren**: Klicken Sie zum Aktivieren oder deaktivieren auf diese Option.

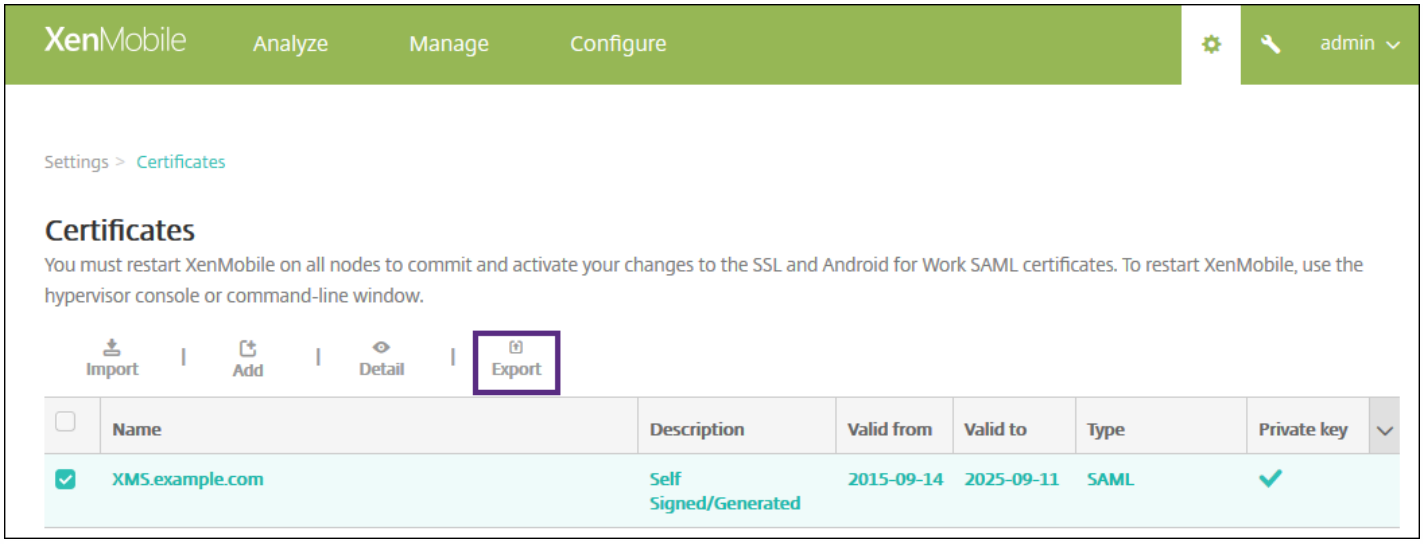
3. Klicken Sie auf **Speichern**.

Aktivieren des SAML-basierten Single Sign-Ons

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

2. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

3. Klicken Sie auf **Zertifikate**. Die Seite **Zertifikate** wird angezeigt.

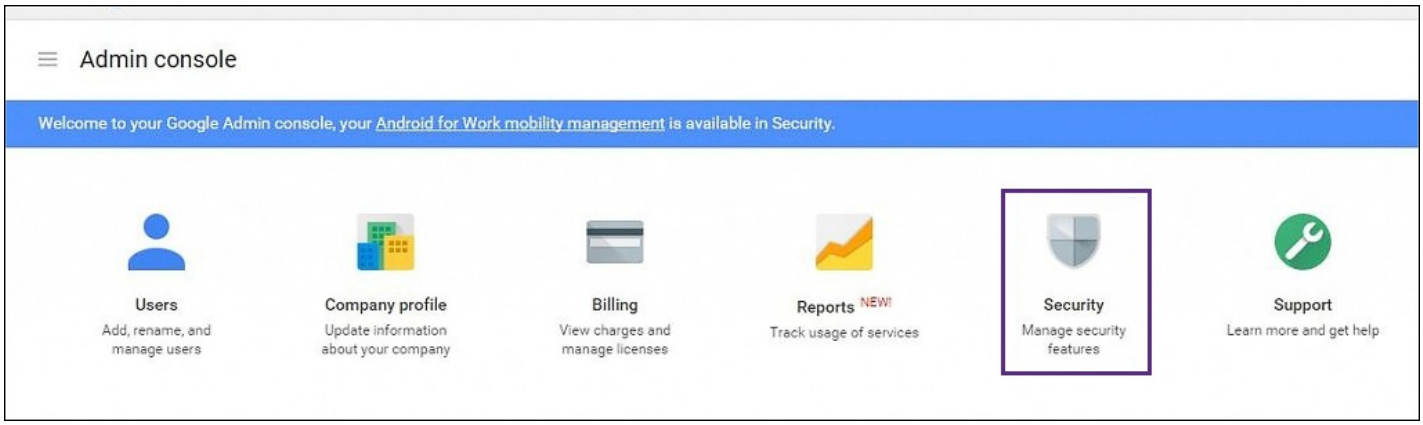


3. Klicken Sie in der Liste der Zertifikate auf das SAML-Zertifikat.

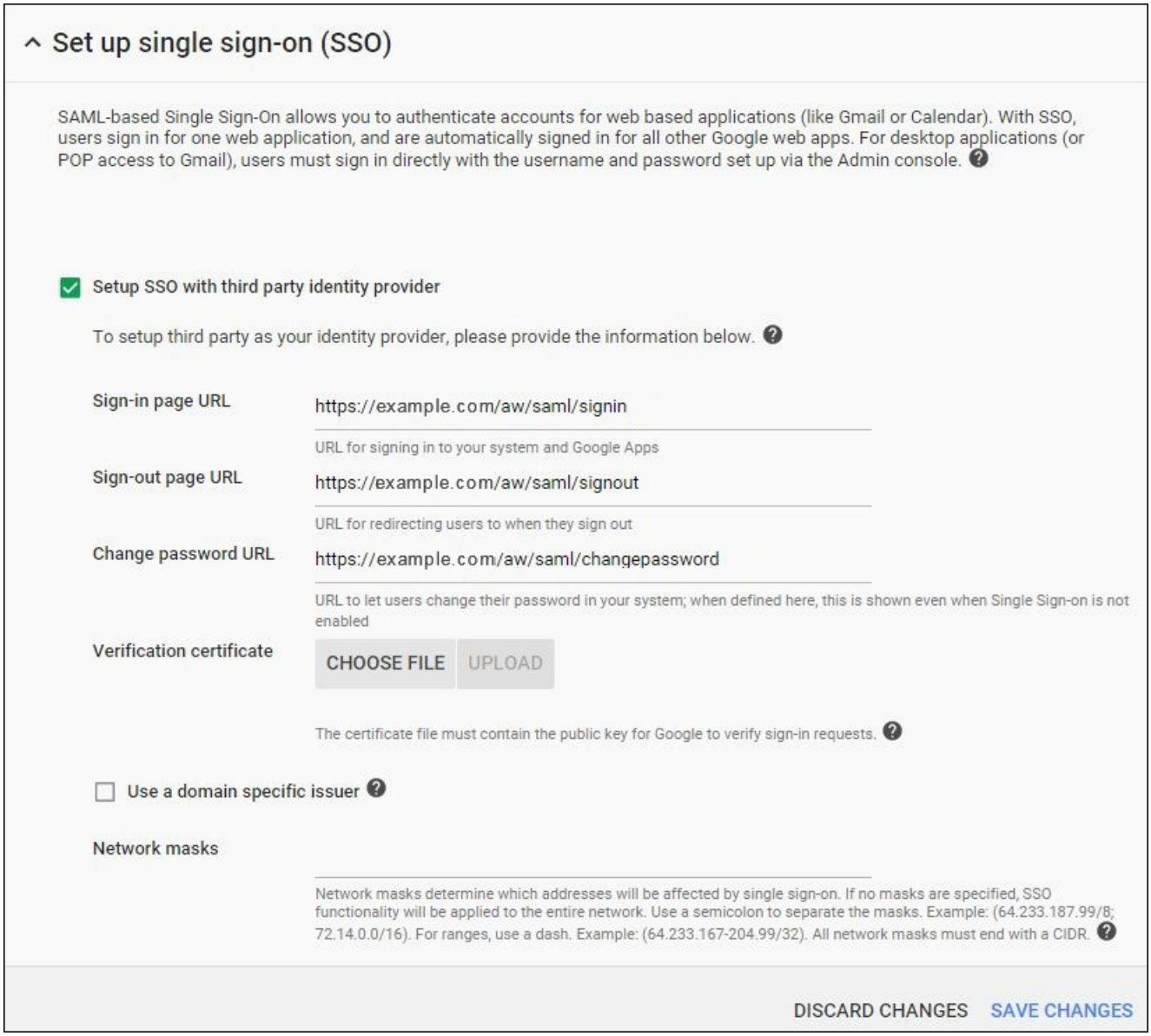
4. Klicken Sie auf **Exportieren** und speichern Sie das Zertifikat auf Ihrem Computer.

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

6. Klicken Sie auf **Security**.



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

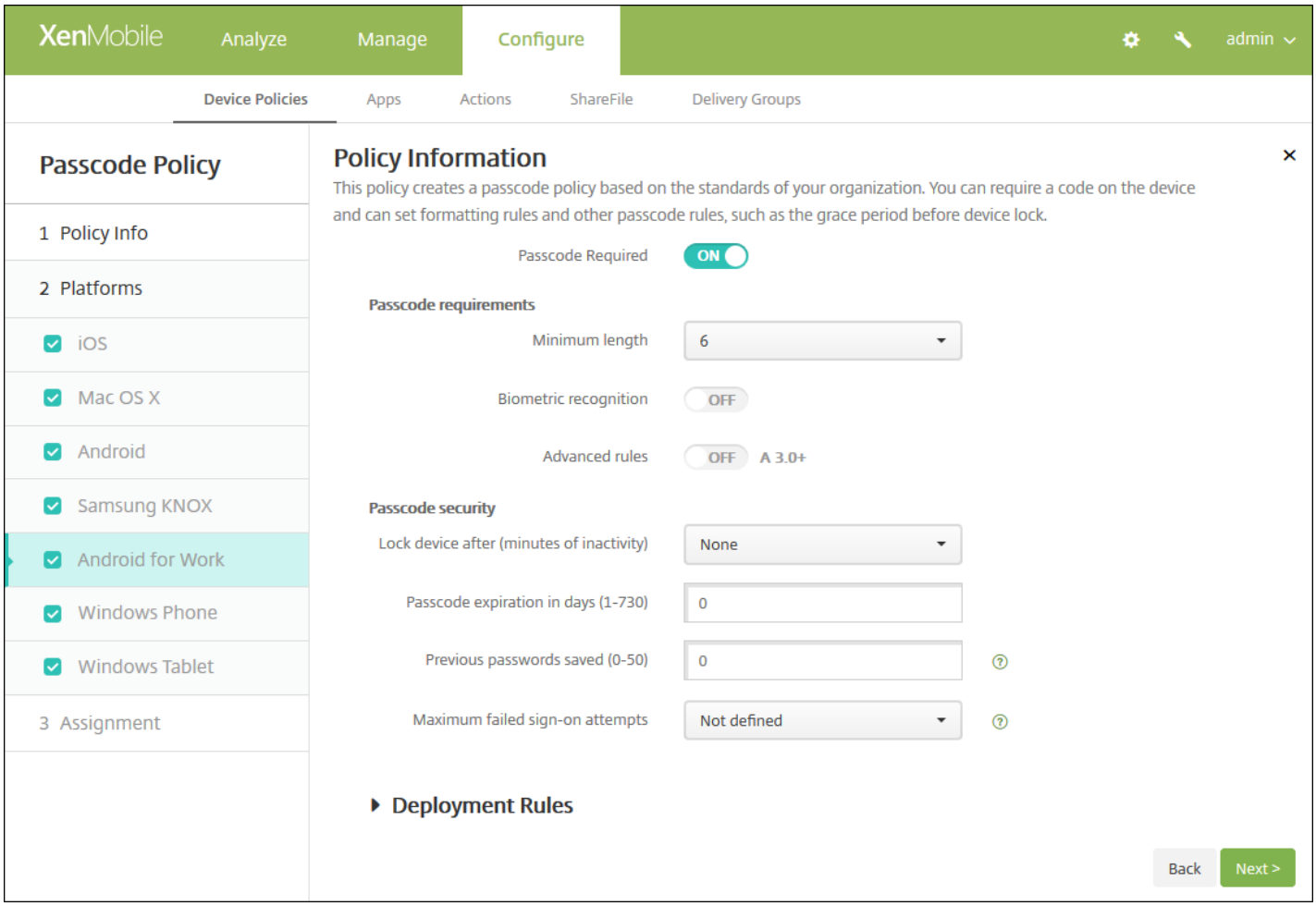


- **Sign-in page URL**: Geben Sie die URL der Seite an, über die Benutzer sich bei Ihrem System und Google-Apps anmelden. Beispiel: https:///aw/saml/signin.
- **Sign-out page URL**: Geben Sie die URL an, an die die Benutzer weitergeleitet werden, wenn sie sich abmelden. Beispiel: https:///aw/saml/signout.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

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

Einrichten einer Android for Work-Richtlinie

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



Die grundlegenden Schritte zum Einrichten einer Geräterichtlinie sind folgende:

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

2. Klicken Sie auf **Konfigurieren > Geräterichtlinien**.

3. Klicken Sie auf **Hinzufügen** und wählen Sie dann im Dialogfeld **Neue Richtlinie hinzufügen** die Richtlinie aus, die Sie hinzufügen möchten (in diesem Beispiel **Passcode**).

4. Füllen Sie die Seite **Richtlinieninformationen** aus.

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

6. Weisen Sie die Richtlinie einer Bereitstellungsgruppe zu.

Weitere Informationen zum Einrichten von anderen Geräterichtlinien für Android for Work finden Sie unter XenMobile-Geräterichtlinien nach Plattform.

Konfigurieren von Android for Work-Kontoeinstellungen

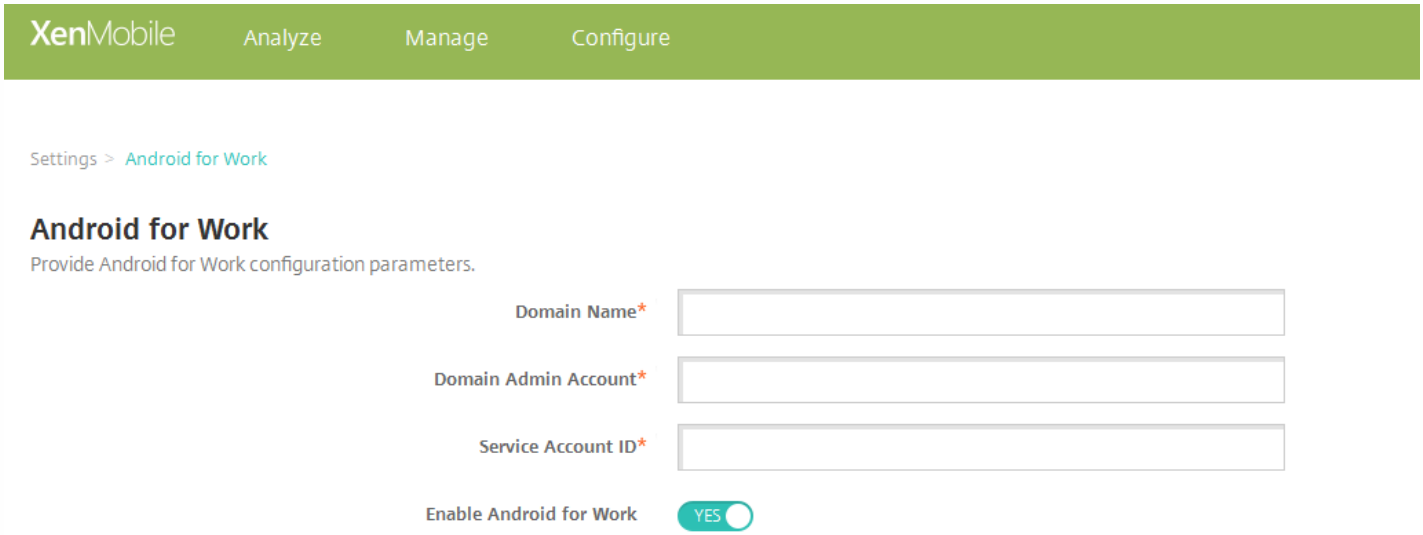
Jul 28, 2016

> ## Warnung
>
> Ein bekanntes Drittanbieterproblem ist, dass Sie über die XenMobile-Konsole Android for Work nicht aktivieren können. Weitere Informationen zu diesem Problem und zum Konfigurieren einer Servereigenschaft als Workaround finden Sie unter Problem #615118 im Abschnitt Bekannte Probleme bei XenMobile Server 10.3.

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

1. Klicken Sie in der XenMobile-Webkonsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **Android for Work**. Die Seite **Android for Work** wird angezeigt.



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

- **Domänenname**: Geben Sie Ihren Domänennamen ein.
- **Domänenadministratorkonto**: Geben Sie Ihren Domänenadministrator-Benutzernamen ein.
- **Dienstkonto-ID**: Geben Sie die ID Ihres Google-Dienstkontos ein.

- **Android for Work aktivieren**: Wählen Sie aus, ob Android for Work aktiviert werden soll.

4. Klicken Sie auf **Speichern**.

Bereitstellen des Gerätebesitzermodus in Android for Work

Jul 28, 2016

Zum Bereitstellen von Android for Work im Gerätebesitzermodus müssen Sie mit den in diesem Dokument beschriebenen Schritten Daten über NFC (Near Field Communication) zwischen zwei Geräten übertragen. Dazu muss auf dem einen Gerät das Worx Provisioning Tool ausgeführt werden und das andere Gerät muss auf die Werkseinstellungen zurückgesetzt sein. Der Gerätebesitzermodus ist nur für Unternehmensgeräte verfügbar.

Warum wird NFC verwendet? Bluetooth, WiFi und andere Kommunikationsmodi sind auf einem Gerät mit Werkseinstellungen deaktiviert. NFC ist das einzige Kommunikationsprotokoll, das das Gerät in diesem Zustand versteht.

Eine Übersicht über das Bereitstellen von Android for Work in der XenMobile-Umgebung finden Sie unter Verwalten von Geräten mit Android for Work in XenMobile.

Voraussetzungen

- Ein XenMobile-Server, Versionen 10.1 und 10.3, der für Android for Work aktiviert ist.
- Ein auf die Werkseinstellungen zurückgesetztes Gerät, das für Android for Work im Gerätebesitzermodus bereitgestellt ist. Die Schritte dazu sind nachstehend beschrieben.
- Ein Gerät mit NFC-Funktion, auf dem das konfigurierte Worx Provisioning Tool ausgeführt wird. Das Worx Provisioning Tool ist in Worx Home 10.3 oder auf der Citrix Downloadseite verfügbar.

Jedes Gerät kann nur ein Android for Work-Profil haben, das von einer Enterprise Mobility Management-App (EMM) verwaltet wird. In XenMobile ist Worx Home die EMM-App. Es ist nur ein Profil pro Gerät zulässig. Wenn Sie versuchen, eine zweite EMM-App hinzuzufügen, wird die erste gelöscht.

Sie können den Gerätebesitzermodus auf neuen Geräten oder auf Geräten mit Werkseinstellungen aktivieren. Das gesamte Gerät wird mit XenMobile verwaltet.

NFC-Übertragung im Gerätebesitzermodus

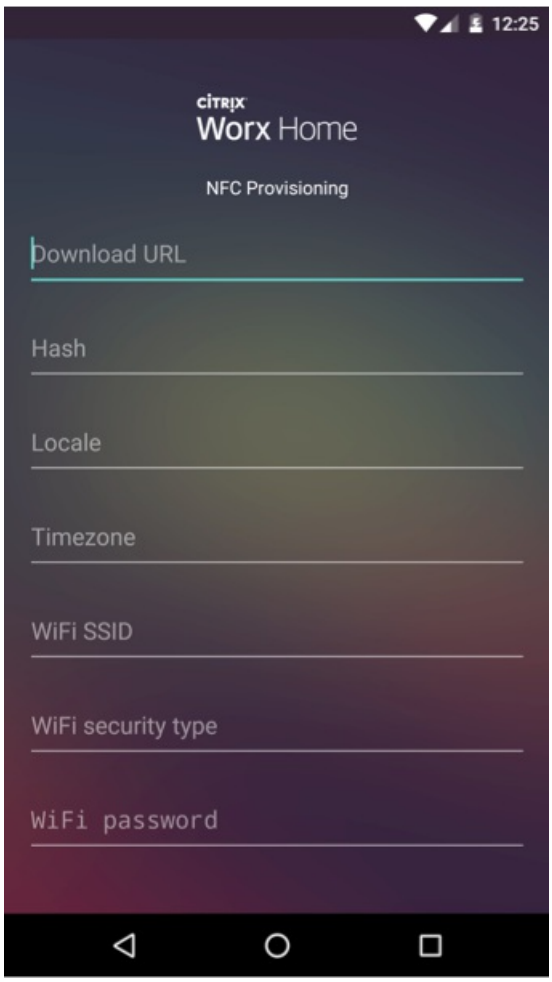
Für das Provisioning eines auf Werkseinstellungen zurückgesetzten Geräts müssen Sie die folgenden Daten über NFC senden, damit Android for Work funktioniert:

- Paketname der EMM-Anbieter-App, die als Gerätebesitzer (Worx Home) fungiert.
- Intranet-/Internetspeicherort, von dem das Gerät die EMM-Anbieter-App herunterlädt.
- SHA-1-Hash der EMM-Anbieter-App, um zu überprüfen, ob der Download erfolgreich war.
- WiFi-Verbindungsdetails, sodass ein auf Werkseinstellungen zurückgesetztes Gerät eine Verbindung herstellen und die EMM-Anbieter-App herunterladen kann. (802.1x WiFi wird für diesen Vorgang von Android derzeit nicht unterstützt.)
- Zeitzone für das Gerät (optional).
- Geografischer Standort des Geräts (optional).

Wenn die beiden Geräte eine Verbindung herstellen, werden die Daten vom Worx Provisioning Tool an das Gerät mit den Werkseinstellungen gesendet. Diese Daten werden dann zum Download von Worx Home mit Administratoreinstellungen verwendet. Wenn Sie keine Werte für Zeitzone und Speicherort eingeben, konfiguriert Android sie automatisch auf dem neuen Gerät.

Konfigurieren des Worx Provisioning Tools

Bevor Sie Daten per NFC übertragen können, müssen Sie das Worx Provisioning Tool konfigurieren. Diese Konfiguration wird dann während der NFC-Übertragung an das auf die Werkseinstellungen zurückgesetzte Gerät gesendet.



Sie können Daten in die erforderlichen Felder eintragen oder die Felder mit einer Textdatei ausfüllen. Die App speichert die eingegebenen Informationen nicht. Erstellen Sie daher eine Textdatei, wenn Sie die Informationen zukünftig verwenden möchten.

Konfigurieren mit einer Textdatei

Nennen Sie die Datei **nfcprovisioning.txt** und speichern Sie sie auf der SD-Karte des Geräts im Ordner /sdcard/Downloads. Die App liest die Textdatei und fügt die Werte ein.

Die Textdatei muss die folgenden Daten enthalten:

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=
Dies ist der Intranet-/Internetspeicherort der EMM-Anbieter-App. Wenn das auf Werkseinstellungen zurückgesetzte Gerät nach der NFC-Übertragung mit den zuvor eingegebenen Daten (SSID, Sicherheitstyp und Kennwort) eine Verbindung mit WiFi herstellt, muss es für den Download Zugriff auf diesen Speicherort haben. Die URL ist eine normale URL ohne spezielle Formatierung.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=

Dies ist die Prüfsumme der EMM-Anbieter-App. Mit ihr wird überprüft, ob der Download erfolgreich war. Nachfolgend werden die Schritte zum Abrufen beschrieben.

android.app.extra.PROVISIONING_WIFI_SSID=
Dies ist die verbundene WiFi-SSID des Geräts, auf dem das Worx Provisioning Tool ausgeführt wird.

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=
Unterstützte Werte sind WEP und WPA2. Wenn das WiFi nicht geschützt ist, muss dieses Feld leer sein.

android.app.extra.PROVISIONING_WIFI_PASSWORD=
Wenn das WiFi nicht geschützt ist, muss dieses Feld leer sein.

android.app.extra.PROVISIONING_LOCALE=
Geben Sie die Sprach- und Ländercodes ein. Die Sprachcodes sind gemäß ISO 639-1 definiert und bestehen aus zwei Kleinbuchstaben (z. B. de). Ländercodes sind nach ISO 3166-1 definiert und bestehen aus zwei Großbuchstaben (z. B. DE). Geben Sie z. B. de_DE für Deutsch/Deutschland ein. Wenn Sie keine Länder- und Sprachcodes eingeben, werden sie automatisch ausgefüllt.

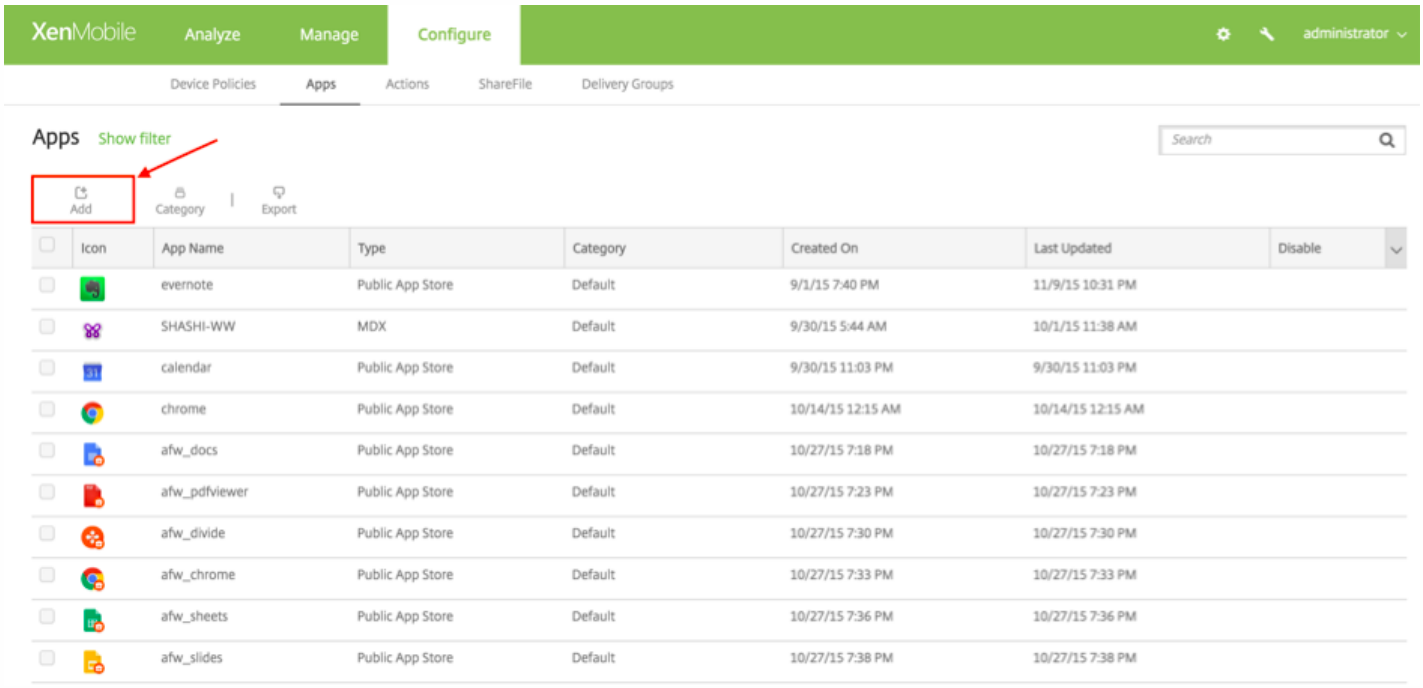
android.app.extra.PROVISIONING_TIME_ZONE=
Die Zeitzone, in der das Gerät ausgeführt wird. Geben Sie einen Namen im Format Gebiet/Ort ein. Beispiel: America/Los_Angeles für Pacific Time. Wenn Sie keine Zeitzone eingeben, wird sie automatisch eingetragen.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=
Keine Eingabe ist erforderlich, da der Wert in der App als Worx Home hartcodiert ist. Er wird hier nur der Vollständigkeit halber angegeben.

Abrufen der Worx Home-Prüfsumme

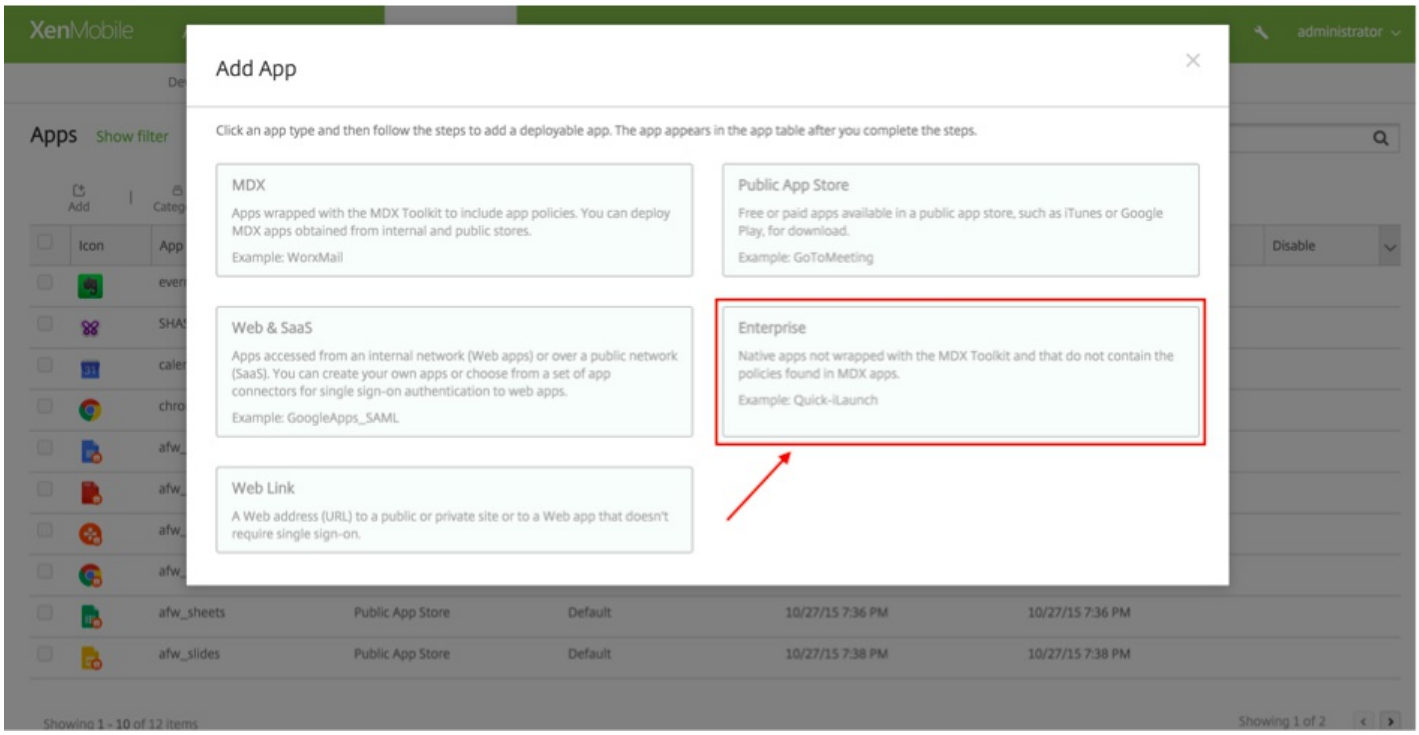
Wenn Sie die Prüfsumme einer App abrufen möchten, fügen Sie die App als Unternehmensapp hinzu.

1. Navigieren Sie in der XenMobile-Konsole zu **Konfigurieren > Apps > Hinzufügen**.



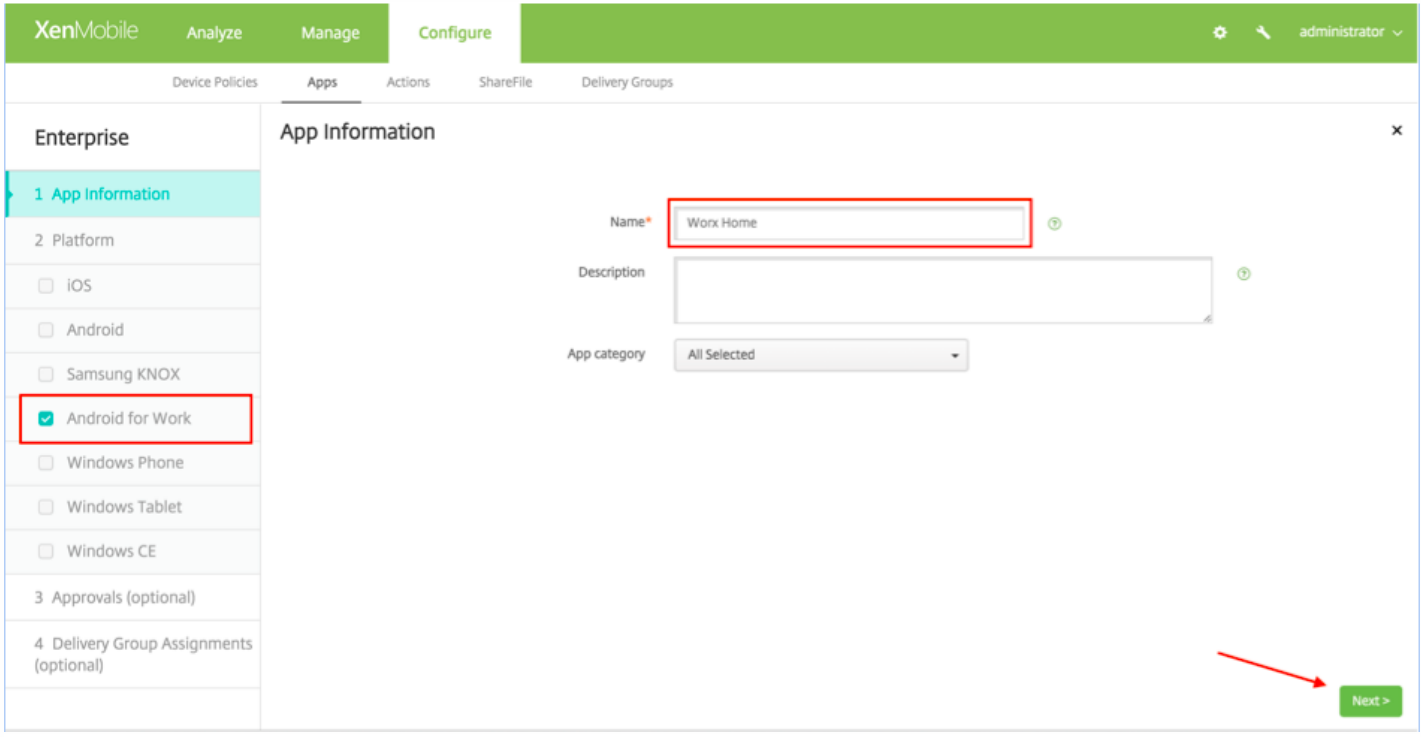
Der Bereich zum Hinzufügen von Apps wird angezeigt.

2. Klicken Sie auf **Enterprise**.



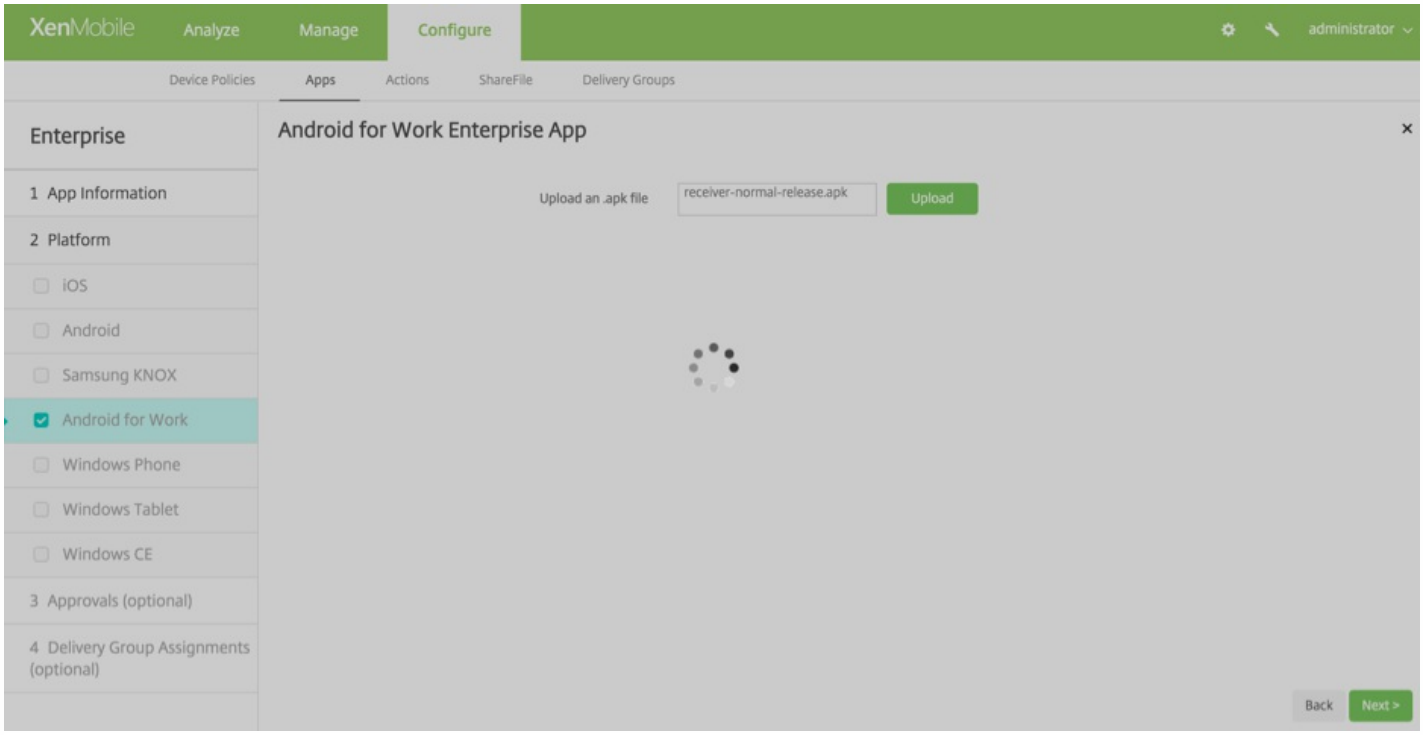
Der Bildschirm **App-Informationen** wird angezeigt.

3. Wählen Sie die folgende Konfiguration und klicken Sie auf **Weiter**.

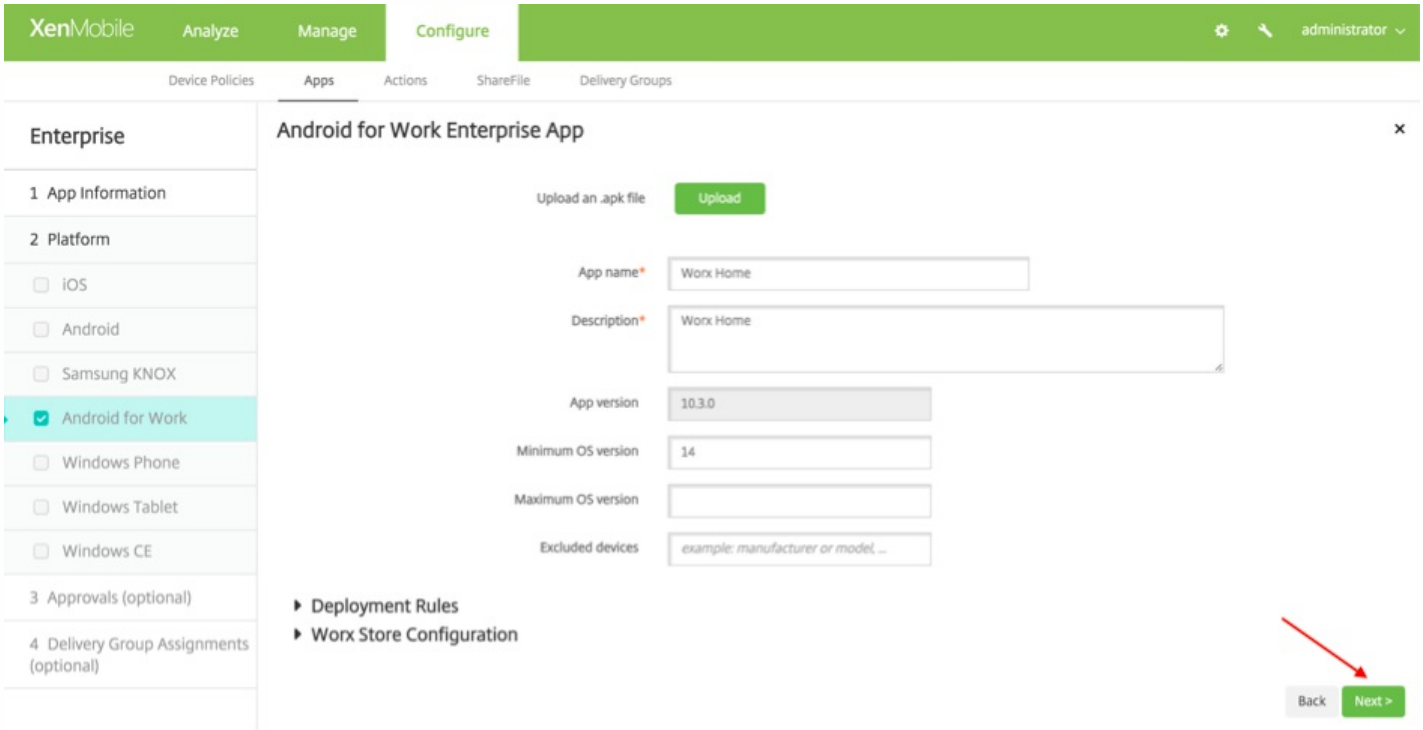


Der Bildschirm der Unternehmensapp **Android for Work** wird angezeigt.

4. Geben Sie den Pfad für die APK-Datei an und klicken Sie auf **Weiter**, um die Datei hochzuladen.

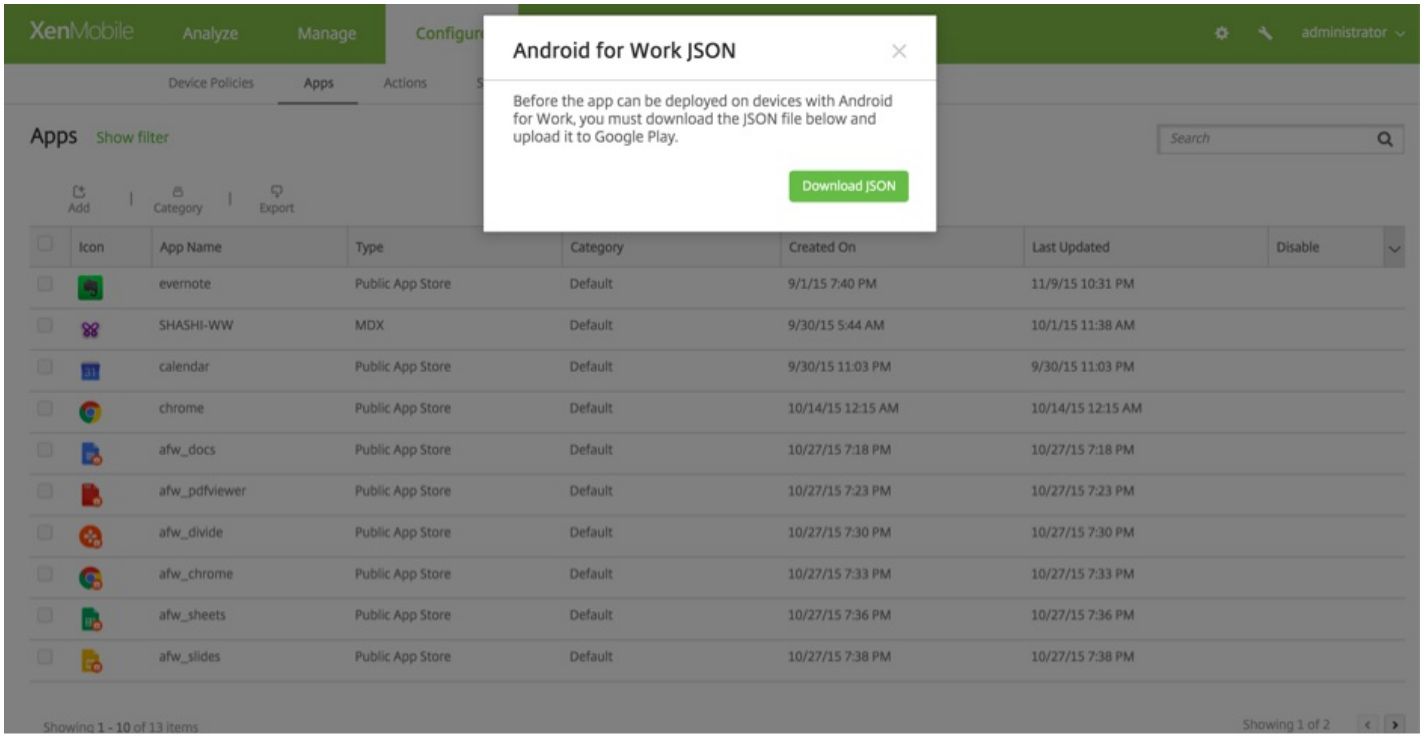


Wenn der Upload abgeschlossen ist, werden die Details des hochgeladenen Pakets angezeigt.



5. Klicken Sie auf **Weiter**, damit ein Bildschirm zum Herunterladen der JSON-Datei angezeigt wird, die Sie für den Upload

nach Google Play verwenden. Für Worx Home ist kein Upload nach Google Play erforderlich, aber Sie benötigen die JSON-Datei, um den SHA-1-Wert zu lesen.



Eine typische JSON-Datei sieht wie folgt aus:

6. Kopieren Sie den Wert **file_sha1_base64** und geben Sie ihn in das Feld **Hash** im Worx Provisioning Tool ein. **Hinweis:** Der Hash-Wert muss URL-sicher sein.

- Konvertieren Sie alle **+**-Zeichen in **-**
- Konvertieren Sie alle **/**-Zeichen in **_**
- Ersetzen Sie die Zeichen **\u003d** durch **=**

Die App führt die Sicherheitskonvertierung durch, wenn Sie den Hash-Wert in der Datei nfcprovisioning.txt auf der SD-Karte des Geräts speichern. Wenn Sie den Hash-Wert manuell eingeben, sind Sie dafür verantwortlich, dass die URL sicher ist.

Verwendete Bibliotheken

Das Worx Provisioning Tool verwendet die folgenden Bibliotheken im Quellcode:

- v7 appcompat library von Google unter Apache-Lizenz 2.0
- Design support library von Google unter Apache-Lizenz 2.0
- v7 Palette library von Google unter Apache-Lizenz 2.0

- Butter Knife von Jake Wharton unter Apache-Lizenz 2.0

Konfigurieren von Bereitstellungsregeln

Oct 13, 2016

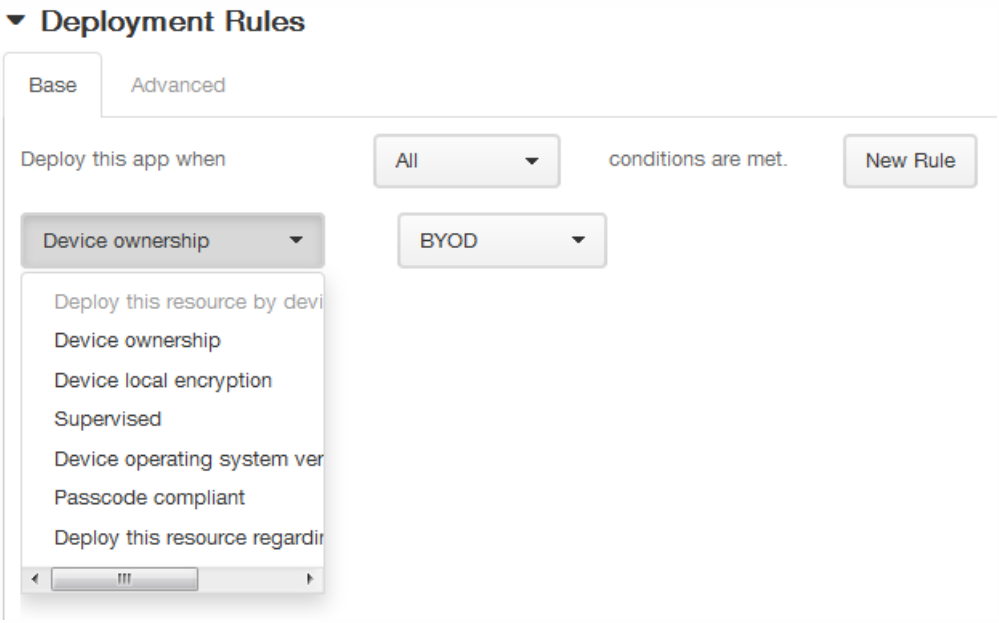
In diesem Abschnitt wird Folgendes beschrieben:

- 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.

Konfigurieren von Bereitstellungsregeln

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

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



Einfache Bereitstellungsregeln

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

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

Hinweis: Der Regelassistent enthält weitere testspezifische Informationen.

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

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

Erweiterte Bereitstellungsregeln

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

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

Konfigurieren von Bereitstellungszeitplänen

XenMobile verwendet den Bereitstellungszeitplan, den Sie für Aktionen, Apps und Geräterichtlinien angeben, um die Bereitstellung dieser Elemente zu steuern. Sie können festlegen, dass eine Bereitstellung sofort, zu einem bestimmten Datum und einer bestimmten Uhrzeit oder basierend auf Bereitstellungsbedingungen stattfindet. Der Bereitstellungsplan gilt für alle Plattformen.

Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS. iOS verwendet APNs.

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 die Bereitstellung verhindern möchten, legen Sie die Einstellung auf **AUS** fest.

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

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

Bereitstellen für immer aktive Verbindungen: Der Standardwert ist **AUS**. Diese Richtlinie gilt nur für Android-Geräte. Für die XenMobile-Servereigenschaft **Hintergrundbereitstellung** muss **Bereitstellen für immer aktive Verbindungen** für jede auf Android-Geräten bereitgestellte Richtlinie auf **EIN** festgelegt werden. Weitere Informationen über immer aktive Verbindungen finden Sie in der XenMobile-Bereitstellungsdokumentation unter "Other Server Optimizations" und "Optimizing Deployment Scheduling for Android Devices" in Tuning XenMobile Operations und "Scheduling policy" in Device and App Policies.

Hinzufügen von Geräten und Anzeigen von Gerätedetails

Jul 28, 2016

In der Datenbank auf dem XenMobile-Server wird eine Liste der Mobilgeräte gespeichert. Jedes Mobilgerät ist durch eine eindeutige Seriennummer 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. Weitere Informationen zu Dateiformaten für das Geräte-Provisioning finden Sie unter Geräte-Provisioningdateiformate.

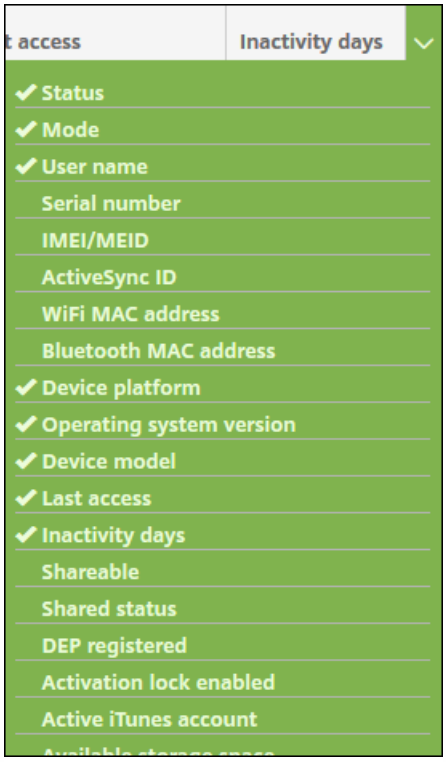
Die Seite **Geräte** der XenMobile-Konsole enthält eine Tabelle der Geräte mit folgenden Informationen: **Status** (Symbole, die anzeigen, ob ein Gerät per Jailbreak manipuliert wurde, ob es verwaltet wird, ob Active Sync Gateway verfügbar ist und ob das Gerät bereitgestellt ist), **Modus** (MDM oder MAM oder beides), **Benutzername**, **Geräteplattform**, **Betriebssystemversion**, **Gerätemodell**, **Letzter Zugriff**, und **Inaktivität (Tage)**.

Sie können Geräte manuell hinzufügen, Geräte aus einer Geräteprovisioningdatei importieren, Gerätedetails bearbeiten, Benachrichtigungen an Geräte senden und Geräte löschen. Sie können auch alle Gerätedaten aus der Tabelle in eine CSV-Datei exportieren und damit einen benutzerdefinierten Bericht generieren. Der Server exportiert alle Geräteattribute und wenn Sie Filter anwenden, werden diese beim Erstellen der CSV-Datei berücksichtigt.

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

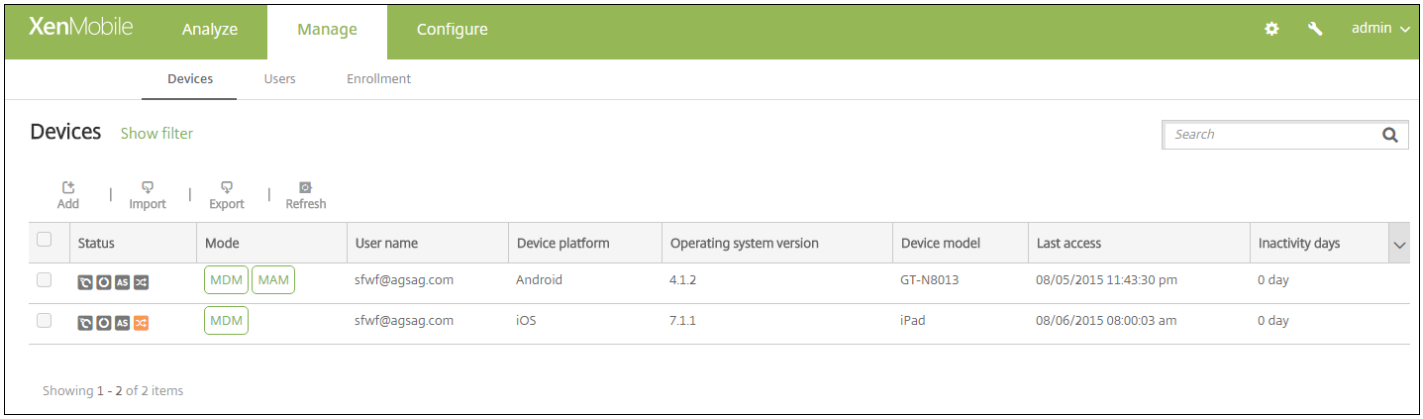
In den folgenden Abschnitten finden Sie weitere Informationen zu den verfügbaren Aktionen für die Tabelle **Geräte**:

- Gerät manuell hinzufügen
- Geräte aus einer Provisioningdatei importieren
- Geräte bearbeiten
- Benachrichtigungen an Geräte senden
- Geräte löschen
- Tabelle **Geräte** in eine CSV-Datei exportieren

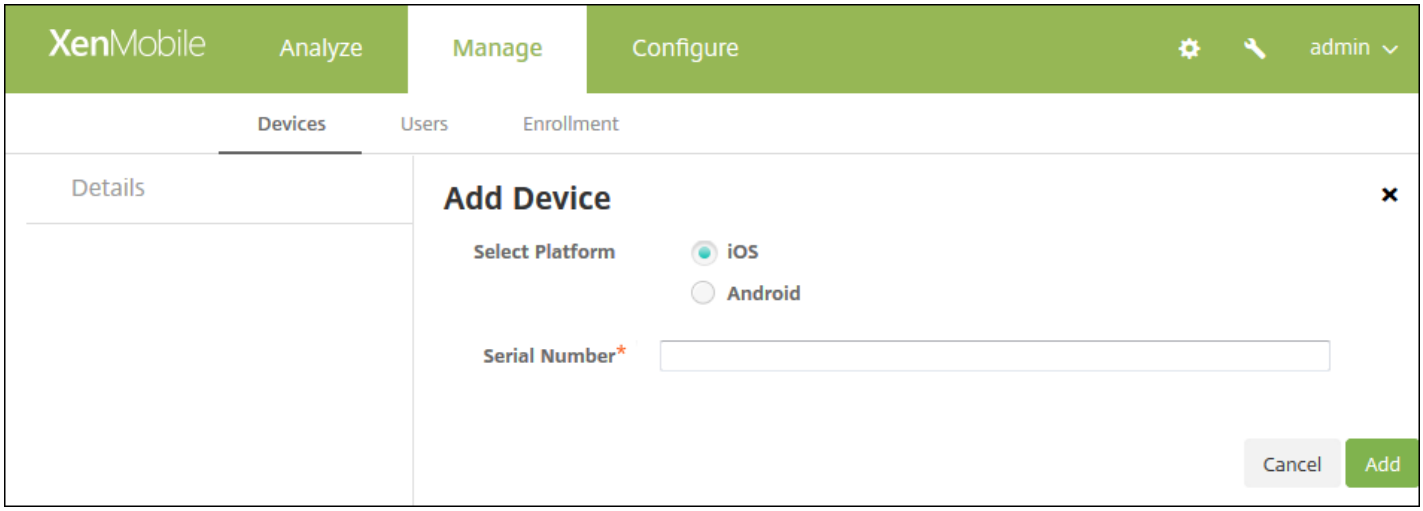


Manuelles Hinzufügen von Geräten

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



2. Klicken Sie auf **Hinzufügen**. Die Seite **Gerät hinzufügen** wird angezeigt.

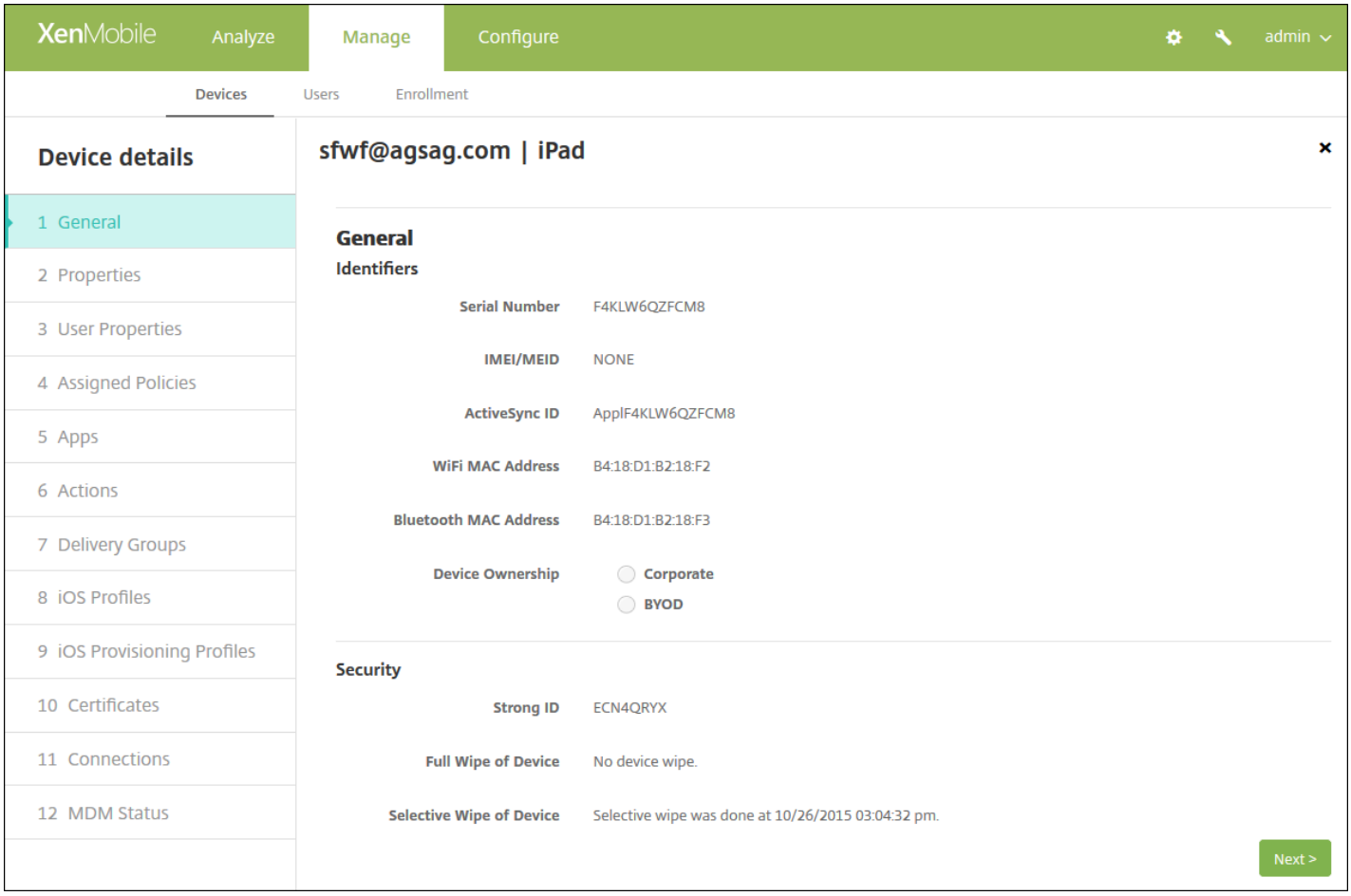


3. Konfigurieren Sie die folgenden Einstellungen:

- **Plattform wählen**: Klicken Sie auf **iOS** oder **Android**.
- **Seriennummer**: Geben Sie die Seriennummer des Geräts ein.
- **IMEI/MEID**: Geben Sie optional die IMEI/MEID des Geräts ein (nur Android-Geräte).

4. Klicken Sie auf **Hinzufügen**. Die Tabelle **Geräte** wird angezeigt. Das hinzugefügte Gerät befindet sich am Ende der Liste. Wählen Sie in der Liste das hinzugefügte Gerät aus und klicken Sie in dem nun angezeigten Menü auf **Bearbeiten**, 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.



5. Prüfen Sie unter **Allgemein Bezeichner** die angezeigten Informationen (die Liste variiert je nach Plattformtyp).

- Seriennummer
- IMEI/MEID
- ActiveSync-ID
- WiFi MAC-Adresse
- Bluetooth MAC-Adresse
- Gerätebesitz

6. Prüfen Sie unter **Sicherheit** die angezeigten Informationen (die Liste variiert je nach Plattformtyp).

- Starke ID
- Gerät vollständig löschen
- Gerät selektiv löschen
- Gerät sperren
- Entsperren des Geräts
- Gerät suchen
- Gerätetracking aktivieren
- Gerät ausschließen
- Aktivierungssperre umgehen
- Einschränkungen für Gerät deaktivieren
- AirPlay-Synchronisierung anfordern

- AirPlay-Synchronisierung beenden

Hinweis: Die Funktion "Gerät sperren" ist verfügbar für iOS 7 und höher.

7. Klicken Sie auf **Weiter**. Die Seite **Eigenschaften** wird angezeigt. Hier können Sie dem Gerät Eigenschaften hinzufügen.

8. Klicken Sie auf **Hinzufügen**. Eine Liste der verfügbaren Eigenschaften wird angezeigt.

9. Führen für jedes Gerät, das Sie hinzufügen möchten, folgende Schritte aus:

- Klicken Sie in der Liste auf die gewünschte Eigenschaft und legen Sie deren Wert fest. Wählen Sie beispielsweise **Aktivierungssperre aktiviert** aus und legen Sie **Ja** oder **Nein** fest.
- Klicken Sie auf **Fertig**.

10. Klicken Sie auf **Weiter**.

Hinweis: Hinzugefügte Eigenschaften werden unter **Eigenschaften** angezeigt. Wenn Sie anschließend zur Seite **Eigenschaften** zurückkehren, werden die Eigenschaften separat in verschiedenen Kategorien angezeigt.

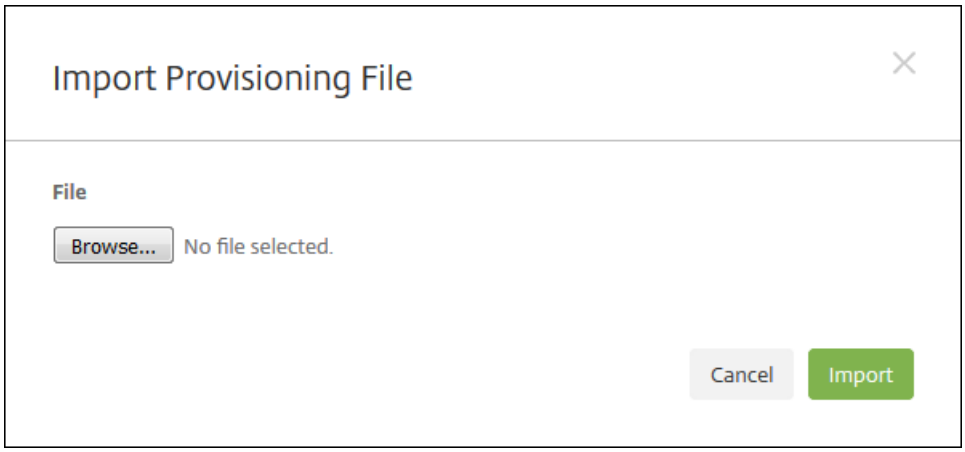
Der Bereich **Zugewiesene Richtlinien** und die nachfolgenden Bereiche enthalten zusammengefasste Informationen zu dem Gerät.

- **Zugewiesene Richtlinien**: 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.
- **Aktionen**: zeigt die Anzahl der zugewiesenen bereitgestellten, ausstehenden und fehlgeschlagenen Aktionen an. Für jede Aktion werden Name und Datum der letzten Bereitstellung angezeigt.
- **Bereitstellungsgruppen**: 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-Profile** (nur iOS-Geräte): zeigt den aktuellsten iOS-Profilbestand mit Namen, Typ, Unternehmen und Beschreibung an.
- **Zertifikate**: zeigt die Anzahl der gültigen, abgelaufenen und gesperrten Zertifikate mit Typ, Anbieter, Herausgeber, Seriennummer und Gültigkeitszeitraum an.
- **Verbindungen**: 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.

12. Klicken Sie auf **Speichern**.

Importieren von Geräten aus einer Provisioningdatei

Sie können die Datei eines Mobilfunkanbieters oder Geräteherstellers oder Ihre eigene Provisioningdatei importieren. Siehe Geräte-Provisioningdateiformate.
1. Klicken Sie im Menü oberhalb der Tabelle **Geräte** auf **Importieren**. Das Dialogfeld **Provisioningdatei importieren** wird angezeigt.

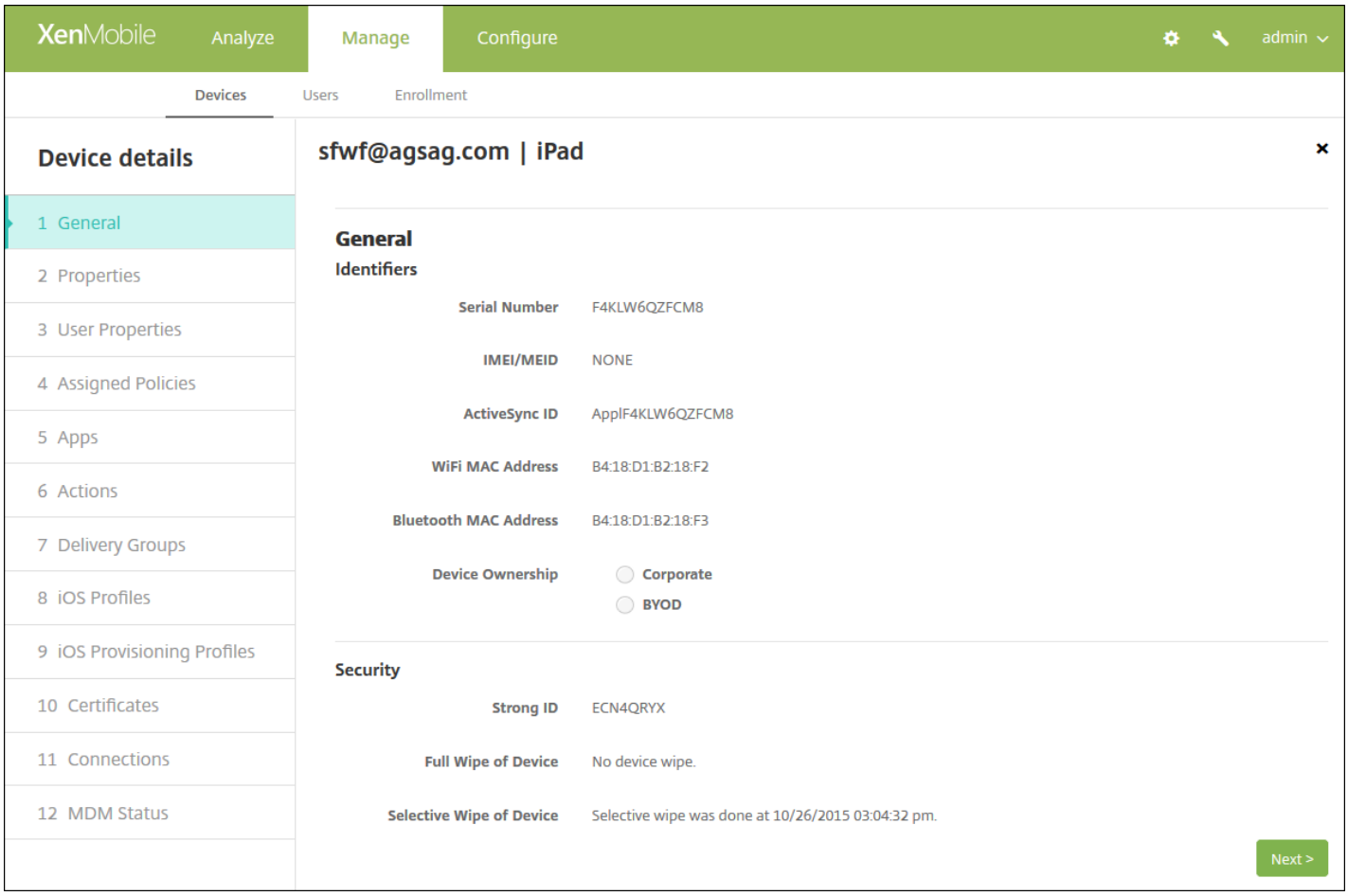


2. Klicken Sie zur Auswahl der zu importierenden Datei auf **Durchsuchen** und navigieren Sie zum Speicherort der Datei.

3. Klicken Sie auf **Importieren**. Die importierten Dateien werden der Tabelle **Geräte** hinzugefügt.

Bearbeiten von Geräten

1. Wählen Sie das gewünschte Gerät aus und klicken Sie auf Bearbeiten. Die Seite Gerätedetails wird angezeigt.



2. Das einzige Feld unter **Allgemein Bezeichner**, das Sie ändern können, ist **Gerätebesitz**. Sie können **Unternehmensbesitz** oder **BYOD** auswählen.

3. Klicken Sie auf **Weiter**. Die Seite **Eigenschaften** wird angezeigt.

4. Auf der Seite **Eigenschaften** können Sie Eigenschaften hinzufügen, bearbeiten und löschen.

- Zum Hinzufügen einer Eigenschaft klicken Sie in der Kategorie, der Sie die Eigenschaft hinzufügen möchten, auf "Hinzufügen", klicken Sie auf die gewünschte Eigenschaft in der nun eingeblendeten Liste und fügen Sie den Wert der Eigenschaft hinzu. Klicken Sie auf **Fertig**.
- Zum Bearbeiten klicken Sie auf die gewünschte Eigenschaft, ändern Sie deren Einstellungen und klicken Sie dann auf **Fertig** oder auf **Abbrechen**.
- 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 **Weiter**. Die nächste Seite hängt von dem ausgewählten Gerät ab. Bei einigen Geräten werdenBenutzereigenschaften, bei anderen zugewiesene Richtlinien angezeigt.

6. Werden Benutzereigenschaften angezeigt, können Sie diese wie nachfolgend beschrieben hinzufügen, bearbeiten und löschen. Die restlichen Seiten enthalten zusammengefasste Informationen für das Gerät. Eine Beschreibung dieser Seiten finden Sie unter Manuelles Hinzufügen von Geräten.

Hinweis: Der obere Teil der Seitemit den Benutzereigenschaften kann nicht bearbeitet werden.

- Für jede Eigenschaft, die Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - Klicken Sie in der eingeblendeten Liste auf die gewünschte Eigenschaft, geben Sie den Wert ein und klicken Sie auf **Fertig** oder auf **Abbrechen**.
- Zum Bearbeiten klicken Sie auf die gewünschte Eigenschaft, ändern Sie deren Einstellungen und klicken Sie dann auf **Fertig** oder auf **Abbrechen**.
- 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. Prüfen Sie die zusammengefassten Informationen auf den nachfolgenden Seiten und klicken Sie auf **Weiter**.

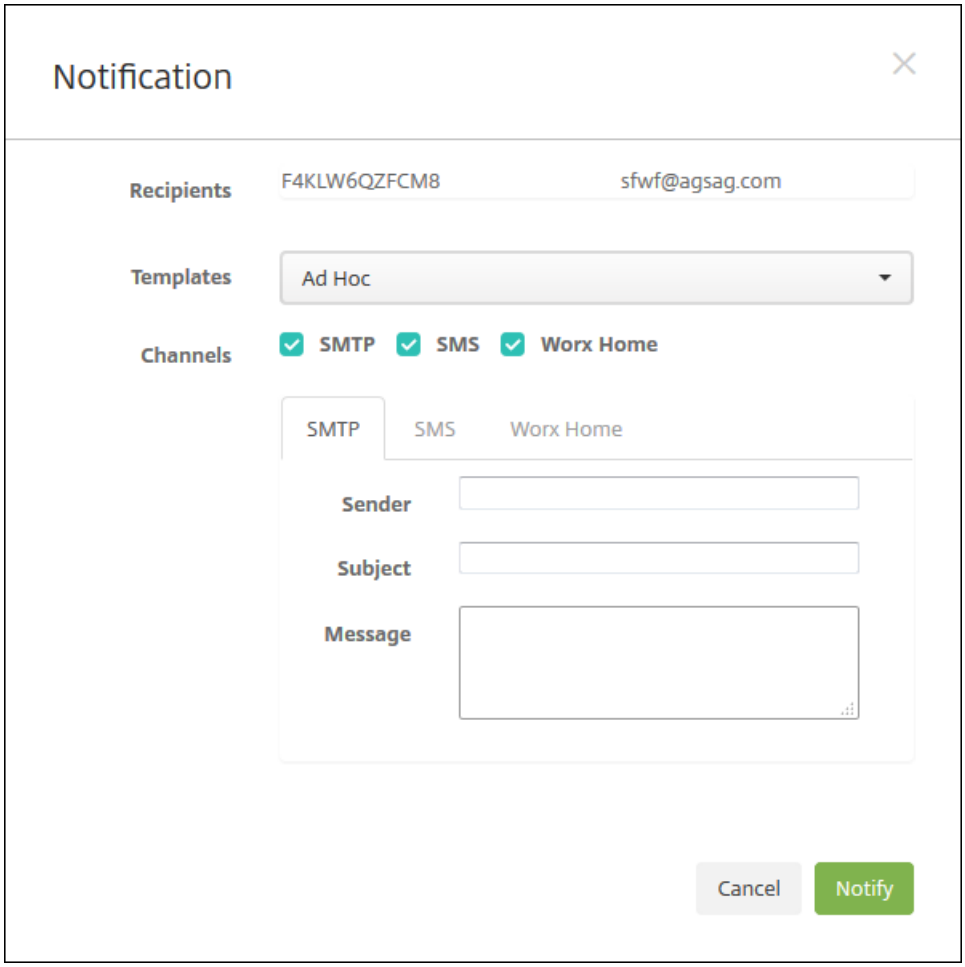
8. Klicken Sie auf der letzten Seite auf **Speichern**, um die Änderungen für das Gerät zu speichern.

Senden einer Benachrichtigung an Geräte

Sie können Benachrichtigungen an Geräte über die Seite Geräte senden. Weitere Informationen über Benachrichtigungen finden Sie unter Erstellen oder Aktualisieren von Benachrichtigungsvorlagen in XenMobile.

1. Wählen Sie das oder die Geräte aus, an die Sie Benachrichtigung senden möchten.

2. Klicken Sie auf **Benachrichtigen**. Das Dialogfeld **Benachrichtigung** wird angezeigt. Im Feld **Empfänger** werden alle Geräte aufgeführt, die die Benachrichtigung erhalten werden.



3. Konfigurieren Sie die folgenden Einstellungen:

- **Vorlagen**: Klicken Sie in der Liste auf den gewünschten Benachrichtigungstyp. Die Felder **Betreff** und **Nachricht** werden mit den vorkonfigurierten Angaben aus der ausgewählten Vorlage (Ausnahme: **Ad hoc**) ausgefüllt.
- **Kanäle**: Wählen Sie aus, wie die Benachrichtigung gesendet werden soll. Standardmäßig sind **SMTP**, **SMS** und **Worx Home** ausgewählt. Sie können auf die Registerkarten **SMTP**, **SMS** und **Worx Home** klicken, um das jeweilige Nachrichtenformat anzuzeigen.
- **Absender**: Geben Sie optional einen Absender ein.
- **Betreff**: Geben Sie für eine Ad-hoc-Nachricht einen Betreff ein.
- **Nachricht**: Geben Sie für eine Ad-hoc-Nachricht einen Text ein.

4. Klicken Sie auf **Benachrichtigen**.

Löschen von Geräten

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

Exportieren der Gerätetabelle

1. Klicken Sie auf die Schaltfläche **Exportieren** oberhalb der Tabelle **Geräte**. Die Informationen in der Tabelle "Geräte" werden extrahiert und in eine CSV-Datei konvertiert.

2. Öffnen oder speichern Sie die CSV-Datei. Ihre Vorgehensweise hängt von dem verwendeten Browser ab. Sie können den Vorgang auch abbrechen.

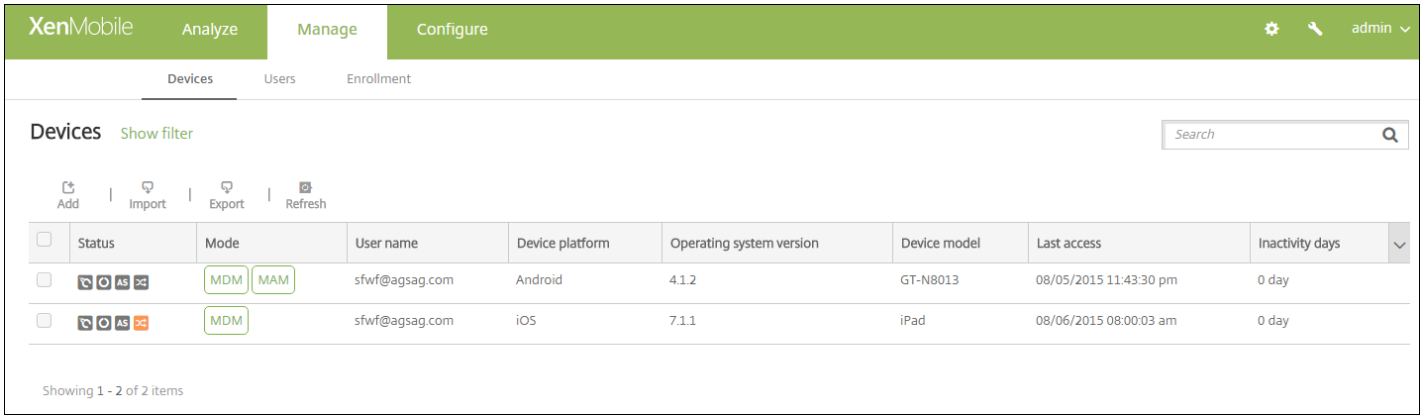
Sperren von iOS-Geräten

Jul 28, 2016

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

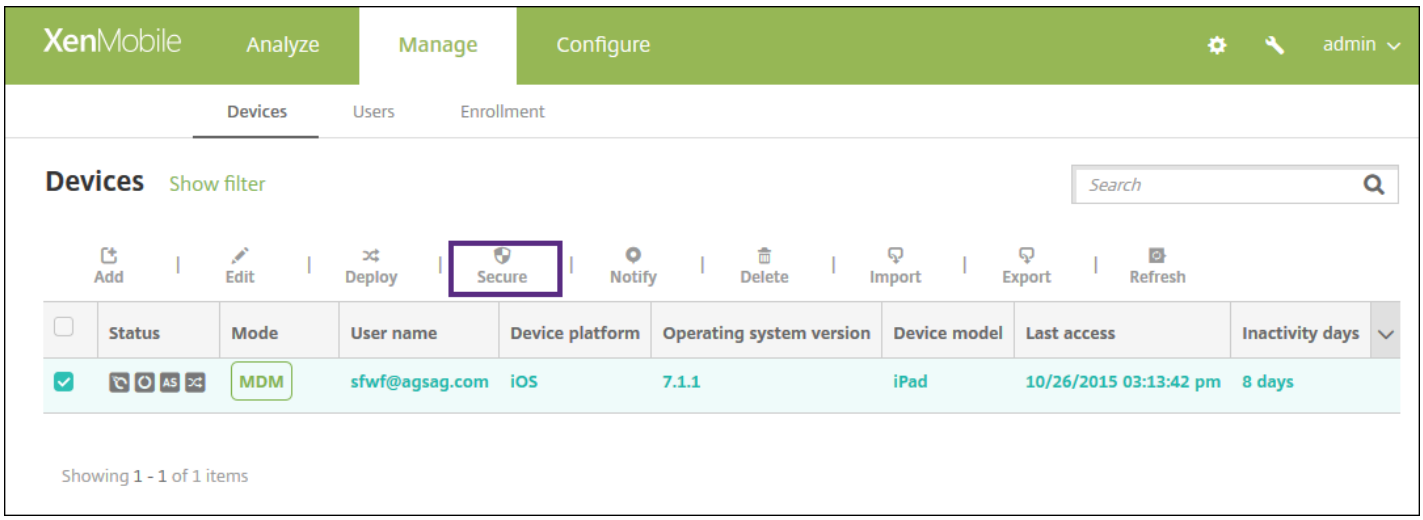
Wenn Sie sich für die Anzeige einer Nachricht und Telefonnummer auf dem Sperrbildschirm entscheiden, werden diese nur dann angezeigt, wenn Sie die Passcode-Richtlinie in der XenMobile-Konsole festgelegt oder wenn Benutzer den Passcode manuell auf Geräten aktiviert haben.

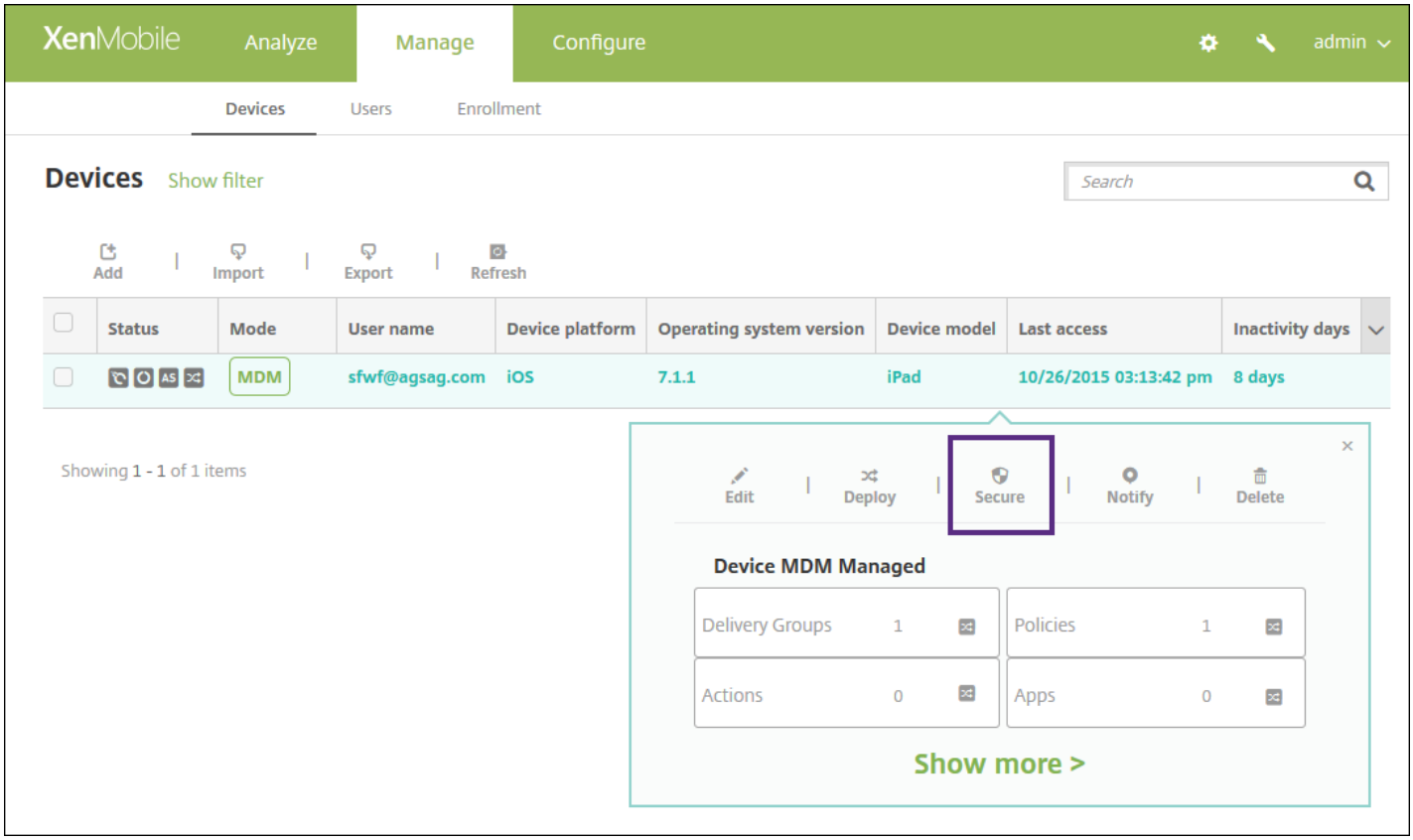
1. Klicken Sie in der XenMobile-Konsole auf **Verwalten > Geräte**. Die Seite **Geräte** wird angezeigt.



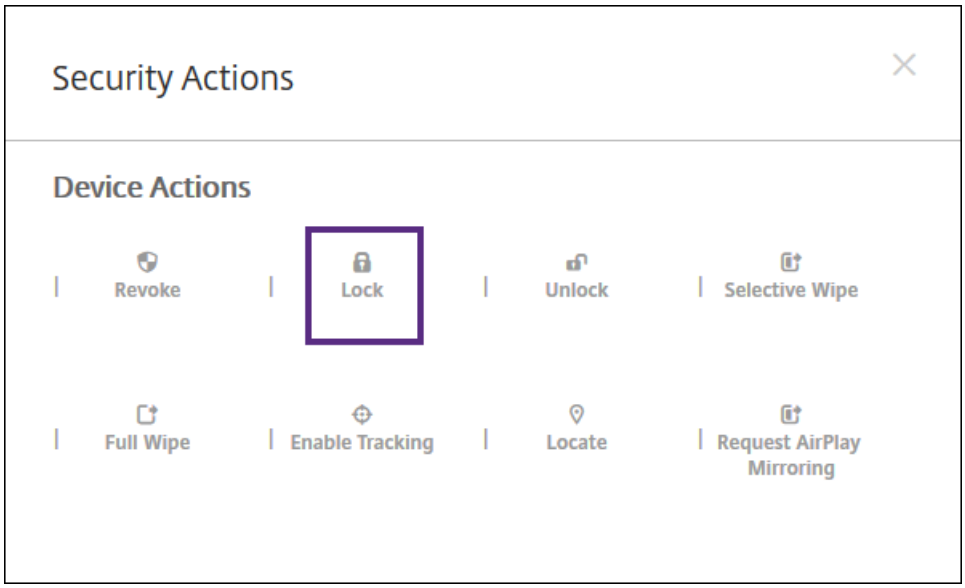
2. Wählen Sie das iOS-Gerät aus, das Sie sperren möchten.

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

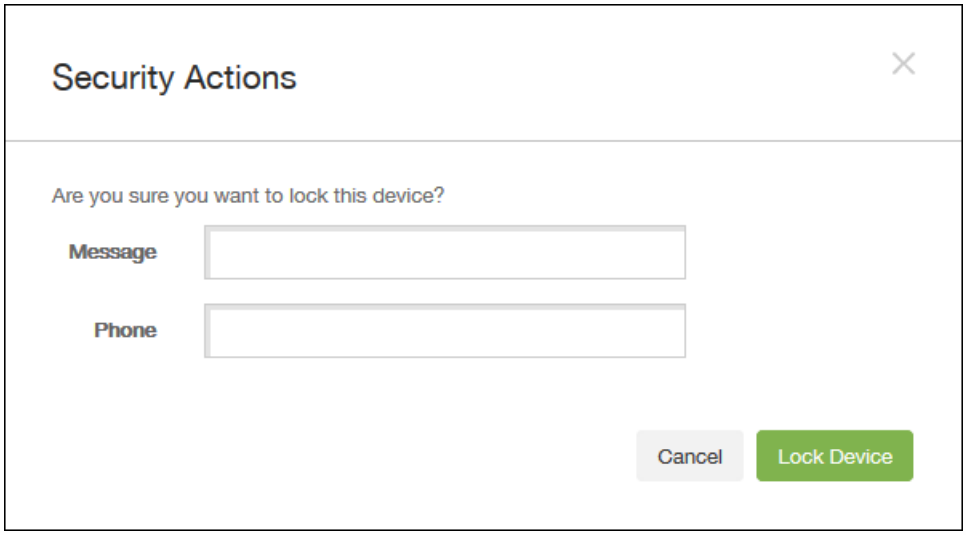




3. Wählen Sie im Menü "Optionen" die Option **Sicherung**. Das Dialogfeld **Sicherheitsaktionen** wird angezeigt.



4. Wählen Sie **Sperren**. Das Bestätigungsdialogfeld **Sicherheitsaktionen** wird angezeigt.



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

6. Klicken Sie auf **Gerät sperren**.

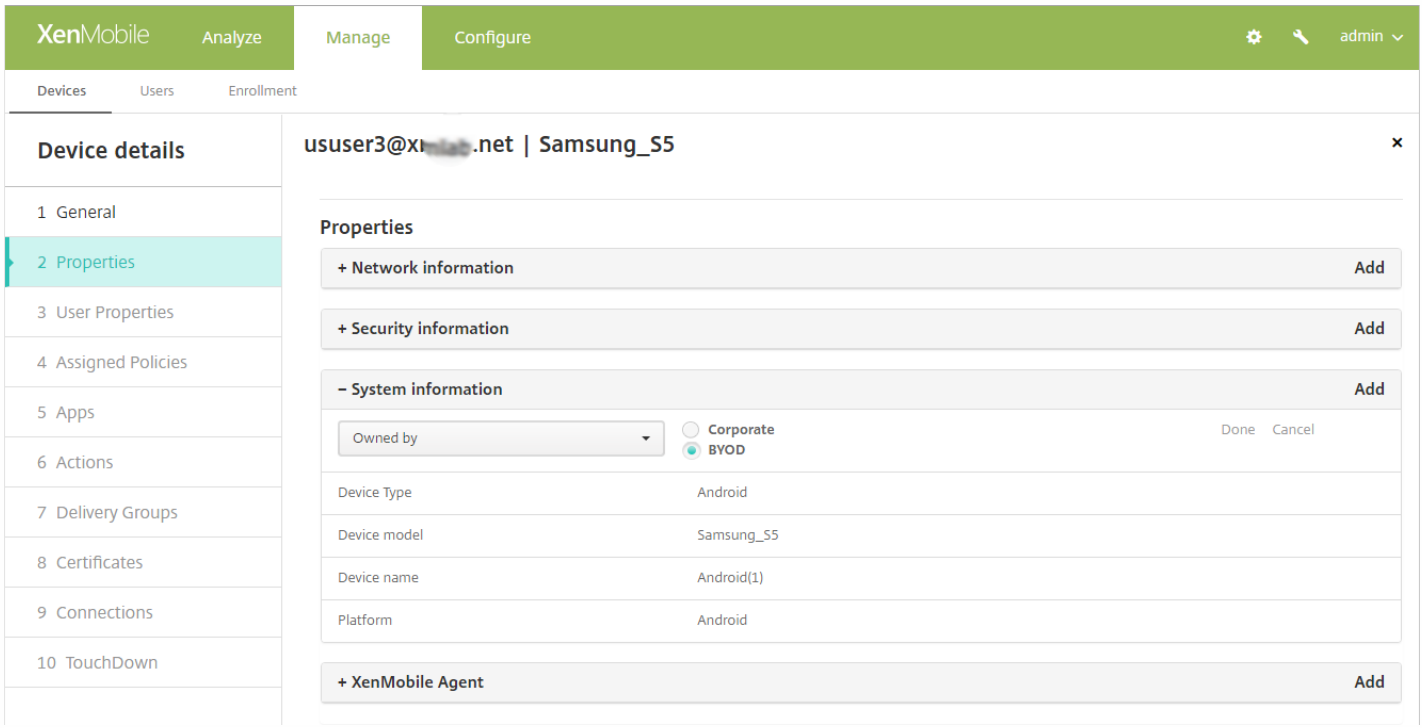
Manuelles Kennzeichnen von Benutzergeräten

Jul 28, 2016

Sie können Geräte in XenMobile auf folgende Weise manuell kennzeichnen:

- bei der Registrierung nach Einladung
- bei der Registrierung über das Selbsthilfeportal
- durch Hinzufügen von Gerätebesitz als Geräteeigenschaft

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



Geräte-Provisioningdateiformate

Jul 28, 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: Die Eigenschaft "propertyV;test;1;2" würde als "propertyV\;test\;1\;2" in der Provisioningdatei eingegeben werden.
- "SerialNumber" ist erforderlich, wenn "IMEI" nicht angegeben wird.
- "SerialNumber" ist für iOS-Geräte erforderlich, da die Seriennummer bei iOS als Geräte-ID verwendet wird.
- "IMEI" ist erforderlich, wenn "SerialNumber" nicht angegeben wird.
- Gültige Werte für "OperatingSystemFamily" sind: WINDOWS, ANDROID und iOS.

Beispiel einer Geräteprovisioningdatei

Die folgenden Zeilen beschreiben ein Gerät in einer Geräteprovisioningdatei.

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

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

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;

Der erste Eintrag bedeutet Folgendes:

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

Geräterichtlinien

Oct 13, 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. Eine Matrix mit Richtlinien nach Plattform finden Sie unter XenMobile-Geräterichtlinien nach Plattform.

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)

Sie können die folgenden Geräterichtlinien in XenMobile konfigurieren.

Name der Geräterichtlinie	**Beschreibung der Geräterichtlinie**
AirPlay-Spiegelung	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.
AirPrint	Mit einer AirPrint-Geräterichtlinie können Sie AirPrint-Drucker der AirPrint-Druckerliste auf den iOS-Geräten der Benutzer hinzufügen. 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.
Android for Work-App-Einschränkungen	Mit dieser Richtlinie können Sie Einschränkungen für Android for Work-Apps ändern. Hierfür müssen jedoch die folgenden Vorbereitungen getroffen werden: • Einrichtung von Android for Work auf Google Weitere Informationen finden Sie unter Verwalten von Geräten mit Android for Work.

	• Erstellen einer Reihe von Google Play-Anmeldeinformationen Weitere Informationen finden Sie unter Google Play-Anmeldeinformationen. • Erstellen eines Android for Work-Kontos Weitere Informationen finden Sie unter Erstellen eines Android for Work-Kontos. • Hinzufügen von Android for Work-Apps in XenMobile Weitere Informationen finden Sie unter Hinzufügen von Apps in XenMobile.
APN	Sie verwenden diese Richtlinie, wenn Ihr Unternehmen keinen Consumer-APN verwendet, über den mit mobilen Geräten eine Verbindung zum Internet hergestellt werden kann. Eine APN-Richtlinie definiert die Einstellungen für die Verbindung zwischen den Geräten und dem General Packet Radio Service (GPRS) eines Netzbetreibers. Diese Einstellung ist bei den meisten neueren Telefonen bereits definiert.
App-Zugriff	Mit einer 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.
App-Attribute	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.
App-Konfiguration	Mit dieser Richtlinie können Sie remote eine App Store-App konfigurieren, die eine verwaltete Konfiguration unterstützt, indem Sie eine XML-Konfigurationsdatei (eine sogenannte Eigenschaftenliste oder "plist") auf die iOS-Geräten der Benutzer bereitstellen, um verschiedene Einstellungen und Verhalten in der App zu konfigurieren.
App-Bestand	Mit einer App-Bestandsrichtlinie können Sie 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.
App-Sperre	Sie können in XenMobile mit einer Richtlinie eine Liste von Apps definieren, die auf einem Gerät ausgeführt werden dürfen, oder eine Liste von Apps, die auf einem Gerät blockiert werden. Sie können diese Richtlinie für iOS- und Android-Geräte konfigurieren, die Richtlinie funktioniert jedoch auf den Plattformen unterschiedlich. Auf einem iOS-Gerät können Sie beispielsweise nicht mehrere Apps blockieren.

	Hinweis: Obwohl die Geräterichtlinie auf den meisten Android L- und M-Geräten funktioniert, funktioniert App-Sperre nicht auf Android N oder neueren Geräten, da die erforderliche API von Google eingestellt wurde. Auf iOS-Geräten können Sie nur eine iOS-App pro Richtlinie auswählen. Dies bedeutet, dass Benutzer mit ihrem Gerät nur eine einzige App ausführen können. Außer den Optionen, die ausdrücklich zulässig sind, wenn die Richtlinie für die App-Sperre erzwungen wird, können Benutzer keine anderen Aktivitäten auf dem Gerät ausführen.
App-Netzwerkauslastung	Sie können Netzwerkauslastungsregeln festlegen, um vorzugeben, wie Netzwerke, z. B. mobile Datennetzwerken durch verwaltete Apps auf iOS-Geräten verwendet werden. Die Regeln gelten nur für verwaltete Apps. Verwaltete Apps sind Apps, die Sie über XenMobile auf den Geräten der Benutzer bereitstellen. Dazu gehören keine Apps, die Benutzer direkt auf ihre Geräte heruntergeladen haben und die nicht über XenMobile bereitgestellt wurden, und keine Apps, die bereits auf den Geräten installiert waren, als die Geräte bei XenMobile registriert wurden.
App-Einschränkungen	Mit dieser Richtlinie können Sie Sperrlisten mit Apps erstellen, für die Sie verhindern möchten, dass Benutzer sie auf Samsung KNOX-Geräten installieren, sowie Positivlisten mit Apps, die Benutzer installieren dürfen.
App-Tunneling	Sie können die App-Tunnelingrichtlinie konfigurieren, um die Dienstkontinuität und die Zuverlässigkeit bei der Datenübertragung für mobile Apps zu erhöhen. 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.
App-Deinstallation	Mit einer App-Deinstallationsrichtlinie können Sie aus verschiedenen Gründen Apps von Benutzergeräten entfernen. Gründe für das Entfernen von Apps sind beispielsweise, dass Sie 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.
Einschränkungen für App-Deinstallation	Mit dieser Richtlinie geben Sie die Apps an, die Benutzer deinstallieren können sowie die Apps, die sie nicht deinstallieren dürfen.
Browser	Sie können Browsergeräterichtlinien erstellen, mit denen Sie festlegen, ob auf den

	Benutzergeräten der Browser verwendet werden kann, oder um einzuschränken, welche Browserfunktionen auf den Benutzergeräten verwendet werden können. Auf Samsung-Geräten können Sie den Browser vollständig deaktivieren oder Popupfenster, JavaScript, Cookies, automatisches Ausfüllen und Betrugswarnungen aktivieren oder deaktivieren. Auf Android for Work-Geräten können Sie URLs einer Sperr- oder Positivliste hinzufügen und sichere Browserlesezeichen hinzufügen.
Kalender (CalDAV)	Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen eines Kalenderkontos (CalDAV) zu iOS- oder Mac OS X-Geräten einrichten, damit die Benutzer Kalendereinträge mit einem beliebigen Server, der CalDAV unterstützt, synchronisieren können.
Mobilfunk	Mit dieser Richtlinie können Sie mobile Netzwerkeinstellungen konfigurieren.
Verbindungsmanager	In XenMobile können Sie die Verbindungseinstellungen für Apps vorgeben, die automatisch eine Verbindung mit dem Internet und privaten Netzwerken herstellen. Diese Richtlinie ist nur für Microsoft Pocket PCs verfügbar.
Verbindungszeitplan	Diese Richtlinie ist für Android- und Windows Mobile-Geräte erforderlich, damit sie für die MDM-Verwaltung, App-Push und die Richtlinienbereitstellung wieder eine Verbindung mit dem XenMobile-Server herstellen. Wenn Sie diese Richtlinie nicht senden und Google GCM nicht aktiviert haben, stellt das Gerät eine Verbindung mit dem Server nicht wieder her. Daher ist es wichtig, diese Richtlinie per Push mit dem Basispaket für die registrierenden Geräte bereitzustellen.
Kontakte (CardDAV)	Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen eines iOS-Kontaktekontos (CardDAV) zu iOS- oder Mac OS X-Geräten einrichten, damit die Benutzer Kontaktdaten mit einem beliebigen Server, der CardDAV unterstützt, synchronisieren können.
Apps in Samsung Container kopieren	Sie können festlegen, dass für unterstützte Samsung-Geräte bereits auf dem Gerät installierte Apps in einen SEAMS-Container oder in einen Samsung KNOX-Container kopiert werden. In den SEAMS-Container kopierte Apps stehen auf dem Homebildschirm zur Verfügung, während Apps im KNOX-Container nur verfügbar sind, wenn die Benutzer sich am KNOX-Container anmelden.
Anmeldeinformationen	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. Jede Geräteplattform erfordert andere Werte. Diese werden im Artikel über die Richtlinien für Anmeldeinformationen beschrieben.

	Hinweis: Vor dem Erstellen dieser Richtlinie müssen Sie die Anmeldeinformationen für jede Plattform sowie jegliche Zertifikate und Kennwörter zusammenstellen.
Apps in Samsung Container kopieren	Sie können festlegen, dass für unterstützte Samsung-Geräte bereits auf dem Gerät installierte Apps in einen SEAMS-Container oder in einen Samsung KNOX-Container kopiert werden. Weitere Informationen zu den unterstützten Geräten finden Sie auf der Website von Samsung unter Von Samsung KNOX unterstützte Geräte: In den SEAMS-Container kopierte Apps stehen auf dem Homebildschirm zur Verfügung, während Apps im KNOX-Container nur verfügbar sind, wenn die Benutzer sich am KNOX-Container anmelden.
Anmeldeinformationen	Diese Richtlinie wird oft zusammen mit einer WiFi-Richtlinie verwendet. Sie ermöglicht Unternehmen, Authentifizierungszertifikate bereitzustellen, die für die Authentifizierung bei internen Ressourcen benötigt werden, die eine Zertifikatauthentifizierung erfordern.
Benutzerdefinierte XML	Sie können benutzerdefinierte XML-Richtlinien in XenMobile erstellen, wenn Sie die folgenden Features 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 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.
Dateien und Ordner löschen	Sie können in XenMobile eine Richtlinie erstellen, mit der bestimmte Dateien und Ordner von Windows Mobile-/CE-Geräten gelöscht werden.
Registrierungsschlüssel und -werte löschen	Sie können in XenMobile eine Richtlinie erstellen, mit der bestimmte Registrierungsschlüssel und -werte von Windows Mobile-/CE-Geräten gelöscht werden.
Integritätsnachweise für das Gerät	Sie können in XenMobile eine Richtlinie erstellen, dass Windows 10-Geräte ihren Integritätszustand melden müssen. Hierfür werden von den Geräten bestimmte

	Daten und Laufzeitinformationen an den Health Attestation Service (HAS) zur Analyse gesendet. Der HAS erstellt ein Health Attestation-Zertifikat und sendet es an das Gerät, von wo aus es an XenMobile gesendet wird. Basierend auf dem Inhalt des Health Attestation-Zertifikats kann XenMobile dann automatische Aktionen auslösen, die Sie zuvor eingerichtet haben. Vom HAS werden folgende Parameter geprüft: • AIK Present? • Bit Locker Status • Boot Debugging Enabled? • Boot Manager Rev List Version • Code Integrity Enabled? • Code Integrity Rev List Version • DEP Policy • ELAM Driver Loaded? • Issued At • Kernel Debugging Enabled? • PCR • Reset Count • Restart Count • Safe Mode Enabled? • SBCP Hash • Secure Boot Enabled? • Test Signing Enabled? • VSM Enabled? • WinPE Enabled? Weitere Informationen finden Sie auf der Microsoft-Website unter HealthAttestation CSP.
Gerätename	Mit einer Gerätenamensrichtlinie können Sie für iOS- und Mac OS X-Geräte die Namen einstellen, sodass Sie die Geräte leicht identifizieren können. Sie können Makros, Text oder eine Kombination daraus verwenden, um Gerätenamen festzulegen. Weitere Informationen zu Makros finden Sie unter Makros in XenMobile.
Unternehmenshub	Mit einer Unternehmenshub-Geräterichtlinie für Windows Phone können Sie Apps über den Unternehmenshub-Unternehmensstore 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 Hinweis: XenMobile unterstützt nur eine Unternehmenshubrichtlinie für einen

	Modus von Windows Phone-Worx Home. Zum Hochladen von Worx Home für Windows Phone für XenMobile Enterprise Edition dürfen Sie beispielsweise nicht mehrere Unternehmenshubrichtlinien mit mehreren Versionen von Worx Home für XenMobile Enterprise Edition erstellen. Sie können nur die erste Unternehmenshubrichtlinie bei der Geräteregistrierung bereitstellen.
Exchange	Mit XenMobile haben Sie zwei Optionen zum Bereitstellen von E-Mail. Sie können entweder ActiveSync-E-Mail mit der in einen Container verpackten WorxMail-App bereitstellen, oder Sie können diese MDM-Exchange-Richtlinie verwenden, um ActiveSync-E-Mail für den nativen E-Mail-Client auf dem Gerät aktivieren.
Dateien	Mit dieser Richtlinie können Sie XenMobile Skriptdateien hinzufügen, um bestimmte Funktionen für Benutzer auszuführen. Sie können auch Dokumentdateien hinzufügen, die Benutzern von Android-Geräten auf deren Geräten zugänglich sein sollen. Beim Hinzufügen einer Datei können Sie festlegen, in welchem Verzeichnis diese auf dem Gerät gespeichert werden soll. Wenn Sie beispielsweise Android-Benutzern ein Unternehmensdokument oder eine PDF-Datei zukommen lassen möchten, können Sie die Datei auf den Geräten bereitstellen und die Benutzer dann darüber informieren, wo sie ist. Sie können mit dieser Richtlinie die folgenden Dateitypen hinzufügen: • Textbasierte Dateien (.xml, .html, .py, usw.) • Andere Dateien (z. B. Dokumente, Präsentationen Bilder, Kalkulationstabellen) • Nur für Windows Mobile und Windows CE: mit MortScript erstellte Skriptdateien
Schriftart	Sie können in XenMobile diese Geräterichtlinie einrichten, um zusätzliche Schriftarten auf iOS- und Mac OS X-Geräten hinzuzufügen. Schriftarten müssen im Format TrueType (.ttf) oder OpenType (.oft) vorliegen. Schriftsammlungen (.ttc oder .otc) werden nicht unterstützt. Hinweis für iOS: Die Richtlinie gilt nur für Version 7.0 und höher.
iOS- und Mac OSx-Profilimport	Sie können XML-Dateien für die Konfiguration von iOS- und OS X-Geräten in XenMobile importieren. Die Datei enthält Gerätesicherheitsrichtlinien und -einschränkungen, die Sie mit Apple Configurator vorbereitet haben. Weitere Informationen über das Erstellen von Konfigurationsdateien mit Apple Configurator finden Sie auf der Apple-Website in der Apple Configurator-Hilfe.
Kiosk	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.
LDAP	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.
Speicherort	Mit der Ortungsrichtlinie können Sie den Standort der Geräte auf einer Karte abrufen, vorausgesetzt auf dem Gerät ist GPS für WorxHome aktiviert. Nachdem diese Richtlinie per Push auf den Geräten bereitgestellt wurde, können Administratoren einen Ortungsbefehl vom XenMobile-Server senden und das Gerät antwortet mit den Koordinaten des Standorts. Geofencing- und Gerätetrackingrichtlinien werden auch unterstützt.
E-Mail	Sie können in XenMobile eine E-Mail-Richtlinie hinzufügen, um ein E-Mail-Konto auf iOS- oder MAC OS X-Geräten zu konfigurieren.
Verwaltete Domänen	Sie können über diese Richtlinie verwaltete Domänen für E-Mail und den Safari-Browser definieren. Mit verwalteten Domänen können Sie zum Schutz von Unternehmensdaten steuern, welche Apps Dokumente, die mit Safari heruntergeladen wurden, öffnen können. Durch Angabe von URLs oder Unterdomänen geben Sie vor, wie Benutzer Dokumente, Anlagen und über Browser heruntergeladene Objekte öffnen können. Diese Richtlinie wird nur für betreute Geräte mit iOS 8 und höher unterstützt. Anweisungen zum Versetzen von iOS-Geräten in den betreuten Modus finden Sie unter Versetzen eines iOS-Geräts mit dem Apple Configurator in den betreuten Modus. Wenn ein Benutzer eine E-Mail an einen Empfänger sendet, dessen Domäne nicht auf der Liste der verwalteten E-Mail-Domänen steht, wird auf seinem Gerät eine Warnung angezeigt, dass die E-Mail an eine Person außerhalb der Domäne des Unternehmens gesendet wird. Versucht ein Benutzer ein Element (Dokument, Anlage oder heruntergeladenes Objekt) über Safari von einer Domänen auf der Liste der verwalteten Webdomänen zu öffnen, wird dieses Element in der geeigneten Unternehmensapp geöffnet. Steht das Element nicht auf der Liste der verwalteten Webdomänen, kann es in Unternehmensapps nicht geöffnet werden. Der Benutzer muss es stattdessen in einer privaten, nicht verwalteten App öffnen.

Microsoft Exchange ActiveSync	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. Jede Plattform erfordert andere Werte. Diese werden im Detail im Artikel über Microsoft Exchange ActiveSync in diesem Abschnitt beschrieben.
MDM-Optionen	Sie können in XenMobile eine Geräterichtlinie zum Verwalten der Aktivierungssperre des Features "Mein iPhone/iPad suchen" auf betreuten Geräten mit iOS 7.0 und höher erstellen. Anweisungen zum Versetzen von iOS-Geräten in den betreuten Modus finden Sie unter Versetzen von iOS-Geräten mit dem Apple Configurator in den betreuten Modus und iOS-Massenregistrierung. Das Feature "Mein iPhone/iPad suchen" umfasst eine Aktivierungssperre, die verhindert, dass verlorene oder gestohlene Geräte verwendet werden können, indem zum Deaktivieren des Features, Löschen der Daten auf dem Gerät, Reaktivieren und Nutzen des Geräts die Apple-ID und das Kennwort des Benutzers angefordert werden. In XenMobile können Sie das Erfordernis von Apple-ID und Kennwort umgehen, indem Sie die Aktivierungssperre über die MDM-Optionsrichtlinie aktivieren. Gibt ein Benutzer ein Gerät mit aktiviertem Feature "Mein iPhone suchen" zurück, können Sie es über die XenMobile-Konsole ohne Apple-Anmeldeinformationen verwalten.
Informationen zum Unternehmen	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.
Passcode	Mit einer Passcoderichtlinie können Sie einen PIN-Code oder ein Kennwort auf einem verwalteten Gerät durchsetzen. Sie können in der Passcoderichtlinie die Komplexität des Passcodes und Timeouts auf dem Gerät einstellen.
Persönlicher Hotspot	Mit dieser Richtlinie können Sie zulassen, dass Benutzer mit dem iOS-Feature für persönliche Hotspots eine Verbindung mit dem Internet per Mobilfunknetz herstellen, wenn sie nicht im Bereich eines WiFi-Netzwerks sind. Verfügbar für iOS 7.0 und höher.
Profilentfernung	Sie können eine Richtlinie zum Entfernen von App-Profilen in XenMobile erstellen. Bei ihrer Bereitstellung entfernt die Richtlinie das App-Profil von iOS- bzw. Mac OS X-Geräten.
Provisioningprofil	Beim Entwickeln und Signieren einer iOS-Unternehmensapp wird normalerweise ein Provisioningprofil eingeschlossen, das gemäß Apple für die Ausführung der App auf iOS-Geräten erforderlich ist. Wenn das Provisioningprofil fehlt oder abgelaufen ist, stürzt die App ab, wenn der Benutzer darauf tippt.

	Das Hauptproblem bei Provisioningprofilen besteht darin, dass sie ein Jahr, nachdem sie im Apple Developer-Portal generiert wurden, ablaufen und Sie die Ablaufdaten für alle Provisioningprofile auf allen registrierten iOS-Geräten nachverfolgen müssen. Zur Nachverfolgung von Ablaufdaten müssen Sie nicht nur die Daten selbst im Auge behalten, sondern auch wissen, welche Benutzer welche Version der einzelnen Apps verwenden. Zwei Lösungen bestehen darin, Provisioningprofile per E-Mail an die Benutzer zu senden oder sie über ein Webportal für Download und Installation zur Verfügung zu stellen. Beide funktionieren zwar, sind jedoch fehleranfällig, da Benutzer auf Anweisungen in einer E-Mail reagieren müssen oder das Webportal besuchen und das richtige Profil herunterladen und installieren müssen. Um die Benutzer mit diesem Vorgang nicht zu behelligen, können Sie in XenMobile Provisioningprofile über Geräterichtlinien installieren und entfernen. Fehlende oder abgelaufene Profile werden nach Bedarf entfernt und aktuelle Profile auf den Geräten installiert, sodass Apps bei Antippen normal geöffnet und verwendet werden können.
Provisioningprofilentfernung	Sie können iOS-Provisioningprofile mit Geräterichtlinien entfernen. Weitere Informationen zu Provisioningprofilen finden Sie unter Hinzufügen von Provisioningprofilen.
Proxy	Sie können in XenMobile eine Richtlinie zum Festlegen globaler HTTP-Proxy-Einstellungen für Geräte mit Windows Mobile/CE oder 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 Versetzen von iOS-Geräten mit dem Apple Configurator in den betreuten Modus.
Registrierung	In der Registrierung von Windows Mobile und Windows CE werden Daten zu Apps, Treibern, Benutzereinstellungen und Konfigurationseinstellungen gespeichert. Sie können in XenMobile Registrierungsschlüssel und -werte zum Verwalten von Windows Mobile-/CE-Geräten definieren.
Remote Support	Sie erstellen eine Remotesupportrichtlinie in XenMobile, um Remotezugriff auf Samsung KNOX-Geräte zu erhalten. Sie können Support zweierlei Art konfigurieren: • Einfacher Remotesupport: 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. • Premiumremotesupport: 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.
Einschränkungen	Die Einschränkungsrichtlinie gibt Administratoren verschiedene Optionen, Features und Funktionalität auf dem verwalteten Gerät zu sperren und zu steuern. Es gibt Hunderte von Einschränkungsoptionen für Geräte, vom Deaktivieren der Kamera oder des Mikrofons auf einem Gerät bis zum Durchsetzen von Roamingregeln und Steuern des Zugriffs auf Drittanbieterdienste, wie App-Stores. Sie können eine Geräterichtlinie in XenMobile hinzufügen, um Features und Funktionalität auf den Geräten der Benutzer einzuschränken. 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 EIN (zugelassen) festgelegt. Die wichtigsten Ausnahmen bilden das Feature "iOS-Sicherheit - Erzwingen" sowie alle Windows-Tablet-Features, die standardmäßig auf AUS bzw. "Beschränkt" festgelegt sind. Tipp: Alle Optionen, die Sie auf EIN festlegen, bedeuten, dass die Benutzer den entsprechenden Vorgang ausführen oder das Feature verwenden können. Beispiel: • Kamera: Bei Auswahl von EIN können Benutzer die Kamera auf Geräten verwenden. Bei Auswahl von AUS können Benutzer die Kamera auf ihren Geräten nicht verwenden. • Screenshots: Bei Auswahl von EIN können Benutzer Screenshots auf den Geräten erstellen. Bei Auswahl von AUS können Benutzer keine Screenshots auf den Geräten erstellen.
Roaming	Sie können in XenMobile eine Geräterichtlinie einrichten, um vorzugeben, ob auf iOS- bzw. Windows Mobile/CE-Geräten Sprach- und Datenroaming zugelassen wird. Wird Sprachroaming deaktiviert, dann wird Datenroaming automatisch auch deaktiviert. Hinweis zu iOS: Diese Richtlinie gilt nur für iOS 5.0 und höher.
Samsung SAFE-Firewall	Mit dieser Richtlinie können Sie die Firewall-Einstellungen für Samsung-Geräte konfigurieren. Sie geben dabei IP-Adressen, Ports und Hostnamen ein, auf die Geräte zugreifen können bzw. die Sie blockieren möchten. Sie können außerdem Proxy- und Proxyumleitungseinstellungen konfigurieren.
Samsung MDM-Lizenzschlüssel	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 SAFE API verfügbar" Wahr.
SCEP	Mit dieser Richtlinie können Sie iOS- und Mac OS X-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.
Sideloadingschlüssel	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 • Die Schlüsselaktivierung, die über die Befehlszeile erstellen, nachdem Sie den Produktschlüssel für das Sideloading erhalten haben
Signaturzertifikat	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-Tablets installieren können.

Single Sign-On-Konto	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.
Speicherverschlüsselung	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 Phone- und Android-Sony-Geräte erstellen. Jede Plattform erfordert andere Werte. Diese werden im Detail im Artikel über die Speicherverschlüsselung in diesem Abschnitt beschrieben.
Abonnierte Kalender	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.
Nutzungsbedingungen	Sie erstellen Geräterichtlinien mit Nutzungsbestimmungen in XenMobile, wenn die Benutzer die unternehmensspezifischen Richtlinien für Verbindungen mit dem Unternehmensnetzwerk akzeptieren sollen. 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. Sie müssen eine eigene Datei für jede angebotene Plattform-/Sprachkombination bereitstellen. Für Android- und iOS-Geräte müssen Sie PDF-Dateien bereitstellen. Für Windows-Geräte müssen Sie TXT-Dateien und zugehörige Bilddateien bereitstellen.
VPN	Für Kunden, die mit Legacy-VPN-Gatewaytechnologie den Zugriff auf Back-End-Systeme gewähren möchten, kann mit dieser VPN-Richtlinie ein Push der VPN-Gatewayverbindungsinformationen auf das Gerät durchgeführt werden. Eine Reihe von VPN-Anbietern werden über die Richtlinie unterstützt, einschließlich Cisco AnyConnect, Juniper sowie Citrix VPN. Diese Richtlinie kann mit einer

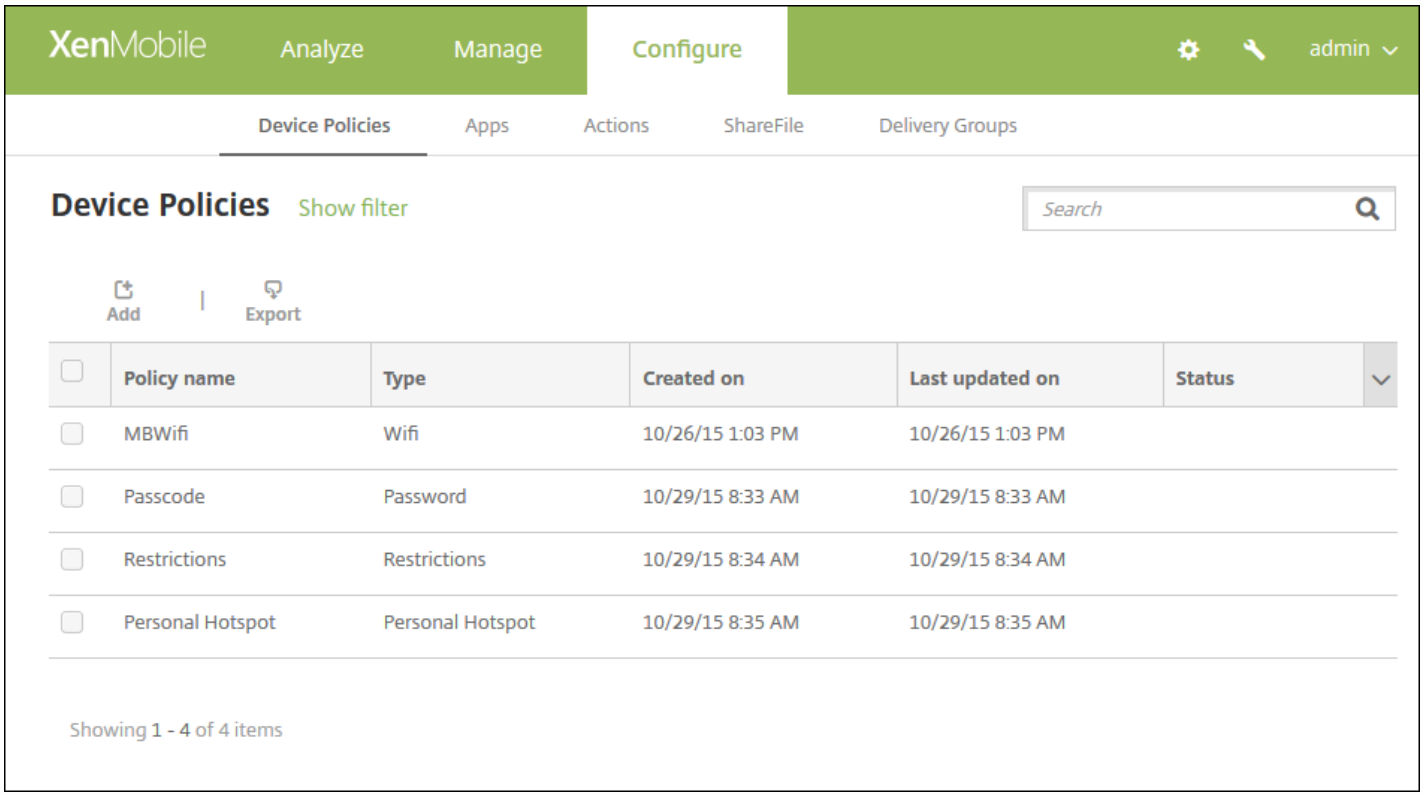
	Zertifizierungsstelle verbunden werden und VPN bei Bedarf aktivieren (vorausgesetzt, das VPN-Gateway unterstützt diese Option). Sie können in XenMobile eine Geräterichtlinie hinzufügen, um die Einstellungen für ein VPN (virtuelles privates Netzwerk) für eine sichere Verbindung zwischen Geräten und Unternehmensressourcen zu konfigurieren. Jede Plattform erfordert andere Werte. Diese werden im Detail im VPN-Artikel in diesem Abschnitt beschrieben.
Hintergrundbild	Sie können eine PNG- oder JPG-Datei hinzufügen, um Hintergrundbilder auf dem Sperr- und/oder Homebildschirm von iOS-Geräten festzulegen. In iOS 7.1.2 und höher verfügbar. Zum Verwenden verschiedener Bilder auf iPads und iPhones müssen Sie unterschiedliche Richtlinien erstellen und den entsprechenden Benutzern bereitstellen.
Webinhaltsfilterung	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 dazu, wie Sie Geräte in den betreuten Modus versetzen, finden Sie unter Versetzen von iOS-Geräten mit dem Apple Configurator in den betreuten Modus.
Webclip	Mit dieser Richtlinie können Sie Verknüpfungen oder Webclips in Websites platzieren, sodass sie neben den Apps auf den Benutzergeräten angezeigt werden. Für iOS, Mac OS X- und Android-Geräte können Sie Symbole für die Webclips angeben; für Windows Tablet ist nur eine Beschriftung und eine URL erforderlich.
WiFi	Mit der WiFi-Richtlinie können Administratoren bequem WiFi-Routerdetails, SSID, Authentifizierungs- und Konfigurationsdaten per Push auf ein verwaltetes Gerät bereitstellen. 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. Sie können WiFi-Einstellungen für Benutzer der zugeordneten Plattformen konfigurieren, die auf der linken Seite aufgelistet werden. Jede Plattform erfordert andere Werte. Diese werden im Detail im WiFi-Artikel in diesem Abschnitt beschrieben.
Windows CE-Zertifikat	Fügen Sie diese Richtlinie hinzu, um Windows Mobile/CE-Zertifikate von einer externen PKI zu erstellen und auf Benutzergeräten bereitzustellen. Weitere Informationen über Zertifikate und PKI-Entitäten, finden Sie unter Zertifikate.

Worx Store	Sie können in XenMobile eine Richtlinie erstellen, mit der Sie angeben, ob auf iOS-, Android- und Windows Tablet-Geräten ein WorxStore-Webclip auf dem Homebildschirm des Geräts angezeigt wird.
XenMobile-Optionen	Sie fügen eine XenMobile-Optionsrichtlinie hinzu, um das Worx Home-Verhalten für Verbindungen zwischen XenMobile und Android- bzw. Windows Mobile/CE-Geräten zu konfigurieren.
XenMobile-Deinstallation	Sie können in XenMobile diese Geräterichtlinie hinzufügen, um XenMobile von Android- und Windows Mobile-/CE-Geräten zu deinstallieren. Wenn diese Richtlinie bereitgestellt wird, entfernt sie XenMobile von allen Geräten in der Bereitstellungsgruppe.

Geräterichtlinienseite in der Konsole

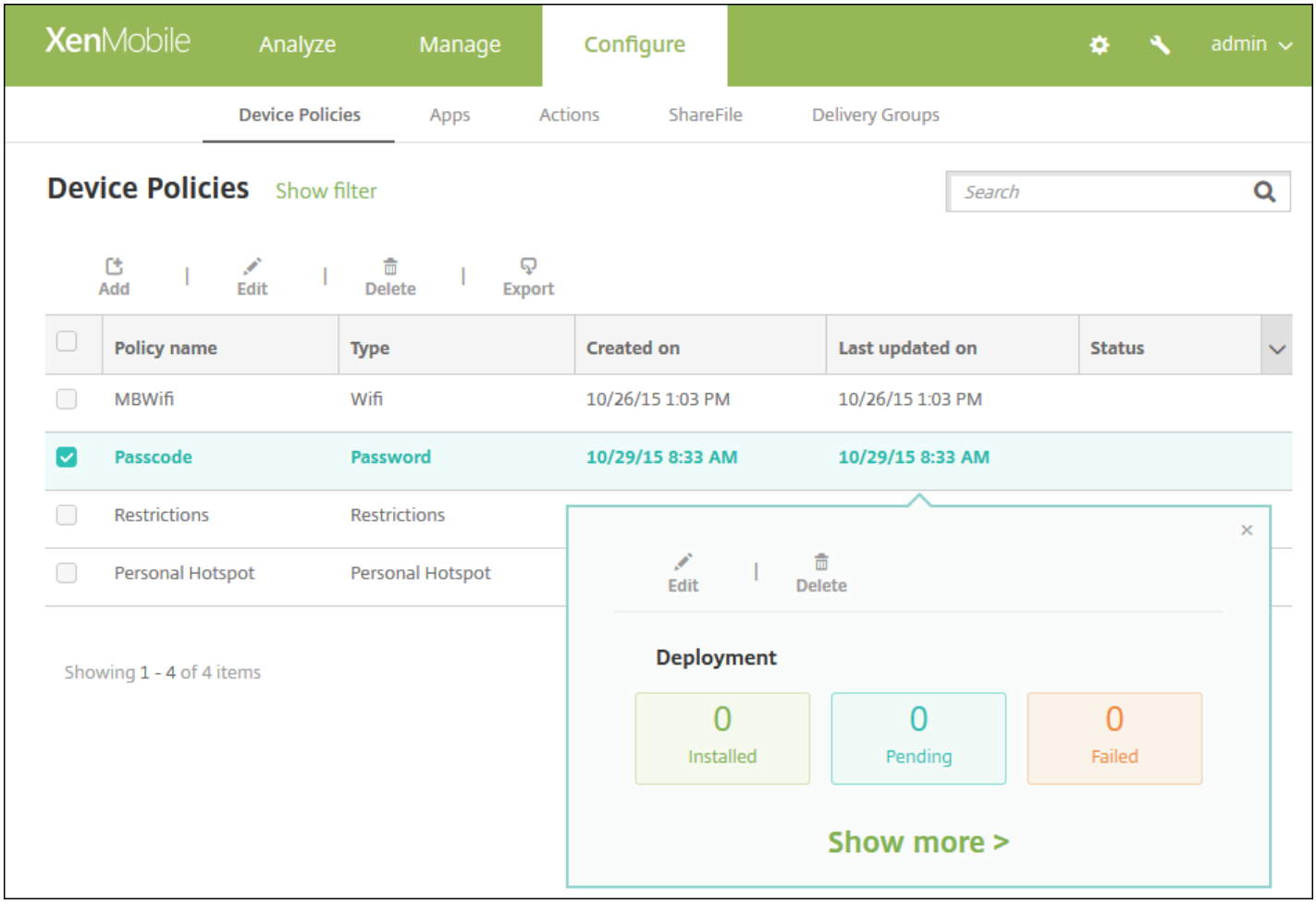
Die Arbeit mit Geräterichtlinien erfolgt in der XenMobile-Konsole auf der Seite **Geräterichtlinien**. Zum Aufrufen der Seite **Geräterichtlinien** klicken Sie auf **Konfigurieren > Geräterichtlinien**. Auf dieser Seite können Sie neue Richtlinien hinzufügen, den Status vorhandener Richtlinien prüfen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

Die Seite **Geräterichtlinien** enthält eine Tabelle aller aktuellen Richtlinien.



Zum Bearbeiten oder Löschen einer Richtlinie auf der Seite **Geräterichtlinien** 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

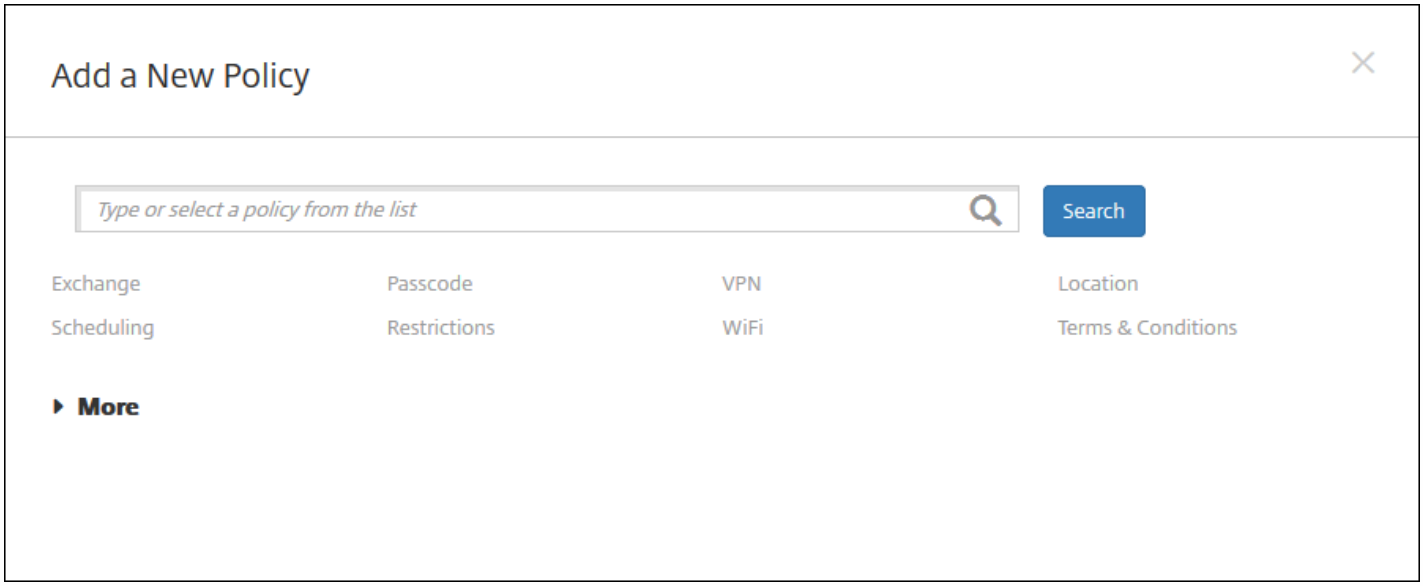
klicken, um das Menü rechts neben dem Eintrag einzublenden. Wenn Sie auf **Mehr anzeigen** klicken, werden die Richtliniendetails angezeigt.



Hinzufügen einer Geräterichtlinie

1. Klicken Sie auf der Seite **Geräterichtlinien** auf **Hinzufügen**.

Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt. Mit **Mehr** können Sie weitere Richtlinien einblenden.

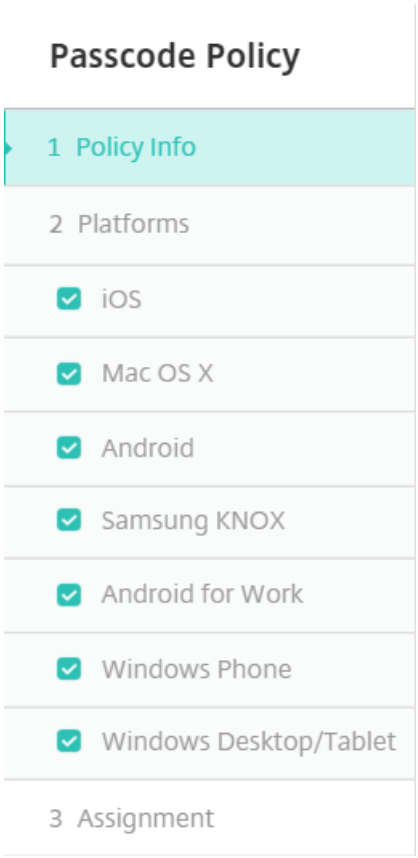


2. Zur Suchen der gewünschten Richtlinie haben Sie folgende Möglichkeiten:

- Klicken Sie auf die Richtlinie.
  Die Seite **Richtlinieninformationen** 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 **Richtlinieninformationen** zu öffnen.
  Wichtig: Wenn die ausgewählte Richtlinie im Bereich **Mehr** ist, wird sie nur angezeigt, wenn Sie **Mehr** 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.

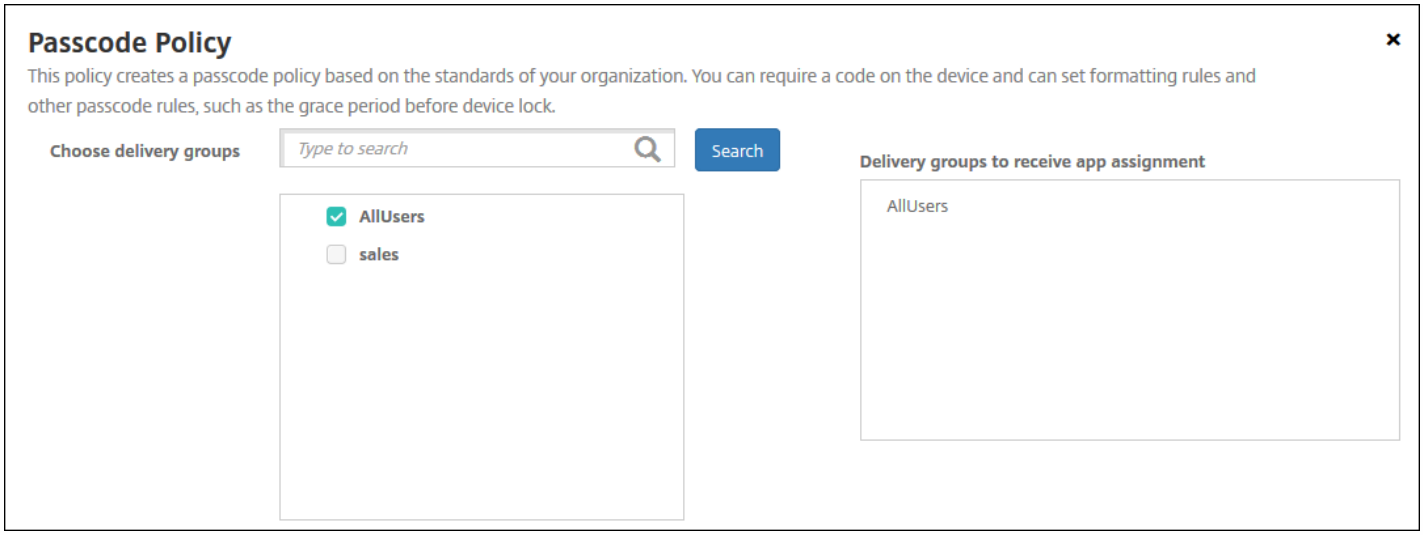


4. Geben Sie die erforderlichen Informationen auf der Seite **Richtlinieninformationen** ein und klicken Sie dann auf **Weiter**. Die Seite **Richtlinieninformationen** enthält Informationen zum Identifizieren und Verfolgen von Richtlinien (z. B. Richtlinienname). Diese Seite ist bei allen Richtlinien 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 **Weiter**, um zur nächsten Plattformseite bzw., wenn alle Plattformseiten ausgefüllt sind, zur Seite **Zuweisung** zu gehen.

6. Wählen Sie auf der Seite **Zuweisungen** die Bereitstellungsgruppen aus, auf die die Richtlinie angewendet werden soll. Wenn Sie auf eine Bereitstellungsgruppe klicken, wird deren Name im Feld **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

Hinweis: Das "Feld Bereitstellungsgruppen für App-Zuweisung" wird erst eingeblendet, wenn Sie auf eine Bereitstellungsgruppe klicken.



7. Klicken Sie auf **Speichern**.

Die Richtlinie wird der Tabelle **Gerätericht linien** hinzugefügt.

Bearbeiten oder Löschen einer Gerätericht linie

1. Aktivieren Sie in der Tabelle **Gerätericht linien** das Kontrollkästchen neben die Richtlinie, die Sie bearbeiten oder löschen möchten.

2. Klicken Sie auf **Bearbeiten** oder **Löschen**.

- Wenn Sie auf **Bearbeiten** klicken, bearbeiten Sie beliebige Einstellungen nach Bedarf.
- Wenn Sie auf **Löschen** klicken, wird ein Bestätigungsdialogfeld angezeigt. Klicken Sie darin erneut auf **Löschen**.

XenMobile-Geräterichtlinien nach Plattform

Aug 22, 2016

Zum Anzeigen einer Liste der Richtlinien nach Plattform laden Sie die PDF-Datei Geräterichtlinien nach Plattform herunter.

Zum Hinzufügen und Konfigurieren von Geräterichtlinien verwenden Sie die Option **Konfigurieren > Geräterichtlinien** der XenMobile-Konsole.
XenMobile 10.3 unterstützt Geräterichtlinien für folgende Plattformen:

- Amazon
- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android for Work
- Android
- Samsung SAFE
- Samsung SEAMS
- Windows Phone 8/Windows 10 Mobile
- Windows 8 und Windows 10 Desktop/Tablet (.86)

> ## Hinweis
>
> Unterstützung für Symbian-Geräte gibt es in XenMobile 10.3 nicht mehr.

Geräterichtlinie für die AirPlay-Synchronisierung

Aug 22, 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.

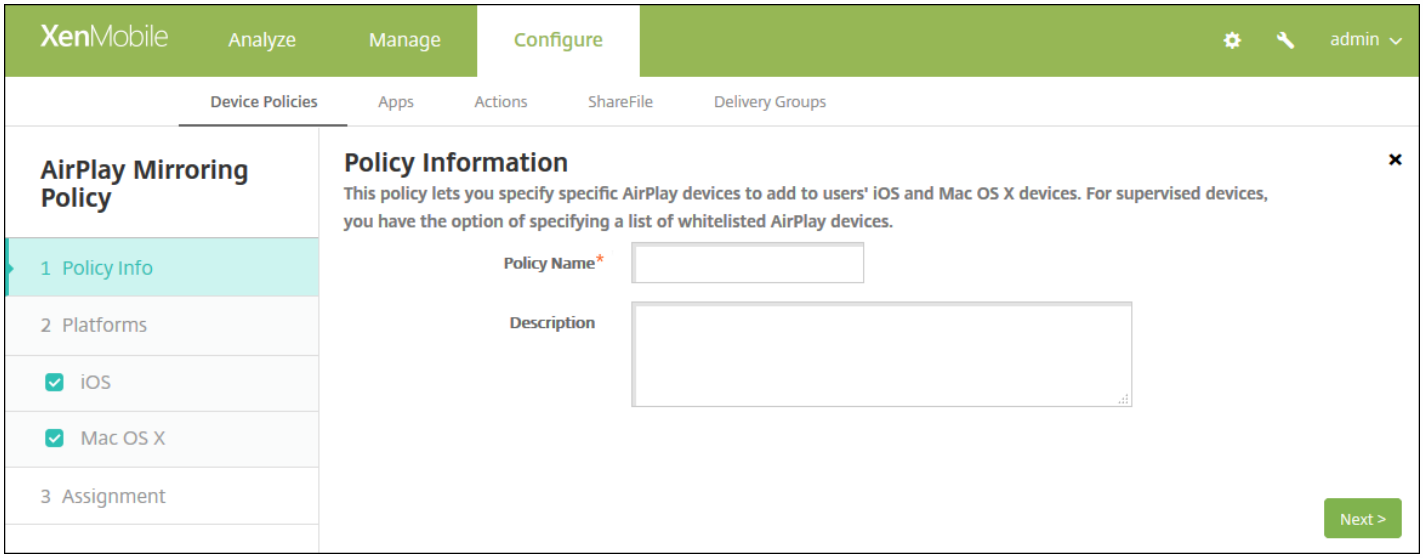
Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen spezifischer AirPlay-Geräte (z. B. Apple TV oder einen anderen Mac-Computer) einrichten und iOS-Geräten hinzufügen. Zudem können Sie Geräte zu einer Positivliste überwachter Geräte hinzufügen, sodass Benutzer nur die AirPlay-Geräte auf der Positivliste verwenden können. Informationen zum Versetzen von Geräten in den betreuten Modus finden Sie unter Versetzen von iOS-Geräten 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 **Konfigurieren > Geräterichtlinien**. Die Seite **Geräterichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Klicken Sie auf **Mehr** und dann unter **Endbenutzer** auf **AirPlay-Synchronisierung**. Die Seite **AirPlay-Synchronisierung** wird angezeigt.



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

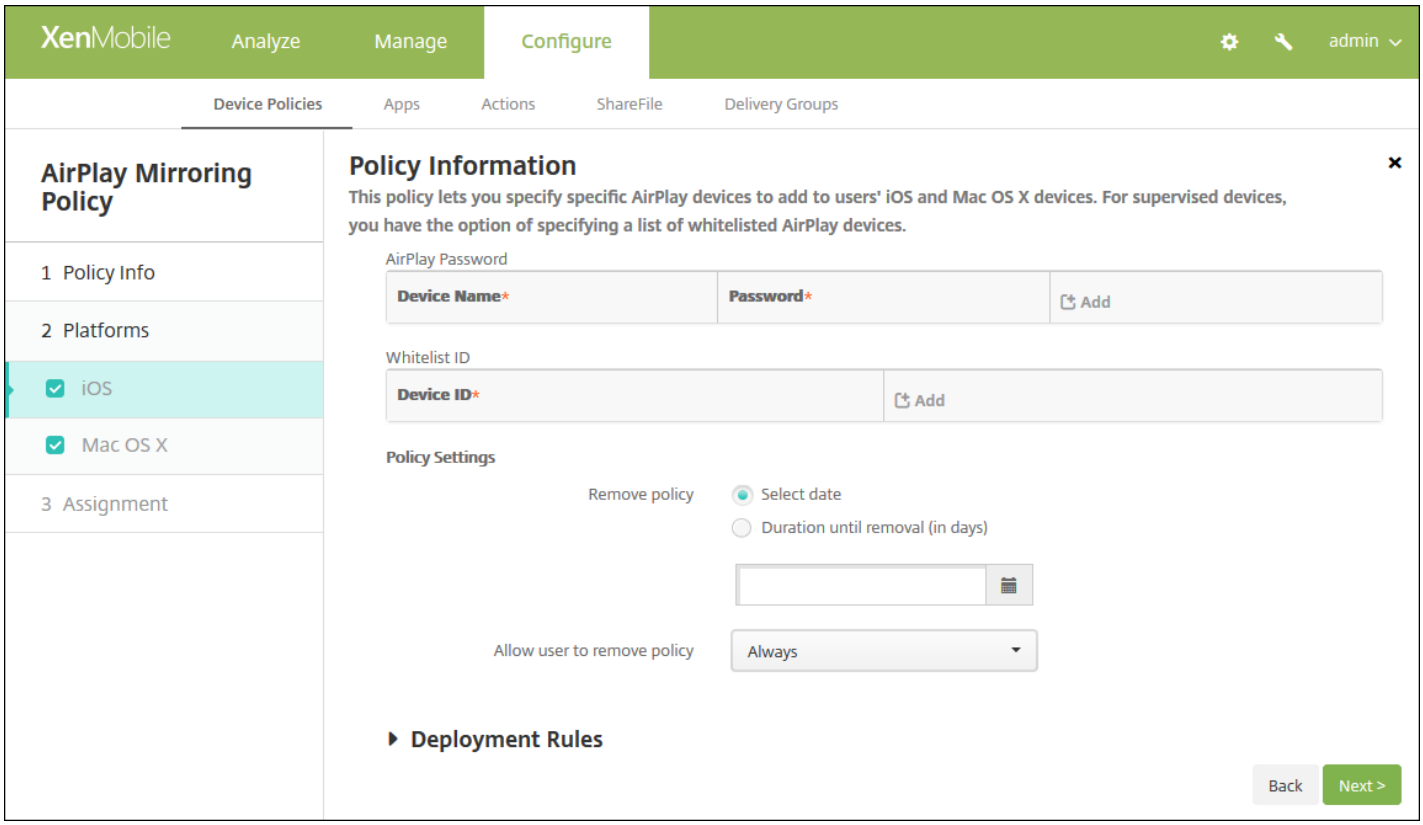
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

Konfigurieren von iOS-Einstellungen



Konfigurieren Sie folgende Einstellungen:

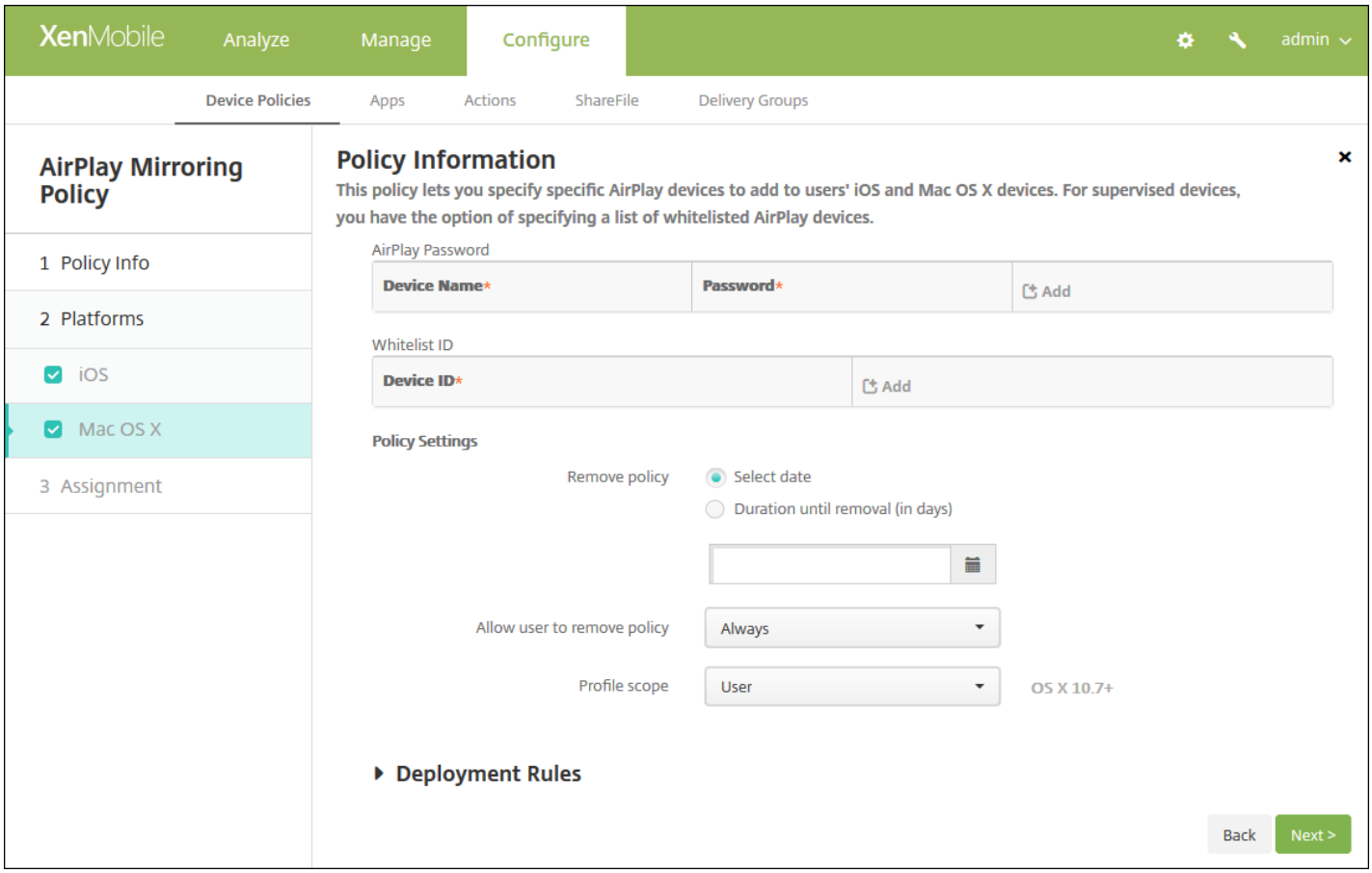
- **AirPrint-Kennwort**: Für jedes Gerät, das Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Geräte-ID**: Geben Sie die Hardware-Adresse (MAC-Adresse) im Format xx: xx: xx: xx: xx: xx ein. Bei diesem Feld wird nicht zwischen Groß- und Kleinschreibung unterschieden.
  - **Kennwort**: Geben Sie optional ein Kennwort für das Gerät ein.
  - Klicken Sie auf **Hinzufügen**, um das Gerät hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Positivlisten-ID:** Diese Liste wird bei nicht betreuten Geräten ignoriert. Die Gerätekennungen in dieser Liste repräsentieren die einzigen AirPlay-Geräte, die Benutzern zur Verfügung stehen. Für jedes AirPlay-Gerät, das Sie der Liste hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Geräte-ID**: Geben Sie die Gerätekennung im Format xx:xx:xx:xx:xx:xx ein. Bei diesem Feld wird nicht zwischen Groß- und Kleinschreibung unterschieden.
  - Klicken Sie auf **Hinzufügen**, um das Gerät hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

    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 **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Richtlinieneinstellungen**
  - Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.

- Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
- Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

Konfigurieren von Mac OS X-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **AirPrint-Kennwort**: Für jedes Gerät, das Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Geräte-ID**: Geben Sie die Hardware-Adresse (MAC-Adresse) im Format xx: xx: xx: xx: xx: xx ein. Bei diesem Feld wird nicht zwischen Groß- und Kleinschreibung unterschieden.
  - **Kennwort**: Geben Sie optional ein Kennwort für das Gerät ein.
  - Klicken Sie auf **Hinzufügen**, um das Gerät hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.
- **Positivlisten-ID:** Diese Liste wird bei nicht betreuten Geräten ignoriert. Die Gerätekennungen in dieser Liste repräsentieren die einzigen AirPlay-Geräte, die Benutzern zur Verfügung stehen. Für jedes AirPlay-Gerät, das Sie der Liste hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Geräte-ID**: Geben Sie die Gerätekennung im Format xx:xx:xx:xx:xx:xx ein. Bei diesem Feld wird nicht zwischen Groß- und Kleinschreibung unterschieden.
  - Klicken Sie auf **Hinzufügen**, um das Gerät hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

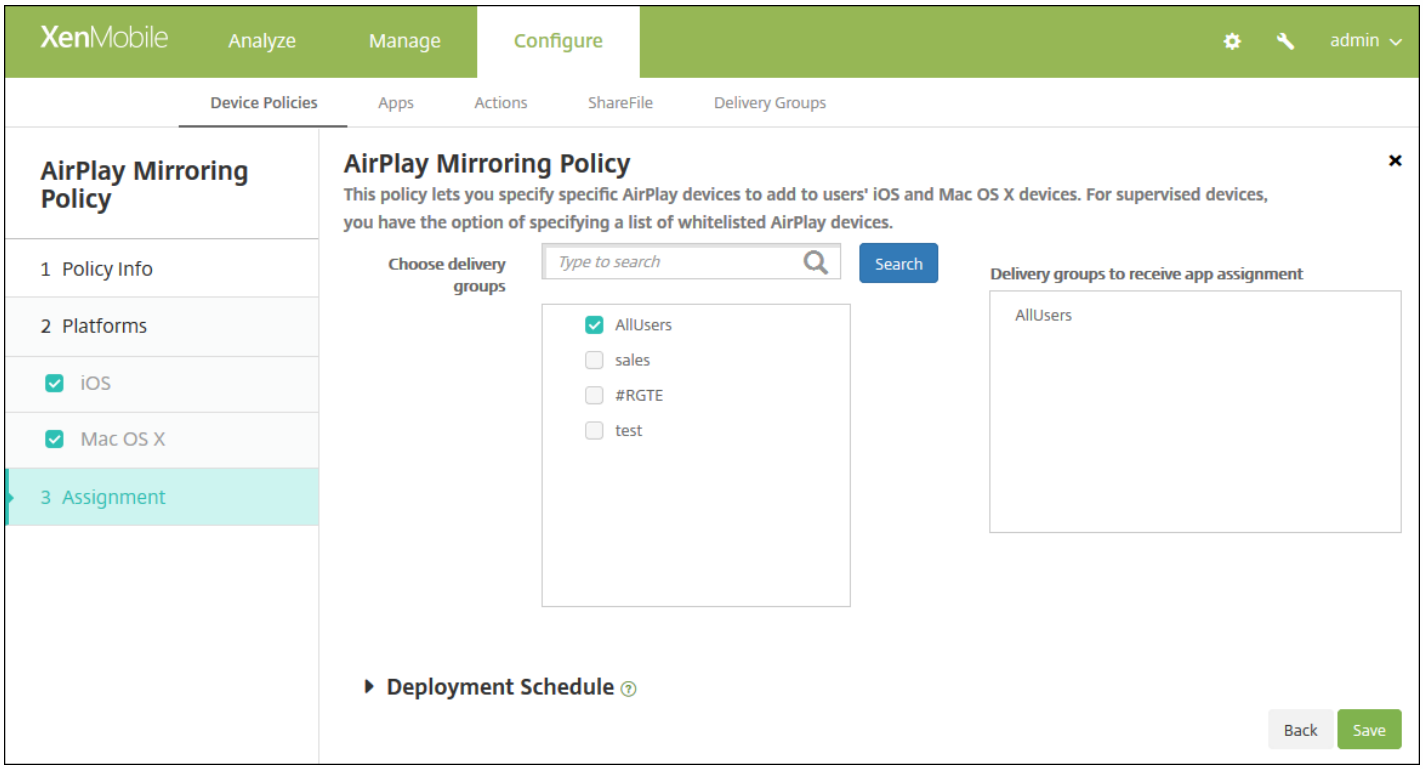
    Hinweis: Zum Löschen eines vorhandenen Geräts zeigen Sie auf dessen Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, um ihn beizubehalten.

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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

- **Richtlinieneinstellungen**
  - Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.
  - Klicken Sie neben **Gültigkeitsbereich für Profil** auf **Benutzer** oder **System**. Der Standardwert ist **Benutzer**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die AirPlay-Synchronisierungsrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.

- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen gemachten Änderungen werden auf alle Plattformen angewendet. Ausnahme bildet die Einstellung **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

AirPrint-Geräterichtlinie

Jul 28, 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.

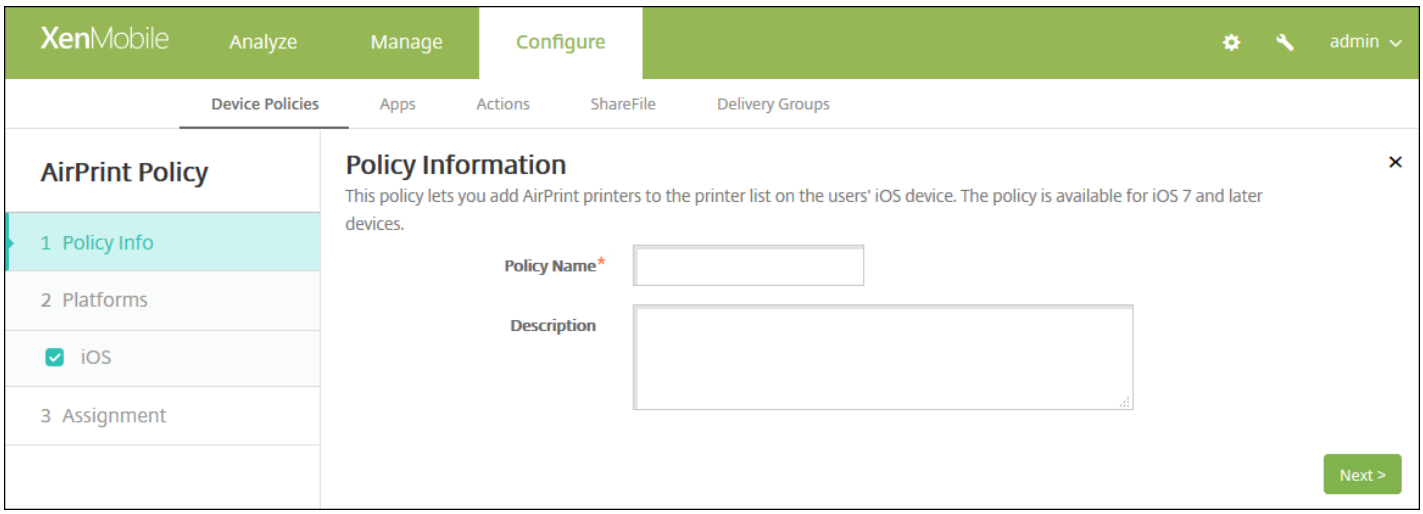
Hinweis:

- 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 **Konfigurieren > Geräterichtlinien**. Die Seite **Geräterichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

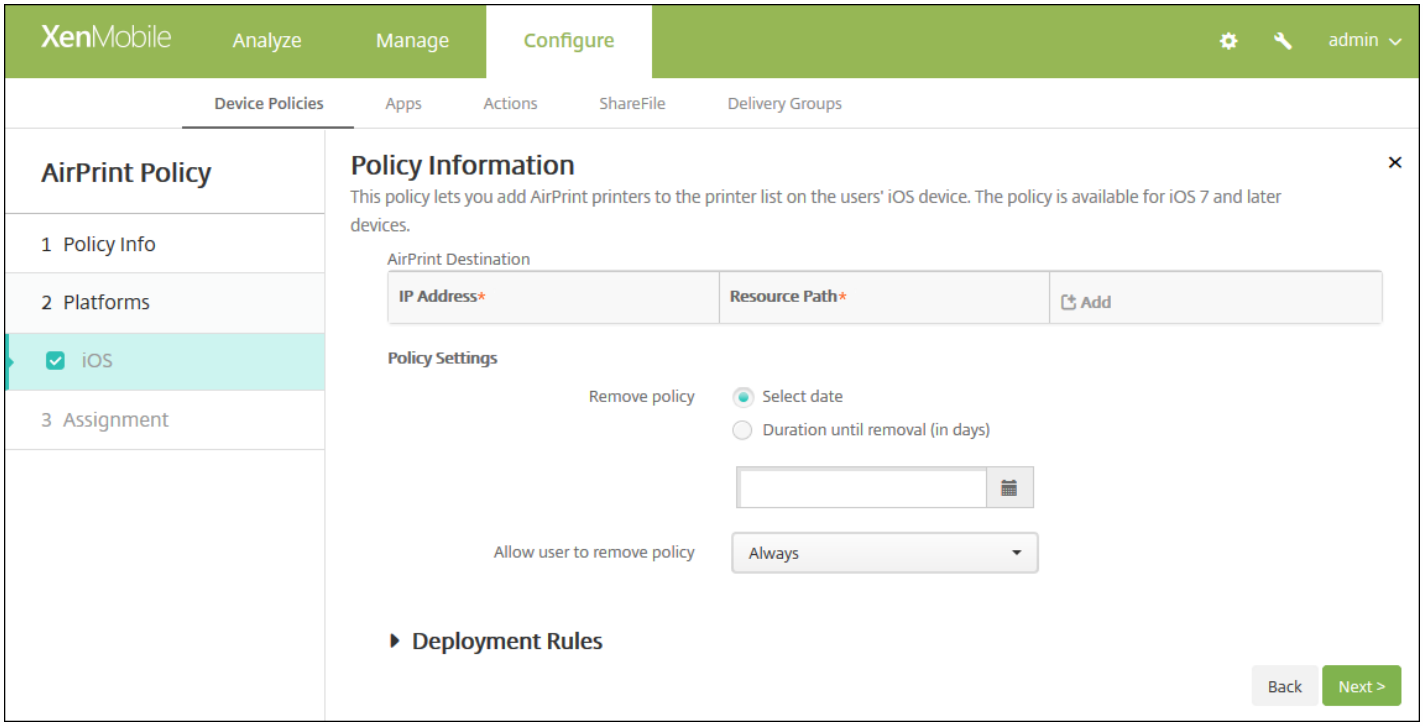
3. Klicken Sie auf **Mehr** und dann unter **Endbenutzer** auf **AirPrint**. Die Seite für die Richtlinieninformationen der Richtlinie **AirPrint** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite mit den Plattforminformationen für **iOS** wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:

- **AirPrint-Ziel**: Für jedes AirPrint-Ziel, das Sie hinzufügen möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **IP-Adresse**: Geben Sie die IP-Adresse des AirPrint-Druckers ein.
  - **Ressourcenpfad**: 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.
  - Klicken Sie auf **Speichern**, um den Drucker hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

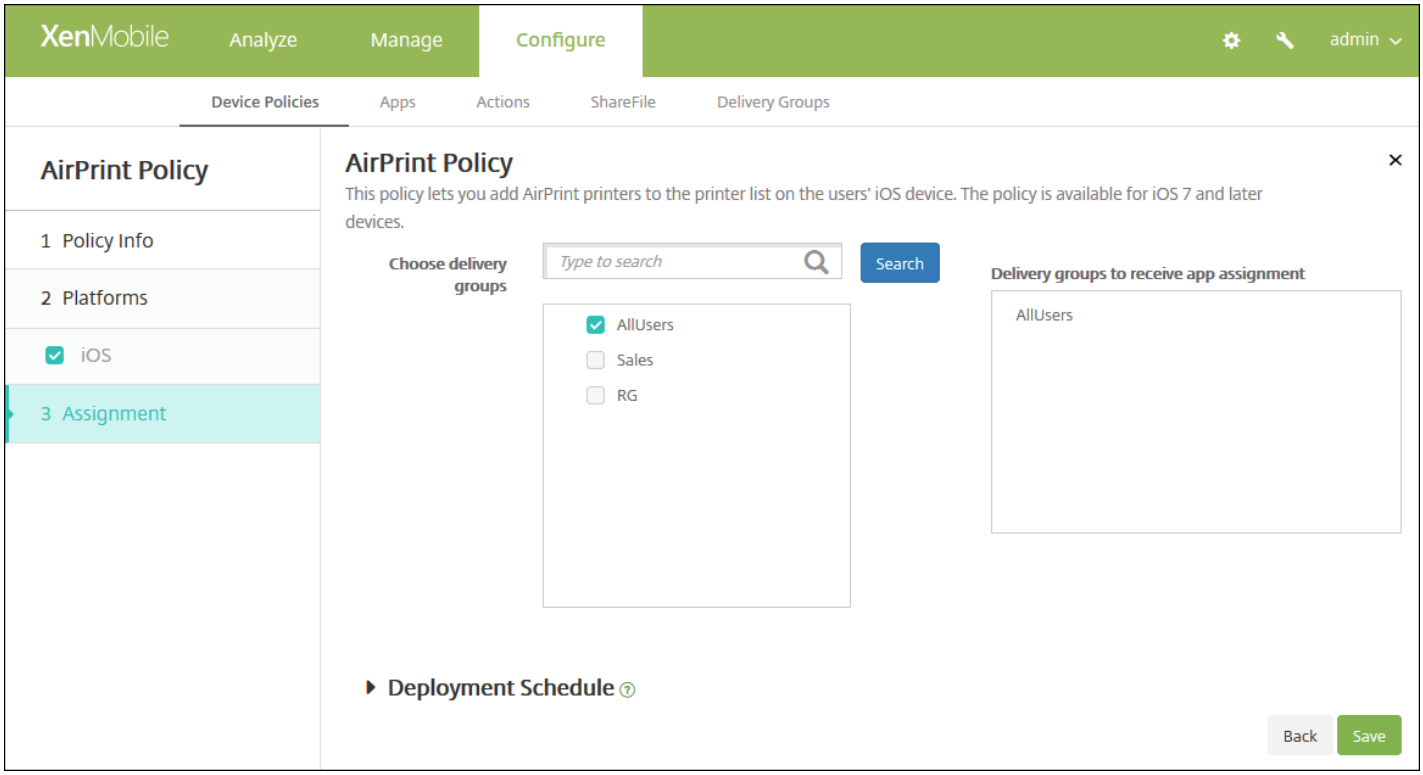
    Hinweis: Zum Löschen eines vorhandenen Druckers zeigen Sie auf dessen Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf "Löschen" zum Löschen des Eintrags oder auf "Bearbeiten", um ihn beizubehalten.

    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 "Speichern", um die Änderungen zu speichern oder auf "Abbrechen", um den Vorgang abzubrechen.

- **Richtlinieneinstellungen**
  - Klicken Sie unter **Richtlinieneinstellungen** neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die AirPrint-Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Einschränkungsrichtlinie für Android for Work-Apps

Jul 28, 2016

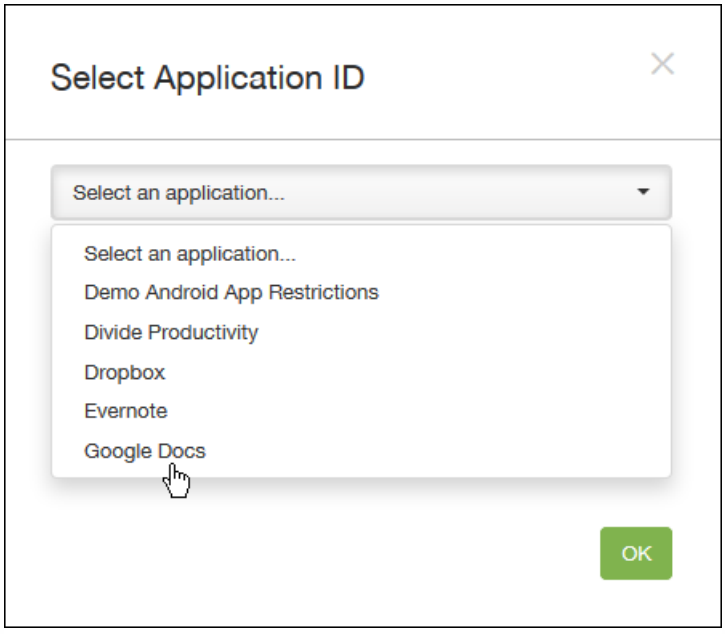
Sie können Einschränkungen für Android for Work-Apps ändern. Hierfür müssen jedoch die folgenden Vorbereitungen getroffen werden:

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

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

2. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.

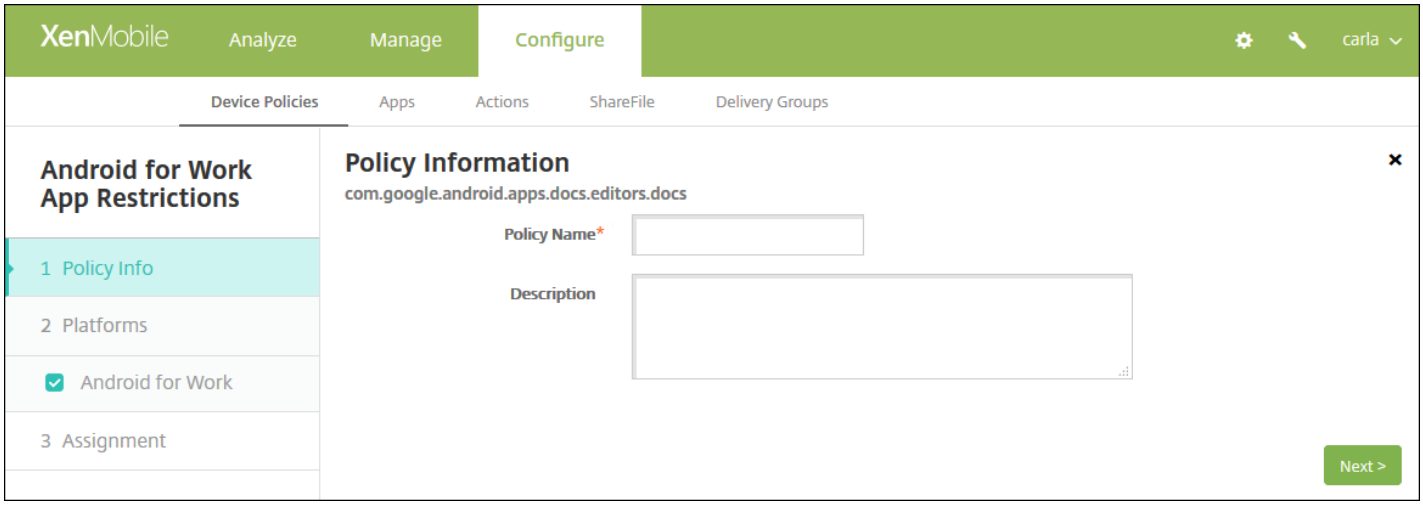
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **Android for Work - Einschränkungen**. Ein Dialogfeld wird angezeigt, in dem Sie zum Auswählen der App aufgefordert werden.



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

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

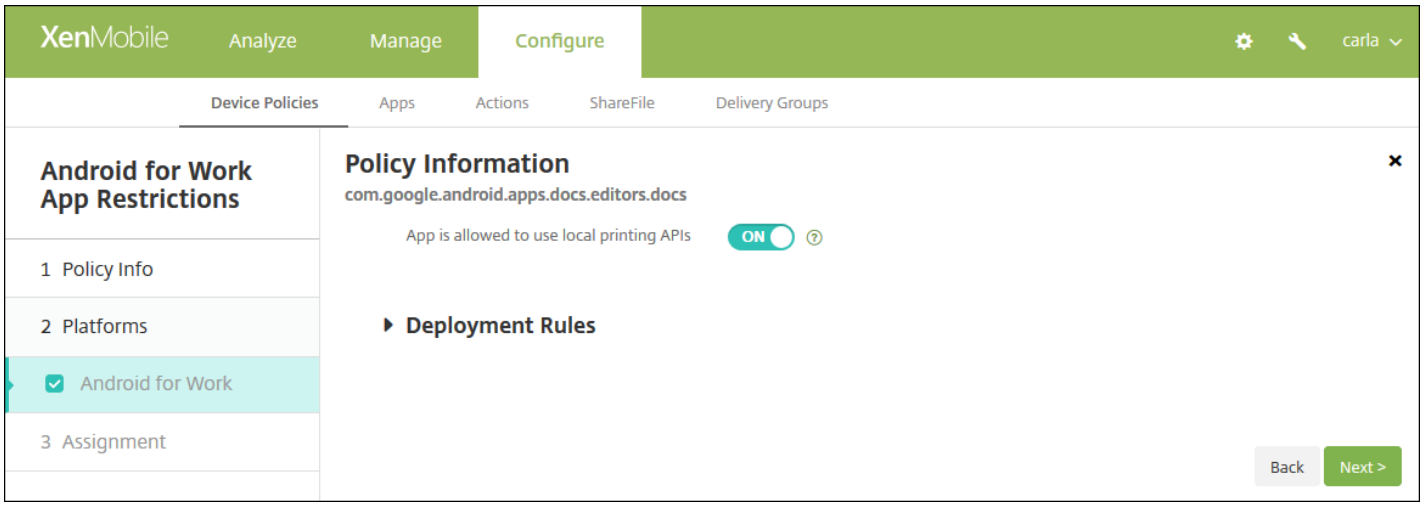
Einschränkungen angezeigt.



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

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

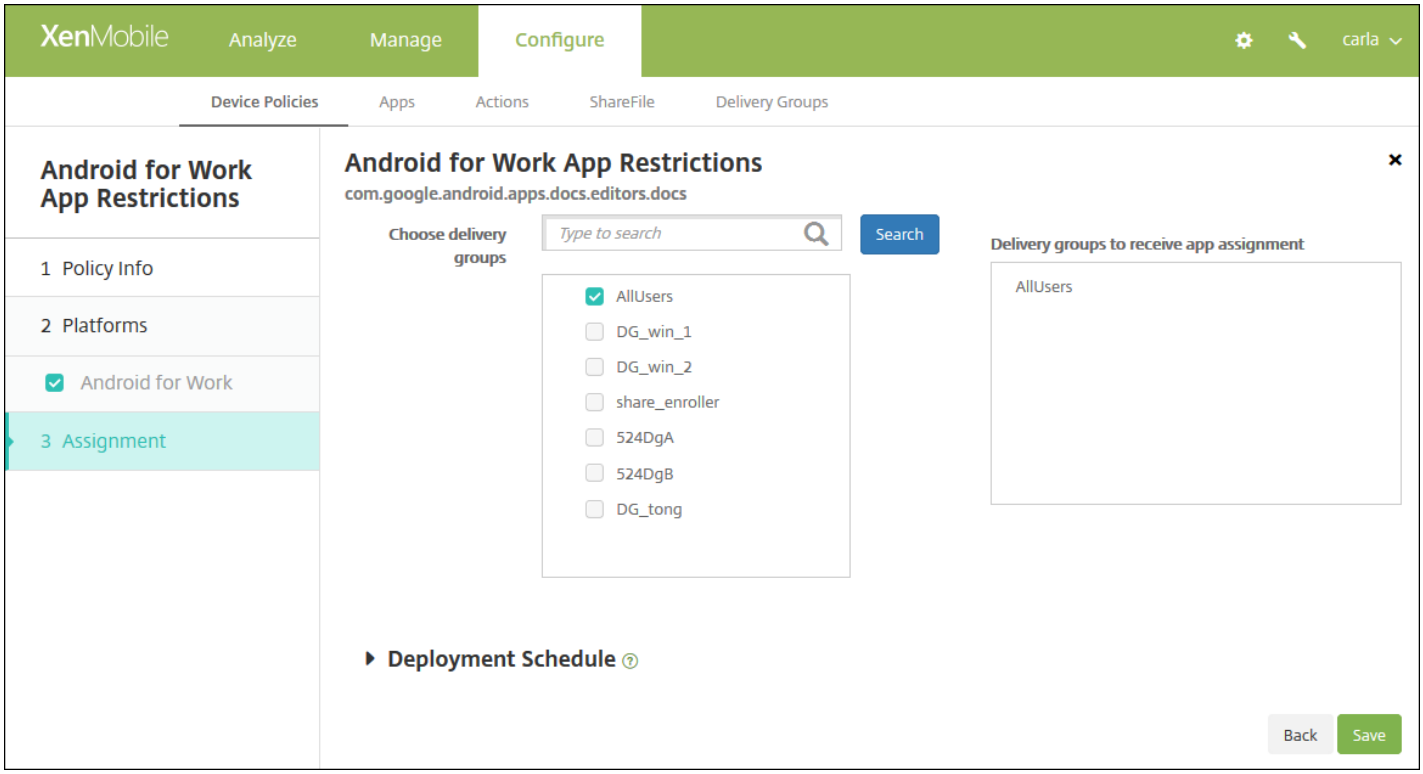
6. Klicken Sie auf **Weiter**. Die Plattformseite wird angezeigt.



7. Konfigurieren Sie die Einstellungen für die ausgewählte App. Welche Einstellungen angezeigt werden, hängt von den Einschränkungen ab, die der ausgewählten App zugeordnet sind.

8. Konfigurieren der Bereitstellungsregeln

9. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die App-Einschränkungsrichtlinie für Android for Work wird angezeigt.



10. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

11. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **oder auf Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen gemachten Änderungen werden auf alle Plattformen angewendet. Ausnahme bildet die Einstellung **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

12. Klicken Sie auf **Speichern**.

APN-Geräterichtlinien

Jul 28, 2016

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

iOS-Einstellungen

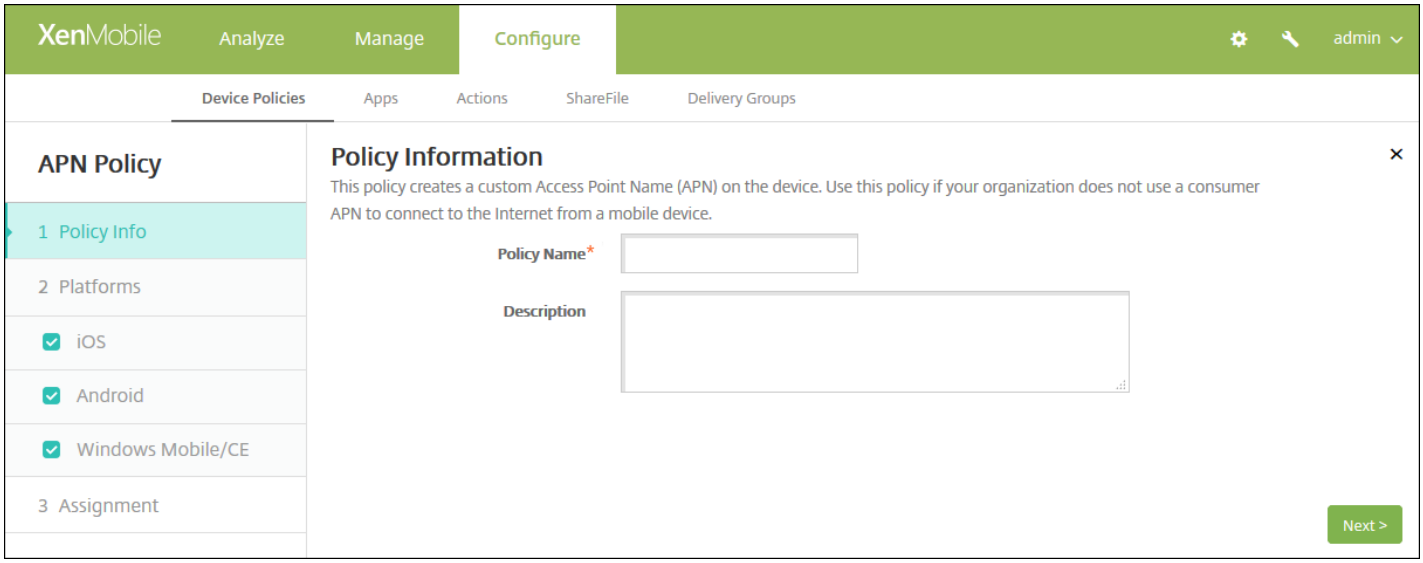
Android-Einstellungen

Windows Mobile-/CE-Einstellungen

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Klicken Sie auf **Mehr** und dann unter **Netzwerkzugriff** auf **APN**. Die Seite für die Richtlinieninformationen der Richtlinie **APN** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

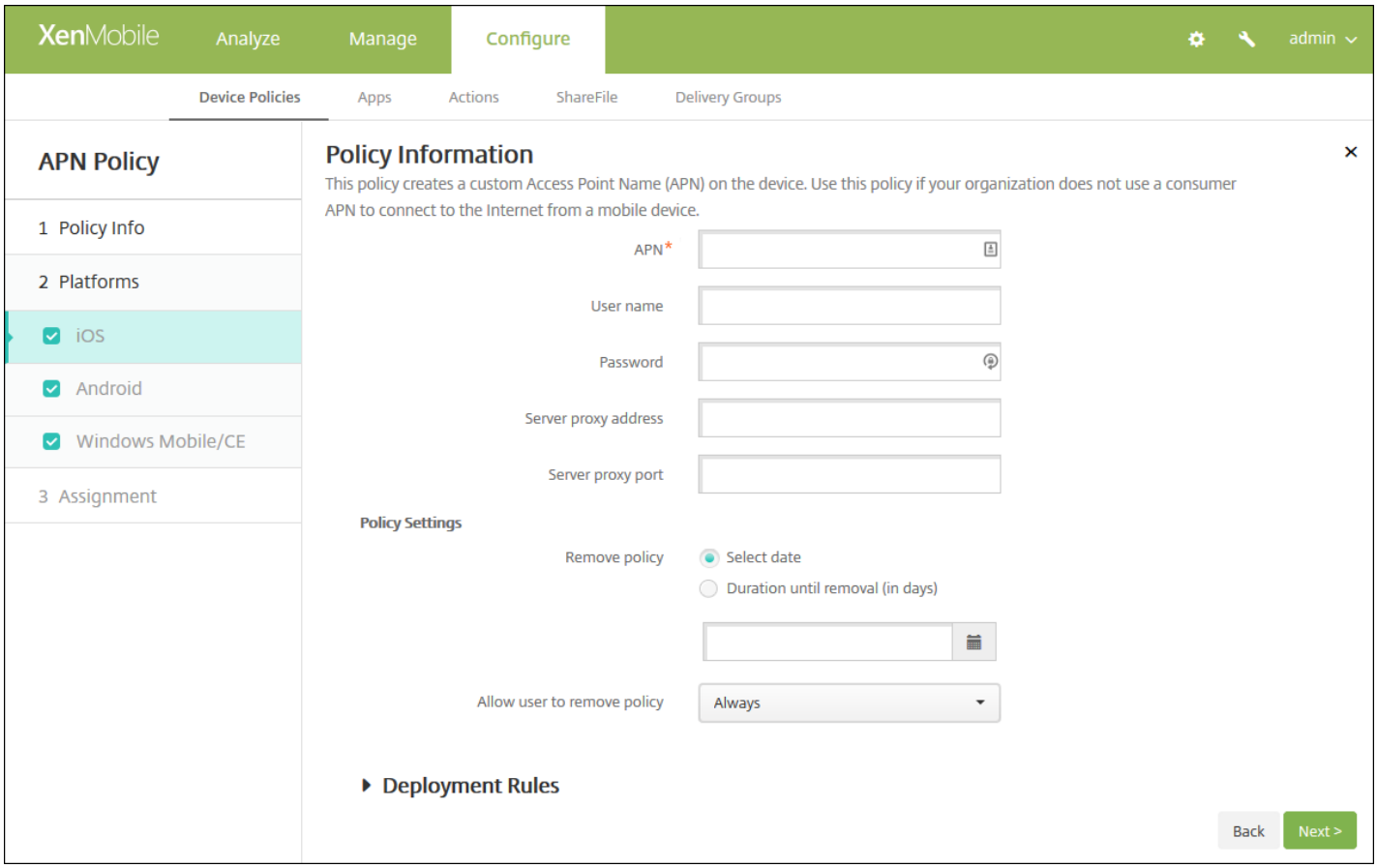
Hinweis: Auf der Seite **Plattformen** sind alle Plattformen ausgewählt und die iOS-Plattform wird als erste angezeigt.

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

Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der

Bereitstellungsregeln für diese Plattform unter Schritt 7.

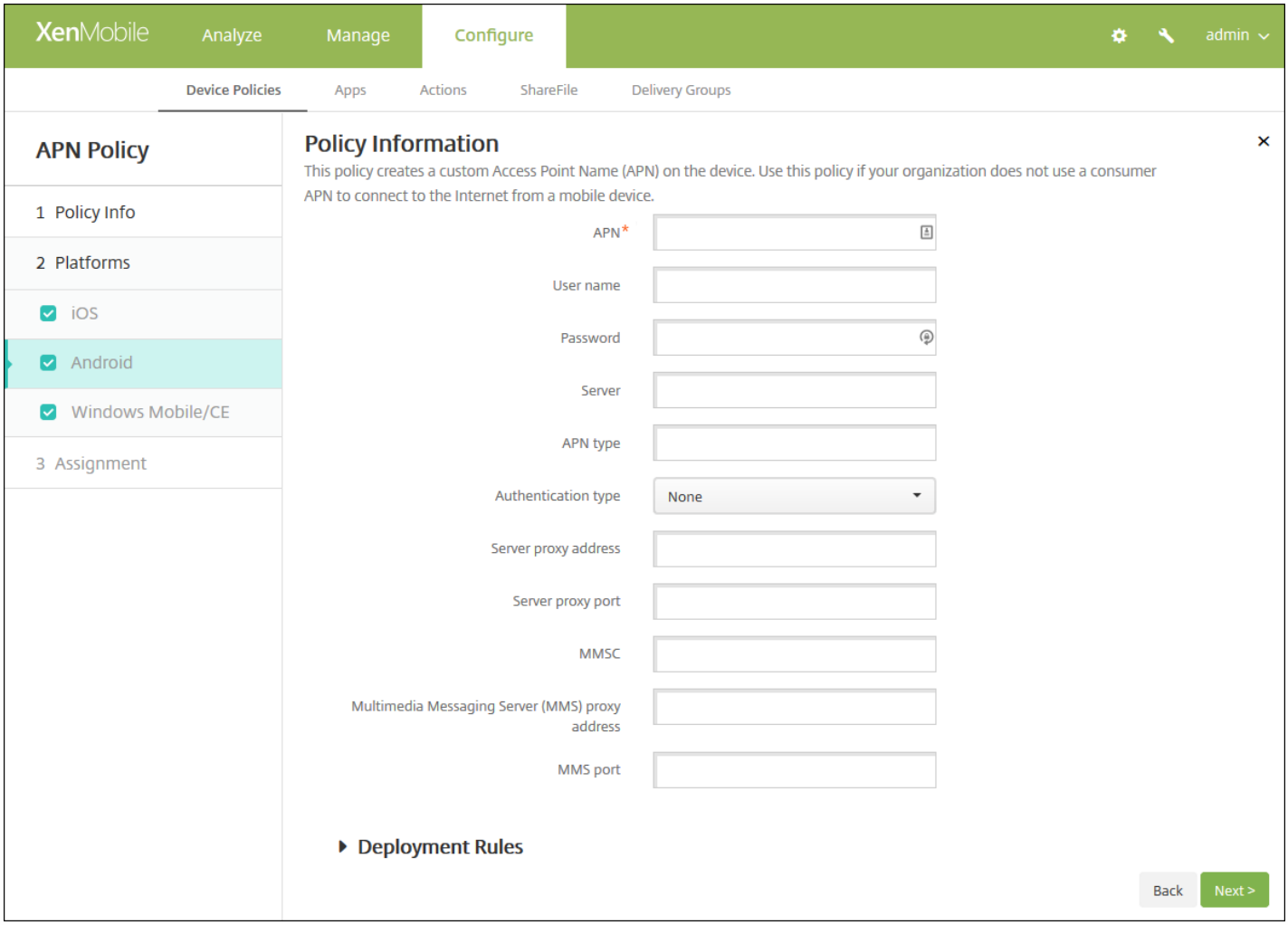
Konfigurieren von iOS-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **APN**: Geben Sie den Namen des Zugriffspunkts ein. Der Name muss mit einem akzeptierten iOS-Zugriffspunkt übereinstimmen, sonst schlägt die Richtlinie fehl.
- **Benutzername**: Diese Zeichenfolge repräsentiert den Benutzernamen für diesen APN. Fehlt der Benutzername, wird die Zeichenfolge während der Profilinstallation angefordert.
- **Kennwort**: 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.
- **Serverproxyadresse**: IP-Adresse oder URL des APN-Proxys
- **Serverproxyport: Portnummer**des APN-Proxys Sie ist erforderlich, wenn Sie eine Serverproxyadresse eingegeben haben.
- Klicken Sie unter **Richtlinieneinstellungen** neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

Konfigurieren von Android-Einstellungen



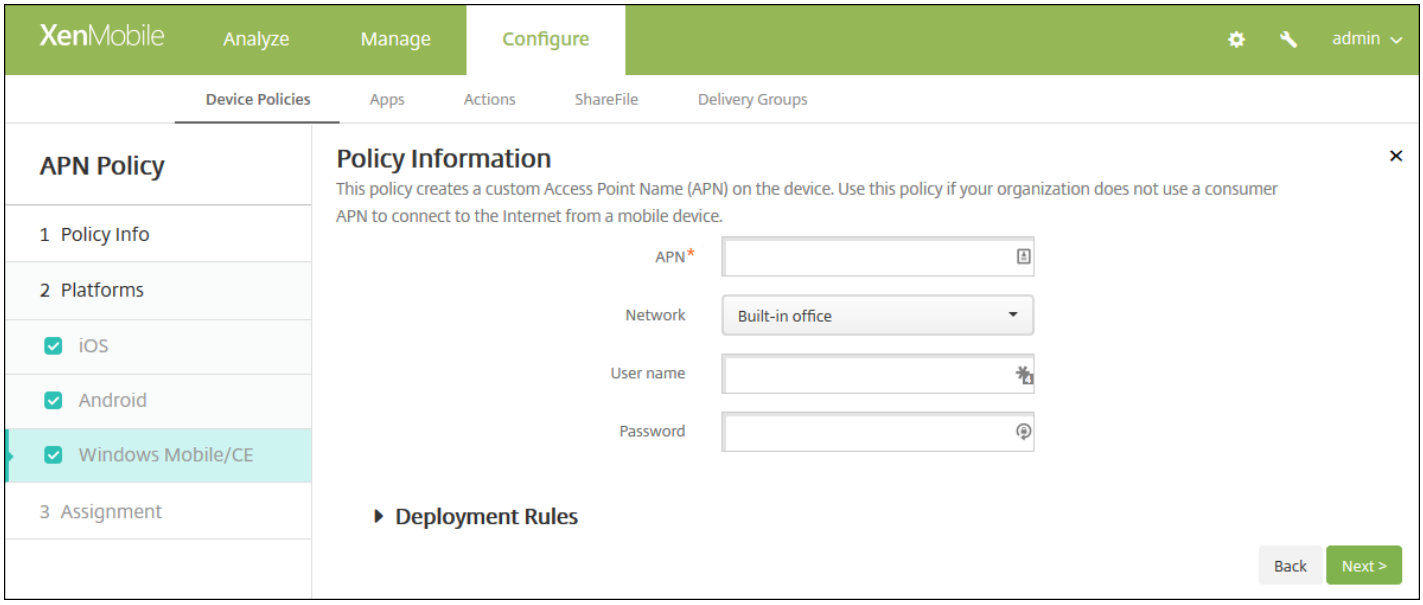
Konfigurieren Sie folgende Einstellungen:

- **APN**: Geben Sie den Namen des Zugriffspunkts ein. Der Name muss mit einem akzeptierten Android-Zugriffspunkt übereinstimmen, sonst schlägt die Richtlinie fehl.
- **Benutzername**: Diese Zeichenfolge repräsentiert den Benutzernamen für diesen APN. Fehlt der Benutzername, wird die Zeichenfolge während der Profilinstallation angefordert.
- **Kennwort**: Das Kennwort für den Benutzer für den APN. Für höhere Sicherheit ist das Kennwort codiert. Fehlt es, fordert das Gerät die Zeichenfolge während der Profilinstallation an.
- **Server**: Diese Einstellung stammt aus der Zeit vor Smartphonesund ist in der Regel leer. Sie verweist auf einen WAP-Gateway-Server (Wireless Application-Protokoll) für Telefone, bei denen der Zugriff auf oder das Rendern von Standardwebsites nicht möglich war.
- **APN-Typ**: 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.

- **Authentifizierungstyp**: Klicken Sie in der Liste auf den gewünschten Authentifizierungstyp. Standardwert ist "Ohne".
- **Serverproxyadresse**: IP-Adresse oder URL des APN-HTTP-Proxys des Netzbetreibers.
- **Serverproxyport**: Portnummer des APN-Proxys. Sie ist erforderlich, wenn Sie eine Serverproxyadresse eingegeben haben.
- **MMSC**: Die vom Netzbetreiber angegebene Adresse des MMS Gateway Servers.
- **MMS-Proxyadresse**: Dies ist der Multimedia-Messaging-Dienstserver für MMS. MMS ist der Nachfolger von SMS und eignet sich für das Senden größerer Nachrichten mit Multimediainhalten z. B. Bilder oder Videos. Diese Server erfordern bestimmte Protokolle (z. B. MM1,... MM11).
- **MMS-Port**: Der Port des MMS-Proxyservers.

Konfigurieren von Windows Mobile-/CE-Einstellungen

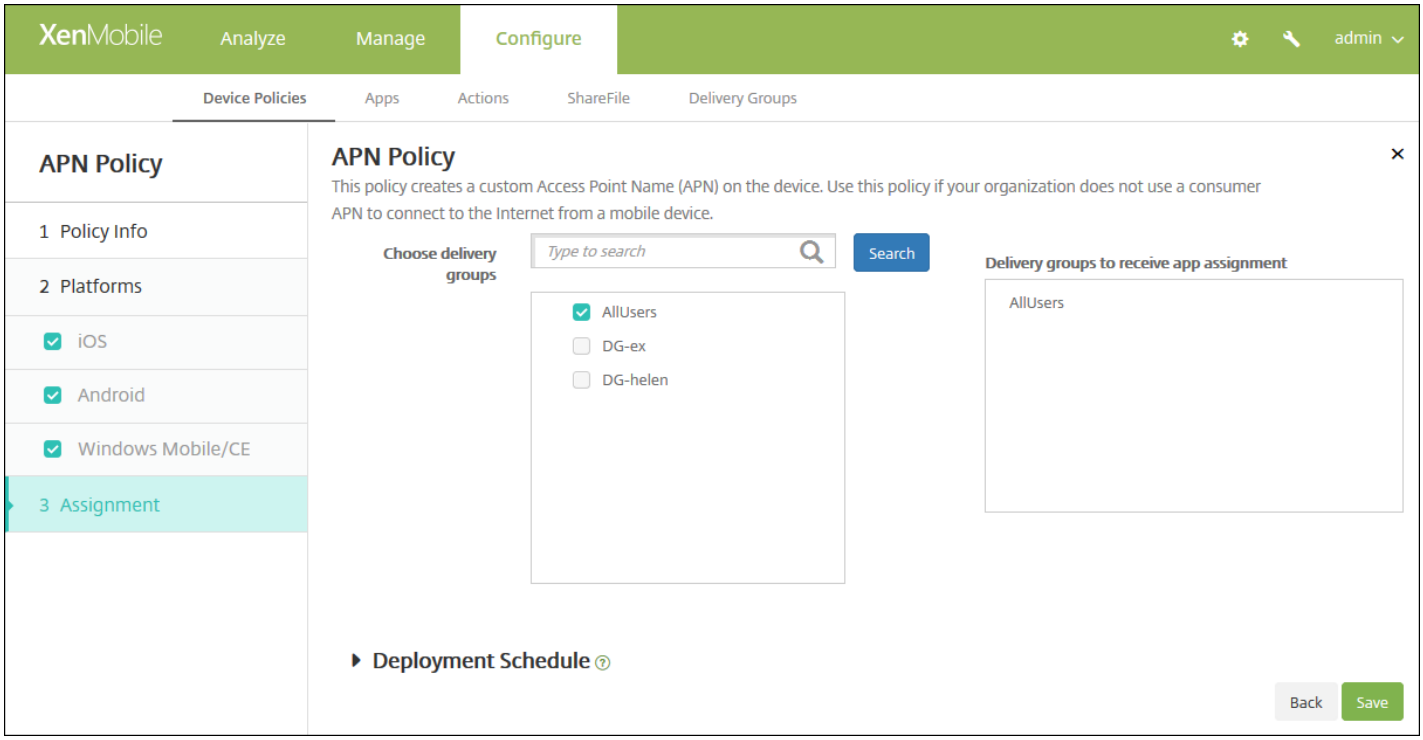


Konfigurieren Sie die folgenden Einstellungen:

- **APN**: Geben Sie den Namen des Zugriffspunkts ein. Der Name muss mit einem akzeptierten Android-Zugriffspunkt übereinstimmen, sonst schlägt die Richtlinie fehl.
- **Netzwerk**: Klicken Sie in der Liste auf den gewünschten Netzwerktyp. Der Standardwert ist **Büro (integriert)**.
- **Benutzername**: Diese Zeichenfolge repräsentiert den Benutzernamen für diesen APN. Wenn der Benutzername fehlt, wird die Zeichenfolge während der Profilinstallation angefordert.
- **Kennwort**: 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.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die APN-Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

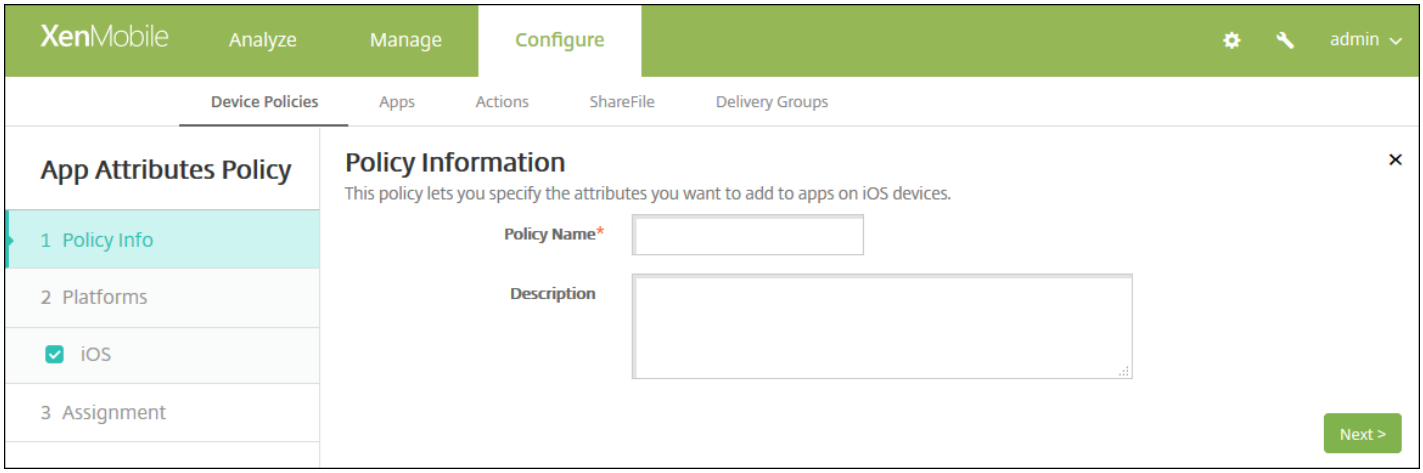
Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen gemachten Änderungen werden auf alle Plattformen angewendet. Ausnahme bildet die Einstellung **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Geräterichtlinie für App-Attribute

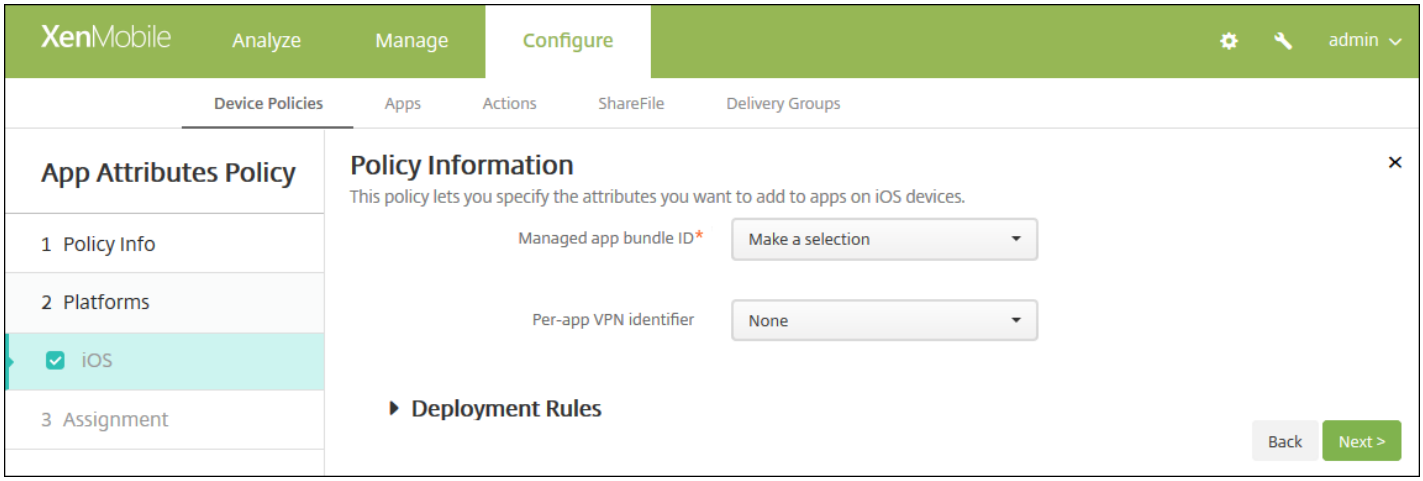
Jul 28, 2016



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

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

5. Klicken Sie auf **Weiter**. Die Plattformseite wird angezeigt.

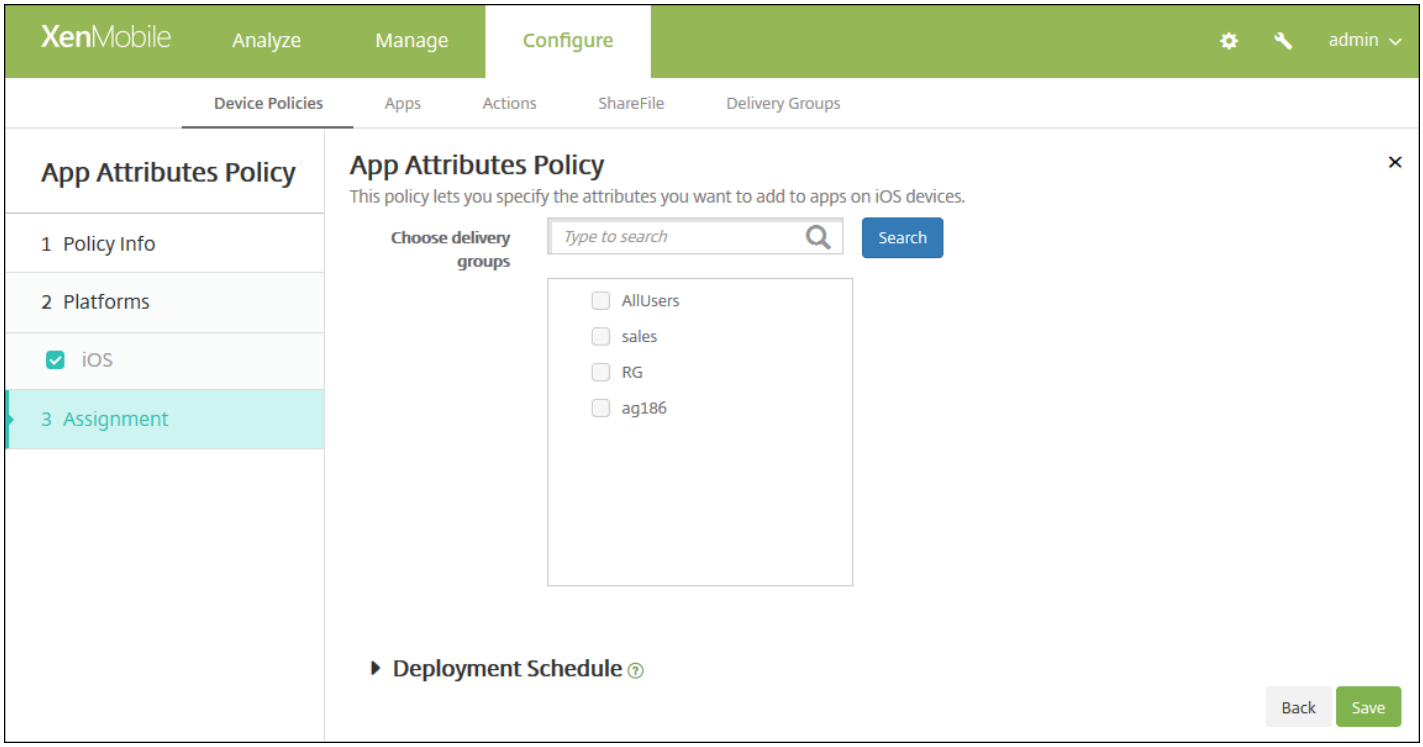


6. Konfigurieren Sie die folgenden Einstellungen:

- **Paket-ID für verwaltete App**: Klicken Sie in der Liste auf eine App-Paket-ID oder auf **Hinzufügen**.
  - Wenn Sie auf **Hinzufügen** klicken, geben Sie die App-Paket-ID in dem nun eingeblendeten Feld ein.
- **ID für VPN-Zugriff pro App**: Klicken Sie in der Liste auf die Pro-App-VPN-ID.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite "Zuweisung" für die App-Attributerichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter "Einstellungen" > "Servereigenschaften" den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

App-Zugriffsrichtlinien für Geräte

Jul 28, 2016

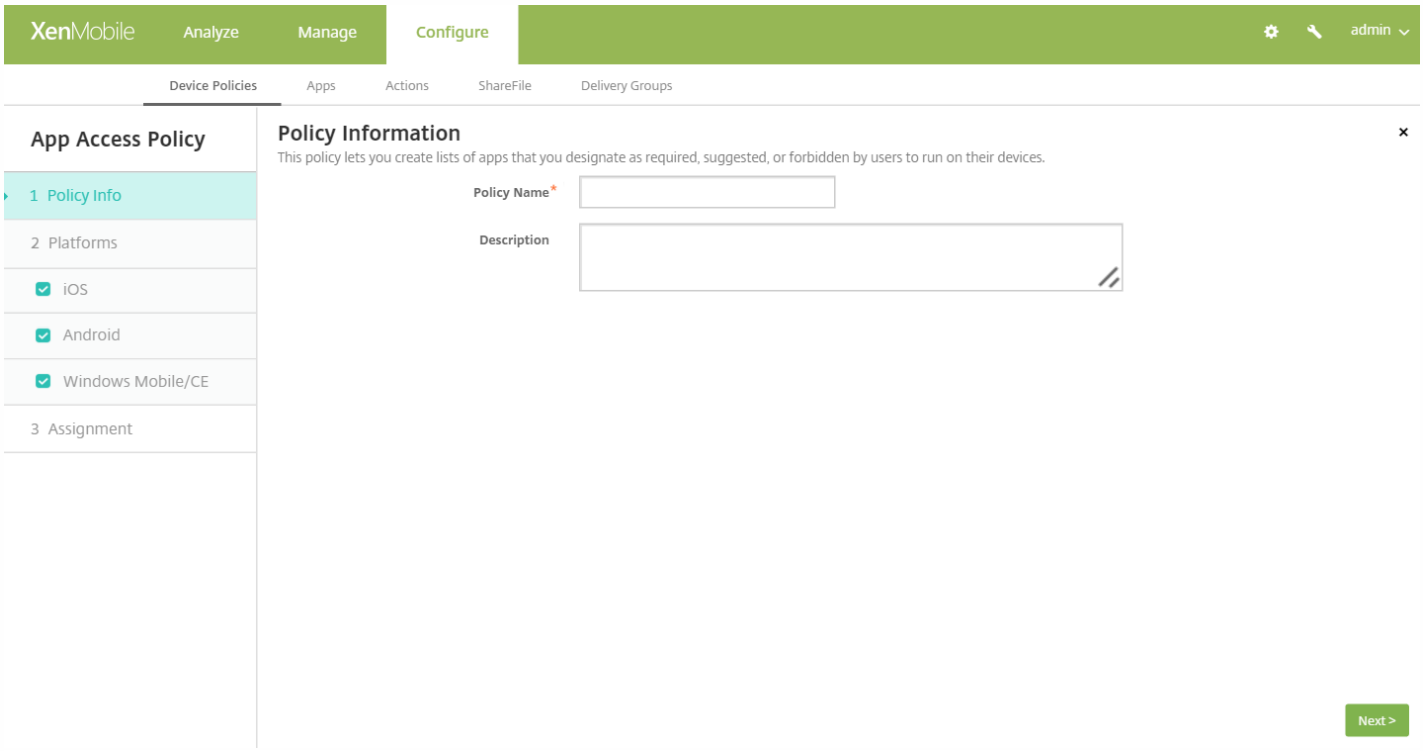
Über eine App-Zugriffsrichtlinie für Geräte können Sie in XenMobile eine Liste der Apps definieren, die auf Geräten installiert werden müssen, nach Wahl installiert werden können oder nicht installiert werden dürfen. Sie können dann eine automatisierte Aktion erstellen, mit der die Reaktion auf die Richtlinientreue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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **App-Zugriff**. Die Seite für die Richtlinieninformationen der Richtlinie **App-Zugriff** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

6. Konfigurieren Sie für jede ausgewählte Plattform die folgenden Einstellungen:

- **Zugriffsrichtlinie**: Klicken Sie auf "Erforderlich", "Empfohlen" oder "Verboten". Der Standardwert ist "Erforderlich".
- Zum Hinzufügen von Apps zu der Liste klicken Sie auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **App-Name**: Geben Sie einen App-Namen ein.
  - **App-ID**: Geben Sie optional eine App-ID ein.
  - Klicken Sie auf **Speichern** oder **Abbrechen**.
  - Wiederholen Sie diese Schritte 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 **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf "Weiter". Die nächste Plattformseite oder die Zuweisungsseite **App-Zugriffsrichtlinie** wird angezeigt.

9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

App-Konfigurationsrichtlinie für Geräte

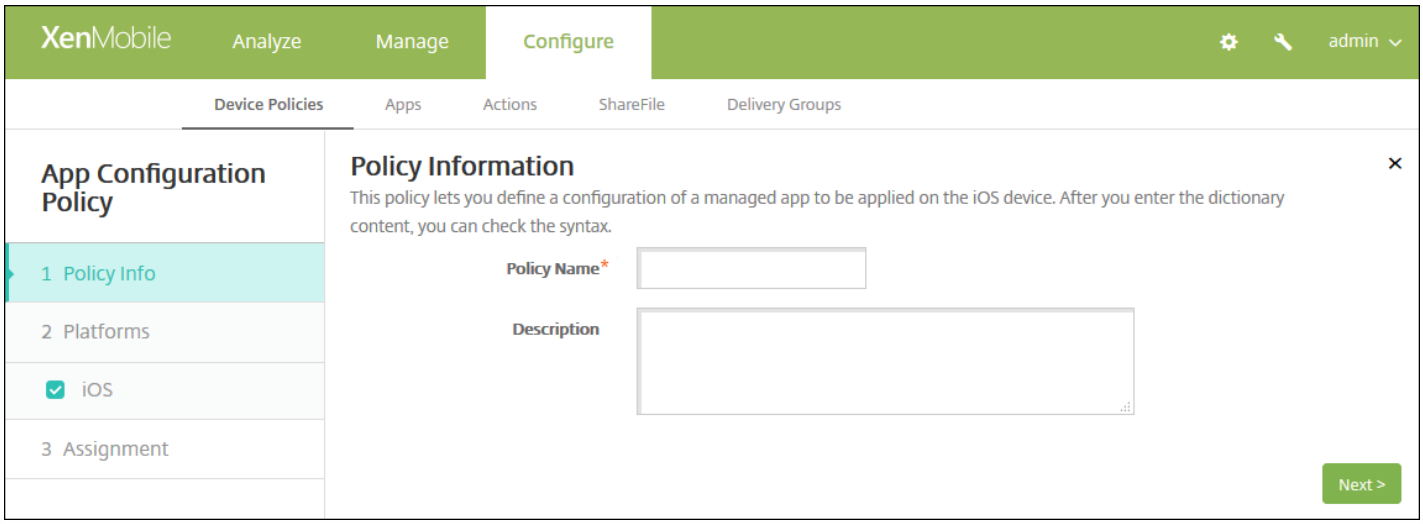
Jul 28, 2016

Sie können eine App Store-App, die die verwaltete Konfiguration unterstützt, remote konfigurieren, indem Sie eine XML-Konfigurationsdatei (eine Eigenschaftenliste oder "plist") zum Konfigurieren verschiedener Einstellungen und Verhalten der App auf iOS-Geräten bereitstellen. Welche Einstellungen und Verhalten Sie konfigurieren können, hängt von der App ab und geht über den Rahmen dieses Artikels hinaus.

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

2. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.

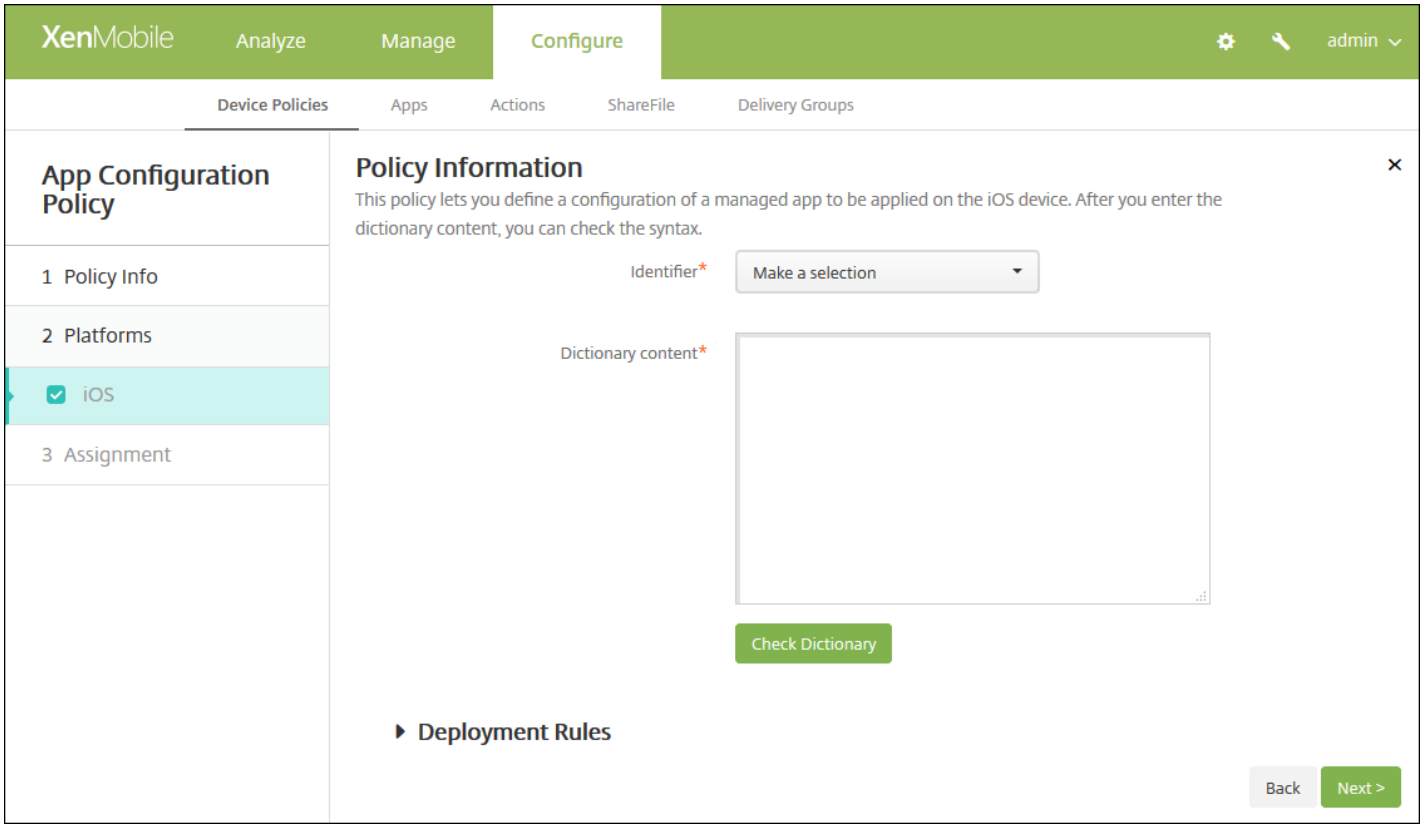
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **App-Konfiguration**. Die Seite **App-Konfiguration** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite mit den Plattforminformationen für **iOS** wird angezeigt.

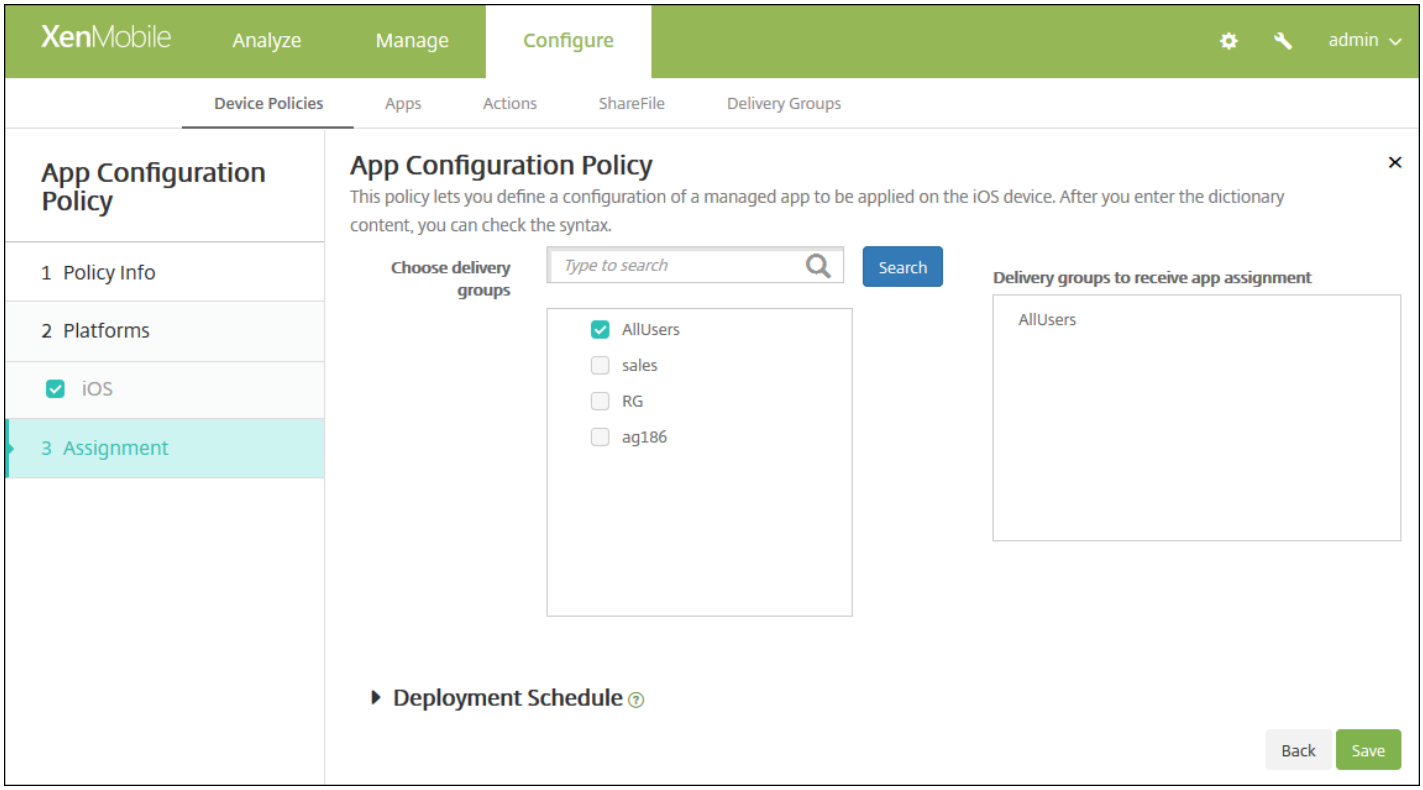


6. Konfigurieren Sie die folgenden Einstellungen:

- **Bezeichner**: Klicken Sie in der Liste auf die gewünschte App oder auf **Hinzufügen**, um der Liste eine App hinzuzufügen.
  - Wenn Sie auf **Hinzufügen** klicken, geben Sie den App-Bezeichner in dem nun eingeblendeten Feld ein.
- **Wörterbuchinhalt**: Geben Sie die Konfigurationsinformationen der Eigenschaftenliste (plistein, bzw. kopieren Sie die Informationen und fügen Sie sie ein.
- Klicken Sie auf **Wörterbuch prüfen**. XenMobile prüft die XML-Datei. Werden keine Fehler gefunden, wird unterhalb des Inhaltsfelds **Gültige XML** angezeigt. Werden unterhalb des Inhaltsfelds Syntaxfehler angezeigt, müssen Sie sie korrigieren, bevor Sie fortfahren können.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die App-Konfigurationsrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **oder auf Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

App-Bestandsgeräterichtlinien

Jul 28, 2016

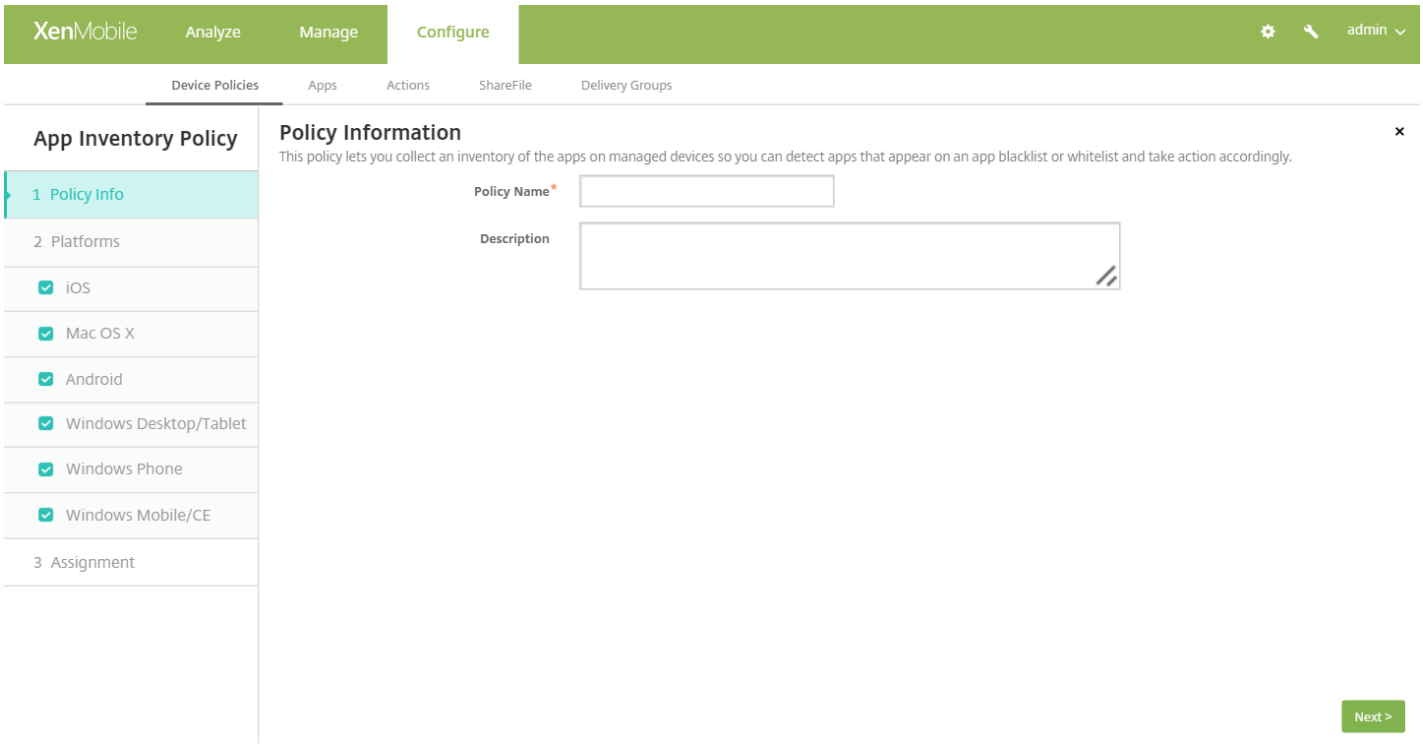
Mit einer App-Bestandsrichtlinie können Sie in XenMobile einen Bestand der Apps auf verwalteten Geräten sammeln und dann mit allen auf diesen Geräten bereitgestellten App-Zugriffsrichtlinien vergleichen. Auf diese Weise können Sie Apps erkennen, die in einer App-Sperrliste (d. h. in einer App-Zugriffsrichtlinie verboten) oder einer App-Positivliste (d. h. gemäß einer App-Zugriffsrichtlinie erforderlich) sind, und entsprechende Maßnahmen ergreifen. Sie können App-Zugriffsrichtlinien für iOS-, Mac OS X-, Android- (einschließlich Android for Work), Windows Desktop-/Tablet-, Windows Phone- und Windows Mobile-/CE-Geräte erstellen.

> ## Important
>
> Damit aktualisierte Apps in der Liste der verfügbaren Updates im WorxStore auf Android-Geräten angezeigt werden, müssen Sie auf den Geräten diese Richtlinie bereitstellen.

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

2. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.

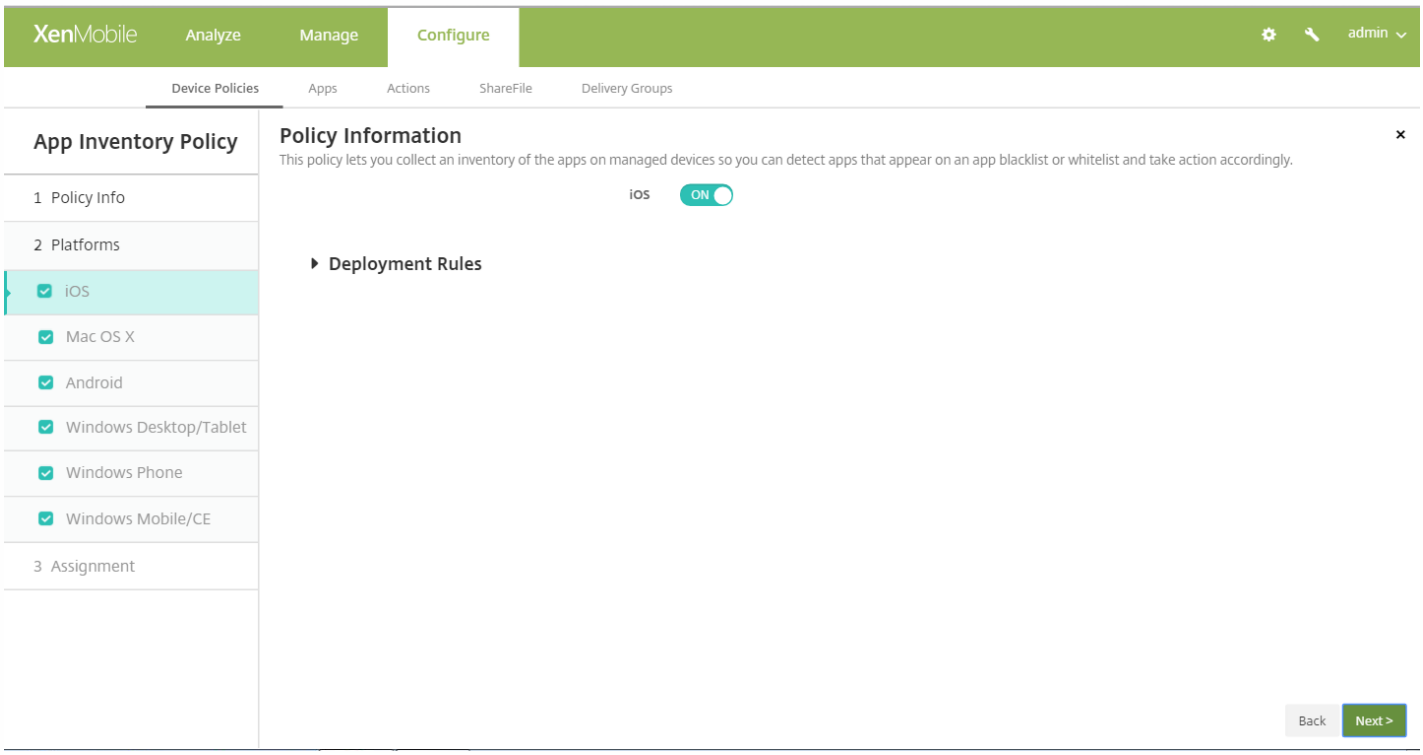
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **App-Bestand**. Die Seite **App-Bestand** wird angezeigt.



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

- **Richtlinienname**: Geben Sie einen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.



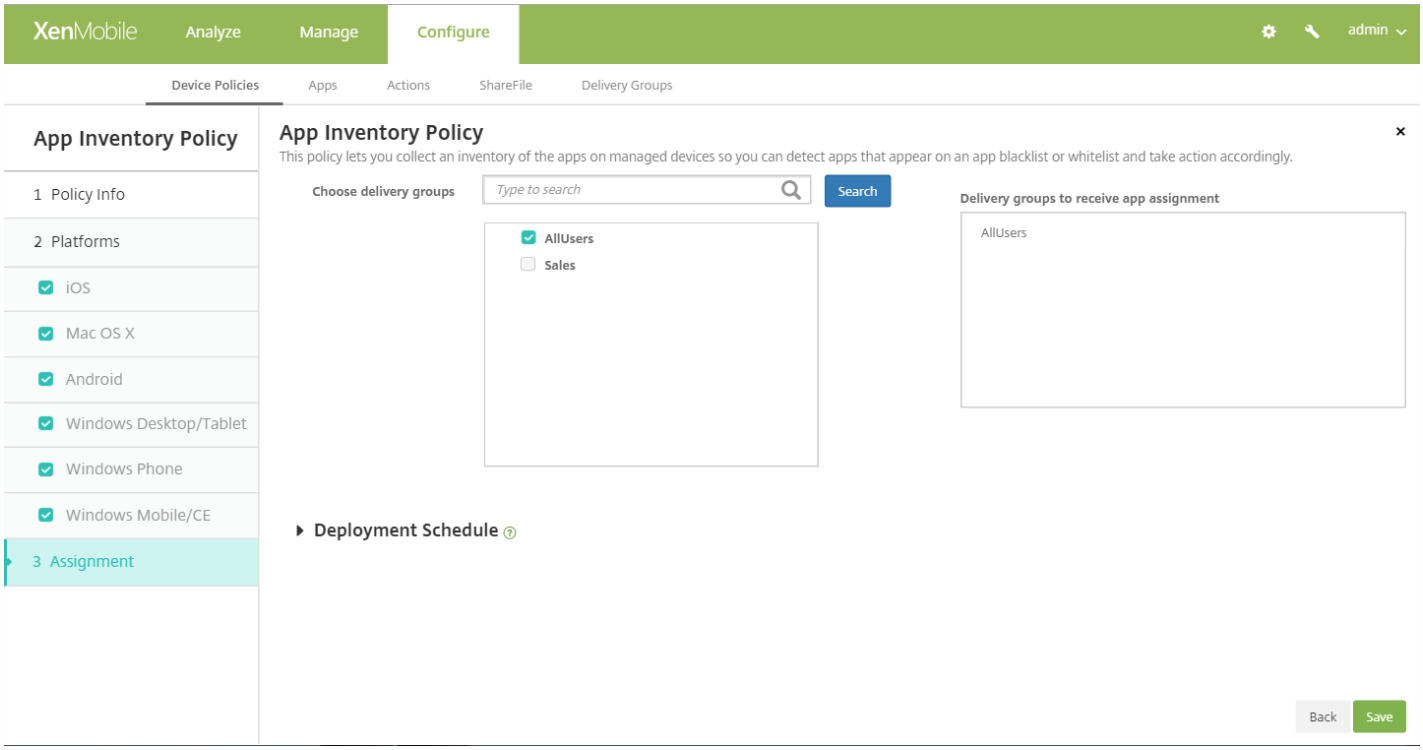
Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

6. Behalten Sie für jede ausgewählte Plattform Standardwert bei oder klicken Sie auf **AUS**. Die Standardeinstellung ist **EIN**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die App-Bestandsrichtlinie wird angezeigt.



9. Machen Sie neben Bereitstellungsgruppen wählen 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.

10. Erweitern Sie Bereitstellungszeitplan und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben Bereitstellungszeitplan auf Jetzt oder Später. Die Standardeinstellung ist Jetzt.
- Wenn Sie auf Später klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben Bereitstellungsbedingung auf Bei jeder Verbindung oder auf Nur bei Fehler in der vorherigen Bereitstellung. Die Standardeinstellung ist Bei jeder Verbindung.
- Klicken Sie neben Bereitstellen für immer aktive Verbindungen auf EIN oder AUS. Die Standardeinstellung ist AUS.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Geräterichtlinie zum Sperren von Apps

Aug 22, 2016

Sie können in XenMobile mit einer Richtlinie eine Liste von Apps definieren, die auf einem Gerät ausgeführt werden dürfen, oder eine Liste von Apps, die auf einem Gerät blockiert werden. Sie können diese Richtlinie für iOS- und Android-Geräte konfigurieren, die Richtlinie funktioniert jedoch auf den Plattformen unterschiedlich. Auf einem iOS-Gerät können Sie beispielsweise nicht mehrere Apps blockieren.

Auf iOS-Geräten können Sie auch nur eine iOS-App pro Richtlinie auswählen. Dies bedeutet, dass Benutzer mit ihrem Gerät nur eine einzige App ausführen können. Außer den Optionen, die ausdrücklich zulässig sind, wenn die Richtlinie für die App-Sperre erzwungen wird, können Benutzer keine anderen Aktivitäten auf dem Gerät ausführen.

Darüber hinaus müssen sich iOS-Geräte im betreuten Modus befinden, damit die Richtlinie für die App-Sperre per Push bereitgestellt werden kann.

Obwohl die Geräterichtlinie auf den meisten Android L- und M-Geräten funktioniert, funktioniert App-Sperre nicht auf Android N oder neueren Geräten, da die erforderliche API von Google eingestellt wurde.

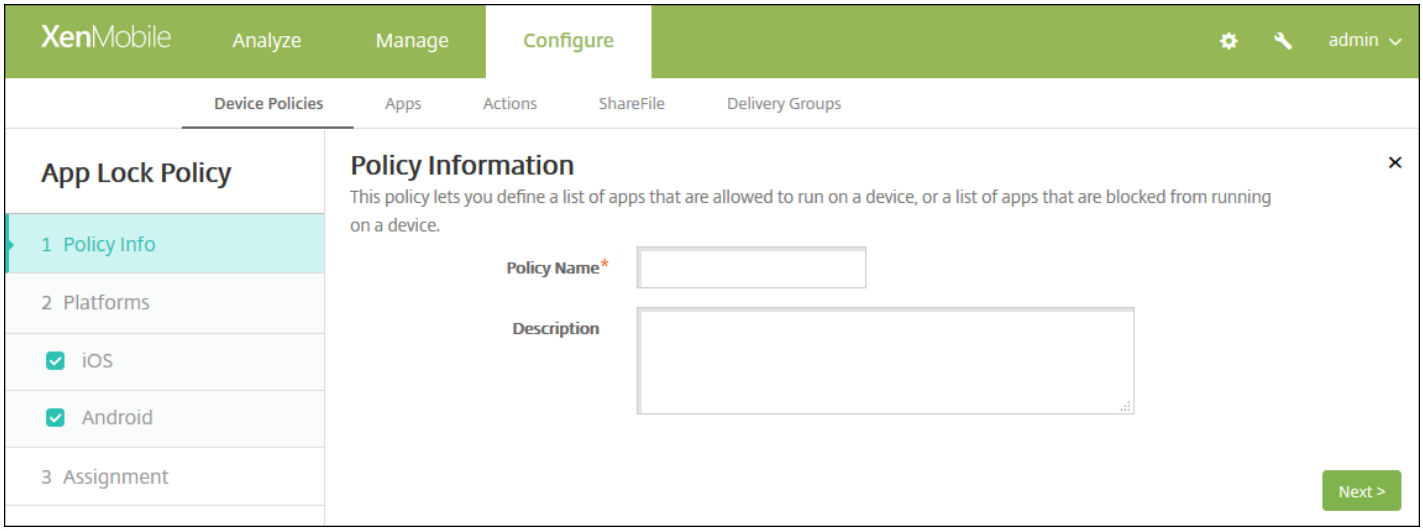
iOS-Einstellungen

Android-Einstellungen

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **App-Sperre**. Die Seite **App-Sperre** wird angezeigt.



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

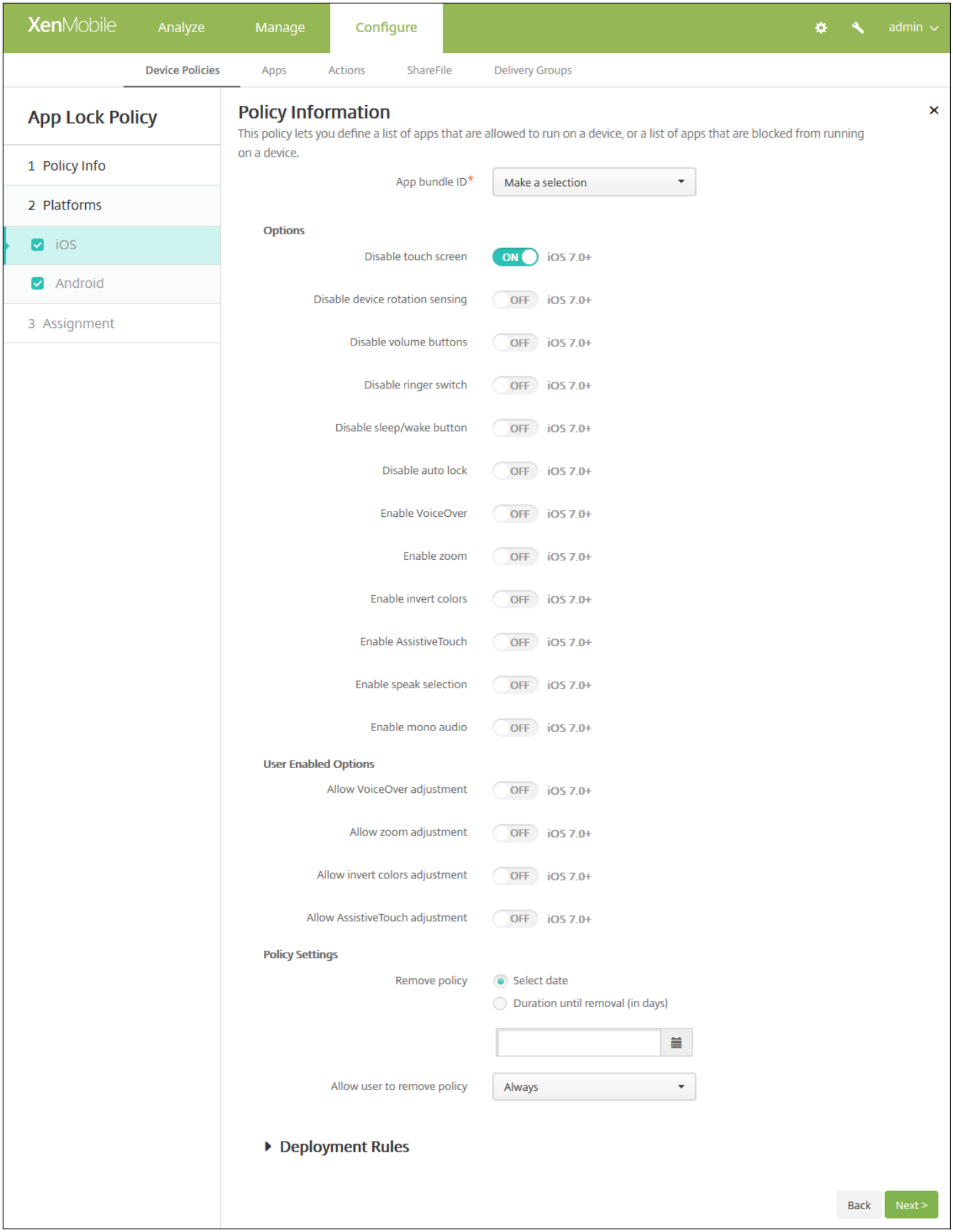
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung für die Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

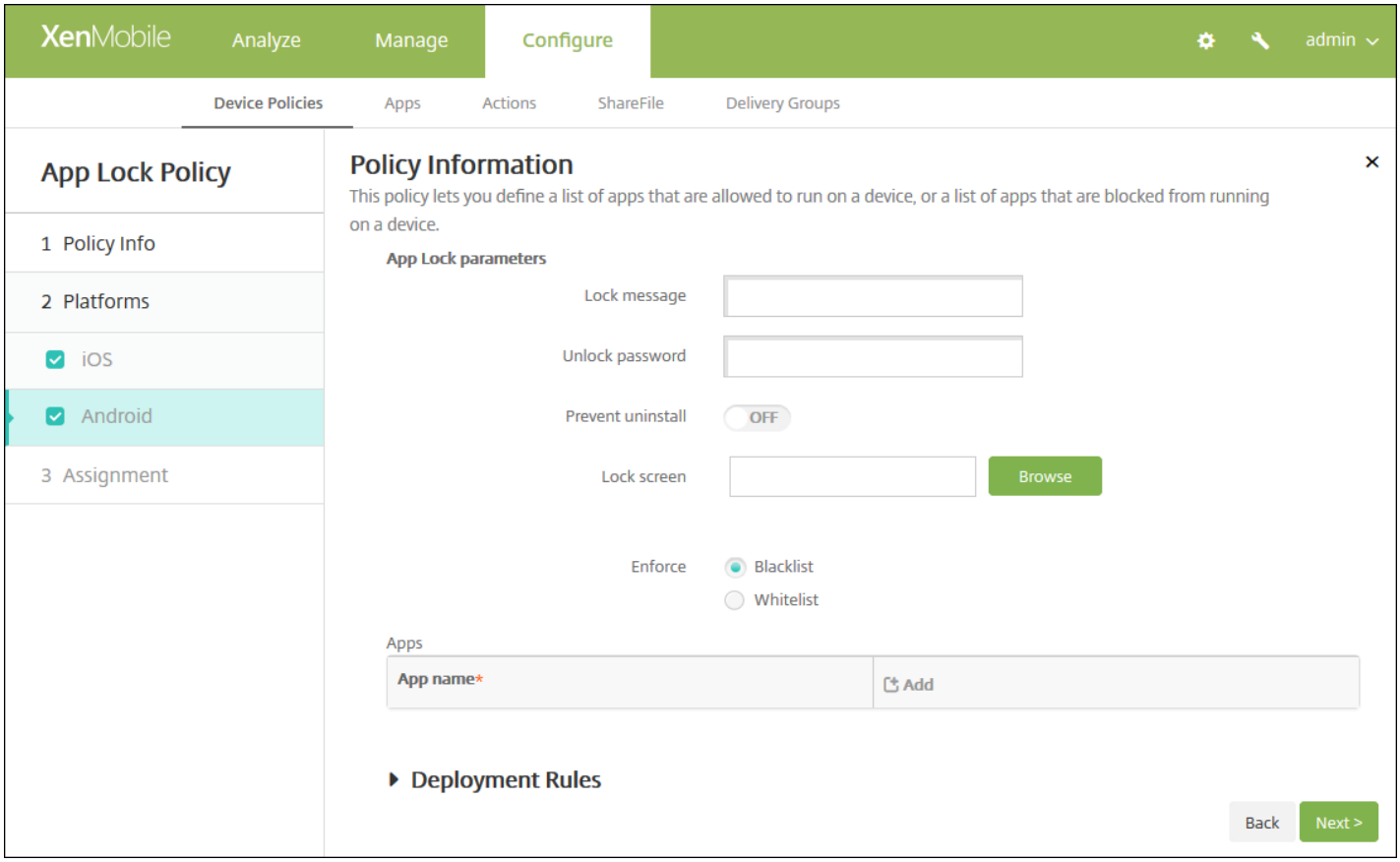
Konfigurieren von iOS-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **App-Paket-ID**: Klicken Sie in der Liste auf die App, auf die die Richtlinie angewendet werden soll, oder auf **Hinzufügen**, um der Liste eine App hinzuzufügen. Wenn Sie auf **Hinzufügen** klicken, geben Sie den App-Namen in dem nun eingeblendeten Feld ein.
- **Optionen**: Die folgenden Optionen gelten nur für iOS 7.0 oder höher. Der Standardwert aller Optionen mit Ausnahme von **Touchscreen deaktivieren** ist **AUS**.
  - Touchscreen deaktivieren
  - Geräteausrichtungserkennung deaktivieren
  - Lautstärketasten deaktivieren
  - Ruftonschalter deaktivieren – **Hinweis**: Wenn diese Option deaktiviert wird, erfolgt die Ruftonausgabe gemäß der Schalterposition beim ersten Deaktivieren der Option.
  - Standbymodusschalter deaktivieren
  - Automatische Sperre deaktivieren
  - VoiceOver aktivieren
  - Zoom aktivieren
  - Umkehren der Farben aktivieren
  - AssistiveTouch aktivieren
  - Sprachauswahl aktivieren
  - Monoaudio aktivieren
- **Benutzeraktivierte Optionen**: Die folgenden Optionen gelten nur für iOS 7.0 oder höher. Der Standardwert aller Optionen ist **AUS**.
  - Anpassen von VoiceOver zulassen
  - Anpassen von Zoom zulassen
  - Anpassen von Farbumkehrung zulassen
  - Anpassen von AssistiveTouch zulassen
- **Richtlinieneinstellungen**
  - o Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - o Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - o Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Kennwort erforderlich** oder **Nie**.
  - o Bei Auswahl von **Kennwort erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

Konfigurieren von Android-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Parameter für App-Sperre**
  - **Sperrmeldung**: Geben Sie eine Meldung ein, die angezeigt wird, wenn ein Benutzer versucht, eine gesperrte App zu öffnen.
  - **Entsperrkennwort**: Geben Sie das Kennwort zum Entsperren der App ein.
  - **Deinstallation verhindern**: Wählen Sie aus, ob eine Deinstallation der App durch die Benutzer zulässig sein soll. Der Standardwert ist **AUS**.
  - **Sperrbildschirm**: Klicken Sie auf "Durchsuchen", navigieren Sie zum Speicherort der Sperrbildschirmdatei und wählen Sie diese aus.
  - **Erzwingen**: Klicken Sie auf **Sperrliste**, um eine Liste von Apps zu erstellen, deren Ausführung auf den Geräten nicht zulässig ist, oder auf **Positivliste**, um eine Liste von Apps zu erstellen, deren Ausführung auf den Geräten zulässig ist.
- **Apps**: Klicken Sie auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **App-Name**: Klicken Sie in der Liste auf die App, die der Positiv- bzw. Sperrliste hinzugefügt werden soll, oder auf **Hinzufügen**, um der Liste der verfügbaren Apps eine App hinzuzufügen.
  - Wenn Sie auf **Hinzufügen** klicken, geben Sie den App-Namen in dem nun eingeblendeten Feld ein.
  - Klicken Sie auf **Speichern** oder **Abbrechen**.
  - Wiederholen Sie diese Schritte für jede App, die Sie der Positiv- bzw. Sperrliste hinzufügen möchten.

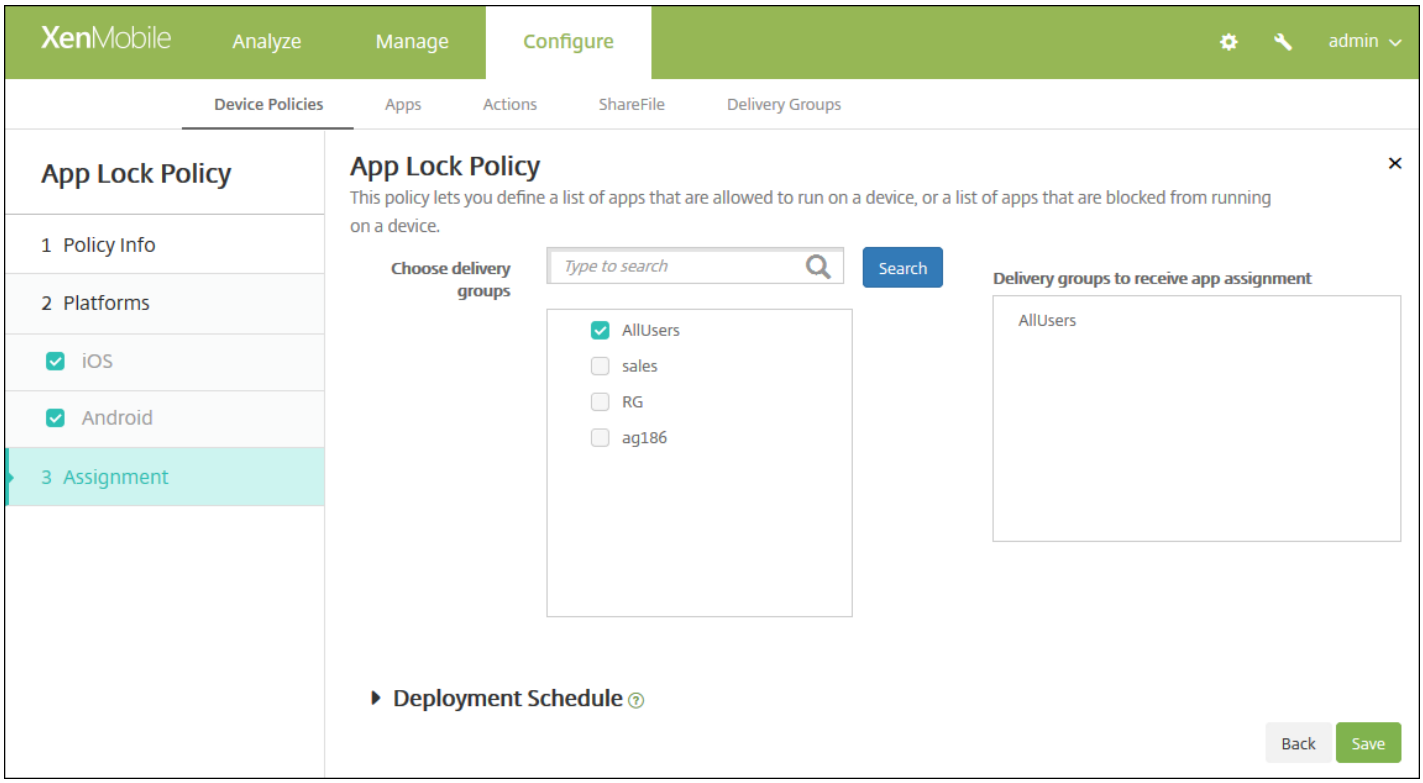
    Hinweis: Zum Löschen einer vorhandenen App zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, um ihn beizubehalten.

    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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuordnung** für die App-Sperrrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.

- 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.

11. Klicken Sie auf **Speichern**.

Richtlinie für die App-Netzwerkauslastung

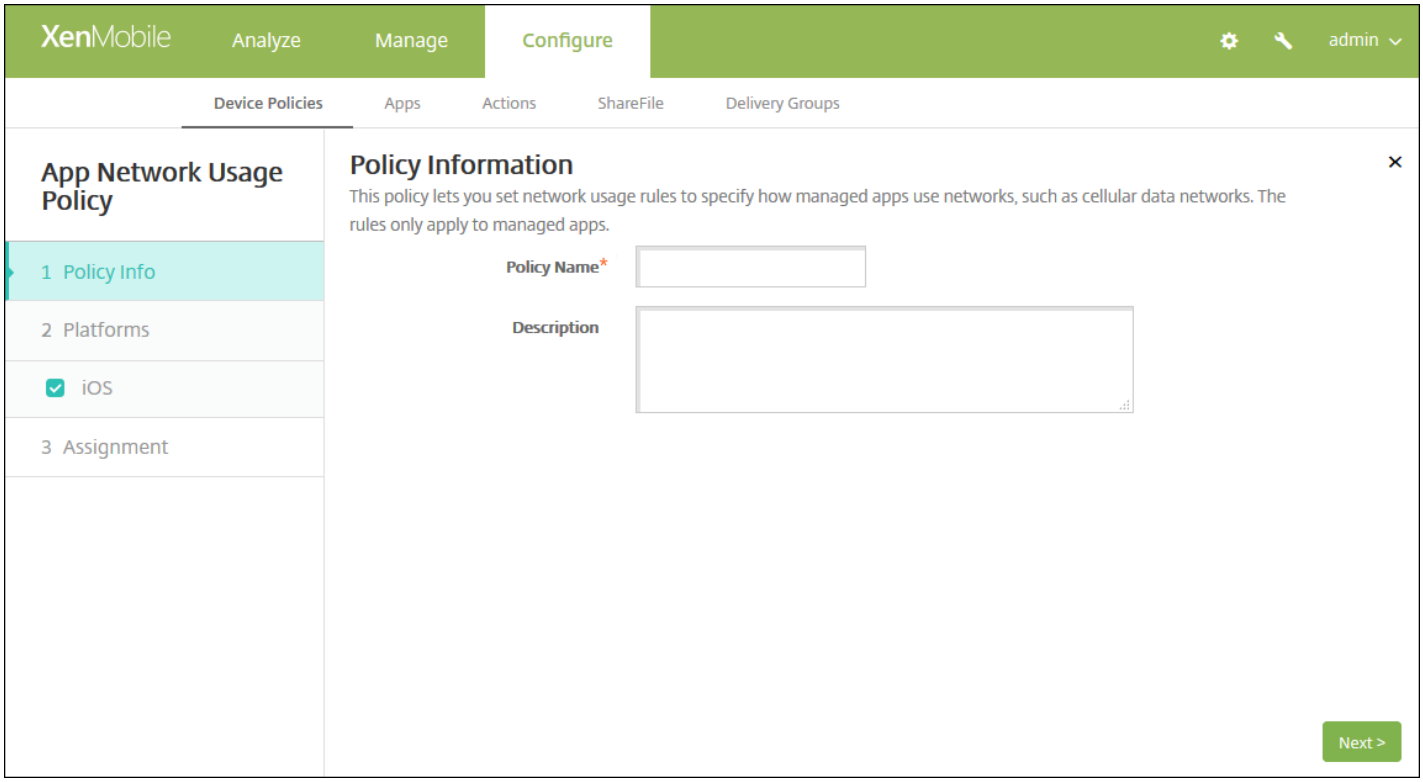
Jul 28, 2016

Sie können Netzwerkauslastungsregeln festlegen, um vorzugeben, wie Netzwerke, z. B. mobile Datennetzwerken durch verwaltete Apps auf iOS-Geräten verwendet werden. Die Regeln gelten nur für verwaltete Apps. Verwaltete Apps sind diejenigen, die Sie über XenMobile bereitstellen. Dazu gehören keine Apps, die Benutzer direkt auf ihre Geräte heruntergeladen haben und die nicht über XenMobile bereitgestellt wurden, und keine Apps, die bereits auf den Geräten installiert waren, wenn diese bei XenMobile registriert wurden.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Geräterichtlinien**.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

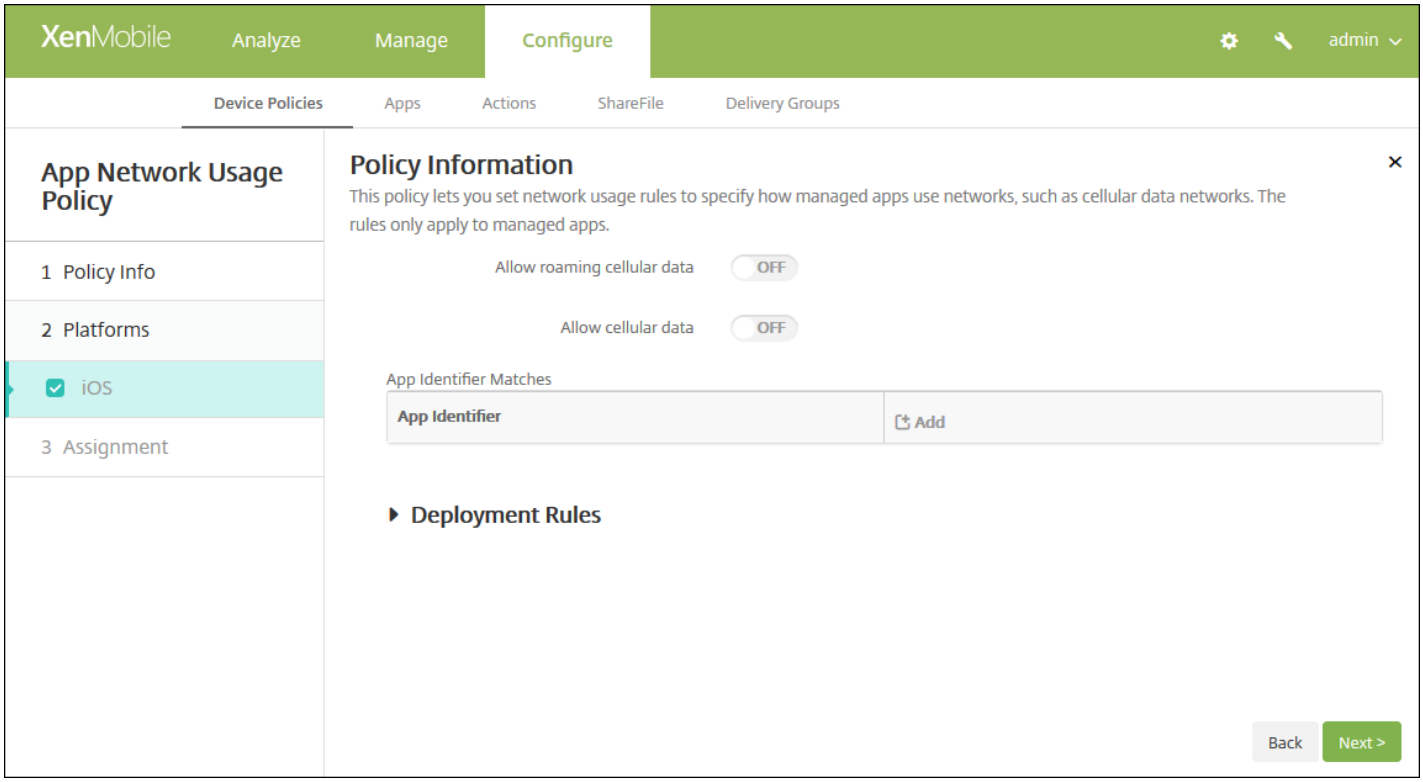
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **App-Netzwerkauslastung**. Die Seite **App-Netzwerkauslastung** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.



6. Konfigurieren Sie diese Einstellungen.

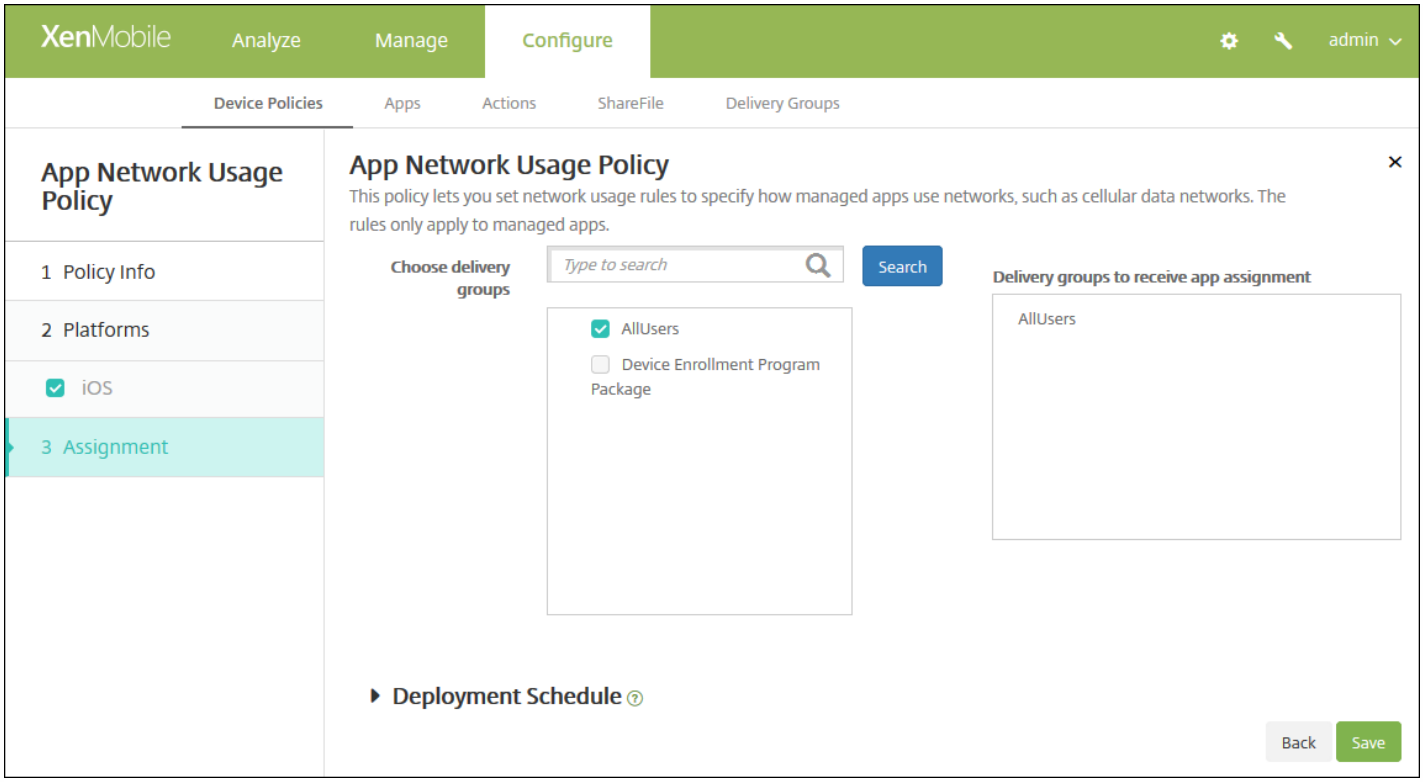
- **Roaming für mobile Daten zulassen**: Wählen Sie aus, ob die angegebenen Apps beim Roaming eine Mobilfunkdatenverbindung herstellen dürfen. Der Standardwert ist **AUS**.
- **Mobile Daten zulassen**: Wählen Sie aus, ob die angegebenen Apps eine Mobilfunkdatenverbindung verwenden dürfen. Der Standardwert ist **AUS**.
- **App-ID-Übereinstimmungen**: Klicken Sie für jede App, die Sie der Liste hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **App-ID**: Geben Sie die App-ID ein.
  - Klicken Sie auf **Speichern**, um die App der Liste hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

    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 **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die App-Netzwerkauslastungsrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

App-Einschränkungsrichtlinien

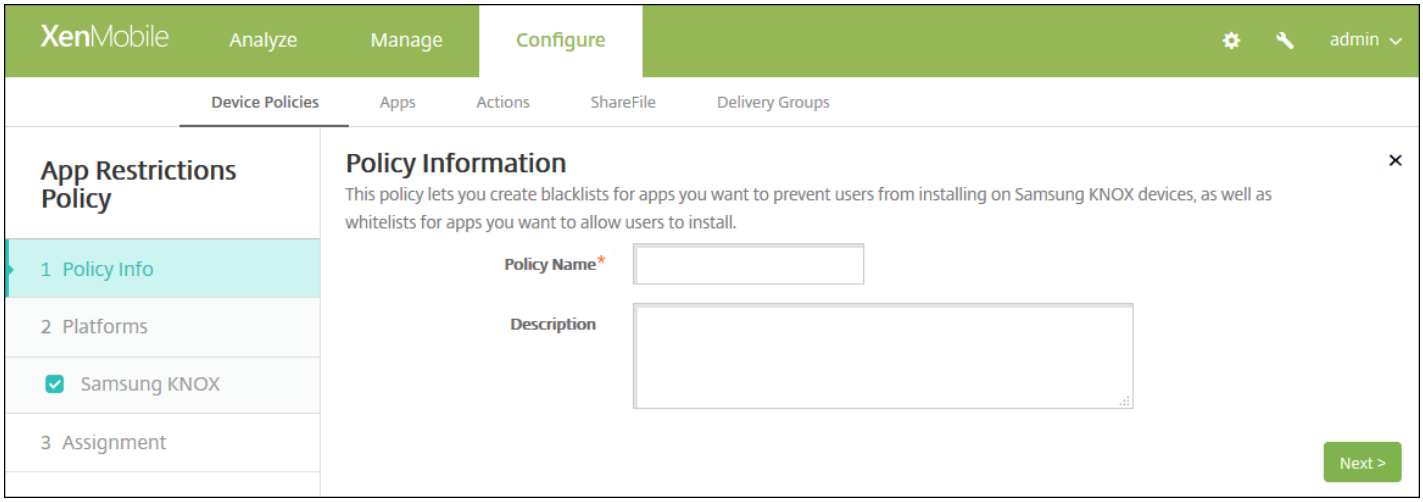
Jul 28, 2016

Sie können Sperrlisten mit Apps erstellen, für die Sie verhindern möchten, dass Benutzer sie auf Samsung KNOX-Geräten installieren, sowie Positivlisten mit Apps, die Benutzer installieren dürfen.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

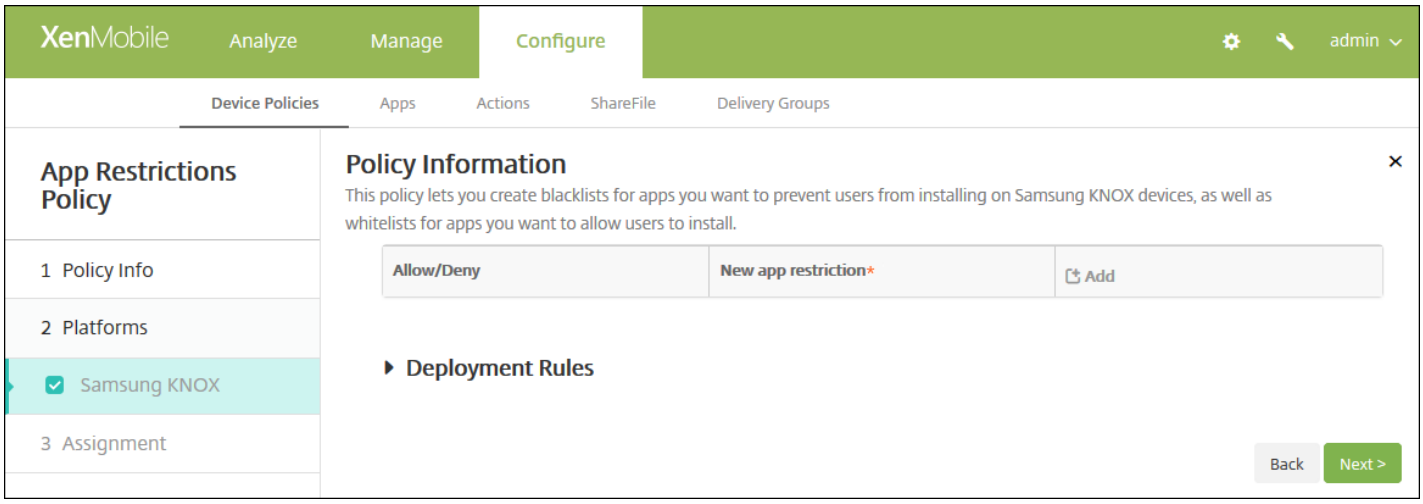
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **App-Einschränkungen**. Die Seite **App-Einschränkungen** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Plattformseite für Samsung KNOX wird angezeigt.



6. Klicken Sie für jede App, die Sie der Zulassen/Verweigern-Liste hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:

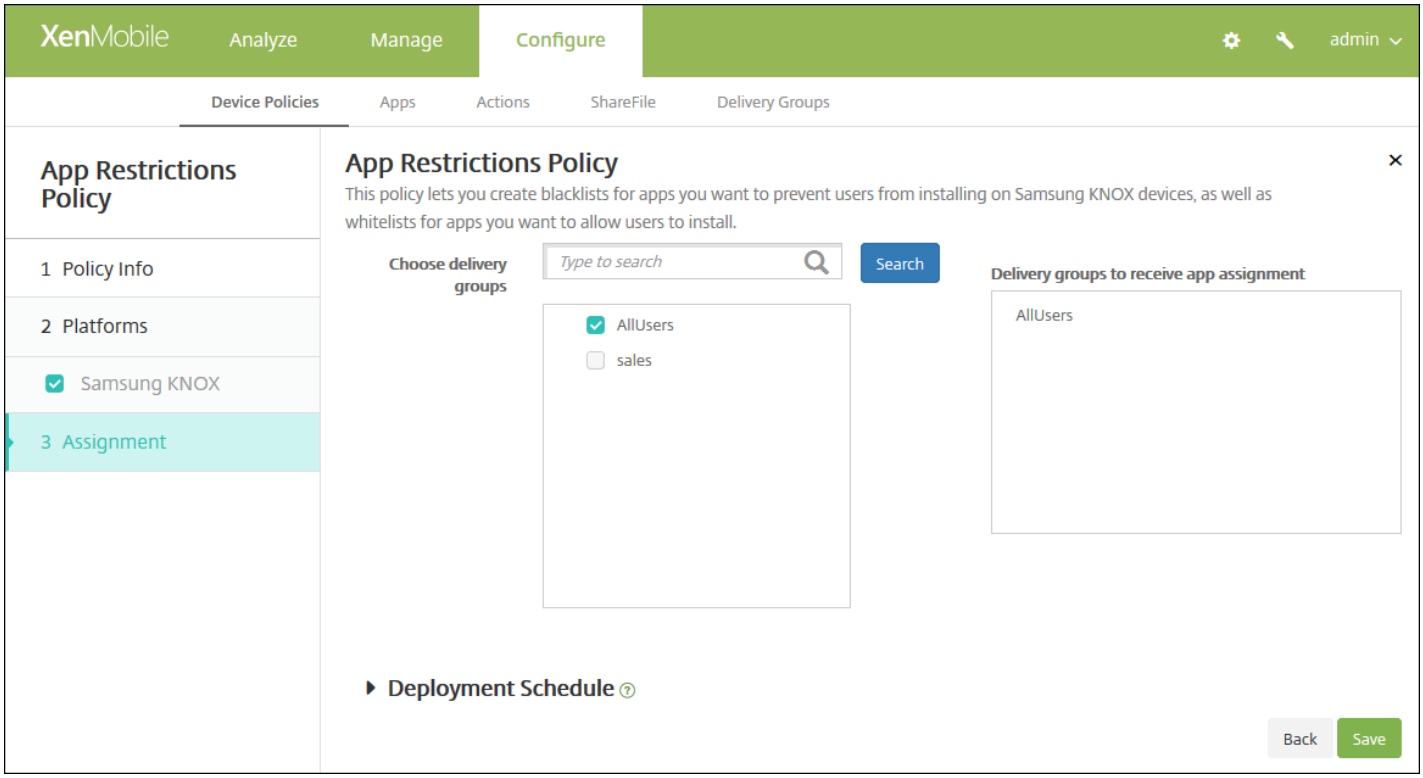
- **Zulassen/Verweigern**: Wählen Sie aus, ob Benutzern die Installation der App gestattet werden soll.
- **Neue App-Einschränkung**: Geben Sie die App-Paket-ID ein, z. B. "com.kmdm.af.crackle".
- Klicken Sie auf **Speichern**, um die App der Zulassen/Verweigern-Liste hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

  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 **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die App-Einschränkungsrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.

- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

App-Tunnelrichtlinien für Geräte

Jul 28, 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. Sie können App-Tunnelrichtlinien für Android- und Windows Mobile/CE-Geräte konfigurieren.

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.

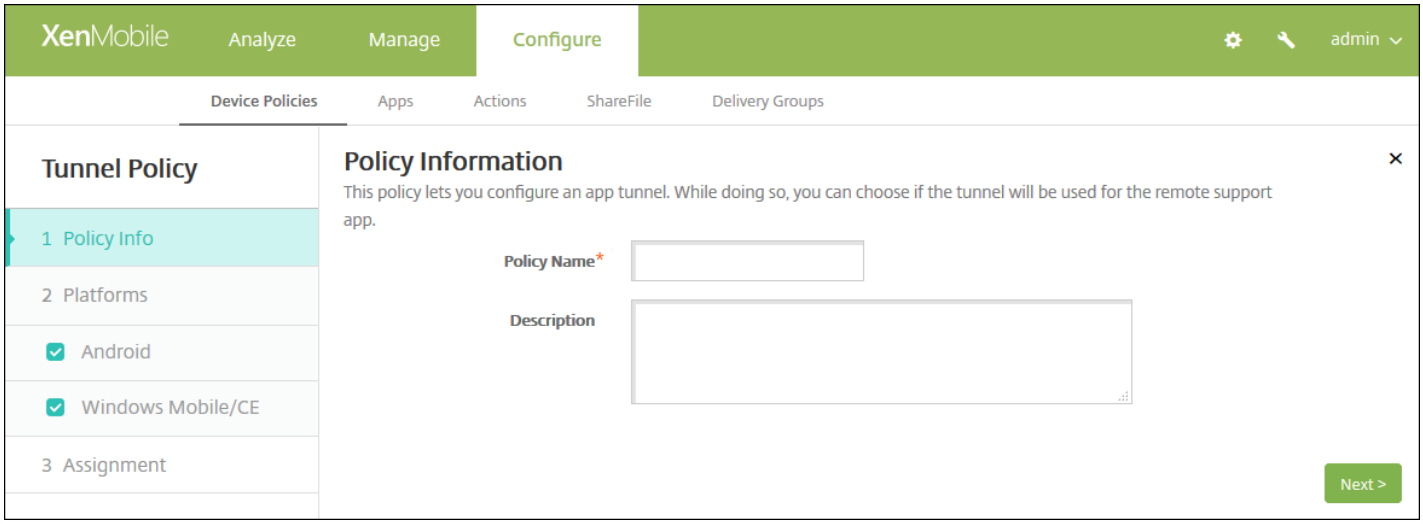
Android-Einstellungen

Windows Mobile-/CE-Einstellungen

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Klicken Sie auf **Mehr** und dann unter **Netzwerkzugriff** auf **Tunnel**. Die Seite **Tunnel** wird angezeigt.



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

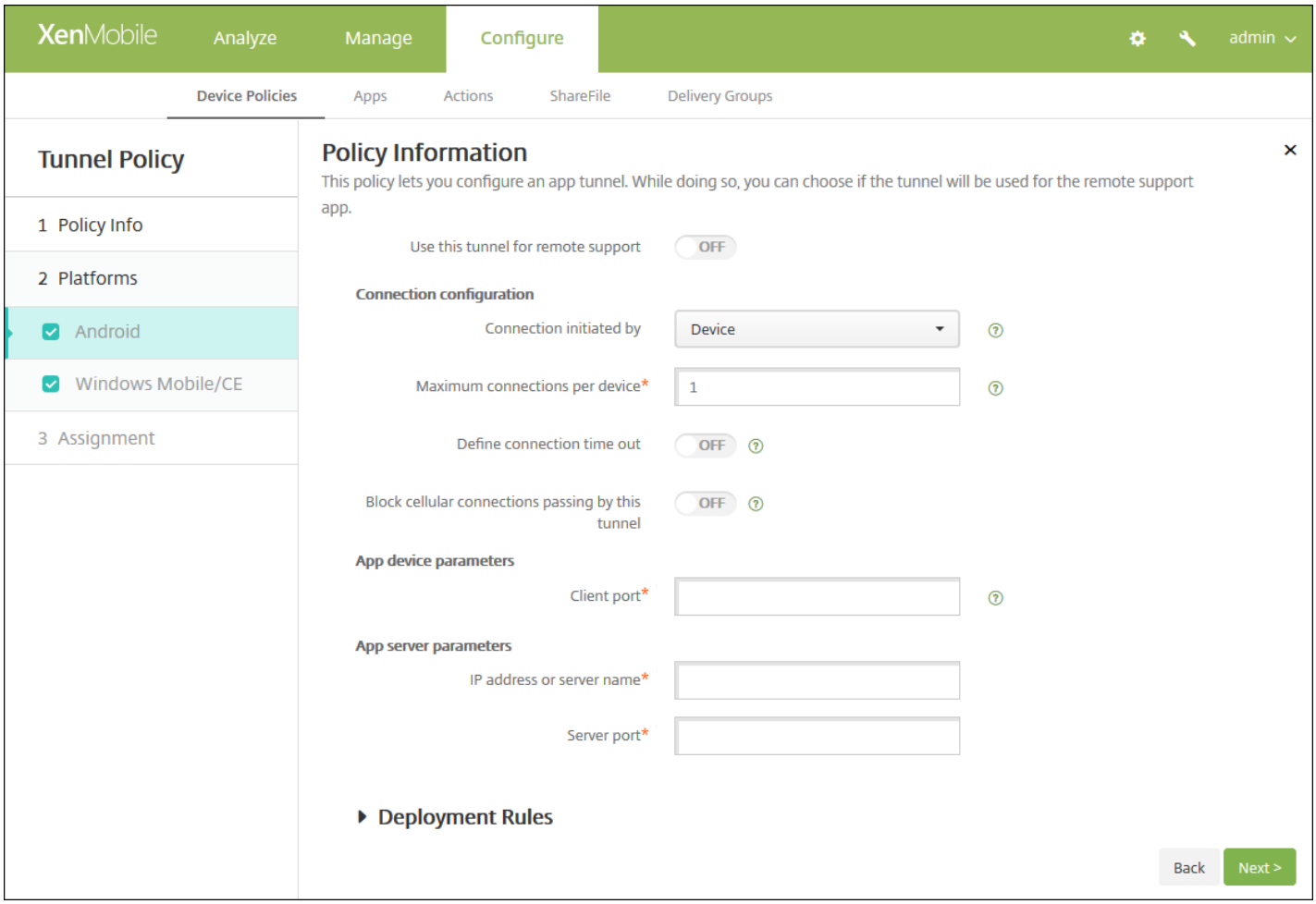
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

Konfigurieren von Android-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Tunnel für Remotesupport verwenden**: Geben Sie an, ob der Tunnel für Remotesupport verwendet werden soll.

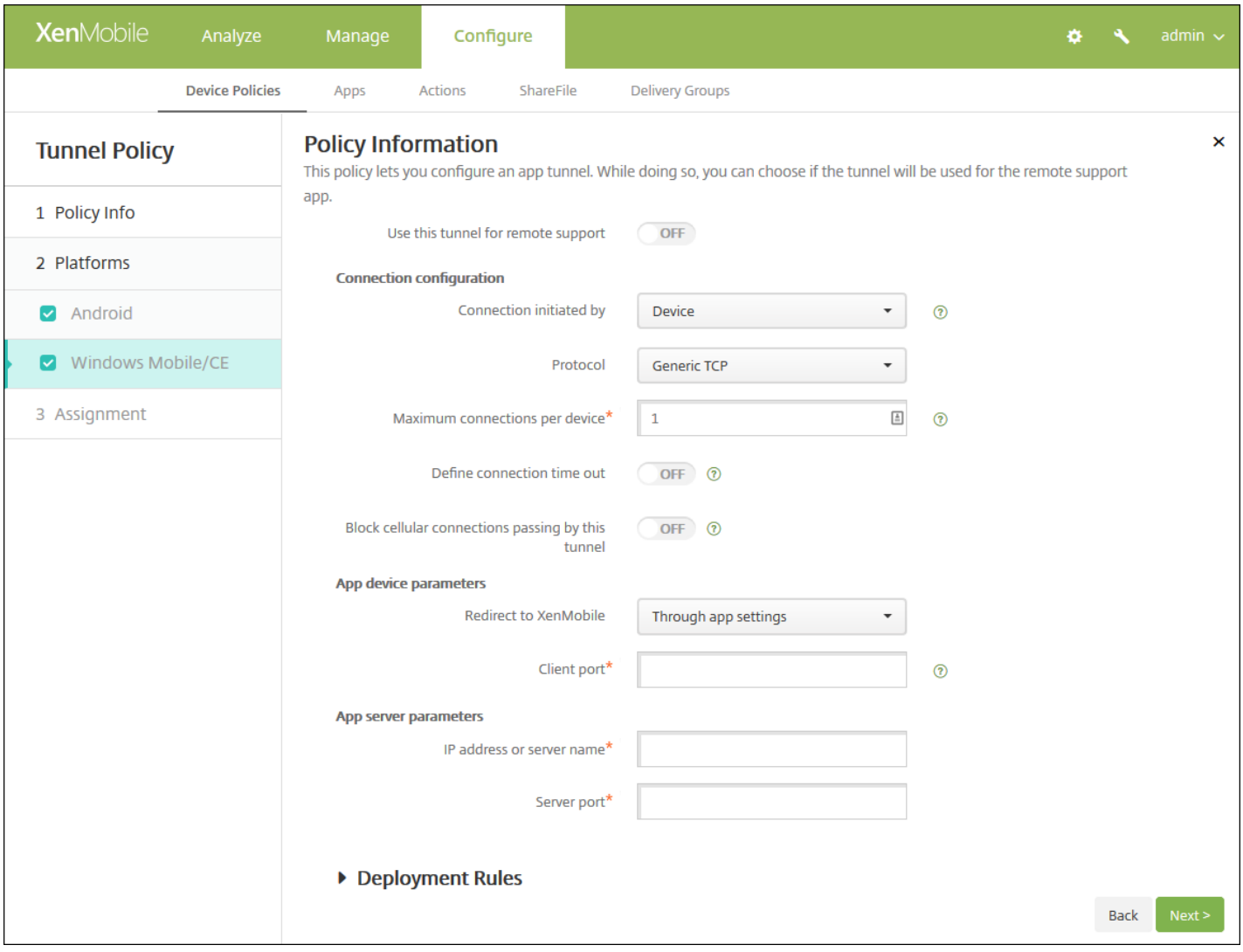
  Hinweis: Die Konfigurationsschritte unterscheiden sich je nachdem, ob Sie hier Remotesupport auswählen.

- Wenn Sie Remotesupport nicht auswählen, führen Sie folgende Schritte aus:
  - **Verbindung Initiiert von**: Klicken Sie auf **Gerät** oder **Server**, um die Quelle für die Aufnahme der Verbindung anzugeben.
  - **Maximale Verbindungen pro Gerät**: Geben Sie die Zahl der gleichzeitig zulässigen TCP-Verbindungen für die App ein. Dieses Feld gilt nur für geräteseitig initiierte Verbindungen.
  - **Verbindungstimeout definieren**: Wählen Sie aus, ob festgelegt werden soll, wie lange eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
    - **Verbindungstimeout: Wenn**Sie für **Verbindungstimeout definieren** die Option **Ein** festgelegt haben, geben Sie hier die Zeitdauer in Sekunden ein, die eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
  - **Mobilnetzverbindungen durch diesen Tunnel blockieren**: Wählen Sie aus, ob der Tunnel beim Roaming blockiert werden soll.
    Hinweis: WiFi- und USB-Verbindungen werden nicht blockiert.

  - **Clientport**: Geben Sie die Nummer des Clientports ein. In den meisten Fällen entspricht diese der Nummer des Serverports.
  - **IP-Adresse oder Servername**: Geben Sie die IP-Adresse oder den Namen des App-Servers ein. Dieses Feld gilt nur für

geräteseitig initiierte Verbindungen.
  - **Serverport**: Geben Sie die Nummer des Serverports ein.
- Wenn Sie Remotesupport auswählen, führen Sie folgende Schritte aus:
  - **Tunnel für Remotesupport verwenden**: Legen Sie **Ein** fest.
  - **Verbindungstimeout definieren**: Wählen Sie aus, ob festgelegt werden soll, wie lange eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
    - **Verbindungstimeout: Wenn**Sie für **Verbindungstimeout definieren** die Option "Ein" festgelegt haben, geben Sie hier die Zeitdauer in Sekunden ein, die eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
  - **SSL-Verbindung verwenden**: Wählen Sie aus, ob für den Tunnel eine SSL-Verbindung verwendet werden soll.
  - **Mobilnetzverbindungen durch diesen Tunnel blockieren**: Wählen Sie aus, ob der Tunnel beim Roaming blockiert werden soll.
    Hinweis: WiFi- und USB-Verbindungen werden nicht blockiert.

Konfigurieren von Windows Mobile-/CE-Einstellungen



Konfigurieren Sie folgende Einstellungen:

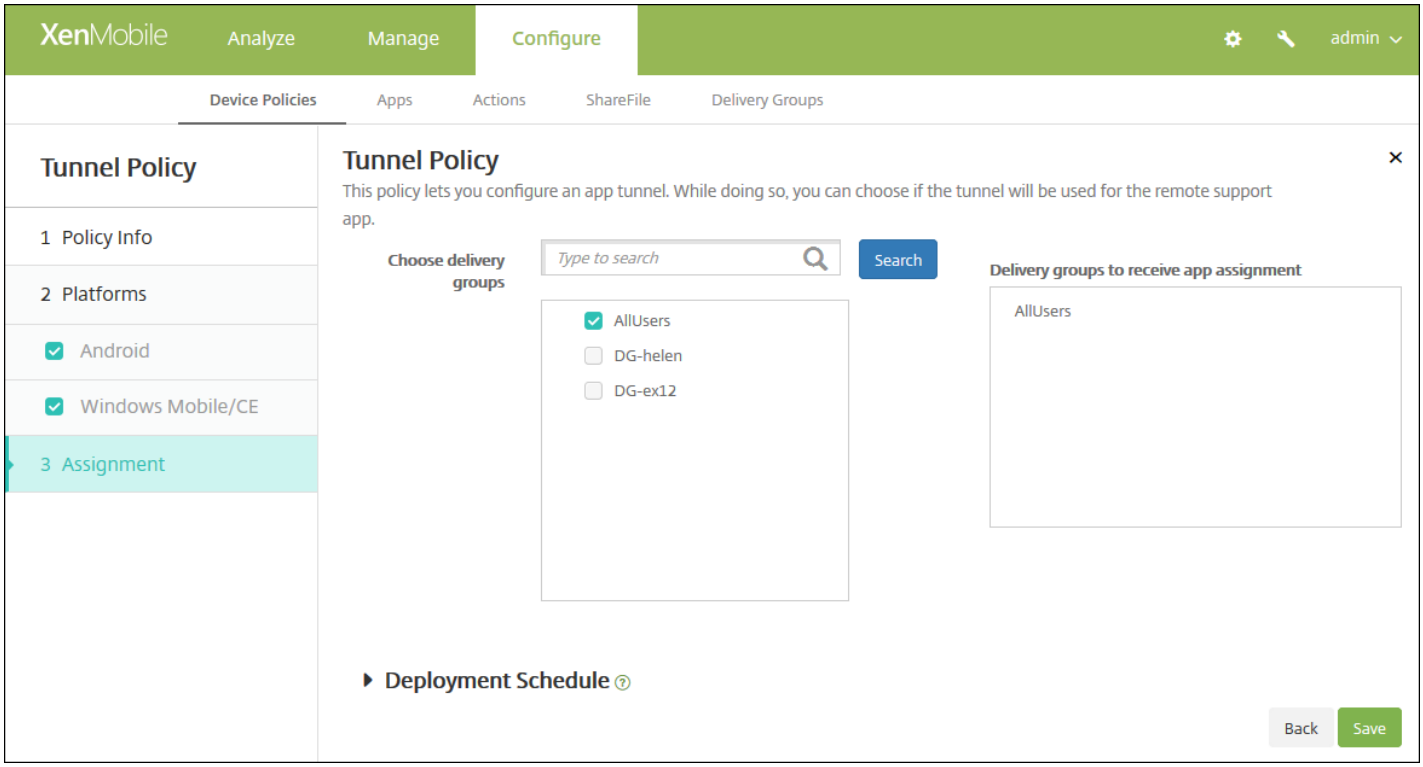
- **Tunnel für Remotesupport verwenden**: Geben Sie an, ob der Tunnel für Remotesupport verwendet werden soll.

Hinweis: Die Konfigurationsschritte unterscheiden sich je nachdem, ob Sie hier Remotesupport auswählen.

- Wenn Sie Remotesupport nicht auswählen, führen Sie folgende Schritte aus:
  - Verbindung**initiiert von: Klicken**Sie auf **Gerät** oder **Server**, um die Quelle für die Aufnahme der Verbindung anzugeben.
  - **Protokoll**: Klicken Sie in der Liste auf das Protokoll, das verwendet werden soll. Der Standardwert ist **Generisches TCP**.
  - **Maximale Verbindungen pro Gerät**: Geben Sie die Zahl der gleichzeitig zulässigen TCP-Verbindungen für die App ein. Dieses Feld gilt nur für geräteseitig initiierte Verbindungen.
  - **Verbindungstimeout definieren**: Wählen Sie aus, ob festgelegt werden soll, wie lange eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
    - **Verbindungstimeout: Wenn**Sie für **Verbindungstimeout definieren** die Option **Ein** festgelegt haben, geben Sie hier die Zeitdauer in Sekunden ein, die eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
  - **Mobilnetzverbindungen durch diesen Tunnel blockieren**: Wählen Sie aus, ob der Tunnel beim Roaming blockiert werden soll.
    Hinweis: WiFi- und USB-Verbindungen werden nicht blockiert.
  - **Umleiten zu XenMobile**: Klicken Sie in der Liste auf die Methode des Verbindungsaufbaus zwischen Gerät und XenMobile. Der Standardwert ist **Über App-Einstellungen**.
    - Bei Verwendung von **Mit einem lokalen Alias** geben Sie den Alias in **Lokaler Alias** ein. Der Standardwert ist **localhost**.
    - Bei Verwendung von **IP-Adressbereich** geben Sie die erste IP-Adresse des Bereichs in **IP-Adressbereich von** und die letzte IP-Adresse in **IP-Adressbereich bis** ein.
  - **Clientport**: Geben Sie die Nummer des Clientports ein. In den meisten Fällen entspricht diese der Nummer des Serverports.
  - **IP-Adresse oder Servername**: Geben Sie die IP-Adresse oder den Namen des App-Servers ein. Dieses Feld gilt nur für geräteseitig initiierte Verbindungen.
  - **Serverport**: Geben Sie die Nummer des Serverports ein.
- Wenn Sie Remotesupport auswählen, führen Sie folgende Schritte aus:
  - **Tunnel für Remotesupport verwenden**: Legen Sie **Ein** fest.
  - **Verbindungstimeout definieren**: Wählen Sie aus, ob festgelegt werden soll, wie lange eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
    - **Verbindungstimeout: Wenn**Sie für "Verbindungstimeout definieren" die Option "Ein" festgelegt haben, geben Sie hier die Zeitdauer in Sekunden ein, die eine App im Leerlauf sein darf, bevor der Tunnel geschlossen wird.
  - **SSL-Verbindung verwenden**: Wählen Sie aus, ob für den Tunnel eine SSL-Verbindung verwendet werden soll.
  - **Mobilnetzverbindungen durch diesen Tunnel blockieren**: Wählen Sie aus, ob der Tunnel beim Roaming blockiert werden soll.
    Hinweis: WiFi- und USB-Verbindungen werden nicht blockiert.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Tunnelrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

App-Deinstallationsrichtlinien für Geräte

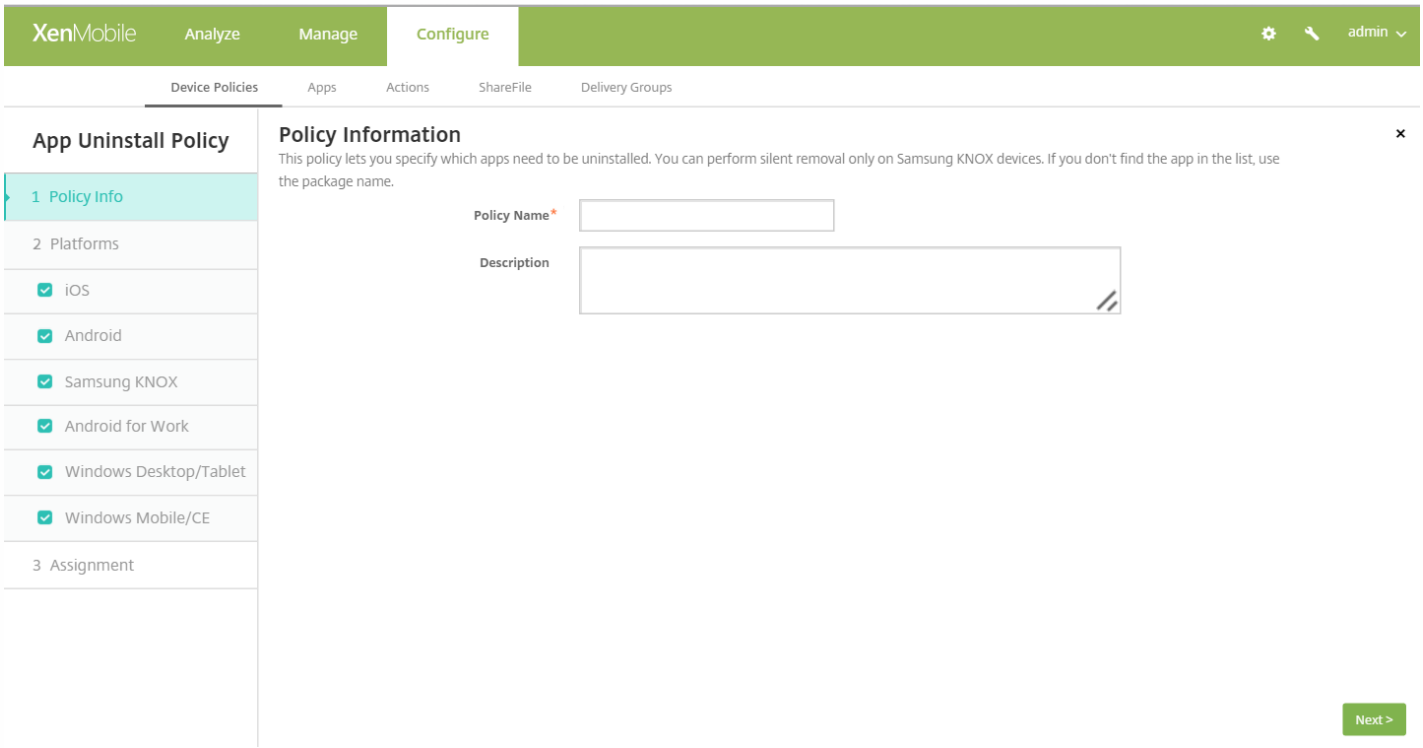
Jul 28, 2016

Sie können App-Deinstallationsrichtlinien für die folgenden Plattformen erstellen: iOS, Android, Samsung KNOX, Android for Work, Windows-Desktop/Tablet und Windows Mobile/CE. 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 **Konfigurieren > Gerätерichtlinien**. Die Seite **Gerätерichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **App-Deinstallation**. Die Seite **App-Deinstallation** wird angezeigt.



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

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

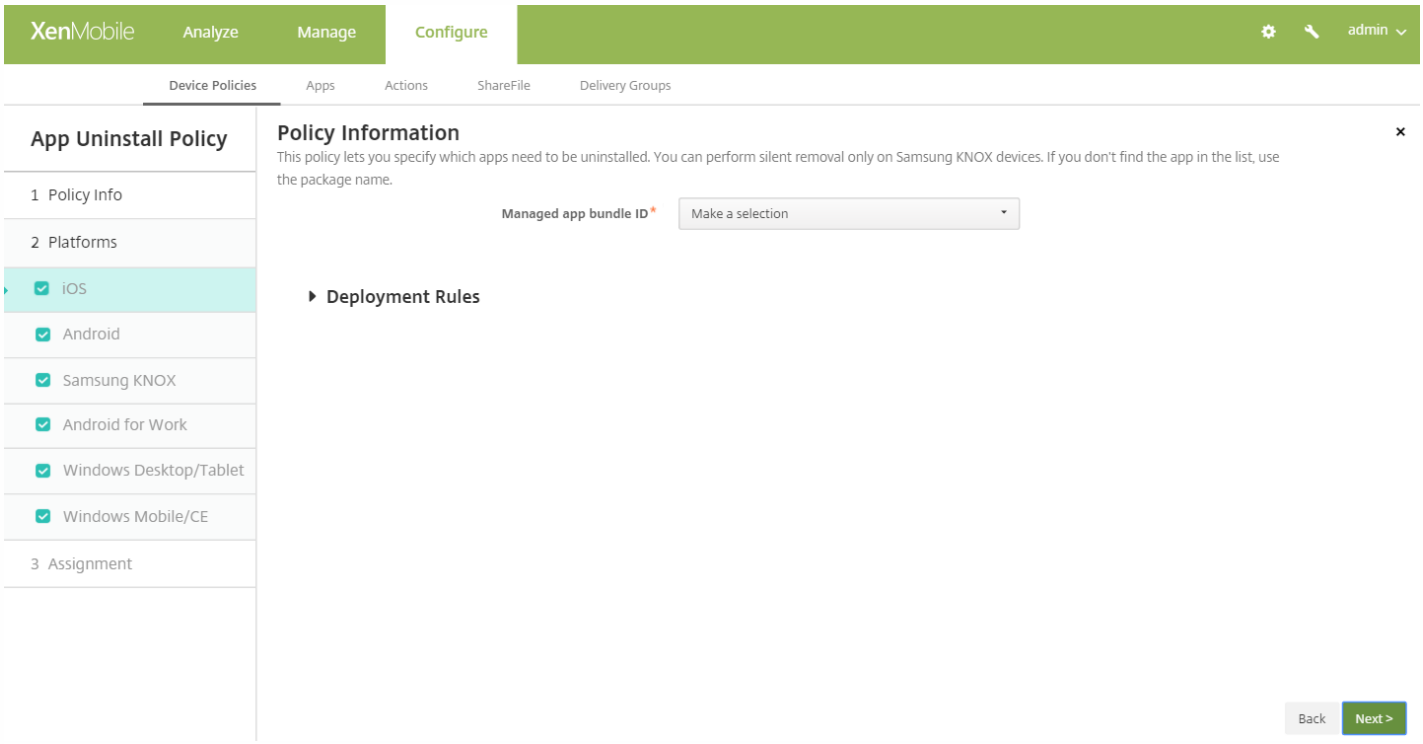
5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der

Bereitstellungsregeln für diese Plattform unter Schritt 7.

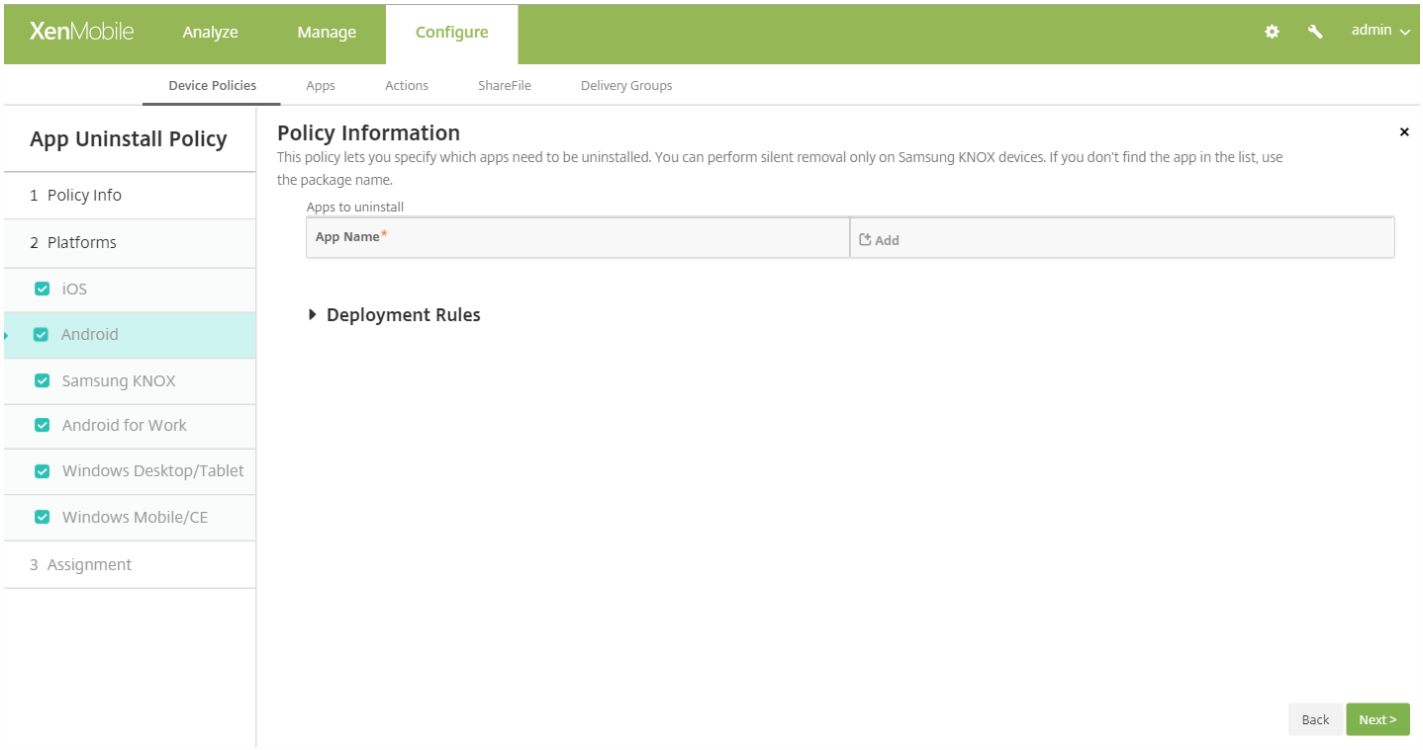
Konfigurieren von iOS-Einstellungen



Konfigurieren Sie folgende Einstellung:

- **Paket-ID für verwaltete App**: Klicken Sie in der Liste auf eine vorhandene App oder auf **Hinzufügen**. Wenn keine Apps für diese Plattform konfiguriert sind, ist die Liste leer und Sie müssen eine neue App hinzufügen.
  - Wenn Sie auf **Hinzufügen** klicken, wird ein Feld eingeblendet, in dem Sie einen Namen für die App eingeben können.

Konfigurieren aller anderen Plattformeinstellungen



Konfigurieren Sie folgende Einstellung:

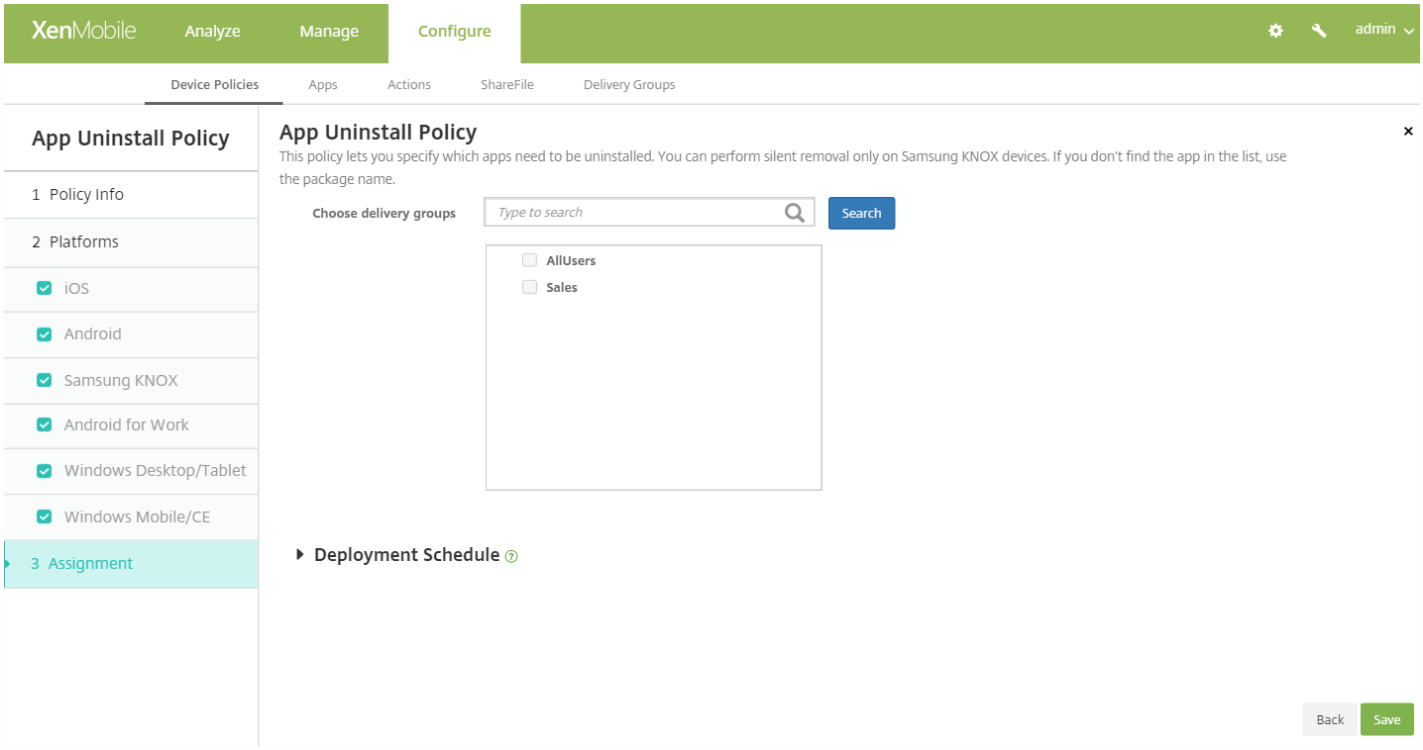
- **Apps zum Deinstallieren**: Klicken Sie für jede App, die Sie hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **App-Name**: Klicken Sie in der Liste auf eine vorhandene App oder klicken Sie auf **Add**, um einen neuen App-Namen einzugeben. Wenn keine Apps für diese Plattform konfiguriert sind, ist die Liste leer und Sie müssen neue Apps hinzufügen.
  - Klicken Sie auf **Hinzufügen**, um die App hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

    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 **Löschen** zum Löschen des Eintrags oder auf **Bearbeiten**, 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Deinstallationsrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Einschränkungsrichtlinien für die App-Deinstallation

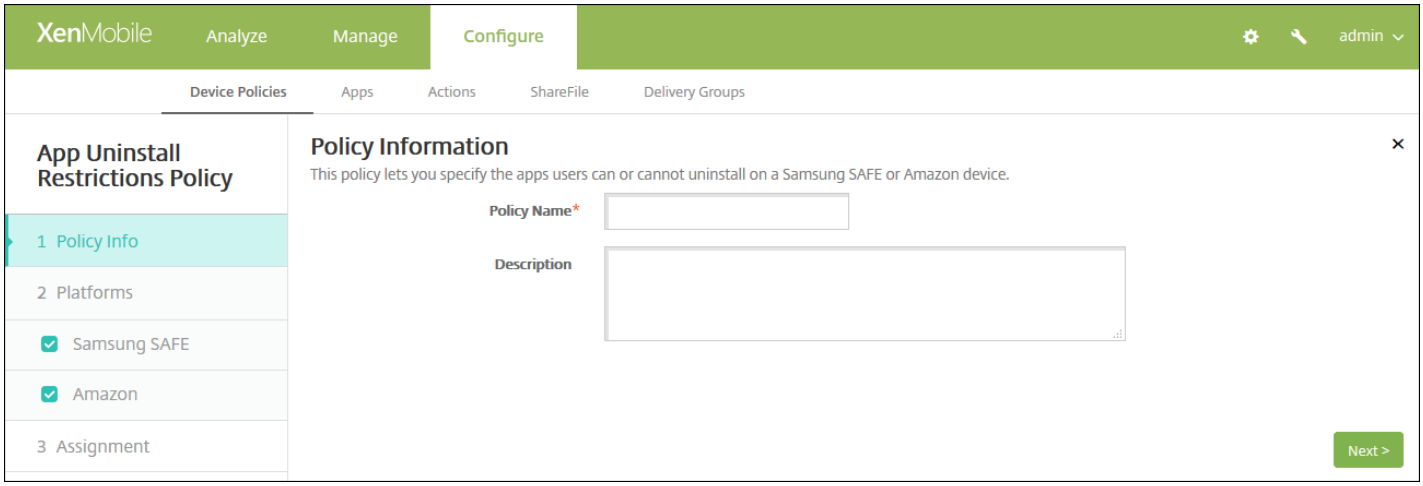
Jul 28, 2016

Sie können vorgeben, welche Apps Benutzer von einem Samsung SAFE- oder Amazon-Gerät deinstallieren dürfen.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Geräterichtlinien**.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

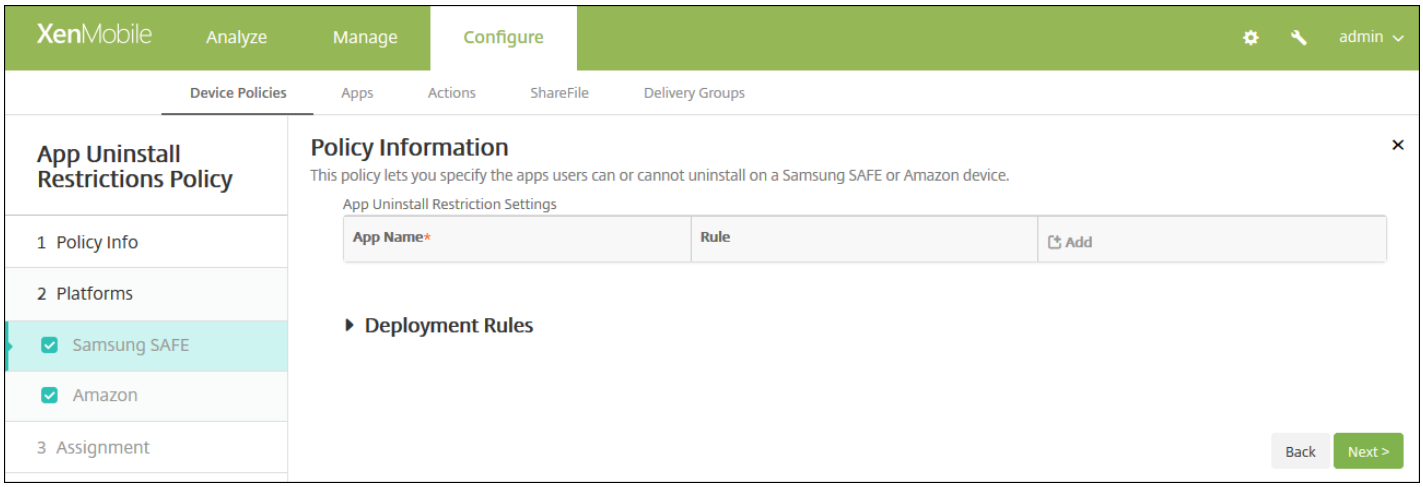
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Einschränkungen der App-Deinstallation**. Die Seite **Einschränkungen der App-Deinstallation** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.



6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren,

deaktivieren Sie die anderen.

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

7. Konfigurieren Sie für jede ausgewählte Plattform die folgenden Einstellungen:

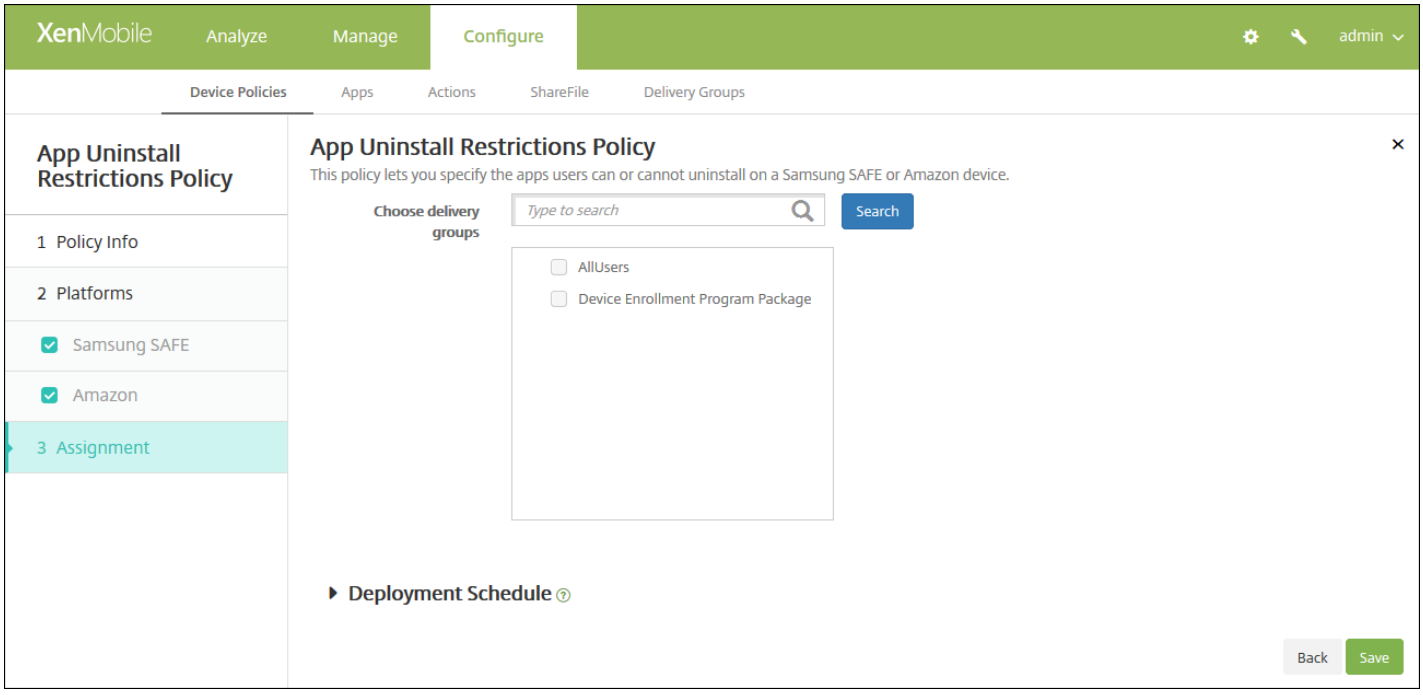
- **Einstellungen zum Einschränken der App-Deinstallation**: Klicken Sie für jede Regel, die Sie hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **App-Name**: Klicken Sie in der Liste auf eine vorhandene App oder klicken Sie auf **Hinzufügen**, um eine neue App hinzuzufügen.
  - **Regel**: Wählen Sie aus, ob Benutzer die App deinstallieren können sollen. Standardmäßig ist die Deinstallation zulässig.
  - Klicken Sie auf **Speichern** oder **Abbrechen**.

    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 **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

8. Konfigurieren der Bereitstellungsregeln

9. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Richtlinie wird angezeigt.



10. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

11. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Browserrichtlinien für Geräte

Jul 28, 2016

Sie können Browserrichtlinien für Samsung SAFE-, Samsung KNOX- und Android for Work-Geräte erstellen, um festzulegen, ob die Benutzer den Browser verwenden können, oder um die Browserfunktionen einzuschränken, die auf den Geräten verwendet werden können. Auf Samsung-Geräten können Sie den Browser vollständig deaktivieren oder Popupfenster, JavaScript, Cookies, automatisches Ausfüllen und Betrugswarnungen aktivieren oder deaktivieren. Auf Android for Work-Geräten können Sie URLs einer Sperr- oder Positivliste hinzufügen und sichere Browserlesezeichen hinzufügen.

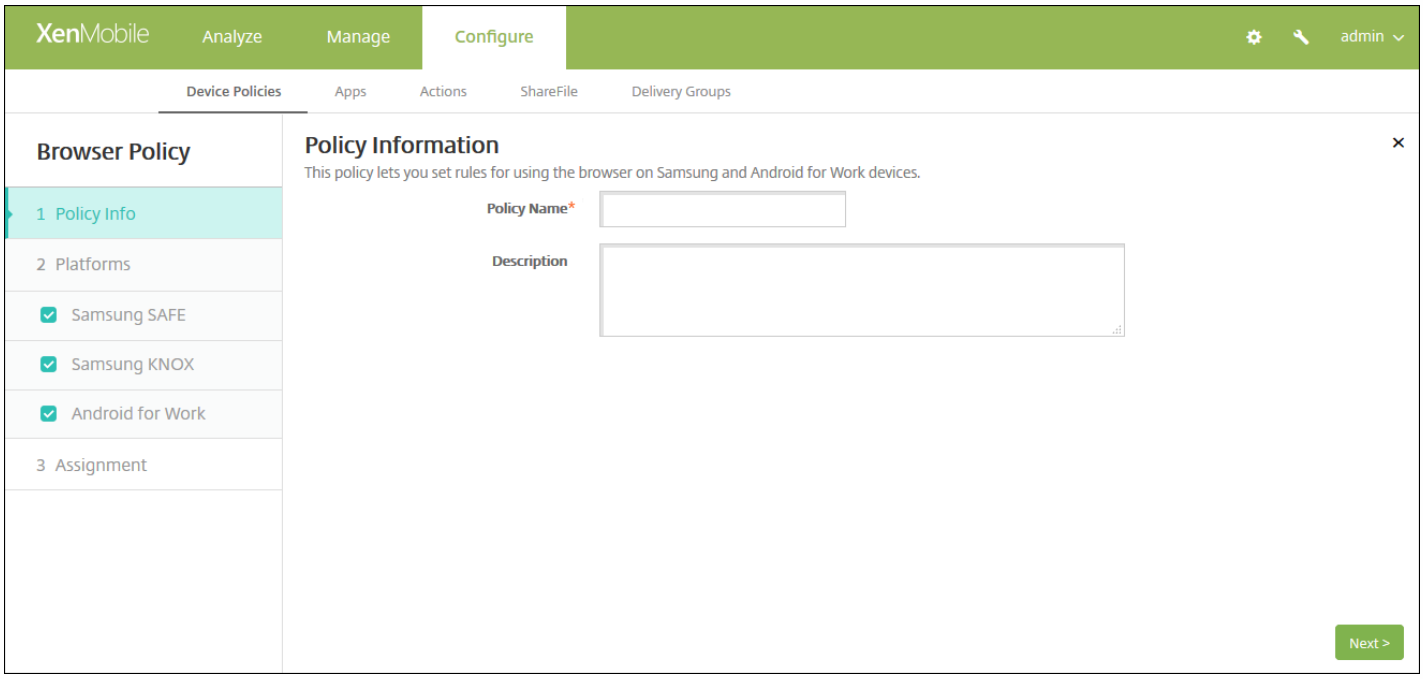
Samsung SAFE- und Samsung KNOX-Einstellungen

Android for Work-Einstellungen

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

2. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Klicken Sie auf **Mehr** und dann unter **Apps** auf **Browser**. Die Seite **Browser** wird angezeigt.



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

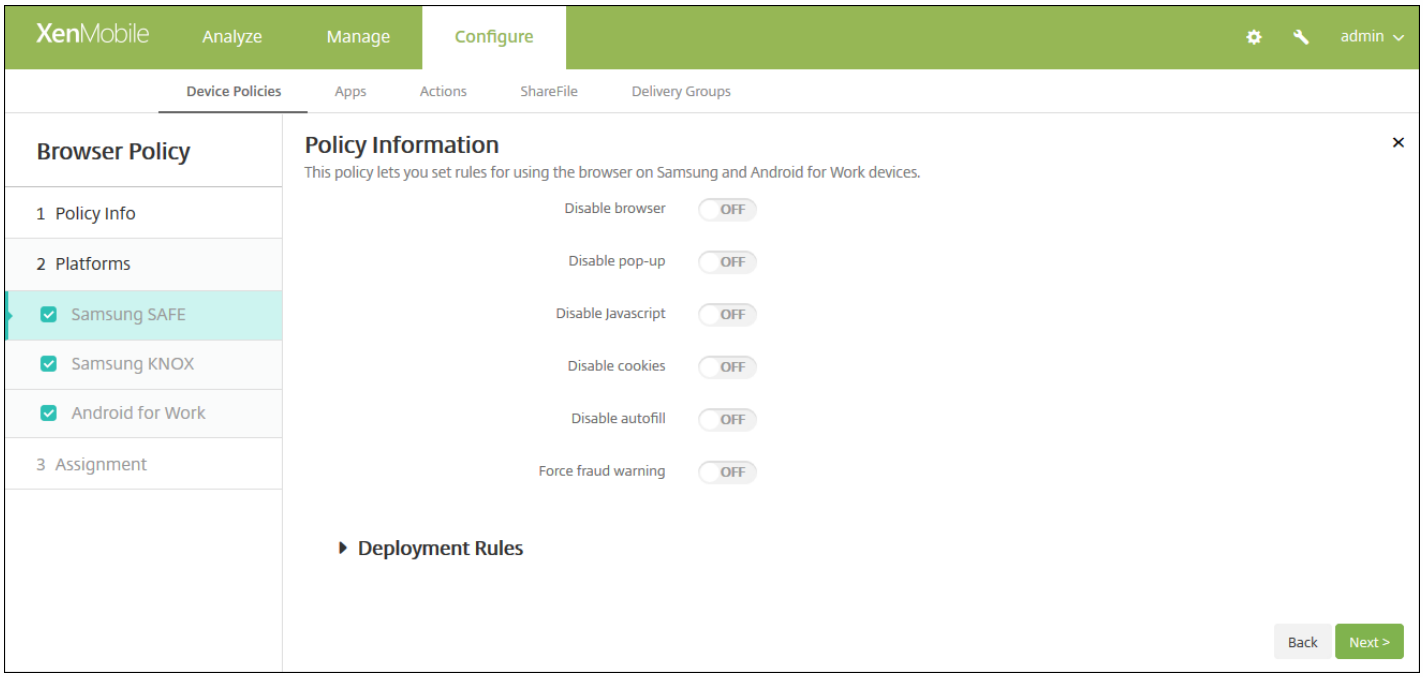
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

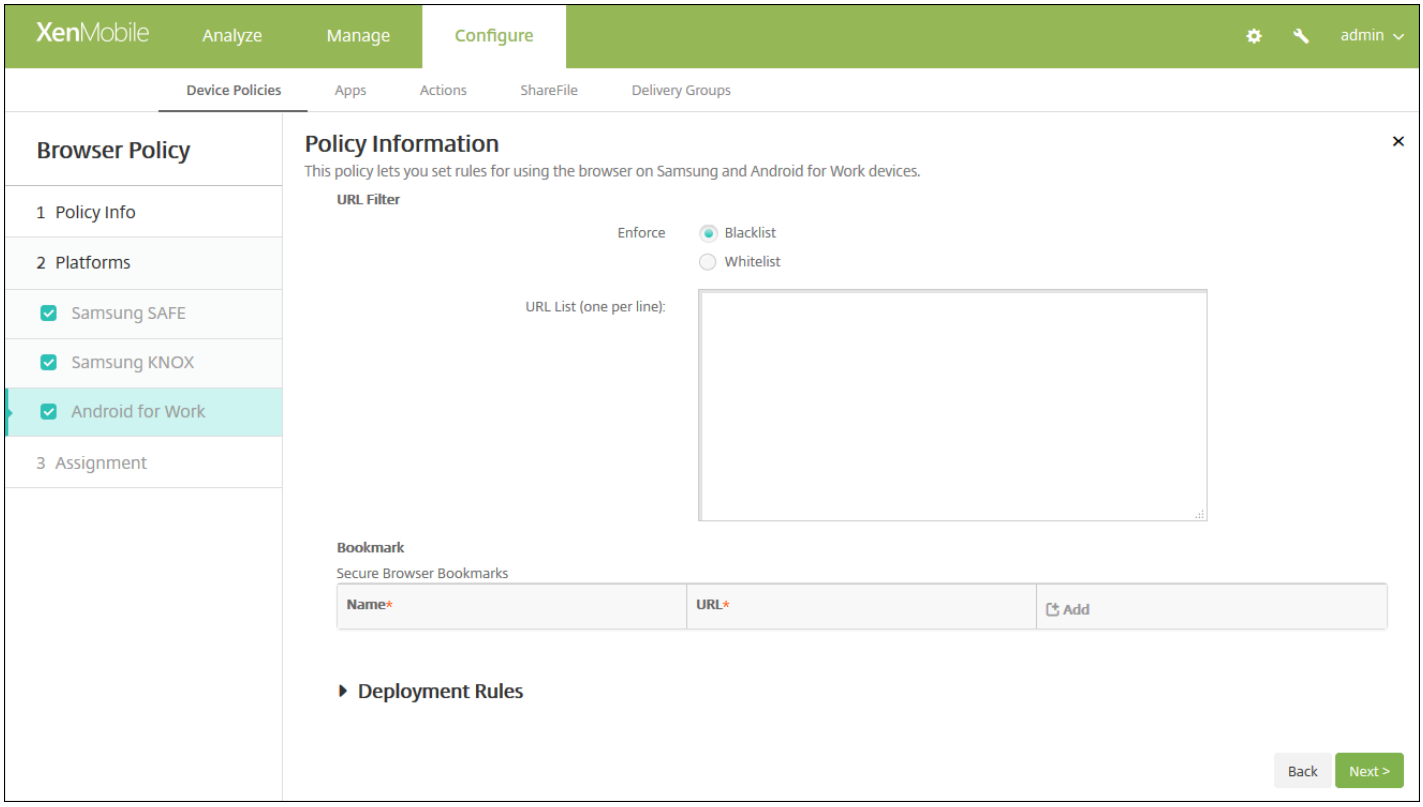
Konfigurieren von Samsung SAFE- und Samsung KNOX-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Browser deaktivieren**: Wählen Sie aus, ob der Samsung-Browser auf den Geräten komplett deaktiviert werden soll. Der Standardwert ist **AUS**, d. h. die Benutzer können den Browser verwenden. Wenn Sie den Browser deaktivieren, werden die nachfolgend aufgeführten Optionen ausgeblendet.
- **Popups deaktivieren**: Wählen Sie aus, ob Popupfenster im Browser zugelassen werden sollen.
- **JavaScript deaktivieren**: Wählen Sie aus, ob die Ausführung von JavaScript im Browser zugelassen werden soll.
- **Cookies deaktivieren**: Wählen Sie aus, ob Cookies zugelassen werden sollen.
- **AutoAusfüllen deaktivieren**: Wählen Sie aus, ob die Funktion zum automatischen Ausfüllen im Browser aktiviert werden soll.
- **Betrugswarnung erzwingen**: Wählen Sie aus, ob eine Warnung angezeigt werden soll, wenn Benutzer eine betrügerische oder manipulierte Website besuchen.

Konfigurieren von Amazon für Work-Einstellungen

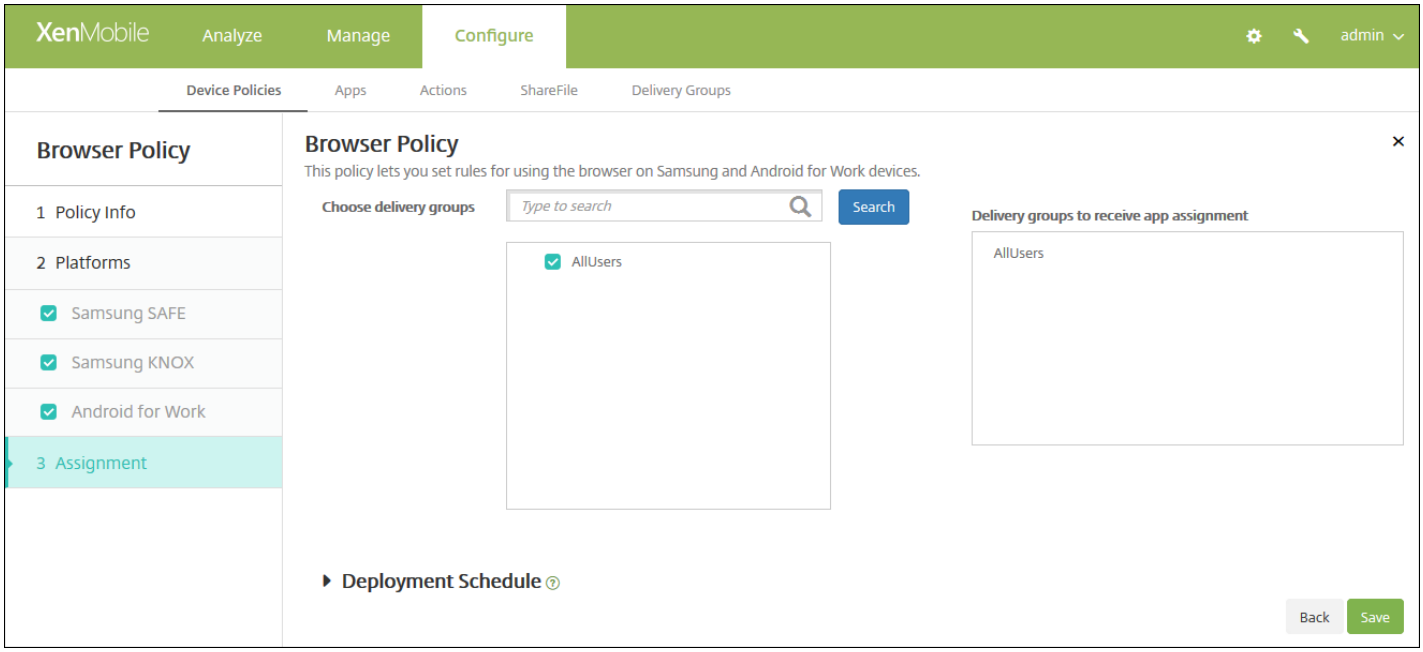


Konfigurieren Sie folgende Einstellungen:

- Konfigurieren Sie unter **URL-Filter** die folgenden Einstellungen:
  - **Erzwingen**: Wählen Sie **Sperrliste** oder **Positivliste** aus. Wenn Sie **Sperrliste** auswählen, können die Benutzer auf alle URLs *außer* den von Ihnen angegebenen zugreifen. Wenn Sie **Positivliste** auswählen, können die Benutzer *nur* auf die URLs zugreifen, die Sie angeben.
  - **URL-Liste**: Geben Sie die URLs (eine pro Zeile) für die ausgewählte URL-Liste ein und klicken Sie auf **Erzwingen**.
- Klicken Sie auf für **Lesezeichen** auf **Hinzufügen** und füllen Sie die Felder **Name** und **URL** für die Lesezeichen aus, die im sicheren Browser der Benutzer erscheinen sollen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Browserrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Kalenderrichtlinien

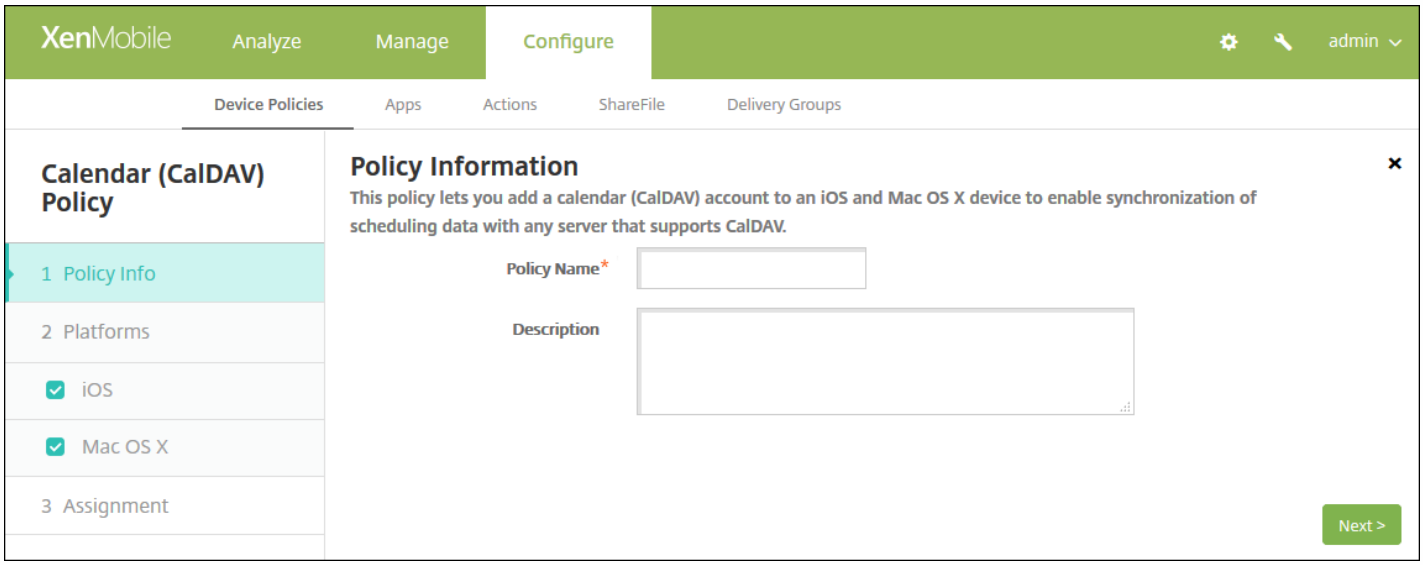
Jul 28, 2016

Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen eines Kalenderkontos (CalDAV) zu iOS- oder Mac OS X-Geräten einrichten, damit die Benutzer Kalendereinträge mit einem beliebigen Server, der CalDAV unterstützt, synchronisieren können.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie unter **Endbenutzer** auf **Kalender (CalDAV)**. Die Seite für die Richtlinieninformationen der Richtlinie **Kalender (CalDAV)** wird angezeigt.



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

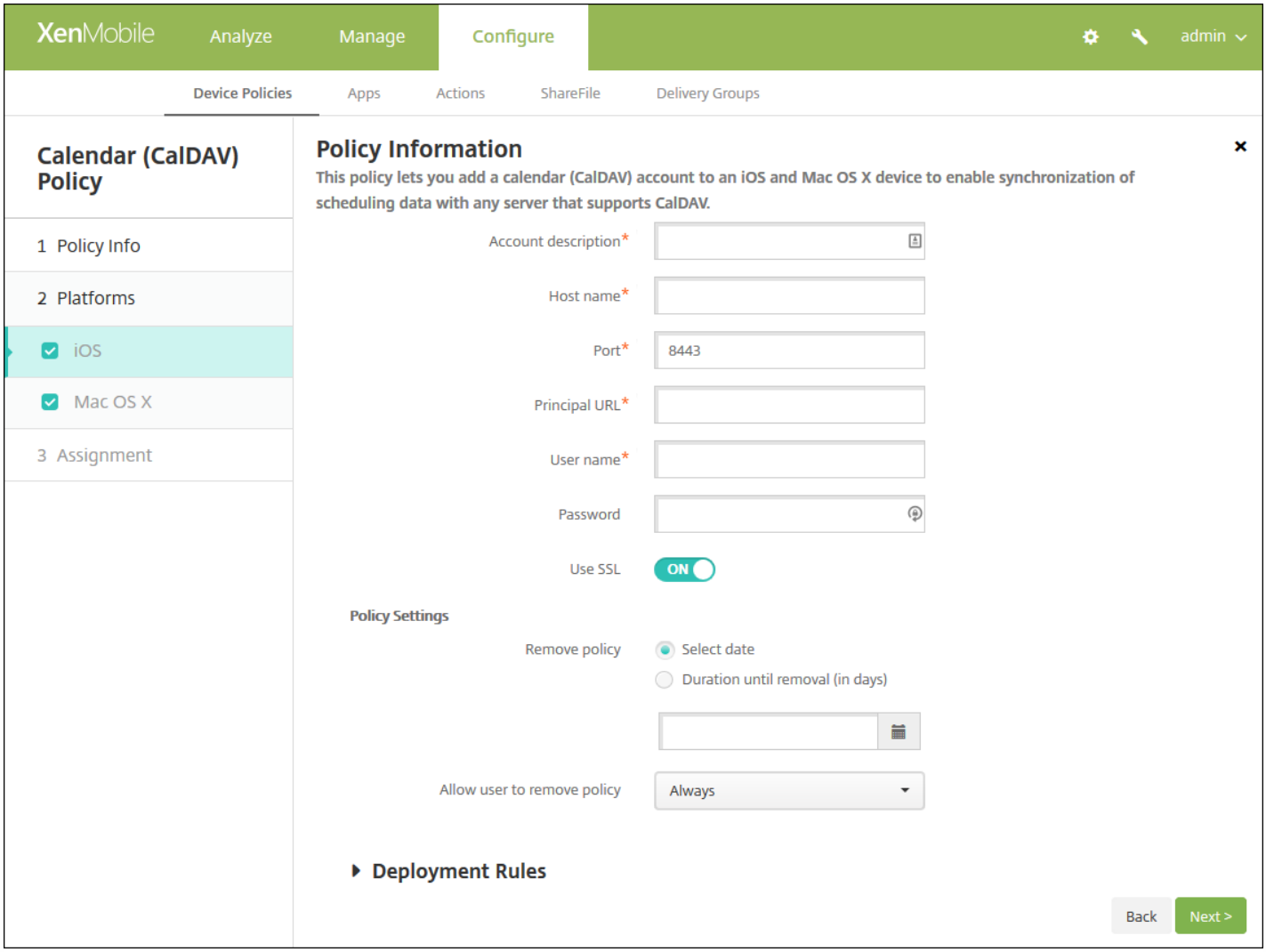
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

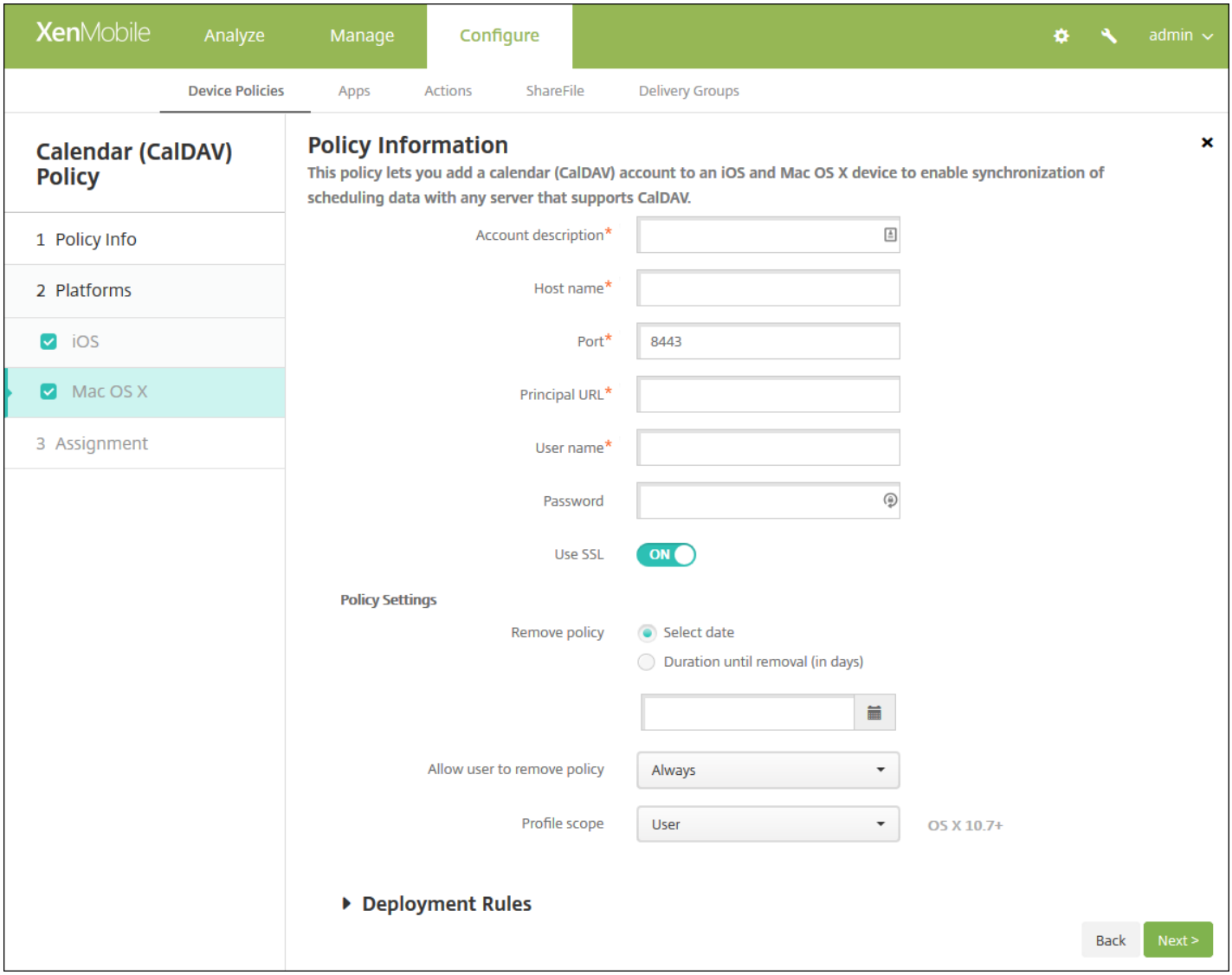
Konfigurieren von iOS-Einstellungen



Konfigurieren Sie die folgenden Einstellungen:

- **Kontobeschreibung**: Geben Sie eine Kontobeschreibung ein. Diese Angabe ist erforderlich.
- **Hostname**: Geben Sie die Adresse des CalDAV-Servers ein. Diese Angabe ist erforderlich.
- **Port**: Geben Sie den Port für die Verbindung mit dem CalDAV-Server ein. Diese Angabe ist erforderlich. Der Standardwert ist **8443**.
- **Principal URL**: Geben Sie die Basis-URL des Kalenders des Benutzers ein.
- **Benutzername**: Geben Sie den Anmeldenamen des Benutzers ein. Diese Angabe ist erforderlich.
- **Kennwort**: Geben Sie ein optionales Benutzerkennwort ein.
- **SSL verwenden**: Wählen Sie aus, ob für die Verbindung mit dem CalDAV-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist **EIN**.
- **Richtlinieneinstellungen**
  - Klicken Sie für **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

Konfigurieren von Mac OS X-Einstellungen



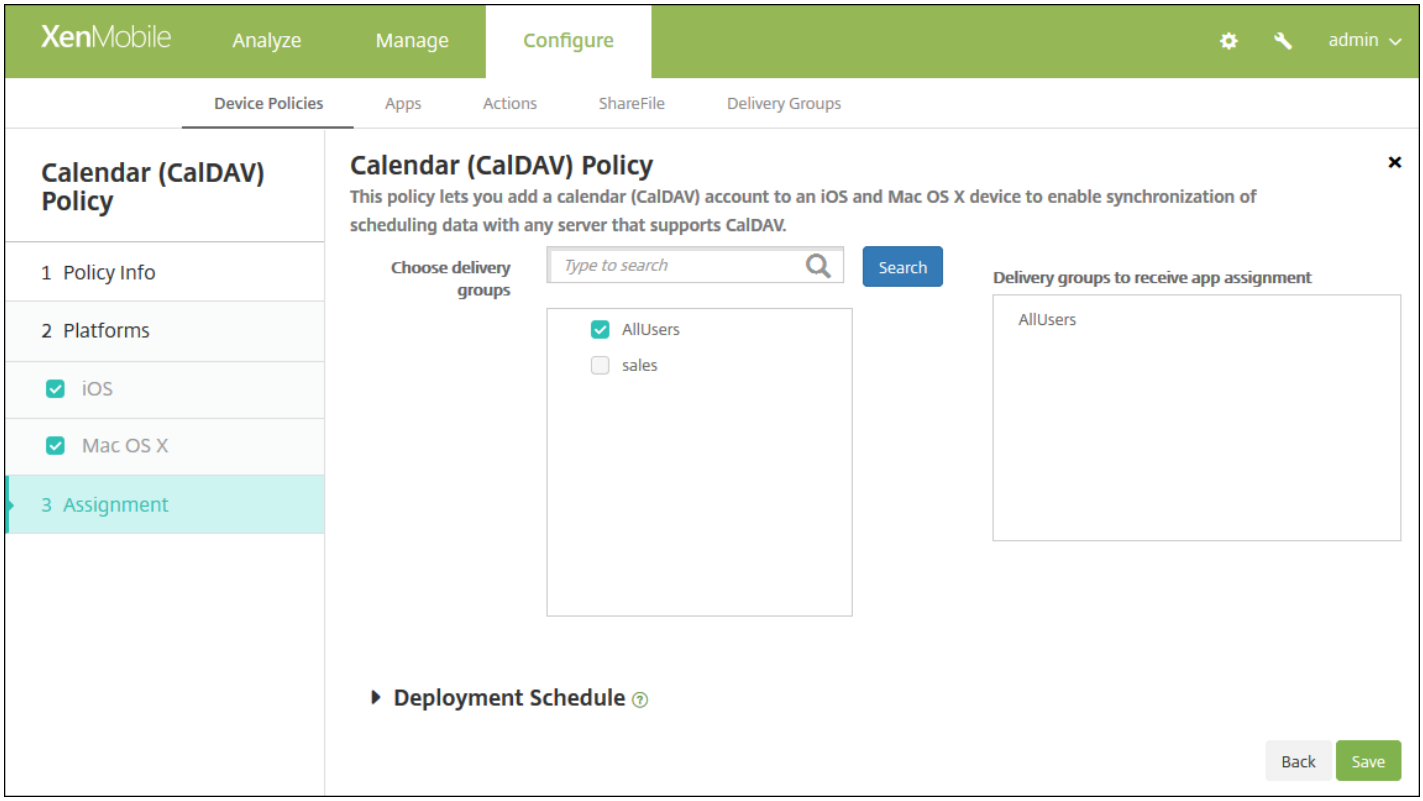
Konfigurieren Sie die folgenden Einstellungen:

- **Kontobeschreibung**: Geben Sie eine Kontobeschreibung ein. Diese Angabe ist erforderlich.
- **Hostname**: Geben Sie die Adresse des CalDAV-Servers ein. Diese Angabe ist erforderlich.
- **Port**: Geben Sie den Port für die Verbindung mit dem CalDAV-Server ein. Diese Angabe ist erforderlich. Der Standardwert ist **8443**.
- **Principal URL**: Geben Sie die Basis-URL des Kalenders des Benutzers ein.
- **Benutzername**: Geben Sie den Anmeldenamen des Benutzers ein. Diese Angabe ist erforderlich.
- **Kennwort**: Geben Sie ein optionales Benutzerkennwort ein.
- **SSL verwenden**: Wählen Sie aus, ob für die Verbindung mit dem CalDAV-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist **EIN**.
- **Richtlinieneinstellungen**
  - Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.
  - Klicken Sie neben **Gültigkeitsbereich für Profil** auf **Benutzer** oder **System**. Der Standardwert ist **Benutzer**. Diese

Option ist nur für OS X 10.7 und höher verfügbar.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Kalenderrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Mobilfunkgeräterichtlinie

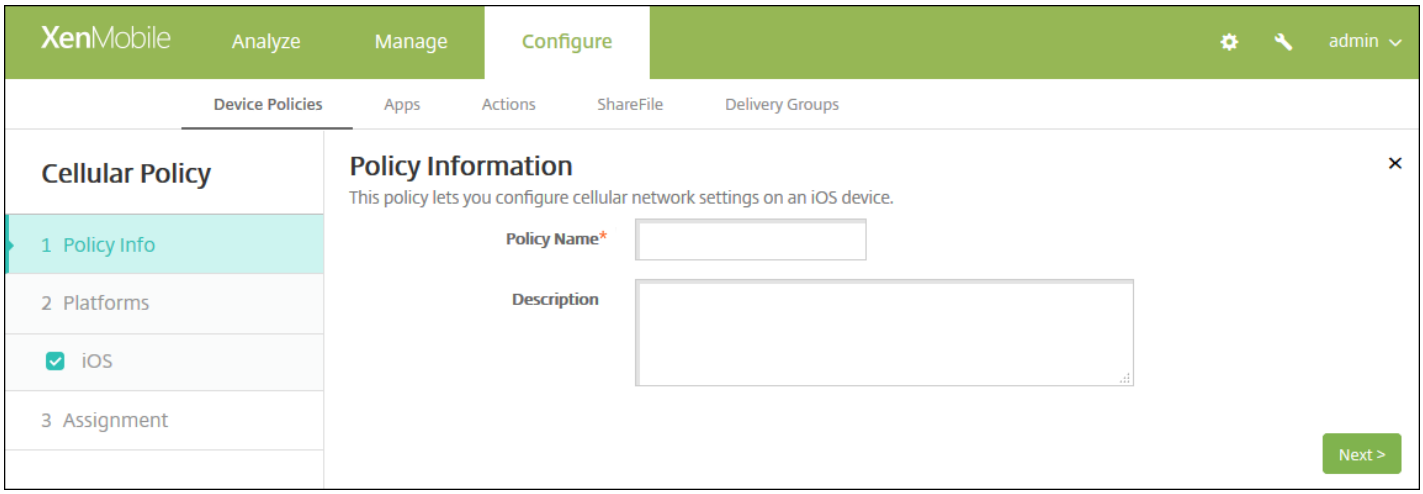
Jul 28, 2016

Mit dieser Richtlinie können Sie Einstellungen für das Mobilfunknetz auf iOS-Geräten konfigurieren.

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

2. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.

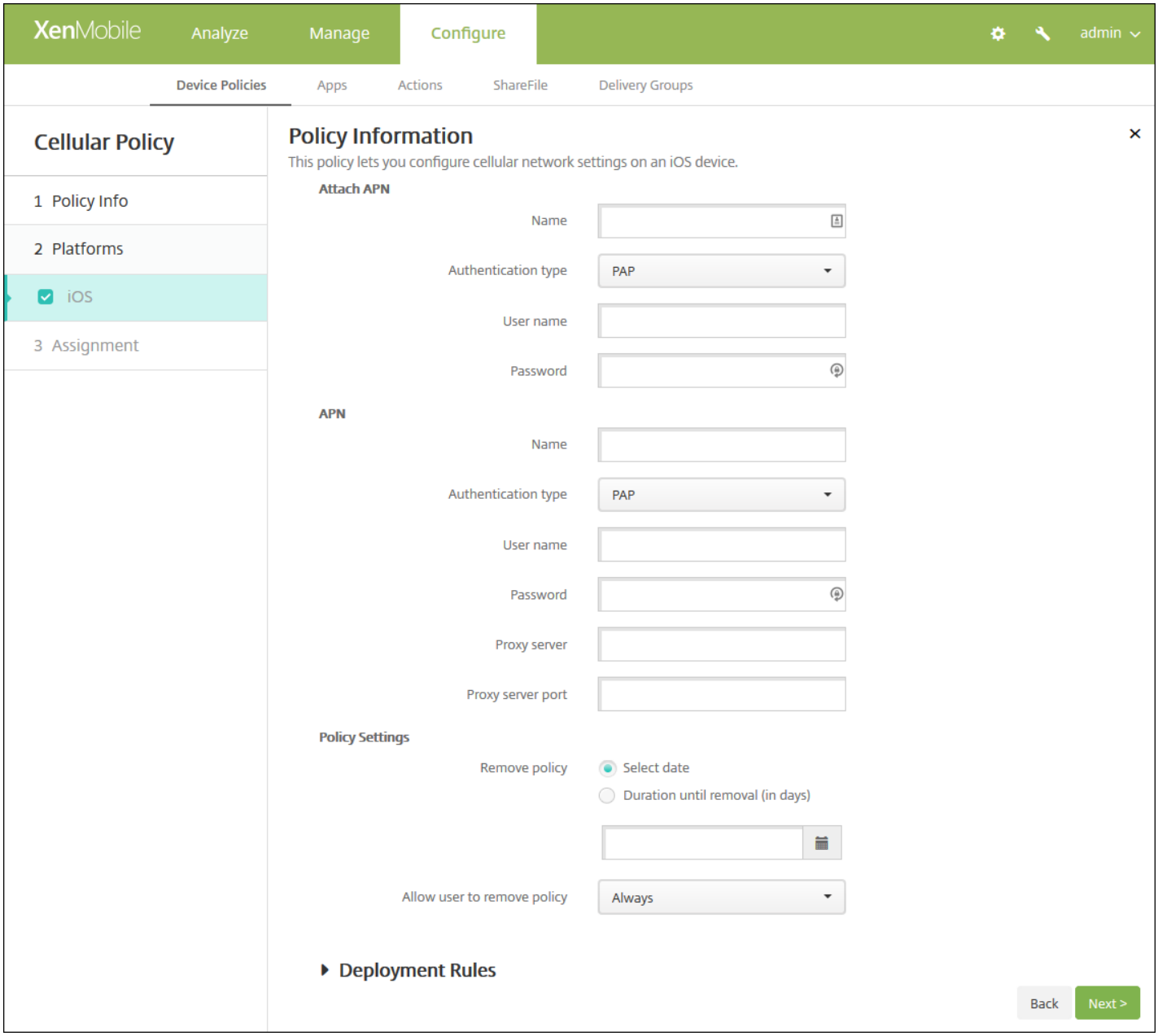
3. Erweitern Sie **Mehr** und klicken Sie unter **Netzwerkzugriff** auf **Mobilnetz**. Die Seite **Mobilnetz** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite mit den Plattforminformationen für **iOS** wird angezeigt.



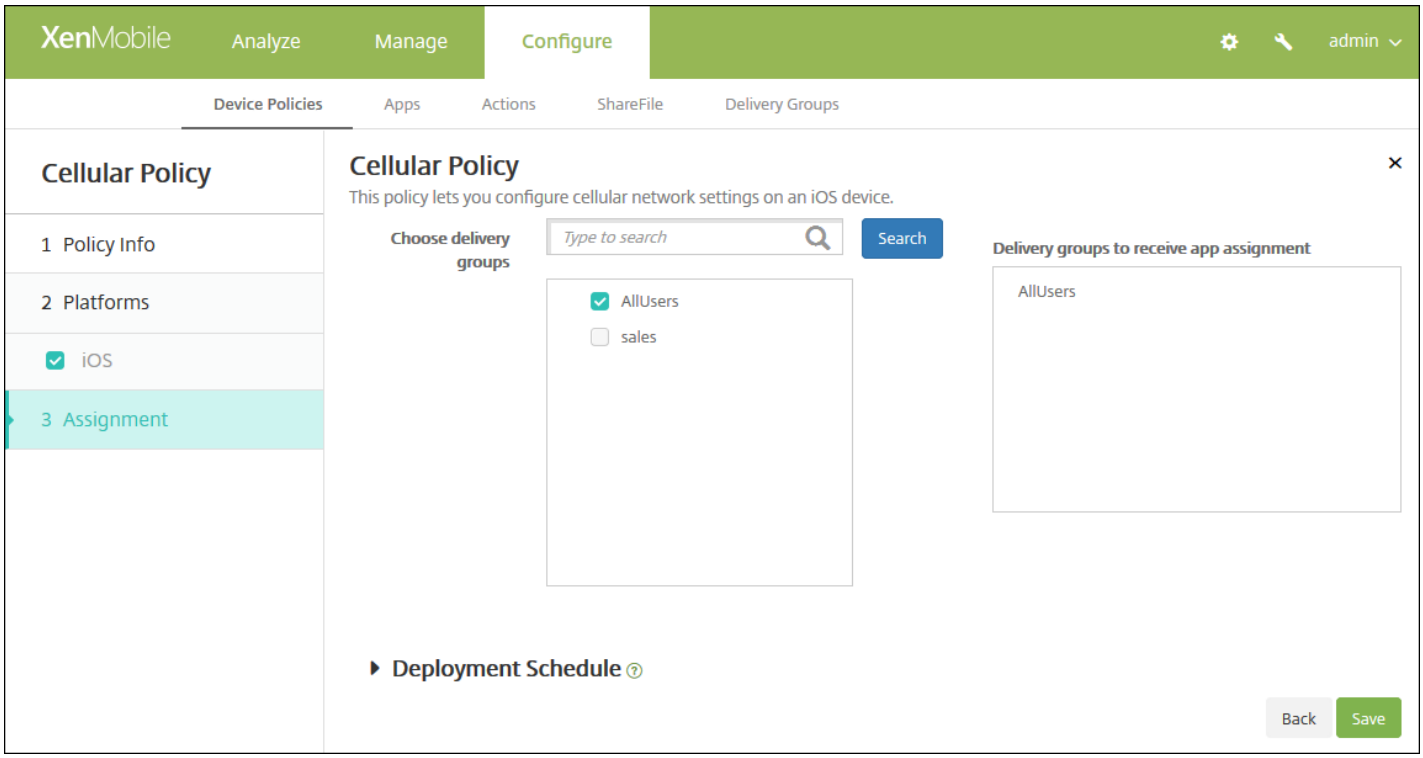
6. Konfigurieren Sie die folgenden Einstellungen:

- **APN anfügen**
  - **Name**: Geben Sie einen Namen für die Konfiguration ein.
  - **Authentifizierungstyp**: Klicken Sie in der Liste auf das Challenge Handshake Authentication-Protokoll (**CHAP**) oder das Password Authentication-Protokoll (**PAP**). Die Standardeinstellung ist **PAP**.
  - **Benutzername**: Geben Sie den Benutzernamen für die Authentifizierung ein.
- **APN**
  - **Name**: Geben Sie einen Namen für die APN-Konfiguration ein.
  - **Authentifizierungstyp**: Klicken Sie in der Liste auf **CHAP** oder **PAP**. Die Standardeinstellung ist **PAP**.
  - **Benutzername**: Geben Sie den Benutzernamen für die Authentifizierung ein.
  - **Kennwort**: Geben Sie ein Kennwort für die Authentifizierung ein.
  - **Proxyserver**: Geben Sie die Netzwerkadresse des Proxyservers ein.

- **Richtlinieneinstellungen**
  - Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Verbindungsmanagerrichtlinie

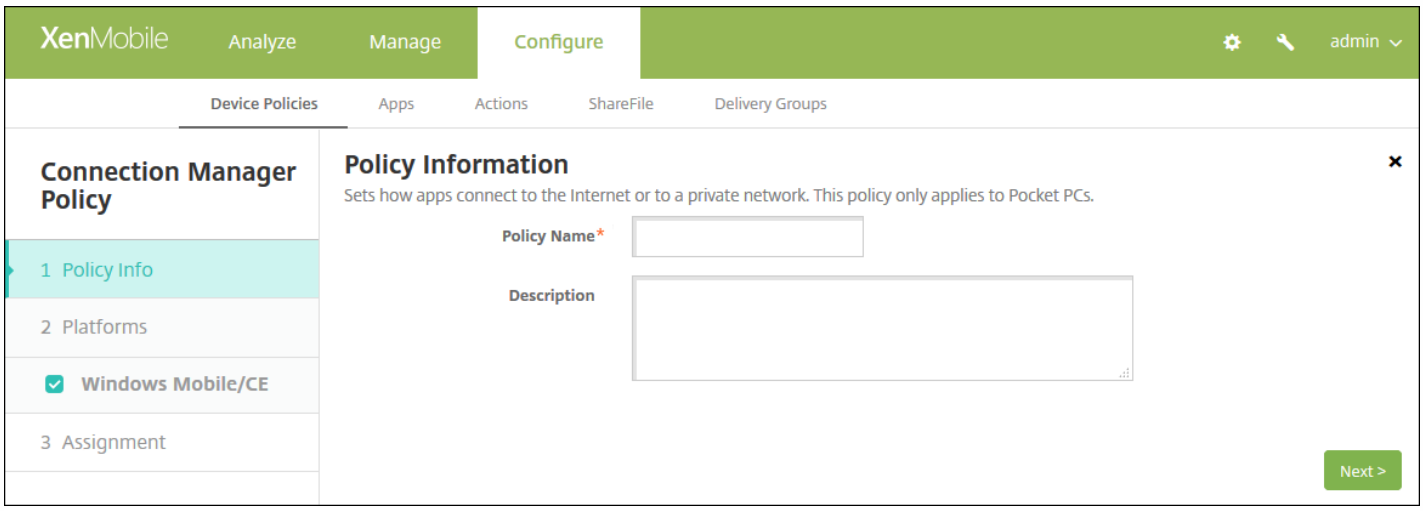
Jul 28, 2016

In XenMobile können Sie die Verbindungseinstellungen für Apps vorgeben, die automatisch eine Verbindung mit dem Internet und privaten Netzwerken herstellen. Diese Richtlinie ist nur für Microsoft Pocket PCs verfügbar.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

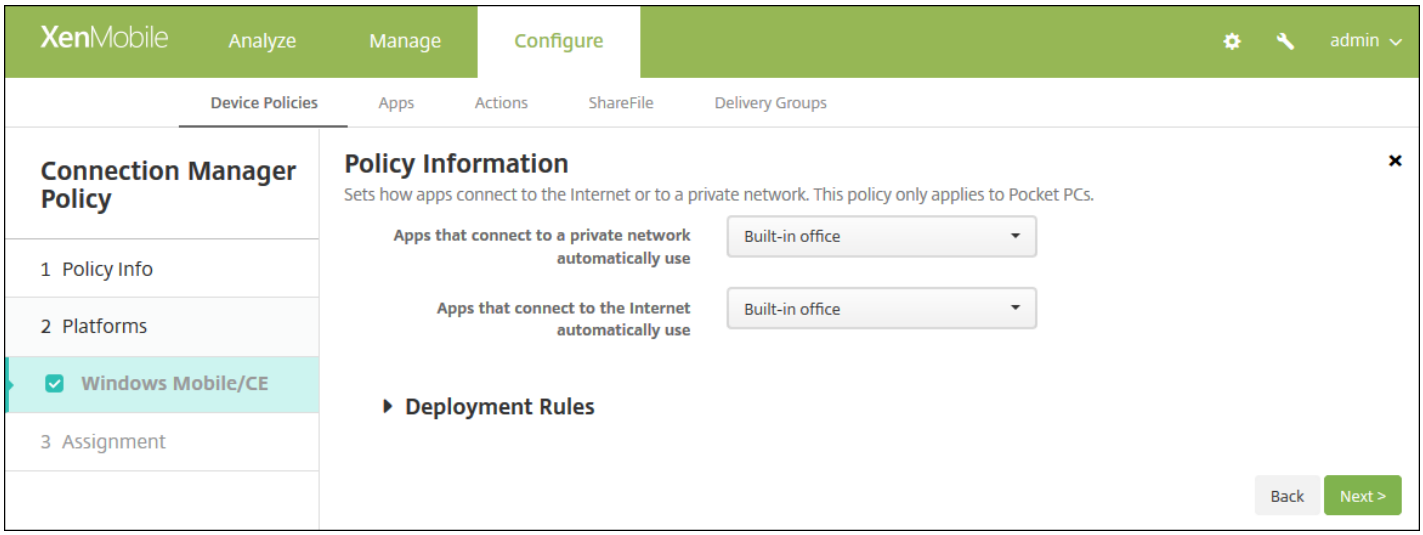
3. Klicken Sie auf **Mehr** und dann unter **Netzwerkzugriff** auf **Verbindungsmanager**. Die Seite **Richtlinieninfo** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Windows Mobile/CE** wird angezeigt.



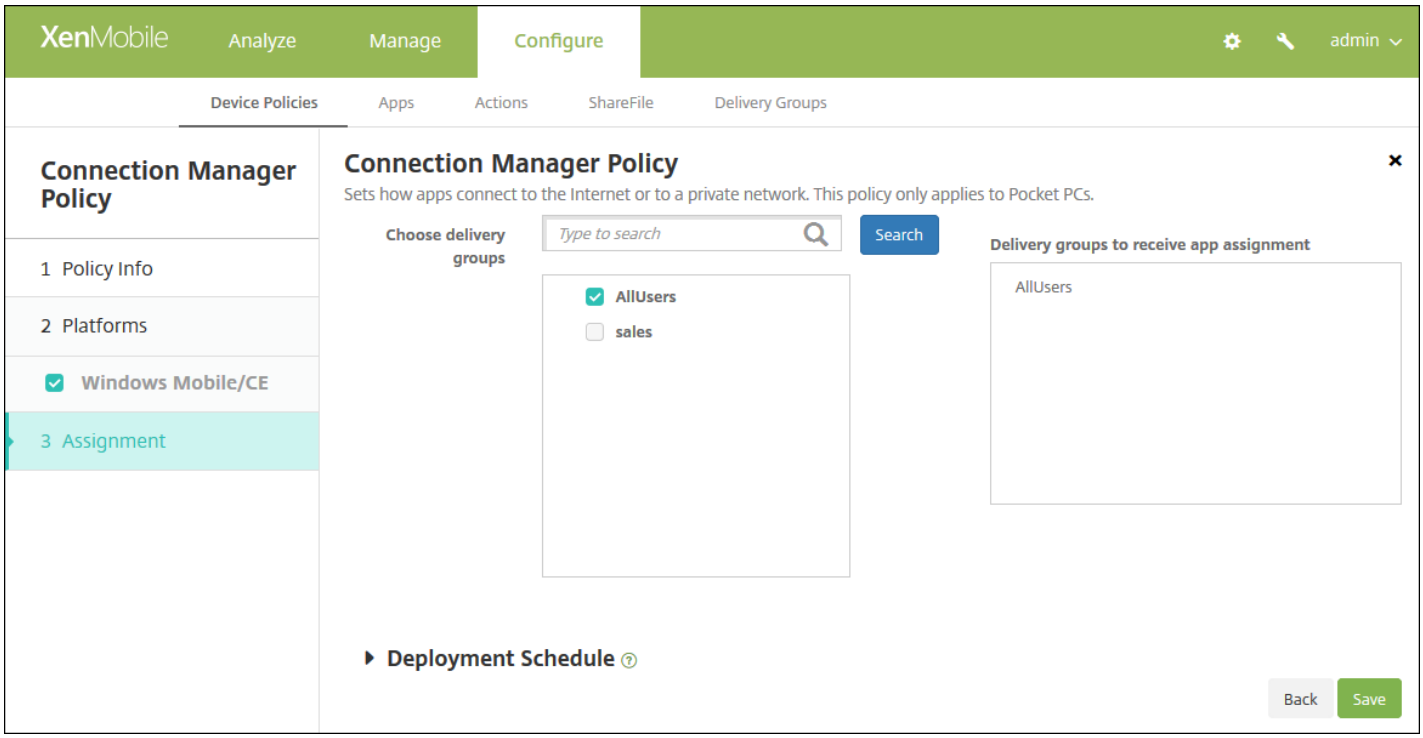
6. Konfigurieren Sie diese Einstellungen.

Hinweis: **Büro (integriert)** steht für Verbindungen mit dem Intranet des Unternehmens und **Internet (integriert)** für Verbindungen mit dem Internet.

- **Für eine Verbindung mit einem privaten Netzwerk verwenden Apps automatisch**: Klicken Sie in der Liste auf **Büro (integriert)** oder **Internet (integriert)**. Der Standardwert ist **Büro (integriert)**.
- **Für eine Verbindung mit dem Internet verwenden Apps automatisch**: Klicken Sie in der Liste auf **Büro (integriert)** oder **Internet (integriert)**. Der Standardwert ist **Büro (integriert)**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen**

Bereitstellung. Die Standardeinstellung ist **Bei jeder Verbindung**.

- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Verbindungszeitplanrichtlinien für Geräte

Jul 28, 2016

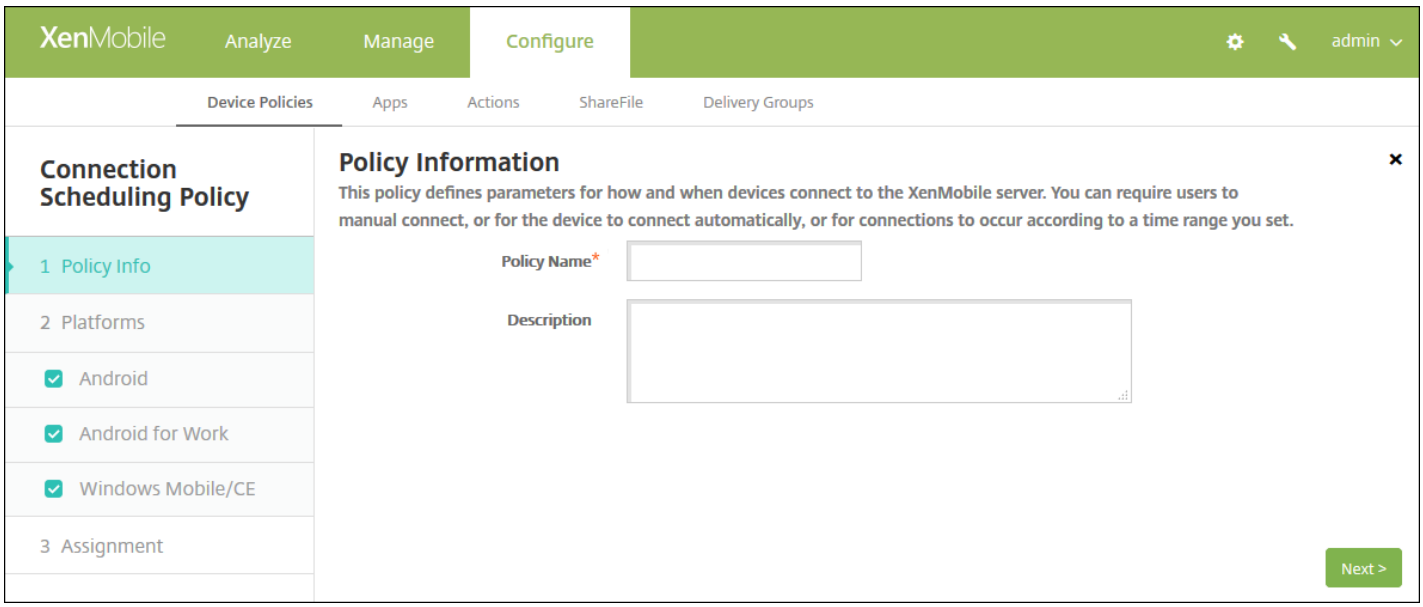
Sie erstellen Verbindungszeitplanrichtlinien, um vorzugeben, wie und wann Geräte eine Verbindung mit XenMobile herstellen sollen. Sie können diese Richtlinie auch für Geräte konfigurieren, die für Android for Work aktiviert sind.

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 **Konfigurieren > Gerätерichtlinien**. Die Seite **Gerätерichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

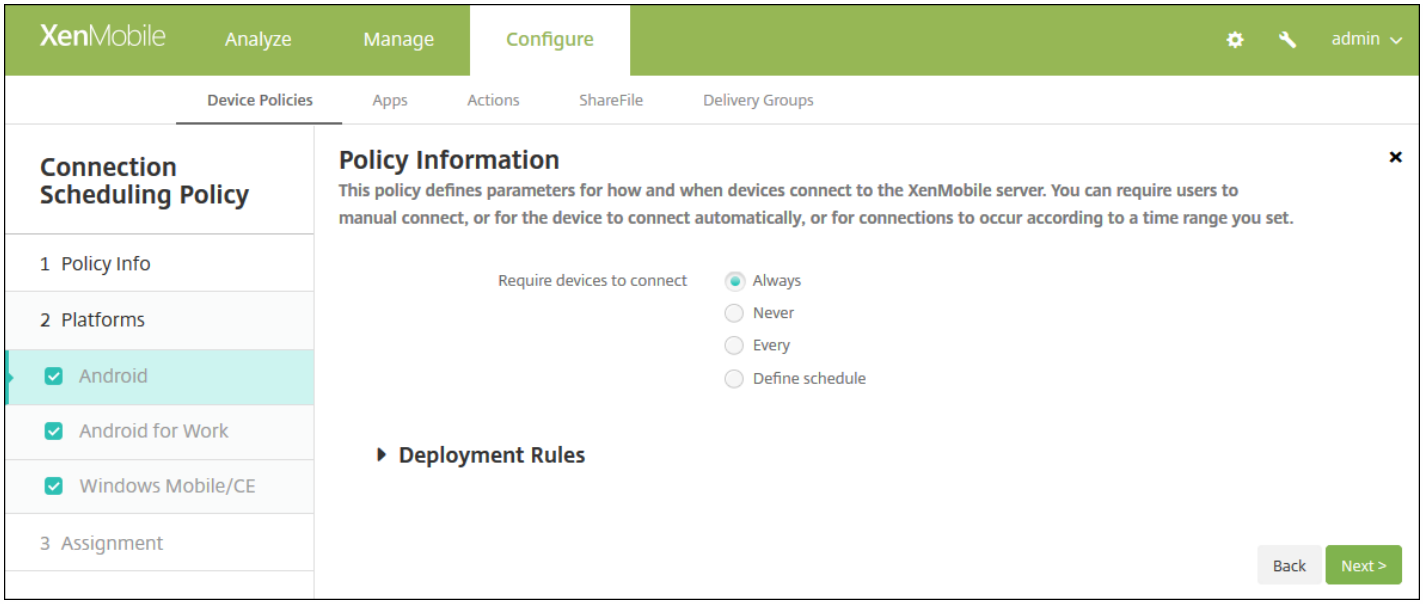
3. Klicken Sie auf **Planung**. Die Seite **Verbindungszeitplan** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.



6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der Bereitstellungsregeln für diese Plattform unter Schritt 8.

7. Konfigurieren Sie für jede ausgewählte Plattform die folgenden Einstellungen:

- **Geräte müssen Verbindung herstellen**: Klicken Sie auf die Option, die Sie für diesen Zeitplan festlegen möchten.
  - **Immer**: 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. Citrix empfiehlt diese Option zur Optimierung der Sicherheit. Wenn Sie **Immer** wählen, verwenden Sie für das Gerät auch die **Tunnelrichtlinie** und legen Sie die Einstellung **Verbindungstimeout definieren** fest, um sicherzustellen, dass die Verbindung nicht den Akku belastet. Wenn Sie die Verbindung aufrechterhalten, können Sie Sicherheitsbefehle, wie Löschen und Sperren, bei Bedarf per Push auf dem Gerät bereitstellen. Aktivieren Sie auch unter **Bereitstellungszeitplan** die Option **Bereitstellen für immer aktive Verbindungen** für jede auf dem Gerät bereitgestellte Richtlinie.
  - **Nie**: Die Verbindung muss manuell hergestellt werden. Die Benutzer müssen die Verbindung mit XenMobile auf ihrem Gerät herstellen. Citrix empfiehlt diese Option nicht für Produktionsbereitstellungen, da die Bereitstellung von Sicherheitsrichtlinien auf den Geräten verhindert wird. Benutzer erhalten daher nie neue Apps oder Richtlinien.
  - **Alle**: Die Verbindung wird in dem hier ausgewählten Intervall hergestellt. Wenn diese Option aktiviert ist und Sie eine Sicherheitsrichtlinie wie eine Sperrung oder eine Datenlöschung senden, verarbeitet XenMobile die Aktion auf dem Gerät, wenn das Gerät das nächste Mal eine Verbindung herstellt. Wenn Sie diese Option auswählen, wird das Feld **Alle N Minuten verbinden** eingeblendet, in dem Sie die Zeitdauer (in Minuten) eingeben müssen, nach der Geräte eine Verbindung wiederherstellen. Der Standardwert ist **20**.
  - **Zeitplan festlegen**: Wird diese Option aktiviert, versucht XenMobile auf dem Benutzergerät 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. Informationen zum Einrichten eines Verbindungszeitrahmens finden Sie unter Definieren eines Verbindungszeitrahmens.
    - **Dauerverbindung während dieser Zeit erhalten**: Die Geräte der Benutzer müssen während der definierten

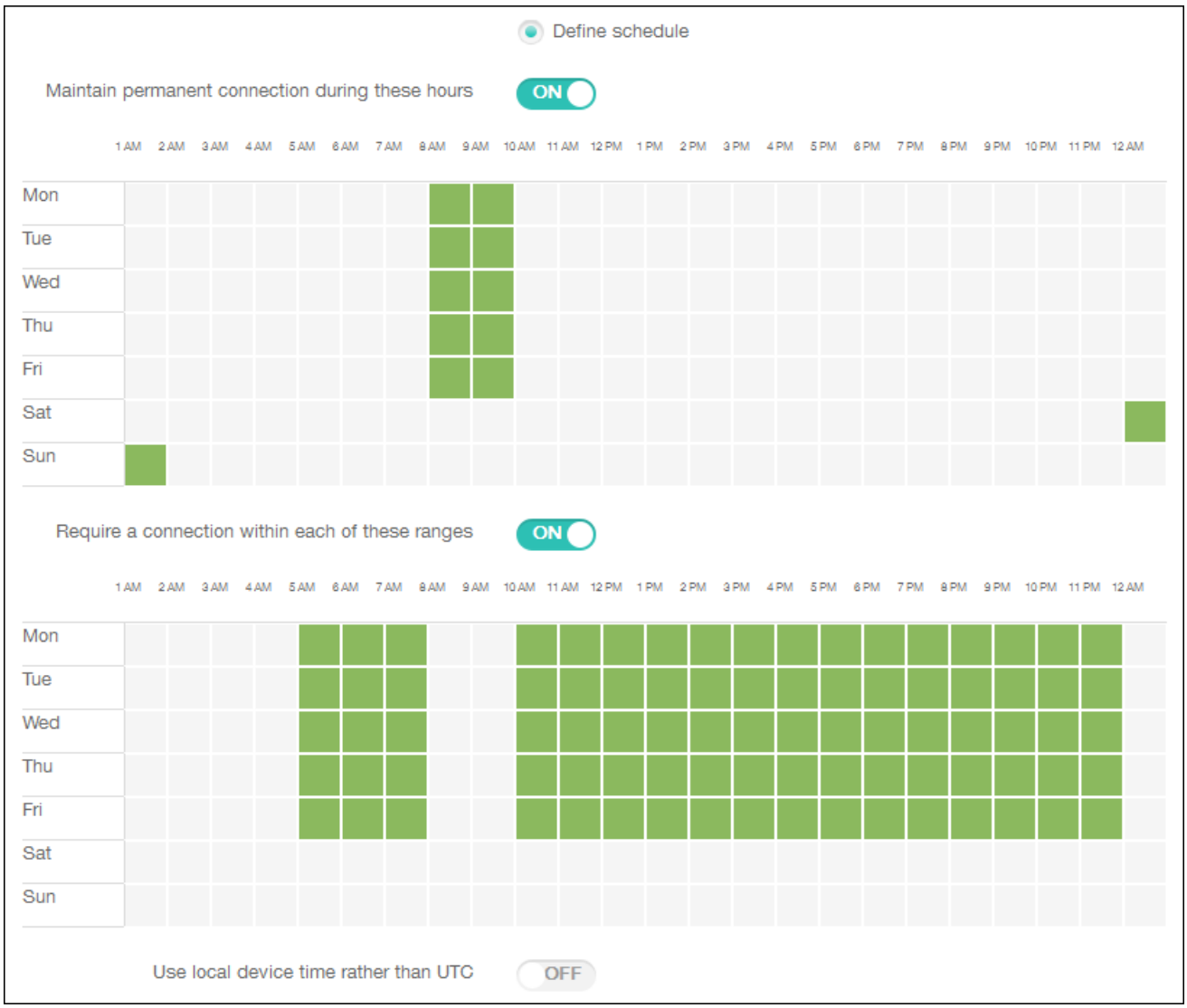
Zeiten verbunden sein.

- **Verbindung in jedem dieser Zeiträume erforderlich**: Die Geräte der Benutzer müssen während der definierten Zeiten mindestens einmal verbunden sein.
- **Lokale Zeitzone des Geräts statt UTC verwenden**: Der Zeitrahmen soll auf die lokale Zeit des Geräts synchronisiert werden, anstelle die koordinierte Weltzeit (UTC) zu verwenden.

Definieren eines Verbindungszeitrahmens

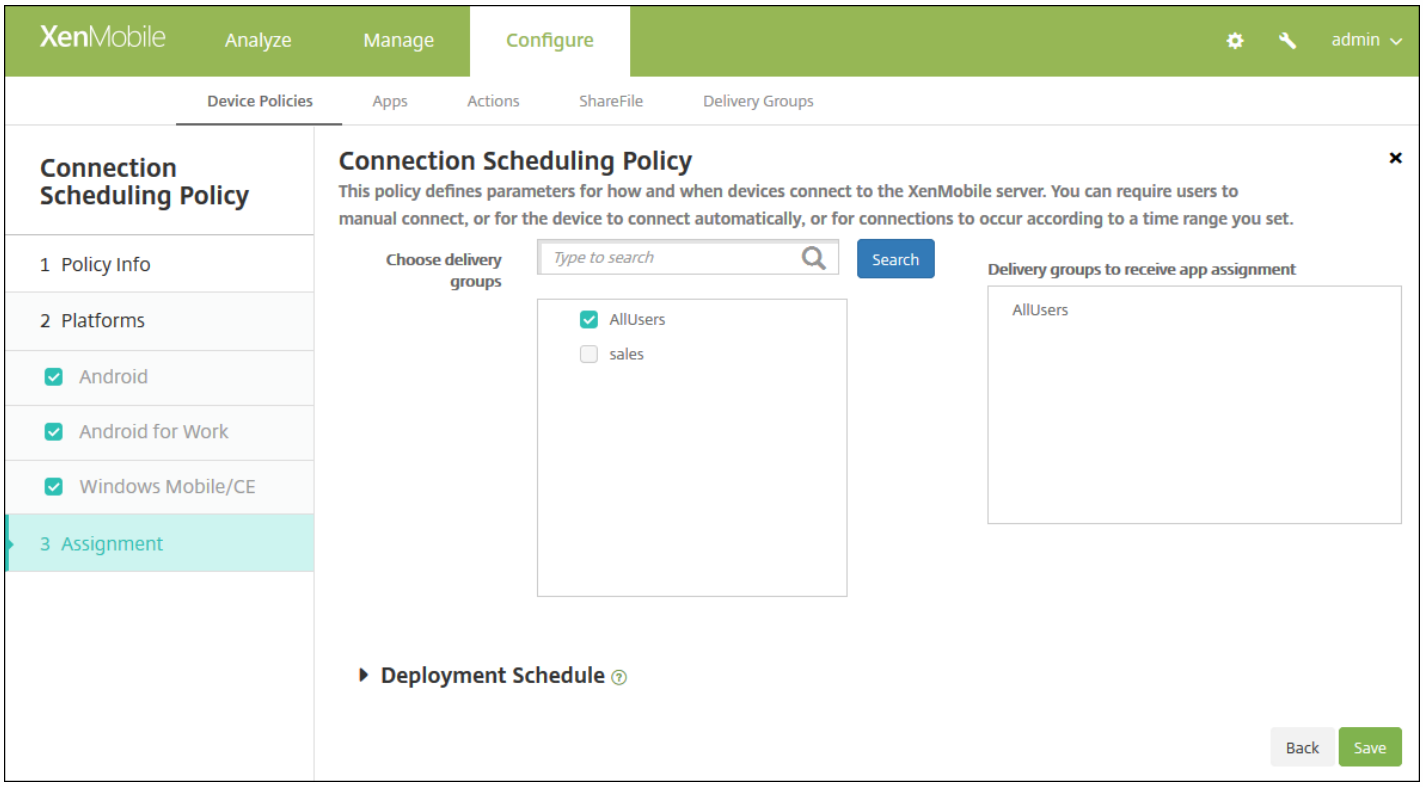
Wenn Sie die folgenden Optionen aktivieren, wird eine Zeitachse angezeigt, mit der Sie den gewünschten Zeitrahmen definieren können. Sie können jeweils eine oder beide Optionen für eine bleibende Verbindung zu einer spezifischen Zeit oder zum Erzwingen einer Verbindung innerhalb bestimmter Zeitrahmen 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.



8. Konfigurieren der Bereitstellungsregeln

9. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Verbindungszeitplanrichtlinie wird angezeigt.



10. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

11. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

12. Klicken Sie auf **Speichern**.

Geräterichtlinie für Kontakte (CardDAV)

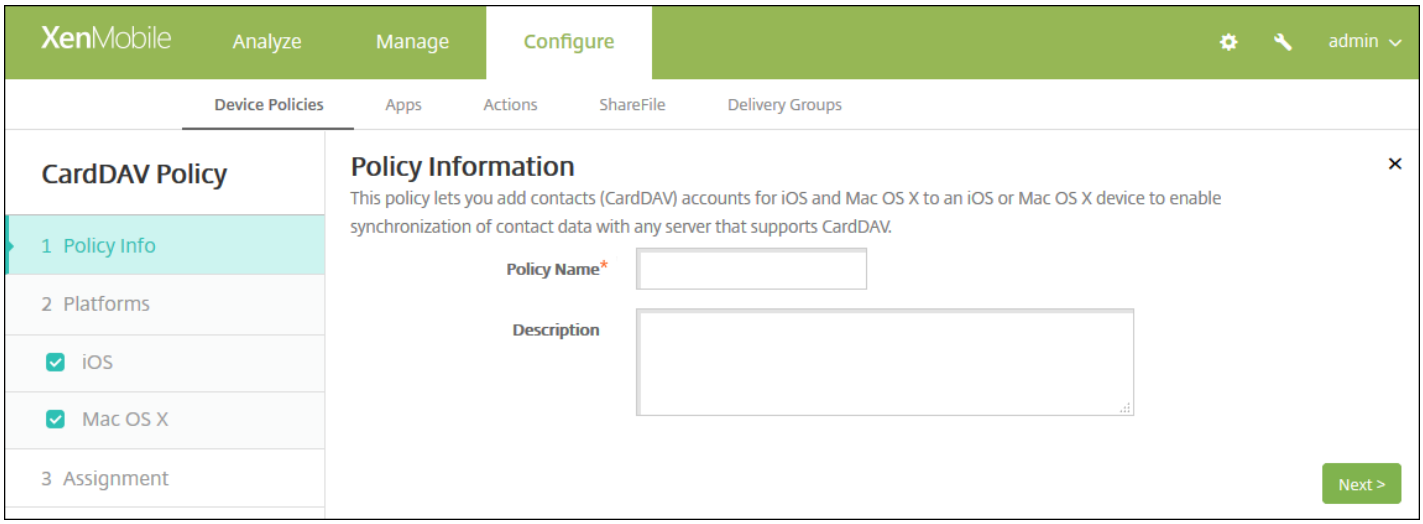
Jul 28, 2016

Sie können in XenMobile eine Geräterichtlinie zum Hinzufügen eines iOS-Kontaktekontos (CardDAV) zu iOS- oder Mac OS X-Geräten einrichten, damit die Benutzer Kontaktdaten mit einem beliebigen Server, der CardDAV unterstützt, synchronisieren können.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **Kontakte (CardDAV)**. Die Seite für die Richtlinieninformationen der Richtlinie **CardDAV** wird angezeigt.



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

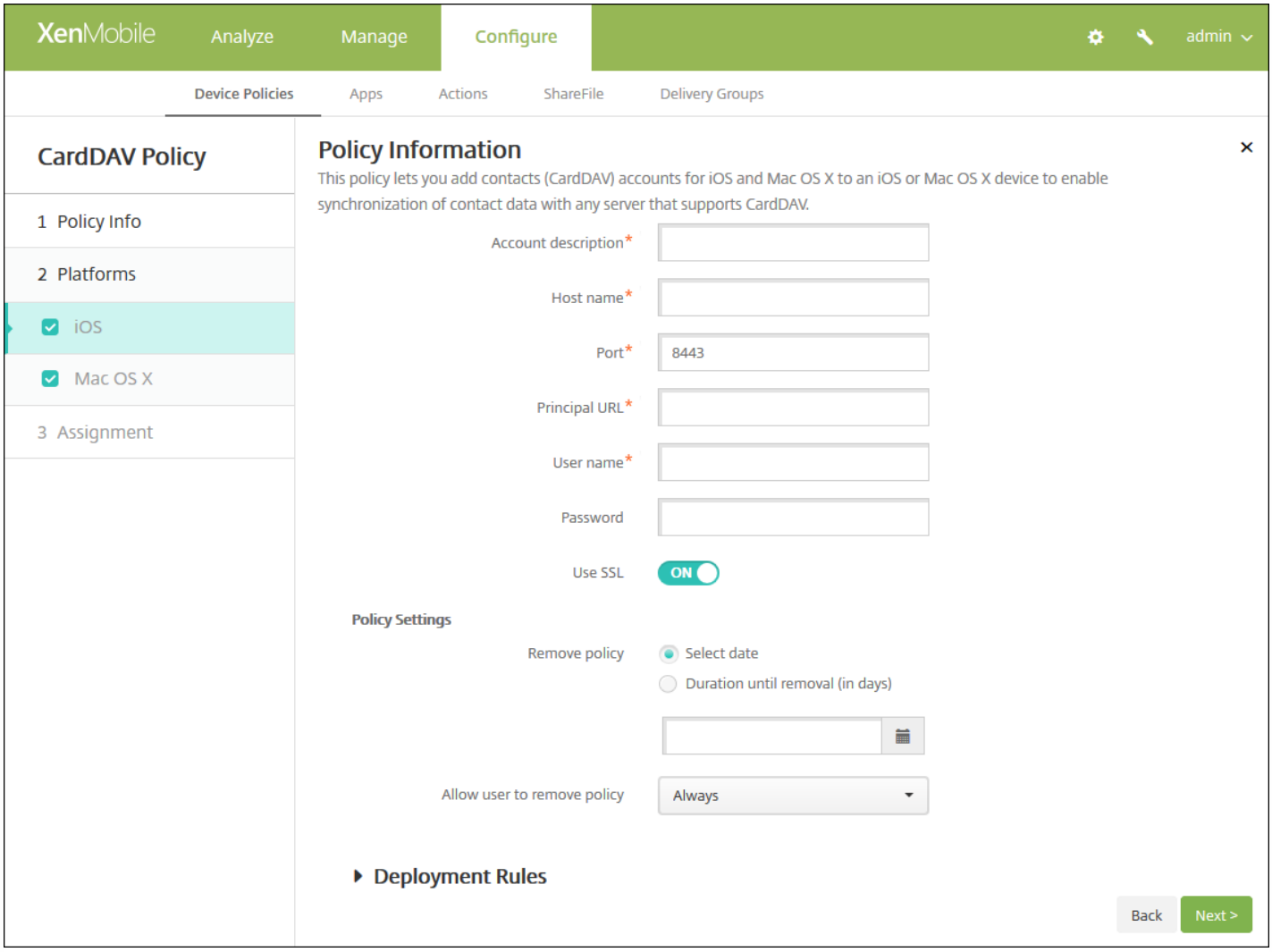
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

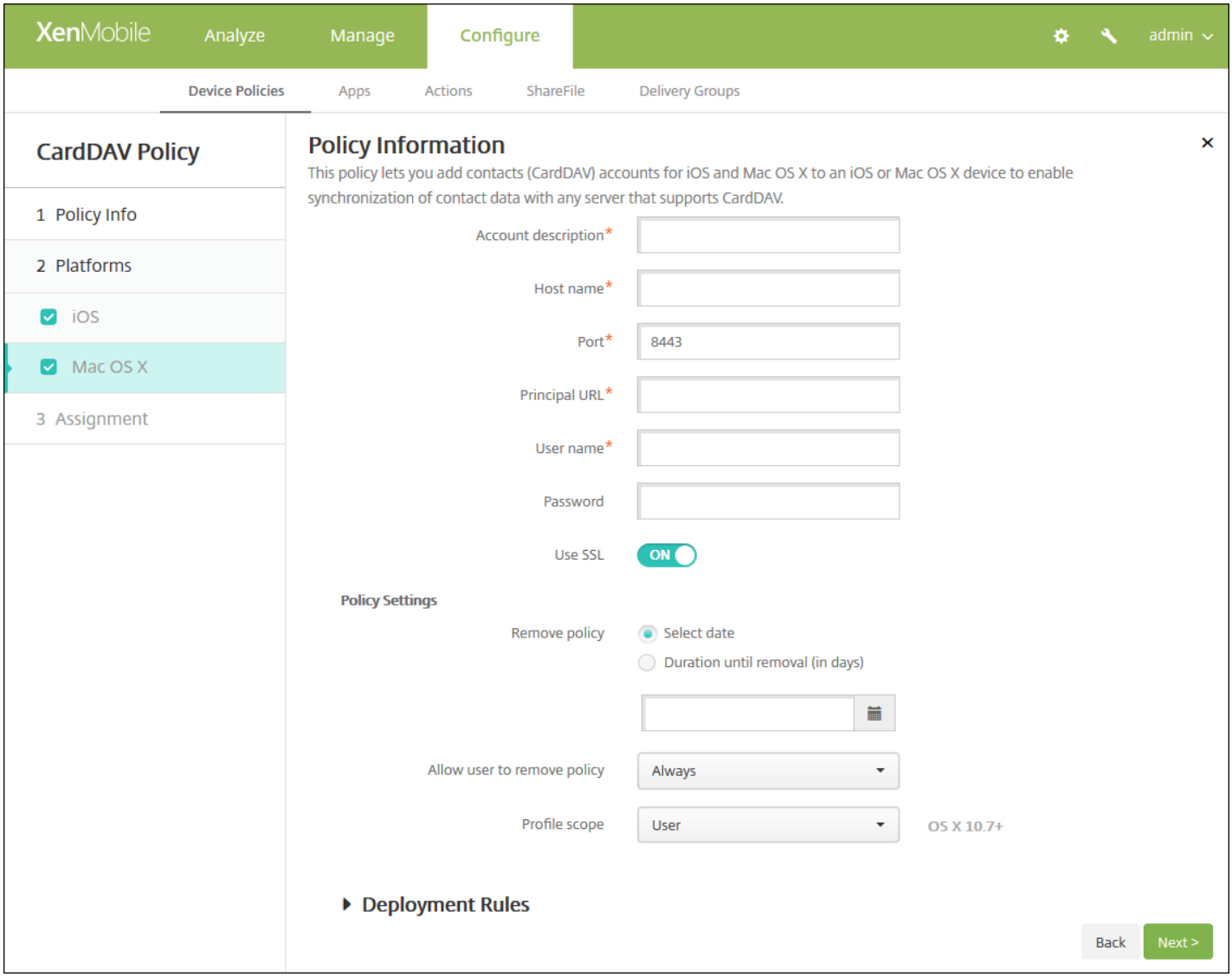
Konfigurieren von iOS-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Kontobeschreibung**: Geben Sie ein Kontobeschreibung ein. Diese Angabe ist erforderlich.
- **Hostname**: Geben Sie die Adresse des CardDAV-Servers ein. Diese Angabe ist erforderlich.
- **Port**: Geben Sie den Port für die Verbindung mit dem CardDAV-Server ein. Diese Angabe ist erforderlich. Der Standardwert ist **8443**.
- **Principal URL**: Geben Sie die Basis-URL des Kalenders des Benutzers ein.
- **Benutzername**: Geben Sie den Anmeldenamen des Benutzers ein. Diese Angabe ist erforderlich.
- **Kennwort**: Geben Sie ein optionales Benutzerkennwort ein.
- **SSL verwenden**: Wählen Sie aus, ob für die Verbindung mit dem CardDAV-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist **EIN**.
- **Richtlinieneinstellungen**
  - Klicken Sie für **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für Passcode zum Entfernen den Passcode ein.

Konfigurieren von Mac OS X-Einstellungen



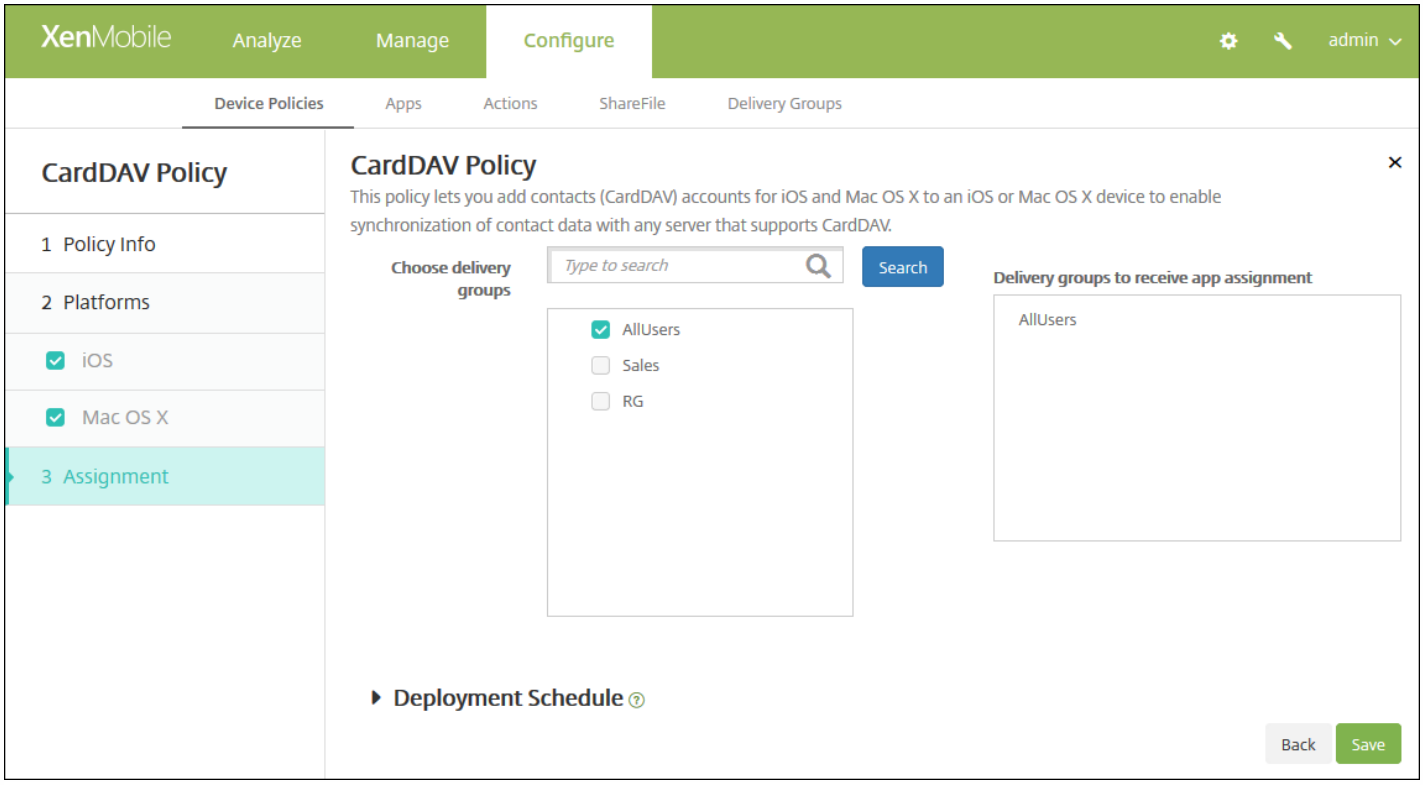
Konfigurieren Sie folgende Einstellungen:

- **Kontobeschreibung**: Geben Sie ein Kontobeschreibung ein. Diese Angabe ist erforderlich.
- **Hostname**: Geben Sie die Adresse des CardDAV-Servers ein. Diese Angabe ist erforderlich.
- **Port**: Geben Sie den Port für die Verbindung mit dem CardDAV-Server ein. Diese Angabe ist erforderlich. Der Standardwert ist **8443**.
- **Principal URL**: Geben Sie die Basis-URL des Kalenders des Benutzers ein.
- **Benutzername**: Geben Sie den Anmeldenamen des Benutzers ein. Diese Angabe ist erforderlich.
- **Kennwort**: Geben Sie ein optionales Benutzerkennwort ein.
- **SSL verwenden**: Wählen Sie aus, ob für die Verbindung mit dem CardDAV-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist **EIN**.
- **Richtlinieneinstellungen**
  - Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für Passcode zum Entfernen den Passcode ein.
  - Klicken Sie neben **Gültigkeitsbereich für Profil** auf **Benutzer** oder **System**. Der Standardwert ist **Benutzer**. Diese

Option ist nur für OS X 10.7 und höher verfügbar.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die CardDAV-Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Richtlinien zum Kopieren von Apps in den Samsung-Container

Jul 28, 2016

Sie können festlegen, dass bereits auf Geräten installierte Apps in einen SEAMS- oder KNOX-Container auf unterstützten Samsung-Geräten kopiert werden (Informationen zu den unterstützten Geräten finden auf der Samsung-Website unter Von Samsung KNOX unterstützte Geräte). In den SEAMS-Container kopierte Apps stehen auf dem Homebildschirm zur Verfügung, während Apps im KNOX-Container nur verfügbar sind, wenn die Benutzer sich beim Samsung KNOX-Container anmelden.

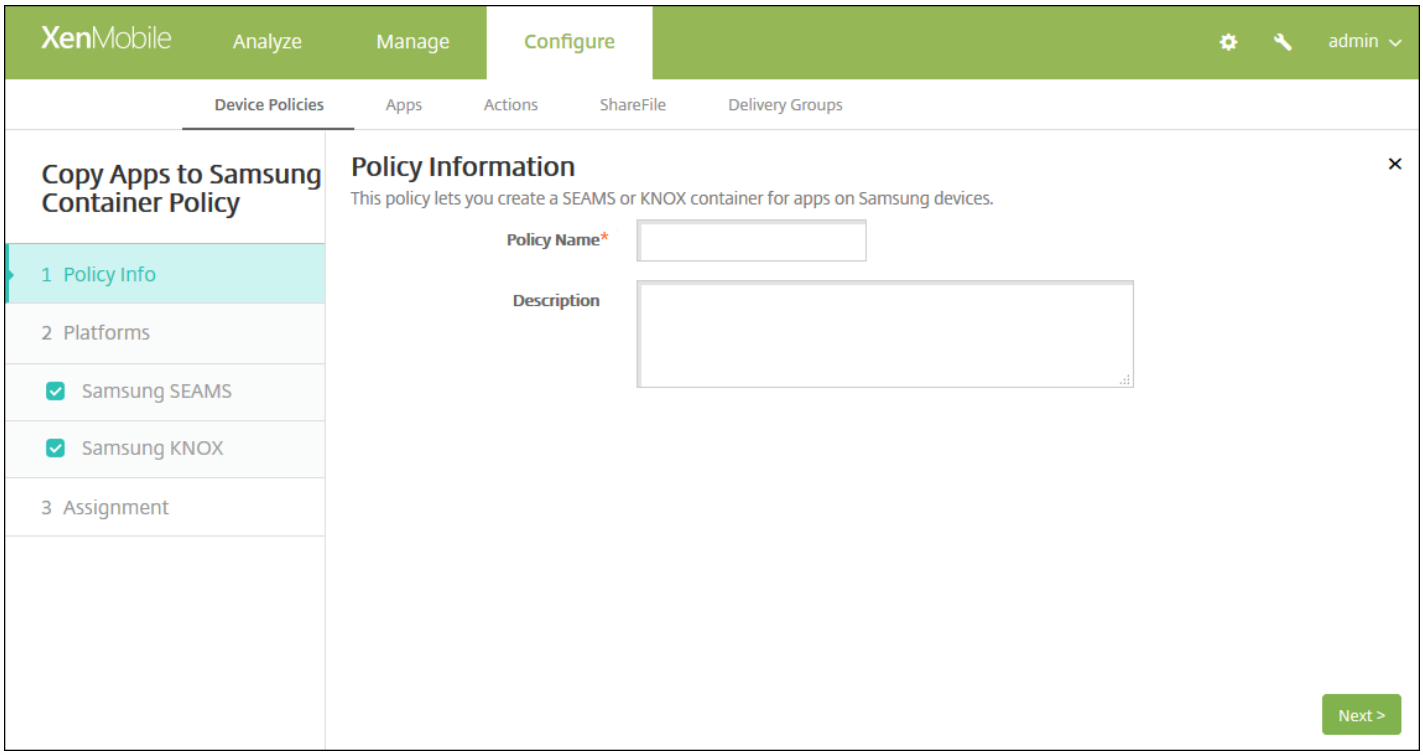
Voraussetzungen:

- Das Gerät muss bei XenMobile registriert sein.
- Die Samsung-MDM-Schlüssel (ELM und KLM) müssen bereitgestellt sein (entsprechende Anweisungen finden Sie unter "Samsung MDM-Richtlinien für Geräte")
- Die Apps sind bereits auf dem Gerät installiert.
- KNOX wurde auf dem gewünschten Gerät initialisiert.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Geräterichtlinien**.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

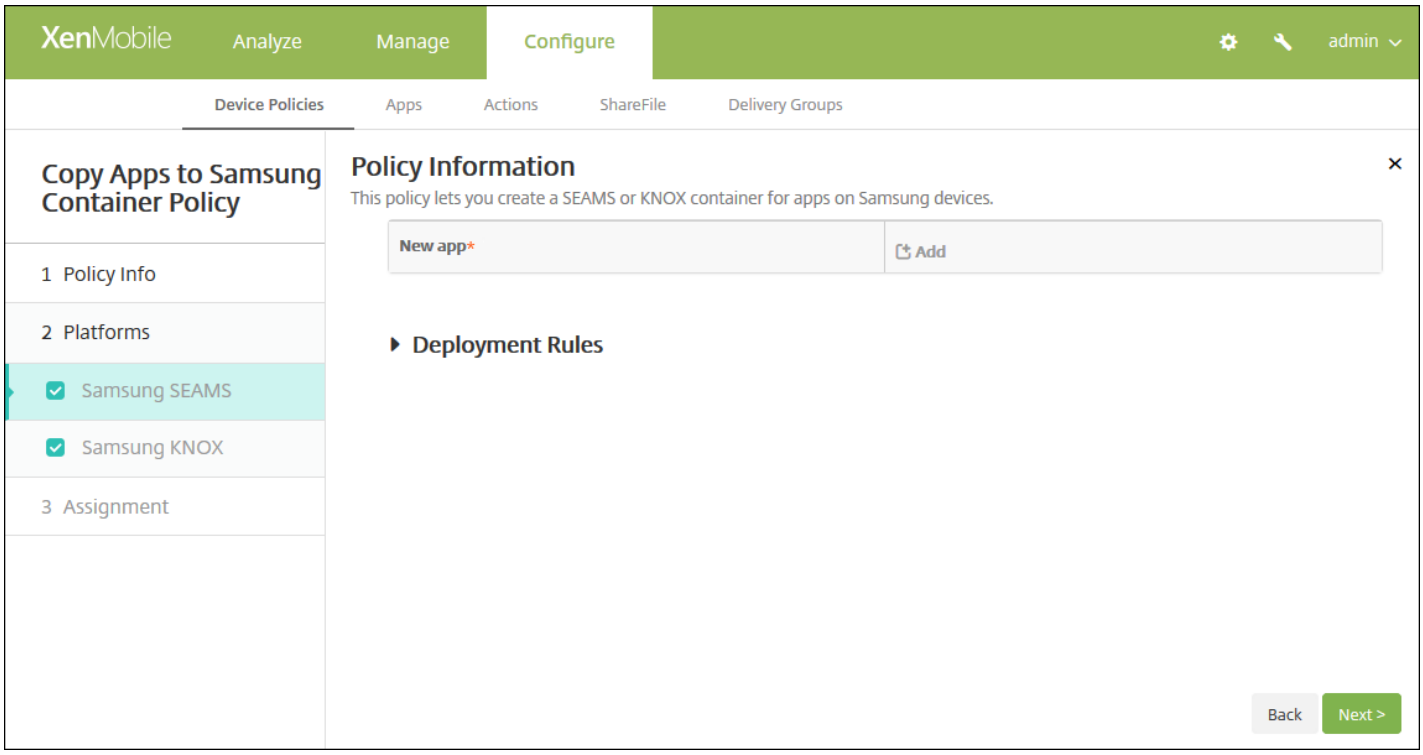
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **Apps in Samsung Container kopieren**. Die Seite **Apps in Samsung Container kopieren** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.



6. Wählen Sie unter "Plattformen" die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der Bereitstellungsregeln für diese Plattform unter Schritt 8.

7. Konfigurieren Sie für jede ausgewählte Plattform die folgende Einstellung:

- **Neue App**: Klicken Sie für jede App, die Sie der Liste hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - Geben Sie die Paket-ID ein, beispielsweise "com.mobiwolf.lacingart" für die LacingArt-App.
  - Klicken Sie auf **Speichern** oder **Abbrechen**.

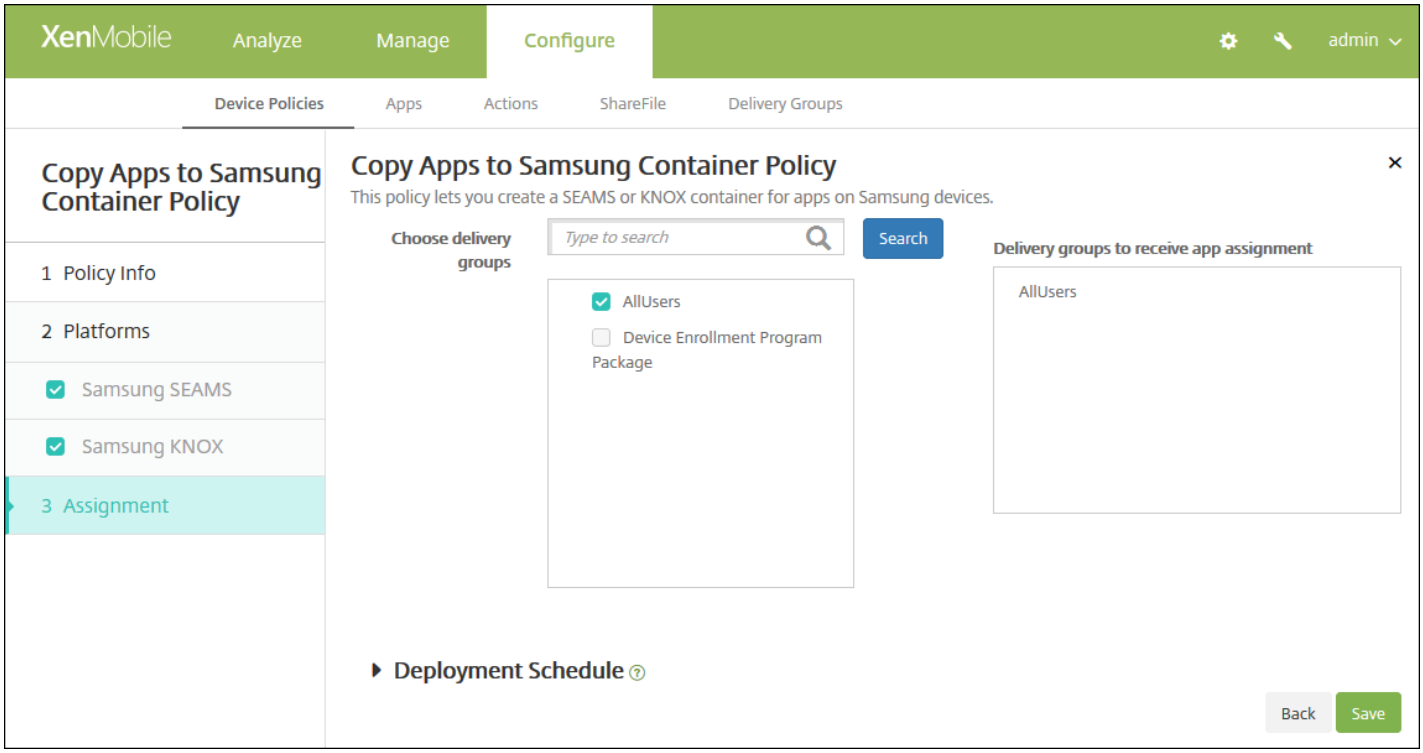
  Hinweis: Zum Löschen einer vorhandenen App zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, um ihn beizubehalten.

  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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

8. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die nächste Plattformseite oder die Zuweisungsseite für **Apps in Samsung Container kopieren**

wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie Later auswählen, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- 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.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen gemachten Änderungen werden auf alle Plattformen angewendet. Ausnahme bildet die Einstellung "Bereitstellen für immer aktive Verbindungen", denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Nachdem Sie die Richtlinie bereitgestellt haben, werden SEAMS-Apps auf der Seite **Gerätedetails** unter der Überschrift **Standort: SEAMS-Standort des Unternehmens** und die KNOX-Apps unter der Überschrift **Standort: Unternehmensstandort** angezeigt.

Anmeldeinformationsrichtlinien für Geräte

Jul 28, 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.

Sie können Anmeldeinformationsrichtlinien für iOS-, Mac OS X-, Android-, Android for Work-, Windows Desktop-/Tablet-, Windows Mobile-/CE- und Windows Phone-Geräte erstellen. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Abschnitt beschrieben.

iOS-Einstellungen

Mac OS X-Einstellungen

Android- und Android for Work-Einstellungen

Windows Desktop-/Tablet-Einstellungen

Windows Mobile-/CE-Einstellungen

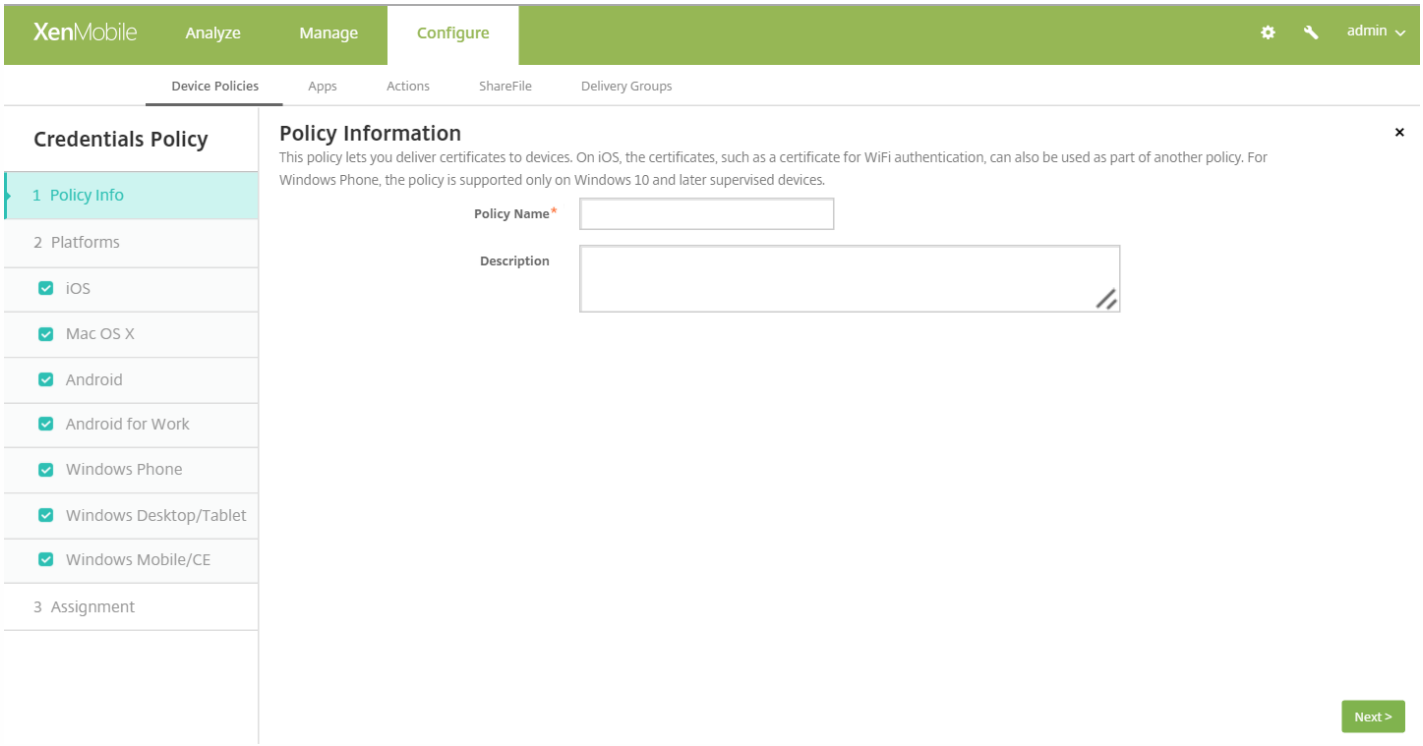
Windows Phone-Einstellungen

Vor dem Erstellen dieser Richtlinie müssen Sie die Anmeldeinformationen für jede Plattform sowie jegliche Zertifikate und Kennwörter zusammenstellen.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **Anmeldeinformationen**. Die Seite für die Richtlinieninformationen der Richtlinie **Anmeldeinformationen** wird angezeigt.



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

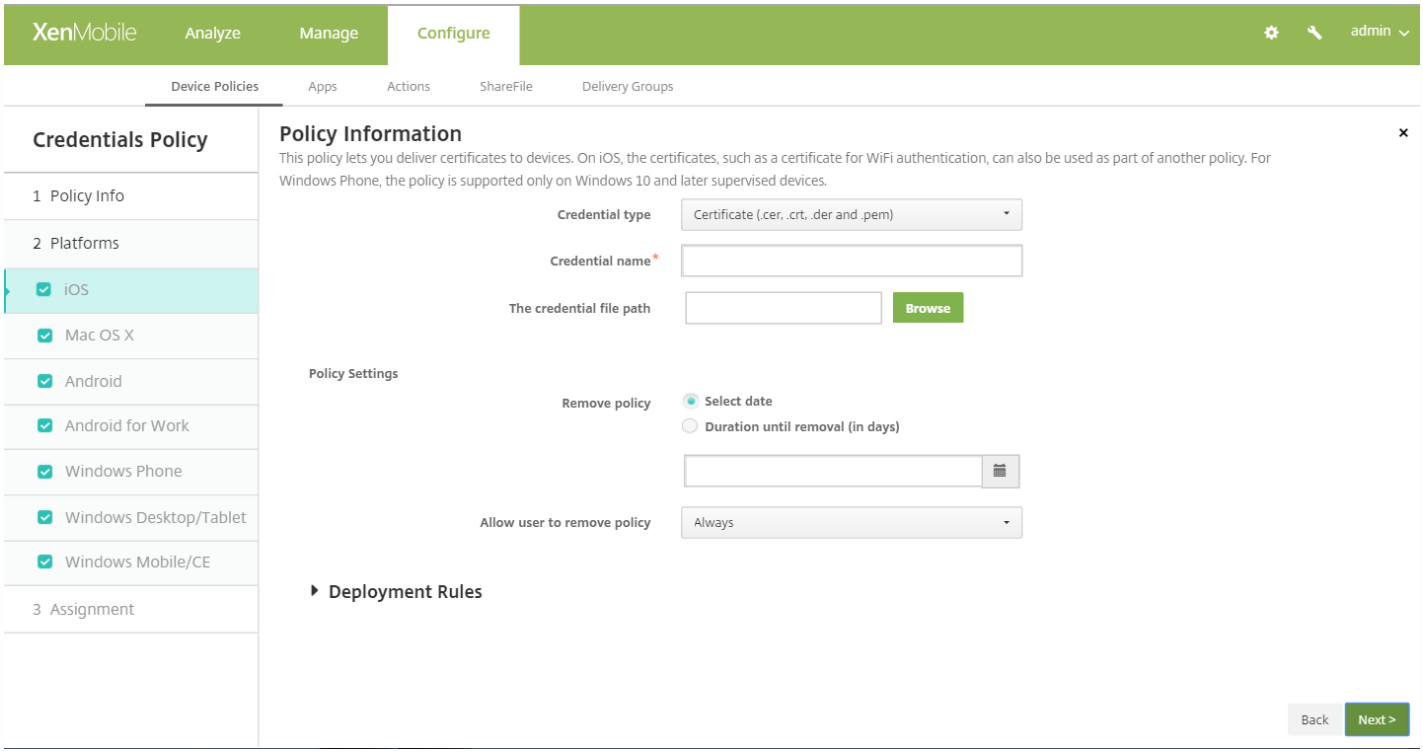
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

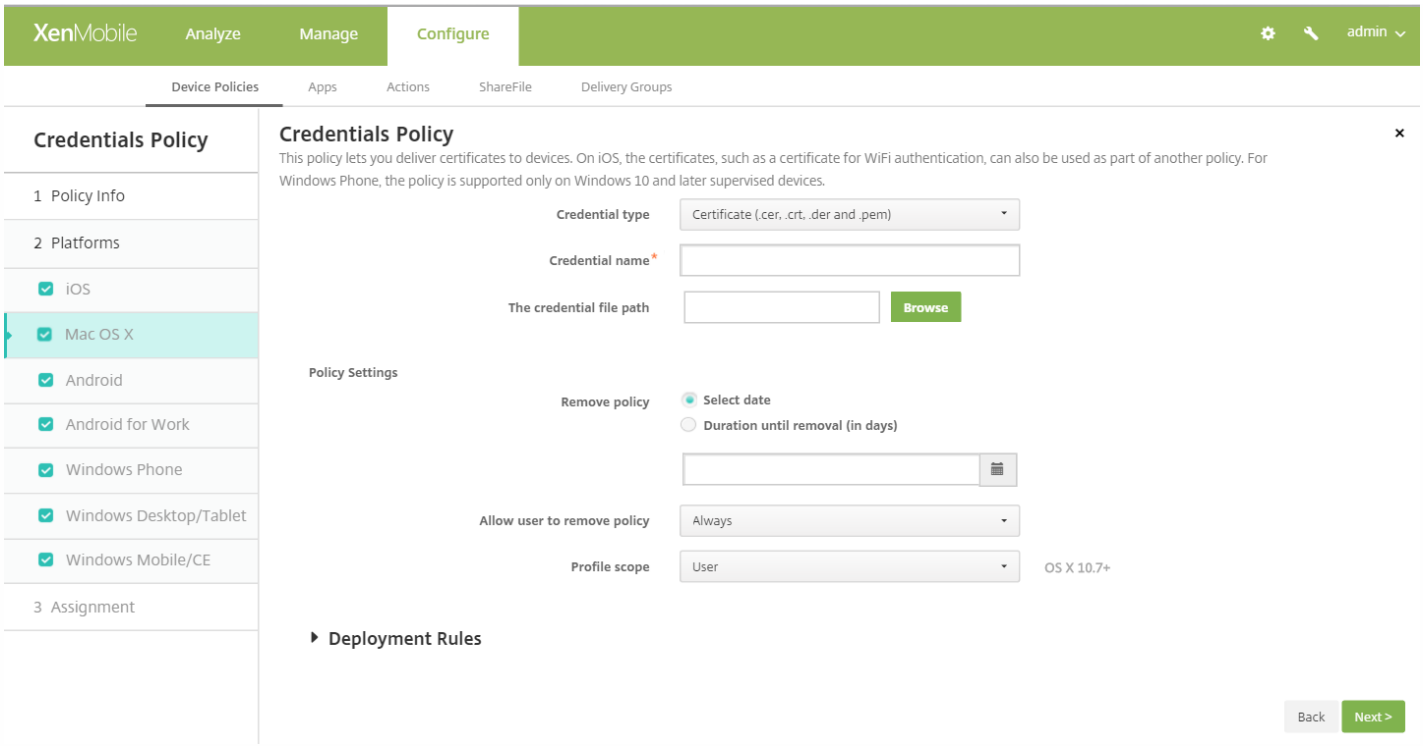
Konfigurieren von iOS-Einstellungen



Konfigurieren Sie die folgenden Einstellungen:

- **Anmeldeinformationstyp**: Klicken Sie in der Liste auf den Typ der Anmeldeinformationen für diese Richtlinie und geben Sie für die ausgewählten Anmeldeinformationen die folgenden Informationen an:
  - **Zertifikat**
    - **Name der Anmeldeinformationen**: Geben Sie einen Namen für die Anmeldeinformationen ein.
    - **Anmeldeinformationsdateipfad**: Klicken Sie auf "Durchsuchen" und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
  - **Schlüsselspeicher**
    - **Name der Anmeldeinformationen**: Geben Sie einen Namen für die Anmeldeinformationen ein.
    - **Anmeldeinformationsdateipfad**: Klicken Sie auf "Durchsuchen" und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
    - **Kennwort**: Geben Sie das Schlüsselspeicherkennwort für die Anmeldeinformationen ein.
  - **Serverzertifikat**
    - **Serverzertifikat**: Klicken Sie in der Liste auf das Zertifikat, das verwendet werden soll.
  - **Anmeldeinformationsanbieter**
    - **Anmeldeinformationsanbieter**: Klicken Sie in der Liste auf den Namen des Anmeldeinformationsanbieters.
- **Richtlinieneinstellungen**
  - Klicken Sie für **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

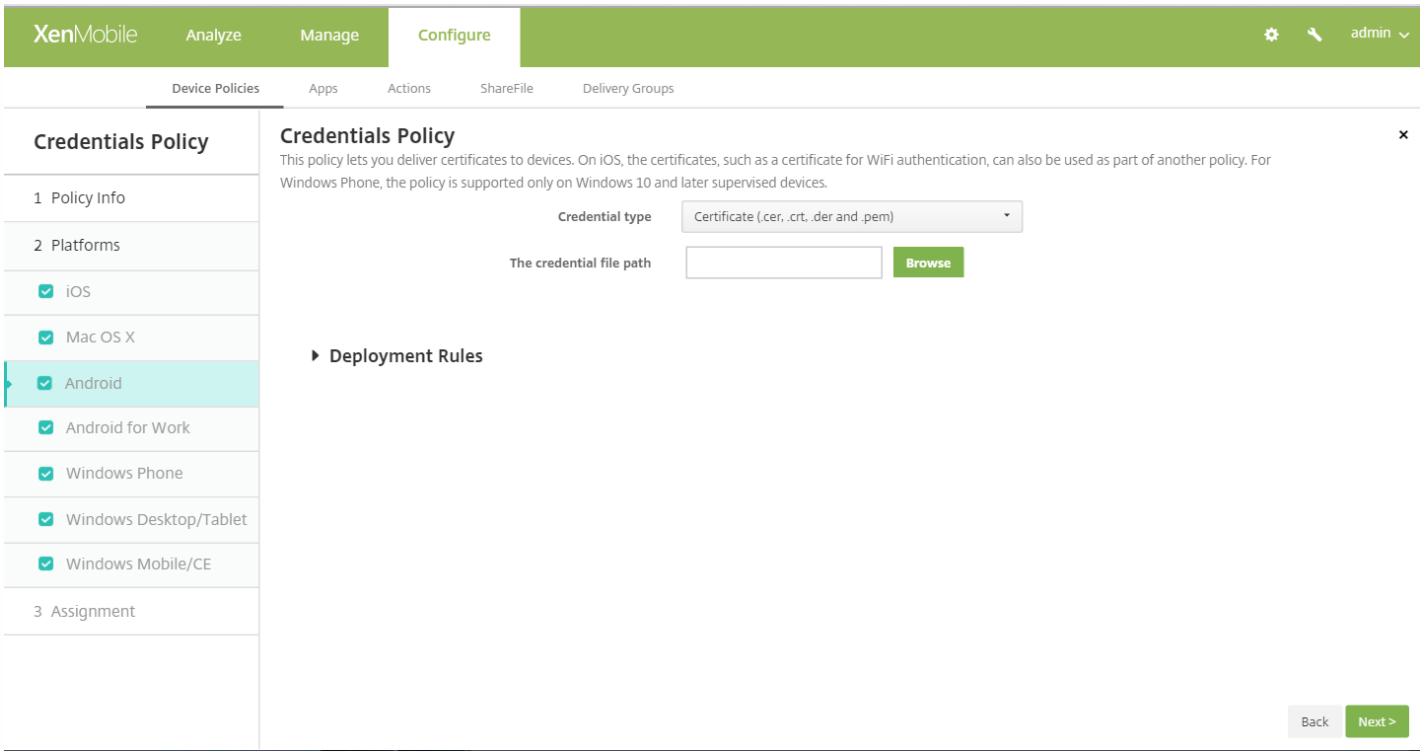
Konfigurieren von Mac OS X-Einstellungen



Konfigurieren Sie die folgenden Einstellungen:

- **Anmeldeinformationstyp**: Klicken Sie in der Liste auf den Typ der Anmeldeinformationen für diese Richtlinie und geben Sie für die ausgewählten Anmeldeinformationen die folgenden Informationen an:
  - **Zertifikat**
    - **Name der Anmeldeinformationen**: Geben Sie einen Namen für die Anmeldeinformationen ein.
    - **Anmeldeinformationsdateipfad**: Klicken Sie auf Browse und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
  - **Schlüsselspeicher**
    - **Name der Anmeldeinformationen**: Geben Sie einen Namen für die Anmeldeinformationen ein.
    - **Anmeldeinformationsdateipfad**: Klicken Sie auf Browse und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
    - **Kennwort**: Geben Sie das Schlüsselspeicherkennwort für die Anmeldeinformationen ein.
  - **Serverzertifikat**
    - **Serverzertifikat**: Klicken Sie in der Liste auf das Zertifikat, das verwendet werden soll.
  - **Anmeldeinformationsanbieter**
    - **Anmeldeinformationsanbieter**: Klicken Sie in der Liste auf den Namen des Anmeldeinformationsanbieters.
- **Richtlinieneinstellungen**
  - Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.
  - Klicken Sie neben **Geltungsbereich für die Richtlinie** auf **Benutzer** oder **System**. Der Standardwert ist **Benutzer**. Diese Option ist nur für OS X 10.7 und höher verfügbar.

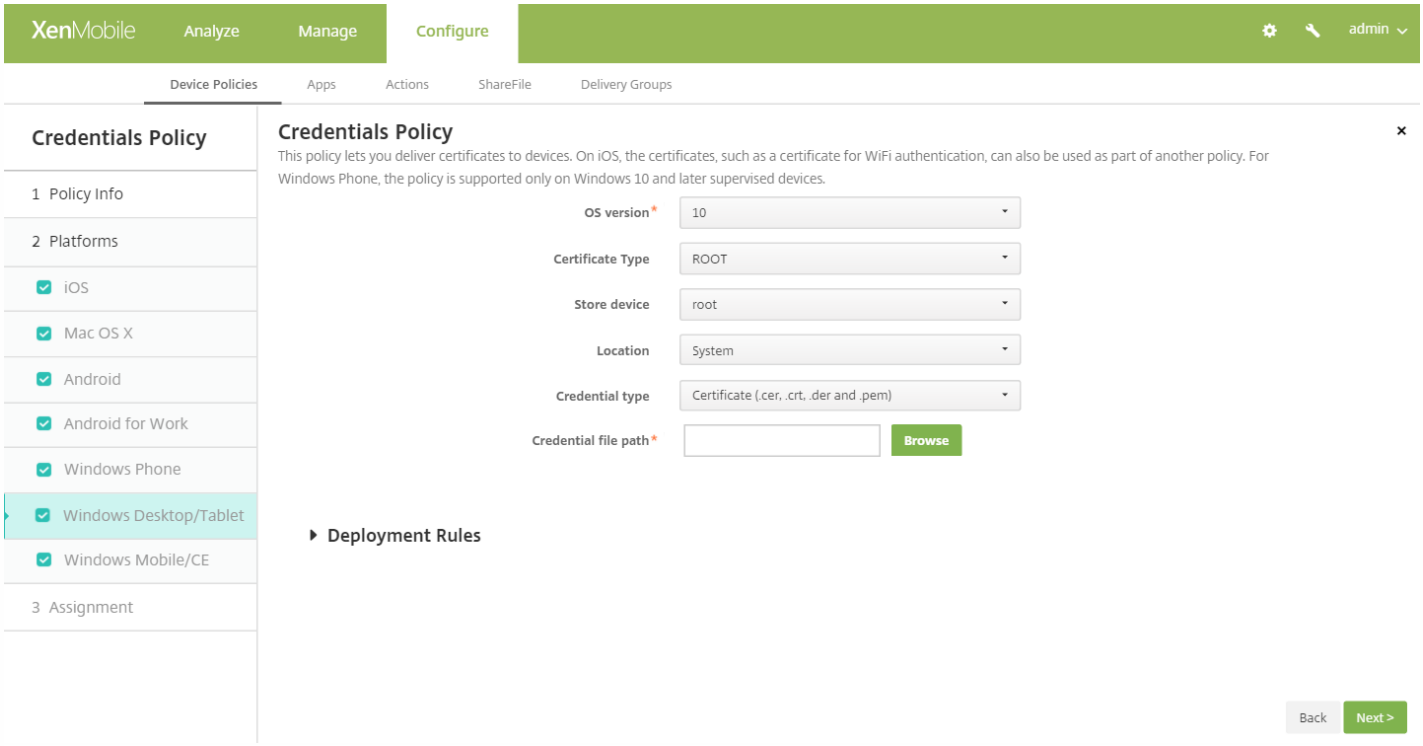
Konfigurieren von Android- und Android for Work-Einstellungen



Konfigurieren Sie die folgenden Einstellungen:

- **Anmeldeinformationstyp**: Klicken Sie in der Liste auf den Typ der Anmeldeinformationen für diese Richtlinie und geben Sie für die ausgewählten Anmeldeinformationen die folgenden Informationen an:
  - **Zertifikat**
    - **Name der Anmeldeinformationen**: Geben Sie einen Namen für die Anmeldeinformationen ein.
    - **Anmeldeinformationsdateipfad**: Klicken Sie auf "Durchsuchen" und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
  - **Schlüsselspeicher**
    - **Name der Anmeldeinformationen**: Geben Sie einen Namen für die Anmeldeinformationen ein.
    - **Anmeldeinformationsdateipfad**: Klicken Sie auf "Durchsuchen" und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
    - **Kennwort**: Geben Sie das Schlüsselspeicherkennwort für die Anmeldeinformationen ein.
  - **Serverzertifikat**
    - **Serverzertifikat**: Klicken Sie in der Liste auf das Zertifikat, das verwendet werden soll.
  - **Anmeldeinformationsanbieter**
    - **Anmeldeinformationsanbieter**: Klicken Sie in der Liste auf den Namen des Anmeldeinformationsanbieters.

Konfigurieren von Windows Desktop-/Tablet-Einstellungen



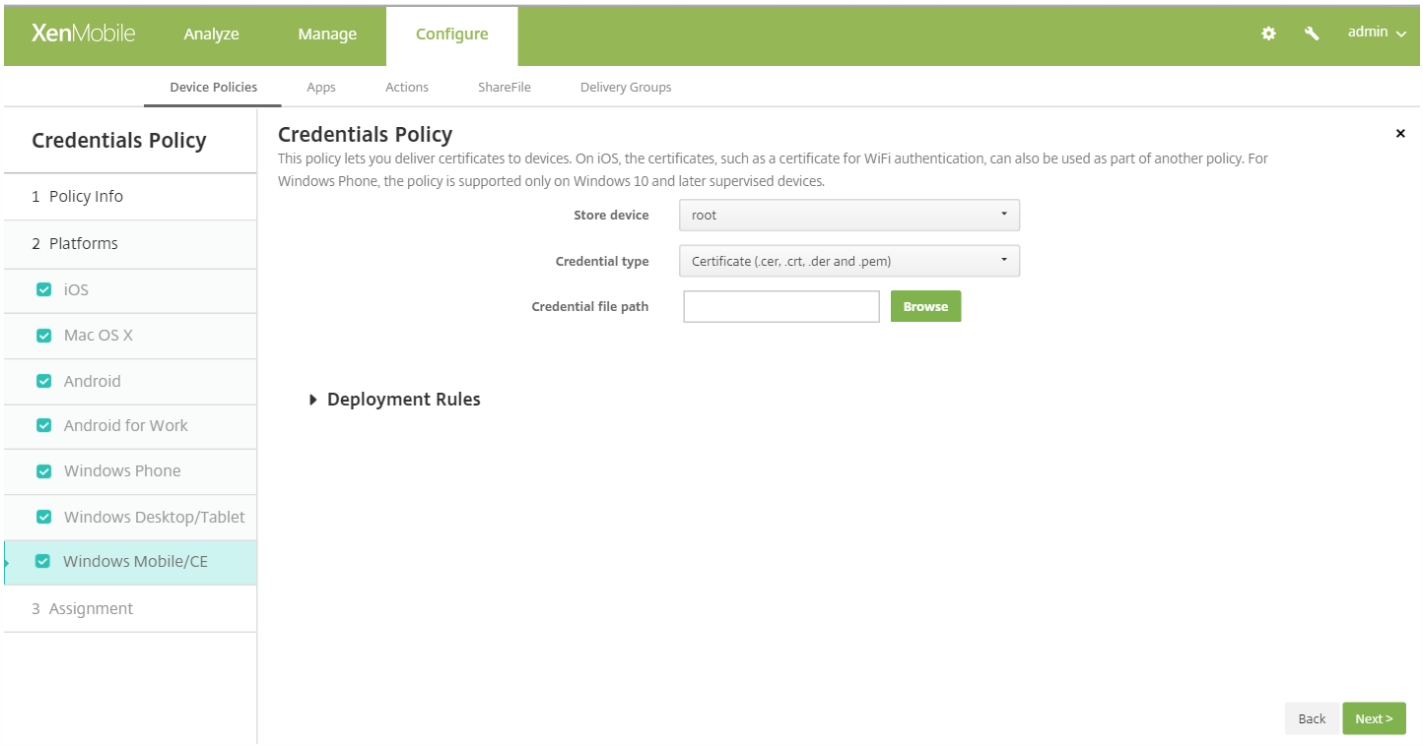
Konfigurieren Sie die folgenden Einstellungen:

- **OS-Version**: Klicken Sie in der Liste auf **8.1** für Windows 8.1 oder auf **10** für Windows 10. Der Standardwert ist **10**.

Windows 10-Einstellungen

Windows 8.1-Einstellungen

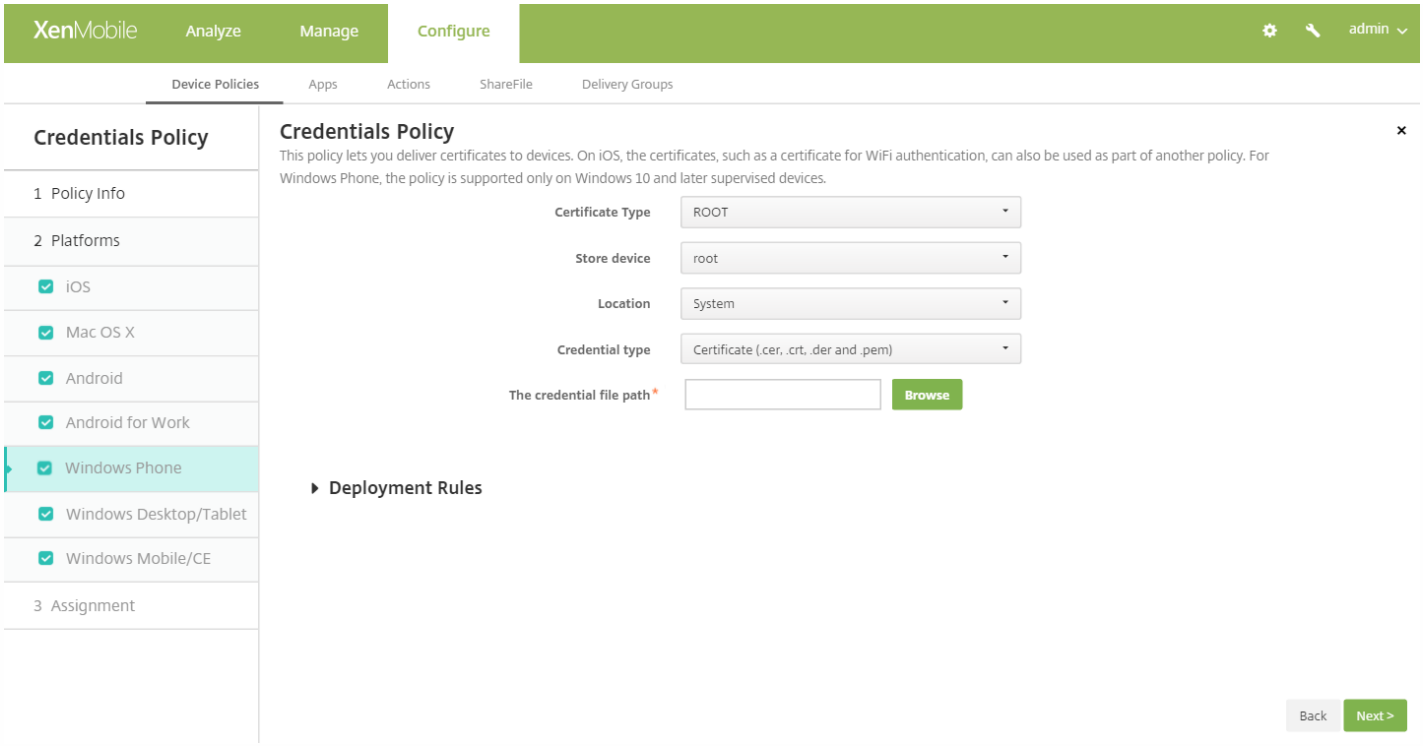
Konfigurieren von Windows Mobile-/CE-Einstellungen



Konfigurieren Sie die folgenden Einstellungen:

- **Speichergerät**: Klicken Sie in der Liste auf den Speicherort des Zertifikatspeichers für die Anmeldeinformationen. Der Standardwert ist **Stamm**. Optionen:
  - **Vertrauensstellen für privilegierte Ausführung**: Anwendungen, die mit einem Zertifikat aus diesem Speicher signiert sind, werden mit privilegierter Vertrauensstellung ausgeführt.
  - **Vertrauensstellen für nicht privilegierte Ausführung**: Anwendungen, die mit einem Zertifikat aus diesem Speicher signiert sind, werden mit normaler Vertrauensstellung ausgeführt.
  - **SPC (Softwareherausgeberzertifikat)**: Das Softwareherausgeberzertifikat wird für die Signierung von CAB-Dateien verwendet.
  - **Stamm**: Zertifikatspeicher, der Stamm-oder selbstsignierte Zertifikate enthält.
  - **ZS**: Zertifikatspeicher mit Kryptografieinformationen, einschließlich Zwischenzertifizierungsstellen.
  - **Eigene**: Zertifikatspeicher mit eigenen Zertifikaten des Endbenutzers.
- **Anmeldeinformationstyp**: Für Windows Mobile-/CE-Geräte steht nur der Typ "Zertifikat" zur Verfügung.
- **Anmeldeinformationsdateipfad**: Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.

Konfigurieren von Windows Phone-Einstellungen

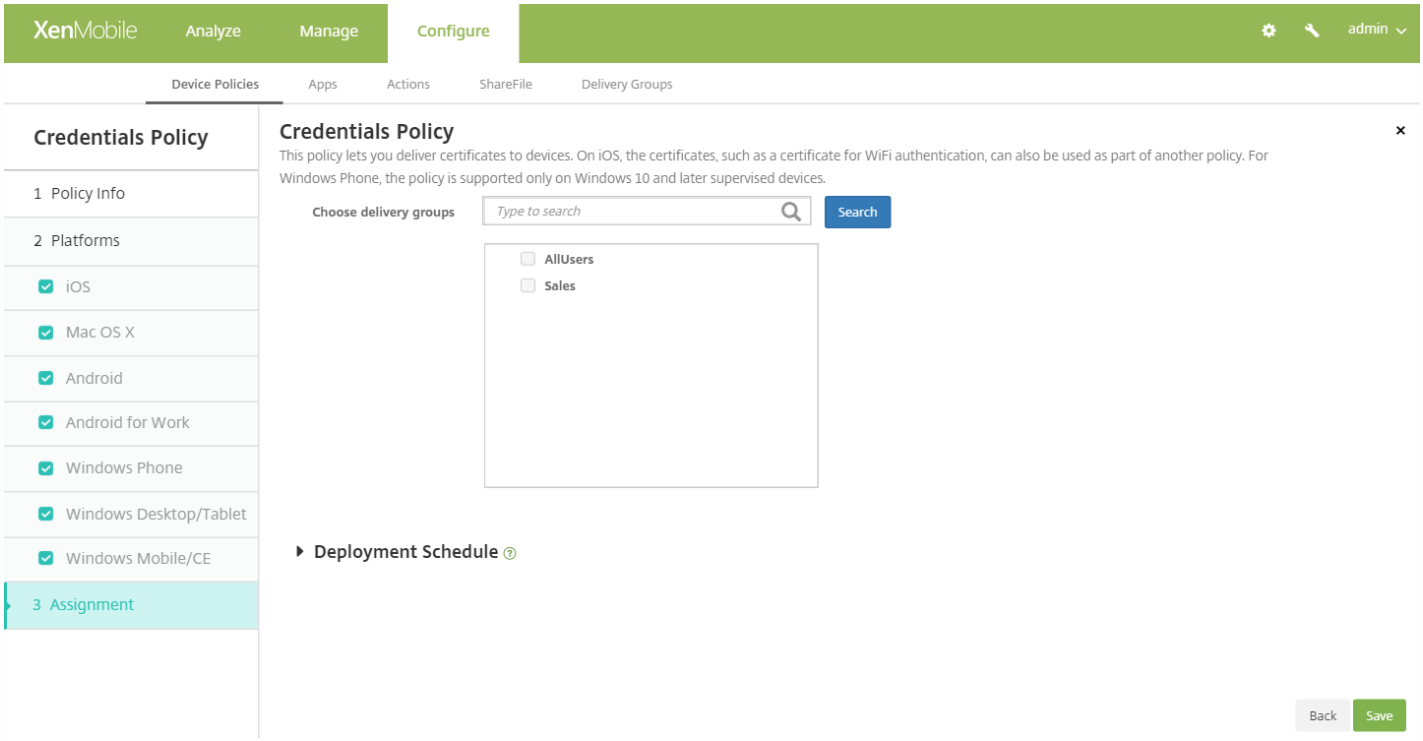


Konfigurieren Sie die folgenden Einstellungen:

- **Zertifikattyp**: Klicken Sie in der Liste auf "ROOT" oder "CLIENT".
- Bei Auswahl von **ROOT** konfigurieren Sie die folgenden Einstellungen:
  - **Speichergerät**: Klicken Sie in der Liste auf **Stamm**, **Eigene** oder **ZS**, um den Speicherort des Zertifikatspeichers für die Anmeldeinformationen anzugeben. Bei Auswahl von **Eigene** wird das Zertifikat in den Zertifikatspeichern der Benutzer gespeichert.
  - **Speicherort**: "System" ist der einzige Speicherort für Windows Phone-Geräte.
  - **Anmeldeinformationstyp**: Für Windows Phone-Geräte steht nur der Typ "Zertifikat" zur Verfügung.
  - **Anmeldeinformationsdateipfad**: Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
- Bei Auswahl von **CLIENT** konfigurieren Sie die folgenden Einstellungen:
  - **Speicherort**: **System** ist der einzige Speicherort für Windows Phone-Geräte.
  - **Anmeldeinformationstyp**: Für Windows Phone-Geräte steht nur der Typ **Schlüsselspeicher** zur Verfügung.
  - **Name der Anmeldeinformationen**: Geben Sie einen Namen für die Anmeldeinformationen ein. Diese Angabe ist erforderlich.
  - **Anmeldeinformationsdateipfad**: Klicken Sie auf "Durchsuchen" und navigieren Sie zum Speicherort der Anmeldeinformationsdatei, um diese auszuwählen.
  - **Kennwort**: Geben Sie das den Anmeldeinformationen zugeordnete Kennwort ein. Diese Angabe ist erforderlich.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Anmeldeinformationsrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Benutzerdefinierte XML-Richtlinien für Geräte

Jul 28, 2016

Sie können benutzerdefinierte XML-Richtlinien in XenMobile erstellen, wenn Sie die folgenden Features auf Windows Phone-, Windows Desktop/Tablet- und Windows Mobile/CE-Geräten anpassen möchten:

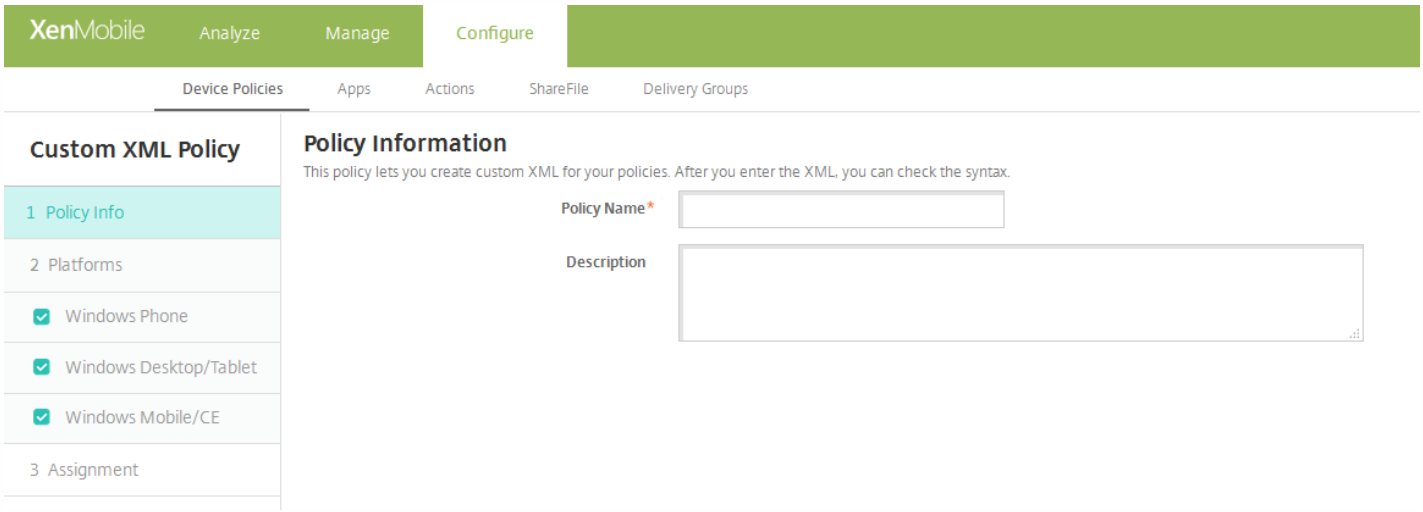
- Provisioning, d. h. Konfiguration des Geräts und Aktivieren bzw. Deaktivieren von Features
- Gerätekonfiguration, einschließlich des Zulassens der Änderung von Einstellungen und Geräteparametern durch die Benutzer
- Softwareupgrades, d. h. Bereitstellung neuer Software oder von Fehlerbehebungen für 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 verwendet. Das Erstellen benutzerdefinierter XML-Konfigurationen mit der OMA DM-API geht über den Rahmen dieses Abschnitts hinaus. Informationen zum Verwenden der OMA DM-API finden Sie auf Microsoft Developer Network unter OMA Device Management.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

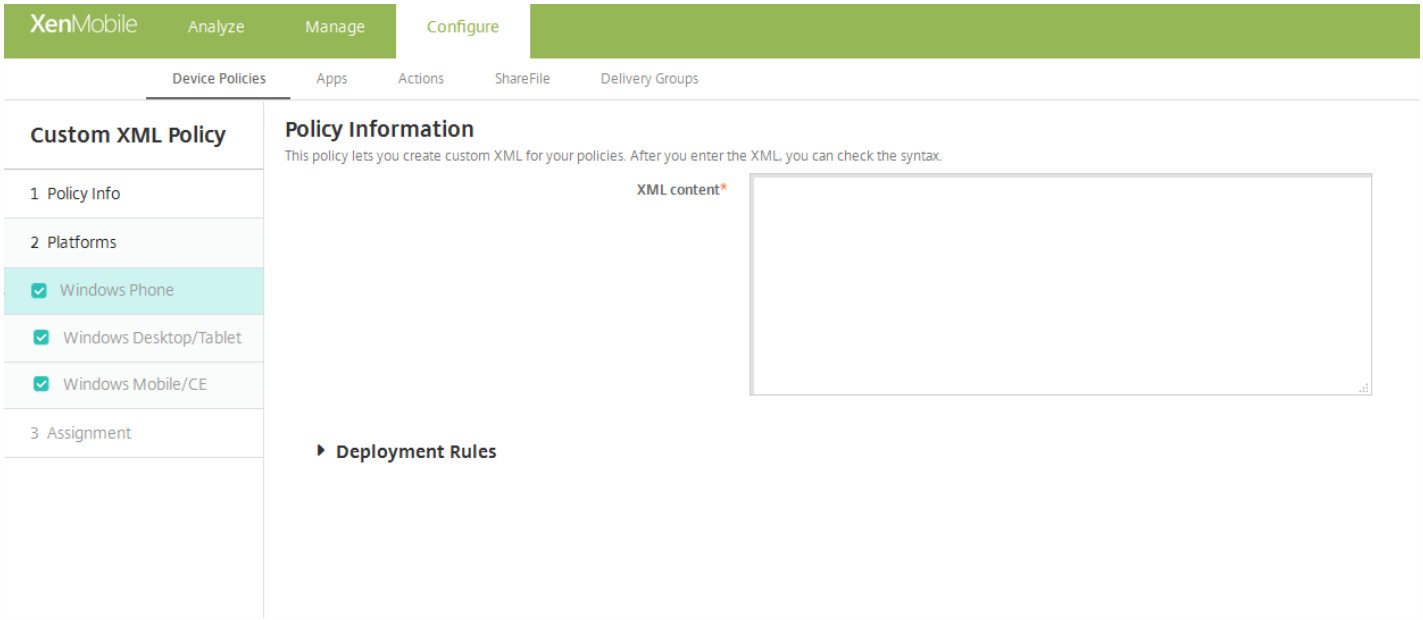
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Benutzerdefiniert** auf **Benutzerdefiniertes XML**. Die Seite für die Richtlinieninformationen der Richtlinie **Benutzerdefiniertes XML** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.



6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

7. Konfigurieren Sie für jede ausgewählte Plattform die folgende Einstellung:

- **XML-Inhalt**: Geben Sie den benutzerdefinierten XML-Code ein, den Sie der Richtlinie hinzufügen möchten, oder kopieren und fügen Sie ihn ein.

8. Konfigurieren der Bereitstellungsregeln

9. Klicken Sie auf **Weiter**. 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 **Zuweisung** für die benutzerdefinierte XML-Richtlinie angezeigt.

10. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

11. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen gemachten Änderungen werden auf alle Plattformen angewendet.

12. Klicken Sie auf **Speichern**.

Geräterichtlinie zum Löschen von Dateien und Ordnern

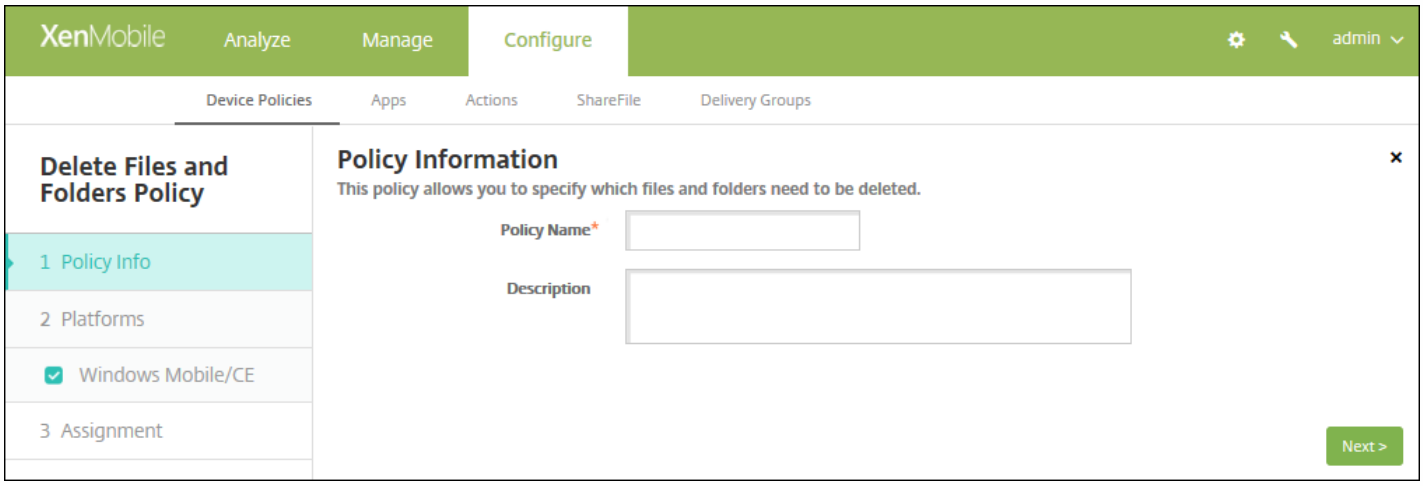
Jul 28, 2016

Sie können in XenMobile eine Richtlinie erstellen, mit der bestimmte Dateien und Ordner von Windows Mobile-/CE-Geräten gelöscht werden.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

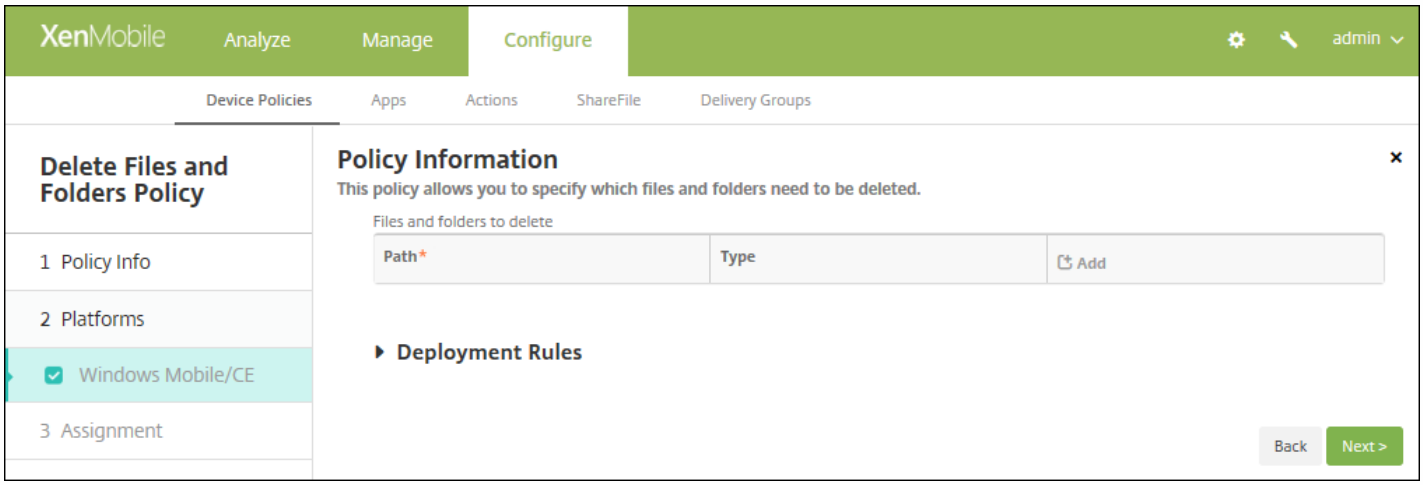
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Dateien und Ordner löschen**. Die Informationsseite für die Richtlinie wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Windows Mobile/CE** wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:

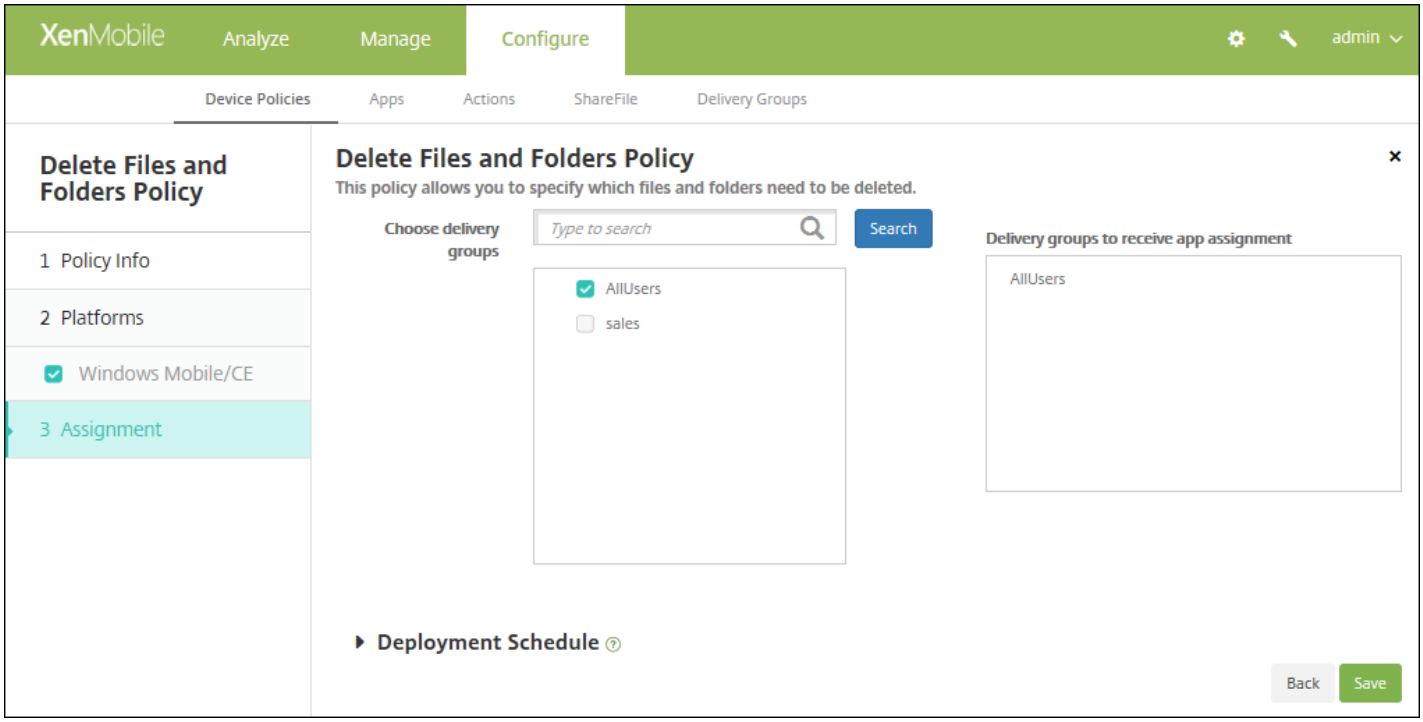
- **Folgende Dateien und Ordner löschen**: Klicken Sie für jedes Element, das gelöscht werden soll, auf "Hinzufügen" und führen Sie folgende Schritte aus:
  - **Pfad**: Geben Sie den Pfad zu der Datei bzw. dem Ordner ein.
  - **Typ**: Klicken Sie in der Liste auf "Datei" oder "Ordner". Die Standardeinstellung ist "Datei".
  - Klicken Sie auf **Speichern**, um die Einstellung zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

    Hinweis: Zum Löschen eines vorhandenen Eintrags zeigen Sie auf dessen Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Löschen** zum Löschen des Eintrags oder auf **Bearbeiten**, um ihn beizubehalten.

    Zum Bearbeiten eines Eintrags 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.

- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Geräterichtlinie zum Löschen von Registrierungsschlüssel und -werten

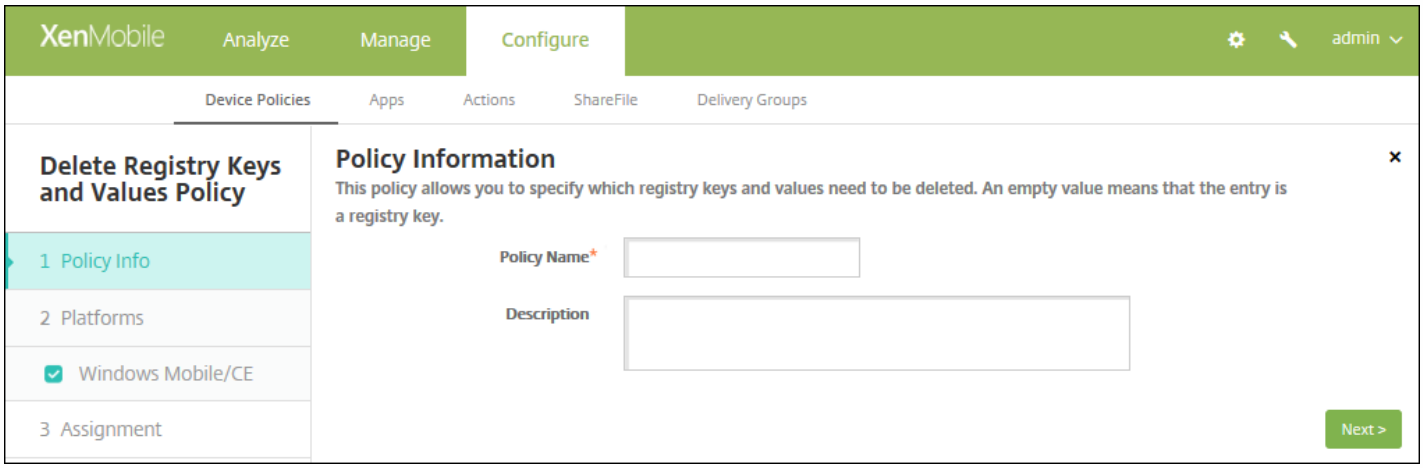
Jul 28, 2016

Sie können in XenMobile eine Richtlinie erstellen, mit der bestimmte Registrierungsschlüssel und -werte von Windows Mobile-/CE-Geräten gelöscht werden.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

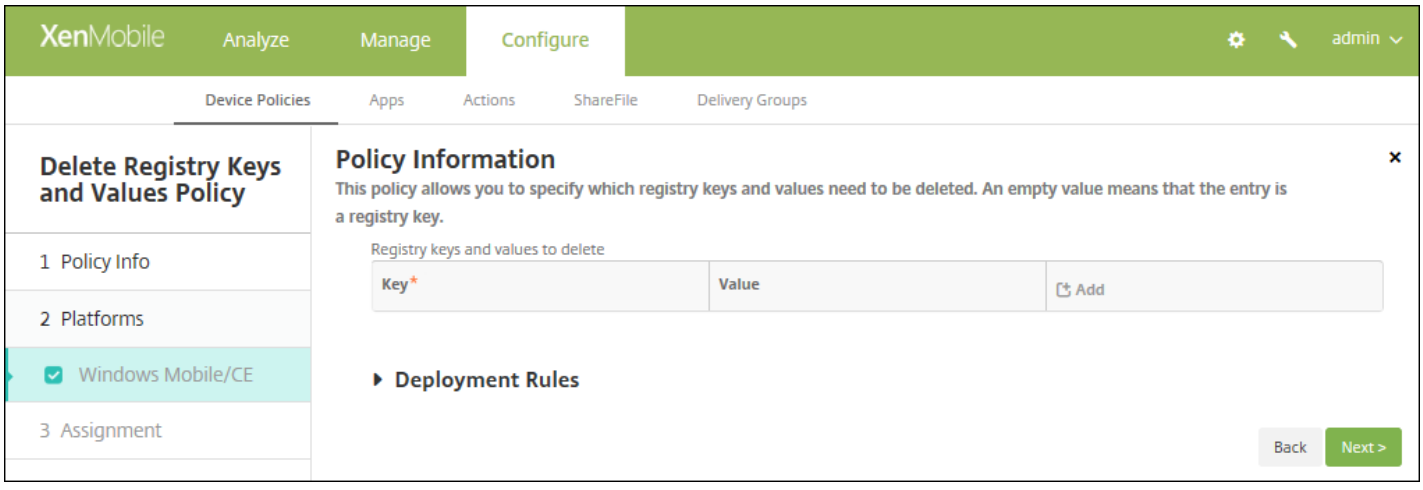
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Registrierungsschlüssel und -werte löschen**. Die Seite **Registrierungsschlüssel und -werte löschen** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Windows Mobile/CE** wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:

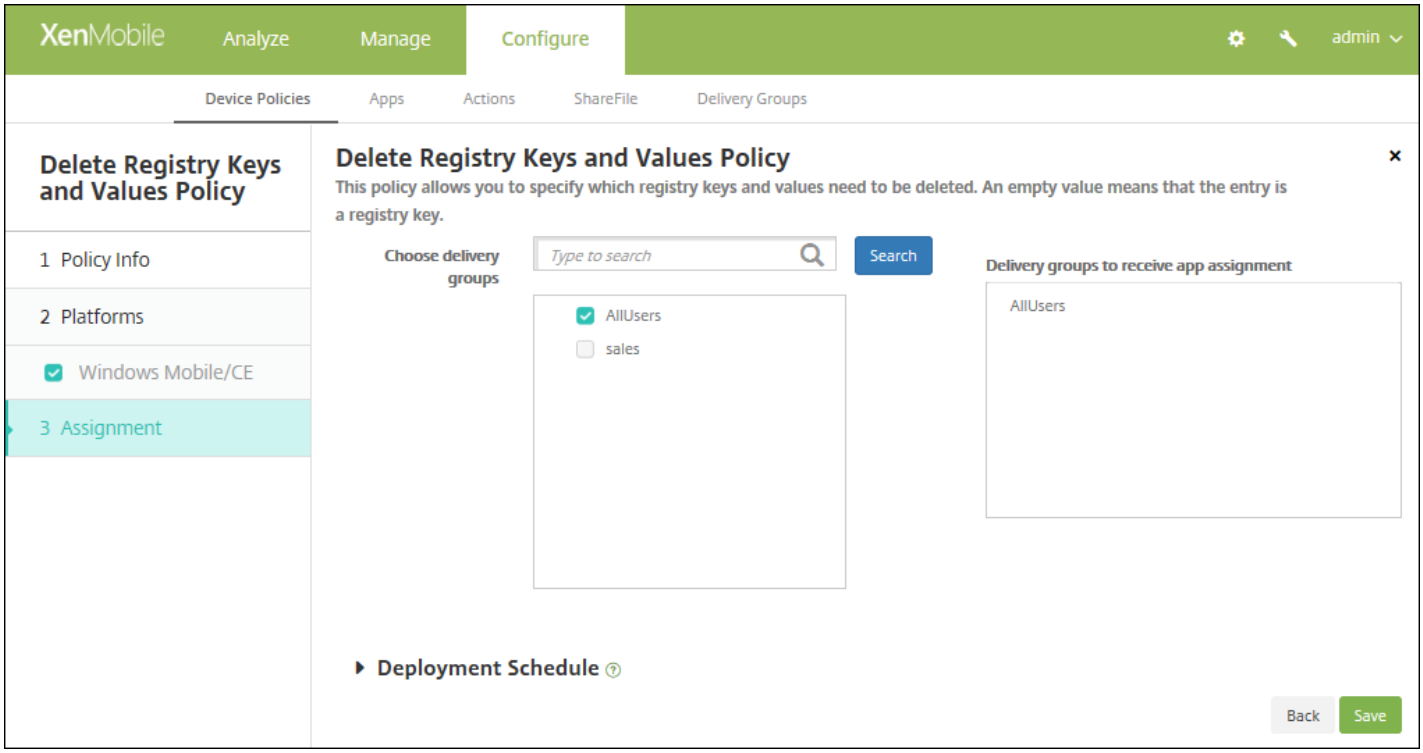
- **Folgende Registrierungsschlüssel und -werte löschen**: Klicken Sie für jeden Registrierungsschlüssel/-wert, der gelöscht werden soll, auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Schlüssel**: Geben Sie den Pfad des Registrierungsschlüssels ein. Diese Angabe ist obligatorisch. Der Pfad muss mit "HKEY_CLASSES_ROOT\", "HKEY_CURRENT_USER\", "HKEY_LOCAL_MACHINE\" oder "HKEY_USERS\" beginnen.
  - **Wert**: Geben Sie den Namen des Werts ein, der gelöscht werden soll, oder lassen Sie dieses Feld leer, um den gesamten Registrierungsschlüssel zu löschen.
  - Klicken Sie auf **Speichern**, um den Schlüssel/Wert zu speichern oder auf **Abbrechen**, um die Angaben nicht zu speichern.

    Hinweis: Zum Löschen eines vorhandenen Eintrags zeigen Sie auf dessen Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Löschen** zum Löschen des Eintrags oder auf **Bearbeiten**, um ihn beizubehalten.

    Zum Bearbeiten eines Eintrags 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** der Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Integritätsnachweisrichtlinie für Geräte

Jul 28, 2016

Sie können in XenMobile festlegen, dass Windows 10-Geräte ihren Integritätszustand melden müssen. Hierfür werden von den Geräten bestimmte Daten und Laufzeitinformationen an den Health Attestation Service (HAS) zur Analyse gesendet. Der HAS erstellt ein Health Attestation-Zertifikat und sendet es an das Gerät, von wo aus es an XenMobile gesendet wird. Basierend auf dem Inhalt des Health Attestation-Zertifikats kann XenMobile dann automatische Aktionen auslösen, die Sie zuvor eingerichtet haben.

Vom HAS werden folgende Parameter geprüft:

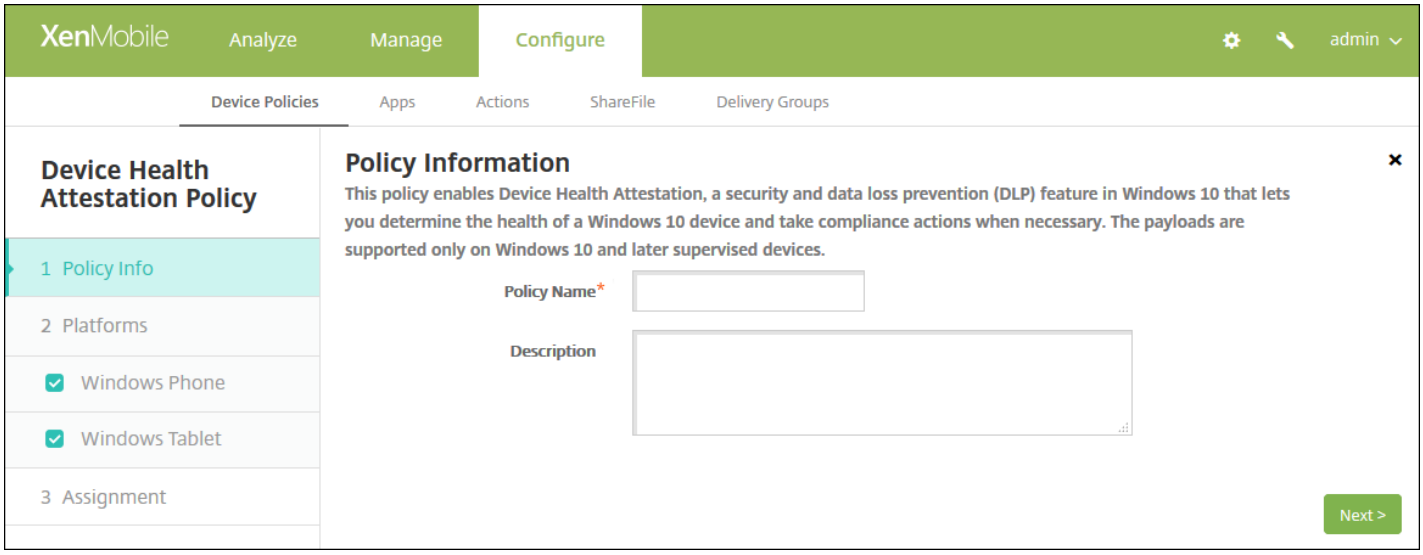
- AIK Present?
- Bit Locker Status
- Boot Debugging Enabled?
- Boot Manager Rev List Version
- Code Integrity Enabled?
- Code Integrity Rev List Version
- DEP Policy
- ELAM Driver Loaded?
- Issued At
- Kernel Debugging Enabled?
- PCR
- Reset Count
- Restart Count
- Safe Mode Enabled?
- SBCP Hash
- Secure Boot Enabled?
- Test Signing Enabled?
- VSM Enabled?
- WinPE Enabled?

Weitere Informationen finden Sie auf der Microsoft-Website unter HealthAttestation CSP.

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

2. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie dann unter **Benutzerdefiniert** auf **Device Health Attestation**. Die Seite **Device Health Attestation** wird angezeigt.



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

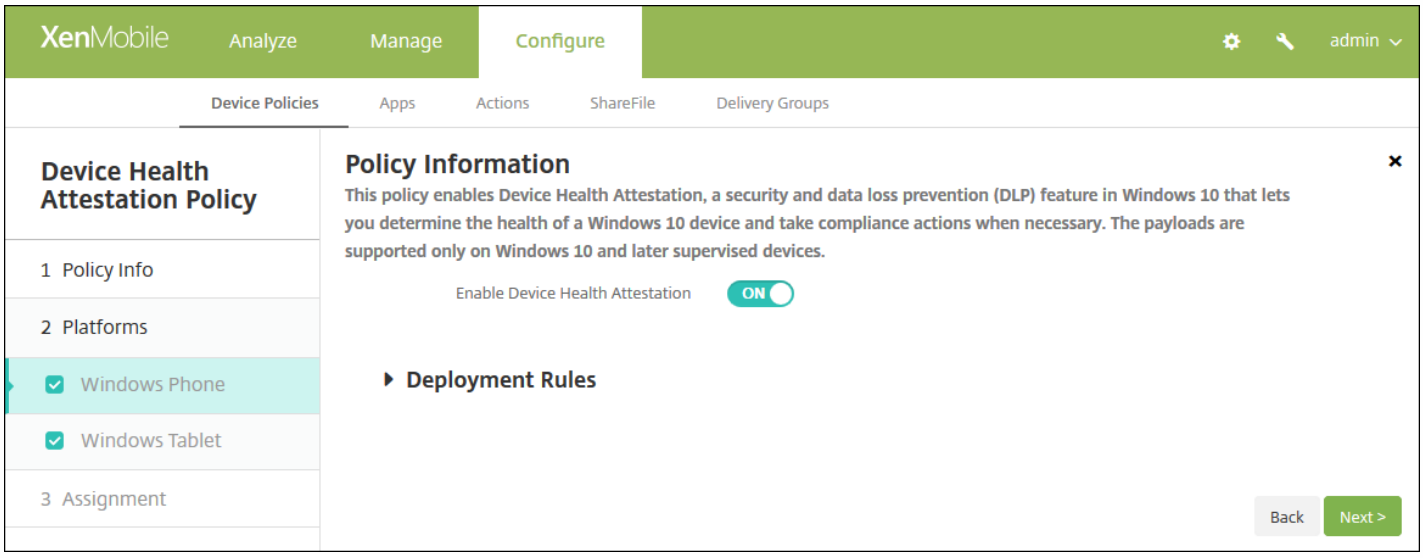
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

Konfigurieren von Windows Phone- und Windows Tablet-Einstellungen



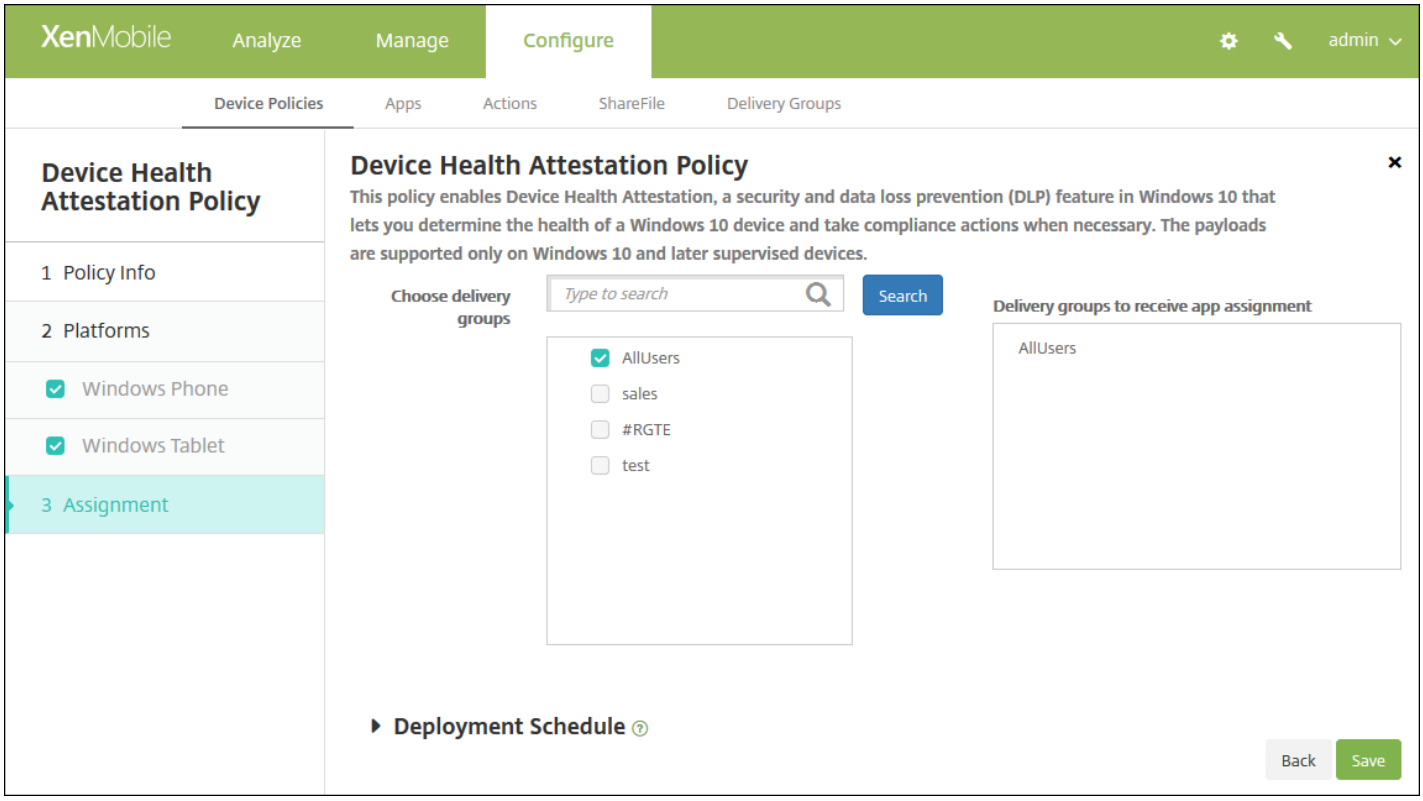
Konfigurieren Sie diese Einstellung für jede ausgewählte Plattform:

- **Integritätsnachweisrichtlinie für Windows-Geräte aktivieren**: Wählen Sie aus, ob ein Integritätsnachweis

erforderlich sein soll. Der Standardwert ist **AUS**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Integritätsnachweisrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Richtlinien für Gerätenamen

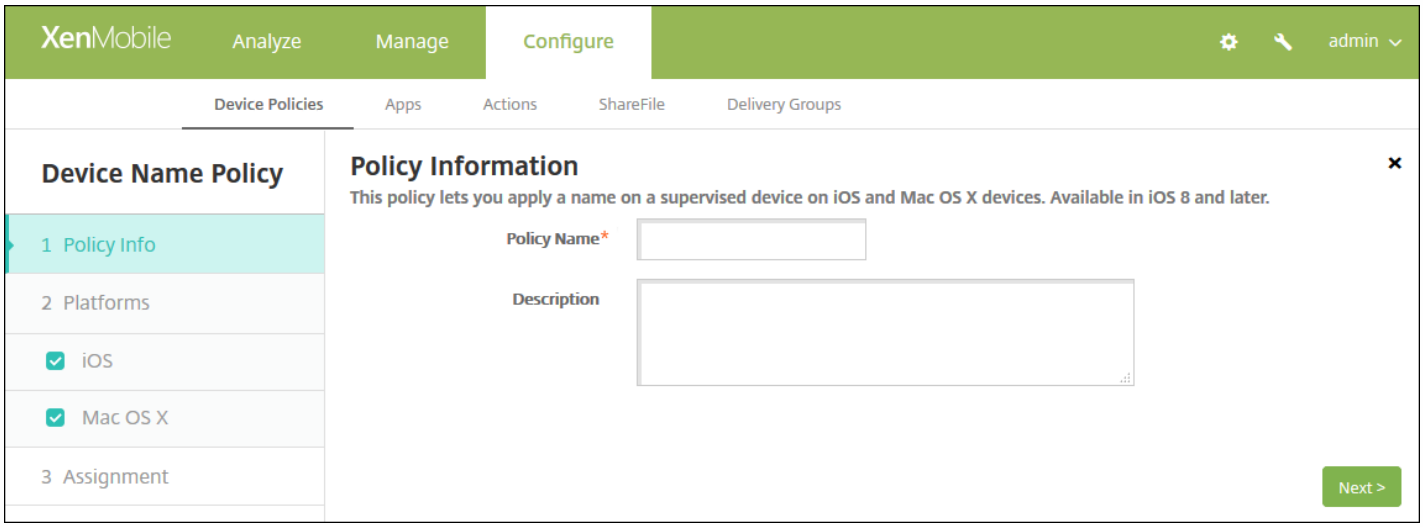
Jul 28, 2016

Sie können die Namen von iOS- und Mac OS X-Geräten zur einfacheren Identifizierung festlegen. Sie können Makros, Text oder eine Kombination daraus verwenden, um Gerätenamen festzulegen. Um beispielsweise als Gerätnamen die Seriennummer festzulegen, verwenden Sie ${device.serialnumber}. Soll der Gerätename sich aus Benutzernamen und dem Namen Ihrer Domäne zusammensetzen, verwenden Sie ${user.username}@example.com. Weitere Informationen finden Sie unter Makros in XenMobile.

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

2. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie unter **Endbenutzer** auf **Gerätename**. Die Seite **Richtlinieninfo** wird angezeigt.



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

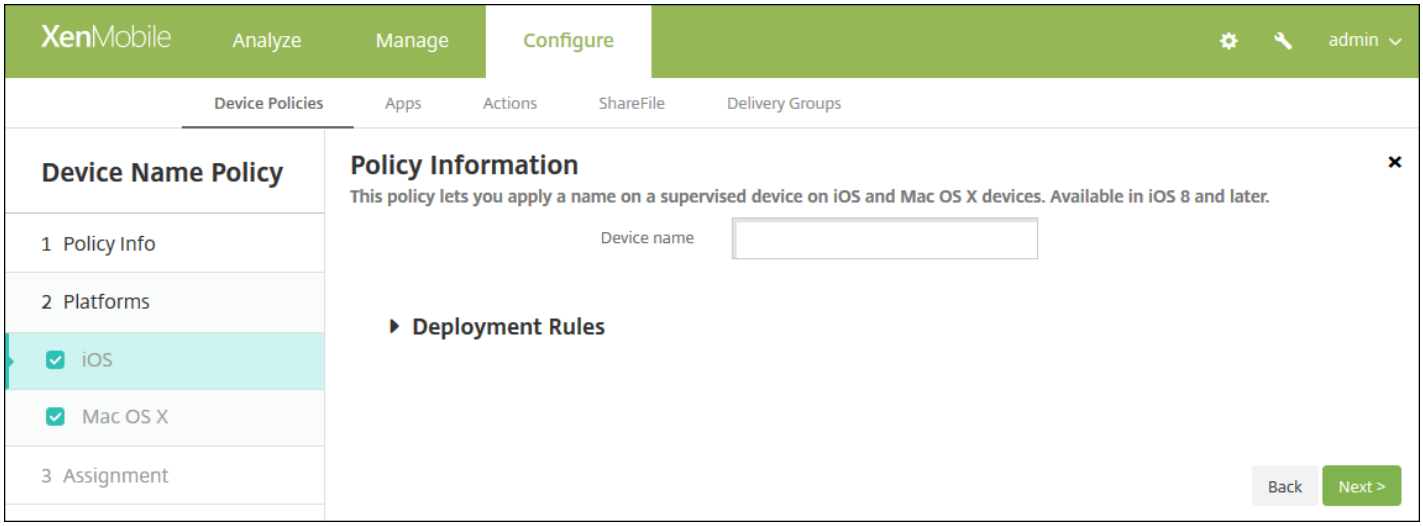
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

Konfigurieren von iOS- und Mac OS X-Einstellungen

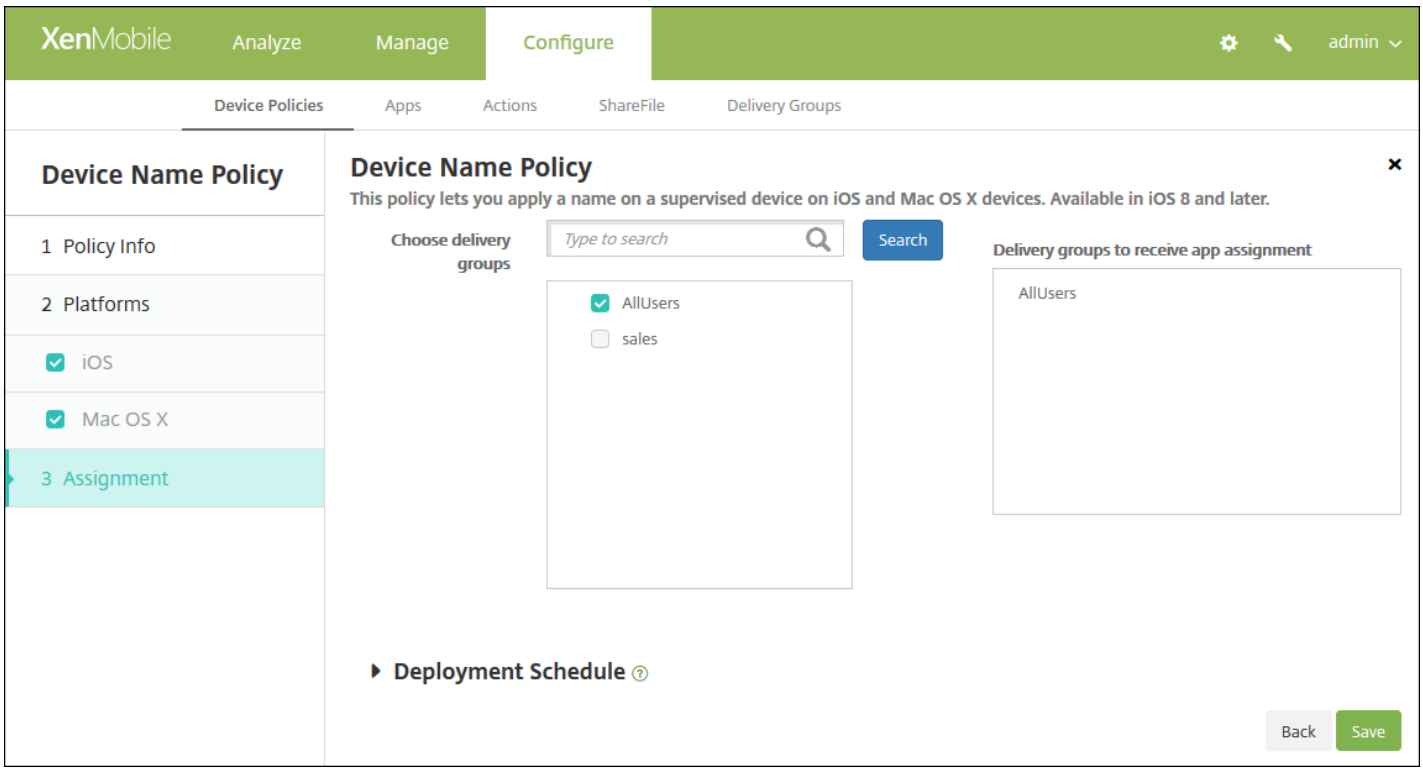


Konfigurieren Sie folgende Einstellung für die ausgewählten Plattformen:

- **Gerätename**: Geben Sie das Makro, eine Kombination aus Makros oder eine Kombination aus Makros und Text zur eindeutigen Benennung aller Geräte ein. Verwenden Sie z. B. ${device.serialnumber}, um als Gerätnamen die Seriennummer festzulegen oder ${device.serialnumber} ${ user.username }, um den Benutzername in den Gerätenamen aufzunehmen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen

Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Unternehmenshub

Jul 28, 2016

Mit einer Unternehmenshub-Geräterichtlinie für Windows Phone können Sie Apps über den Unternehmenshub-Unternehmensstore an Geräte verteilen.

Zum Erstellen der Richtlinie benötigen Sie Folgendes:

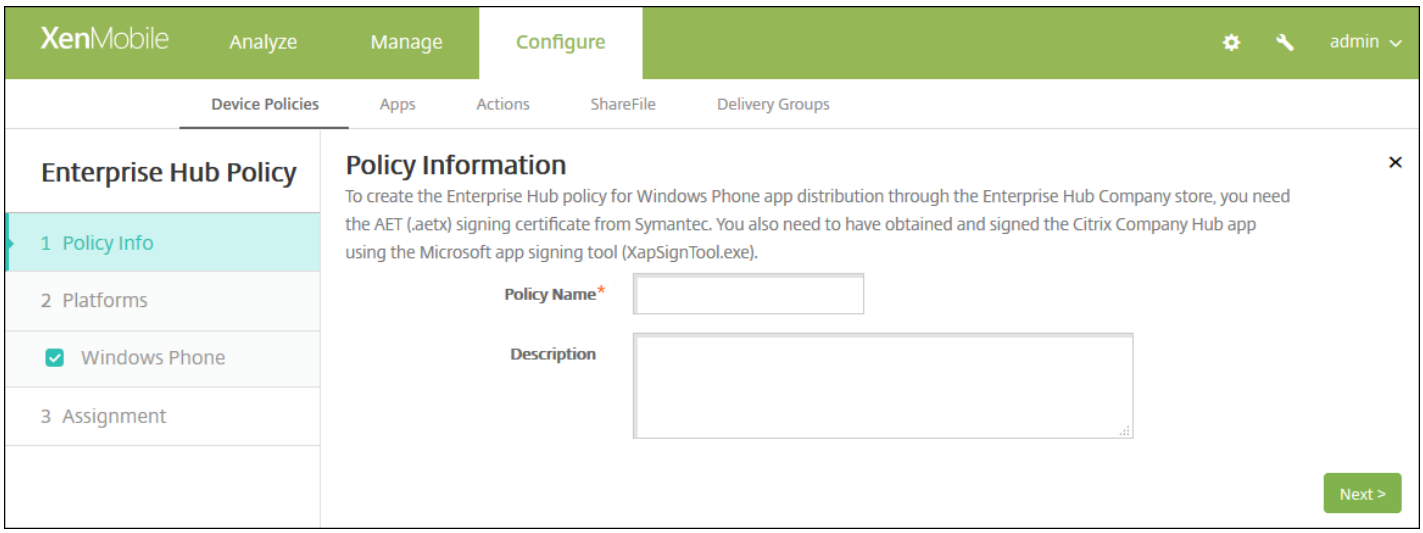
- Ein AET-Signaturzertifikat (.aetx) von Symantec
- Die mit dem Microsoft App-Signierungstool (XapSignTool.exe) signierte Citrix Company Hub-App

Hinweis: XenMobile unterstützt nur eine Unternehmenshub-Richtlinie für einen Modus von Windows Phone-Worx Home. Zum Hochladen von Worx Home für Windows Phone für XenMobile Enterprise Edition dürfen Sie beispielsweise nicht mehrere Unternehmenshub-Richtlinien mit mehreren Versionen von Worx Home für XenMobile Enterprise Edition erstellen. Sie können nur die erste Enterprise Hub-Richtlinie bei der Geräteregistrierung bereitstellen.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

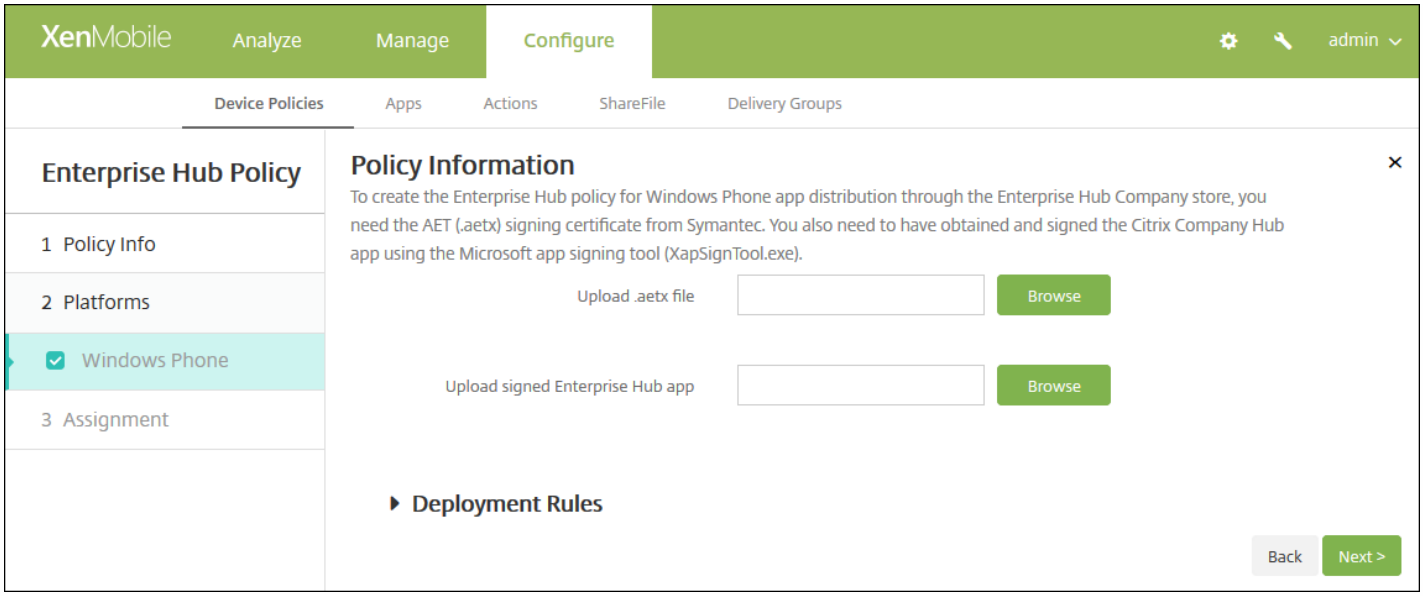
3. Erweitern Sie **Mehr** und klicken Sie dann unter **XenMobile-Agent** auf **Unternehmenshub**. Die Seite **Unternehmenshub** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Windows Phone** wird angezeigt.

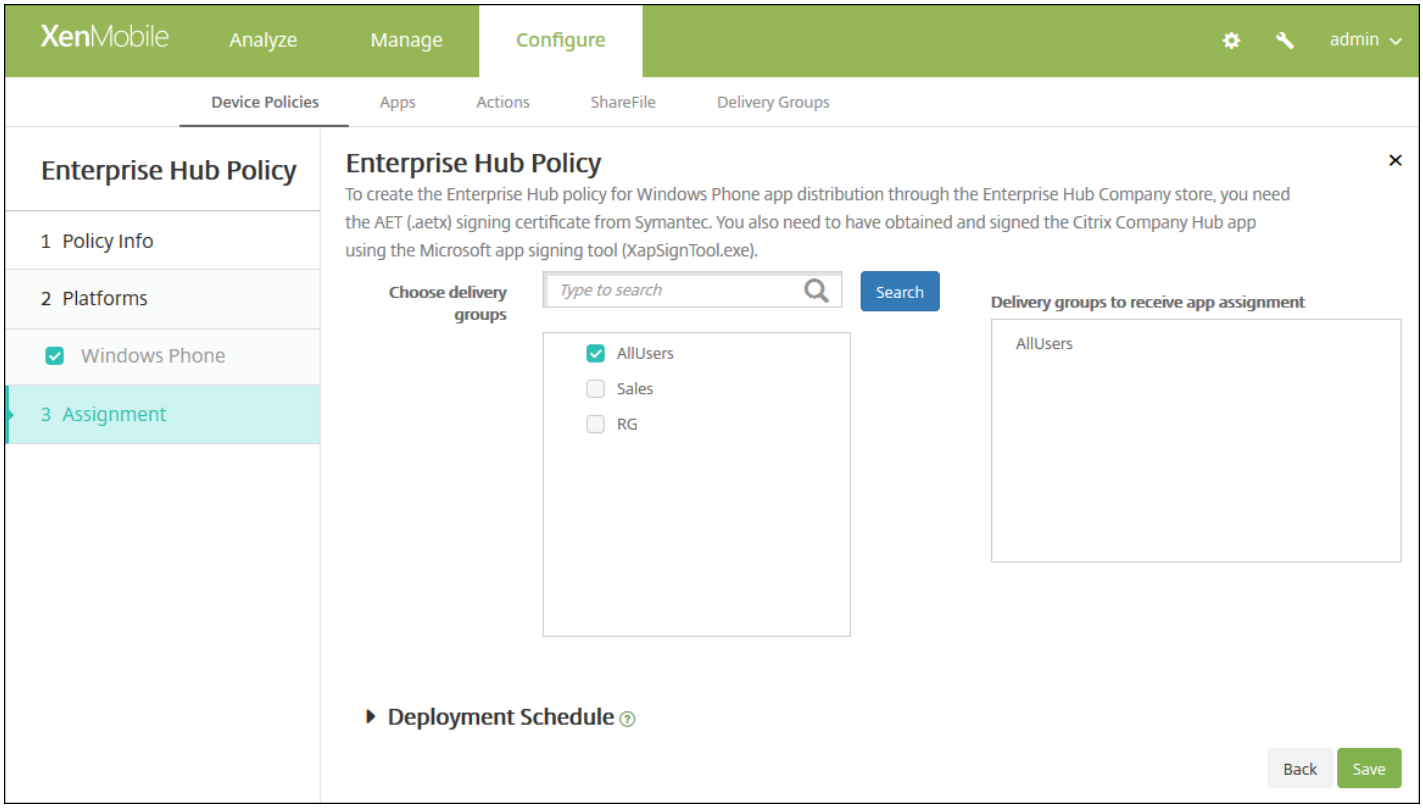


6. Konfigurieren Sie die folgenden Einstellungen:

- **AETX-Datei hochladen**: Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort der AETX-Datei, um diese auszuwählen.
- **Signierte Unternehmenshub-App hochladen**: Klicken Sie auf **Durchsuchen** und navigieren Sie zum Speicherort der Unternehmenshub-App, um diese auszuwählen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Unternehmenshub-Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Dateirichtlinien

Jul 28, 2016

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

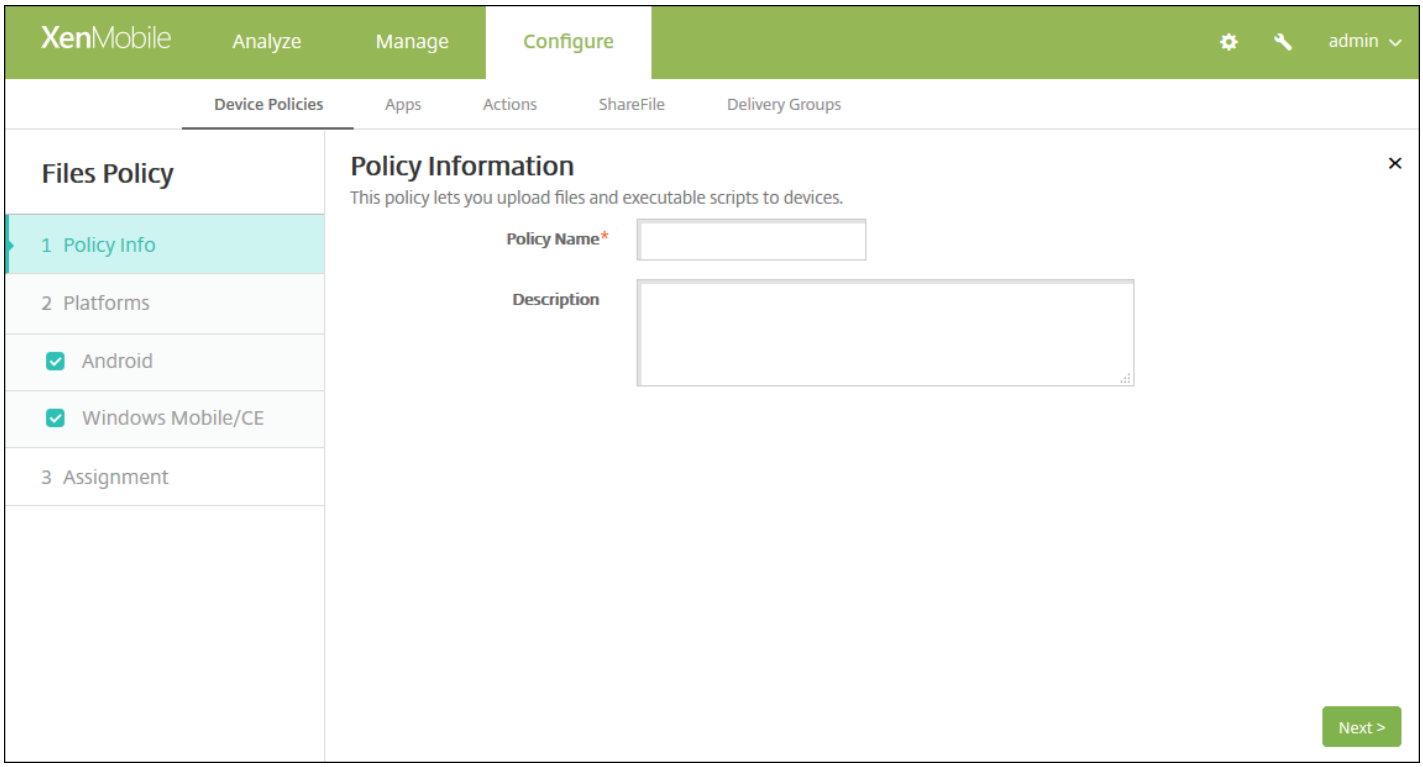
Sie können mit dieser Richtlinie die folgenden Dateitypen hinzufügen:

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

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

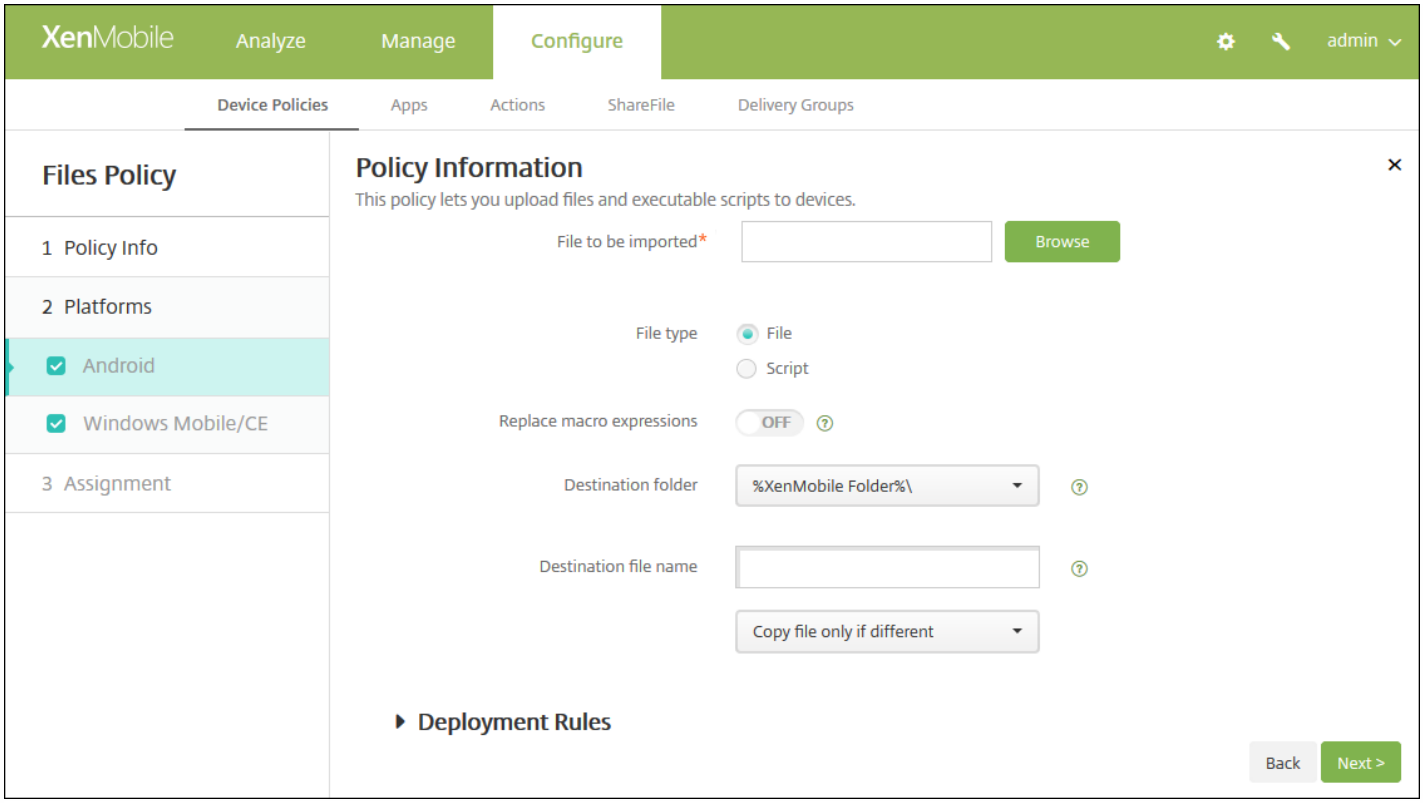
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Dateien**. Die Informationsseite **Dateien** wird angezeigt.



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

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

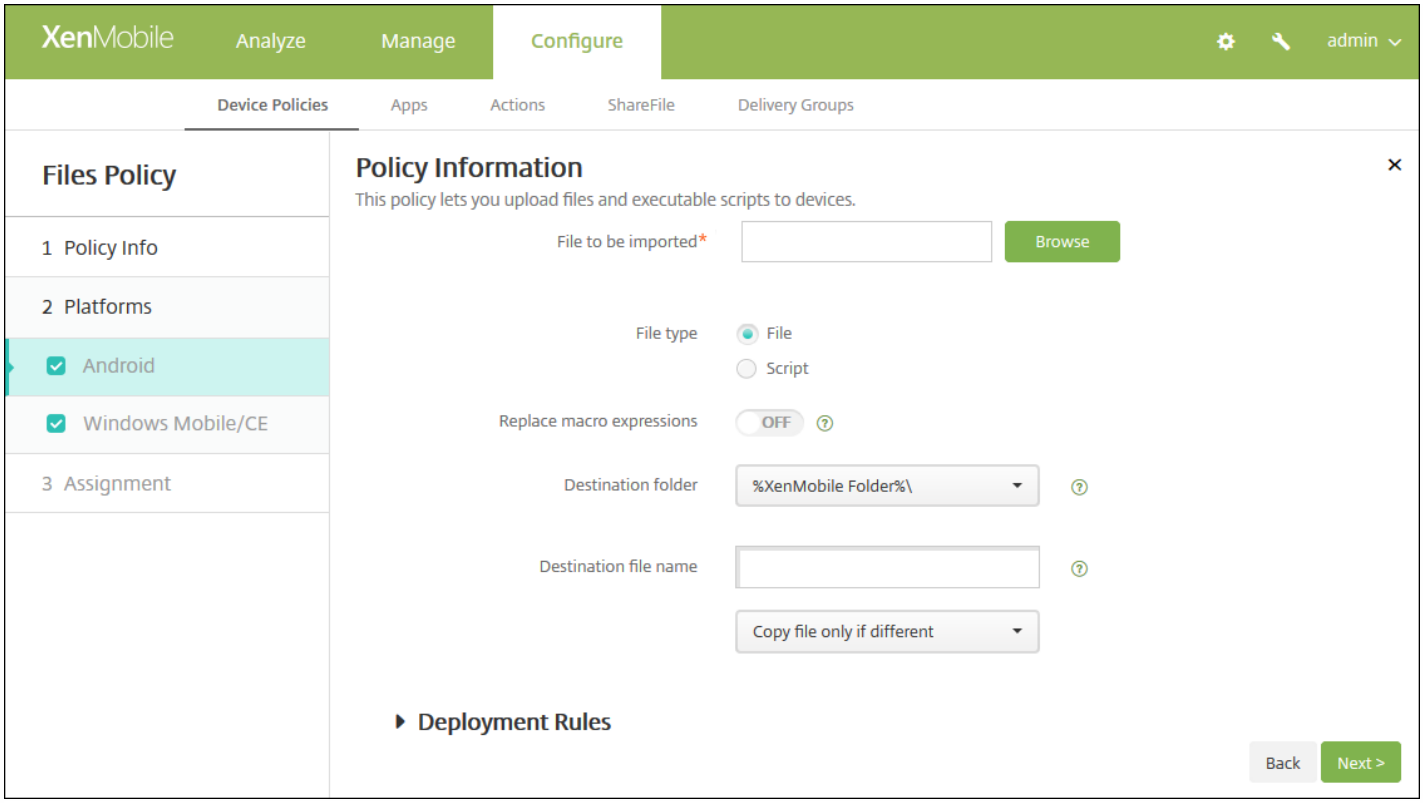
5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.



6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

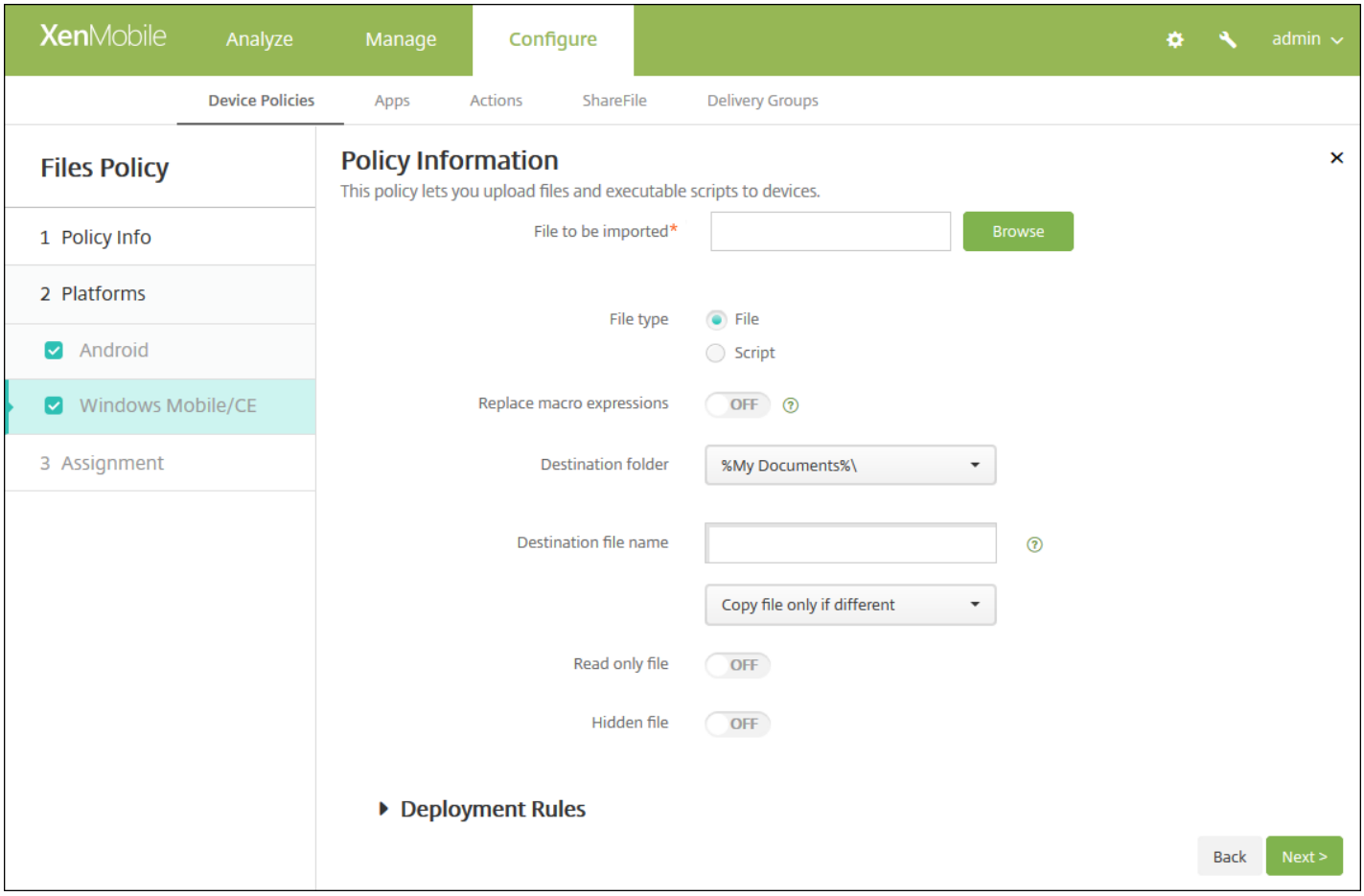
Konfigurieren von Android-Einstellungen



Konfigurieren Sie die folgenden Einstellungen:

- **Zu importierende Datei**: Klicken Sie zur Auswahl der zu importierenden Datei auf Browse und navigieren Sie zum Speicherort der Datei.
- **Dateityp**: Wählen Sie **Datei** oder **Skript** aus. Wenn Sie **Skript** auswählen, wird **Sofort ausführen** angezeigt. Legen Sie fest, ob das Skript ausgeführt werden soll, sobald die Datei hochgeladen wurde. Der Standardwert ist **AUS**.
- **Makroausdrücke ersetzen**: Wählen Sie, ob die Namen von Makrotoken in einem Skript durch eine Geräte- oder Benutzereigenschaft ersetzt werden. Der Standardwert ist **AUS**.
- **Zielordner**: Wählen Sie in der Liste den Speicherort für die hochgeladene Datei aus oder klicken Sie auf **Hinzufügen**, um einen nicht aufgeführten Speicherort auszuwählen. Sie können die Makros "%XenMobile Folder%\" oder "%Flash Storage%\" am Anfang eines Pfads verwenden.
- **Zieldateiname**: Optional können Sie einen anderen Namen für die Datei eingeben, wenn er vor der Bereitstellung auf einem Gerät geändert werden muss.
- **Datei nur kopieren, wenn unterschiedlich**: Wählen Sie in der Liste aus, ob die Datei kopiert werden soll, wenn sie nicht mit der vorhandenen Datei übereinstimmt. Standardmäßig ist vorgegeben, dass Dateien nur kopiert werden, wenn sie Unterschiede aufweisen.

Konfigurieren von Windows Mobile-/CE-Einstellungen

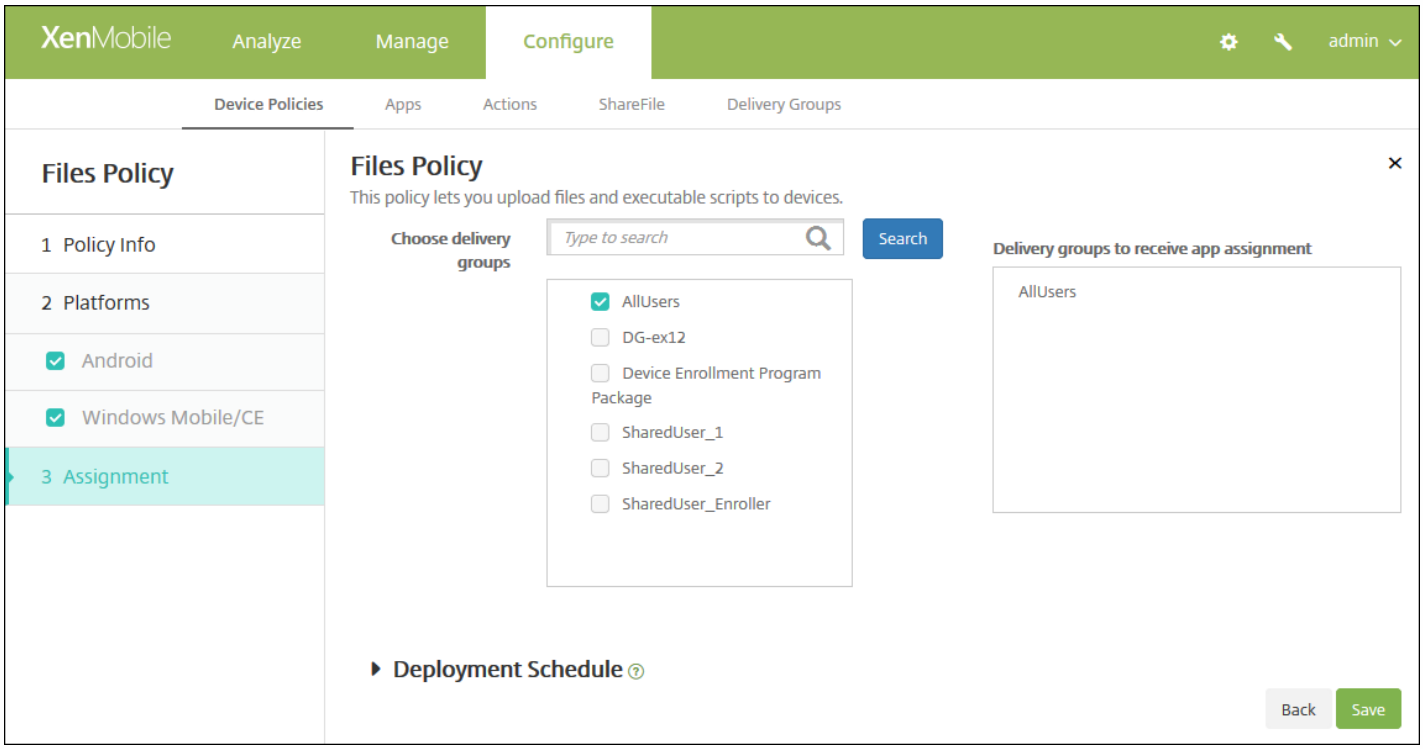


Konfigurieren Sie die folgenden Einstellungen:

- **Zu importierende Datei**: Klicken Sie zur Auswahl der zu importierenden Datei auf Browse und navigieren Sie zum Speicherort der Datei.
- **Dateityp**: Wählen Sie **Datei** oder **Skript** aus. Wenn Sie **Skript** auswählen, wird **Sofort ausführen** angezeigt. Legen Sie fest, ob das Skript ausgeführt werden soll, sobald die Datei hochgeladen wurde. Der Standardwert ist **AUS**.
- **Makroausdrücke ersetzen**: Wählen Sie, ob die Namen von Makrotoken in einem Skript durch eine Geräte- oder Benutzereigenschaft ersetzt werden. Der Standardwert ist **AUS**.
- **Zielordner**: Wählen Sie in der Liste den Speicherort für die hochgeladene Datei aus oder klicken Sie auf **Hinzufügen**, um einen nicht aufgeführten Speicherort auszuwählen. Sie können folgende Makros am Anfang des Pfads verwenden:
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %Eigene Dokumente%\\
  - %Windows%\
- **Zieldateiname**: Optional können Sie einen anderen Namen für die Datei eingeben, wenn er vor der Bereitstellung auf einem Gerät geändert werden muss.
- **Datei nur kopieren, wenn unterschiedlich**: Wählen Sie in der Liste aus, ob die Datei kopiert werden soll, wenn sie nicht mit der vorhandenen Datei übereinstimmt. Standardmäßig ist vorgegeben, dass Dateien nur kopiert werden, wenn sie Unterschiede aufweisen.
- **Schreibgeschützte Datei** : Wählen Sie aus, ob die Datei schreibgeschützt sein soll. Der Standardwert ist **AUS**.
- **Versteckte Datei**: Wählen Sie aus, ob die Datei aus der Liste ausgeblendet werden soll. Der Standardwert ist **AUS**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Dateirichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Geräterichtlinie für Schriftarten

Jul 28, 2016

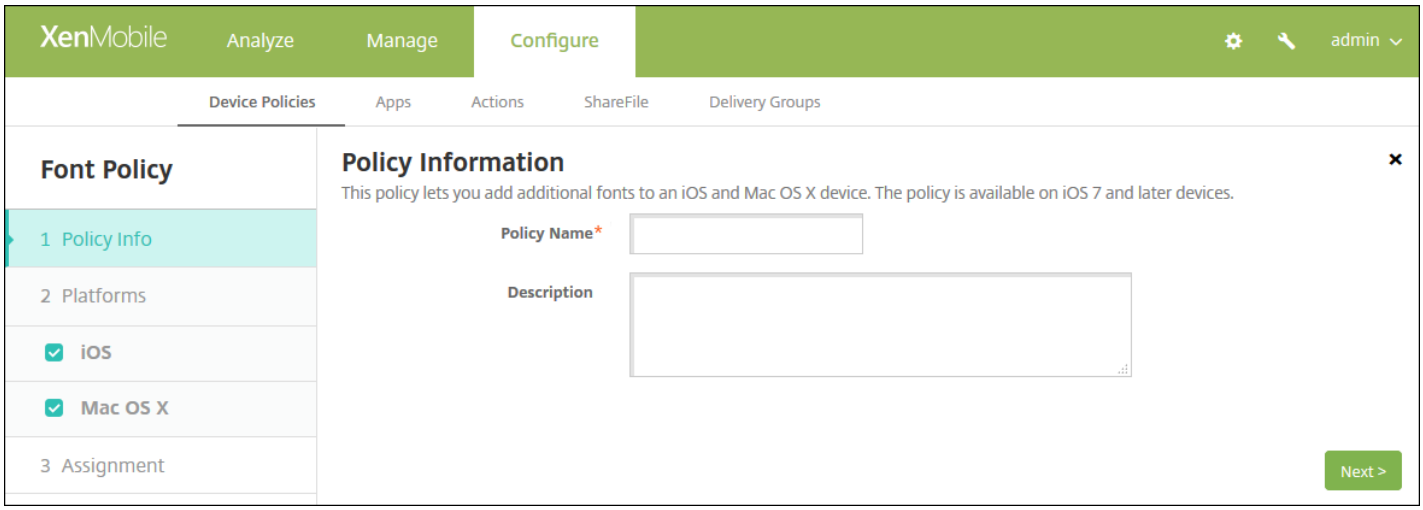
Sie können in XenMobile eine Geräterichtlinie einrichten, mit der zusätzliche Schriftarten auf iOS- und Mac OS X-Geräten hinzugefügt werden. Schriftarten müssen im Format TrueType (.ttf) oder OpenType (.oft) vorliegen. Schriftsammlungen (.ttc oder .otc) werden nicht unterstützt.

Hinweis für iOS: Die Richtlinie gilt nur für Version 7.0 und höher.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie unter **Endbenutzer** auf **Schriftart**. Die Seite für die Richtlinieninformationen für **Schriftarten** wird angezeigt.



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

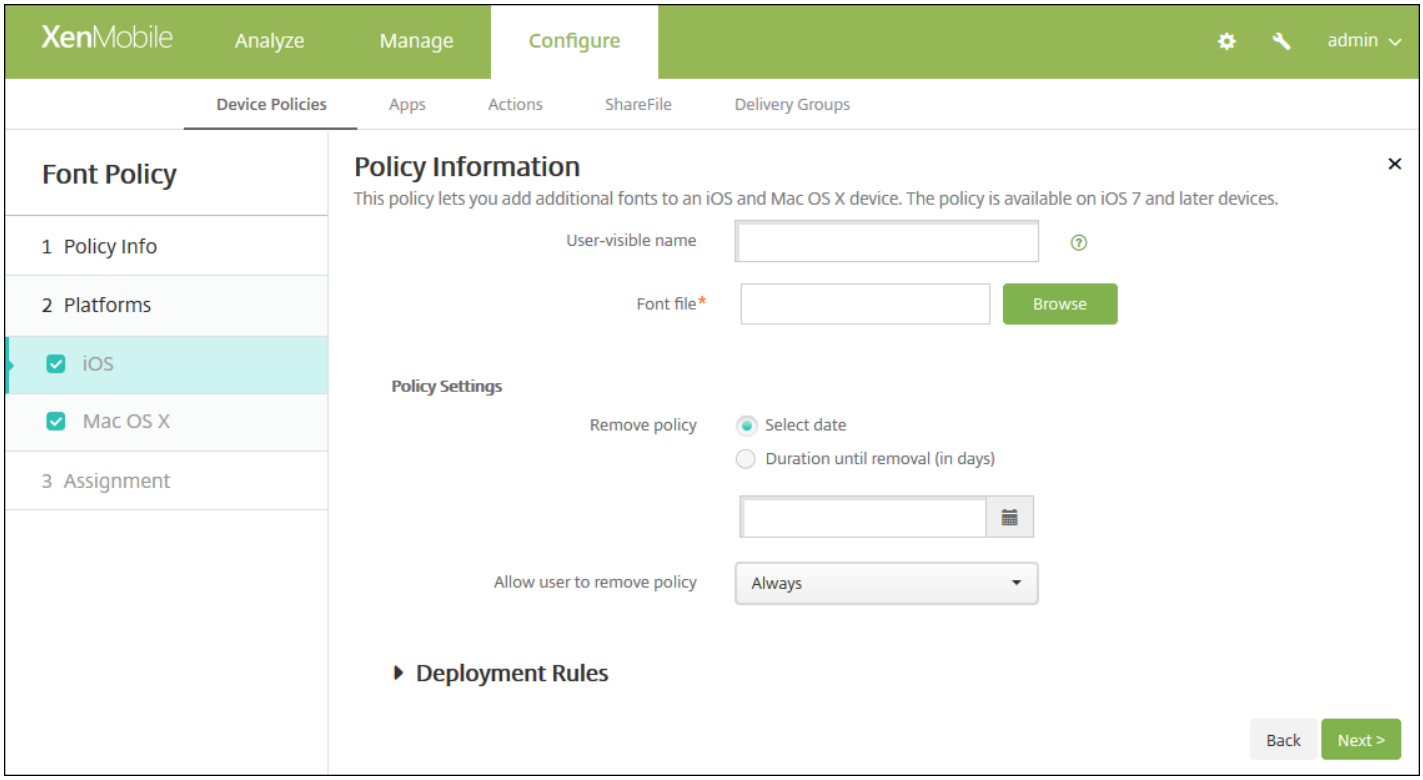
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

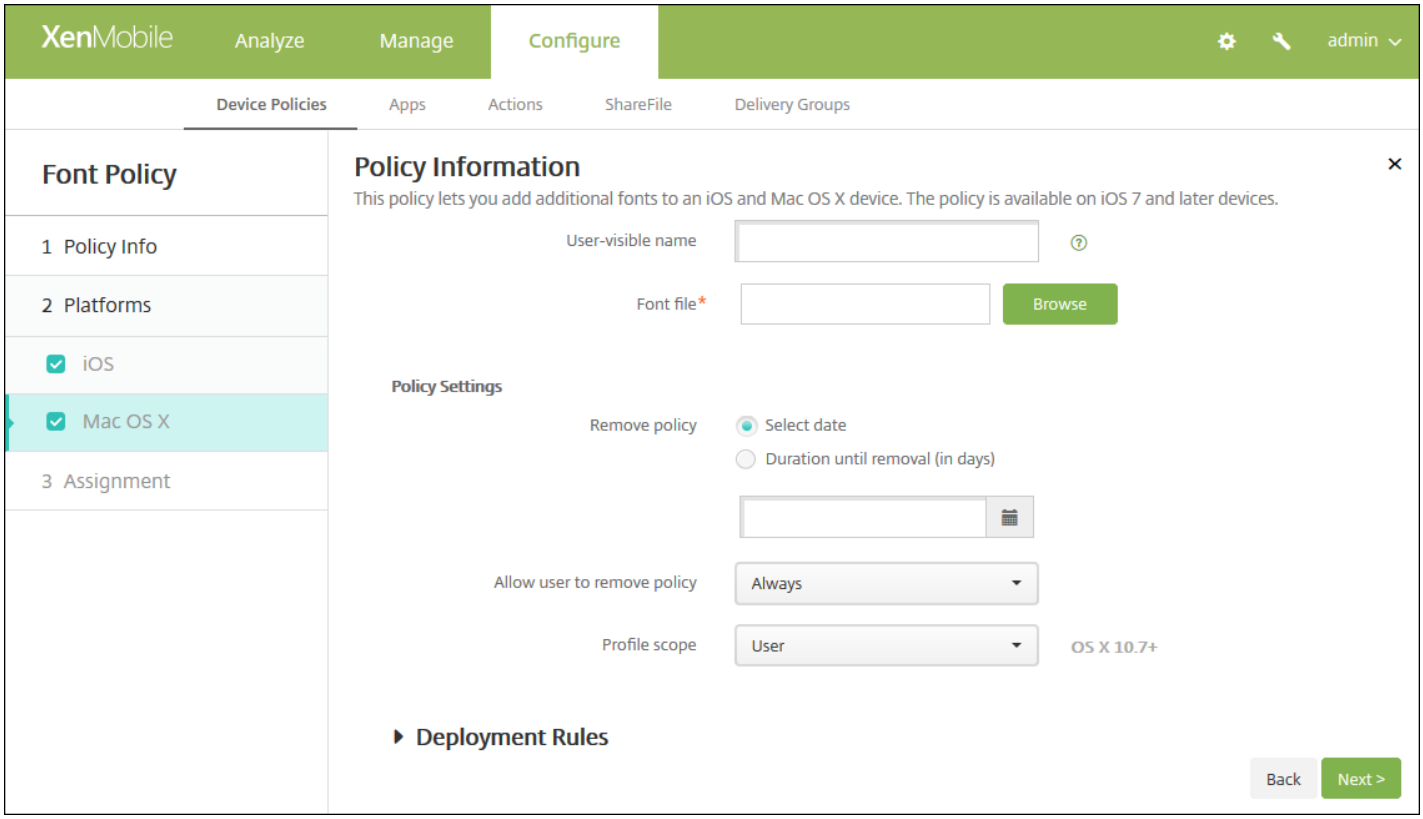
Konfigurieren der iOS-Einstellung



Konfigurieren Sie die folgenden Einstellungen:

- **Benutzern angezeigter Name**: Geben Sie den Namen so ein, wie er in der Liste der Schriftarten auf den Geräten angezeigt werden soll.
- **Schriftartendatei**: Wählen Sie die Schriftartdatei aus, die auf den Geräten der Benutzer hinzugefügt werden soll, indem Sie auf **Durchsuchen** klicken und zum Speicherort der Datei navigieren.
- **Richtlinieneinstellungen**
  - Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

Konfigurieren von Mac OS X-Einstellungen

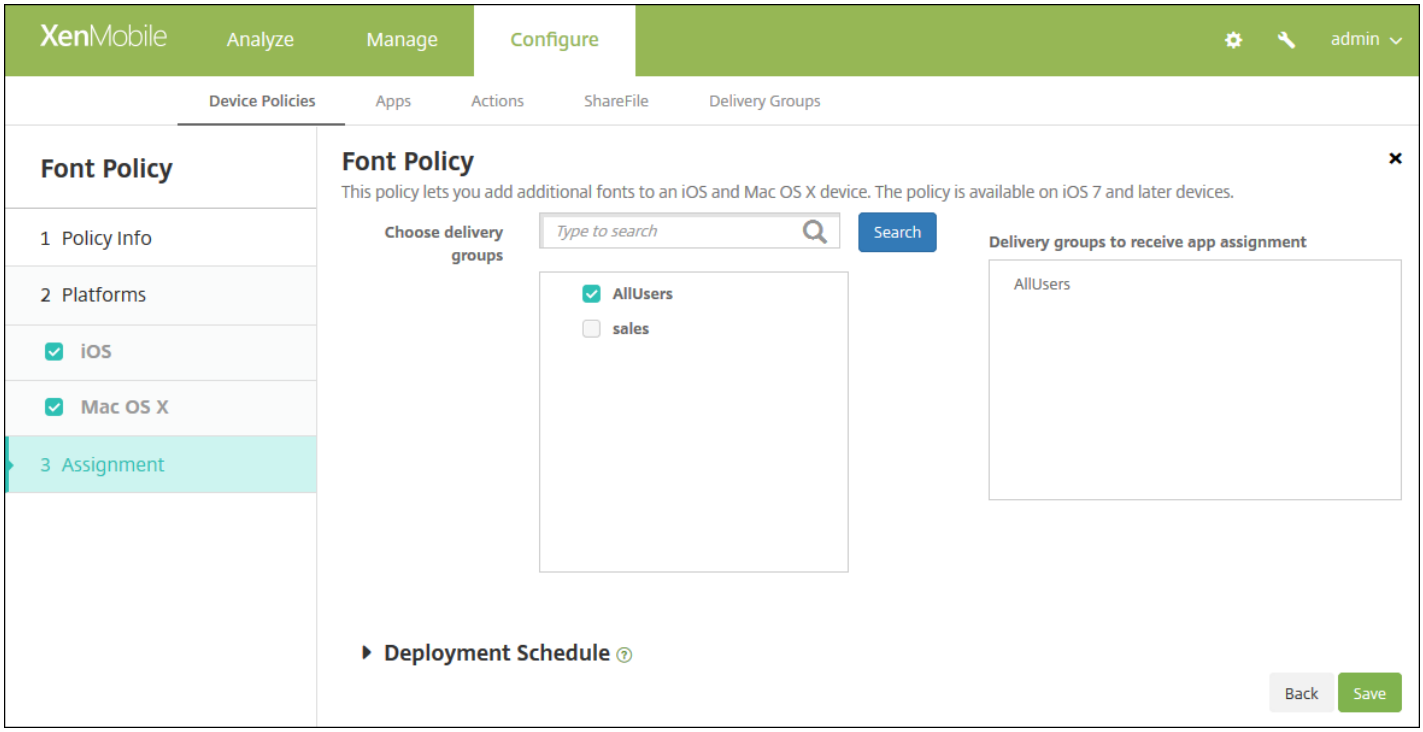


Konfigurieren Sie die folgenden Einstellungen:

- **Benutzern angezeigter Name**: Geben Sie den Namen so ein, wie er in der Liste der Schriftarten auf den Geräten angezeigt werden soll.
- **Schriftartendatei**: Wählen Sie die Schriftartdatei aus, die auf den Geräten der Benutzer hinzugefügt werden soll, indem Sie auf **Durchsuchen** klicken und zum Speicherort der Datei navigieren.
- **Richtlinieneinstellungen**
  - Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.
  - Klicken Sie neben **Gültigkeitsbereich für Profil** auf **Benutzer** oder **System**. Der Standardwert ist **Benutzer**. Diese Option ist nur für OS X 10.7 und höher verfügbar.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Schriftartrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Importieren von Richtlinien für iOS- und Mac OS X-Profile

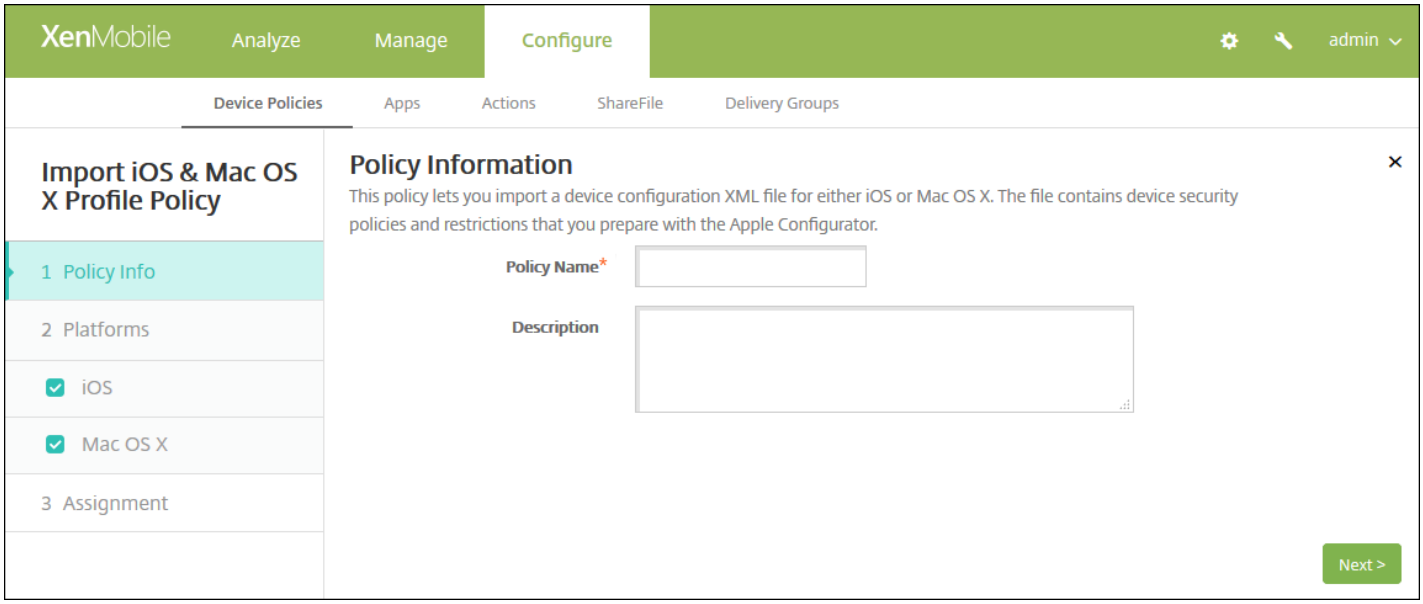
Jul 28, 2016

Sie können XML-Dateien für die Konfiguration von iOS- und OS X-Geräten in XenMobile importieren. Die Datei enthält Gerätesicherheitsrichtlinien und -einschränkungen, die Sie mit Apple Configurator vorbereitet haben. Weitere Informationen über die Verwendung von Apple Configurator zum Erstellen von Konfigurationsdateien finden Sie auf der Apple-Website mit der Hilfe zu Apple Configurator.

1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Gerätericht linien**.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

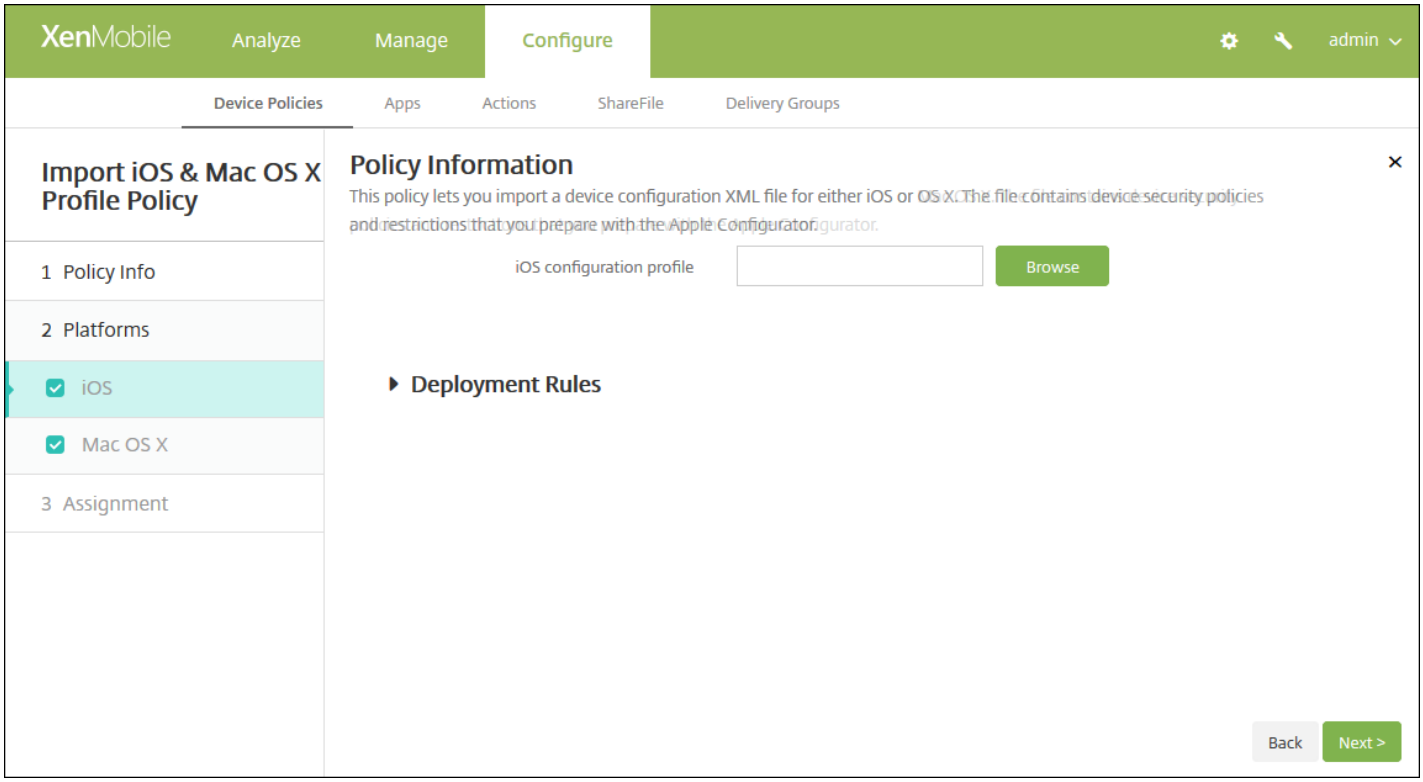
3. Erweitern Sie **Mehr** und klicken Sie unter **Benutzerdefiniert** auf **iOS- und Mac OS X-Profilimport**. Die Seite **iOS- und Mac OS X-Profilimport** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.



6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

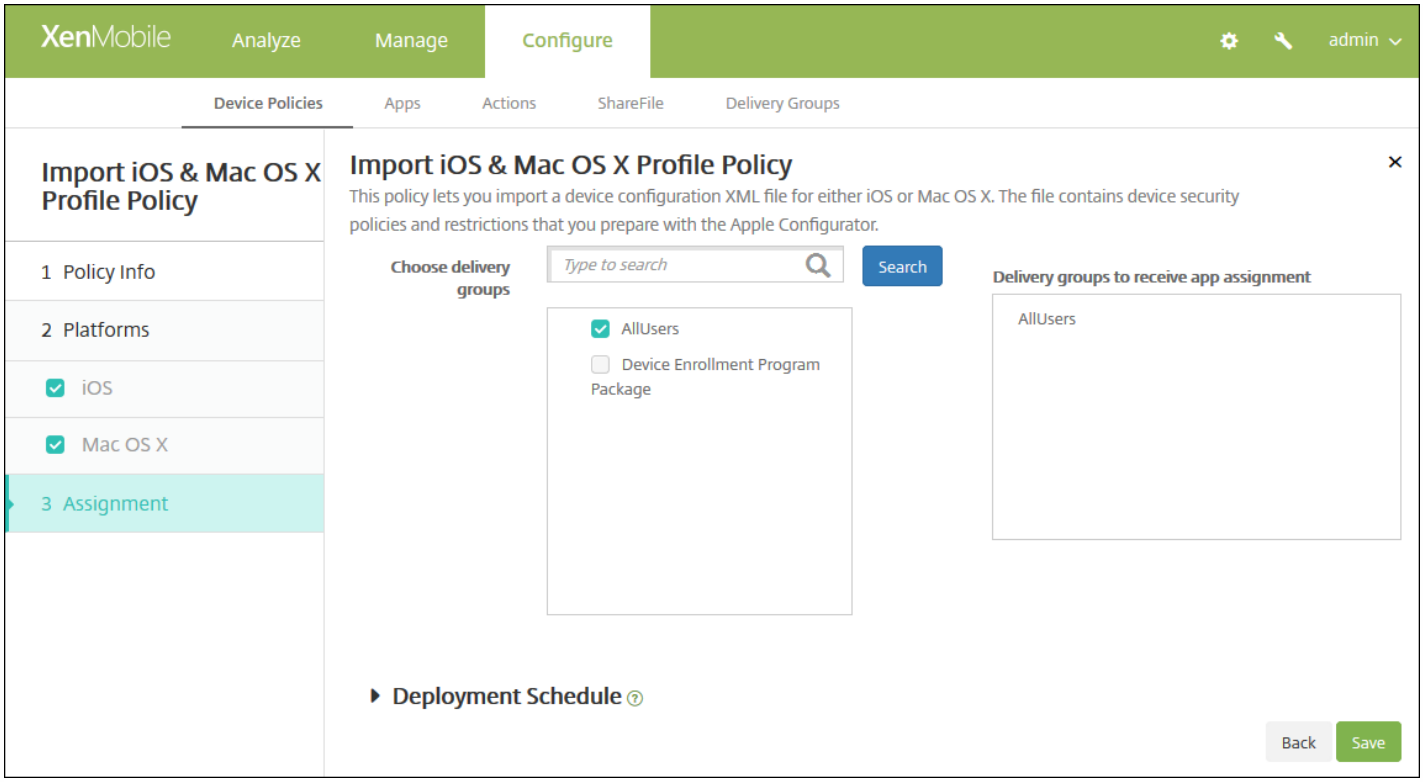
Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der Bereitstellungsregeln für diese Plattform unter Schritt 8. .

7. Konfigurieren Sie für jede ausgewählte Plattform die folgende Einstellung:

- **iOS-Konfigurationsprofil** bzw. **OS X-Konfigurationsprofil**: Klicken Sie auf **Durchsuchen**, navigieren Sie zum Speicherort der Datei und wählen Sie diese aus.

8. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Kioskgeräterichtlinie

Jul 28, 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.

Aktivieren des Kioskmodus für Samsung SAFE-Geräte

1. Aktivieren Sie gemäß den Anweisungen unter Samsung MDM-Richtlinien für Geräte den Samsung SAFE-API-Schlüssel auf dem mobilen Gerät. Dadurch können Sie Richtlinien für Samsung SAFE-Geräte aktivieren.

2. Aktivieren Sie die Richtlinie "Verbindungszeitplan" für Android-Geräte gemäß den Anweisungen unter Verbindungszeitplanrichtlinien für Geräte. Dadurch können Android-Geräte eine Verbindung mit XenMobile herstellen.

3. Fügen wie nachfolgend beschrieben eine Kioskrichtlinie hinzu.

4. Weisen Sie die drei Gerätерichtlinien den entsprechenden Bereitstellungsgruppen zu. Überlegen Sie, ob Sie diesen Bereitstellungsgruppen weitere Richtlinien, z. B. eine App-Bestandsrichtlinie, hinzufügen möchten.

Wenn Sie später den Kioskmodus für Geräte deaktivieren möchten, erstellen Sie eine neue Kioskrichtlinie und legen Sie für **Kioskmodus** die Einstellung **Deaktivieren** fest. Entfernen Sie die Kioskrichtlinie, über die der Kioskmodus aktiviert wird, von den betreffenden Bereitstellungsgruppen und fügen Sie die Richtlinie, über die der Kioskmodus deaktiviert wird, hinzu.

Hinzufügen einer VPN-Richtlinie für Geräte

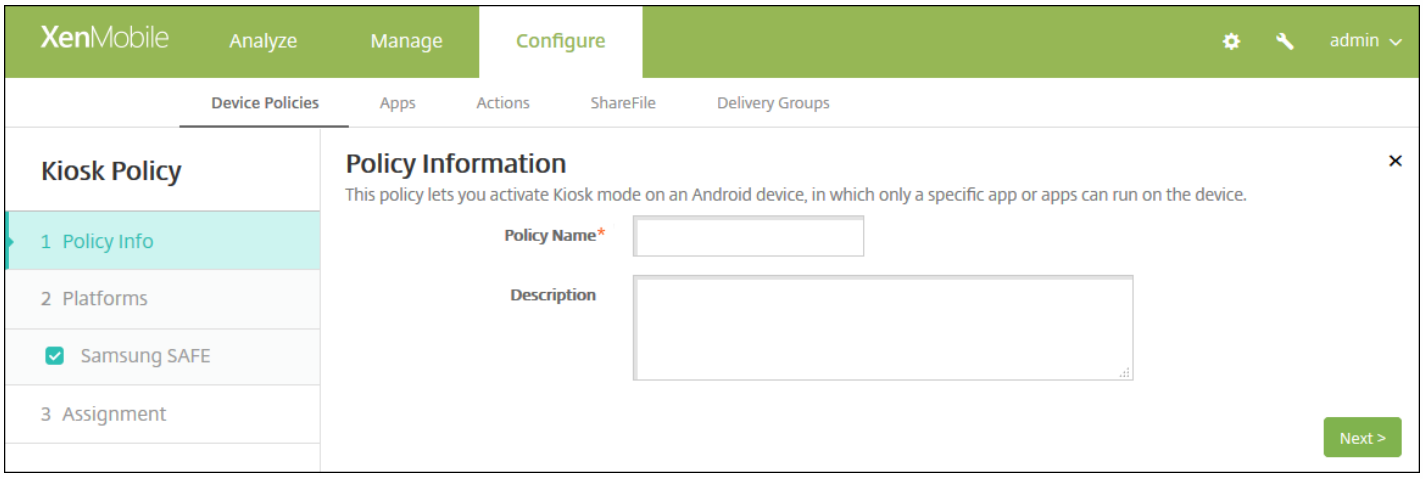
Hinweis:

- 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 **Konfigurieren > Gerätерichtlinien**. Die Seite **Gerätерichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

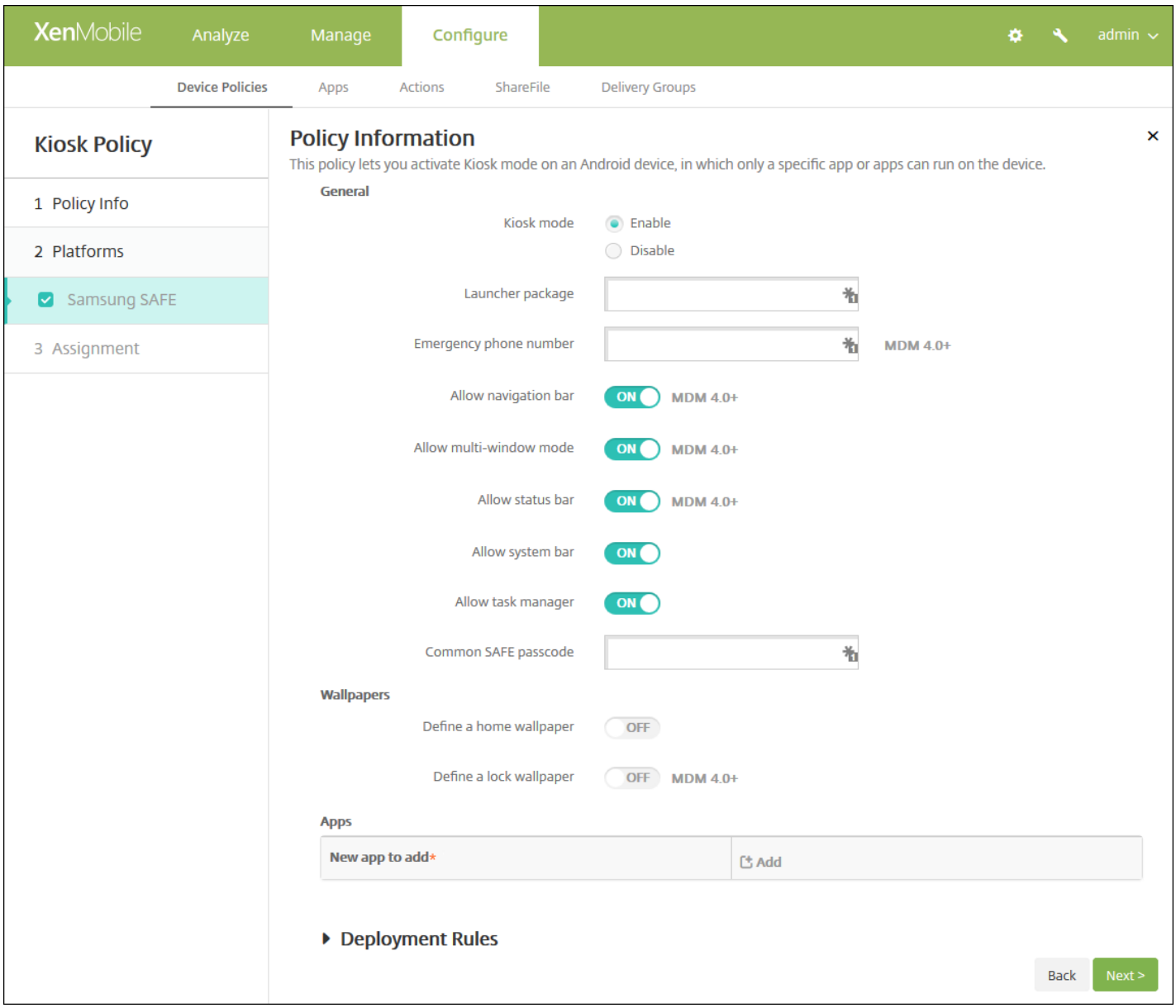
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **Kiosk**. Die Seite **Kiosk** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite für die Plattform **Samsung SAFE** wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:

- **Kioskmodus**: Klicken Sie auf **Aktivieren** oder **Deaktivieren**. Der Standardwert ist **Aktivieren**. Wenn Sie auf **Deaktivieren** klicken, werden die nachfolgend aufgeführten Optionen ausgeblendet.
- **Startprogrammpaket**: Citrix empfiehlt, dieses Feld leer zu lassen, es sei denn, Sie haben ein internes Startprogramm entwickelt, mit dem Benutzer Kiosk-Apps öffnen können. Bei Verwendung eines internen Startprogramms geben Sie den vollständigen Namen des Startprogramm-Anwendungspakets ein.

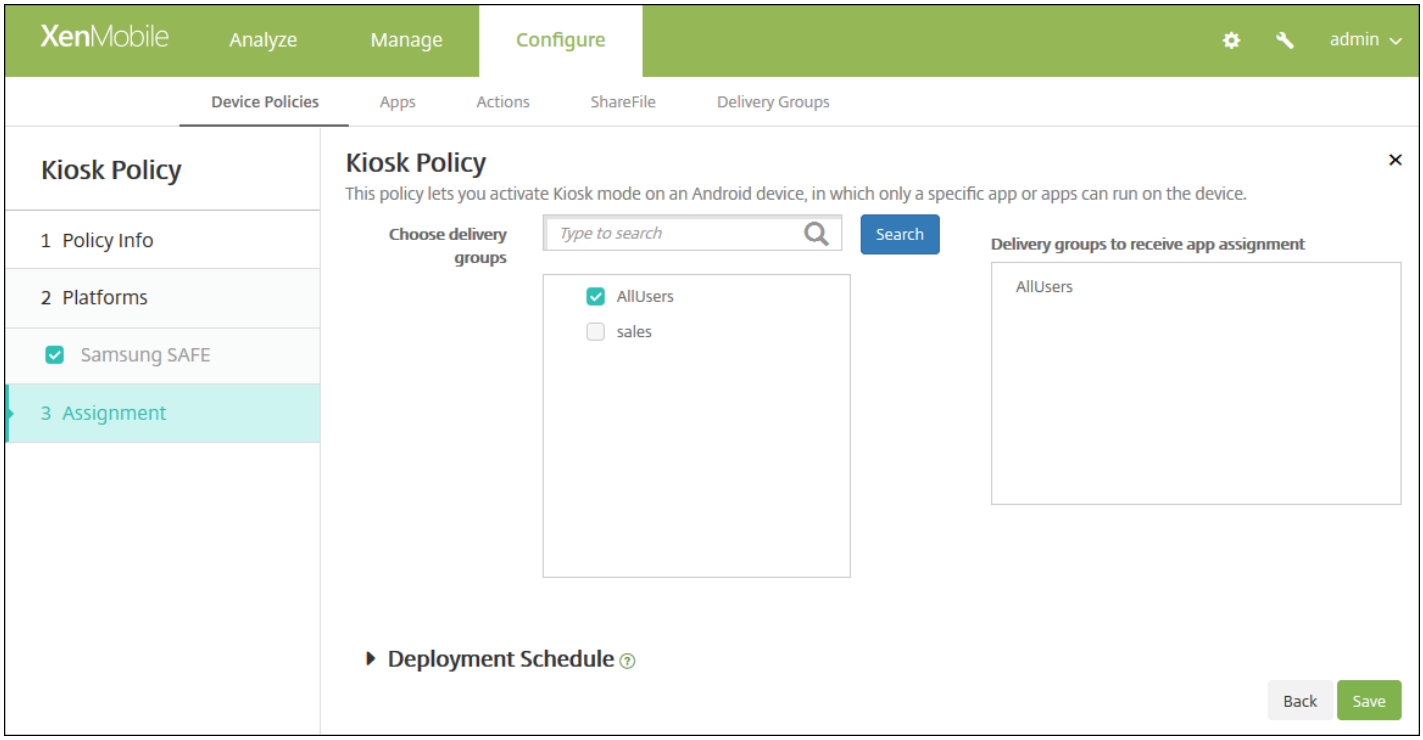
- **Notrufnummer**: Geben Sie optional eine Telefonnummer ein. Über diese Nummer kann der etwaige Finder eines verlorenen Geräts sich an Ihr Unternehmen wenden. Gilt nur für MDM 4.0 und höher.
- **Navigationsleiste zulassen**: Wählen Sie aus, ob Benutzer im Kioskmodus die Navigationsleiste anzeigen und verwenden können sollen. Gilt nur für MDM 4.0 und höher. Die Standardeinstellung ist **EIN**.
- **Mehrfenstermodus zulassen**: Wählen Sie aus, ob Benutzer im Kioskmodus mehrere Fenster verwenden können sollen. Gilt nur für MDM 4.0 und höher. Die Standardeinstellung ist **EIN**.
- **Statusleiste zulassen**: Wählen Sie aus, ob Benutzer im Kioskmodus die Statusleiste anzeigen können sollen. Gilt nur für MDM 4.0 und höher. Die Standardeinstellung ist **EIN**.
- **Systemleiste zulassen**: Wählen Sie aus, ob Benutzer im Kioskmodus die Systemleiste anzeigen können sollen. Die Standardeinstellung ist **EIN**.
- **Task-Manager zulassen**: Wählen Sie aus, ob Benutzer im Kioskmodus den Task-Manager anzeigen und verwenden können sollen. Die Standardeinstellung ist **EIN**.
- **Allgemeiner SAFE-Passcode**: Wenn Sie eine allgemeine Passcoderichtlinie für alle Samsung SAFE Geräte festgelegt haben, geben Sie den optionalen Passcode in dieses Feld ein.
- **Hintergrundbilder**
  - **Hintergrund für Homepage definieren**: Wählen Sie aus, ob für den Homebildschirm im Kioskmodus ein benutzerdefiniertes Bild verwendet werden soll. Der Standardwert ist **AUS**.
    - **Bild für Homepage**: Wenn Sie **Hintergrund für Homepage definieren** aktivieren, klicken Sie auf **Durchsuchen**, navigieren Sie zu der Datei mit dem Bild für die Homepage und wählen Sie diese aus.
  - **Hintergrund für Sperrbildschirm definieren**: Wählen Sie aus, ob für den Sperrbildschirm im Kioskmodus ein benutzerdefiniertes Bild verwendet werden soll. Der Standardwert ist **AUS**. Gilt nur für MDM 4.0 und höher.
    - **Bild für Sperrbildschirm**: Wenn Sie **Hintergrund für Sperrbildschirm definieren** aktivieren, klicken Sie auf **Durchsuchen**, navigieren Sie zu der Datei mit dem Bild für den Sperrbildschirm und wählen Sie diese aus.
- **Apps**: Klicken Sie für jede App, die Sie dem Kioskmodus hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **Neue App zum Hinzufügen**: Geben Sie den vollständigen Namen der App ein. Beispiel: Bei Eingabe von "com.android.calendar" können Benutzer die Android-Kalender-App verwenden.
  - Klicken Sie auf **Speichern**, um die App hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

    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 **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Kioskrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

LDAP-Geräterichtlinien

Jul 28, 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.

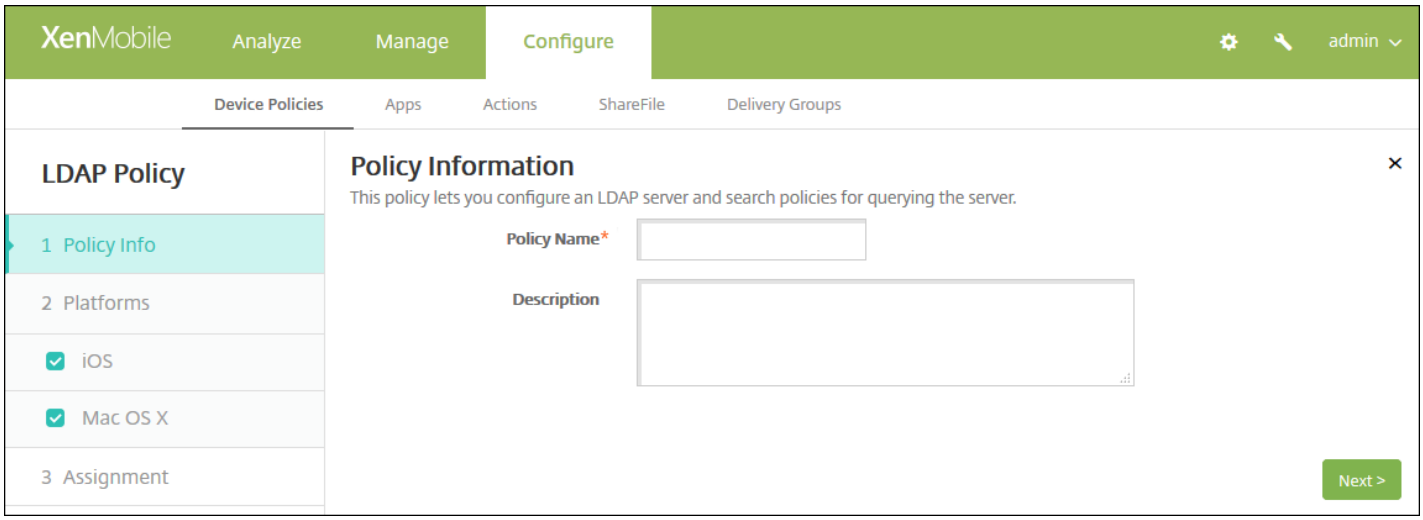
iOS-Einstellungen

Mac OS X-Einstellungen

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

2. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie unter **Endbenutzer** auf **LDAP**. Die Seite **LDAP** wird angezeigt.



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

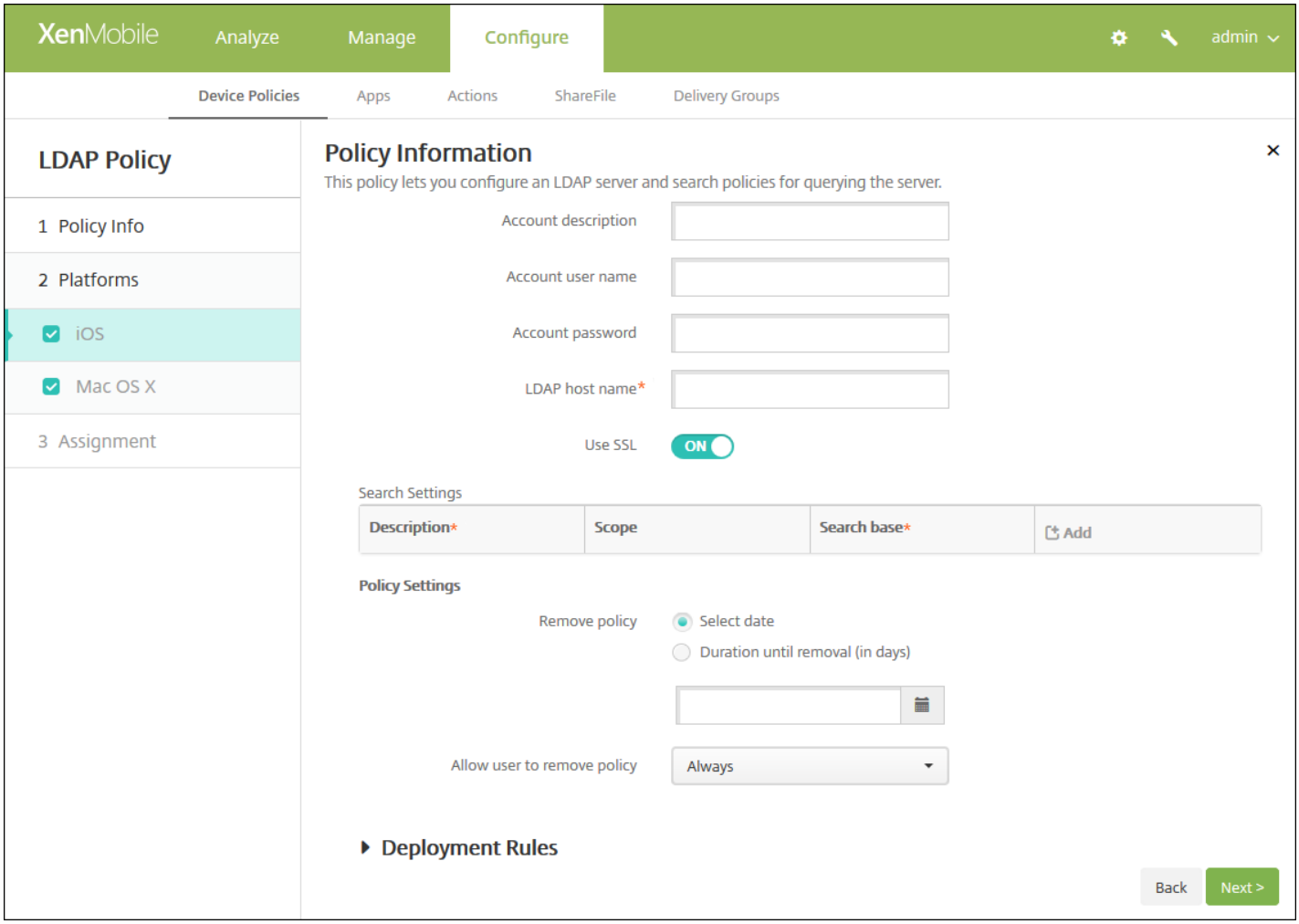
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

Konfigurieren von iOS-Einstellungen



Konfigurieren Sie die folgenden Einstellungen:

- **Kontobeschreibung**: Geben Sie ein optionale Kontobeschreibung ein.
- **Kontobenutzername**: Geben Sie einen optionalen Benutzernamen ein.
- **Kontokennwort**: Geben Sie ein optionales Kennwort ein. Verwenden Sie dieses nur bei verschlüsselten Profilen.
- **LDAP-Hostname**: Geben Sie den Hostnamen des LDAP-Servers ein. Diese Angabe ist erforderlich.
- **SSL verwenden**: Wählen Sie aus, ob für die Verbindung mit dem LDAP-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist **EIN**.
- **Sucheinstellungen**: Fügen Sie die Sucheinstellungen für Abfragen beim LDAP-Server hinzu. Sie können beliebig viele Sucheinstellungen eingeben, es ist jedoch mindestens eine erforderlich, damit das Konto einen Nutzen hat. Klicken Sie auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **Beschreibung:** Geben Sie eine Beschreibung der Sucheinstellung ein. Diese Angabe ist erforderlich.
  - **Geltungsbereich**: Klicken Sie in der Liste auf **Basis**, **Eine Ebene** oder **Unterstruktur**, um die Tiefe der Suche in der LDAP-Struktur anzugeben. Der Standardwert ist "Basis".
    - Mit "Basis" wird der unter "Suchbasis" angegebene Knoten durchsucht.
    - Mit "Eine Ebene" werden der unter "Basis" angegebene Knoten und eine Ebene darunter durchsucht.
    - Mit "Unterstruktur" werden der unter "Basis" angegebene Knoten und alle Ebenen darunter durchsucht.
  - **Suchbasis**: Geben Sie den Pfad des Knotens ein, an dem die Suche beginnen soll. Beispiel: ou=people oder 0=example corp. Diese Angabe ist erforderlich.
  - Klicken Sie auf **Speichern**, um die Sucheinstellung hinzuzufügen, oder auf "Abbrechen", um den Vorgang abzubrechen.

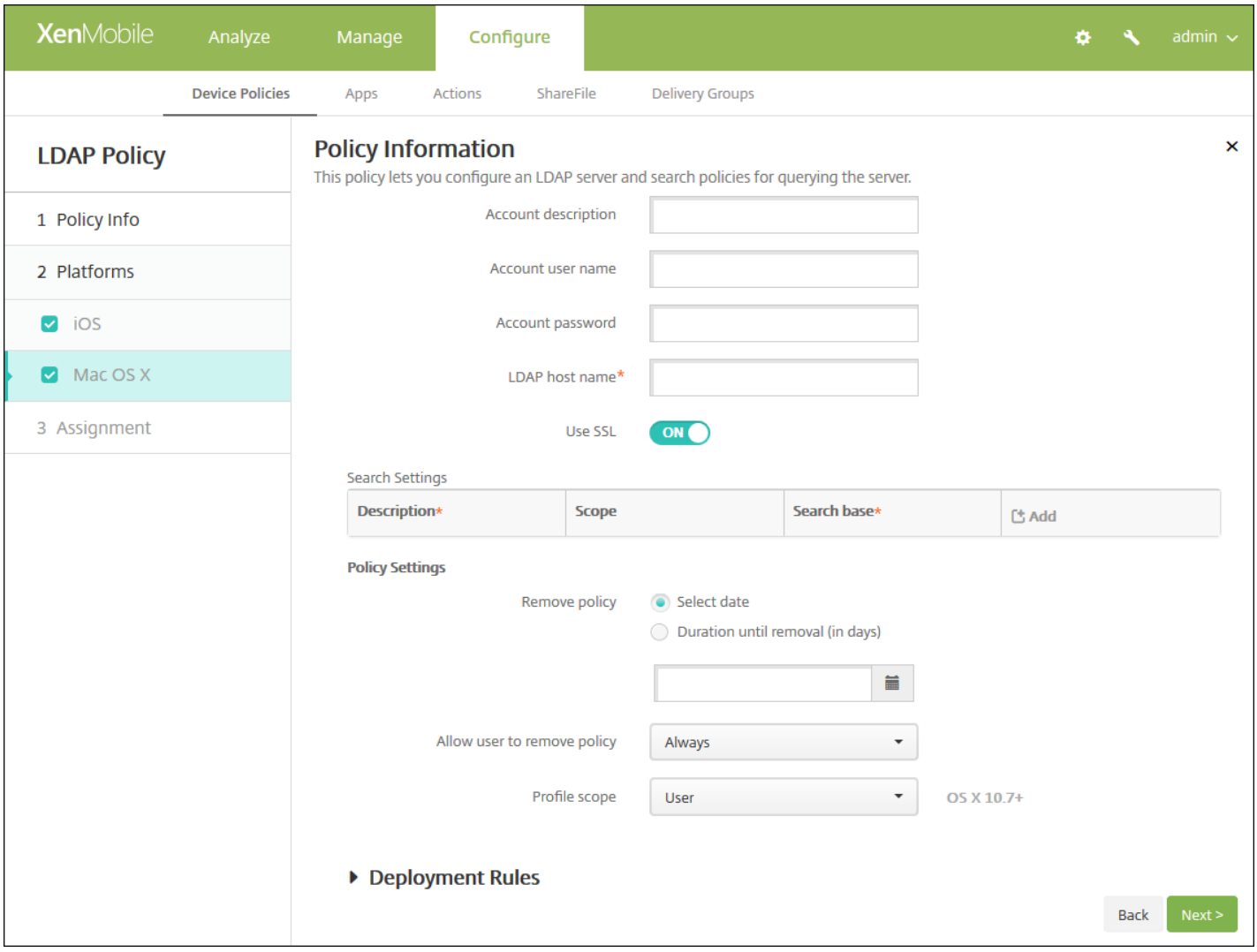
- Wiederholen Sie diese Schritte für jede Sucheinstellung, die Sie hinzufügen möchten.

  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 "Löschen" zum Löschen des Eintrags oder auf "Bearbeiten", 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 "Speichern", um die Änderungen zu speichern oder auf "Abbrechen", um den Vorgang abzubrechen.

- Klicken Sie unter **Richtlinieneinstellungen** für **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen**.
- Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
- Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
- Bei Auswahl von **Kennwort erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

Konfigurieren von Mac OS X-Einstellungen



Konfigurieren Sie die folgenden Einstellungen:

- **Kontobeschreibung**: Geben Sie ein optionale Kontobeschreibung ein.
- **Konto Benutzername**: Geben Sie optional einen Benutzernamen ein.
- **Kontokennwort**: Geben Sie ein optionales Kennwort ein. Verwenden Sie dieses nur bei verschlüsselten Profilen.
- **LDAP-Hostname**: Geben Sie den Hostnamen des LDAP-Servers ein. Diese Angabe ist erforderlich.
- **SSL verwenden**: Wählen Sie aus, ob für die Verbindung mit dem LDAP-Server Secure Socket Layer verwendet werden soll. Die Standardeinstellung ist **EIN**.
- **Sucheinstellungen**: Fügen Sie die Sucheinstellungen für Abfragen beim LDAP-Server hinzu. Sie können beliebig viele Sucheinstellungen eingeben, es ist jedoch mindestens eine erforderlich, damit das Konto einen Nutzen hat. Klicken Sie auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **Beschreibung:** Geben Sie eine Beschreibung der Sucheinstellung ein. Diese Angabe ist erforderlich.
  - **Geltungsbereich**: Klicken Sie in der Liste auf **Basis**, **Eine Ebene** oder **Unterstruktur**, um die Tiefe der Suche in der LDAP-Struktur anzugeben. Der Standardwert ist "Basis".
    - Mit "Basis" wird der unter "Suchbasis" angegebene Knoten durchsucht.
    - Mit "Eine Ebene" werden der unter "Basis" angegebene Knoten und eine Ebene darunter durchsucht.
    - Mit "Unterstruktur" werden der unter "Basis" angegebene Knoten und alle Ebenen darunter durchsucht.
  - **Suchbasis**: Geben Sie den Pfad des Knotens ein, an dem die Suche beginnen soll. Beispiel: ou=people oder 0=example corp. Diese Angabe ist erforderlich.
  - Klicken Sie auf **Speichern**, um die Sucheinstellung hinzuzufügen, oder auf "Abbrechen", um den Vorgang abzubrechen.
  - Wiederholen Sie diese Schritte für jede Sucheinstellung, die Sie hinzufügen möchten.

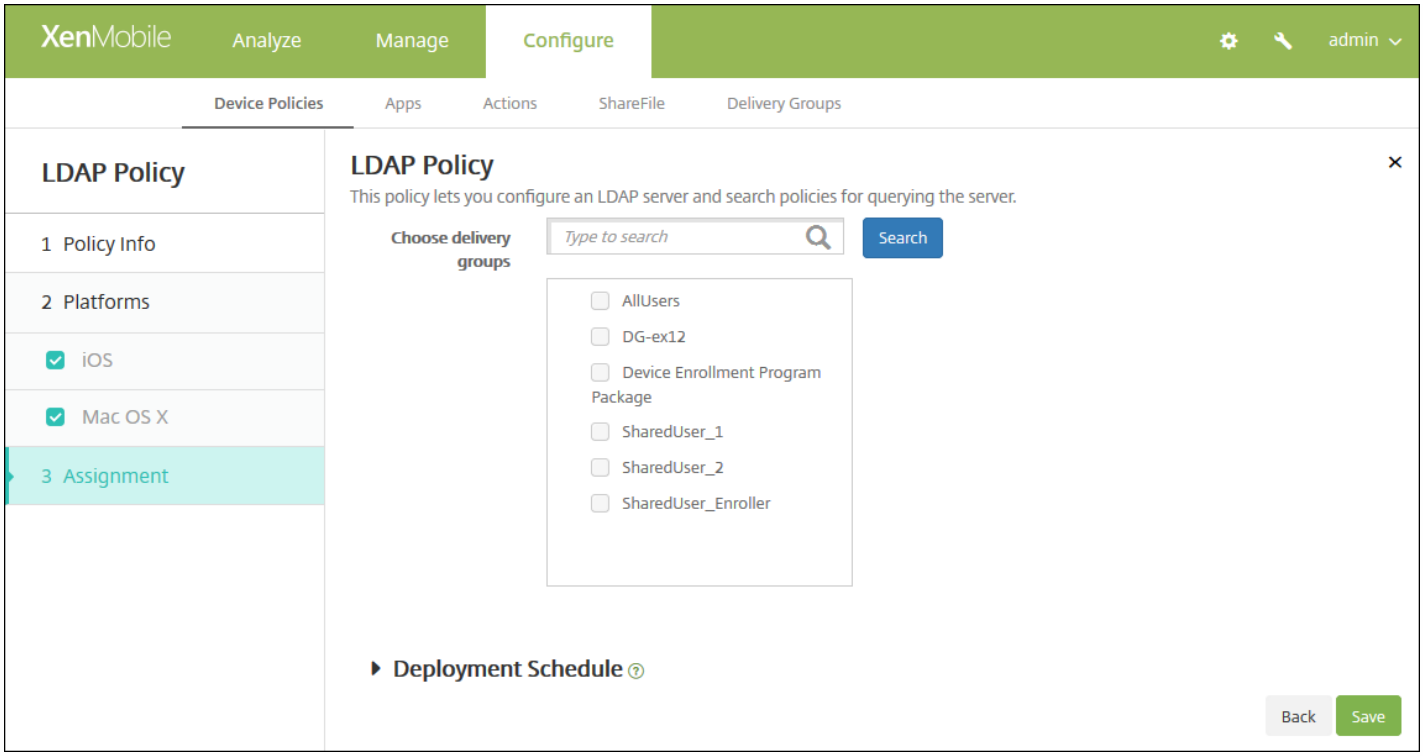
    Hinweis: Zum Löschen einer vorhandenen Sucheinstellung zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf "Löschen" zum Löschen des Eintrags oder auf "Bearbeiten", um ihn beizubehalten.

    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 "Speichern", um die Änderungen zu speichern oder auf "Abbrechen", um den Vorgang abzubrechen.

- Klicken Sie unter **Richtlinieneinstellungen** neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
- Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
- Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
- Bei Auswahl von **Kennwort erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.
- Klicken Sie für **Gültigkeitsbereich für Profil** auf **Benutzer** oder **System**. Der Standardwert ist **Benutzer**. Diese Option ist nur für OS X 10.7 und höher verfügbar.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die LDAP-Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Standortrichtlinien für Geräte

Jul 28, 2016

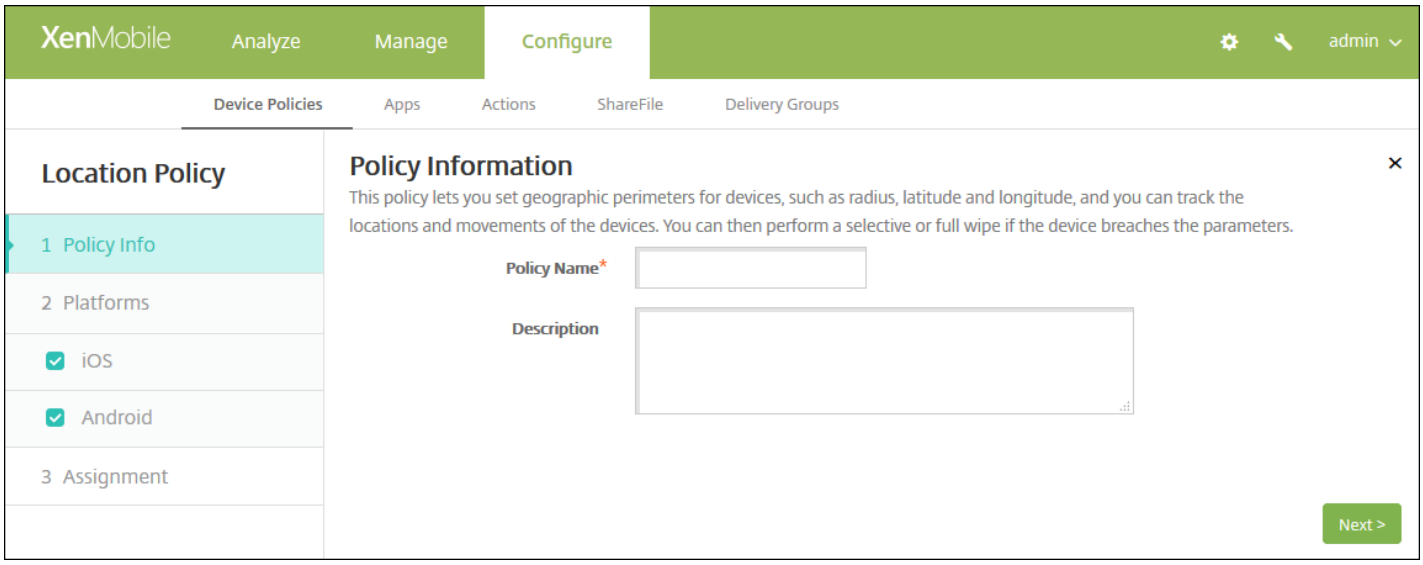
Mit einer Standortrichtlinie legen Sie in XenMobile geografische Grenzen fest und verfolgen den Standort und die Bewegung der Geräte der Benutzer. Wenn ein Benutzer den festgelegten Bereich (*Geofence*) verlässt, kann XenMobile eine selektive oder vollständige Löschung der Daten auf seinem Gerät durchführen. 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 **Konfigurieren > Geräterichtlinien**. Die Seite **Geräterichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Klicken Sie auf **Standort**. Die Seite mit den Richtlinieninformationen für die Richtlinie **Standort/Ortung** wird angezeigt.



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

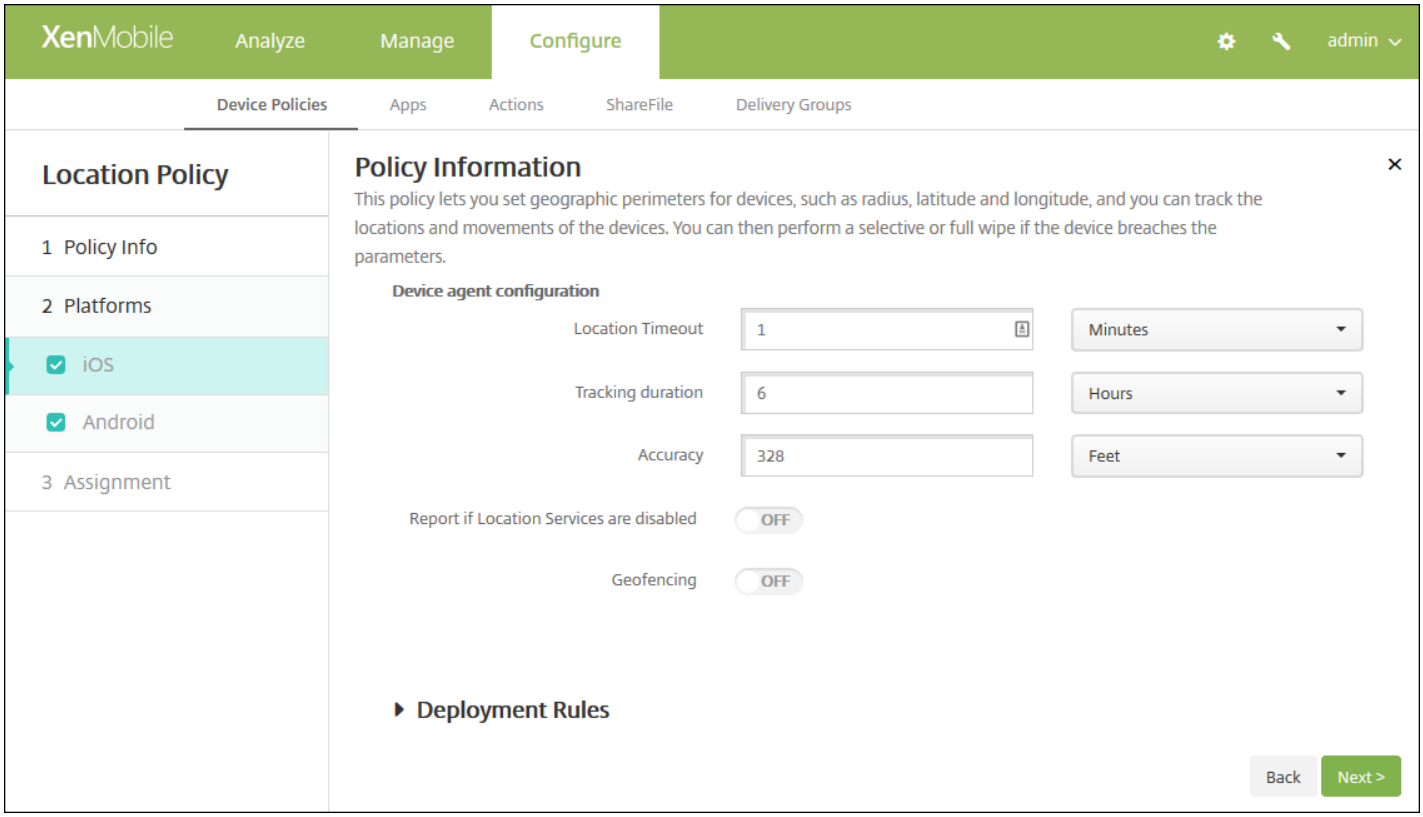
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

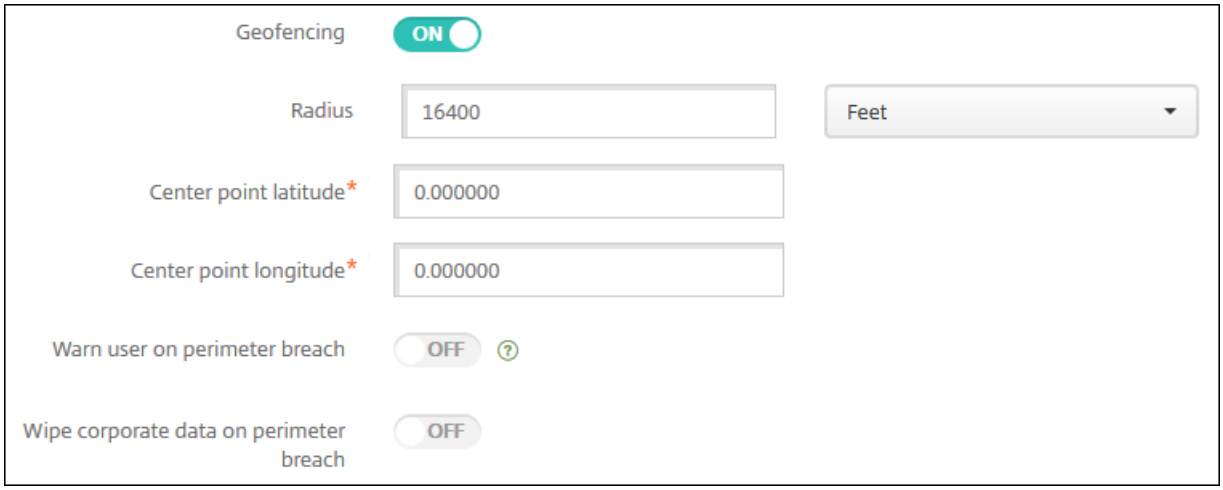
Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der Bereitstellungsregeln für diese Plattform unter Schritt 7.

Konfigurieren von iOS-Einstellungen



Konfigurieren Sie folgende Einstellungen:

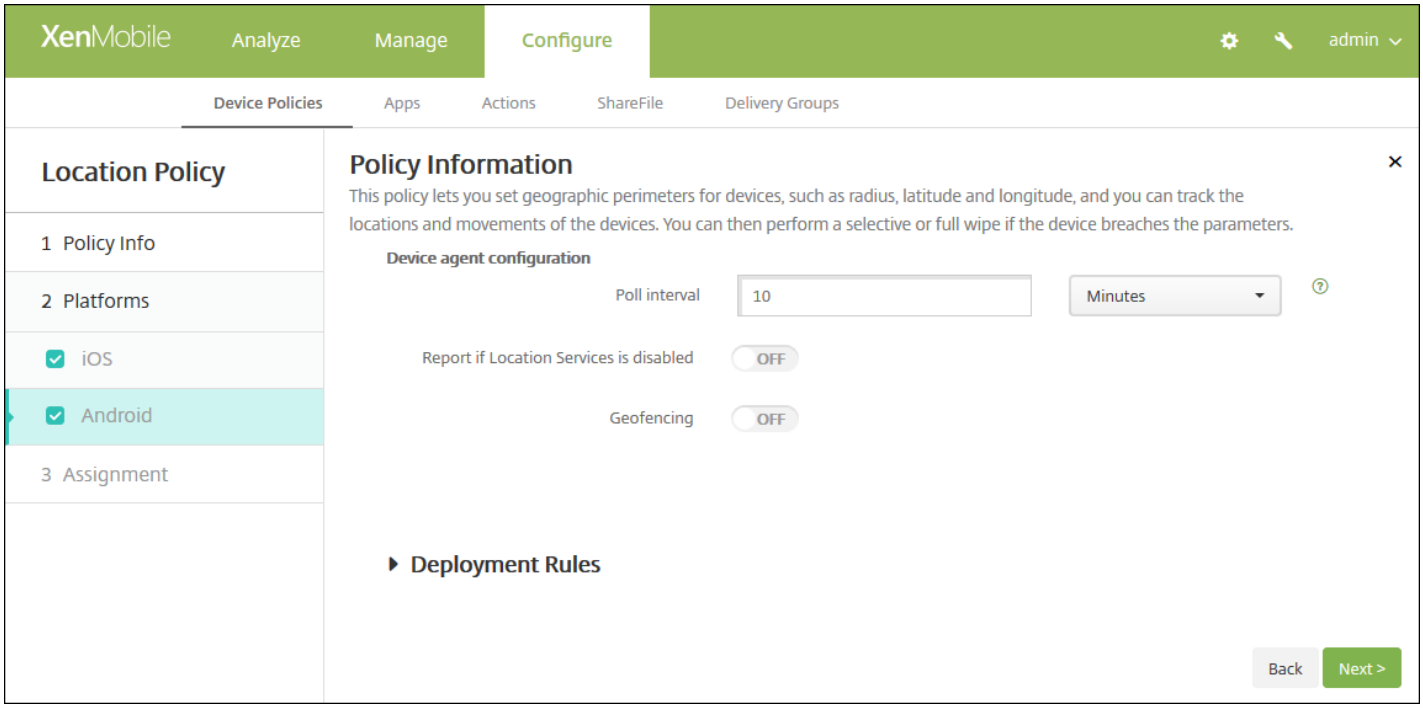
- **Standorttimeout**: Geben Sie eine Ziffer ein und klicken Sie in der Liste auf **Sekunden** oder **Minuten**, um festzulegen, wie häufig XenMobile den Gerätestandort abrufen soll. Gültige Werte sind 60-900 Sekunden oder 1-15 Minuten. Der Standardwert ist 1 Minute.
- **Trackingdauer**: Geben Sie eine Ziffer ein und klicken Sie in der Liste auf **Stunden** oder **Minuten**, um festzulegen, wie lange XenMobile das Gerät verfolgen soll. Gültige Werte sind 1-6 Stunden oder 10-360 Minuten. Der Standardwert ist 6 Stunden.
- **Genauigkeit**: Geben Sie eine Ziffer ein und klicken Sie in der Liste auf **Meter**, **Fuß** 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.
- **Deaktivierte Ortungsdienste melden**: Wählen Sie, ob das Gerät einen Bericht an XenMobile senden soll, wenn GPS deaktiviert ist. Der Standardwert ist **AUS**.
- **Geofencing**



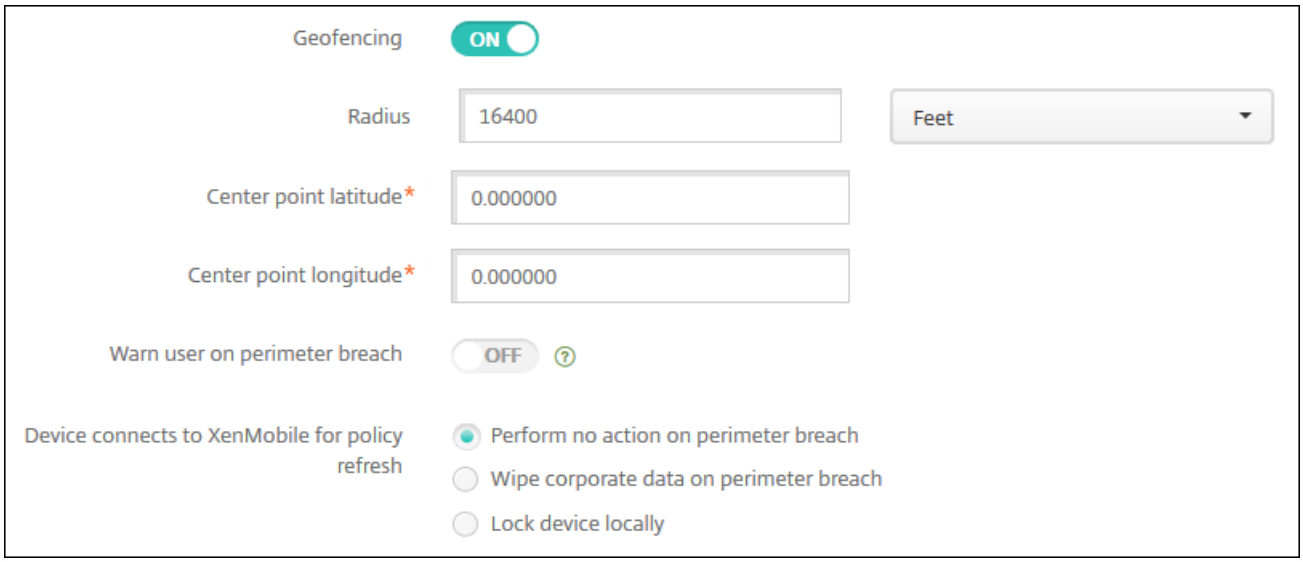
Bei Auswahl von "Geofencing" konfigurieren Sie die folgenden Einstellungen:

- **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
  - 50-50000 Meter
  - 54-54680 Yard
  - 1-31 Meilen
- **Breitengrad von Mittelpunkt**: Geben Sie einen Wert (z. B. 37.787454) zum Festlegen des Breitengrads des Geofence-Mittelpunkts ein.
- **Längengrad von Mittelpunkt**: Geben Sie einen Wert (z. B. 122.402952) zum Festlegen des Längengrads des Geofence-Mittelpunkts ein.
- **Bei Umkreisverletzung Benutzer warnen**: Wählen Sie aus, ob eine Warnmeldung angezeigt werden soll, wenn Benutzer den vorgegebenen Bereich verlassen. Der Standardwert ist **AUS**. Zum Anzeigen der Warnmeldung ist keine Verbindung mit XenMobile erforderlich.
- **Bei Umkreisverletzung Unternehmensdaten löschen**: Wählen Sie aus, ob auf den Geräten bei Verlassen des Bereichs eine Datenlöschung erfolgen soll. Der Standardwert ist **AUS**. Wenn Sie diese Option aktivieren, wird das Feld **Verzögerung beim lokalen Löschen** angezeigt.
  - Geben Sie eine Ziffer ein und klicken Sie in der Liste auf **Sekunden** oder **Minuten**, 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.

Konfigurieren von Android-Einstellungen



- **Abrufintervall**: Geben Sie eine Ziffer ein und klicken Sie in der Liste auf **Minuten**, **Stunden** oder **Tage**, 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. Wenn dieser Wert auf weniger als 10 Minuten festgelegt wird, kann dies die Akkulaufzeit des Geräts nachteilig beeinflussen.
- **Deaktivierte Ortungsdienste melden**: Wählen Sie, ob das Gerät einen Bericht an XenMobile senden soll, wenn GPS deaktiviert ist. Der Standardwert ist **AUS**.
- **Geofencing**



Bei Auswahl von "Geofencing" konfigurieren Sie die folgenden Einstellungen:

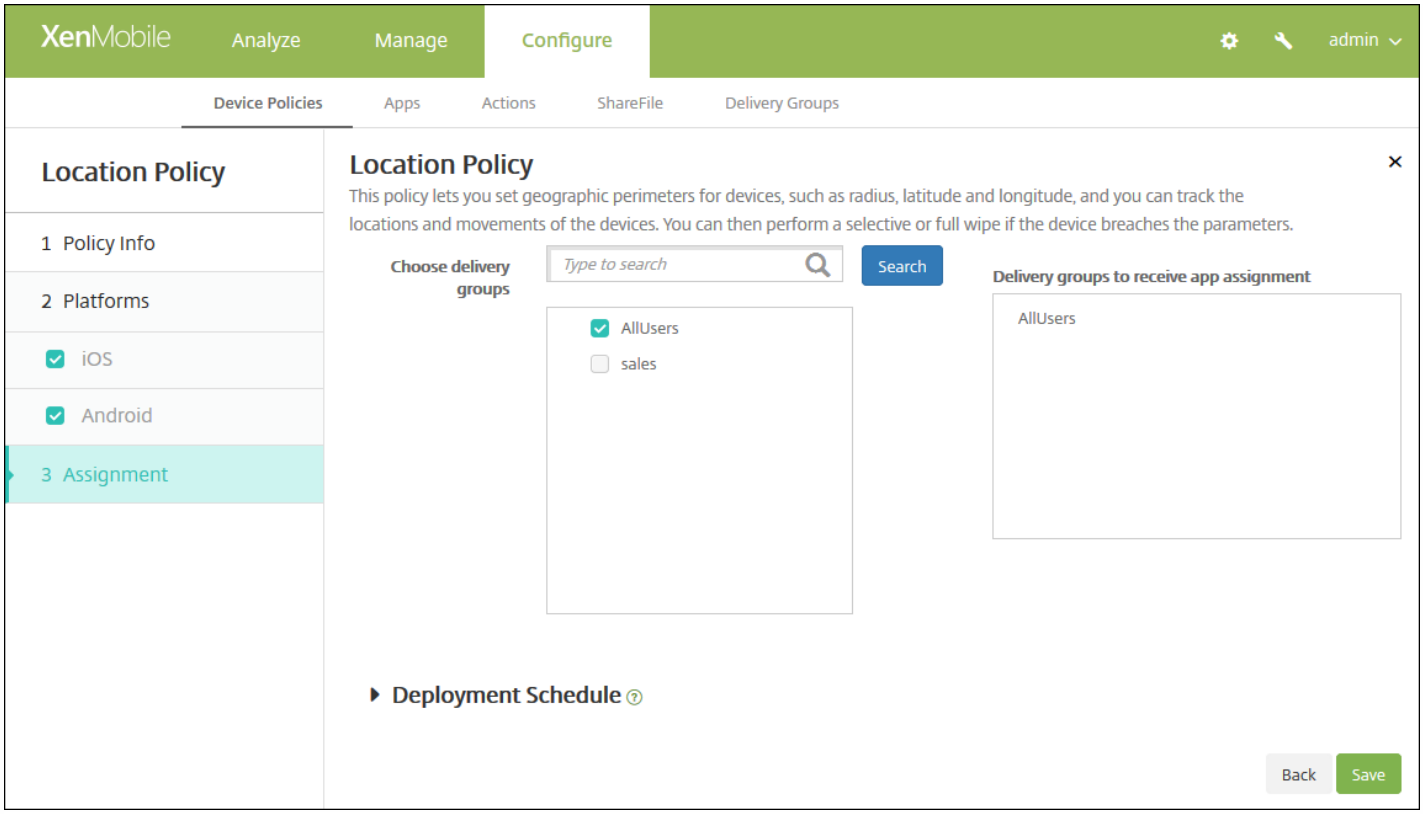
- **Radius**: Geben Sie zur Messung des Radius eine Ziffer ein und klicken Sie in Liste auf die Einheit. Der Standardwert ist 16.400 Fuß. Gültige Werte für den Radius:

- 164-164000 Fuß
- 1-50 Kilometer
- 50-50000 Meter
- 54-54680 Yard
- 1-31 Meilen

- **Breitengrad von Mittelpunkt**: Geben Sie einen Wert (z. B. 37.787454) zum Festlegen des Breitengrads des Geofence-Mittelpunkts ein.
- **Längengrad von Mittelpunkt**: Geben Sie einen Wert (z. B. 122.402952) zum Festlegen des Längengrads des Geofence-Mittelpunkts ein.
- **Bei Umkreisverletzung Benutzer warnen**: Wählen Sie aus, ob eine Warnmeldung angezeigt werden soll, wenn Benutzer den vorgegebenen Bereich verlassen. Der Standardwert ist **AUS**. Zum Anzeigen der Warnmeldung ist keine Verbindung mit XenMobile erforderlich.
- **Gerät mit XenMobile zur Richtlinienaktualisierung verbinden**: Wählen Sie eine der folgenden Aktionen aus, die durchgeführt werden soll, wenn Benutzer den Bereich verlassen:
  - **Bei Umkreisverletzung keine Aktion durchführen**: keine Aktion. Dies ist die Standardeinstellung.
  - **Bei Umkreisverletzung Unternehmensdaten löschen**: Unternehmensdaten werden nach einem festgelegten Zeitraum gelöscht. Wenn Sie diese Option aktivieren, wird das Feld **Verzögerung beim lokalen Löschen** angezeigt.
    - Geben Sie eine Ziffer ein und klicken Sie in der Liste auf Sekunden oder Minuten, 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.
  - **Verzögerung beim Sperren**: Sperrt die Geräte nach einem festgelegten Zeitraum. Wenn Sie diese Option aktivieren, wird das Feld **Verzögerung beim Sperren** angezeigt.
    - Geben Sie eine Ziffer ein und klicken Sie in der Liste auf Sekunden oder Minuten, 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. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Standortrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

E-Mail-Geräterichtlinien

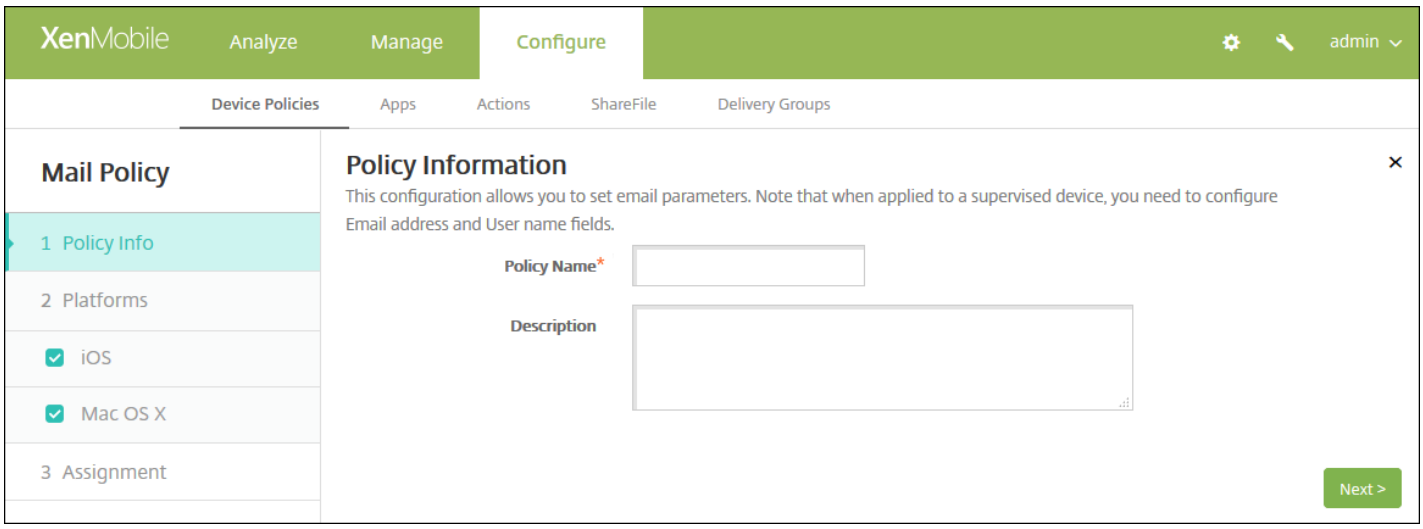
Jul 28, 2016

Sie können in XenMobile eine E-Mail-Richtlinie hinzufügen, um ein E-Mail-Konto auf iOS- oder MAC OS X-Geräten zu konfigurieren.

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

2. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie hinzuzufügen. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

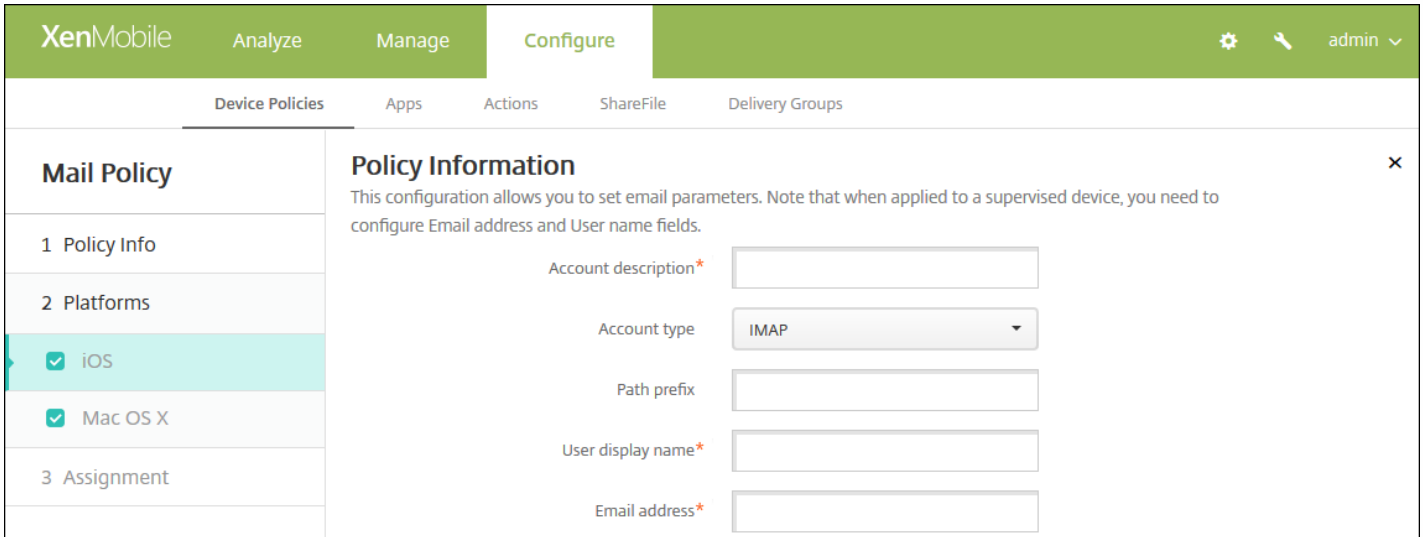
3. Klicken Sie auf **Mehr** und dann unter **Endbenutzer** auf **E-Mail**. Die Seite **E-Mail** wird angezeigt.

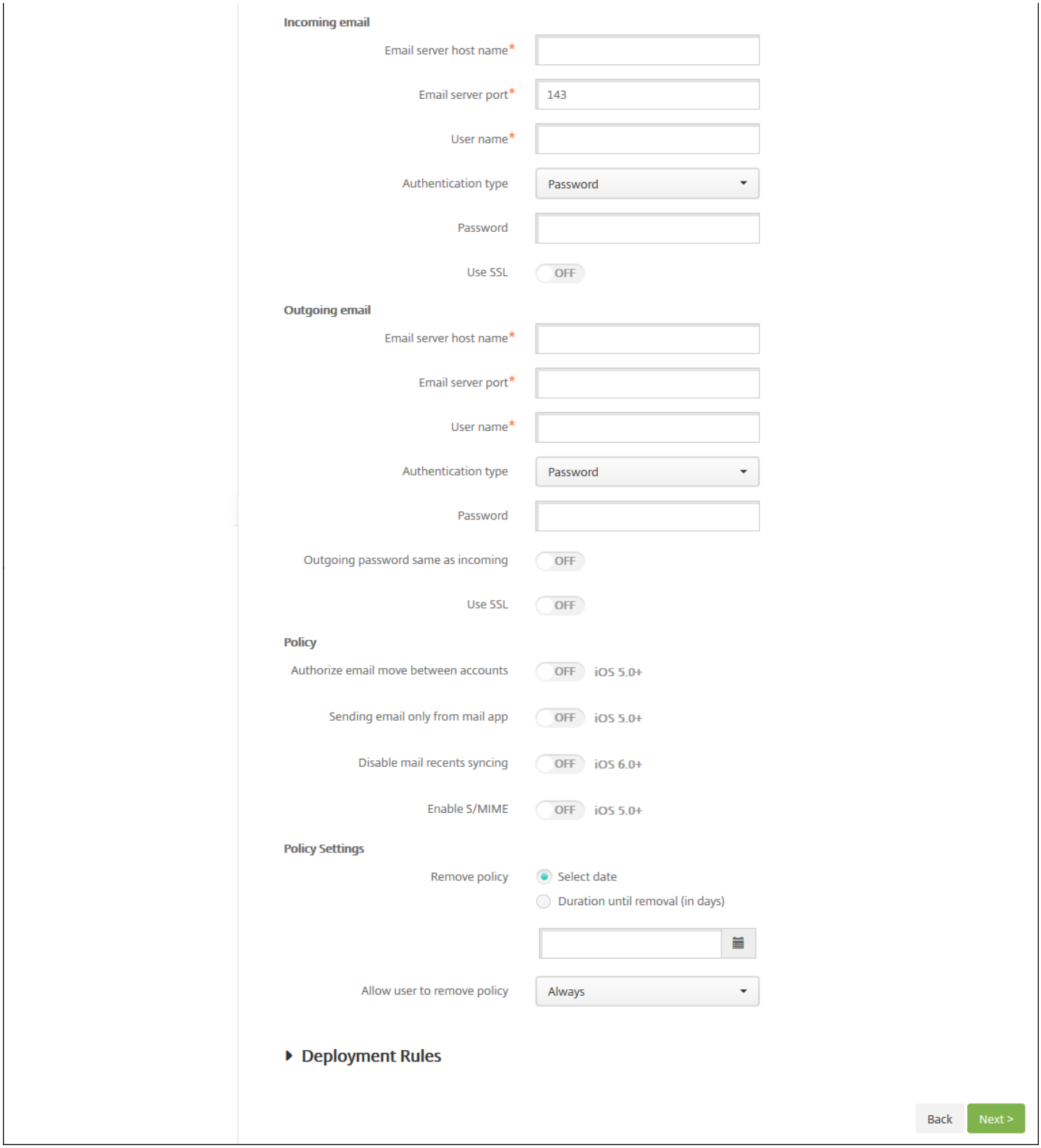


4. Geben Sie im Bereich **Richtlinieninformationen** die folgenden Informationen ein:

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

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.





6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der Bereitstellungsregeln für diese Plattform unter Schritt 8.

7. Konfigurieren Sie für jede ausgewählte Plattform die folgenden Einstellungen:

- **Kontobeschreibung**: Geben Sie eine Kontobeschreibung für die Anzeige in den E-Mail- und Einstellungs-Apps ein. Diese Angabe ist erforderlich.
- **Kontotyp**: Klicken Sie in der Liste auf **IMAP** oder **POP**, um das Protokoll für die Konten auszuwählen. Die Standardeinstellung ist **IMAP**. Wenn Sie **POP** auswählen, wird die im nächsten Schritt erwähnte Option **Pfadpräfix** ausgeblendet.
- **Pfadpräfix**: Geben Sie **INBOX** ein, bzw. das Präfix des IMAP-E-Mail-Kontopfads, sofern dieses nicht **INBOX** ist. Diese Angabe ist erforderlich.
- **Anzeigename für Benutzer**: Geben Sie den vollständigen Benutzernamen für Nachrichten usw. ein. Diese Angabe ist erforderlich.
- **E-Mail-Adresse**: Geben Sie die vollständige E-Mail-Adresse für das Konto ein. Diese Angabe ist erforderlich.
- **Einstellungen für eingehende E-Mail**
  - **Hostname des E-Mail-Servers**: Geben Sie den Hostnamen oder die IP-Adresse des Servers für eingehende E-Mail ein. Diese Angabe ist erforderlich.
  - **Port des E-Mail-Servers**: Geben Sie die Portnummer des Servers für eingehende E-Mail ein. Der Standardwert ist **143**. Diese Angabe ist erforderlich.
  - **Benutzername**: Geben Sie den Benutzernamen für das E-Mail-Konto ein. Dieser Name ist in der Regel identisch mit dem Teil der E-Mail-Adresse des Benutzers bis zum @-Zeichen. Diese Angabe ist erforderlich.
  - **Authentifizierungstyp**: Klicken Sie in der Liste auf den gewünschten Authentifizierungstyp. Der Standardwert ist **Kennwort**. Bei Auswahl von **Ohne** wird das im nächsten Schritt erwähnte Feld **Kennwort** ausgeblendet.
  - **Kennwort**: Geben Sie ein optionales Kennwort für den Server für eingehende E-Mail ein.
  - **SSLverwenden**: Wählen Sie aus, ob der Server für eingehende E-Mail Secure Socket Layer verwenden soll. Der Standardwert ist **AUS**.
- **Einstellungen für ausgehende E-Mail**
  - **Hostname des E-Mail-Servers**: Geben Sie den Hostnamen oder die IP-Adresse des Servers für ausgehende E-Mail ein. Diese Angabe ist erforderlich.
  - **Port des E-Mail-Servers**: Geben Sie die Portnummer des Servers für ausgehende E-Mail ein. Wenn Sie keinen Port angeben, wird der Standardport des angegebenen Protokolls verwendet.
  - **Benutzername**: Geben Sie den Benutzernamen für das E-Mail-Konto ein. Der Name ist in der Regel identisch mit dem Teil der E-Mail-Adresse des Benutzers bis zum @-Zeichen. Diese Angabe ist erforderlich.
  - **Authentifizierungstyp**: Klicken Sie in der Liste auf den gewünschten Authentifizierungstyp. Der Standardwert ist **Kennwort**. Bei Auswahl von **Ohne** wird das im nächsten Schritt erwähnte Feld **Kennwort** ausgeblendet.
  - **Kennwort**: Geben Sie ein optionales Kennwort für den Server für eingehende E-Mail ein.
  - **Ausgehendes Kennwort gleich eingehendem**: Wählen Sie aus, ob für aus- und eingehende E-Mail dasselbe Kennwort verwendet wird. Der Standardwert ist AUS, was bedeutet, dass die Kennwörter unterschiedlich sind. Bei Auswahl von **EIN** wird das oben beschriebene Feld **Kennwort** ausgeblendet.
  - **SSL verwenden**: Wählen Sie aus, ob der Server für ausgehende E-Mail Secure Socket Layer verwenden soll. Der Standardwert ist **AUS**.
- **Richtlinie**
  - **Hinweis**: Diese Optionen gelten nur für iOS 5.0 und höher, bei Mac OS X gibt es keine Einschränkungen.
  - **Verschieben von E-Mails zwischen Konten autorisieren**: Geben Sie an, ob Benutzer E-Mail von diesem Konto in ein anderes Konto verschieben und von einem anderen Konto aus weiterleiten dürfen und ob sie von einem anderen Konto aus antworten dürfen. Der Standardwert ist **AUS**.
  - **E-Mail nur von Mailanwendung senden**: Wählen Sie aus, ob Benutzer E-Mailnur mit der iOS-E-Mail-App senden dürfen.
  - **Synchronisierung aktueller E-Mails deaktivieren**: Wählen Sie aus, ob eine Synchronisierung zuletzt verwendeter

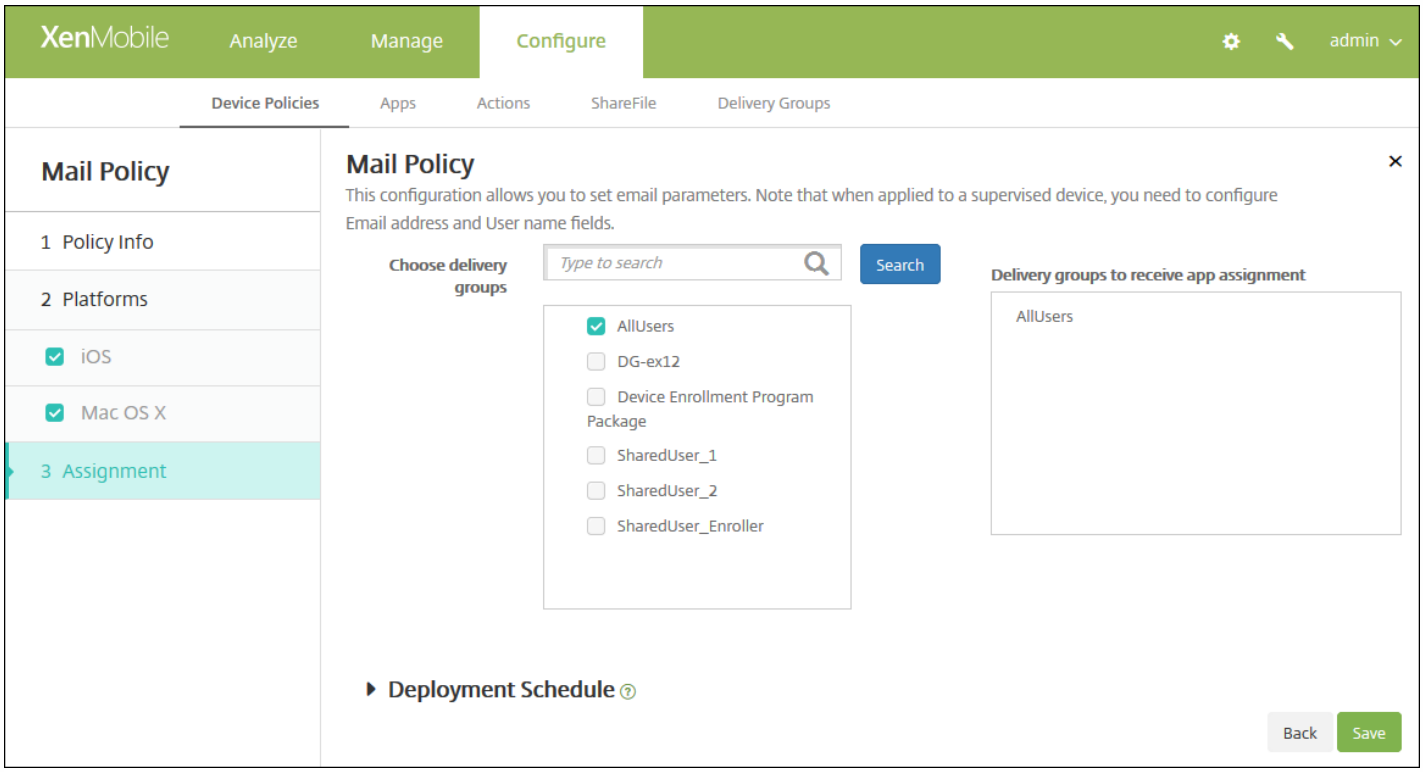
Adressen durch die Benutzer verhindert werden soll. Der Standardwert ist **AUS**. Diese Option gilt nur für iOS 6.0 und höher.

- **S/MIME aktivieren**: Geben Sie an, ob das Konto S/MIME-Authentifizierung und -Verschlüsselung unterstützt. Der Standardwert ist **AUS**. Bei Auswahl von EIN werden folgende Felder eingeblendet.
- **Anmeldeinformationen für Signieridentität**: Wählen Sie in der Liste die Anmeldeinformationen für die Signatur aus.
- **Anmeldeinformationen für Verschlüsselungsidentität**: Wählen Sie in der Liste die Anmeldeinformationen für die Verschlüsselung aus.

- **Richtlinieneinstellungen**
  - Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Kennwort erforderlich** oder **Nie**.
  - Bei Auswahl von **Kennwort erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.
  - Klicken Sie in der Liste neben **Gültigkeitsbereich für Profil** auf **Benutzer** oder **System**. Der Standardwert ist **Benutzer**. Diese Option ist nur für Mac OS X 10.7 und höher verfügbar.

8. Konfigurieren der Bereitstellungsregeln

9. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die E-Mail-Richtlinie wird angezeigt.



10. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

11. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.

- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

12. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Geräterichtlinie für verwaltete Domänen

Jul 28, 2016

Sie können verwaltete Domänen für E-Mail und den Safari-Browser definieren. Mit verwalteten Domänen können Sie zum Schutz von Unternehmensdaten steuern, welche Apps Dokumente, die mit Safari heruntergeladen wurden, öffnen können. Durch Angabe von URLs oder Unterdomänen geben Sie vor, wie Benutzer Dokumente, Anlagen und über Browser heruntergeladene Objekte öffnen können. Diese Richtlinie wird nur für betreute Geräte mit iOS 8 und höher unterstützt. Anweisungen zum Versetzen von iOS-Geräten in den betreuten Modus finden Sie unter Versetzen eines iOS-Geräts mit dem Apple Configurator in den betreuten Modus.

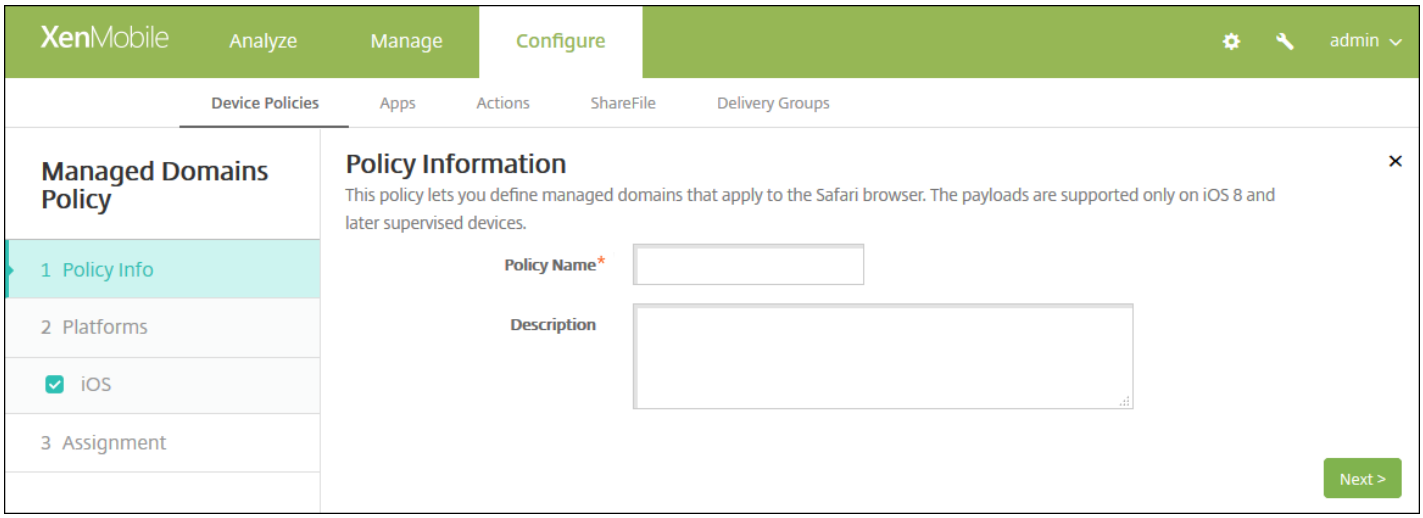
Wenn ein Benutzer eine E-Mail an einen Empfänger sendet, dessen Domäne nicht auf der Liste der verwalteten E-Mail-Domänen steht, wird auf seinem Gerät eine Warnung angezeigt, dass die E-Mail an eine Person außerhalb der Domäne des Unternehmens gesendet wird.

Versucht ein Benutzer ein Element (Dokument, Anlage oder heruntergeladenes Objekt) über Safari von einer Domänen auf der Liste der verwalteten Webdomänen zu öffnen, wird dieses Element in der geeigneten Unternehmensapp geöffnet. Steht das Element nicht auf der Liste der verwalteten Webdomänen, kann es in Unternehmensapps nicht geöffnet werden. Der Benutzer muss es stattdessen in einer privaten, nicht verwalteten App öffnen.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

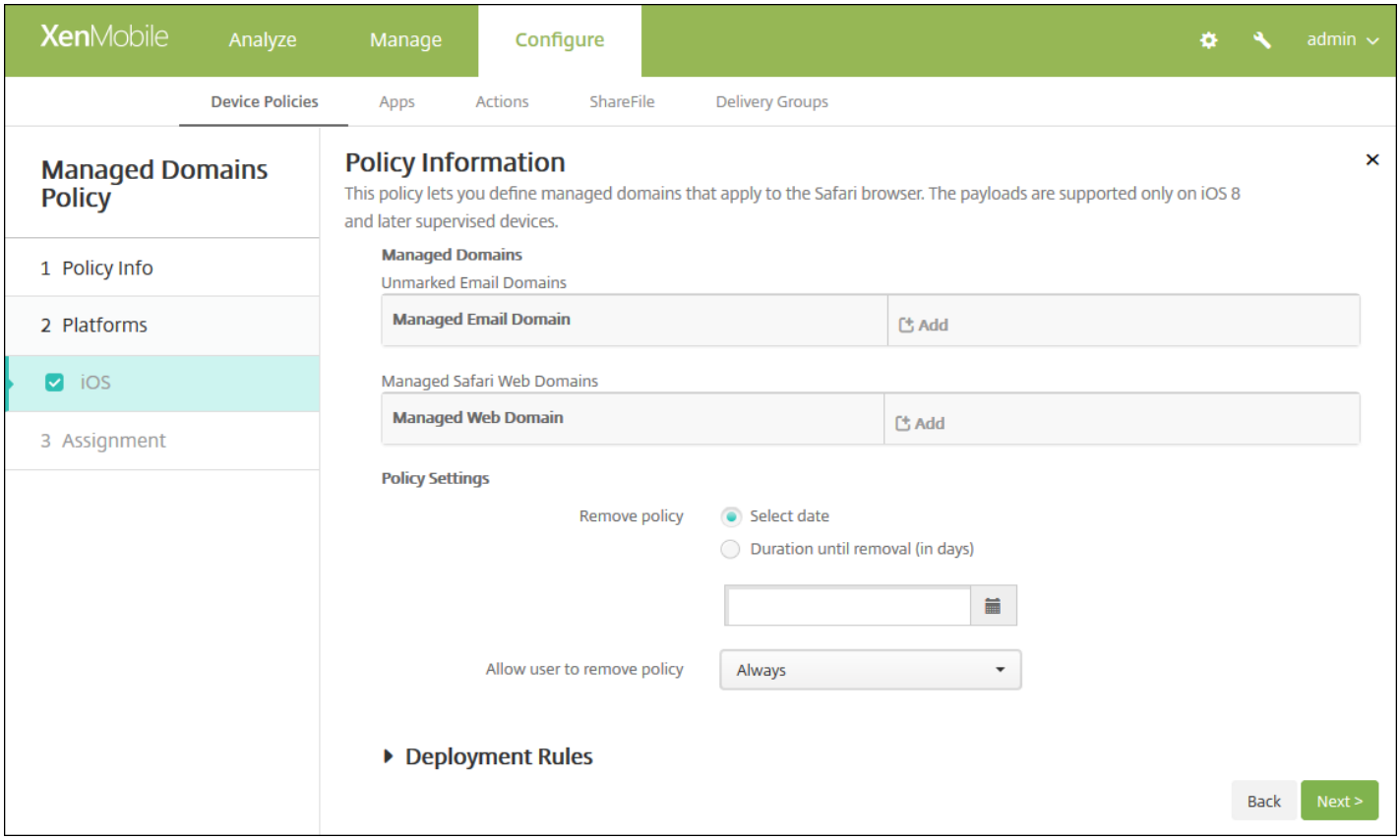
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **Verwaltete Domänen**. Die Seite **Verwaltete Domänen** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Plattformseite wird angezeigt.



Angeben von Domänen

6. Konfigurieren Sie die folgenden Einstellungen:

- **Verwaltete Domänen**
  - **Nicht markierte E-Mail-Domänen**: Klicken Sie auf für jede E-Mail-Domäne, die Sie der Liste hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
    - **Verwaltete E-Mail-Domäne**: Geben Sie die E-Mail-Domäne an.
    - Klicken Sie auf **Speichern**, um die E-Mail-Domäne zu speichern oder auf **Abbrechen**, um sie nicht zu speichern.
  - **Verwaltete Safari-Webdomänen**: Klicken Sie auf für jede Webdomäne, die Sie der Liste hinzufügen möchten, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
    - **Verwaltete Webdomäne**: Geben Sie die Webdomäne an.
    - Klicken Sie auf **Speichern**, um die Webdomäne zu speichern oder auf **Abbrechen**, um sie nicht zu speichern.

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

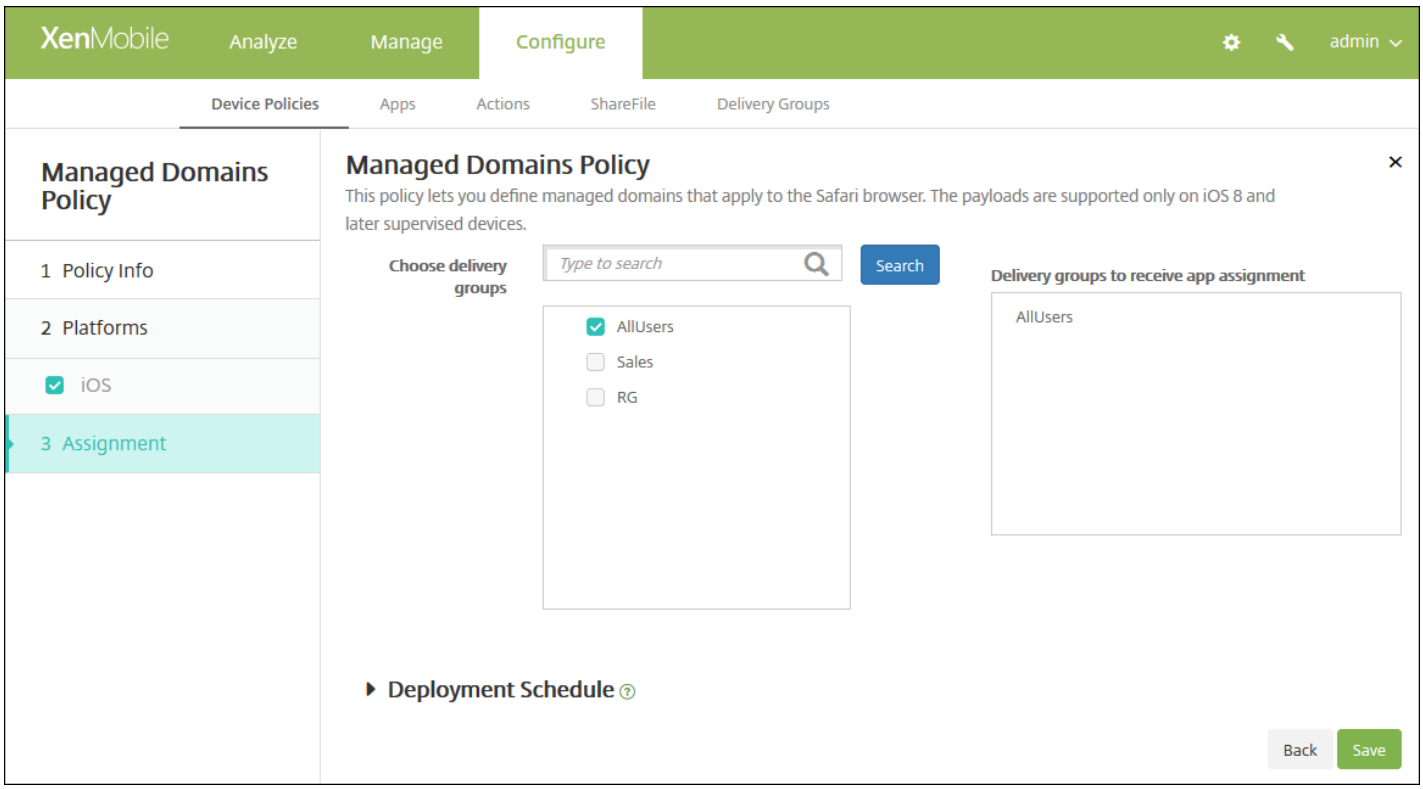
      Zum Bearbeiten eine Domäne zeigen Sie auf deren Zeile und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

- **Richtlinieneinstellungen**
  - Klicken Sie unter **Richtlinieneinstellungen** neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.

- Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
- Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
- Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Verwaltete Domänen** wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist AUS.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im

Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.

- 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.

11. Klicken Sie auf **Speichern**.

MDM-Optionsrichtlinien für Geräte

Jul 28, 2016

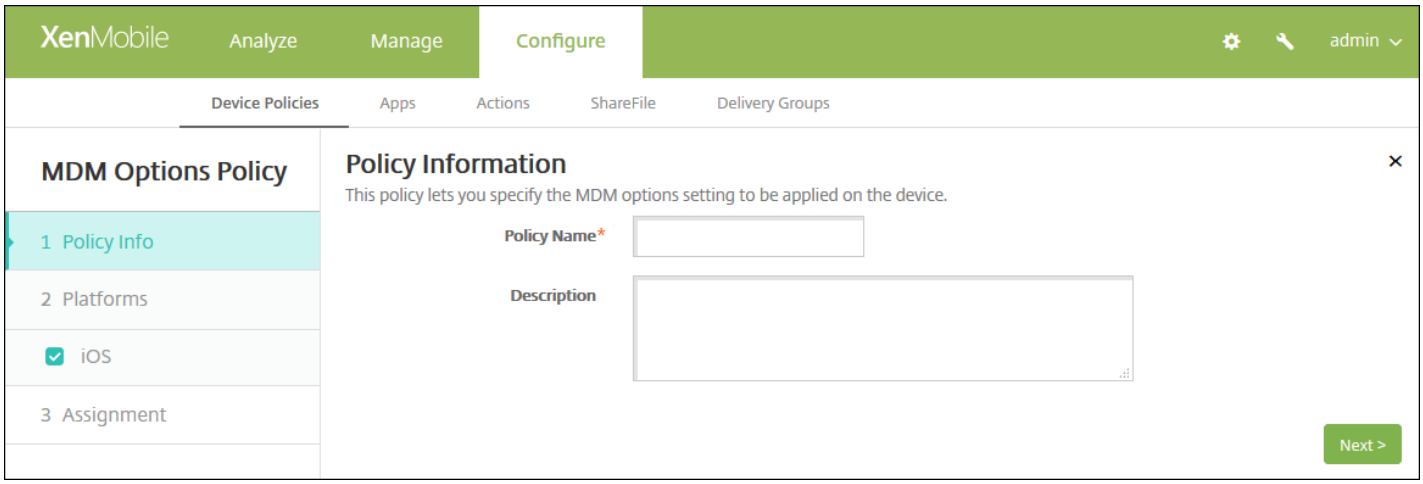
Sie können in XenMobile eine Geräterichtlinie zum Verwalten der Aktivierungssperre des Features "Mein iPhone/iPad suchen" auf betreuten Geräten mit iOS 7.0 und höher erstellen. Anweisungen zum Versetzen von iOS-Geräten in den betreuten Modus finden Sie unter Versetzen von iOS-Geräten mit dem Apple Configurator in den betreuten Modus und iOS-Massenregistrierung.

Das Feature "Mein iPhone/iPad suchen" umfasst eine Aktivierungssperre, die verhindert, dass verlorene oder gestohlene Geräte verwendet werden können, indem zum Deaktivieren des Features, Löschen der Daten auf dem Gerät, Reaktivieren und Nutzen des Geräts die Apple-ID und das Kennwort des Benutzers angefordert werden. In XenMobile können Sie das Erfordernis von Apple-ID und Kennwort umgehen, indem Sie die Aktivierungssperre über die MDM-Optionsrichtlinie aktivieren. Gibt ein Benutzer ein Gerät mit aktiviertem Feature "Mein iPhone suchen" zurück, können Sie es über die XenMobile-Konsole ohne Apple-Anmeldeinformationen verwalten.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

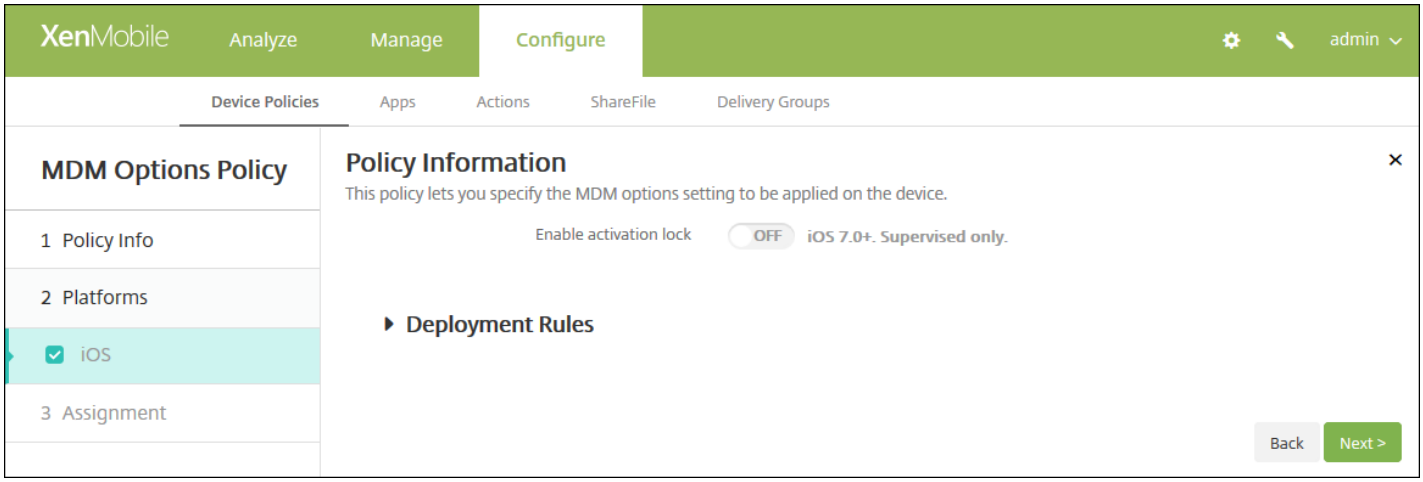
3. Erweitern Sie **Mehr** und klicken Sie unter **Endbenutzer** auf **MDM-Konto**. Die Seite **MDM-Optionen** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Richtlinieninformationen** wird angezeigt.

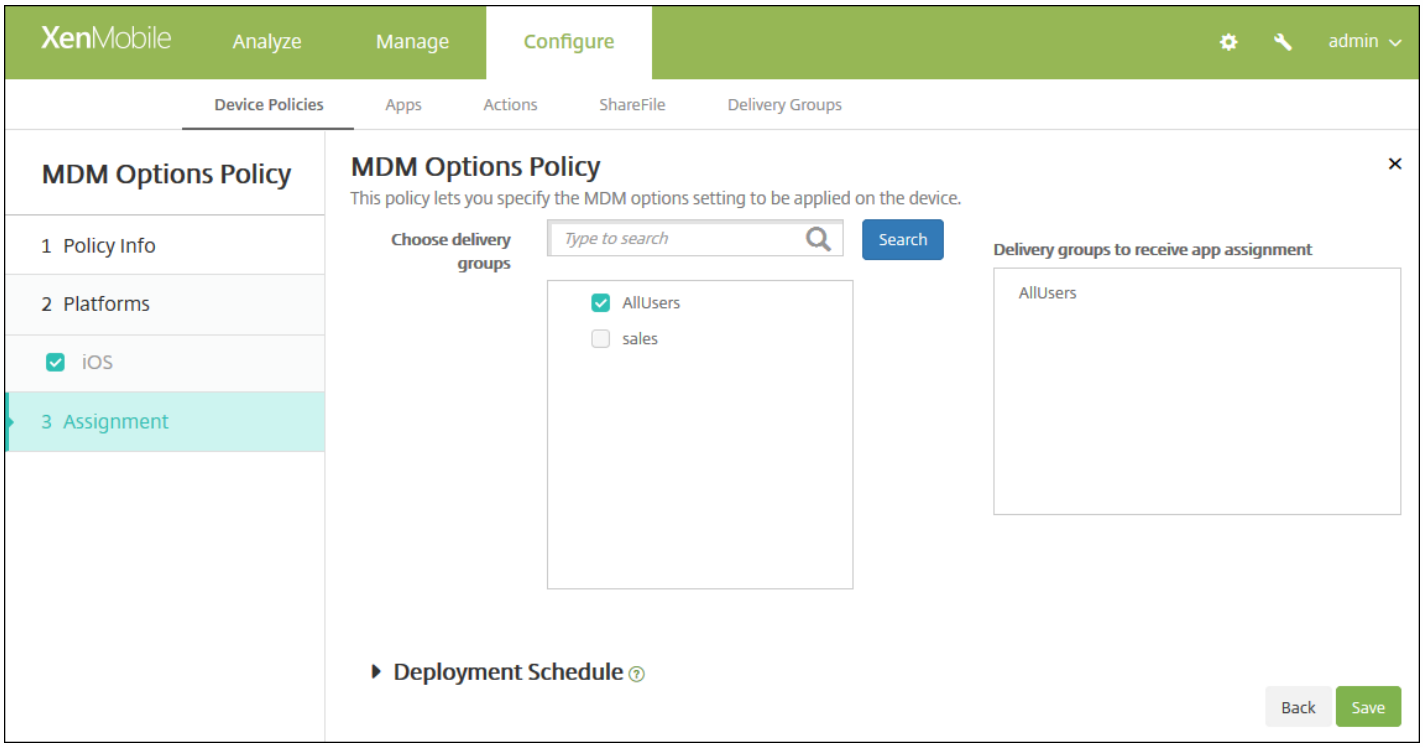


6. Konfigurieren Sie folgende Einstellung:

- **Aktivierungssperre aktivieren**: Wählen Sie aus, ob die Aktivierungssperre auf den Geräten, auf denen Sie die Richtlinie bereitstellen, aktiviert werden soll. Der Standardwert ist **AUS**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die MDM-Optionsrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Microsoft Exchange ActiveSync-Geräterichtlinien

Jul 28, 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, Mac OS X, Android HTC, Android TouchDown, Android for Work, Samsung SAFE, Samsung KNOX und Windows Phone erstellen. Jede Plattform erfordert andere Werte. Diese werden in den folgenden Abschnitten detailliert beschrieben:

iOS-Einstellungen

Mac OS X-Einstellungen

Android HTC-Einstellungen

Android TouchDown-Einstellungen

Android for Work-Einstellungen

Samsung SAFE- und Samsung KNOX-Einstellungen

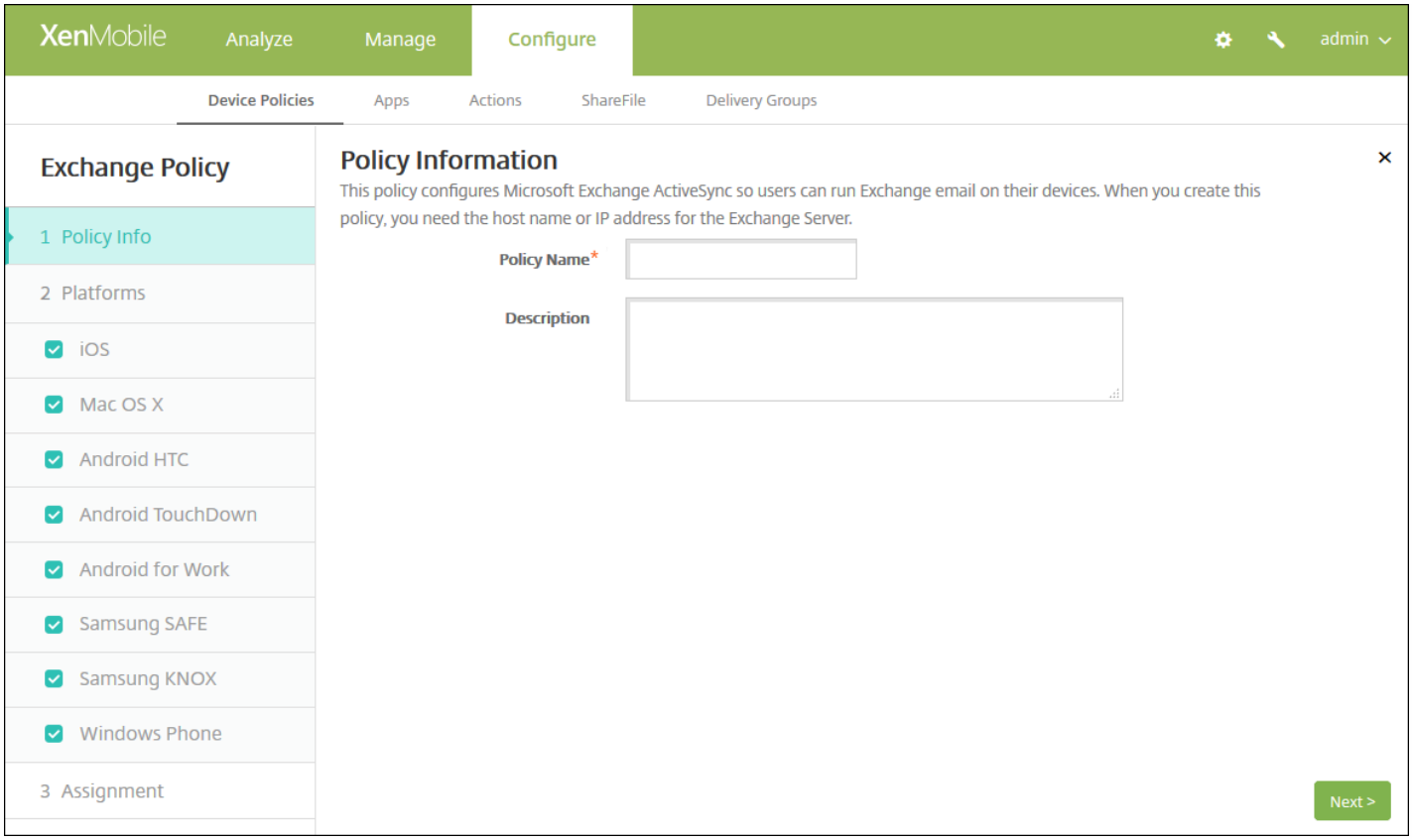
Windows Phone-Einstellungen

Zum Erstellen dieser Richtlinie benötigen Sie den Hostnamen oder die IP-Adresse des Exchange Server-Computers.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Klicken Sie auf **Exchange**. Die Seite **Exchange** wird angezeigt.



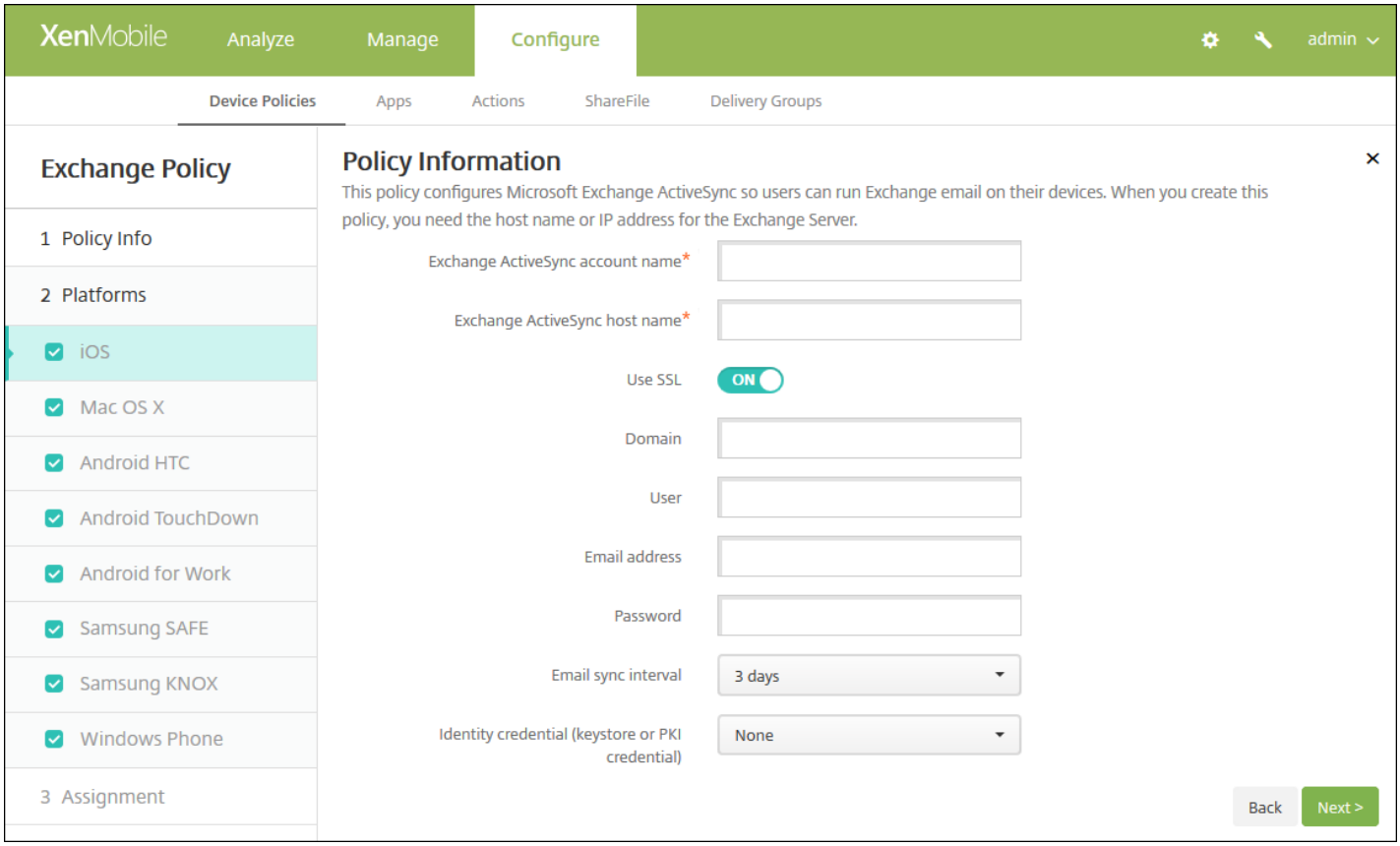
4. Geben Sie im Bereich **Richtlinieninformationen** die folgenden Informationen ein:

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

5. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

Konfigurieren von iOS-Einstellungen

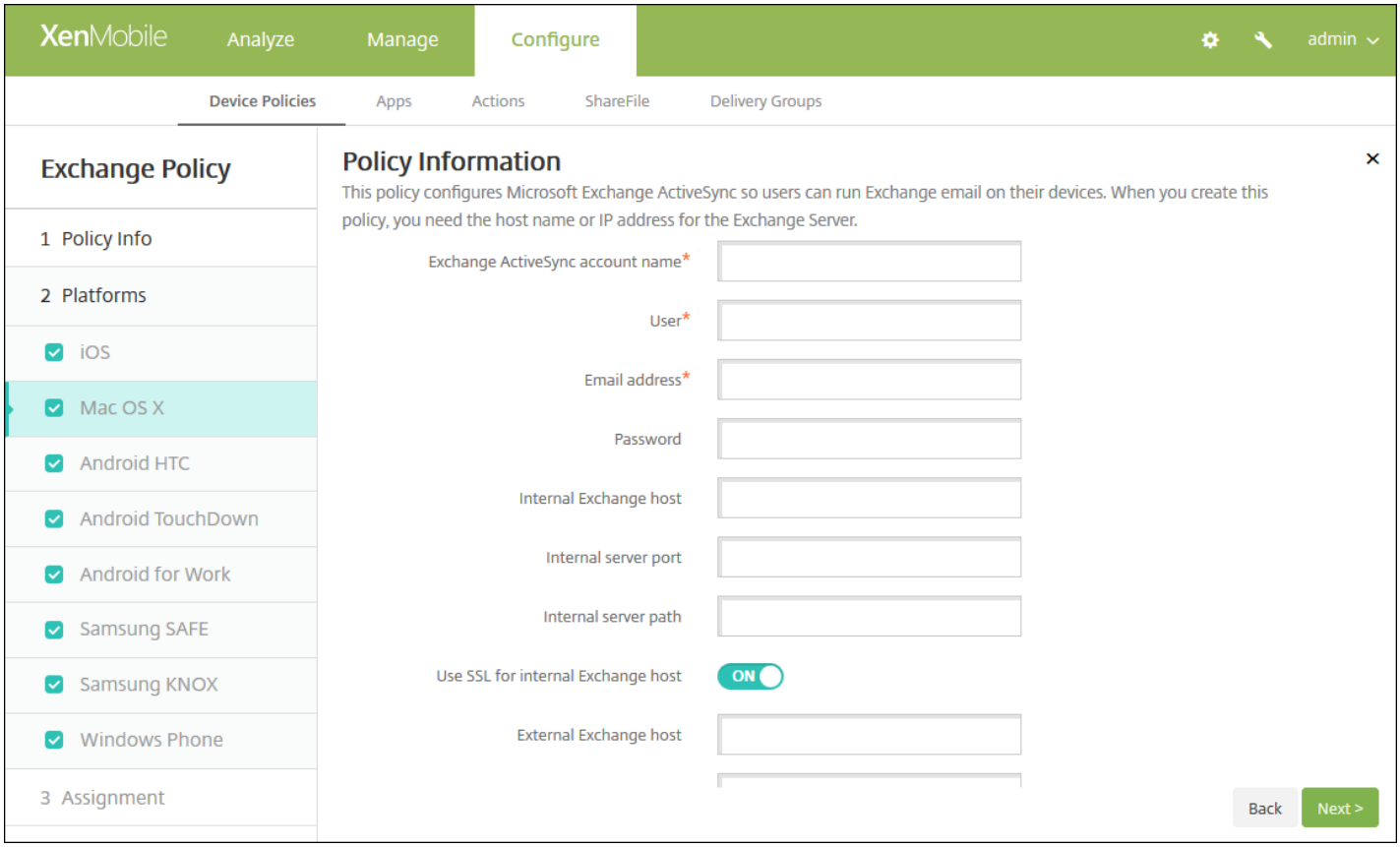


Konfigurieren Sie folgende Einstellungen:

- **Exchange ActiveSync-Kontoname**: Geben Sie die Beschreibung des E-Mail-Kontos ein, die auf den Geräten angezeigt werden soll.
- **Exchange ActiveSync- Hostname**: Geben Sie den Hostnamen des E-Mail-Servers ein.
- **SSL verwenden**: Wählen Sie aus, ob Verbindungen zwischen Benutzergeräten und dem Exchange-Server geschützt werden sollen. Der Standardwert ist **Ein**.
- **Domäne**: Geben Sie die Domäne ein, in der der Exchange-Server residiert. Sie können in diesem Feld das Systemmakro "${user.domainname}" verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
- **Benutzer**: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro "${user.username}" verwenden, um die Benutzernamen automatisch ermitteln zu lassen.
- **E-Mail-Adresse**: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein. Sie können in diesem Feld das Systemmakro "${user.mail}" verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
- **Kennwort**: Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.
- **E-Mail-Synchronisierungsintervall**: Wählen Sie in der Liste aus, wie oft die E-Mail mit Exchange Server synchronisiert werden soll. Der Standardwert ist **3 Tage**.
- **Identitätsanmeldeinformationen (Schlüsselspeicher oder PKI-Anmeldeinformationen)**: Klicken Sie in der Liste optional auf Anmeldeinformationen, wenn Sie einen Identitätsanbieter für XenMobile konfiguriert haben. Diese Angabe ist nur erforderlich, wenn Exchange eine Clientzertifikatauthentifizierung erfordert. Der Standardwert ist **Ohne**.
- **Verschieben von E-Mails zwischen Konten autorisieren**: Geben Sie an, ob Benutzer E-Mail von diesem Konto in ein anderes Konto verschieben und von einem anderen Konto aus weiterleiten dürfen und ob sie von einem anderen Konto aus antworten dürfen. Der Standardwert ist **AUS**.
- **E-Mail nur von Mailanwendung senden**: Wählen Sie aus, ob Benutzer E-Mail nur mit der iOS-E-Mail-App senden dürfen. Der Standardwert ist **Aus**.

- **Synchronisierung aktueller E-Mails deaktivieren**: Wählen Sie aus, ob eine Synchronisierung zuletzt verwendeter Adressen durch die Benutzer verhindert werden soll. Der Standardwert ist **AUS**. Diese Option gilt nur für iOS 6.0 und höher.
- **S/MIME aktivieren**: Geben Sie an, ob das Konto S/MIME-Authentifizierung und -Verschlüsselung unterstützt. Der Standardwert ist **AUS**. Bei Auswahl von **Ein** werden folgende Felder eingeblendet:
  - **Anmeldeinformationen für Signieridentität**: Der Standardwert ist **Ohne**.
  - **Anmeldeinformationen für Verschlüsselungsidentität**: Der Standardwert ist **Ohne**.
- **S/MIME-Option für einzelne Nachrichten aktivieren**: Legen Sie fest, ob Benutzer eine Verschlüsselung für einzelne E-Mail-Nachrichten aktivieren können sollen. Der Standardwert ist **Aus**.

Konfigurieren von Mac OS X-Einstellungen



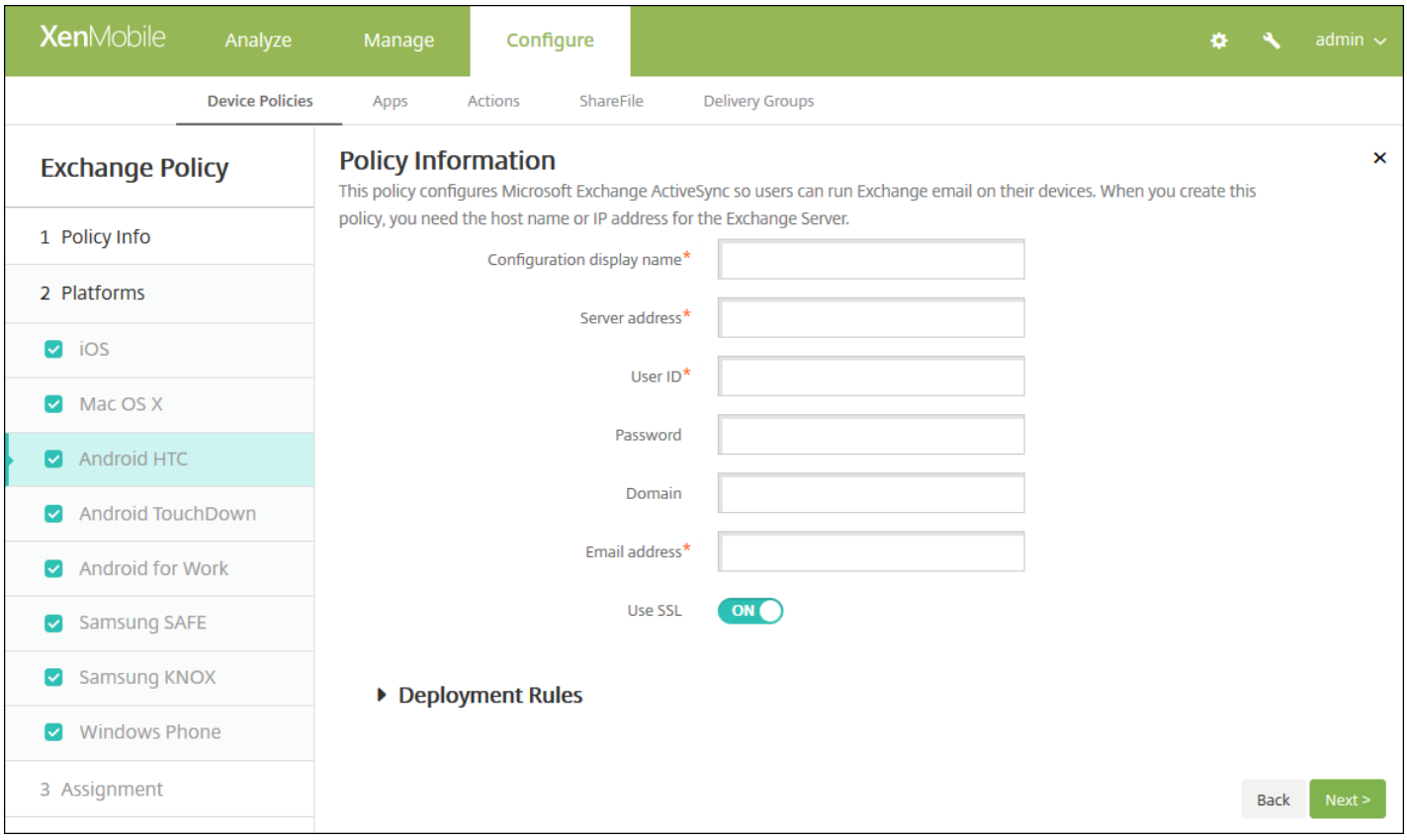
Konfigurieren Sie folgende Einstellungen:

- **Exchange ActiveSync-Kontoname**: Geben Sie die Beschreibung des E-Mail-Kontos ein, die auf den Geräten angezeigt werden soll.
- **Benutzer**: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro "${user.username}" verwenden, um die Benutzernamen automatisch ermitteln zu lassen.
- **E-Mail-Adresse**: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein. Sie können in diesem Feld das Systemmakro "${user.mail}" verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
- **Kennwort**: Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.
- **Interner Exchange-Host**: Soll intern ein anderer Exchange-Hostname verwendet werden als extern, geben Sie einen internen Exchange-Hostnamen ein.
- **Interner Serverport**: Soll intern ein anderer Exchange-Serverport verwendet werden als extern, geben Sie eine interne

Exchange-Serverportnummer ein.

- **Interner Serverpfad**: Soll intern ein anderer Exchange-Serverpfad verwendet werden als extern, geben Sie einen internen Exchange-Serverpfad ein.
- **SSL für internen Exchange-Host verwenden**: Wählen Sie aus, ob zwischen Benutzergeräten und dem internen Exchange-Host sichere Verbindungen verwendet werden sollen. Der Standardwert ist **Ein**.
- **Externer Exchange-Host**: Soll intern ein anderer Exchange-Hostname verwendet werden als extern, geben Sie einen externen Exchange-Hostnamen ein.
- **Externer Serverport**: Soll intern ein anderer Exchange-Serverport verwendet werden als extern, geben Sie eine externe Exchange-Serverportnummer ein.
- **Externer Serverpfad**: Soll intern ein anderer Exchange-Serverpfad verwendet werden als extern, geben Sie einen externen Exchange-Serverpfad ein.
- **SSL für externen Exchange-Host verwenden**: Wählen Sie aus, ob zwischen Benutzergeräten und dem internen Exchange-Host sichere Verbindungen verwendet werden sollen. Der Standardwert ist **Ein**.
- **Mail Drop zulassen**: Legen Sie fest, ob Benutzer Dateien zwischen zwei Macs ohne Verbindung mit einem vorhandenen Netzwerk drahtlos teilen können. Der Standardwert ist **AUS**.

Konfigurieren von Android HTC-Einstellungen

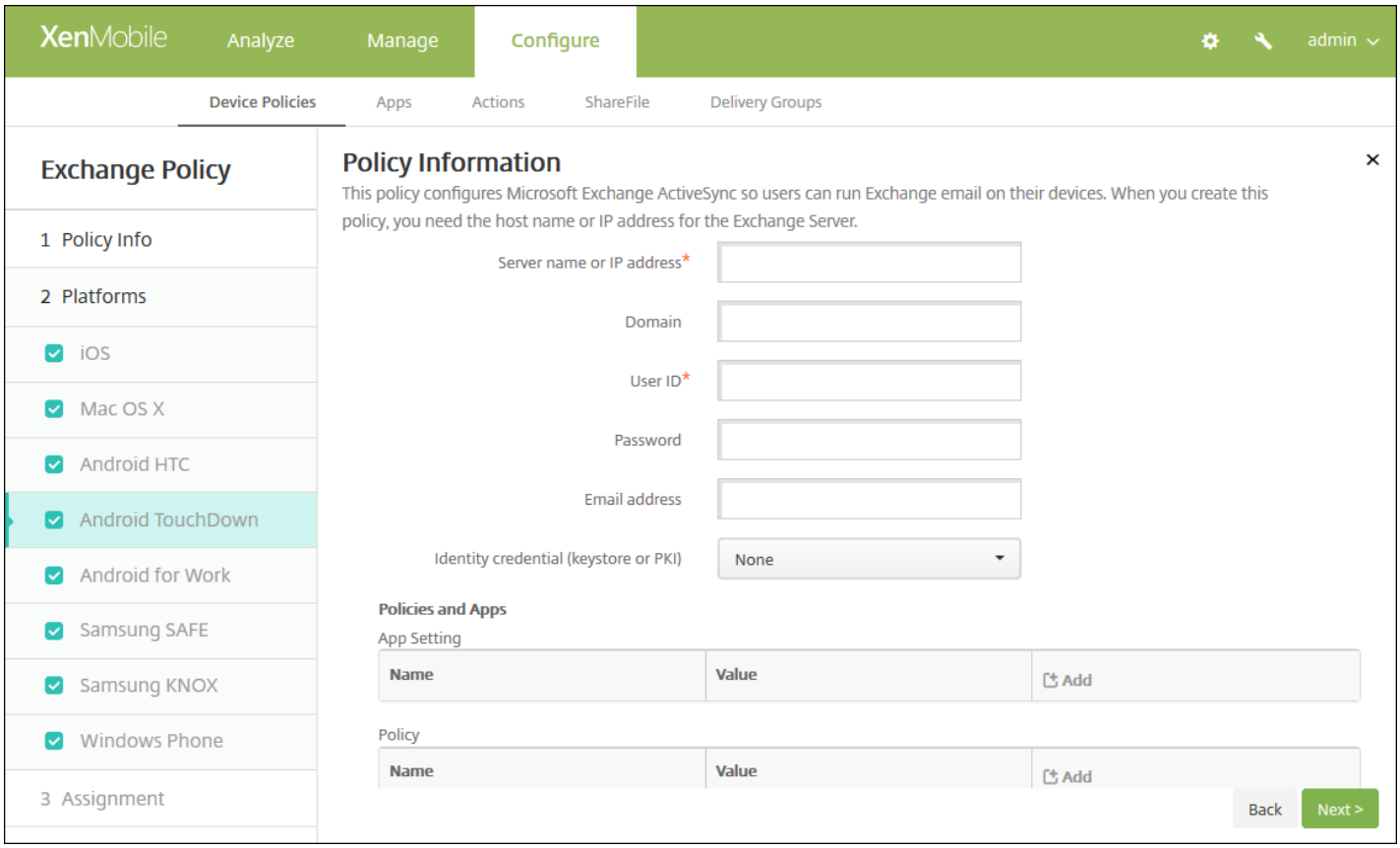


Konfigurieren Sie folgende Einstellungen:

- **Anzeigename für Konfiguration**: Geben Sie den Namen für die Richtlinie ein, wie er auf den Geräten der Benutzer angezeigt werden soll.
- **Serveradresse**: Geben Sie den Hostnamen oder die IP-Adresse des Exchange Server-Computers ein.
- **Benutzer-ID**: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro "${user.username}" verwenden, um die Benutzernamen automatisch ermitteln zu lassen.

- **Kennwort**: Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.
- **Domäne**: Geben Sie die Domäne ein, in der der Exchange-Server residiert. Sie können in diesem Feld das Systemmakro "${user.domainname}" verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
- **E-Mail-Adresse**: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein. Sie können in diesem Feld das Systemmakro "${user.mail}" verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
- **SSL verwenden**: Wählen Sie aus, ob Verbindungen zwischen Benutzergeräten und dem Exchange-Server geschützt werden sollen. Der Standardwert ist **Ein**.

Konfigurieren von Android TouchDown-Einstellungen

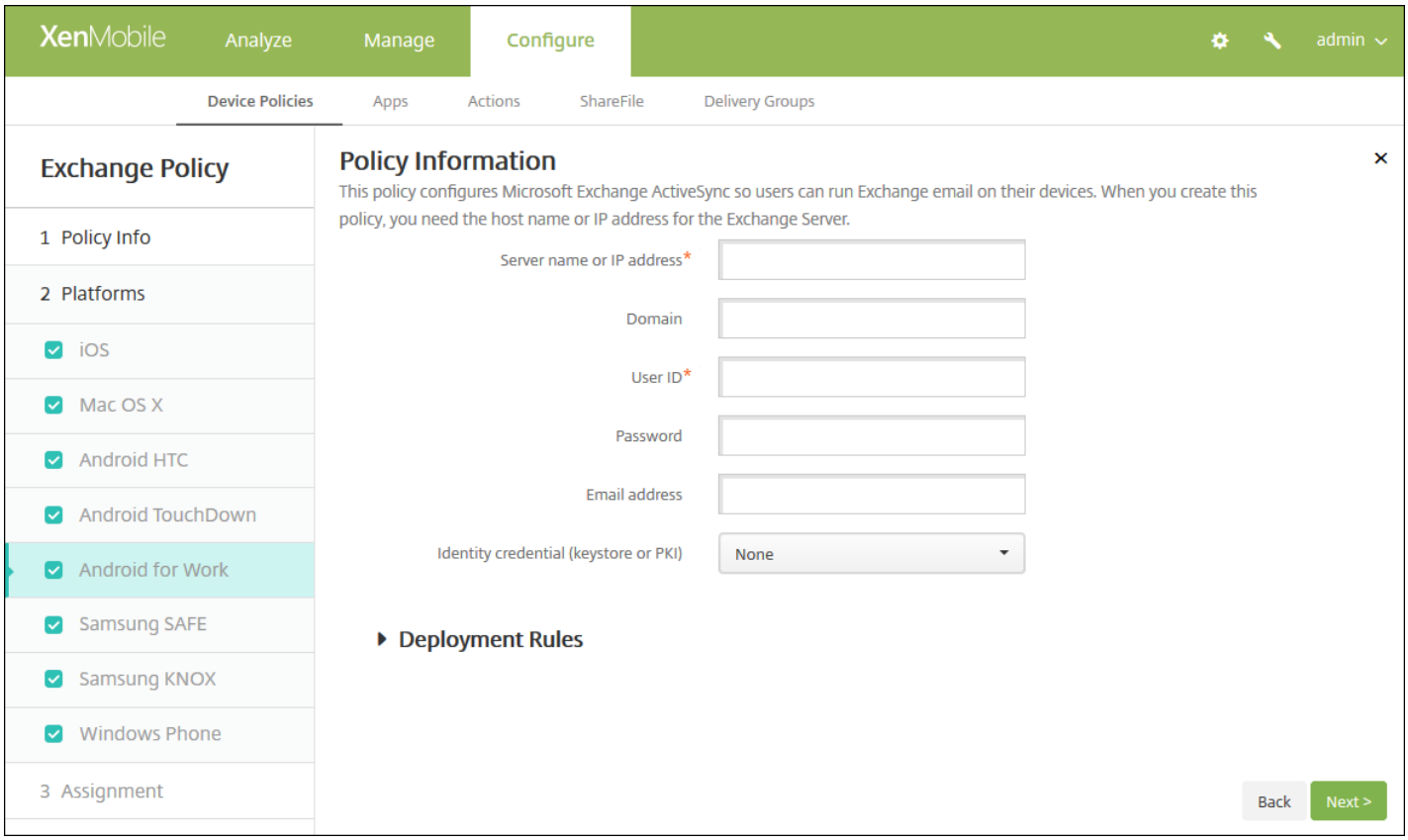


Konfigurieren Sie folgende Einstellungen:

- **Servername oder IP-Adresse**: Geben Sie den Hostnamen oder die IP-Adresse des Exchange Server-Computers ein.
- **Domäne**: Geben Sie die Domäne ein, in der der Exchange-Server residiert. Sie können in diesem Feld das Systemmakro "${user.domainname}" verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
- **Benutzer-ID**: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro "${user.username}" verwenden, um die Benutzernamen automatisch ermitteln zu lassen.
- **Kennwort**: Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.
- **E-Mail-Adresse**: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein. Sie können in diesem Feld das Systemmakro "${user.mail}" verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
- **Identitätsanmeldeinformationen (Schlüsselspeicher oder PKI-Anmeldeinformationen)**: Klicken Sie in der Liste optional auf Anmeldeinformationen, wenn Sie einen Identitätsanbieter für XenMobile konfiguriert haben. Diese Angabe ist nur erforderlich, wenn Exchange eine Clientzertifikatauthentifizierung erfordert. Der Standardwert ist **Ohne**.
- **App-Einstellung**: Fügen Sie optional TouchDown-App-Einstellungen für die Richtlinie hinzu.

- **Richtlinie**: Fügen Sie optional TouchDown-Richtlinien für die Richtlinie hinzu.

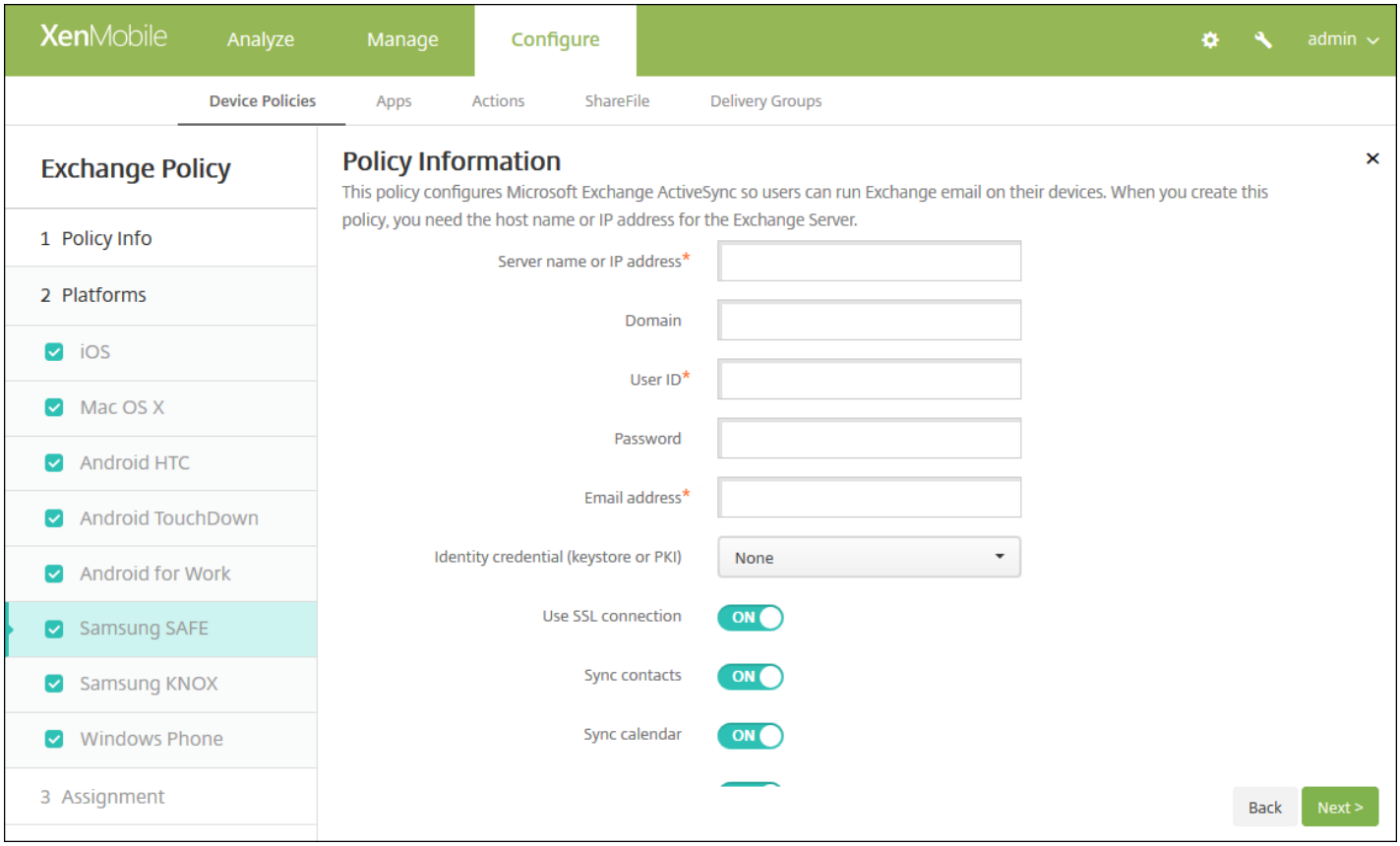
Konfigurieren von Android for Work



Konfigurieren Sie folgende Einstellungen:

- **Servername oder IP-Adresse**: Geben Sie den Hostnamen oder die IP-Adresse des Exchange Server-Computers ein.
- **Domäne**: Geben Sie die Domäne ein, in der der Exchange-Server residiert. Sie können in diesem Feld das Systemmakro "${user.domainname}" verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
- **Benutzer-ID**: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro "${user.username}" verwenden, um die Benutzernamen automatisch ermitteln zu lassen.
- **Kennwort**: Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.
- **E-Mail-Adresse**: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein. Sie können in diesem Feld das Systemmakro "${user.mail}" verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
- **Identitätsanmeldeinformationen (Schlüsselspeicher oder PKI-Anmeldeinformationen)**: Klicken Sie in der Liste optional auf Anmeldeinformationen, wenn Sie einen Identitätsanbieter für XenMobile konfiguriert haben. Diese Angabe ist nur erforderlich, wenn Exchange eine Clientzertifikatauthentifizierung erfordert. Der Standardwert ist **Ohne**.

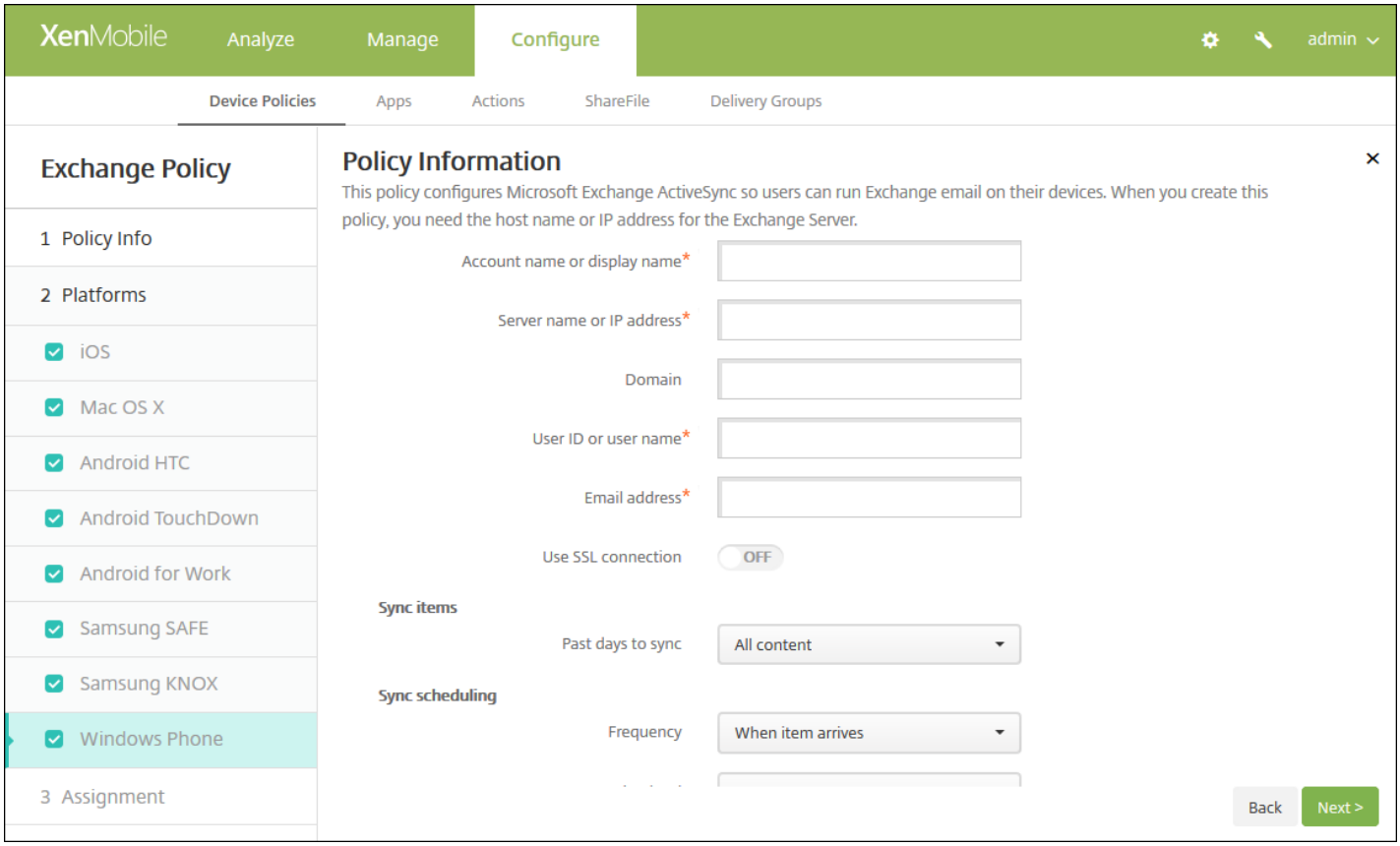
Konfigurieren von Samsung SAFE- und Samsung KNOX-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Servername oder IP-Adresse**: Geben Sie den Hostnamen oder die IP-Adresse des Exchange Server-Computers ein.
- **Domäne**: Geben Sie die Domäne ein, in der der Exchange-Server residiert. Sie können in diesem Feld das Systemmakro "${user.domainname}" verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
- **Benutzer-ID**: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro "${user.username}" verwenden, um die Benutzernamen automatisch ermitteln zu lassen.
- **Kennwort**: Geben Sie ein optionales Kennwort für das Exchange-Benutzerkonto ein.
- **E-Mail-Adresse**: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein. Sie können in diesem Feld das Systemmakro "${user.mail}" verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
- **Identitätsanmeldeinformationen (Schlüsselspeicher oder PKI-Anmeldeinformationen)**: Klicken Sie in der Liste optional auf Anmeldeinformationen, wenn Sie einen Identitätsanbieter für XenMobile konfiguriert haben. Diese Angabe ist nur erforderlich, wenn Exchange eine Clientzertifikatauthentifizierung erfordert.
- **SSL-Verbindung verwenden**: Wählen Sie aus, ob Verbindungen zwischen Benutzergeräten und dem Exchange-Server geschützt werden sollen. Der Standardwert ist **Ein**.
- **Kontakte synchronisieren**: Wählen Sie aus, ob die Synchronisierung von Kontakten zwischen den Benutzergeräten und dem Exchange Server ermöglicht werden soll. Der Standardwert ist **Ein**.
- **Kalender synchronisieren**: Wählen Sie aus, ob die Synchronisierung des Kalenders zwischen den Benutzergeräten und dem Exchange Server ermöglicht werden soll. Der Standardwert ist **Ein**.
- **Option Standardkonto** 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 **Ein**.

Konfigurieren von Windows Phone-Einstellungen



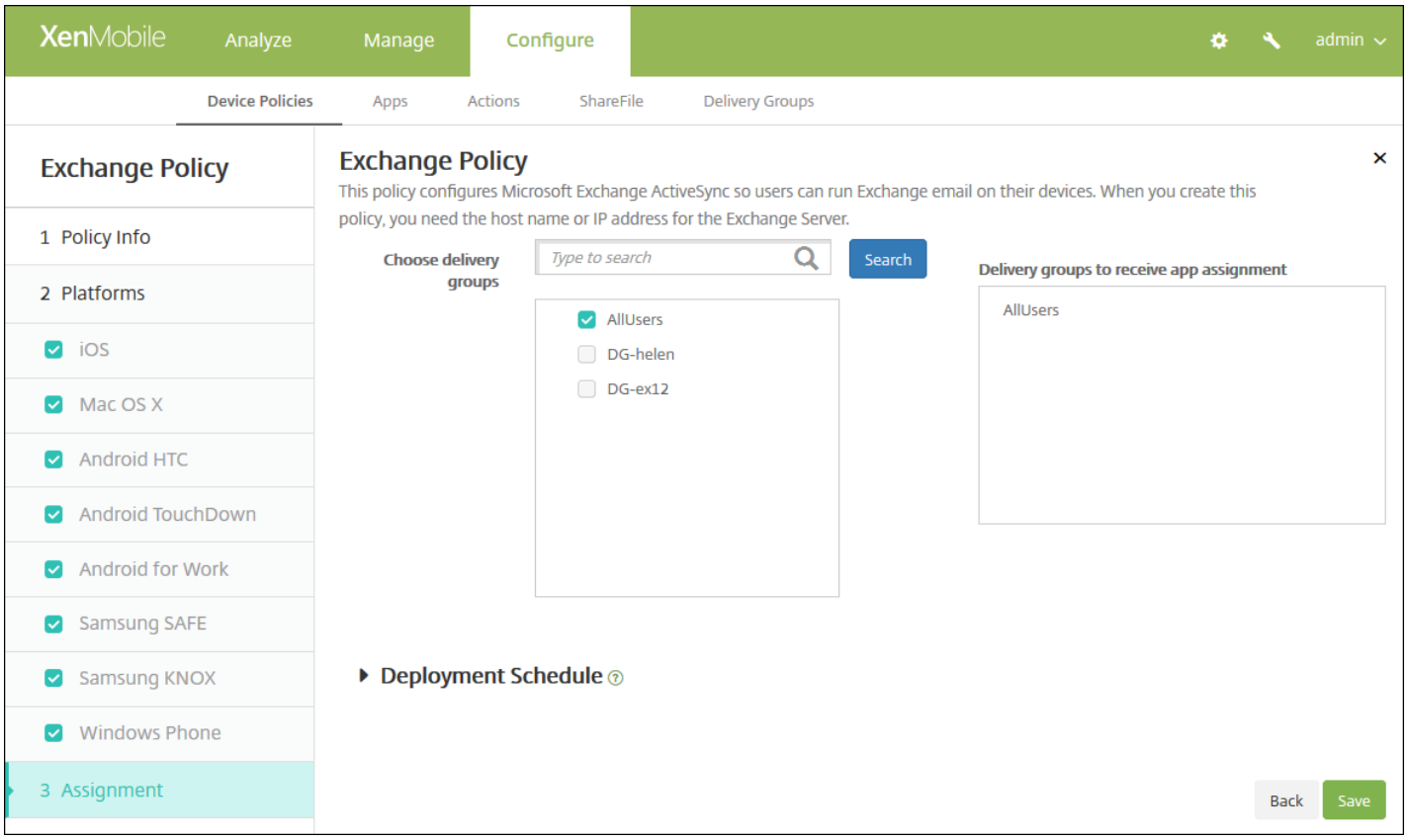
Konfigurieren Sie folgende Einstellungen:

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.

- **Kontoname oder Anzeigename**: Geben Sie den Exchange ActiveSync-Kontonamen ein.
- **Servername oder IP-Adresse**: Geben Sie den Hostnamen oder die IP-Adresse des Exchange-Servers ein.
- **Domäne**: Geben Sie die Domäne ein, in der der Exchange-Server residiert. Sie können in diesem Feld das Systemmakro "${user.domainname}" verwenden, um die Domänennamen der Benutzer automatisch ermitteln zu lassen.
- **Benutzer-ID oder Benutzername**: Geben Sie den Benutzernamen des Exchange-Benutzerkontos ein. Sie können in diesem Feld das Systemmakro "${user.username}" verwenden, um die Benutzernamen automatisch ermitteln zu lassen.
- **E-Mail-Adresse**: Geben Sie die vollständige E-Mail-Adresse des Benutzers ein. Sie können in diesem Feld das Systemmakro "${user.mail}" verwenden, um die E-Mail-Konten der Benutzer automatisch ermitteln zu lassen.
- **SSL-Verbindung verwenden**: Wählen Sie aus, ob Verbindungen zwischen Benutzergeräten und dem Exchange-Server geschützt werden sollen. Der Standardwert ist **Aus**.
- **Zu synchronisierende Tage**: Wählen Sie in der Liste aus, wie viele Tage die Synchronisierung zwischen Gerät und dem Exchange-Server in die Vergangenheit reichen soll. Die Standardeinstellung ist **Alle**.
- **Häufigkeit**: Wählen Sie in der Liste den Zeitplan für die Synchronisierung von Daten, die vom Exchange-Server auf Geräte gesendet werden, aus. Der Standardwert ist **Bei Eingang von Element**.
- **Protokollebene**: Klicken Sie in der Liste auf **Deaktiviert**, **Einfach** oder **Erweitert**, um festzulegen, wie detailliert Exchange-Aktivitäten protokolliert werden sollen. Die Standardeinstellung ist **Deaktiviert**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Exchange-Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Geräterichtlinie für Unternehmensinformationen

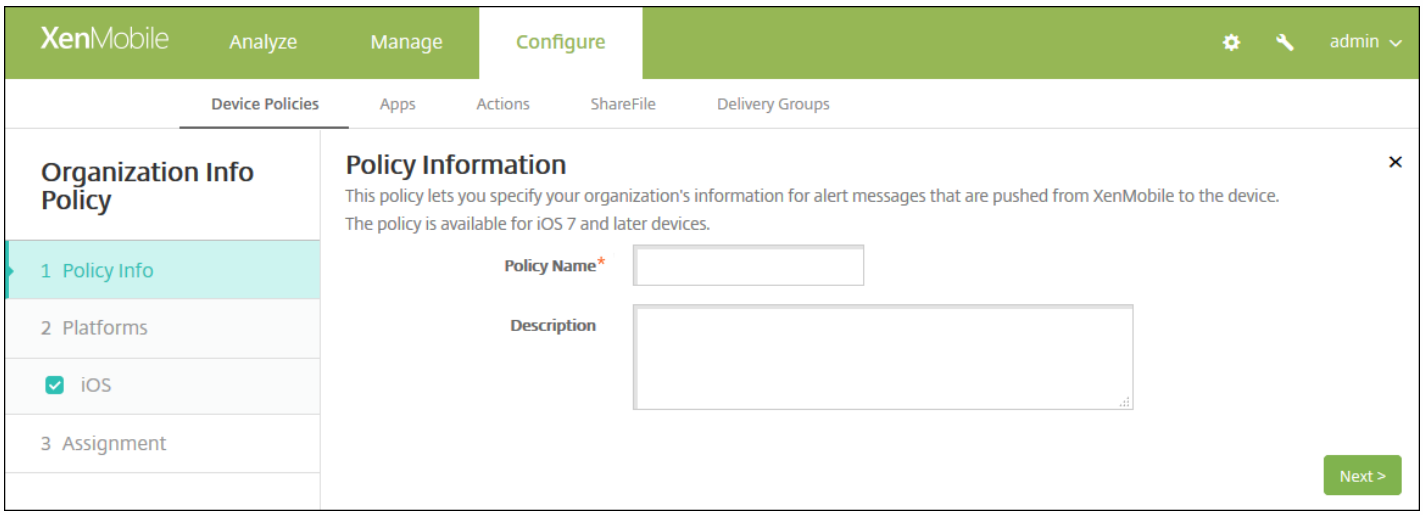
Jul 28, 2016

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 **Konfigurieren > Geräterichtlinien**. Die Seite **Geräterichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

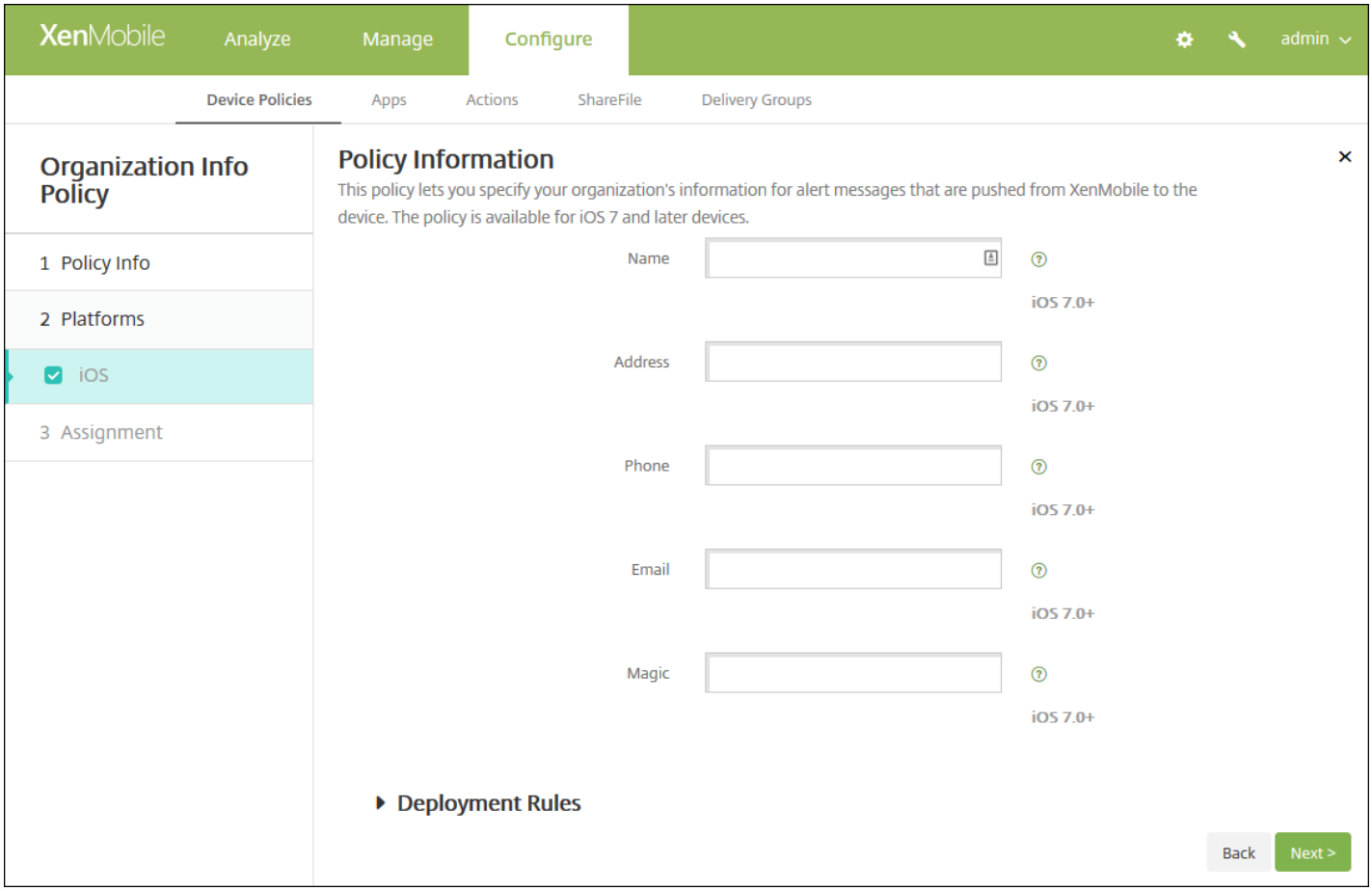
3. Klicken Sie auf **Mehr** und dann unter **Endbenutzer** auf **Informationen zum Unternehmen**. Die Seite für die Richtlinieninformationen der Richtlinie **Unternehmensinformationen** wird angezeigt.



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

- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung für die Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite mit den Plattforminformationen für **iOS** wird angezeigt.

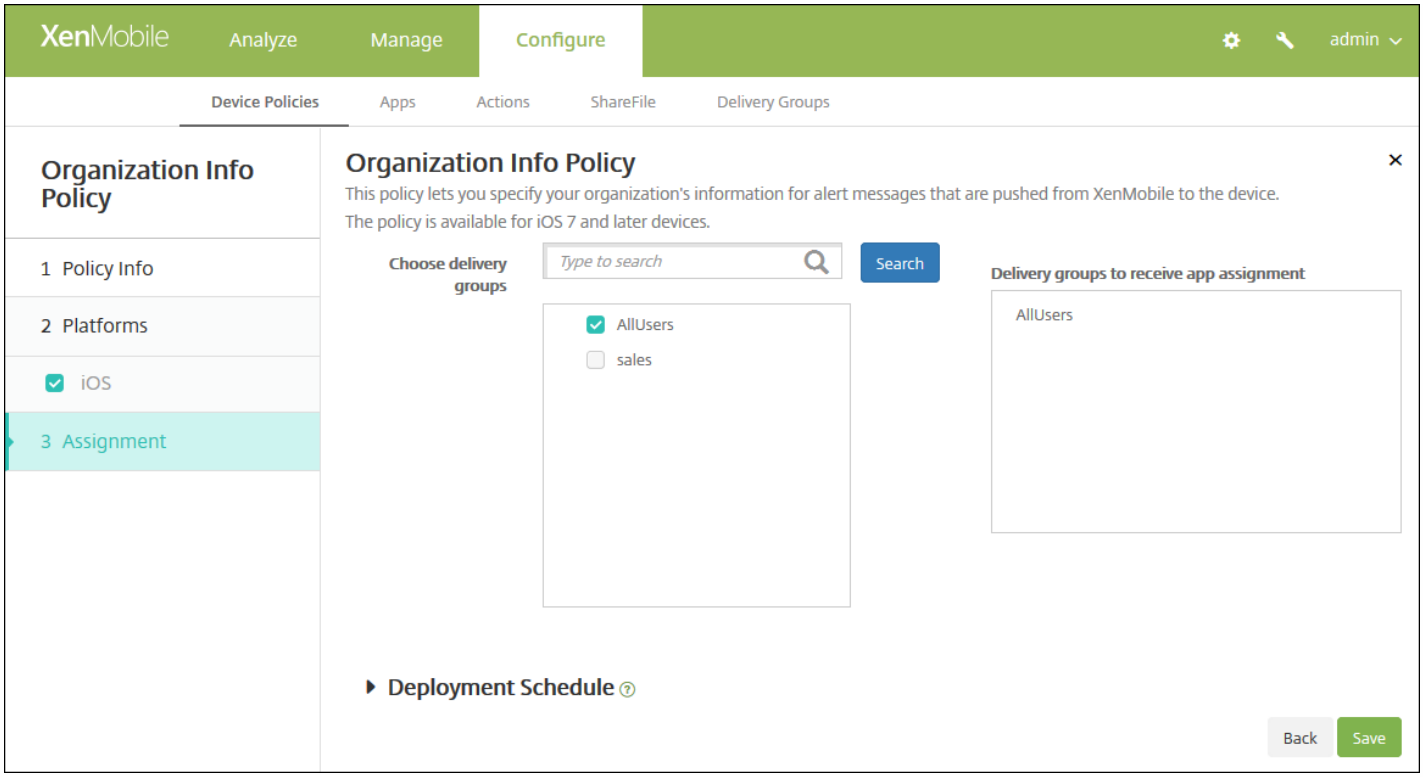


Konfigurieren Sie folgende Einstellungen:

- **Name**: Geben Sie den Namen des Unternehmens ein, das XenMobile ausführt.
- **Adresse**: Geben Sie die Adresse des Unternehmens ein.
- **Telefon**: Geben Sie die Supporttelefonnummer des Unternehmens ein.
- **E-Mail**: Geben Sie die Support-E-Mail-Adresse des Unternehmens ein.
- **Zauberwort**: Geben Sie ein oder mehrere Stichwörter zur Beschreibung der vom Unternehmen verwalteten Dienste ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Richtlinie für Unternehmensinformationen wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Passcoderichtlinien für Geräte

Jul 28, 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. Sie können Richtlinien für iOS, Mac OS X, Android, Android for Work, Samsung KNOX, Windows Phone und Windows Desktop/Tablet erstellen. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Abschnitt beschrieben.

iOS-Einstellungen

Mac OS X-Einstellungen

Android-Einstellungen

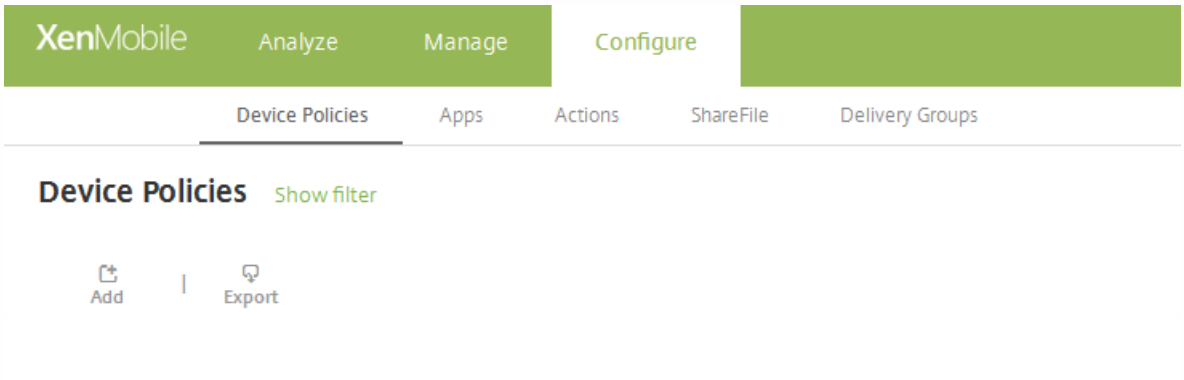
Samsung KNOX-Einstellungen

Android for Work-Einstellungen

Windows Phone-Einstellungen

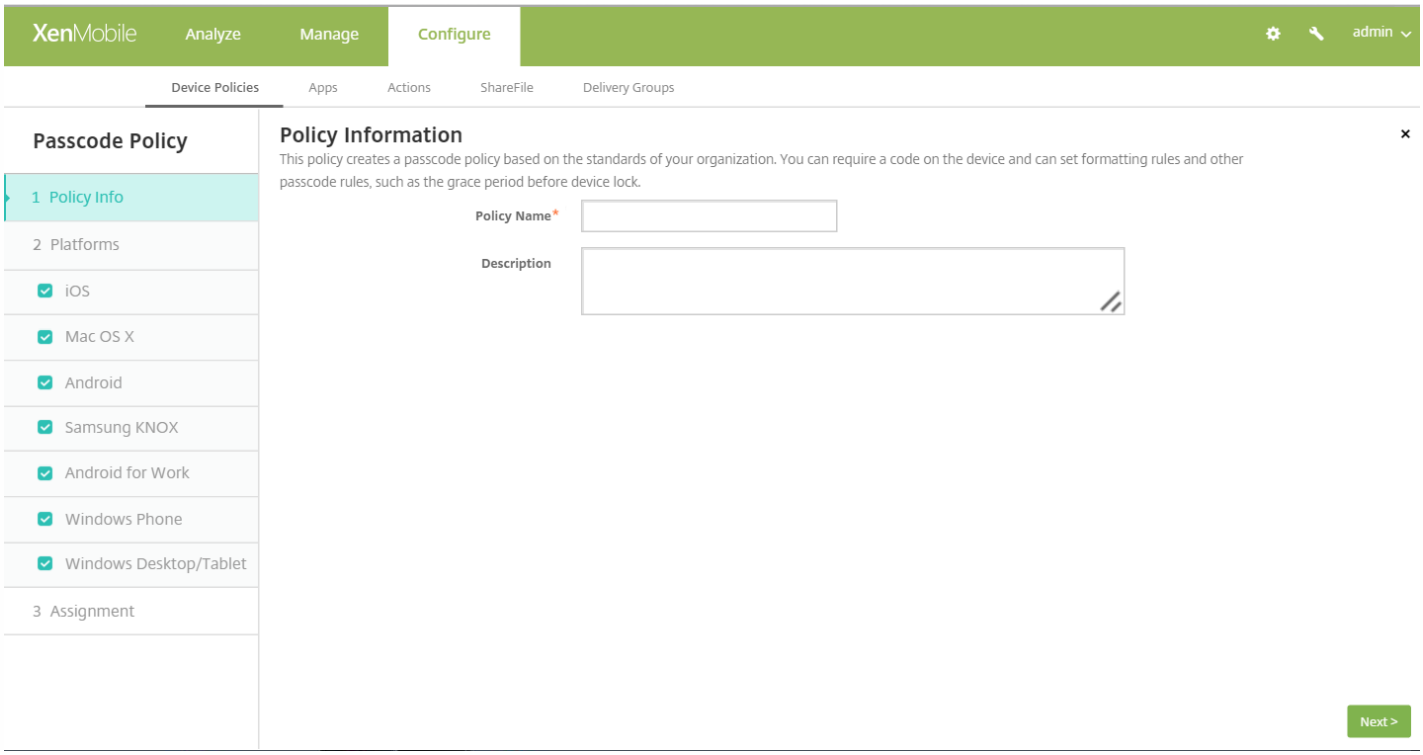
Windows Desktop/Tablet-Einstellungen

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



2. Klicken Sie auf **Hinzufügen**. Die Seite Neue Richtlinie hinzufügen wird angezeigt.

3. Klicken Sie auf **Passcode**. Die Seite Passcode wird angezeigt.



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

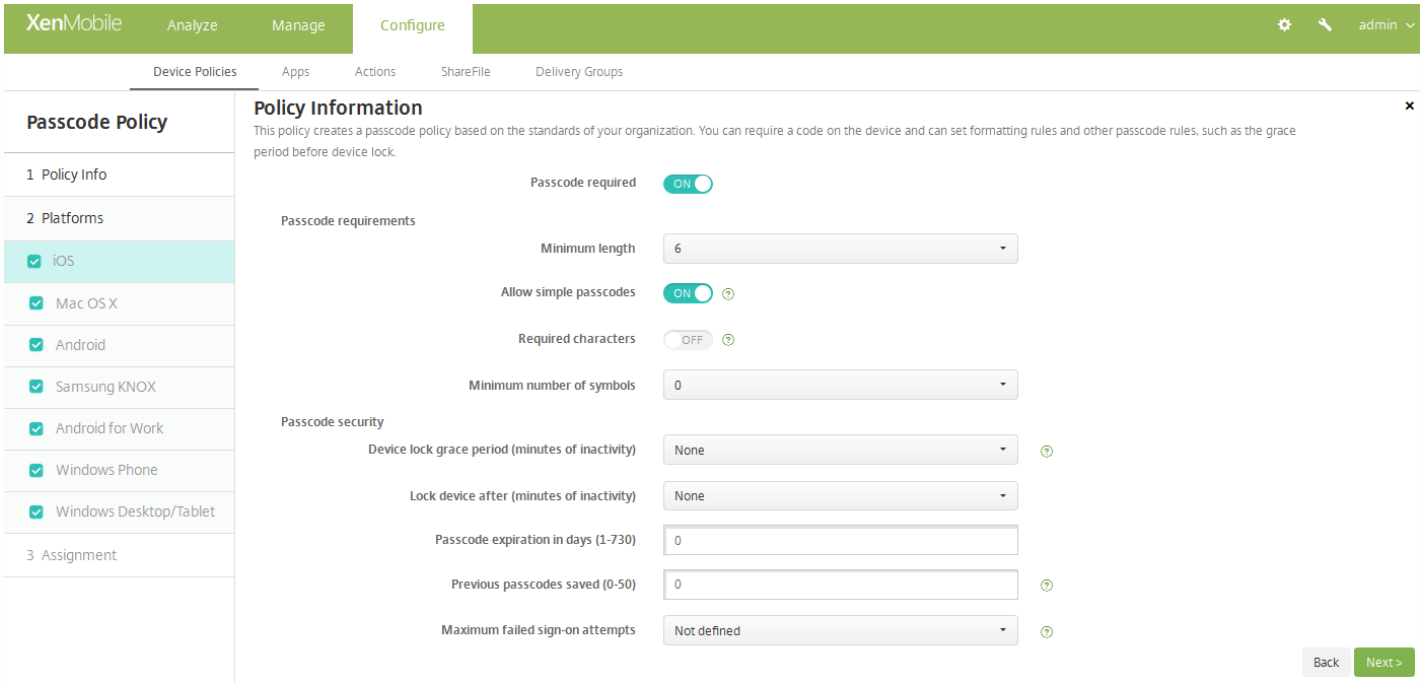
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

Konfigurieren von iOS-Einstellungen

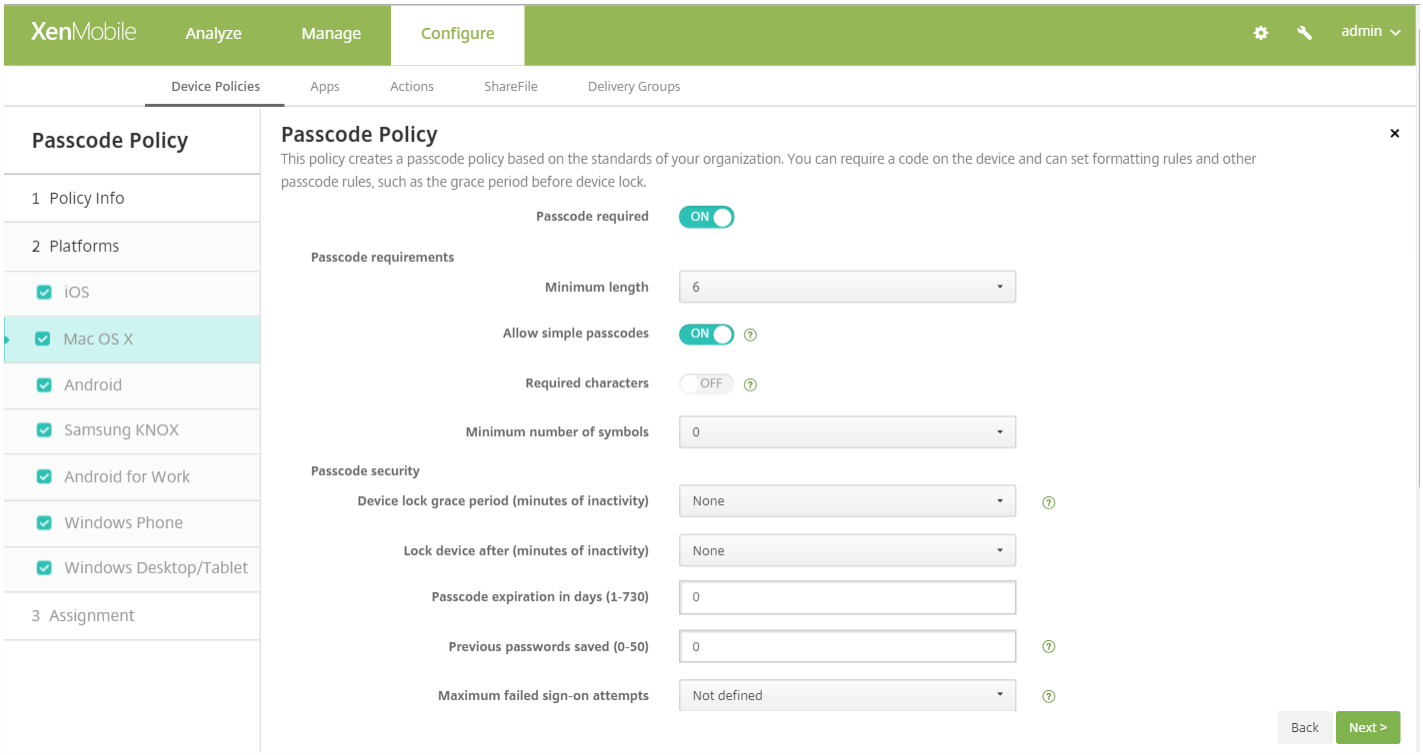


Konfigurieren Sie die folgenden Einstellungen:

- **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. Der Standardwert ist **0**.
- **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".
  - **Passcodeablauf in Tagen (1-730 Tage)**: Geben Sie die Anzahl der Tage ein, nach denen der Passcode ablaufen soll. Gültige Werte sind 1-730. Der Standardwert ist **0**, was bedeutet, dass der Passcode nie abläuft.
  - **Vorherige Kennwörter speichern (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**
  - Klicken Sie für **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.

- Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
- Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
- Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

Konfigurieren von Mac OS X-Einstellungen



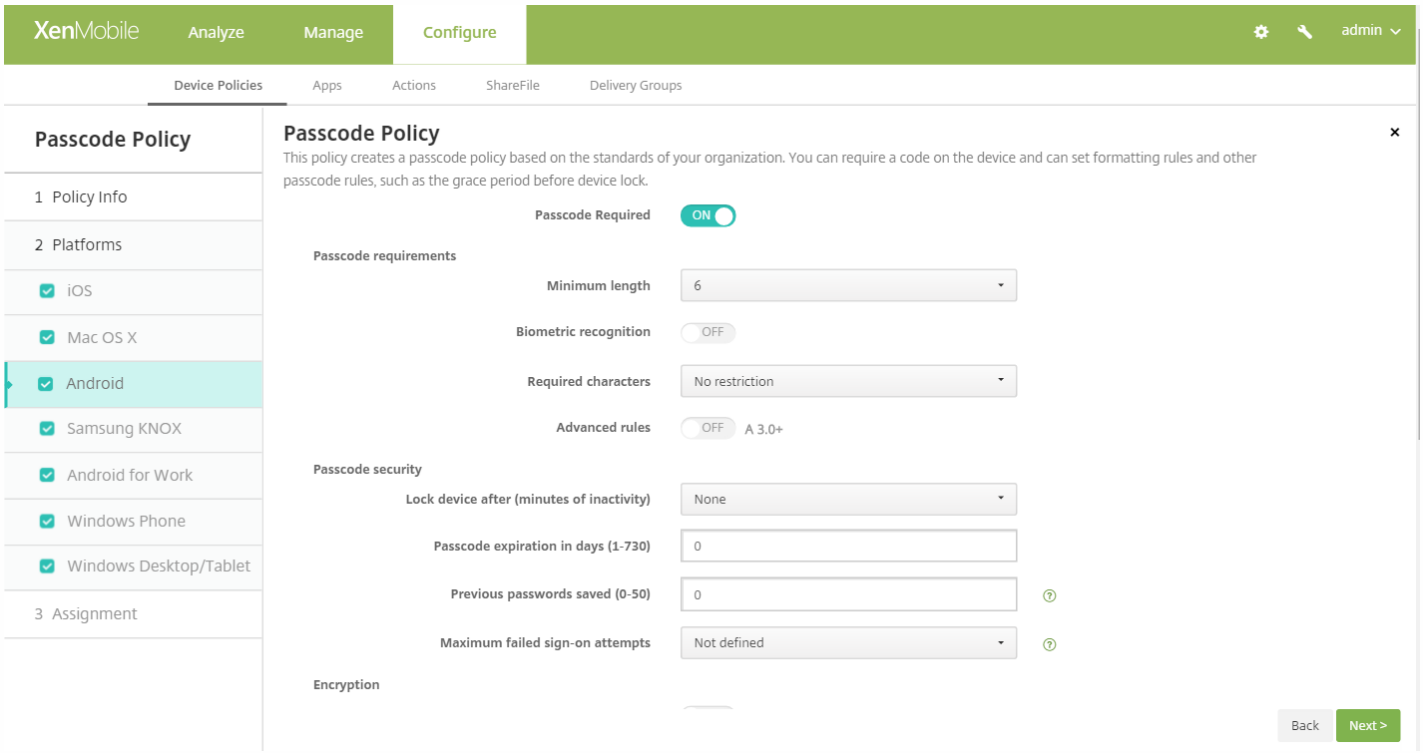
Konfigurieren Sie folgende Einstellungen:

- **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.
- Wenn Sie **Passcode erforderlich** nicht aktivieren, geben Sie für **Verzögerung (in Minuten) nach fehlgeschlagenen Anmeldeversuchen** den Zeitraum in Minuten ein, bis ein Benutzer erneut versuchen darf, seinen Passcode einzugeben.
- Wenn Sie **Passcode erforderlich** auswählen, konfigurieren Sie die folgenden Einstellungen:
- **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. Die Standardeinstellung 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. Der Standardwert ist **0**.
- **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**.

- **Passcodeablauf in Tagen (1-730 Tage)**: Geben Sie die Anzahl der Tage ein, nach denen der Passcode ablaufen soll. Gültige Werte sind 1-730. Der Standardwert ist **0**, was bedeutet, dass der Passcode nie abläuft.
- **Vorherige Kennwörter speichern (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**.
- **Verzögerung (in Minuten) nach fehlgeschlagenen Anmeldeversuchen**: Geben den Zeitraum in Minuten ein, bis ein Benutzer erneut versuchen darf, seinen Passcode einzugeben.

- **Richtlinieneinstellungen**
  - Klicken Sie für **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.
  - Klicken Sie neben **Gültigkeitsbereich für Profil** auf **Benutzer** oder **System**. Der Standardwert ist **Benutzer**. Diese Option ist nur für OS X 10.7 und höher verfügbar.

Konfigurieren von Android-Einstellungen



Konfigurieren Sie folgende Einstellungen:

Hinweis: Die Standardeinstellung für Android ist **AUS**.

- **Passcode erforderlich**: Wählen Sie diese Option aus, damit ein Passcode erforderlich ist, und um die Konfigurationsoptionen für die Android-Passcoderichtlinie anzuzeigen. 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**.
  - **Erforderliche Zeichen**: 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 "Keine Einschränkung".
  - **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 **Erweiterte Regeln** aktivieren, 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**.
  - **Passcodeablauf in Tagen (1-730 Tage)**: Geben Sie die Anzahl der Tage ein, nach denen der Passcode ablaufen soll. Gültige Werte sind 1-730. Der Standardwert ist **0**, was bedeutet, dass der Passcode nie abläuft.
  - **Vorherige Kennwörter speichern (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 die Daten auf dem betroffenen Gerät 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.

    Hinweis: Zum Verschlüsseln von Geräten muss sichergestellt werden, dass der Geräteakku vollständig geladen ist. Außerdem müssen die Geräte während der mindestens eine Stunde dauernden Verschlüsselung am Stromnetz angeschlossen werden. Wird die Verschlüsselung unterbrochen, kann es zum Verlust einiger oder aller Daten auf dem Gerät kommen. Die Verschlüsselung eines Geräts kann nur durch eine Zurücksetzung auf die werkseitige Voreinstellung rückgängig gemacht werden. Bei einer solchen Zurücksetzung werden alle Daten auf dem Gerät gelöscht.

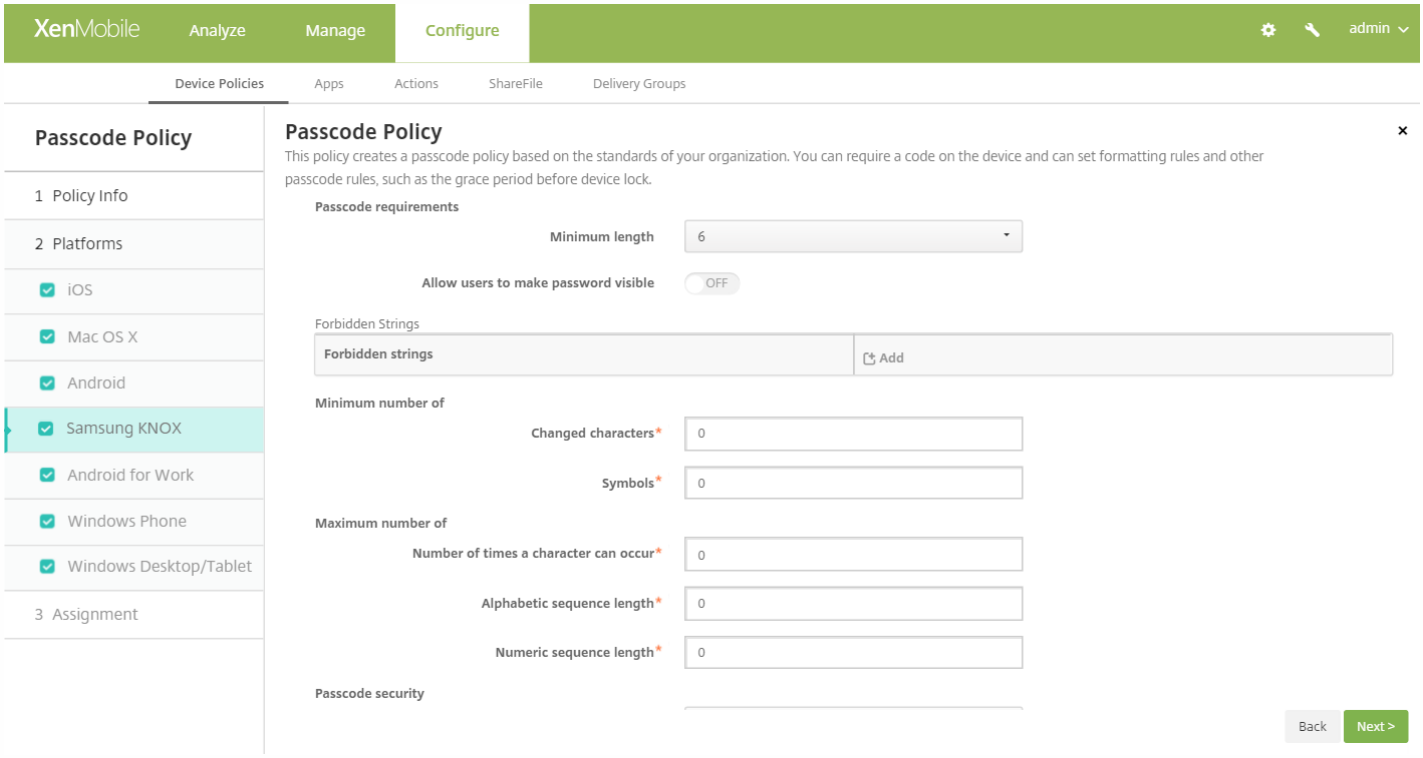
- **Samsung SAFE**
  - **Gleichen Passcode für alle Benutzer verwenden**: Wählen Sie aus, ob der gleiche Passcode für alle Benutzer verwendet werden soll. Der Standardwert ist **AUS**. Diese Einstellung gilt nur für Samsung SAFE-Geräte und ist unabhängig von der Einstellung für **Passcode erforderlich** verfügbar.
  - Wenn Sie **Gleichen Passcode für alle Benutzer verwenden** auswählen, geben Sie im Feld **Passcode** den gewünschten Passcode ein.
  - Wenn Sie **Passcode erforderlich** aktivieren, konfigurieren Sie die folgenden Samsung SAFE-Einstellungen:
    - **Geänderte Zeichen**: Geben Sie an, wie viele Zeichen die Benutzer gegenüber dem vorherigen Passcode ändern müssen. Der Standardwert ist **0**.

- **Maximale Häufigkeit**: Geben Sie an, wie oft ein Zeichen in einem Passcode höchstens vorkommen darf. Der Standardwert ist **0**.
- **Länge der alphabetischen Sequenz**: Geben Sie die maximal zulässige Länge einer Reihe alphabetisch geordneter Zeichen in einem Passcode an. Der Standardwert ist **0**.
- **Länge der numerischen Sequenz**: Geben Sie die maximal zulässige Länge einer Reihe numerisch geordneter Zeichen in einem Passcode an. Der Standardwert ist **0**.
- **Benutzer dürfen Kennwort anzeigen**: Wählen Sie aus, ob Benutzern das Anzeigen des Passcodes ermöglicht werden soll. Die Standardeinstellung ist **EIN**.
- **Verbotene Zeichenfolgen**: Durch das Konfigurieren verbotener Zeichenfolgen verhindern Sie, dass Benutzer unsichere, einfach zu erratende Zeichenfolgen ("Kennwort", "Willkommen", "123456", "111111" usw.) verwenden können. Klicken Sie für jede Zeichenfolge, die Sie verbieten möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Verbotene Zeichenfolgen**: Geben Sie die Zeichenfolge ein, die die Benutzer nicht verwenden dürfen.
  - Klicken Sie auf **Speichern**, um die Zeichenfolge hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

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

    Zum Bearbeiten einer Zeichenfolge 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

Konfigurieren der Samsung KNOX-Einstellungen



Konfigurieren Sie folgende Einstellungen:

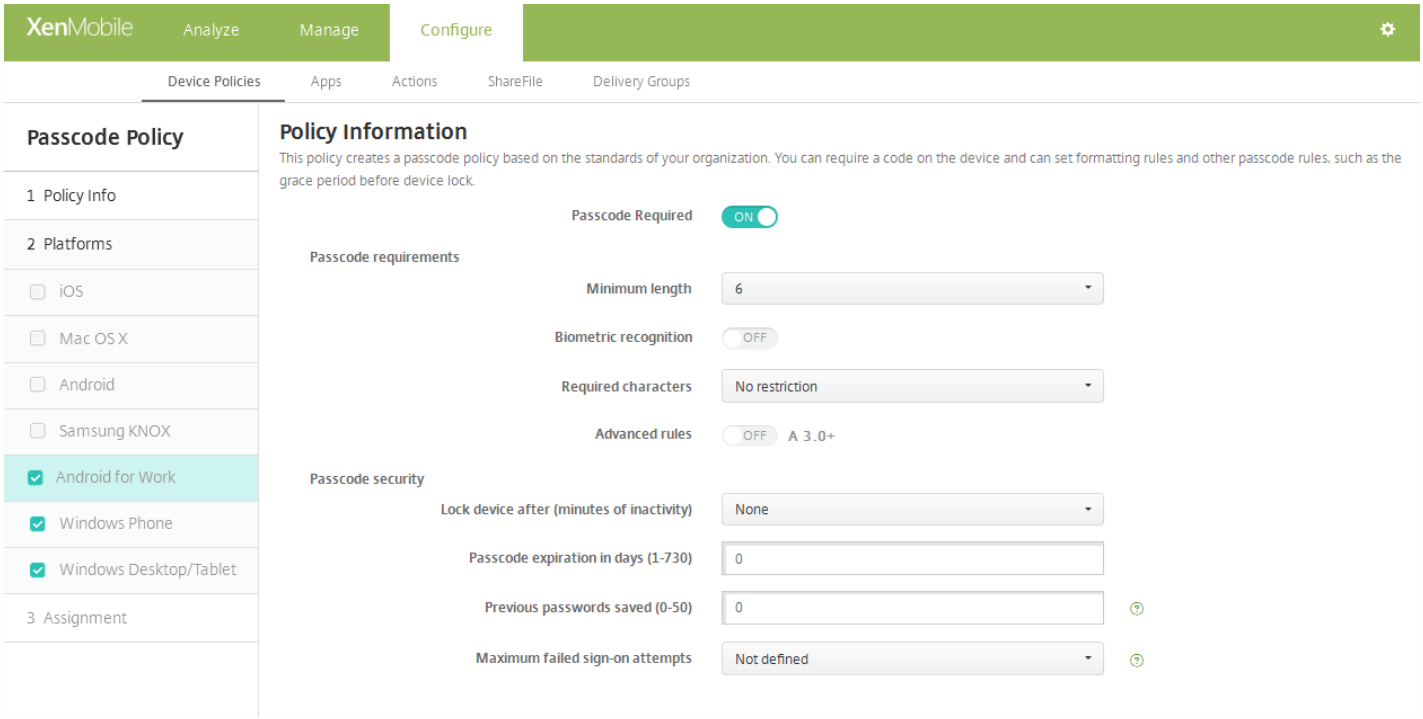
- **Passcodeanforderungen**
  - **Mindestlänge**: Klicken Sie in der Liste auf die Mindestlänge für den Passcode. Der Standardwert ist **6**.
  - **Benutzer dürfen Kennwort anzeigen**: Wählen Sie aus, ob Benutzern das Anzeigen des Kennworts ermöglicht werden soll.
  - **Verbotene Zeichenfolgen**: Durch das Konfigurieren verbotener Zeichenfolgen verhindern Sie, dass Benutzer unsichere, einfach zu erratende Zeichenfolgen ("Kennwort", "Willkommen", "123456", "111111" usw.) verwenden können. Für jede Zeichenfolge, die Sie ausschließen möchten, klicken Sie auf "Hinzufügen" und führen Sie folgende Schritte aus:
    - **Verbotene Zeichenfolgen**: Geben Sie die Zeichenfolge ein, die die Benutzer nicht verwenden dürfen.
    - Klicken Sie auf **Speichern**, um die Zeichenfolge hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

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

      Zum Bearbeiten einer Zeichenfolge 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

- **Mindestanzahl**
  - **Geänderte Zeichen**: Geben Sie an, wie viele Zeichen die Benutzer gegenüber dem vorherigen Passcode ändern müssen. Der Standardwert ist **0**.
  - **Symbole**: Geben Sie die erforderliche Mindestzahl der Symbole in einem Passcode vor. Der Standardwert ist **0**.
- **Maximale Anzahl**
  - **Maximale Häufigkeit**: Geben Sie an, wie oft ein Zeichen in einem Passcode höchstens vorkommen darf. Der Standardwert ist **0**.
  - **Länge der alphabetischen Sequenz**: Geben Sie die maximal zulässige Länge einer Reihe alphabetisch geordneter Zeichen in einem Passcode an. Der Standardwert ist **0**.
  - **Länge der numerischen Sequenz**: 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**.
  - **Passcodeablauf in Tagen (1-730 Tage)**: Geben Sie die Anzahl der Tage ein, nach denen der Passcode ablaufen soll. Gültige Werte sind 1-730. Der Standardwert ist **0**, was bedeutet, dass der Passcode nie abläuft.
  - **Vorherige Kennwörter speichern (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.
  - **Das Gerät wird gesperrt, wenn die Anzahl der fehlgeschlagenen Versuche überschritten wird**: Klicken Sie in der Liste auf die Anzahl fehlgeschlagener Anmeldeversuche, nach denen ein Gerät gesperrt wird. Die Standardeinstellung ist **Nicht definiert**.
  - **Das Gerät wird gelöscht, wenn die Anzahl der fehlgeschlagenen Versuche überschritten wird**: Klicken Sie in der Liste auf die Anzahl fehlgeschlagener Anmeldeversuche, nach denen die Unternehmensdaten von einem Gerät gelöscht werden. Benutzer müssen den KNOX-Container nach dem Löschen neu initialisieren. Die Standardeinstellung ist **Nicht definiert**.

Konfigurieren von Android for Work-Einstellungen

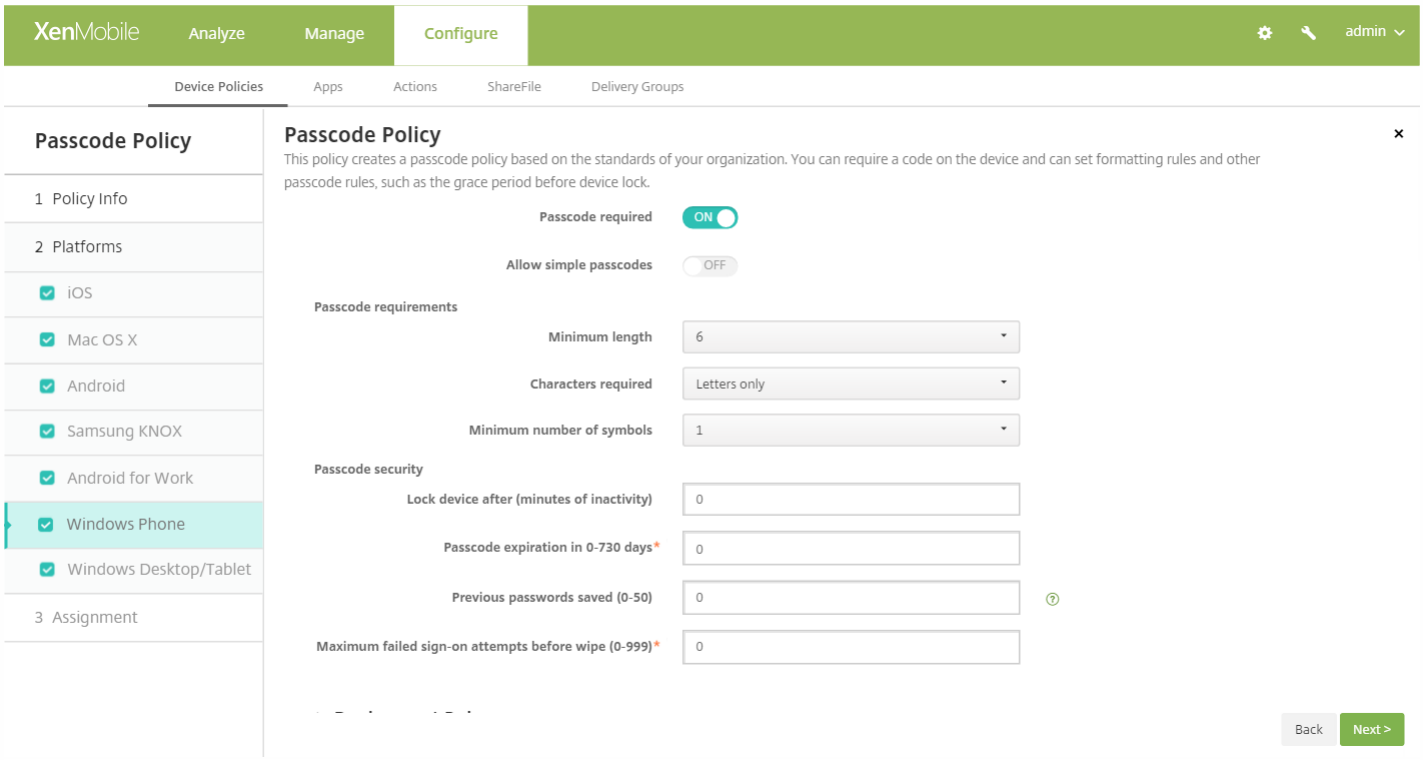


Konfigurieren Sie folgende Einstellungen:

- **Passcode erforderlich**: Wählen Sie diese Option aus, damit ein Passcode erforderlich ist, und um die Konfigurationsoptionen für die Android for Work-Passcoderichtlinie anzuzeigen. Die Seite wird erweitert, damit Sie die Passcodeanforderungen und -sicherheit 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 **Erforderliche Zeichen** ausgeblendet. Der Standardwert ist **AUS**. Dieses Feature wird derzeit nicht unterstützt.
  - **Erforderliche Zeichen**: Klicken Sie in der Liste auf **Keine Einschränkung**, **Ziffern und Buchstaben**, **Nur Ziffern** oder **Nur Buchstaben**, um die Zusammensetzung des Passcodes vorzugeben. Der Standardwert ist **No restriction**.
  - **Erweiterte Regeln**: Wählen Sie aus, ob erweiterte Passcoderegeln angewendet werden sollen. Diese Option steht für Geräte mit Android-Versionen vor 5.0 nicht zur Verfügung. Der Standardwert ist **AUS**.
  - Wenn Sie **Erweiterte Regeln** aktivieren, 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**.
  - **Passcodeablauf in Tagen (1-730 Tage)**: Geben Sie die Anzahl der Tage ein, nach denen der Passcode ablaufen soll. Gültige Werte sind 1-730. Der Standardwert ist **0**, was bedeutet, dass der Passcode nie abläuft.

- **Vorherige Kennwörter speichern (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 der KNOX-Container und die KNOX-Daten von einem Gerät gelöscht werden. Benutzer müssen den KNOX-Container nach dem Löschen neu initialisieren. Die Standardeinstellung ist **Nicht definiert**.

Konfigurieren von Windows Phone-Einstellungen

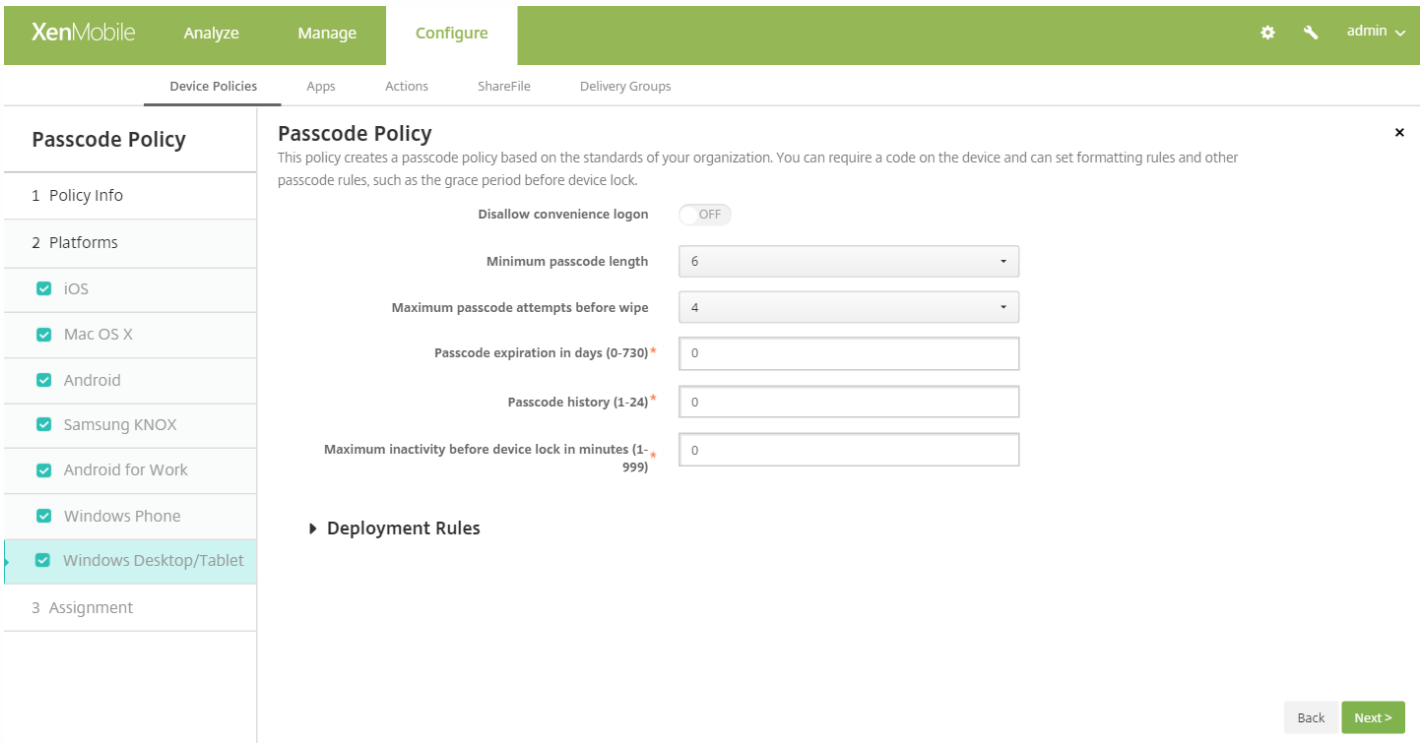


Konfigurieren Sie folgende Einstellungen:

- **Passcode erforderlich**: Deaktivieren Sie diese Option, wenn für Windows Phone-Geräte kein Passcode erforderlich sein soll. Die Standardeinstellung ist **EIN**, ein Passcode ist also erforderlich. Die Seite wird verkleinert und die nachfolgend aufgeführten Optionen werden ausgeblendet, wenn Sie diese Einstellung nicht aktivieren.
- **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)**: Geben Sie die Anzahl der Minuten ein, die ein Gerät inaktiv sein darf, bevor es gesperrt wird. Der Standardwert ist **0**.
  - **Passcodeablauf in 0-730 Tagen**: Geben Sie die Anzahl der Tage ein, nach denen der Passcode ablaufen soll. Gültige Werte sind 0-730. Der Standardwert ist **0**, was bedeutet, dass der Passcode nie abläuft.

- **Vorherige Kennwörter speichern (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.
- **Löschen nach (0-999) Anmeldeversuchsfehlern**: Geben Sie die Anzahl fehlgeschlagener Anmeldeversuche ein, nach der die Unternehmensdaten vom Gerät gelöscht werden. Der Standardwert ist **0**.

Konfigurieren von Windows Desktop-/Tablet-Einstellungen

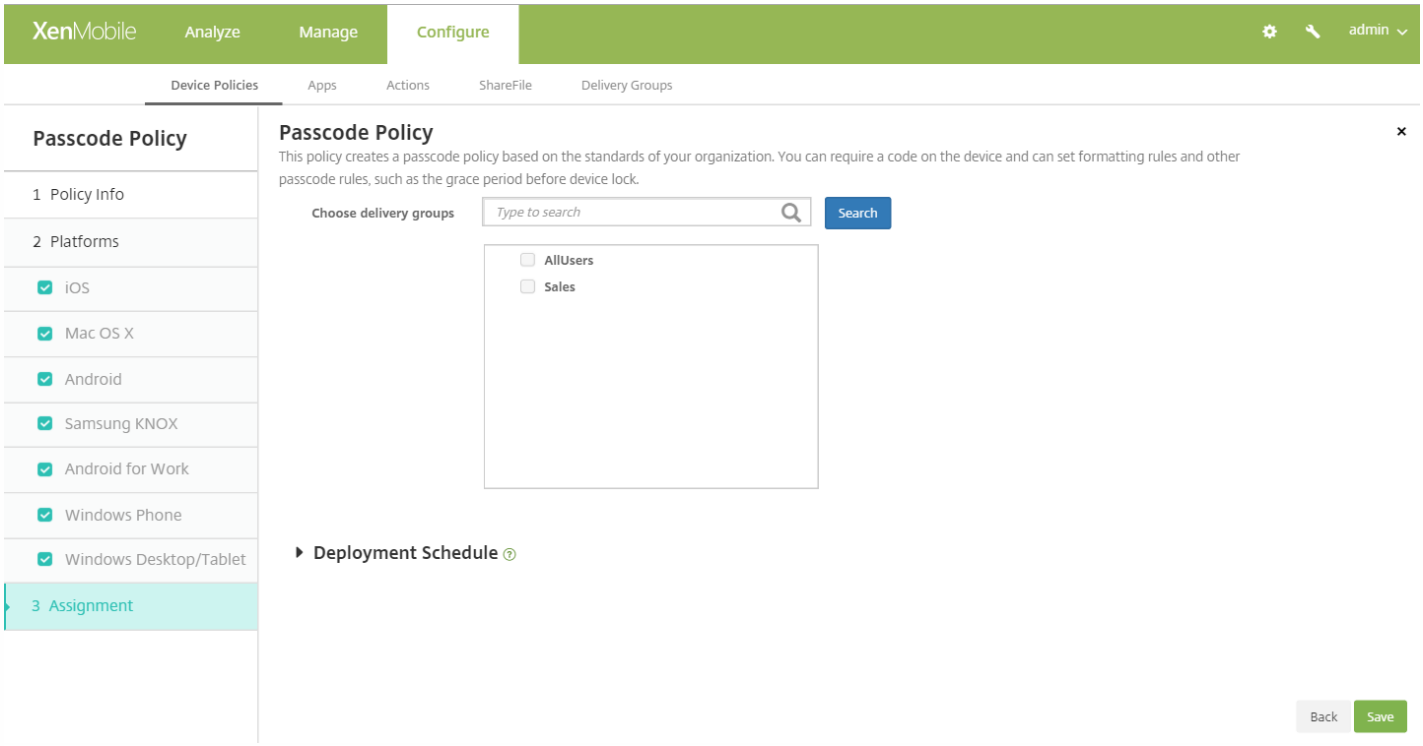


Konfigurieren Sie folgende Einstellungen:

- **Komfortanmeldung nicht zulassen**: Wählen Sie aus, ob Benutzern der Zugriff auf ihre Geräte über Bildkennwörter oder Biometrieanmeldungen gestattet werden soll. Der Standardwert ist **AUS**.
- **Mindestlänge für Passcode**: Klicken Sie in der Liste auf die Mindestlänge für den Passcode. Der Standardwert ist **6**.
- **Maximale Passcodeversuche vor Löschen**: Klicken Sie in der Liste auf die Anzahl fehlgeschlagener Anmeldeversuche, nach der die Unternehmensdaten vom Gerät gelöscht werden. Der Standardwert ist **4**.
- **Passcodeablauf in Tagen (0-730 Tage)**: Geben Sie die Anzahl der Tage ein, nach denen der Passcode ablaufen soll. Gültige Werte sind 0-730. Der Standardwert ist **0**, was bedeutet, dass der Passcode nie abläuft.
- **Passcodeverlauf (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. Der Standardwert ist **0**.
- **Maximale Inaktivität in Minuten, bevor Gerät gesperrt wird (1-999)**: Geben Sie den Zeitraum in Minuten an, während dessen ein Gerät inaktiv sein darf, bevor es gesperrt wird. Gültige Werte sind 1-999. Sie müssen eine Zahl zwischen 1 und 999 in diesem Feld eingeben. Der Standardwert ist **0**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Passcoderichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Richtlinien für persönliche Hotspots

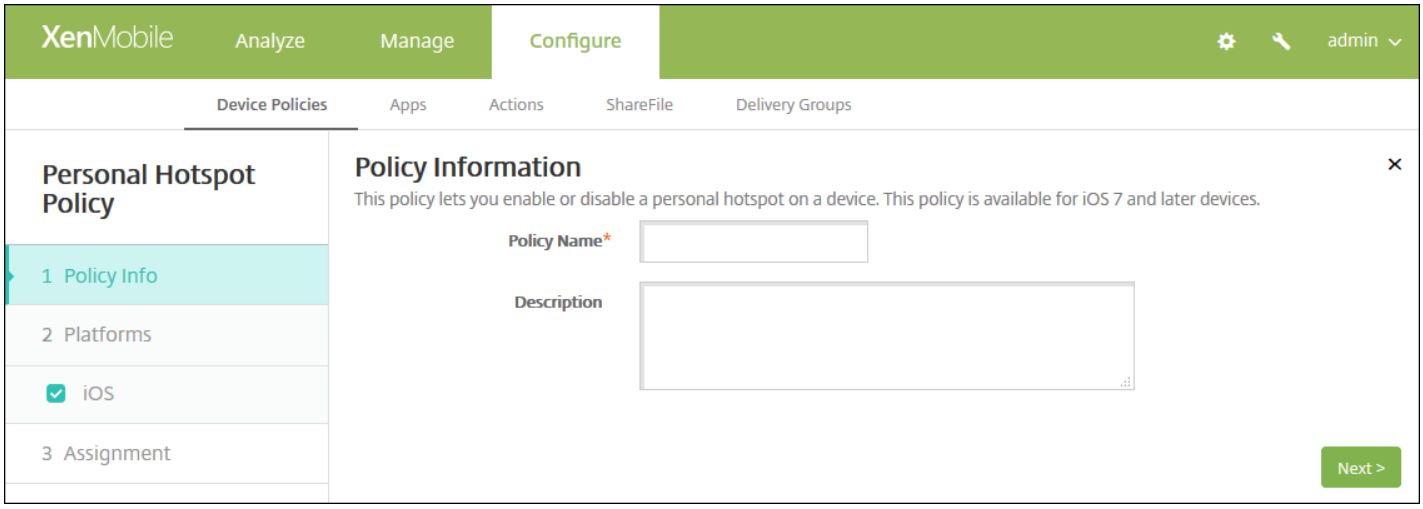
Jul 28, 2016

Sie können zulassen, dass Benutzer mit dem iOS-Feature für persönliche Hotspots eine Verbindung mit dem Internet per Mobilfunknetz herstellen, wenn sie nicht im Bereich eines WiFi-Netzwerks sind. Verfügbar für iOS 7.0 und höher.

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

2. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.

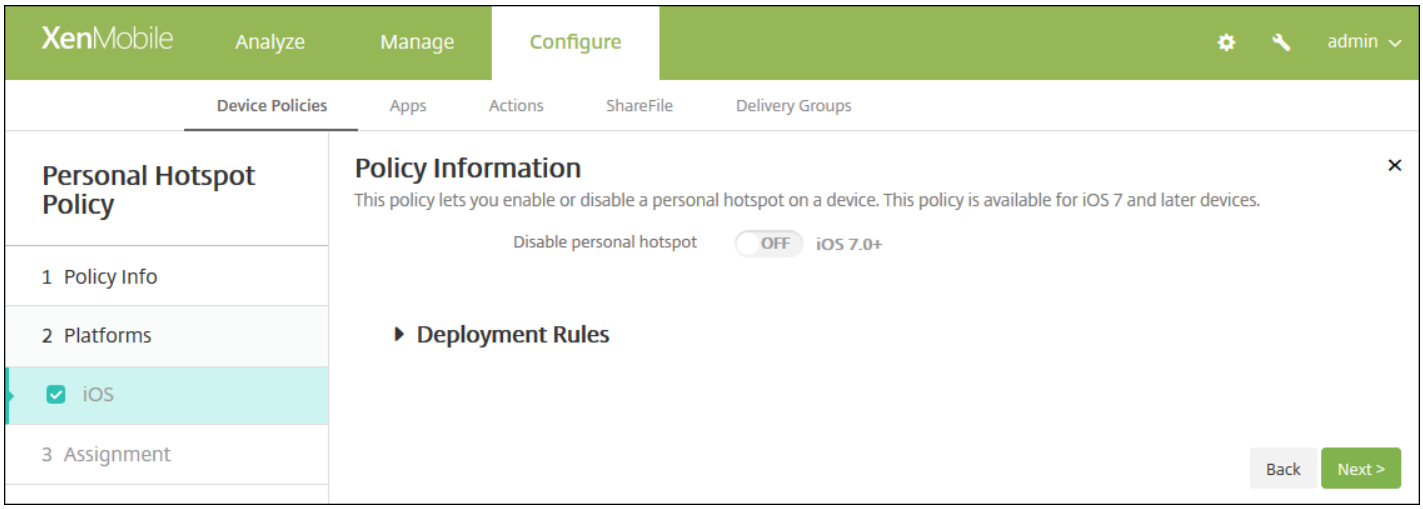
3. Erweitern Sie **Mehr** und klicken Sie unter **Netzwerkzugriff** auf **Persönlicher Hotspot**. Die Seite **Persönlicher Hotspot** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite mit den Plattforminformationen für **iOS** wird angezeigt.

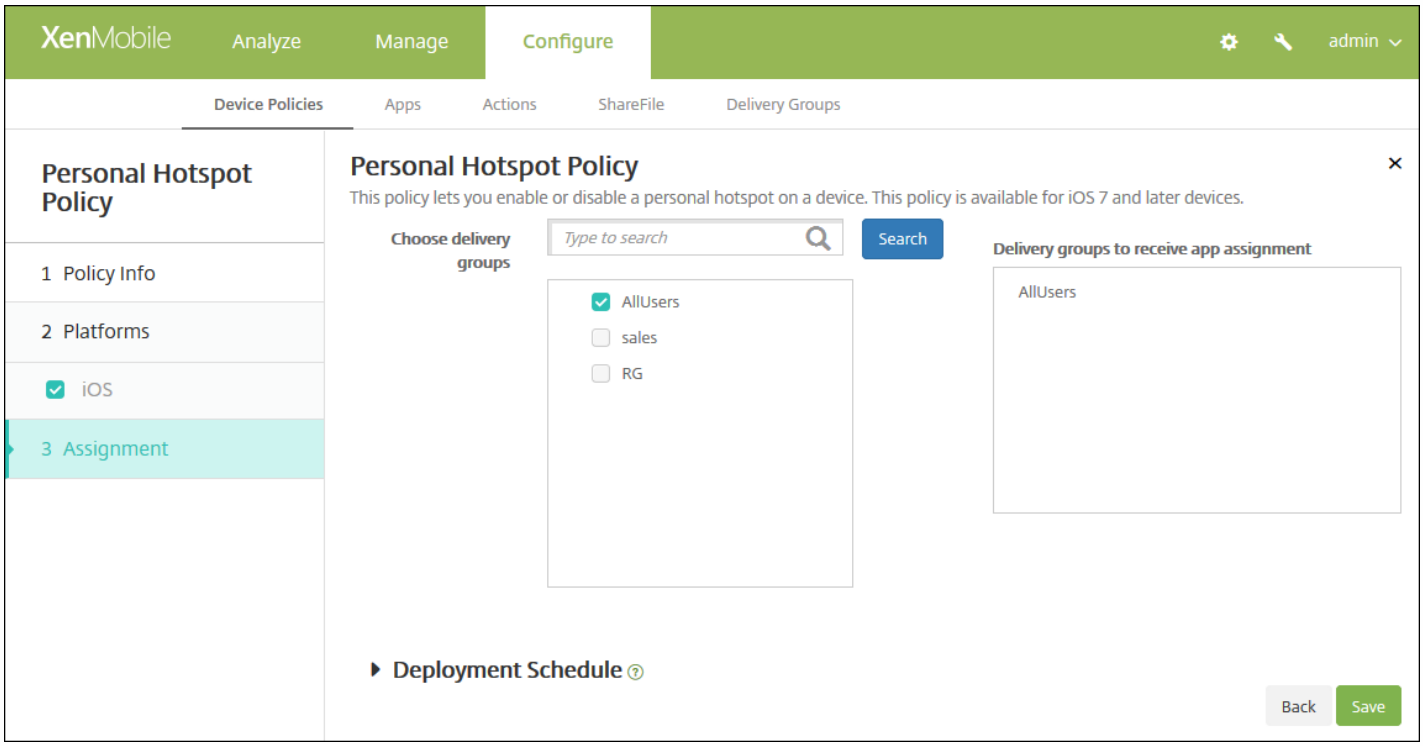


6. Konfigurieren Sie folgende Einstellung:

- **Persönlichen Hotspot deaktivieren**: Wählen Sie aus, ob das Feature für persönliche Hotspots auf den Geräten aktiviert oder deaktiviert werden soll. Die Standardeinstellung ist **AUS**, d. h. die persönlichen Hotspots werden deaktiviert. Die Richtlinie deaktiviert das Feature nicht. Die Benutzer können persönliche Hotspots weiterhin verwenden, doch wenn die Richtlinie bereitgestellt wird, wird der persönliche Hotspot deaktiviert, sodass er nicht standardmäßig aktiviert bleibt.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Richtlinien zum Entfernen von Profilen

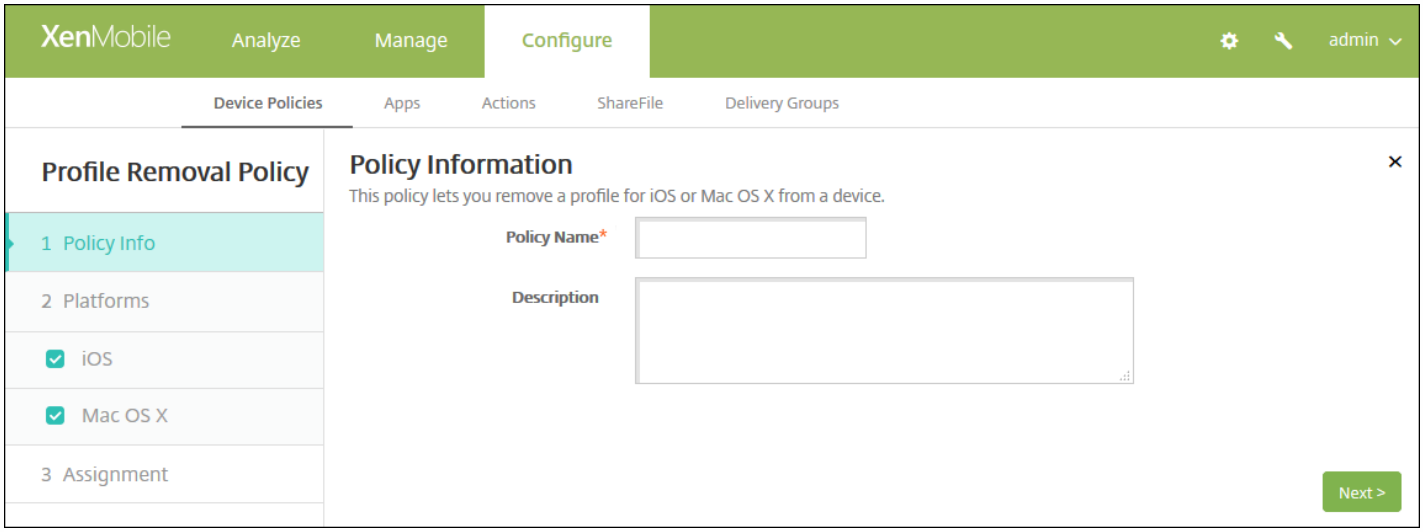
Jul 28, 2016

Sie können eine Richtlinie zum Entfernen von App-Profilen in XenMobile erstellen. Bei ihrer Bereitstellung entfernt die Richtlinie das App-Profil von iOS- bzw. Mac OS X-Geräten.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie dann unter **Entfernen** auf **Profilentfernung**. Die Seite **Profilentfernung** wird angezeigt.



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

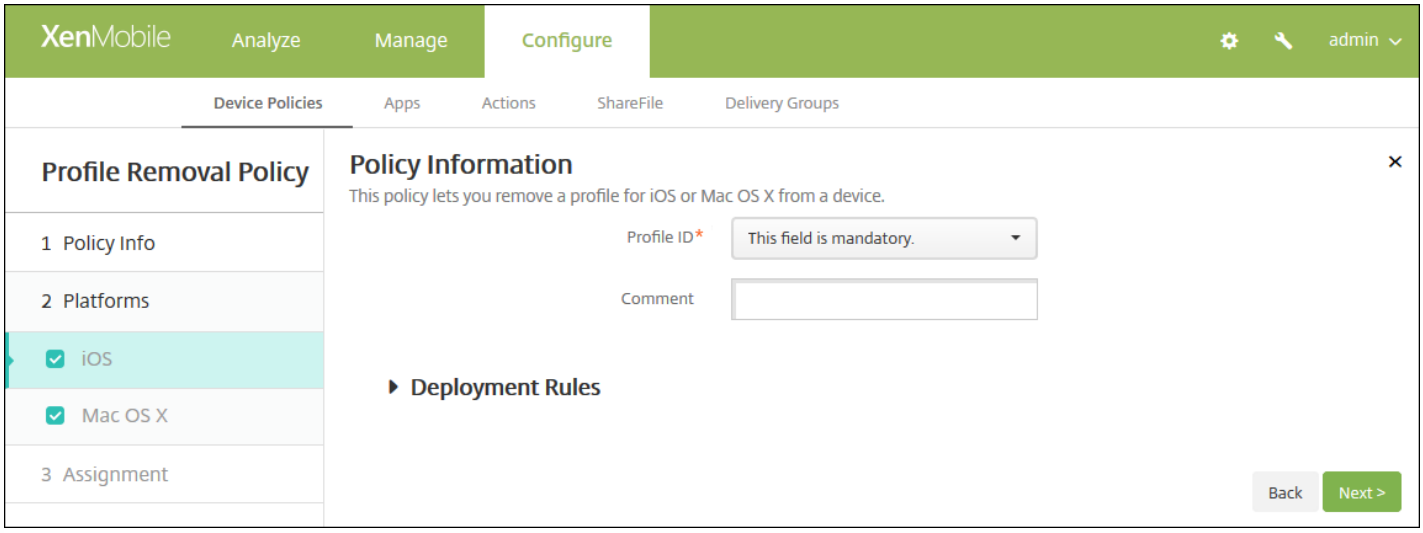
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

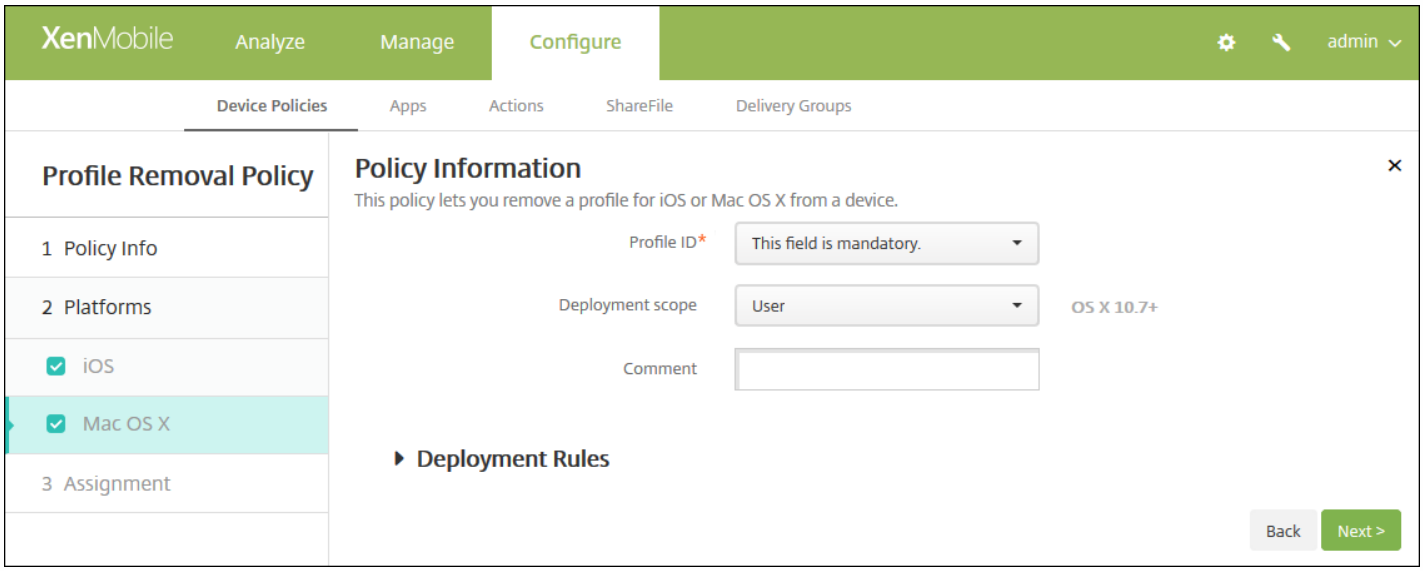
Konfigurieren der iOS-Einstellung



Konfigurieren Sie folgende Einstellungen:

- **Profil-ID**: Klicken Sie in der Liste auf die ID des App-Profils. Diese Angabe ist erforderlich.
- **Kommentar**: Geben Sie optional einen Kommentar ein.

Konfigurieren von Mac OS X-Einstellungen

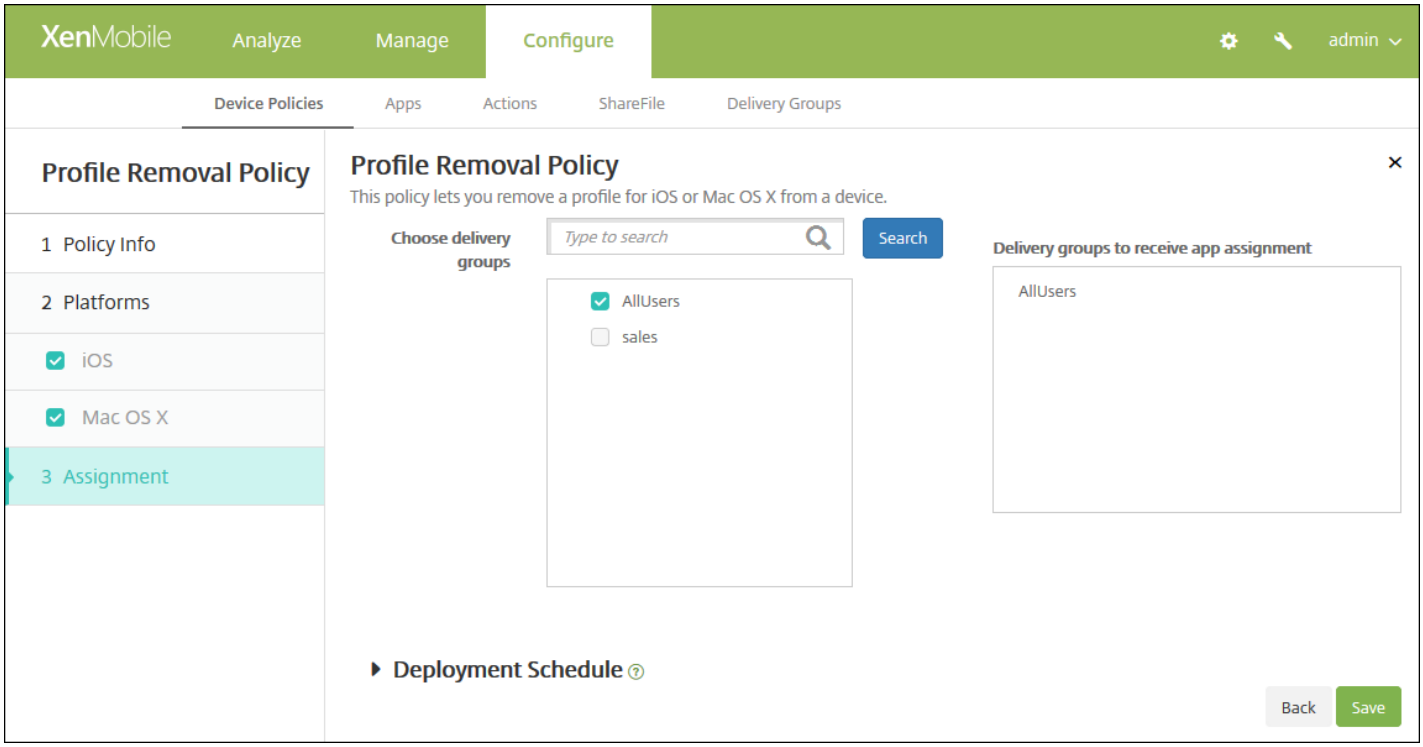


Konfigurieren Sie folgende Einstellungen:

- **Profil-ID**: Klicken Sie in der Liste auf die ID des App-Profils. Diese Angabe ist erforderlich.
- **Bereitstellungsumfang**: Klicken Sie in der Liste auf **Benutzer** oder **System**. Der Standardwert ist **Benutzer**. Diese Option ist nur für OS X 10.7 und höher verfügbar.
- **Kommentar**: Geben Sie optional einen Kommentar ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Profilentfernungsrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen gemachten Änderungen werden auf alle Plattformen angewendet. Ausnahme bildet die Einstellung **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Provisioningprofilrichtlinie

Jul 28, 2016

Beim Entwickeln und Signieren einer iOS-Unternehmensapp wird normalerweise ein Provisioningprofil eingeschlossen, das gemäß Apple für die Ausführung der App auf iOS-Geräten erforderlich ist. Wenn das Provisioningprofil fehlt oder abgelaufen ist, stürzt die App ab, wenn der Benutzer darauf tippt.

Das Hauptproblem bei Provisioningprofilen besteht darin, dass sie ein Jahr, nachdem sie im Apple Developer-Portal generiert wurden, ablaufen und Sie die Ablaufdaten für alle Provisioningprofile auf allen registrierten iOS-Geräten nachverfolgen müssen. Zur Nachverfolgung von Ablaufdaten müssen Sie nicht nur die Daten selbst im Auge behalten, sondern auch wissen, welche Benutzer welche Version der einzelnen Apps verwenden. Zwei Lösungen bestehen darin, Provisioningprofile per E-Mail an die Benutzer zu senden oder sie über ein Webportal für Download und Installation zur Verfügung zu stellen. Beide funktionieren zwar, sind jedoch fehleranfällig, da Benutzer auf Anweisungen in einer E-Mail reagieren müssen oder das Webportal besuchen und das richtige Profil herunterladen und installieren müssen.

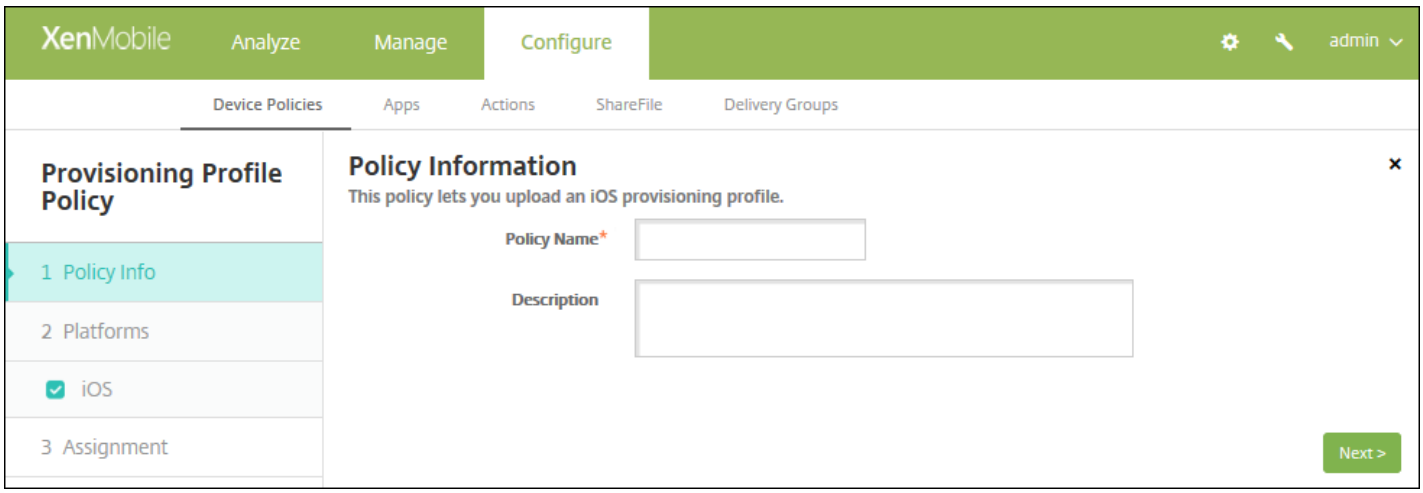
Um die Benutzer mit diesem Vorgang nicht zu behelligen, können Sie in XenMobile Provisioningprofile über Geräterichtlinien installieren und entfernen. Fehlende oder abgelaufene Profile werden nach Bedarf entfernt und aktuelle Profile auf den Geräten installiert, sodass Apps bei Antippen normal geöffnet und verwendet werden können.

Vor dem Erstellen einer Provisioningprofilrichtlinie müssen Sie eine Provisioningprofildatei erstellen. Weitere Informationen finden Sie in dem Artikel zum Erstellen von Provisioningprofilen auf der Apple Developer-Website.

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

2. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.

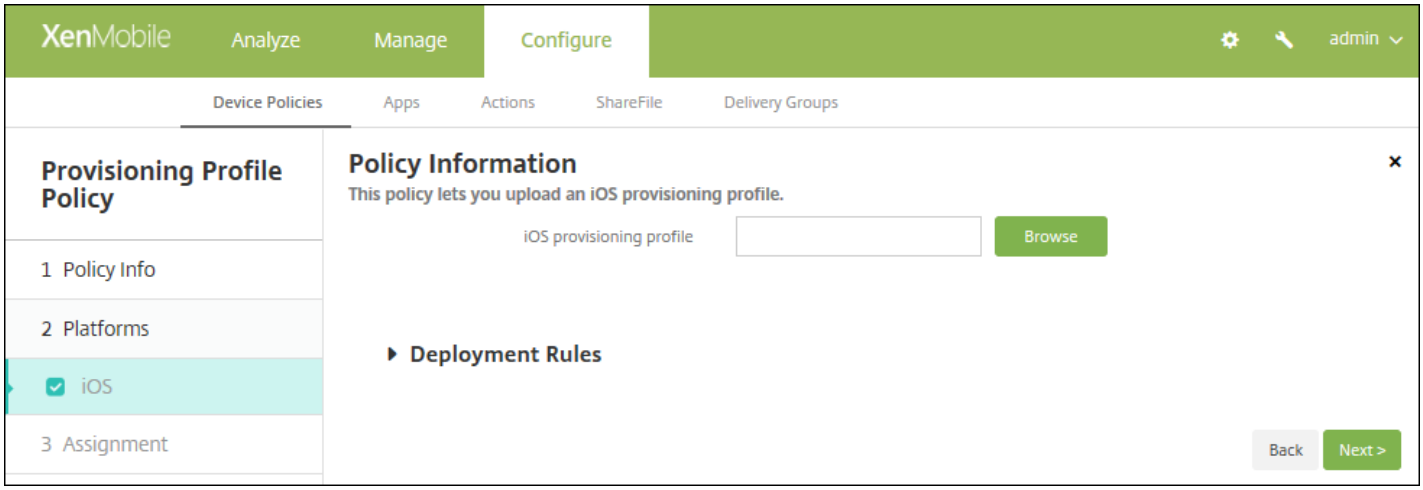
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Provisioningprofil**. Die Seite **Provisioningprofil** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite mit den Plattforminformationen für **iOS** wird angezeigt.

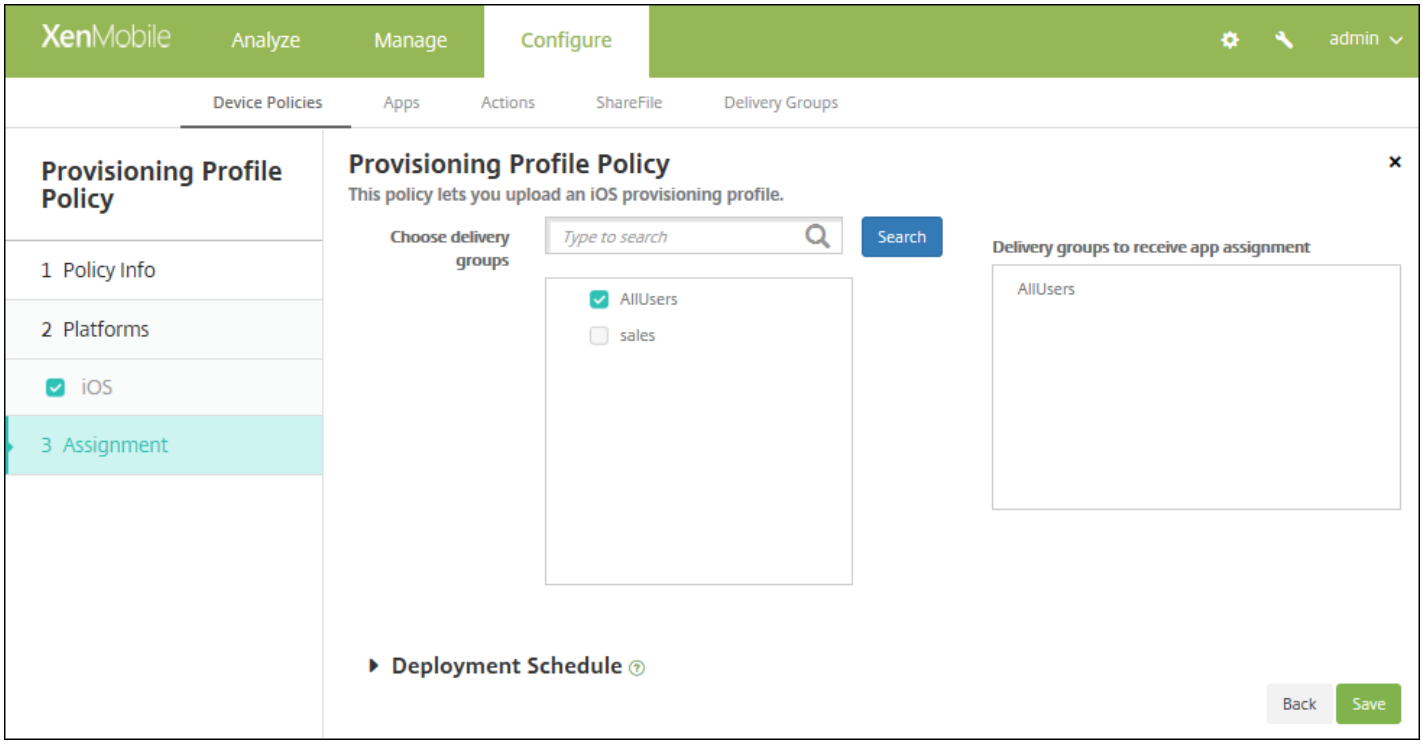


6. Konfigurieren Sie folgende Einstellung:

- **iOS-Provisioningprofil** Klicken Sie auf **Durchsuchen**, navigieren Sie zu der Provisioningprofildatei und wählen Sie diese aus.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Provisioningprofilrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Richtlinie zum Entfernen von Provisioningprofilen

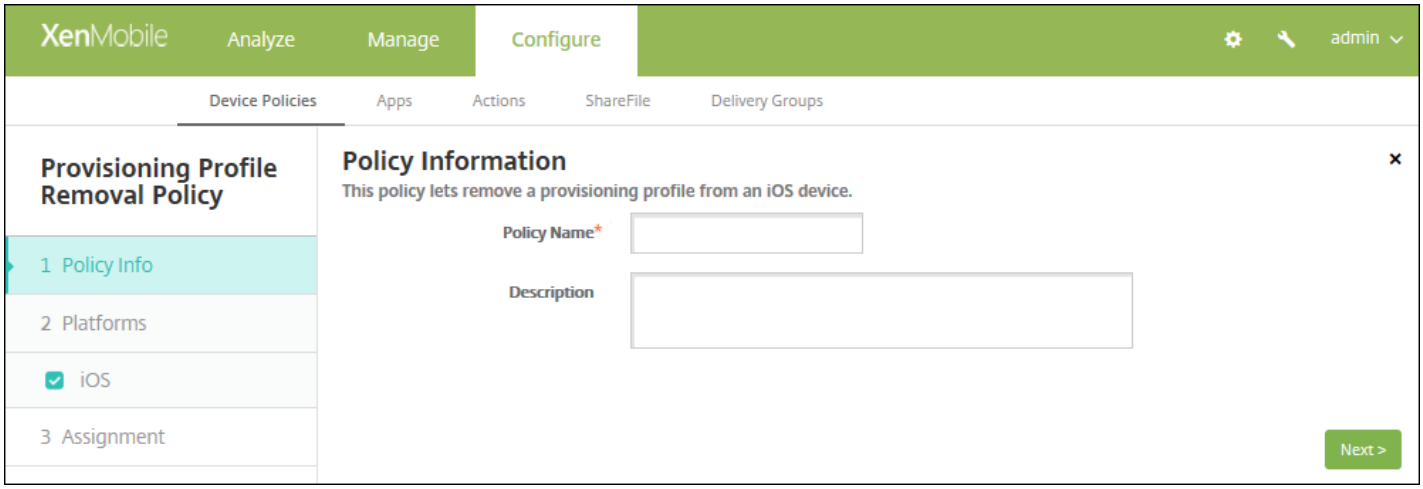
Jul 28, 2016

Sie können iOS-Provisioningprofile mit Geräterichtlinien entfernen. Weitere Informationen zu Provisioningprofilen finden Sie unter Hinzufügen von Provisioningprofilen.

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

2. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.

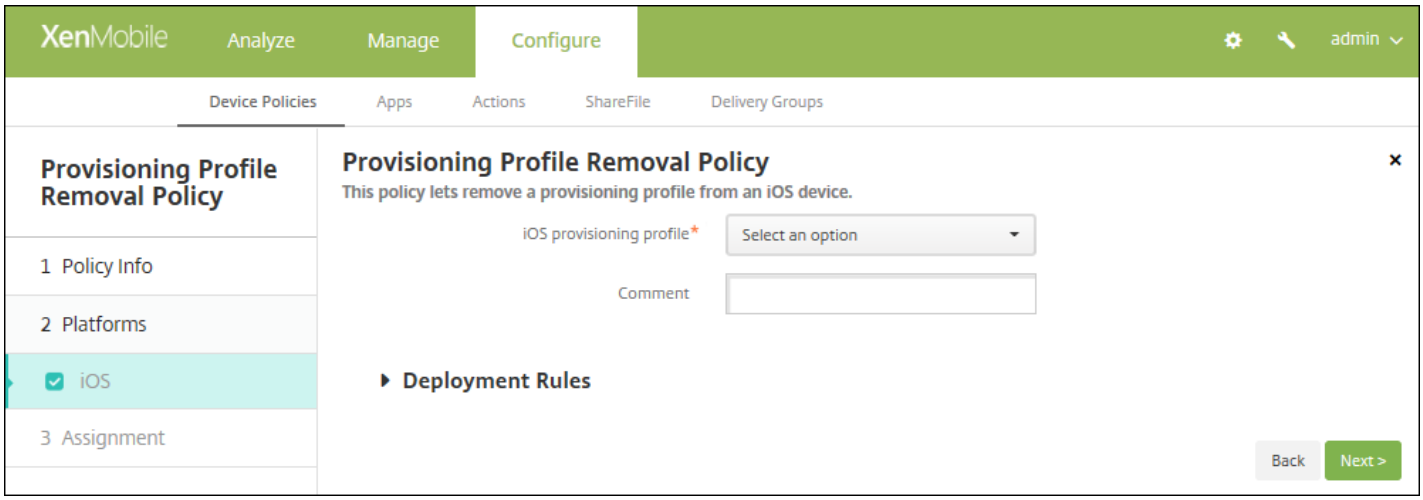
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Entfernen** auf **Entfernen des Provisioningprofils**. Die Seite **Richtlinieninformationen** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Plattformseite wird angezeigt.

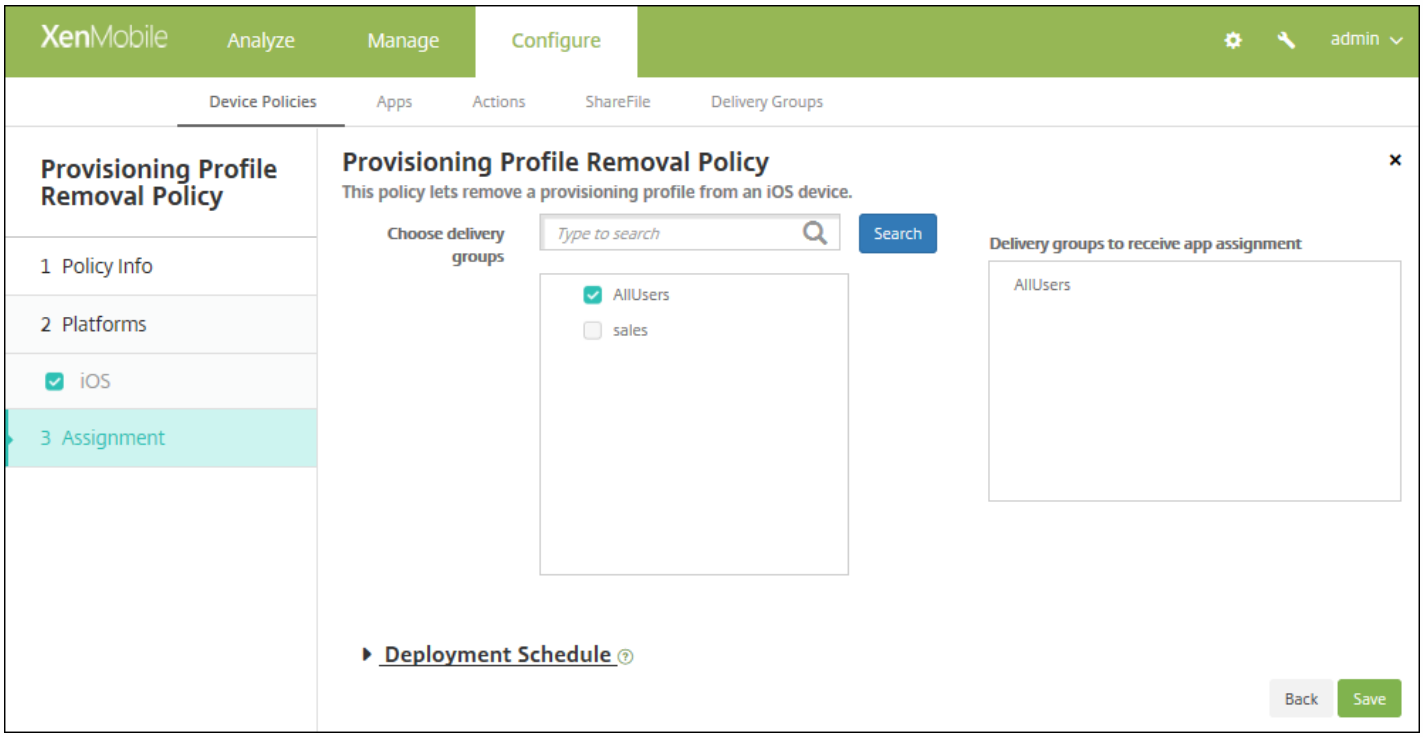


6. Konfigurieren Sie die folgenden Einstellungen:

- **iOS-Provisioningprofil**: Klicken Sie in der Liste auf das Provisioningprofil, das Sie entfernen möchten.
- **Kommentar**: Geben Sie optional einen Kommentar ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.

- 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.

11. Klicken Sie auf **Speichern**.

Proxy-Geräterichtlinien

Jul 28, 2016

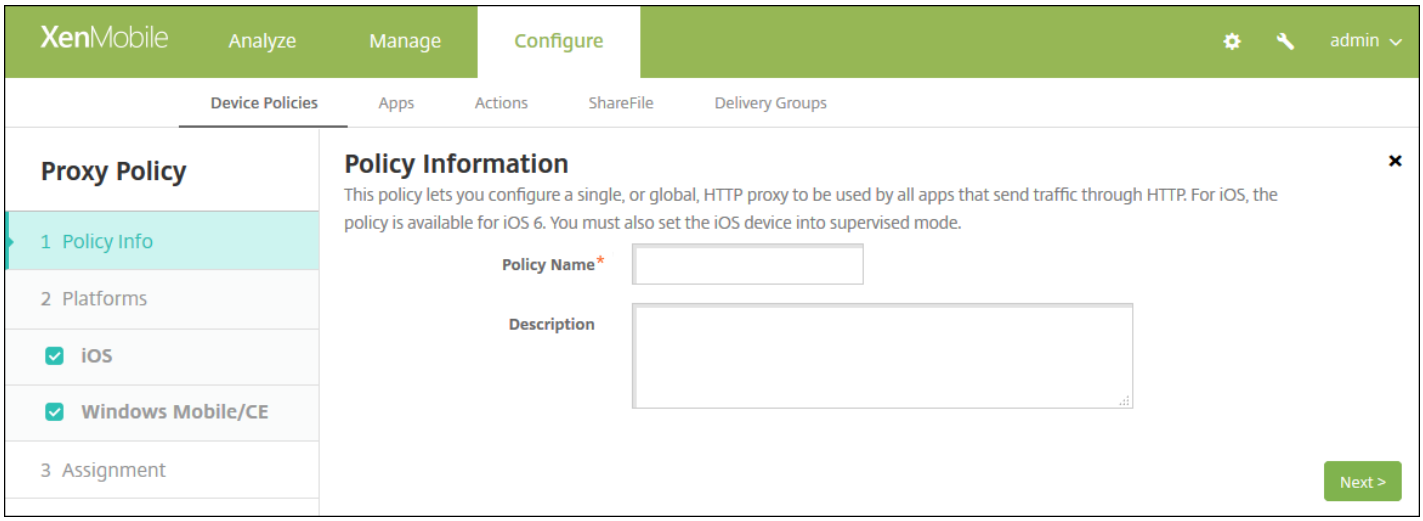
Sie können in XenMobile eine Richtlinie zum Festlegen globaler HTTP-Proxy-Einstellungen für Geräte mit Windows Mobile/CE oder iOS 6.0 oder höher hinzufügen. Sie können nur eine globale HTTP-Proxyrichtlinie pro Gerät bereitstellen.

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 Versetzen von iOS-Geräten mit dem Apple Configurator in den betreuten Modus.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Klicken Sie auf **Mehr** und dann unter **Netzwerkzugriff** auf **Proxy**. Die Seite mit den Richtlinieninformationen für **Proxy** wird angezeigt.



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

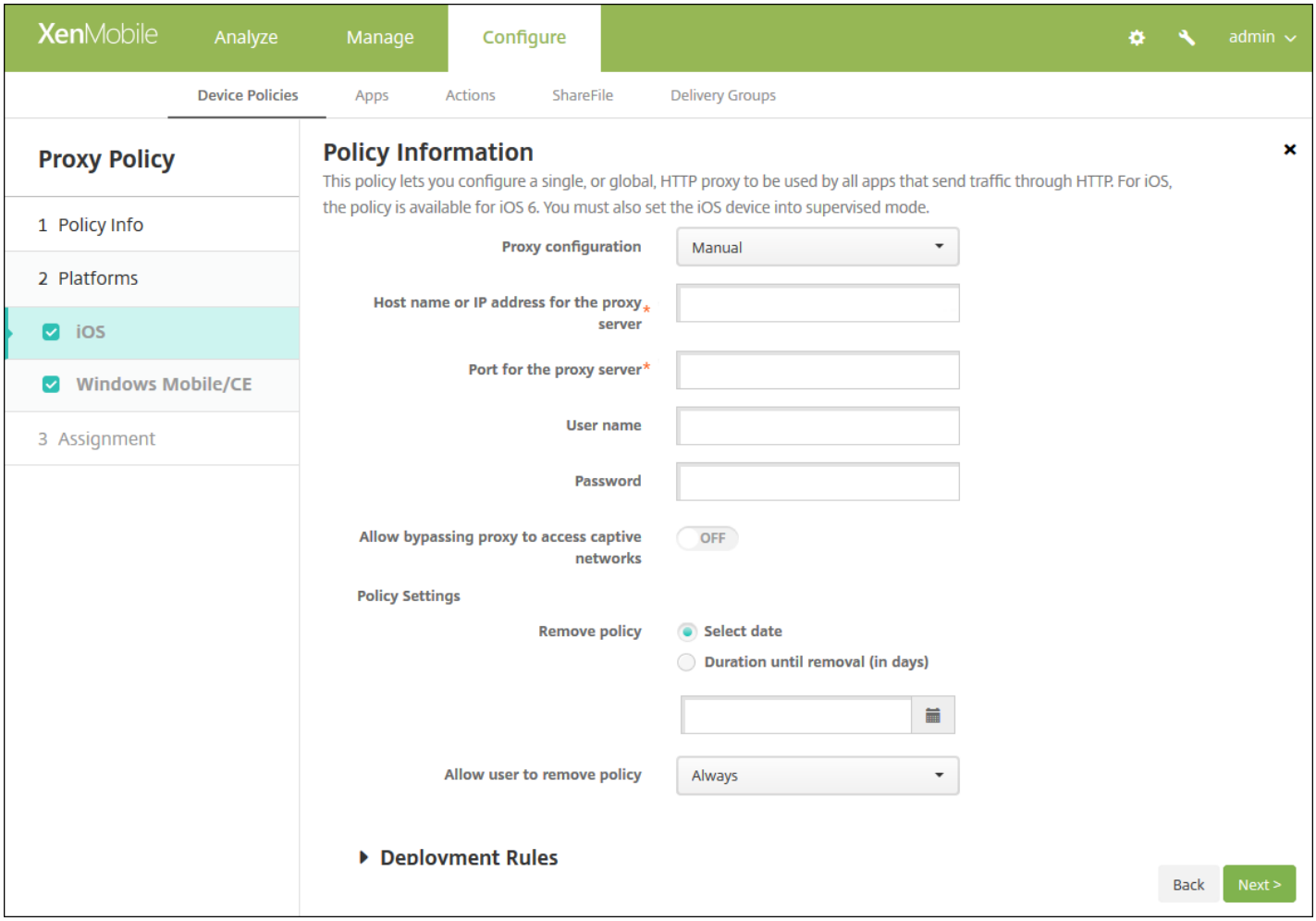
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

Konfigurieren von iOS-Einstellungen

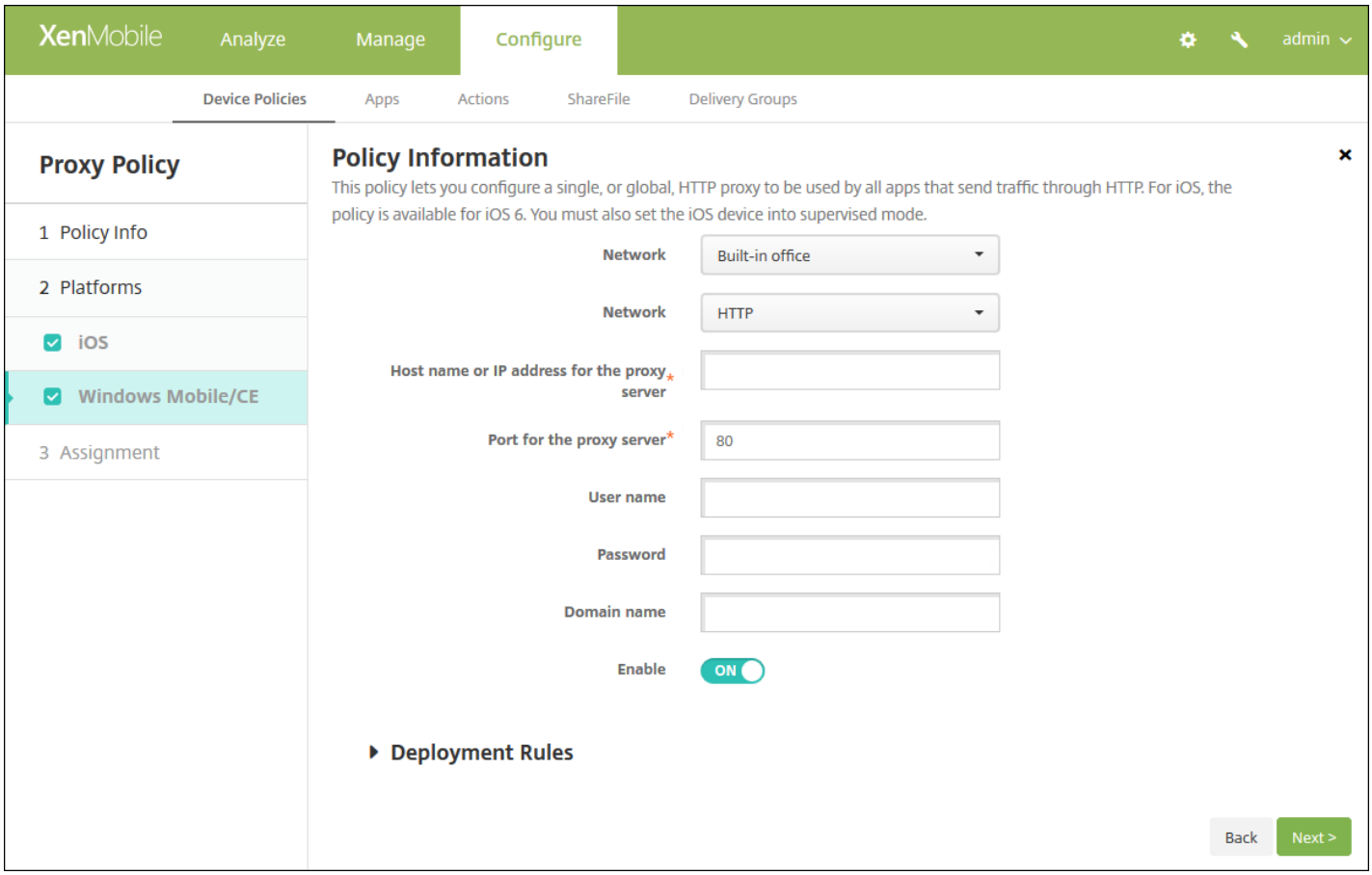


Konfigurieren Sie folgende Einstellungen:

- **Proxykonfiguration**: Klicken Sie auf **Manuell** oder **Automatisch**, um festzulegen, wie der Proxy auf den Geräten der Benutzer konfiguriert wird.
  - Bei Auswahl von **Manuell** konfigurieren Sie die folgenden Einstellungen:
    - **Hostname oder IP-Adresse des Proxyservers**: Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers ein. Diese Angabe ist erforderlich.
    - **Port für den Proxyserver**: Geben Sie die Portnummer des Proxyservers ein. Diese Angabe ist erforderlich.
    - **Benutzername**: Geben Sie optional einen Benutzernamen für die Authentifizierung beim Proxyserver ein.
    - **Kennwort**: Geben Sie optional ein Kennwort für die Authentifizierung beim Proxyserver ein.
  - Bei Auswahl von **Automatisch** konfigurieren Sie die folgenden Einstellungen:
    - **Proxy-PAC-URL**: Geben Sie die URL der PAC-Datei zur Bestimmung der Proxykonfiguration ein.
    - **Direkte Verbindung zulassen, wenn PAC nicht erreichbar ist**: Wählen Sie aus, ob Benutzer eine direkte Verbindung mit dem Ziel herstellen dürfen, wenn die PAC-Datei nicht erreichbar ist. Die Standardeinstellung ist **EIN**. Diese Option ist nur für iOS 7.0 und höher verfügbar.
- **Proxyumgehung zulassen für Zugriff auf Captive-Netzwerke**: Wählen Sie aus, ob die Proxyumgehung für den Zugriff auf Captive-Netzwerke zulässig sein soll. Der Standardwert ist **AUS**.
- **Richtlinieneinstellungen**
  - Klicken Sie für **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.

- Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Kennwort erforderlich** oder **Nie**.
- Bei Auswahl von **Kennwort erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

Konfigurieren von Windows Mobile-/CE-Einstellungen



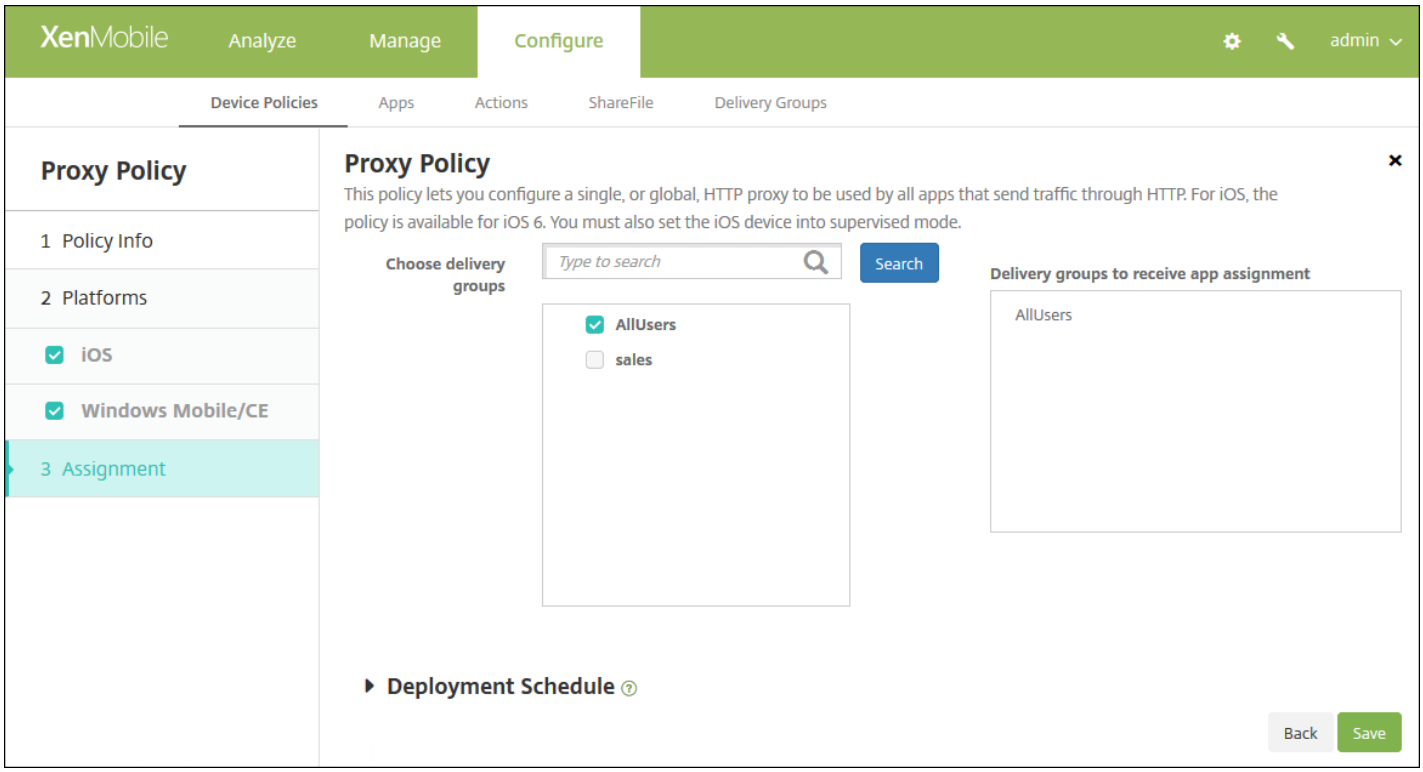
Konfigurieren Sie folgende Einstellungen:

- **Netzwerk**: Klicken Sie in der Liste auf den gewünschten Netzwerktyp. Der Standardwert ist **Büro (integriert)**. Mögliche Optionen:
  - Benutzerdefiniertes Büro
  - Benutzerdefiniertes Internet
  - Büro (integriert)
  - Internet (integriert)
- **Netzwerk**: Klicken Sie in der Liste auf das gewünschte Verbindungsprotokoll. Der Standardwert ist **HTTP**. Mögliche Optionen:
  - HTTP
  - WAP
  - Socks 4
  - Socks 5
- **Hostname oder IP-Adresse des Proxyservers**: Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers ein. Diese Angabe ist erforderlich.
- **Port für den Proxyserver**: Geben Sie die Portnummer des Proxyservers ein. Diese Angabe ist erforderlich. Der Standardwert ist **80**.

- **Benutzername**: Geben Sie optional einen Benutzernamen für die Authentifizierung beim Proxyserver ein.
- **Kennwort**: Geben Sie optional ein Kennwort für die Authentifizierung beim Proxyserver ein.
- **Domänenname**: Geben Sie optional einen Domänennamen ein.
- **Aktivieren**: Wählen Sie aus, ob der Proxyserver aktiviert werden soll. Die Standardeinstellung ist **EIN**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Proxyrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im

Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.

- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen gemachten Änderungen werden auf alle Plattformen angewendet. Ausnahme bildet die Einstellung **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Registrierungsrichtlinie

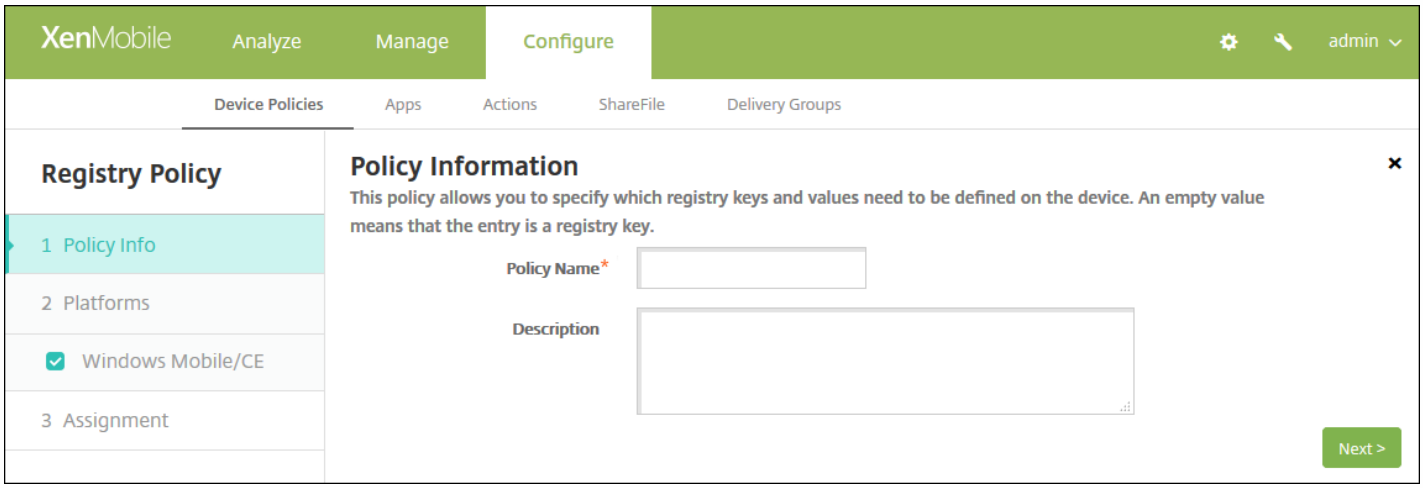
Jul 28, 2016

In der Registrierung von Windows Mobile und Windows CE werden Daten zu Apps, Treibern, Benutzereinstellungen und Konfigurationseinstellungen gespeichert. Sie können in XenMobile Registrierungsschlüssel und -werte zum Verwalten von Windows Mobile-/CE-Geräten definieren.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

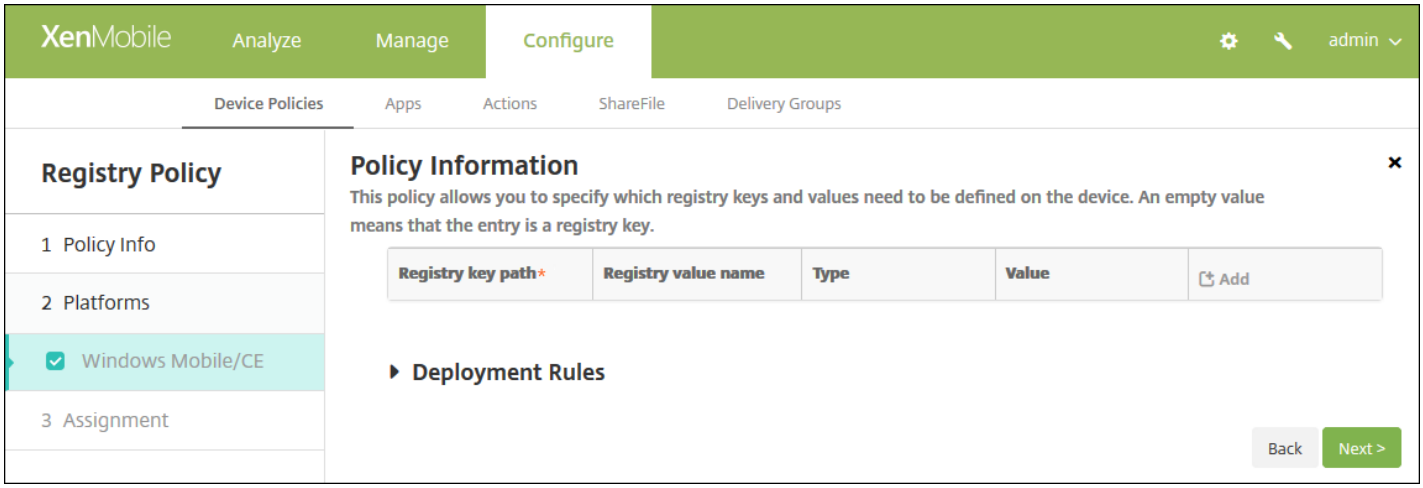
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Benutzerdefiniert** auf **Registrierung**. Die Seite **Registrierung** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite **Windows Mobile/CE** wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:

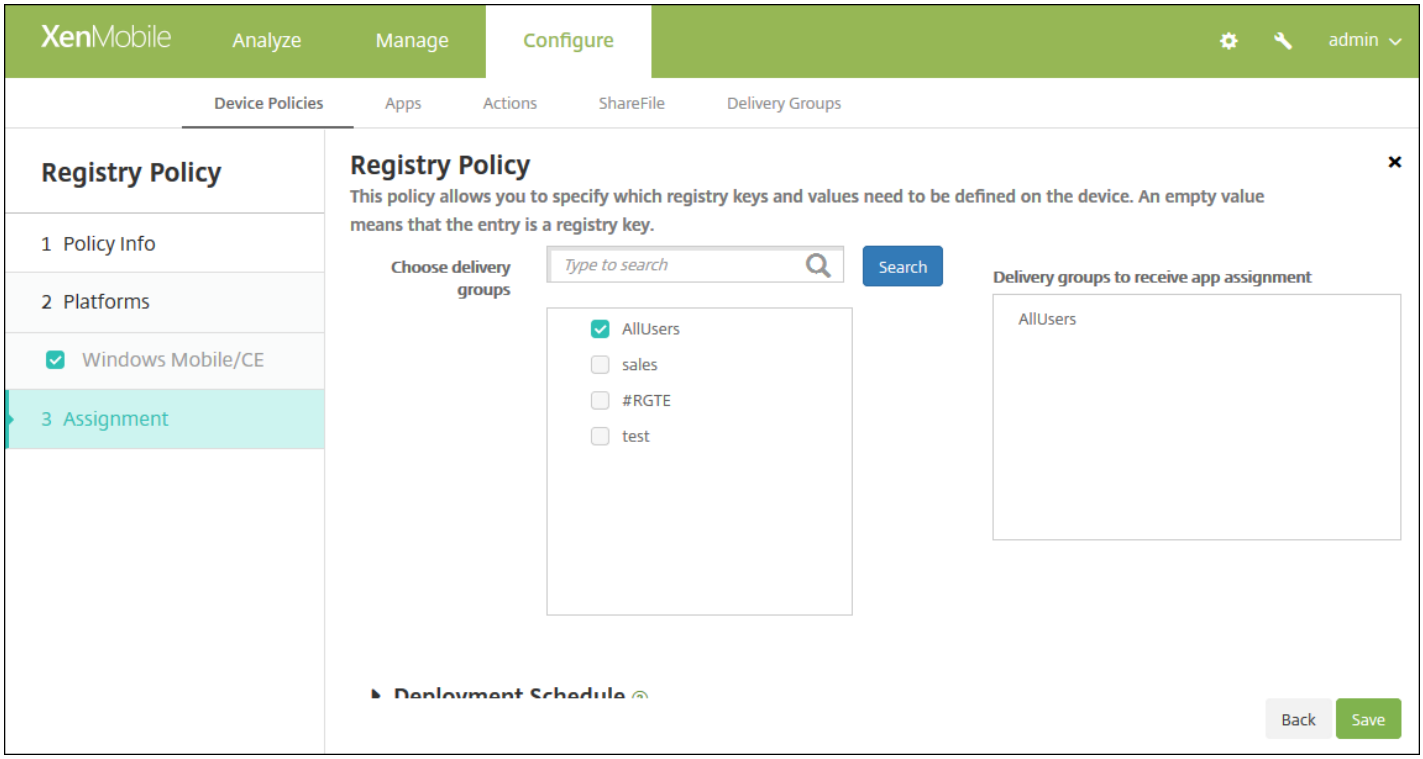
- Klicken Sie für jeden Registrierungsschlüssel bzw. jedes Schlüssel/Wert-Paar, das Sie hinzufügen möchten, auf **Hinzufügen** und führen Sie folgende Schritte aus:
- **Registrierungsschlüsselpfad**: Geben Sie den vollständigen Pfad des Registrierungsschlüssels ein. Geben Sie beispielsweise *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows* ein, um den Pfad des Windows-Schlüssels des HKEY_LOCAL_MACHINE-Stammschlüssels anzugeben.
- **Registrierungswertname**: Geben Sie den Namen des Registrierungsschlüsselwerts ein. Geben Sie beispielsweise *ProgramFilesDir* ein, um diesen Wertnamen dem Registrierungsschlüsselpfad "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion" hinzuzufügen. Wenn Sie dieses Feld leer lassen, bedeutet dies, dass Sie einen Registrierungsschlüssel und kein Schlüssel/Wert-Paar hinzufügen.
- **Typ**: Klicken Sie in der Liste auf den Datentyp für den Wert. Die Standardeinstellung ist **DWORD**. Mögliche Optionen:
  - **DWORD**: 32-Bit-Ganzzahl ohne Vorzeichen
  - **Zeichenfolge**: beliebige Zeichenfolge
  - **Erweiterte Zeichenfolge**: Zeichenfolge, die Umgebungsvariablen enthalten kann, z. B. %TEMP% oder %USERPROFILE%
  - **Binär**: beliebige Binärdaten
- **Wert**: Geben Sie den zum Registrierungswertnamen gehörenden Wert ein. Für den Wert "ProgramFilesDir" geben Sie beispielsweise *C:\Program Files* ein.
- Klicken Sie auf **Speichern**, um die Angaben zu speichern oder auf **Abbrechen**, um die Angaben nicht zu speichern.

  Hinweis: Zum Löschen eines vorhandenen Registrierungsschlüssels zeigen Sie auf dessen Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, um ihn beizubehalten.

  Zum Bearbeiten eines Registrierungsschlüssels 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 **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Registrierungsrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen gemachten Änderungen werden auf alle Plattformen angewendet. Ausnahme bildet die Einstellung **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Geräterichtlinie für Remotesupport

Jul 28, 2016

Sie erstellen eine Remotesupportrichtlinie in XenMobile, um Remotezugriff auf Samsung KNOX-Geräte zu erhalten. Sie können Support zweierlei Art konfigurieren:

- **Einfacher Remotesupport**: 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.
- **Premiumremotesupport**: 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.

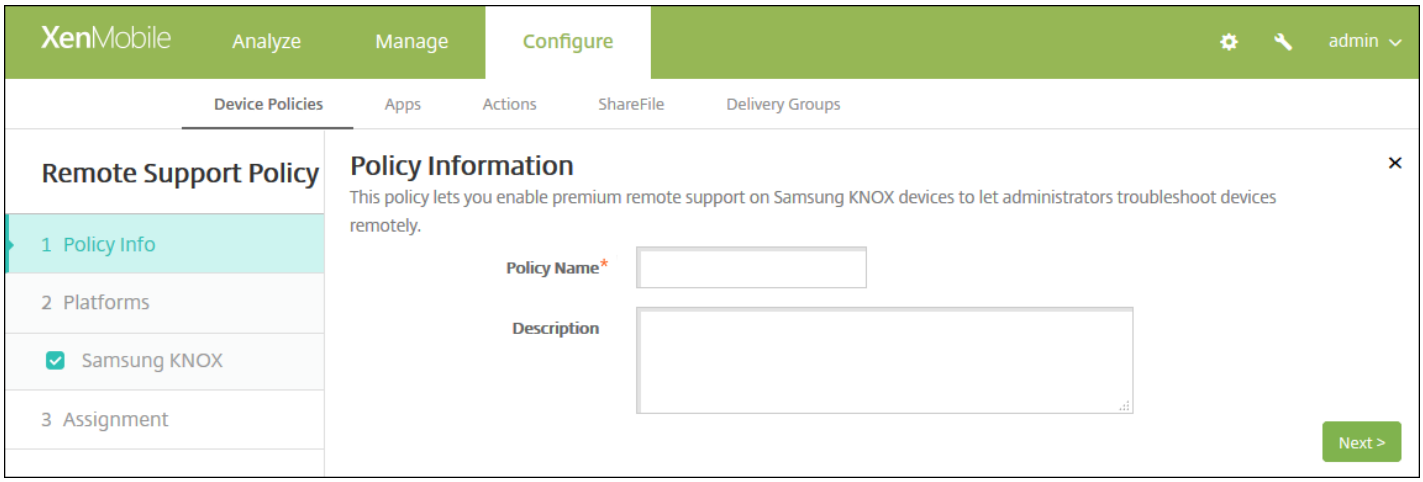
Hinweis: Zum Implementieren der Richtlinie müssen Sie die folgenden Schritte ausführen:

- Installieren der XenMobile Remote Support-App in der Umgebung
- Konfigurieren eines App-Tunnels für Remote Support; Weitere Informationen finden Sie unter App-Tunnelrichtlinien für Geräte.
- 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 **Konfigurieren > Geräterichtlinien**. Die Seite **Geräterichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

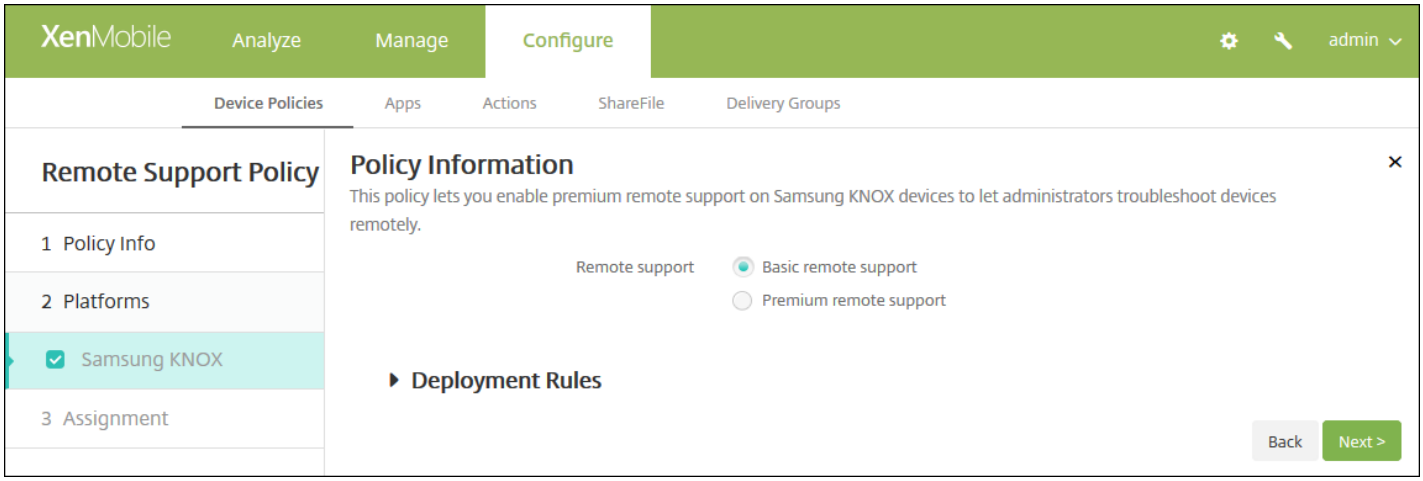
3. Erweitern Sie **Mehr** und klicken Sie unter **Netzwerkzugriff** auf **Remotesupport**. Die Seite **Remotesupport** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite mit Plattforminformationen für **Samsung KNOX** wird angezeigt.

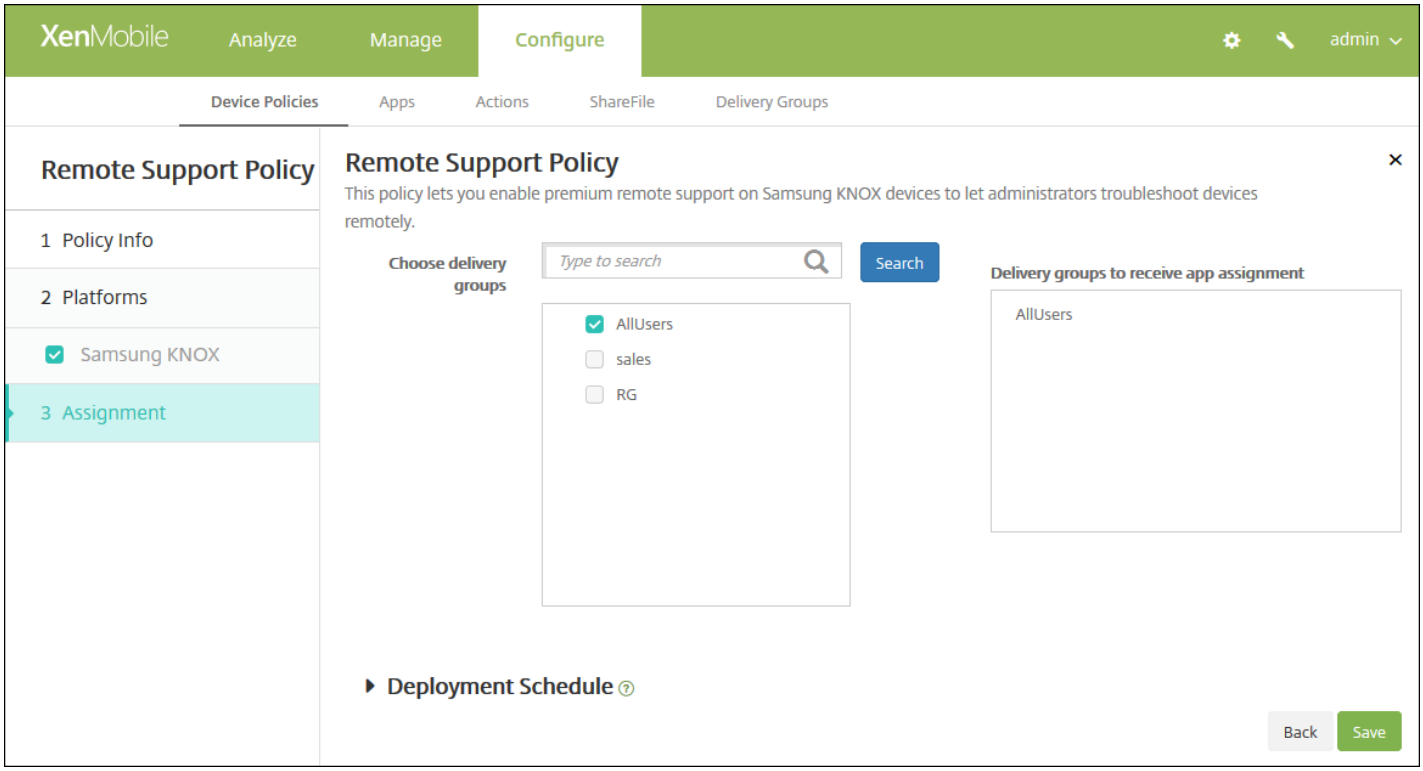


6. Konfigurieren Sie folgende Einstellung:

- **Remotesupport**: Wählen Sie **Einfacher Remotesupport** oder **Premiumremotesupport** aus. Die Standardeinstellung ist **Einfacher Remotesupport**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Remotesupportrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Beschränkungsrichtlinien für Geräte

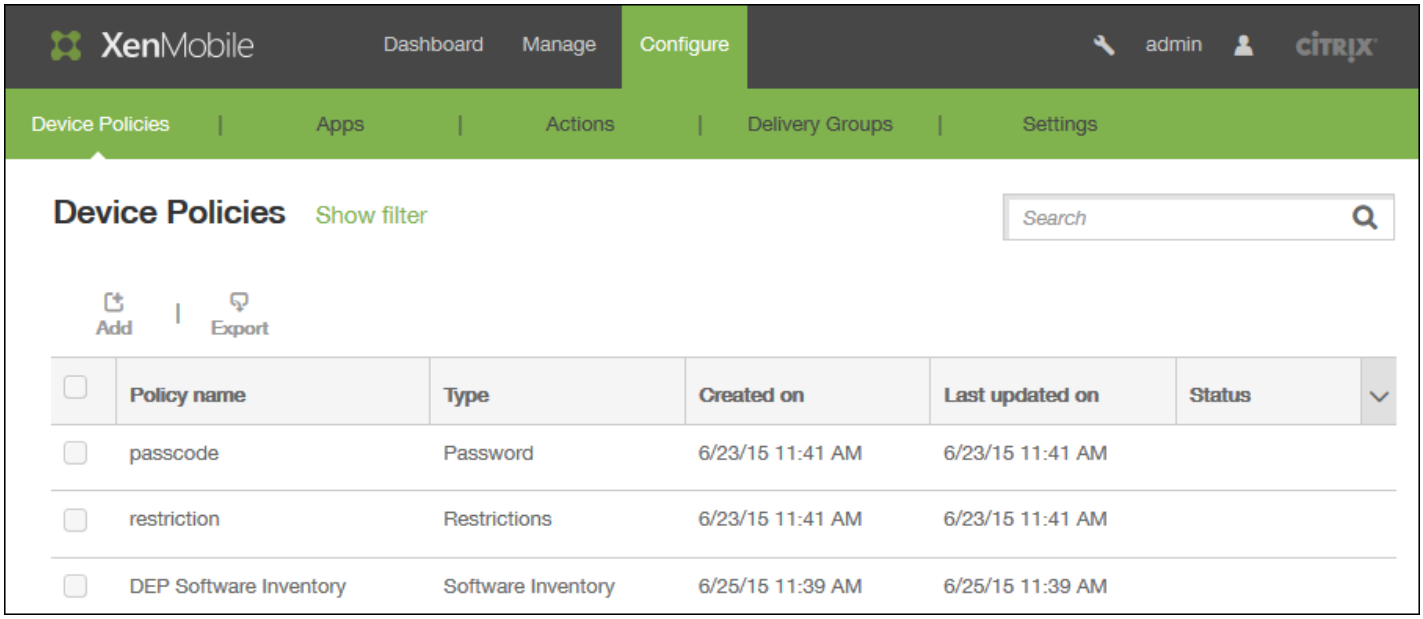
Jul 28, 2016

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, Mac OS X, Samsung SAFE, Samsung KNOX, Windows Tablet, Windows Phone, Amazon und Windows Mobile/CE. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Abschnitt beschrieben.

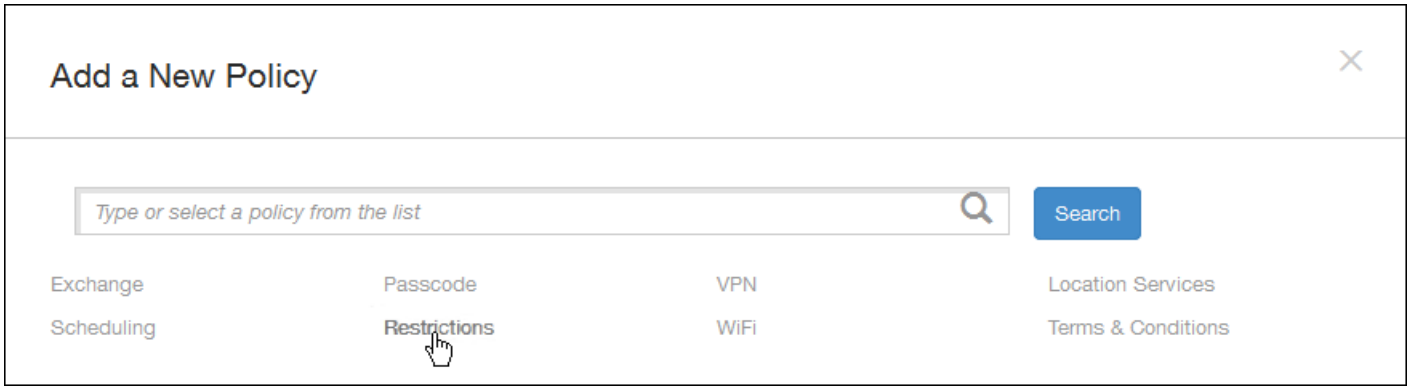
Diese Geräterichtlinie ermöglicht oder verhindert, dass Benutzer auf bestimmte Features auf Geräten, z. B. die Kamera, zugreifen. Sie können außerdem Einschränkungen für Sicherheit und Medieninhalte festlegen und vorgeben, welche App-Typen Benutzer installieren können. Die meisten Einschränkungen sind standardmäßig auf **EIN** (*zugelassen*) festgelegt. Die wichtigsten Ausnahmen bilden das Feature "iOS-Sicherheit - Erzwingen" sowie alle Windows-Tablet-Features, die standardmäßig auf **AUS** bzw. *beschränkt* festgelegt sind.
Tipp: Alle Optionen, die Sie auf **EIN** festlegen, bewirken, dass die Benutzer den entsprechenden Vorgang ausführen oder das Feature verwenden
— können
. Beispiel:

- **Kamera**: Bei Auswahl von **EIN** können Benutzer die Kamera auf Geräten verwenden. Bei Auswahl von **AUS** können Benutzer die Kamera auf Samsung SAFE-Geräten nicht verwenden.
- **Screenshots**: Bei Auswahl von **EIN** können Benutzer Screenshots auf den Geräten erstellen. Bei Auswahl von **AUS** können Benutzer keine Screenshots auf den Geräten erstellen.

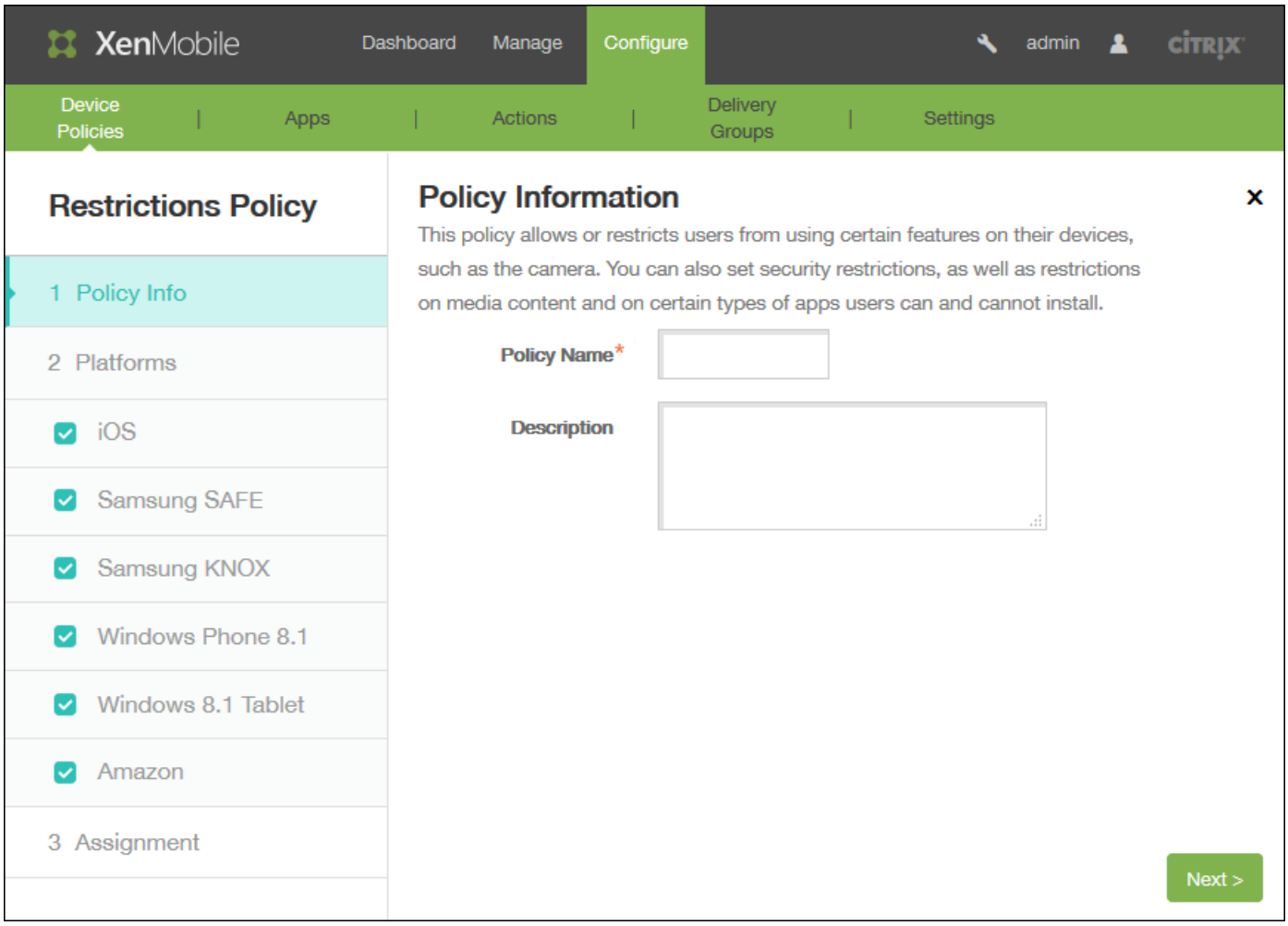
1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren > Geräterichtlinien**. Die Seite **Geräterichtlinien** wird angezeigt.



2. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Richtlinie hinzufügen** wird angezeigt.



3. Klicken Sie auf **Einschränkungen**. Die Seite **Richtlinieninformation** für die Einschränkungen wird angezeigt.



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

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

4. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

5. Wählen Sie unter **Plattformen** die Plattforme(n), die Sie hinzufügen möchten. Sie können dann die

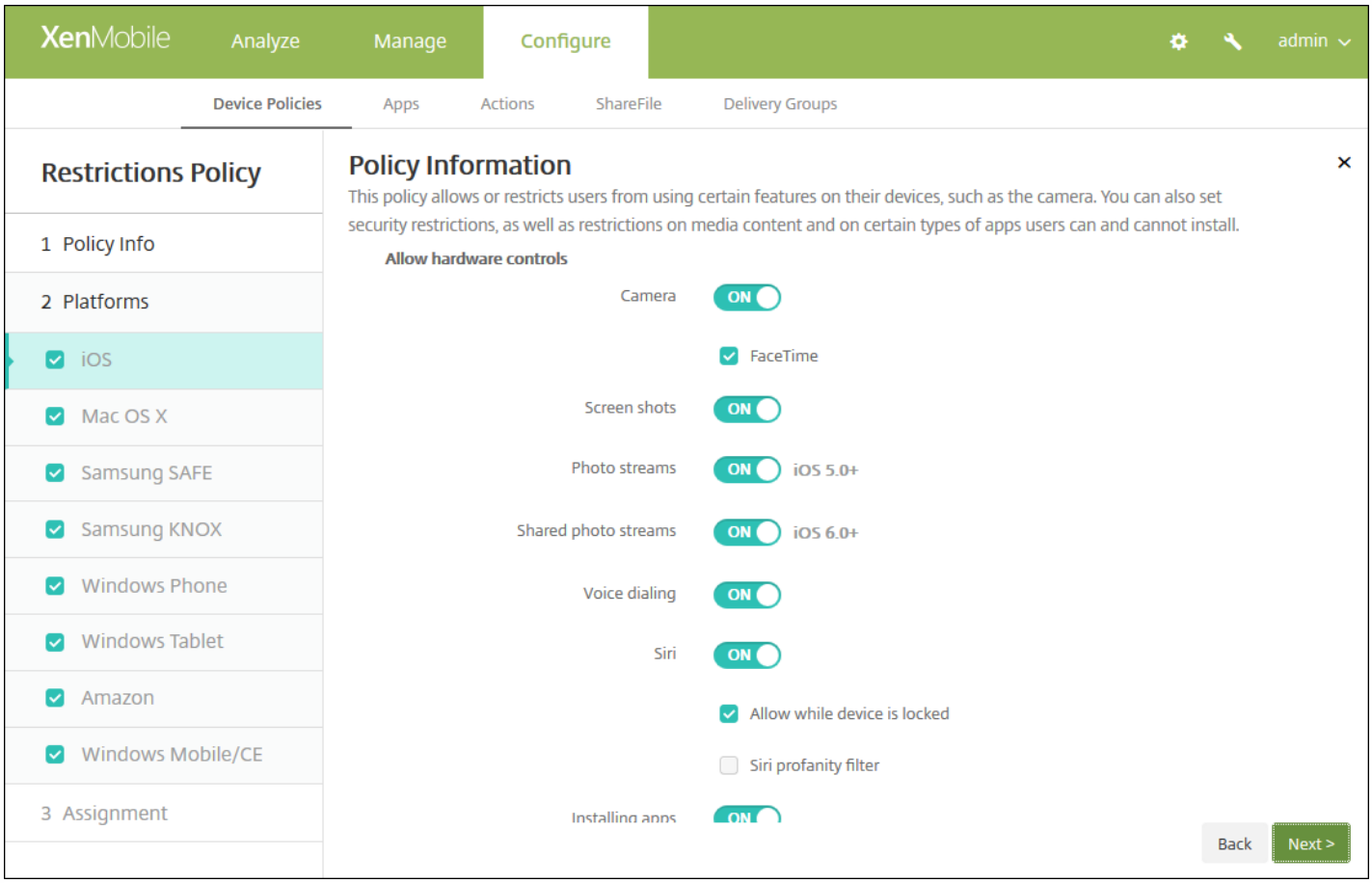
Richtlinieninformationen für jede ausgewählte Plattform ändern. Klicken Sie zum Einschränken auf die gewünschten Features (siehe nachfolgende Abschnitte), wodurch deren Einstellung in **AUS** geändert wird. Wenn nicht anders angegeben, sind Features in der Standardeinstellung aktiviert.

Bei Auswahl von:

iOS konfigurieren Sie diese Einstellungen
Mac OS X konfigurieren Sie diese Einstellungen
Samsung SAFE konfigurieren Sie diese Einstellungen
Samsung KNOX konfigurieren Sie diese Einstellungen
Windows Phone konfigurieren Sie diese Einstellungen
Windows Tablet konfigurieren Sie diese Einstellungen
Amazon konfigurieren Sie diese Einstellungen
Windows Mobile/CE konfigurieren Sie diese Einstellungen

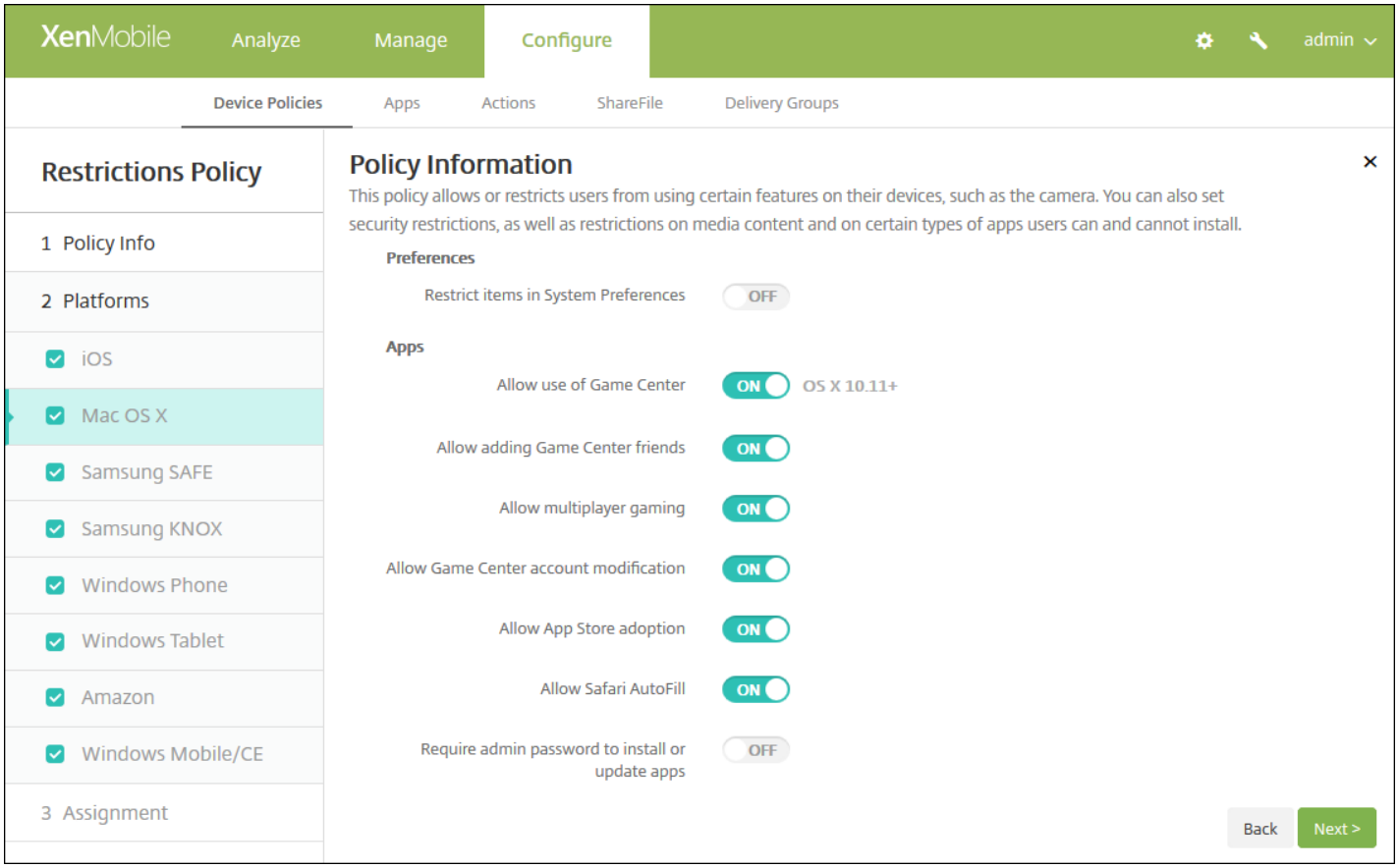
Nachdem Sie die Einschränkungen für eine Plattform festgelegt haben, stellen Sie wie in Schritt 7 in diesem Artikel beschrieben die Bereitstellungsregeln für die Plattform ein.

Bei Auswahl von iOS konfigurieren Sie die folgenden Einstellungen:



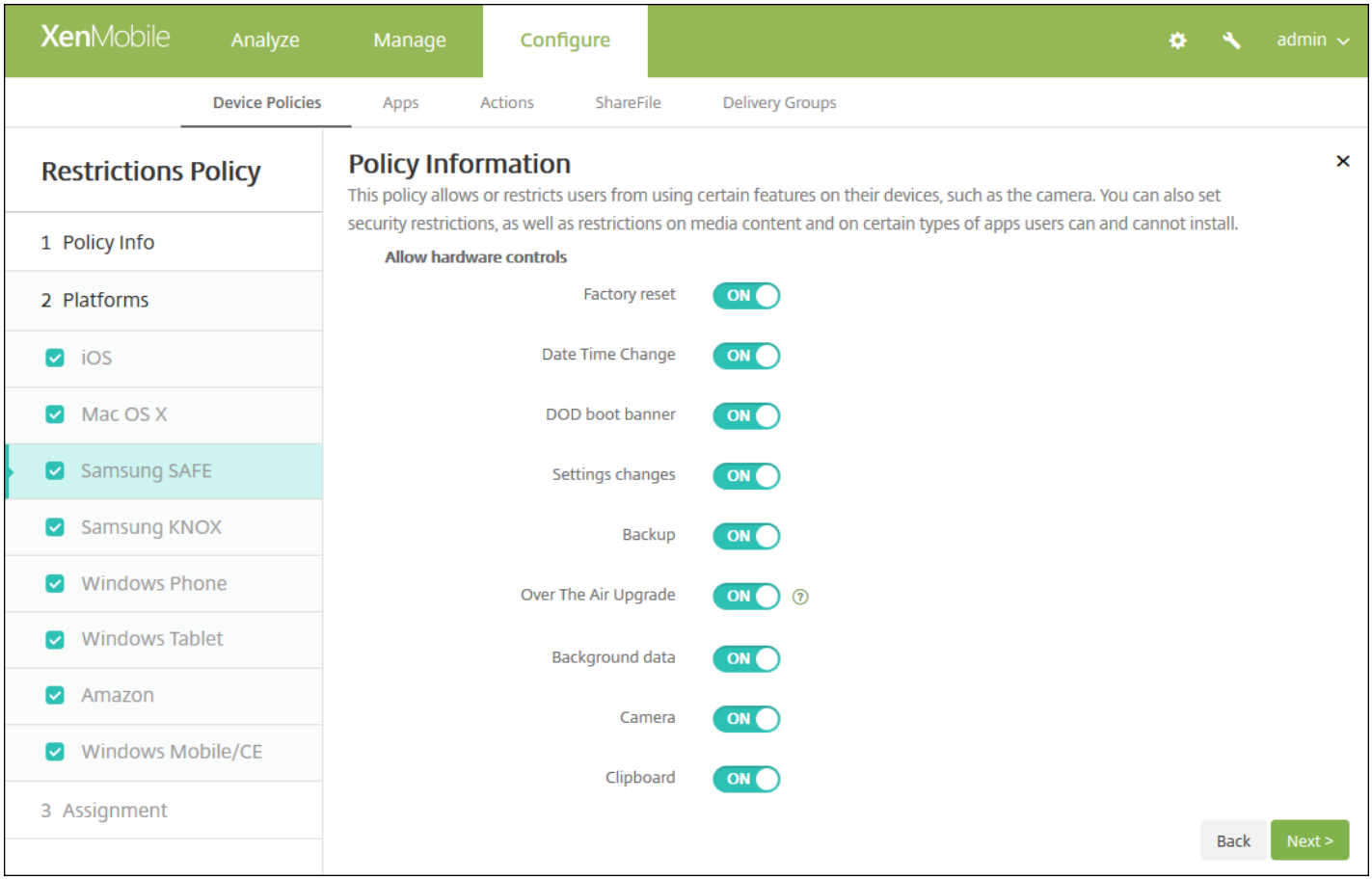
iOS-Einstellungen

Konfigurieren von Mac OS X-Einstellungen



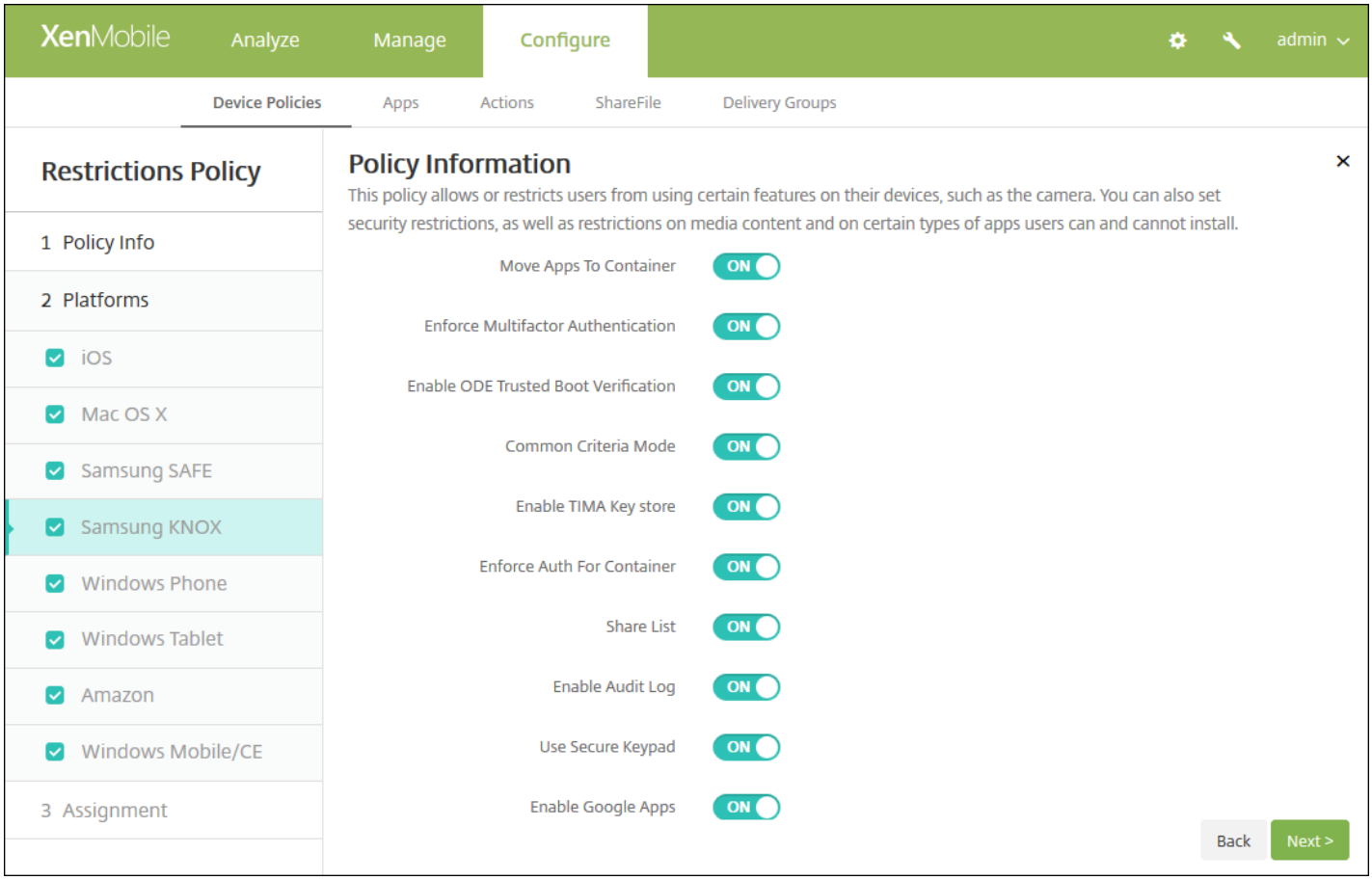
Mac OS X-Einstellungen

Konfigurieren der Samsung SAFE-Einstellungen



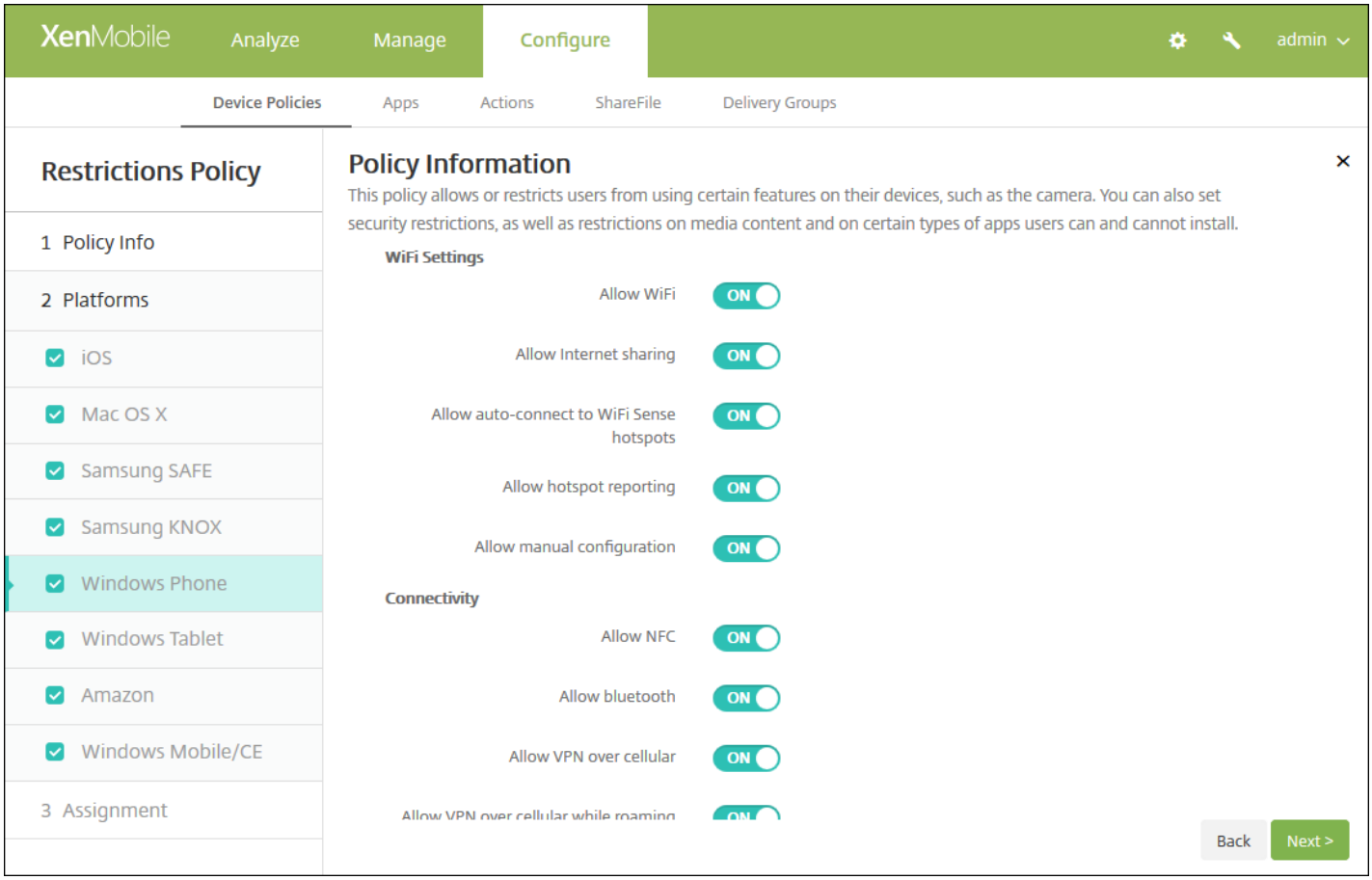
Samsung SAFE-Einstellungen

Konfigurieren der Samsung KNOX-Einstellungen



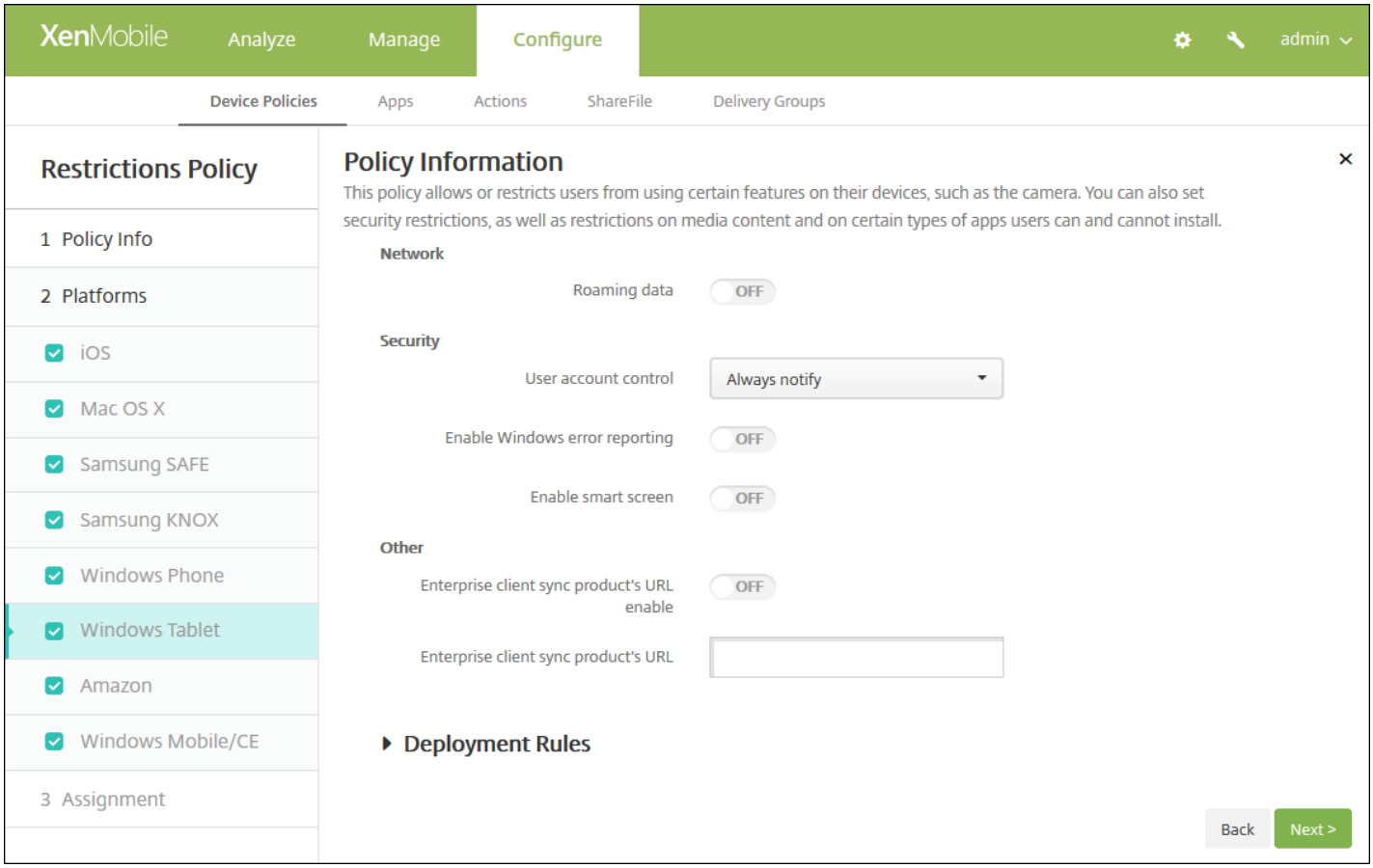
Samsung KNOX-Einstellungen

Konfigurieren von Windows Phone-Einstellungen



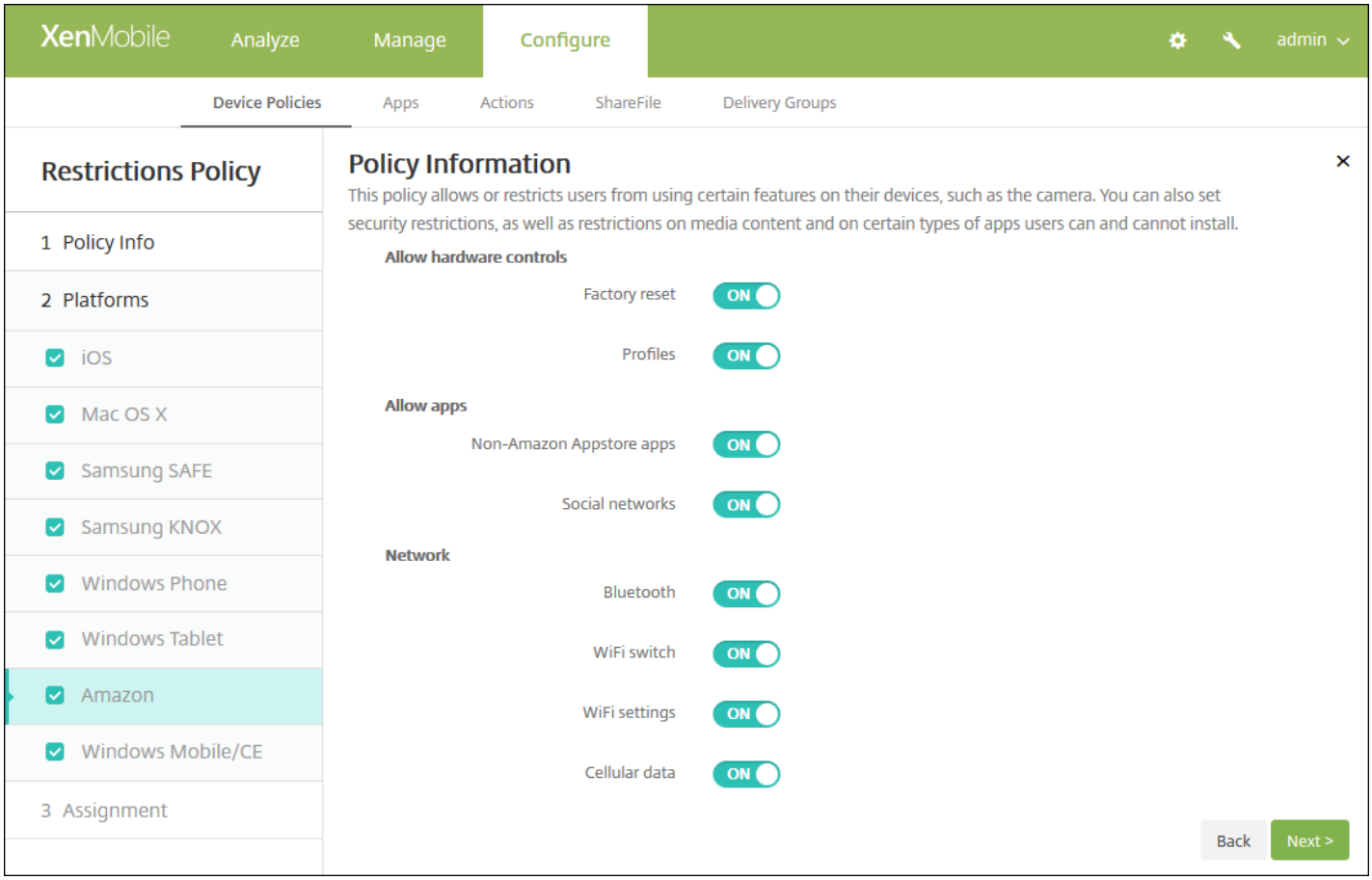
Windows Phone-Einstellungen

Konfigurieren von Windows Tablet-Einstellungen



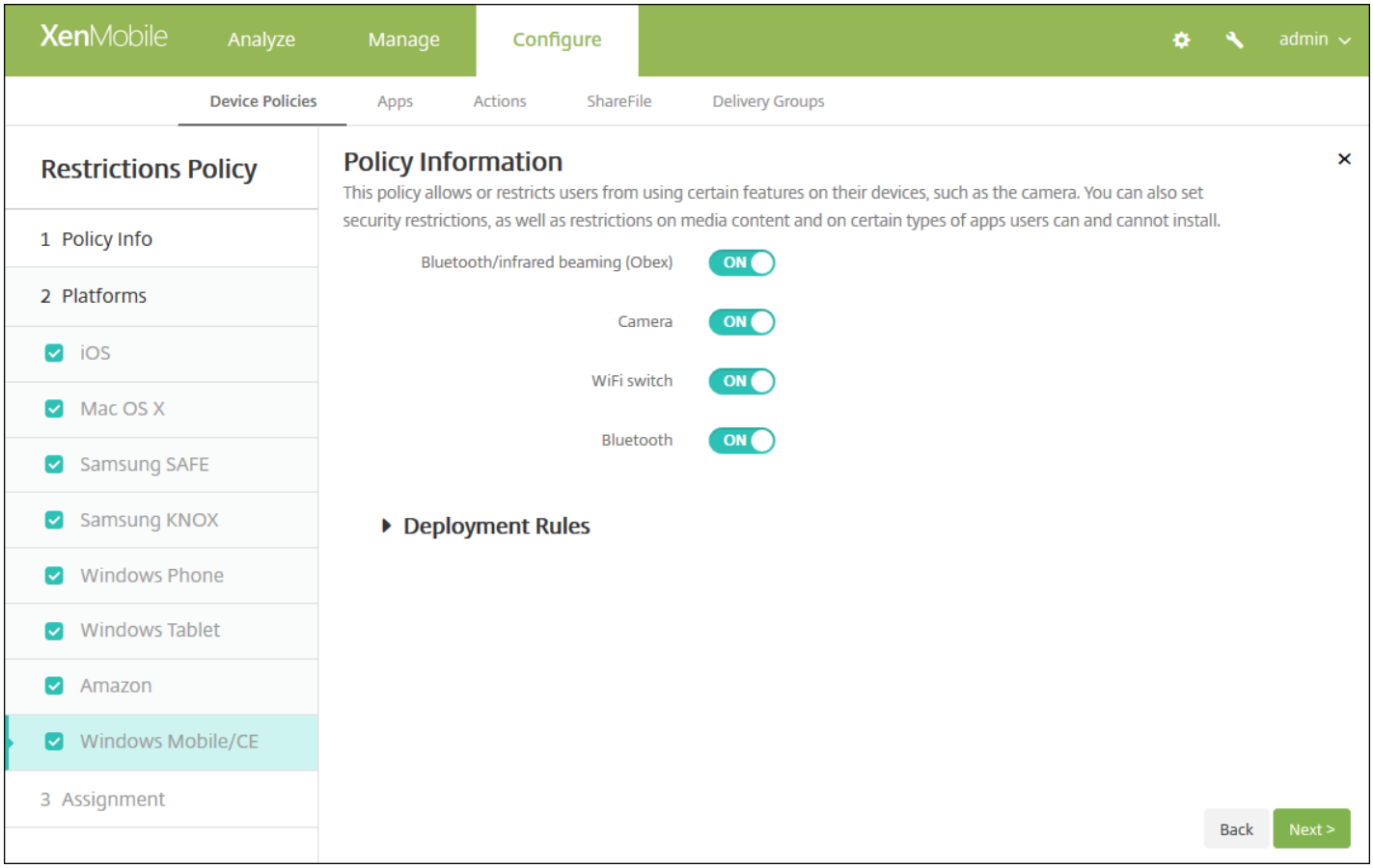
Windows Tablet-Einstellungen

Konfigurieren von Amazon-Einstellungen



Amazon-Einstellungen

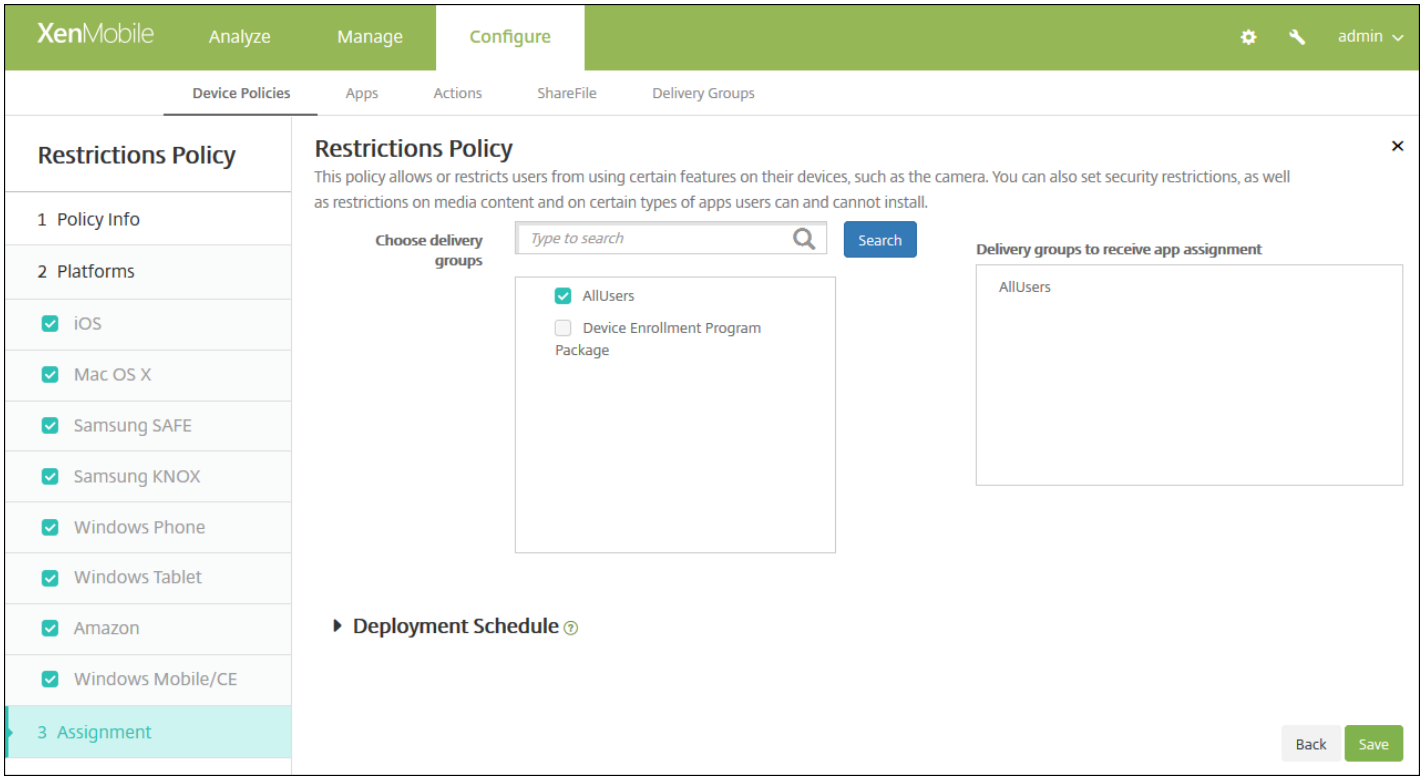
Konfigurieren von Windows Mobile-/CE-Einstellungen



Windows Mobile-/CE-Einstellungen

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuordnung** für die Einschränkungsrichtlinie wird angezeigt.



9. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

10. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Roamingrichtlinien

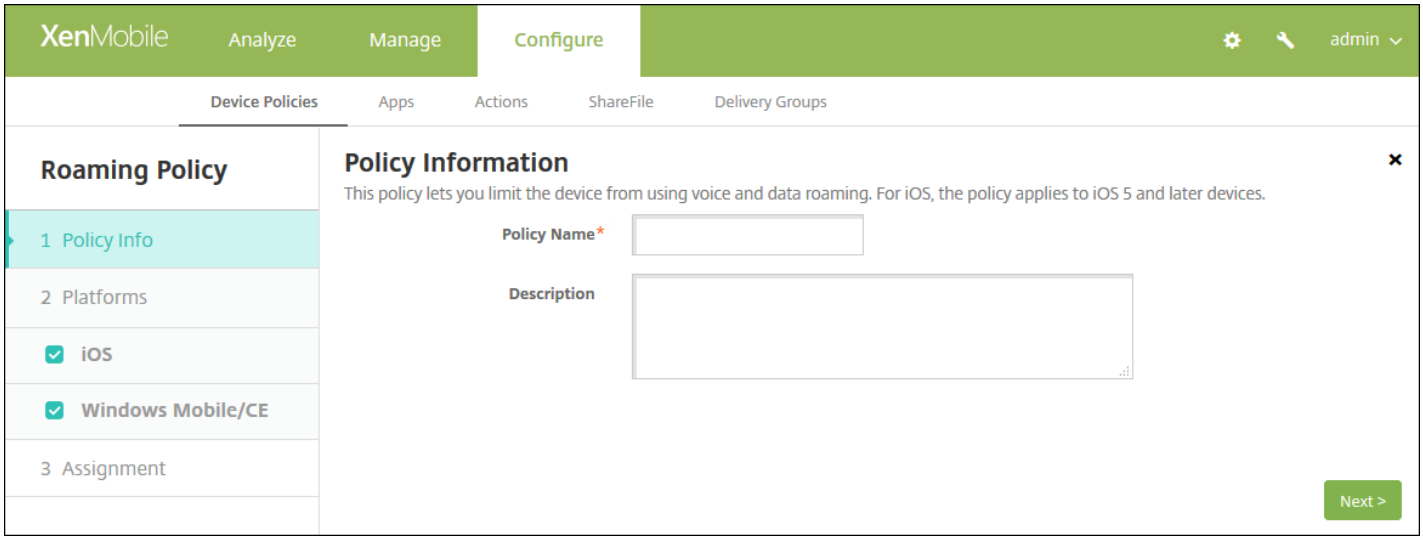
Jul 28, 2016

Sie können in XenMobile eine Geräterichtlinie einrichten, um vorzugeben, ob auf iOS- bzw. Windows Mobile/CE-Geräten Sprach- und Datenroaming zugelassen wird. Wird Sprachroaming deaktiviert, dann wird Datenroaming automatisch auch deaktiviert. Hinweis zu iOS: Diese Richtlinie gilt nur für iOS 5.0 und höher.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Klicken Sie auf **Mehr** und dann unter **Netzwerkzugriff** auf **Roaming**. Die Seite **Roaming** wird angezeigt.



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

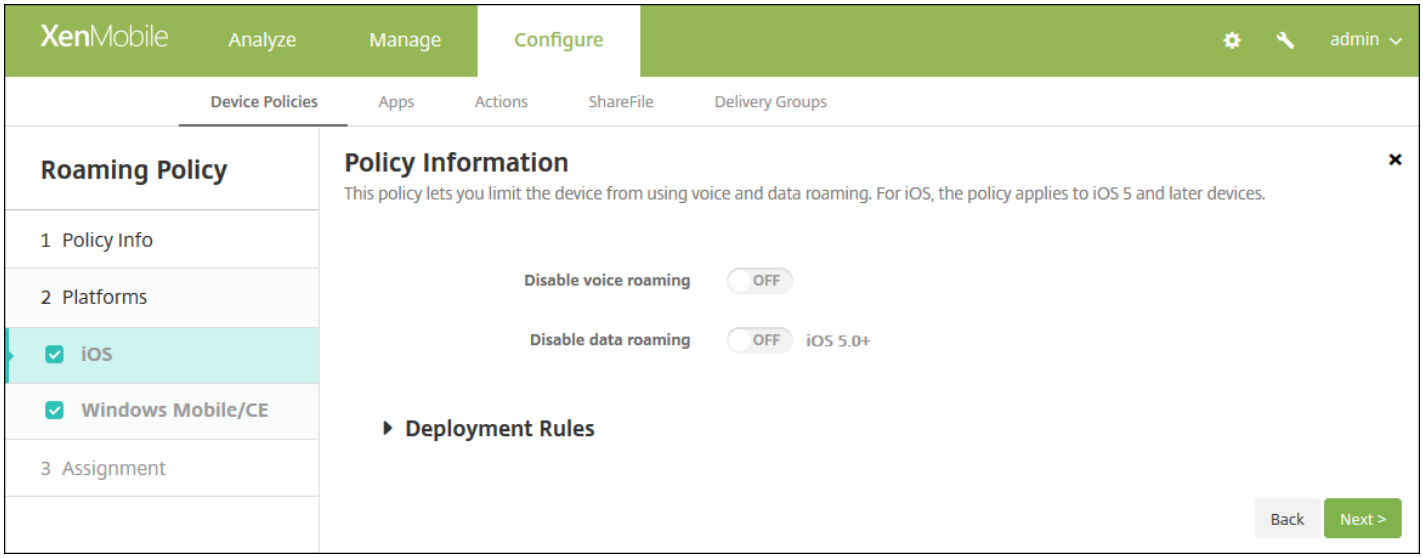
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

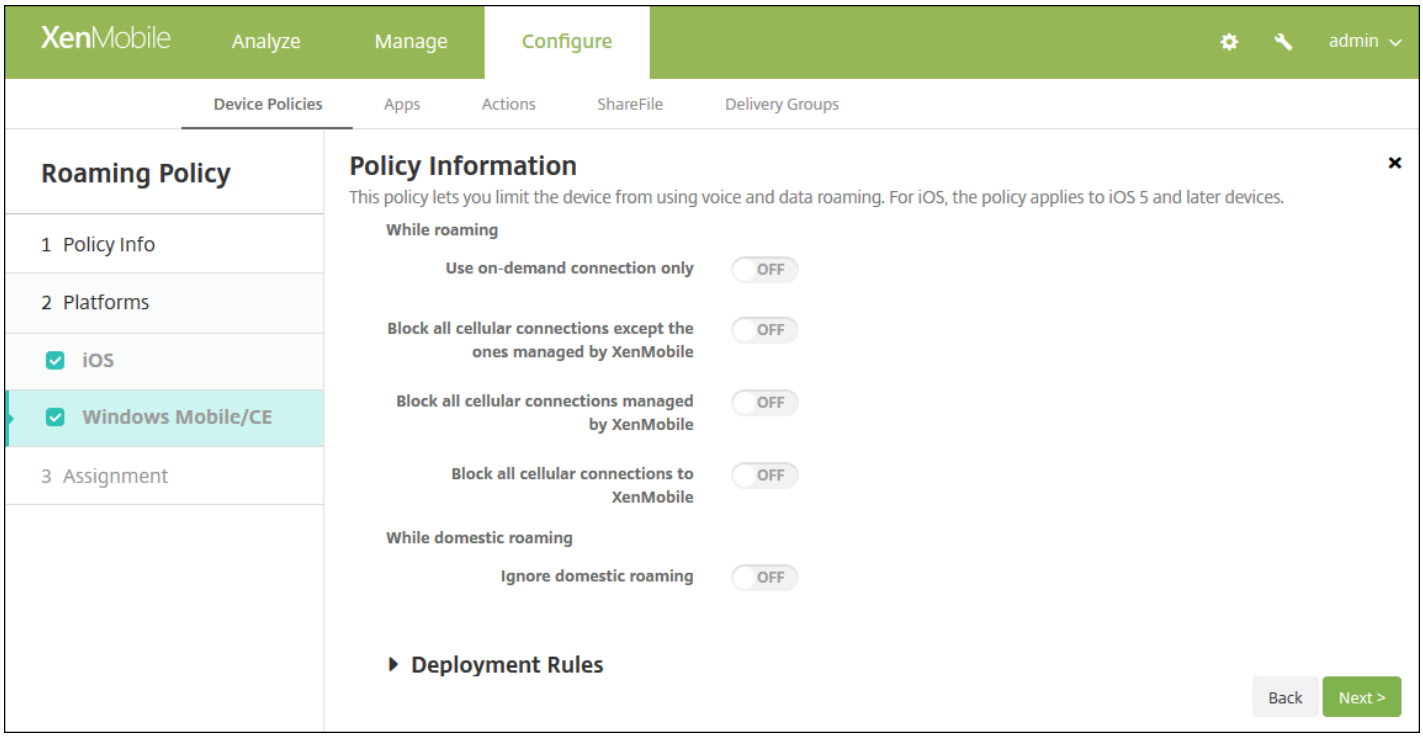
Konfigurieren von iOS-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Sprachroaming deaktivieren**: Wählen Sie aus, ob das Sprachroaming deaktiviert werden soll. Wird diese Option deaktiviert, dann wird Datenroaming automatisch auch deaktiviert. Die Standardeinstellung ist **AUS**, Sprachroaming ist also zugelassen.
- **Datenroaming deaktivieren**: Wählen Sie aus, ob das Datenroaming deaktiviert werden soll. Diese Option ist nur verfügbar, wenn Sprachroaming aktiviert ist. Die Standardeinstellung ist **AUS**, Datenroaming ist also zugelassen.

Konfigurieren von Windows Mobile-/CE-Einstellungen

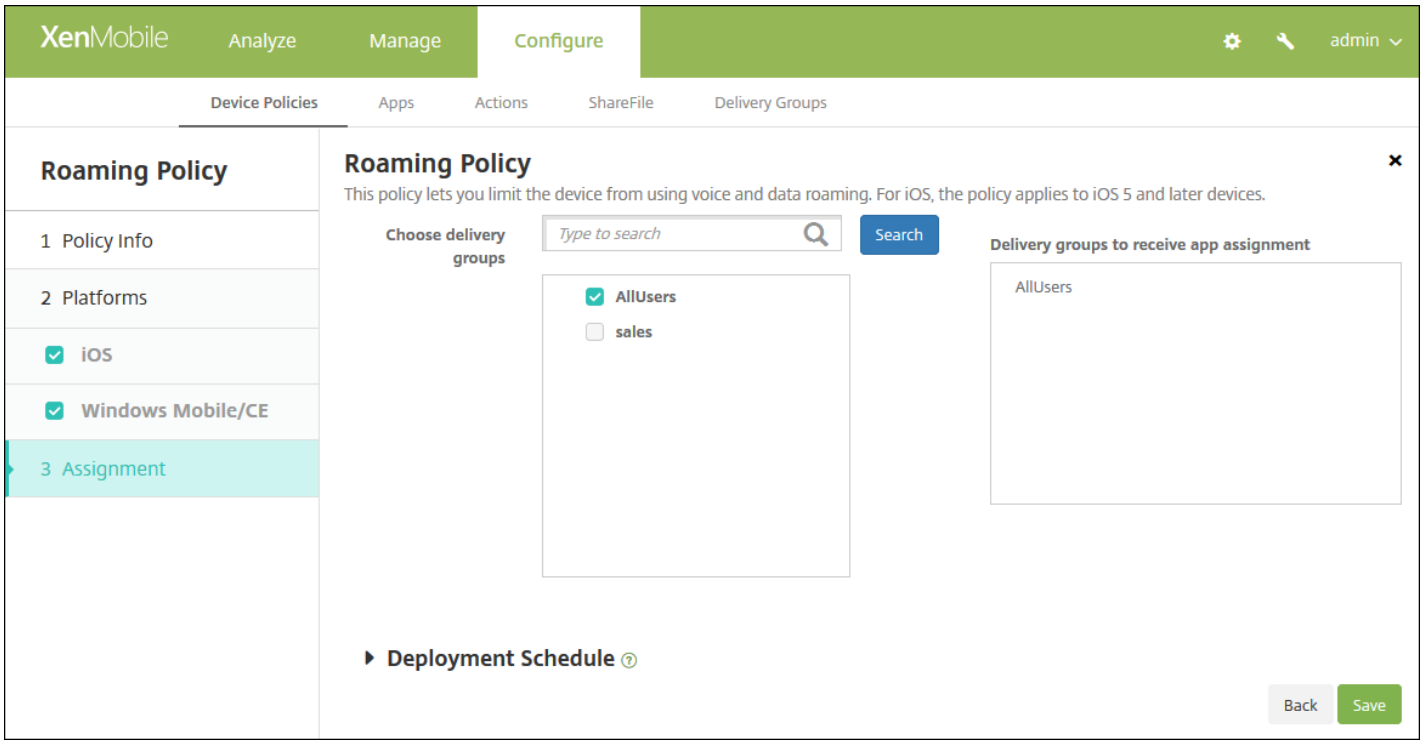


Konfigurieren Sie folgende Einstellungen:

- **Beim Roaming**
  - **Verbindung nur auf Anfrage**: Das Gerät stellt nur eine Verbindung mit XenMobile her, wenn der Benutzer dies auf dem Gerät auslöst oder wenn eine mobile App eine erzwungene Verbindung anfordert (z. B. eine E-Mail-Pushanforderung, wenn der Exchange Server entsprechend eingerichtet ist). Durch diese Option wird die Standardplanungsrichtlinie für Verbindungen vorübergehend deaktiviert.
  - **Alle nicht von XenMobile verwalteten Mobilverbindungen blockieren**: Mit Ausnahme des in einem XenMobile-Tunnel oder einem anderen XenMobile-Task zur Geräteverwaltung offiziell deklarierten Datenverkehrs werden keine Daten von dem Gerät gesendet oder empfangen. Beispielsweise deaktiviert diese Option alle Verbindungen mit dem Internet über den Gerätewebbrowser.
  - **Alle von XenMobile verwalteten Mobilverbindungen blockieren**: Alle App-Daten, die durch einen XenMobile-Tunnel übertragen werden, werden blockiert (einschließlich der XenMobile Remote Support-Daten). Der aus der reinen Geräteverwaltung resultierende Datenverkehr wird nicht blockiert.
  - **Alle Mobilverbindungen zu XenMobile blockieren**: Zwischen Gerät und XenMobile werden keinerlei Daten übertragen, bis das Gerät wieder eine Verbindung über USB, WiFi oder das Mobilfunknetz seines Standardnetzbetreibers herstellt.
- **Beim Inlandsroaming**
  - **Inlandsroaming ignorieren**: Beim Inlandsroaming werden keine Daten blockiert.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Roamingrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen gemachten Änderungen werden auf alle Plattformen angewendet. Ausnahme bildet die Einstellung **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Samsung MDM-Richtlinien für Geräte

Jul 28, 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.

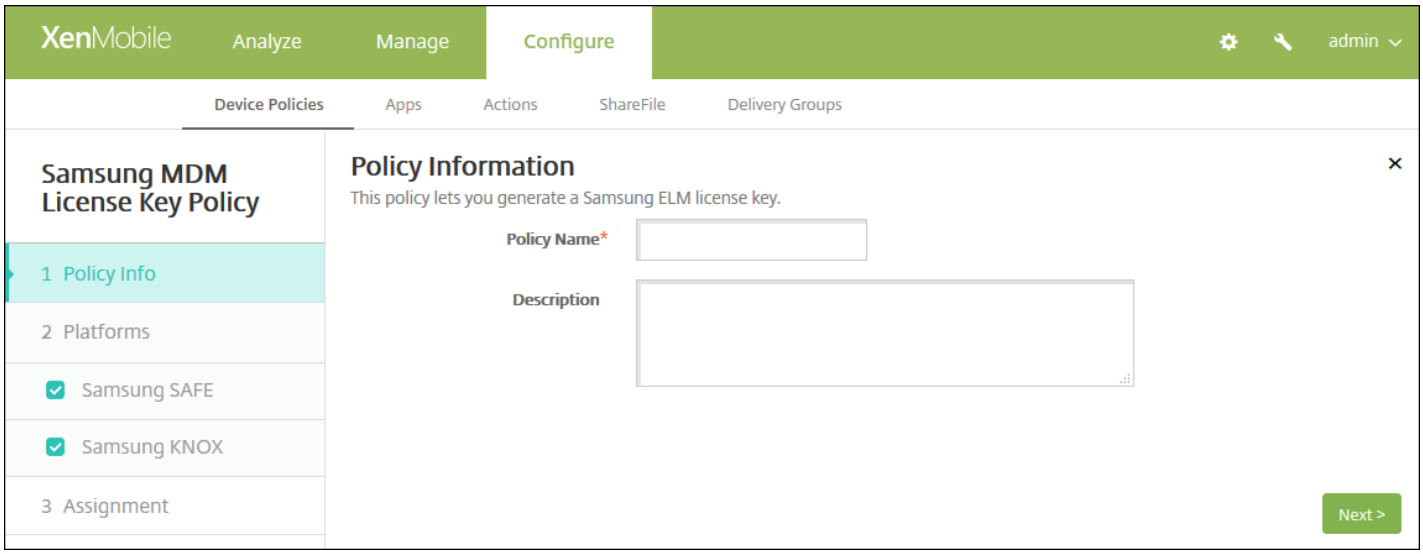
Bevor Sie SAFE-Richtlinien und -Einschränkungen bereitstellen können, müssen Sie die SAFE-APIs durch Bereitstellen des integrierten Samsung Enterprise License Management-Schlüssels (ELM) auf Geräten aktivieren. Zum Aktivieren der Samsung KNOX-API müssen Sie zusätzlich zur Bereitstellung des ELM-Schlüssels über Samsung KNOX License Management System (KLMS) eine Samsung KNOX Workspace-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 SAFE API verfügbar" **Wahr**.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Klicken Sie auf **Mehr** und dann unter **Sicherheit** auf **Samsung MDM-Lizenzschlüssel**. Die Seite **Samsung MDM-Lizenzschlüssel** wird angezeigt.



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

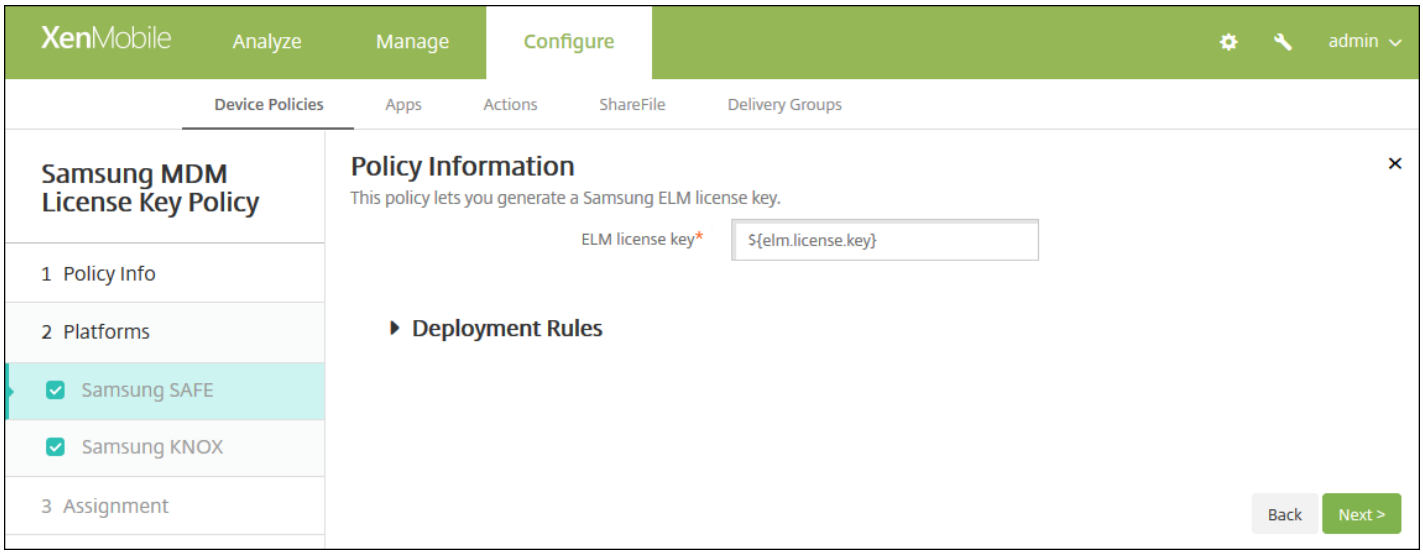
- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

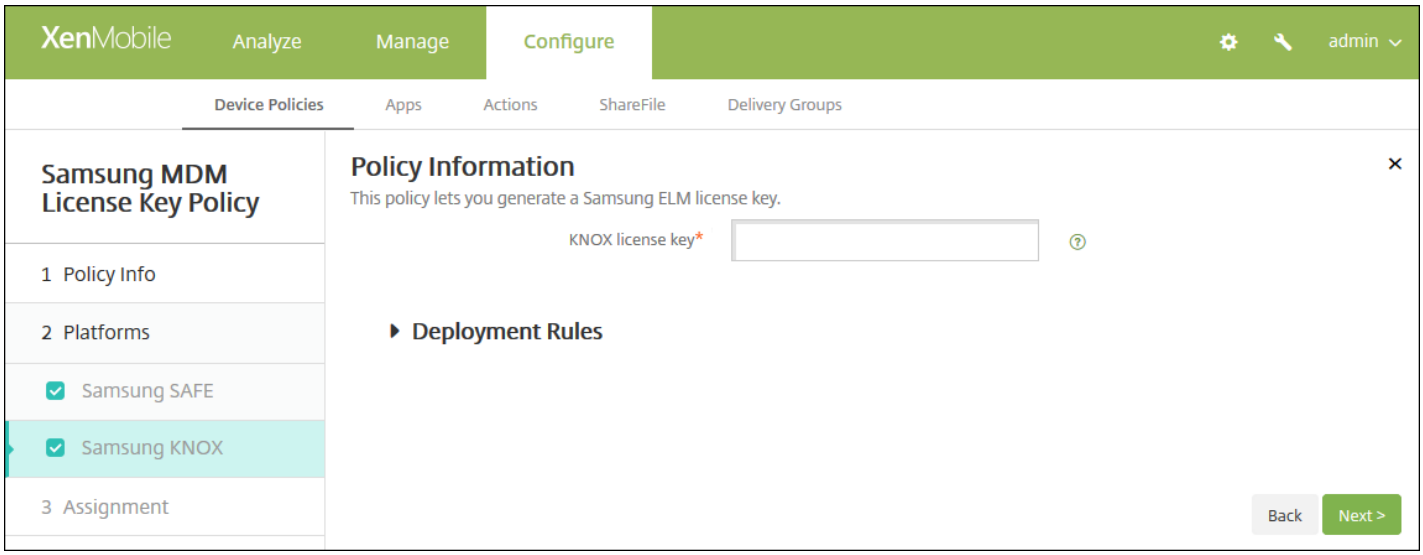
Konfigurieren der Samsung SAFE-Einstellungen



Konfigurieren Sie folgende Einstellung:

- **ELM-Lizenzschlüssel**: Dieses Feld sollte das Makro zur Erstellung des ELM-Lizenzschlüssels bereits enthalten. Wenn das Feld leer ist, geben Sie das Makro "${elm.license.key}" ein.

Konfigurieren der Samsung KNOX-Einstellungen

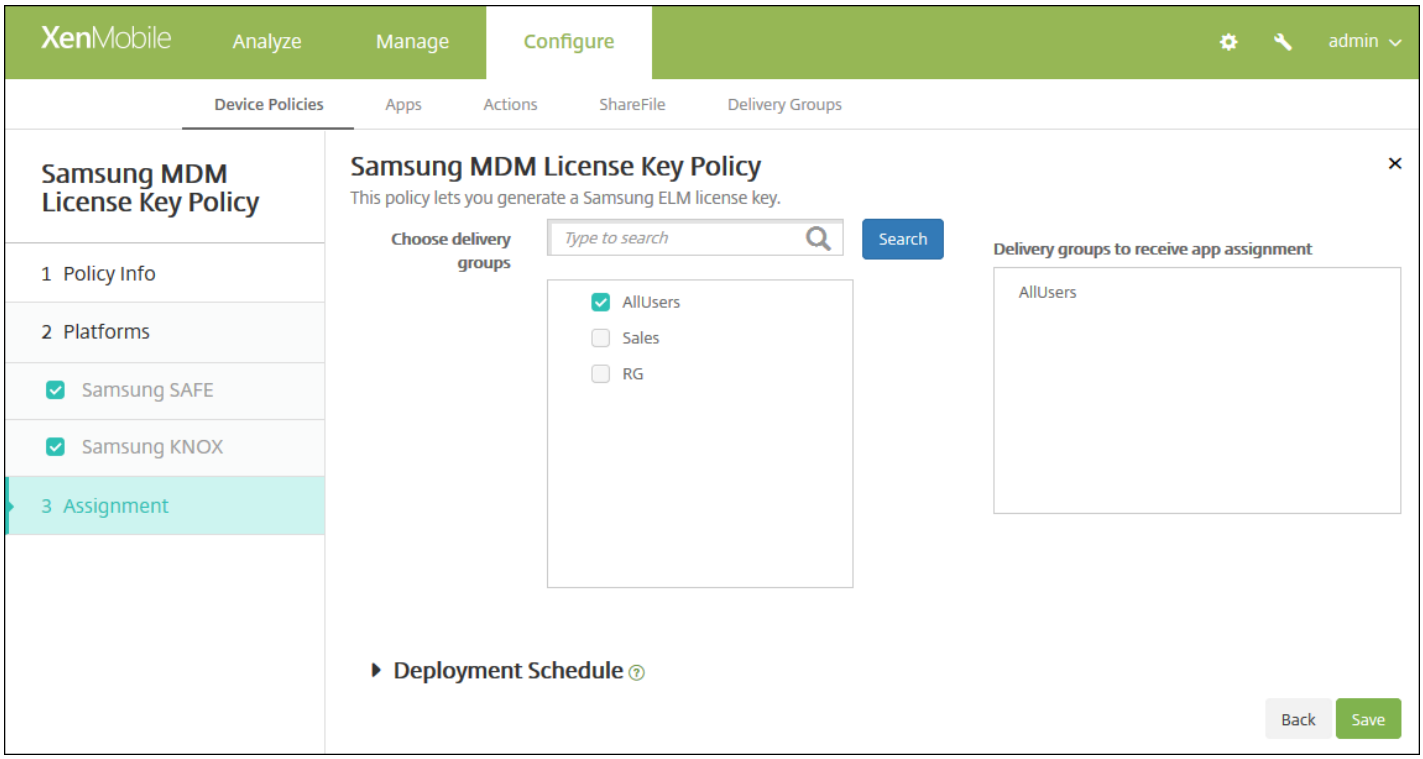


Konfigurieren Sie folgende Einstellung:

- **KNOX-Lizenzschlüssel**: Geben Sie den 25-stelligen KNOX-Lizenzschlüssel ein, den Sie von Samsung erhalten haben.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuordnung** für den Samsung MDM-Lizenzschlüssel wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Samsung SAFE-Firewallrichtlinie

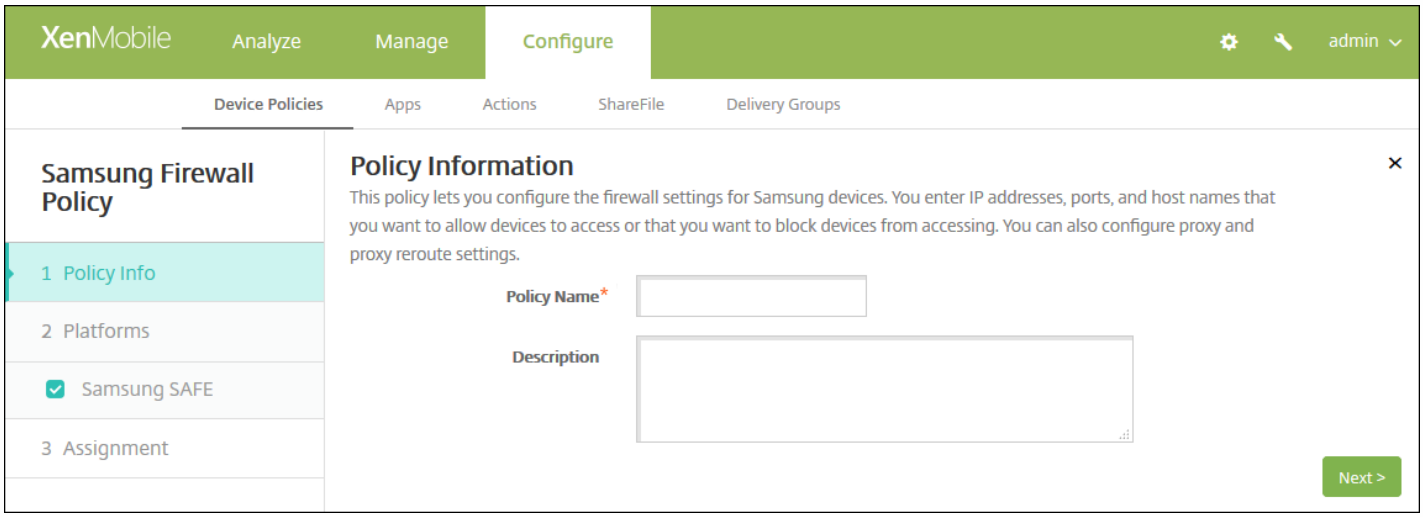
Jul 28, 2016

Mit dieser Richtlinie können Sie die Firewall-Einstellungen für Samsung-Geräte konfigurieren. Sie geben dabei IP-Adressen, Ports und Hostnamen ein, auf die Geräte zugreifen können bzw. die Sie blockieren möchten. Sie können außerdem Proxy- und Proxyumleitungseinstellungen konfigurieren.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

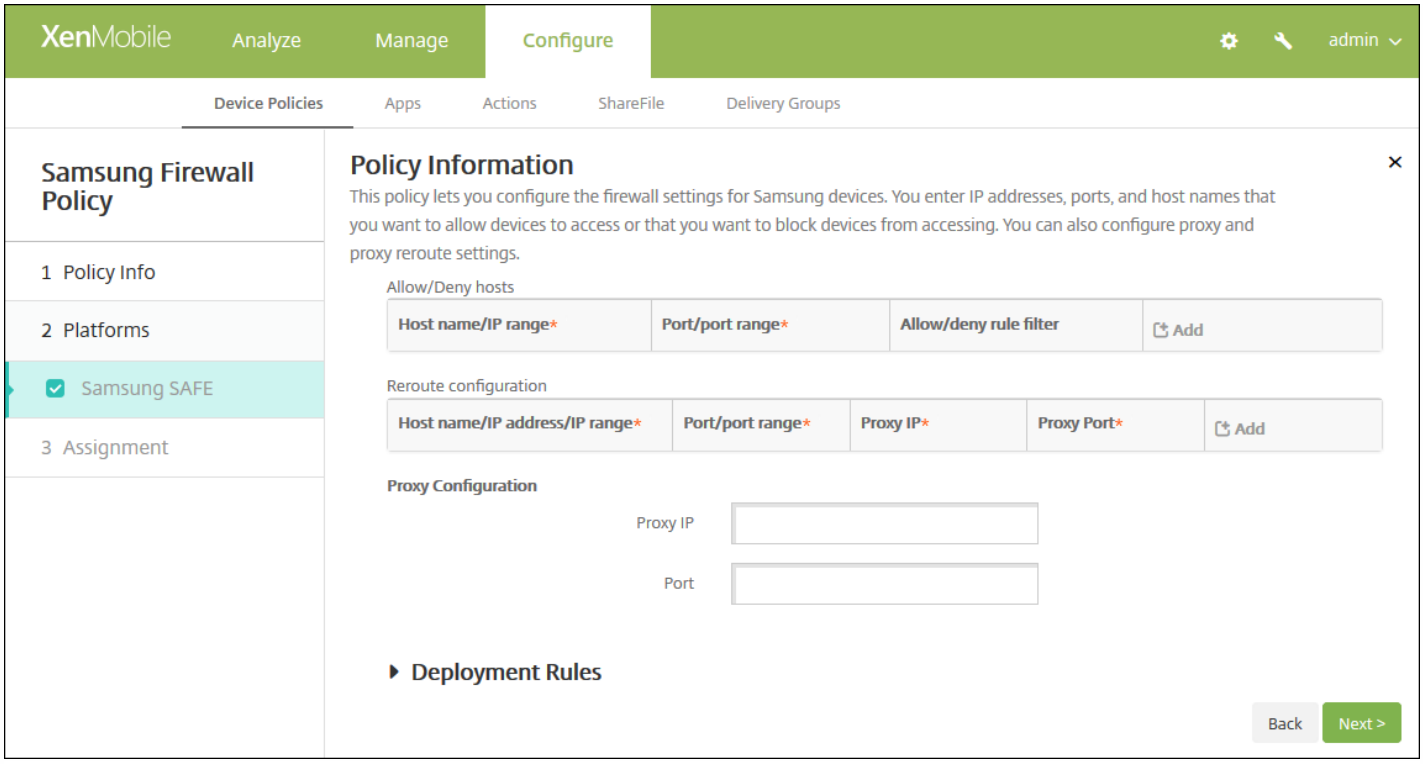
3. Erweitern Sie **Mehr** und klicken Sie unter **Netzwerkzugriff** auf **Samsung-Firewall**. Die Seite **Samsung-Firewall** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite mit Plattforminformationen für **Samsung SAFE** wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:

- **Hosts zulassen/verweigern**
  - Für jeden Host, für den Sie Zugriff zulassen oder verweigern möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
    - **Hostname/IP-Adressbereich**: Geben Sie den Hostnamen oder die IP-Adresse des gewünschten Hoss ein.
    - **Port/Portbereich**: Geben Sie die Portnummer oder den Portbereich ein.
    - **Regelfilter zulassen/verweigern**: Wählen "Positivliste" aus, um den Zugriff zuzulassen, oder "Sperrliste", um den Zugriff zu blockieren.
    - Klicken Sie auf **Speichern** oder **Abbrechen**.
- **Umleitungskonfiguration**
  - Für jeden Proxy, den Sie konfigurieren möchten, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
    - **Hostname/IP-Adressbereich**: Geben Sie den Hostnamen oder die IP-Adresse des Proxys ein.
    - **Port/Portbereich**: Geben Sie die Portnummer oder den Portbereich ein.
    - **Proxy-IP**: Geben Sie die IP-Adresse des Proxyservers ein.
    - **Proxyport**: Geben Sie den Port des Proxyservers ein.
    - Klicken Sie auf **Speichern** oder **Abbrechen**.

    Hinweis: Zum Löschen eines vorhandenen Elements zeigen Sie auf dessen Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf **Löschen** zum Löschen des Eintrags oder auf **Abbrechen**, um ihn beizubehalten.

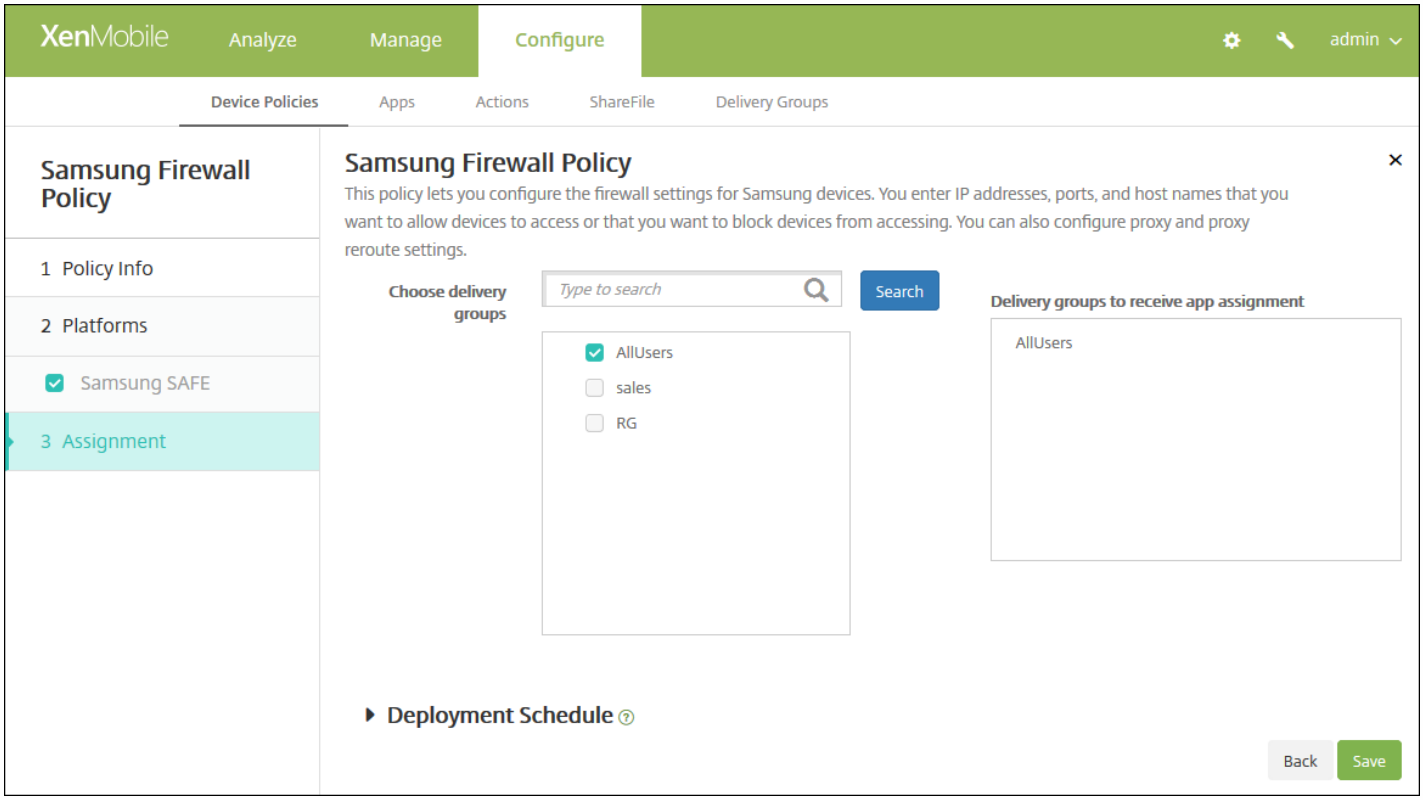
    Zum Bearbeiten eines Elements zeigen Sie auf dessen Zeile und klicken Sie auf das Stiftsymbol auf der rechten Seite. Nehmen Sie die gewünschten Änderungen an dem Eintrag vor und klicken Sie auf **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um den Vorgang abzubrechen.

- **Konfigurieren von Proxy**

- **Proxy-IP**: Geben Sie die Adresse des Proxyservers ein.
- **Port**: Geben Sie den Port des Proxyservers ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Samsung Firewall-Richtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.

- 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.

11. Klicken Sie auf **Speichern**.

SCEP-Geräterichtlinien

Jul 28, 2016

Mit dieser Richtlinie können Sie iOS- und Mac OS X-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.

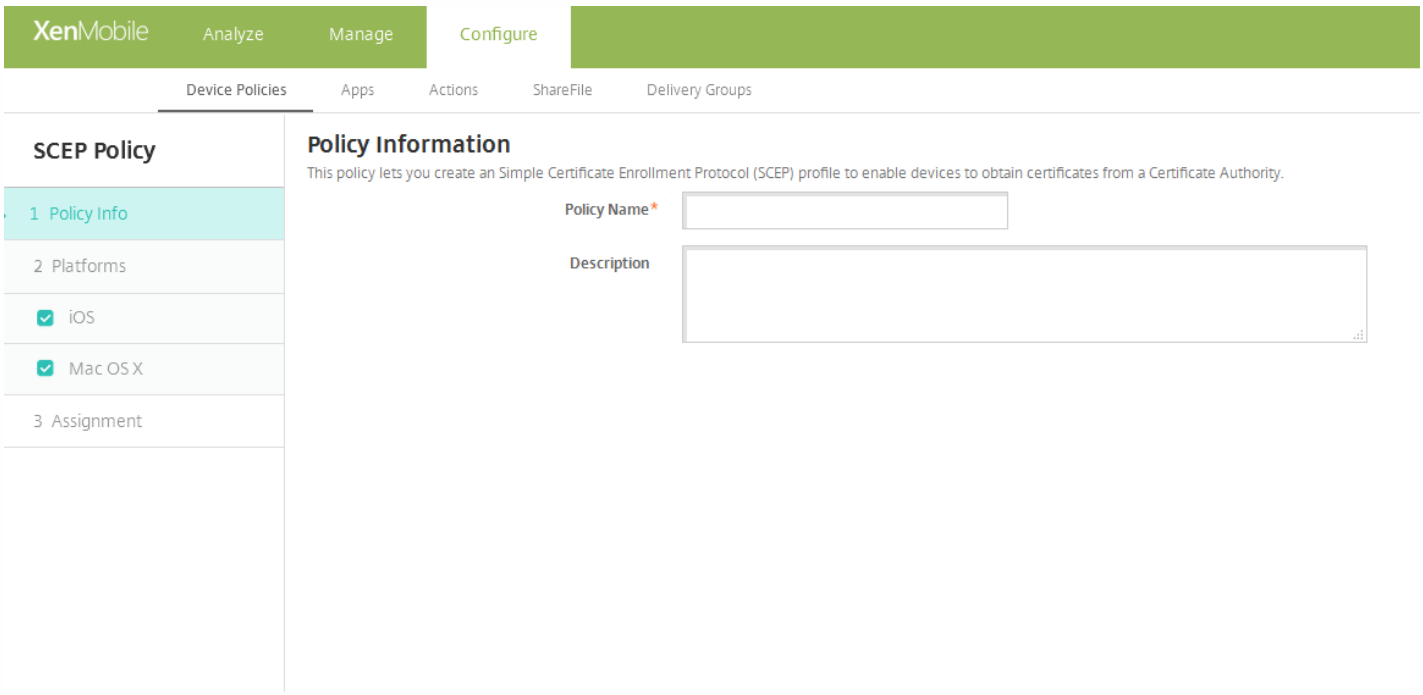
iOS-Einstellungen

Mac OS X-Einstellungen

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Erweitern Sie **Mehr** und klicken Sie dann unter **Sicherheit** auf **SCEP**. Die Seite für die Richtlinieninformationen der Richtlinie **SCEP** wird angezeigt.



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

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

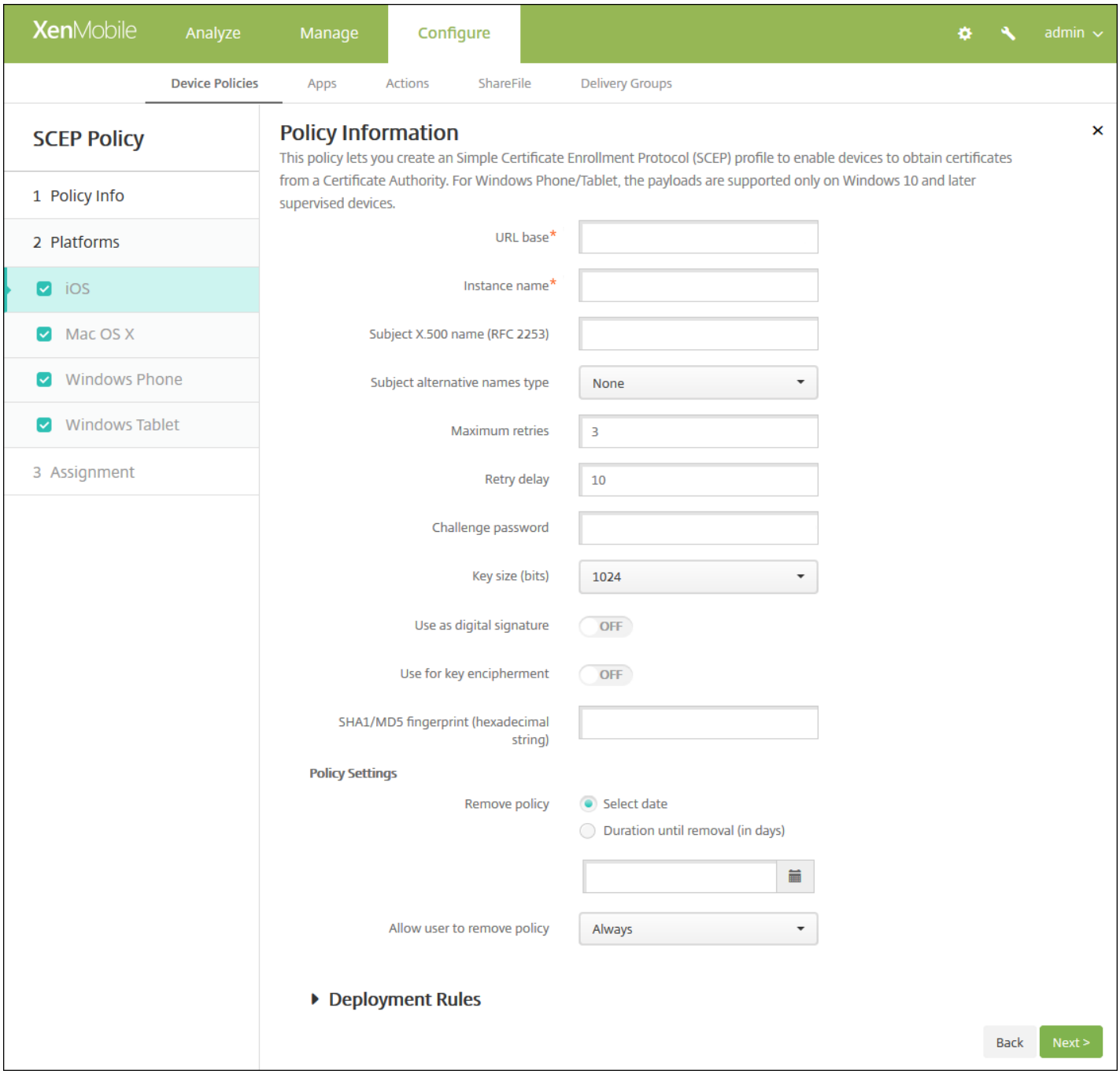
5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

Wenn Sie mit dem Konfigurieren der Einstellungen für eine Plattform fertig sind, finden Sie Anleitungen zum Festlegen der

Bereitstellungsregeln für diese Plattform unter Schritt 7.

Konfigurieren von iOS-Einstellungen



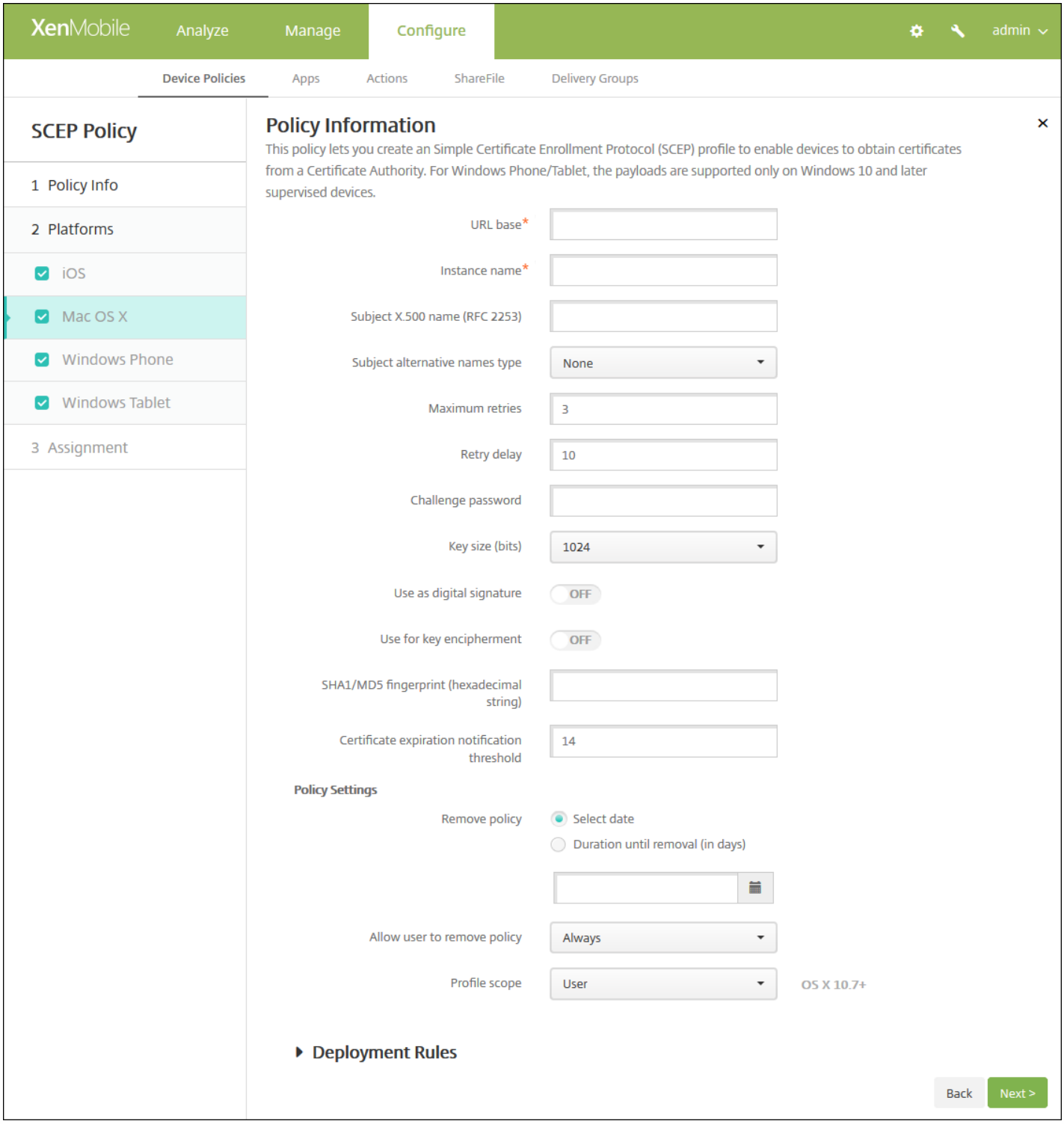
Konfigurieren Sie folgende Einstellungen:

- **URL-Basis**: 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.
- **Instanzname**: 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.

- **X.500-Name des Antragstellers (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.
- Klicken Sie in der Liste **Alternativer Antragstellernamenstyp** 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 **Ohne**, **RFC 822-Name**, **DNS-Name** und **URI**.
- **Wiederholungsversuche maximal**: Geben Sie die Anzahl der Wiederholungsversuche für den Fall ein, dass der SCEP-Server eine AUSSTEHEND-Antwort an Geräte sendet. Der Standardwert ist **3**.
- **Wiederholungsverzögerung**: Geben Sie die Wartezeit in Sekunden zwischen den Wiederholungsversuchen ein. Der erste Wiederholungsversuch erfolgt ohne Verzögerung. Der Standardwert ist **10**.
- **Kennwort überprüfen**: Geben Sie einen gemeinsamen geheimen Schlüssel ein.
- **Schlüsselgröße (Bit)**: Klicken Sie in der Liste auf die Schlüsselgröße in Bit (**1024** oder **2048**). Der Standardwert ist **1024**.
- **Als digitale Signatur verwenden**: 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.
- **Für Schlüsselchiffrierung verwenden**: 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.
- **SHA1/MD5-Fingerabdruck (hexadezimale Zeichenfolge)**: Wenn Ihre Zertifizierungsstelle HTTP verwendet, geben Sie hier den Fingerabdruck des ZS-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.
- **Richtlinieneinstellungen**
  - Klicken Sie unter **Richtlinieneinstellungen** für **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

Konfigurieren von Mac OS X-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **URL-Basis**: 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.
- **Instanzname**: 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.

- **X.500-Name des Antragstellers (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.
- Klicken Sie in der Liste **Alternativer Antragstellernamenstyp** 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 **Ohne**, **RFC 822-Name**, **DNS-Name** und **URI**.
- **Wiederholungsversuche maximal**: Geben Sie die Anzahl der Wiederholungsversuche für den Fall ein, dass der SCEP-Server eine AUSSTEHEND-Antwort an Geräte sendet. Der Standardwert ist **3**.
- **Wiederholungsverzögerung**: Geben Sie die Wartezeit in Sekunden zwischen den Wiederholungsversuchen ein. Der erste Wiederholungsversuch erfolgt ohne Verzögerung. Der Standardwert ist **10**.
- **Kennwort überprüfen**: Geben Sie einen gemeinsamen geheimen Schlüssel ein.
- **Schlüsselgröße (Bit)**: Klicken Sie in der Liste auf die Schlüsselgröße in Bit (**1024** oder **2048**). Der Standardwert ist **1024**.
- **Als digitale Signatur verwenden**: 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.
- **Für Schlüsselchiffrierung verwenden**: 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.
- **SHA1/MD5-Fingerabdruck (hexadezimale Zeichenfolge)**: Wenn Ihre Zertifizierungsstelle HTTP verwendet, geben Sie hier den Fingerabdruck des ZS-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.
- **Richtlinieneinstellungen**
  - Klicken Sie unter **Richtlinieneinstellungen** für **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.
  - Klicken Sie neben **Gültigkeitsbereich für Profil** auf **Benutzer** oder **System**. Der Standardwert ist **Benutzer**. Diese Option ist nur für OS X 10.7 und höher verfügbar.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die SCEP-Richtlinie wird angezeigt.

9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.

- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist "Jetzt".
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Geräterichtlinie für Sideloadingschlüssel

Jul 28, 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.

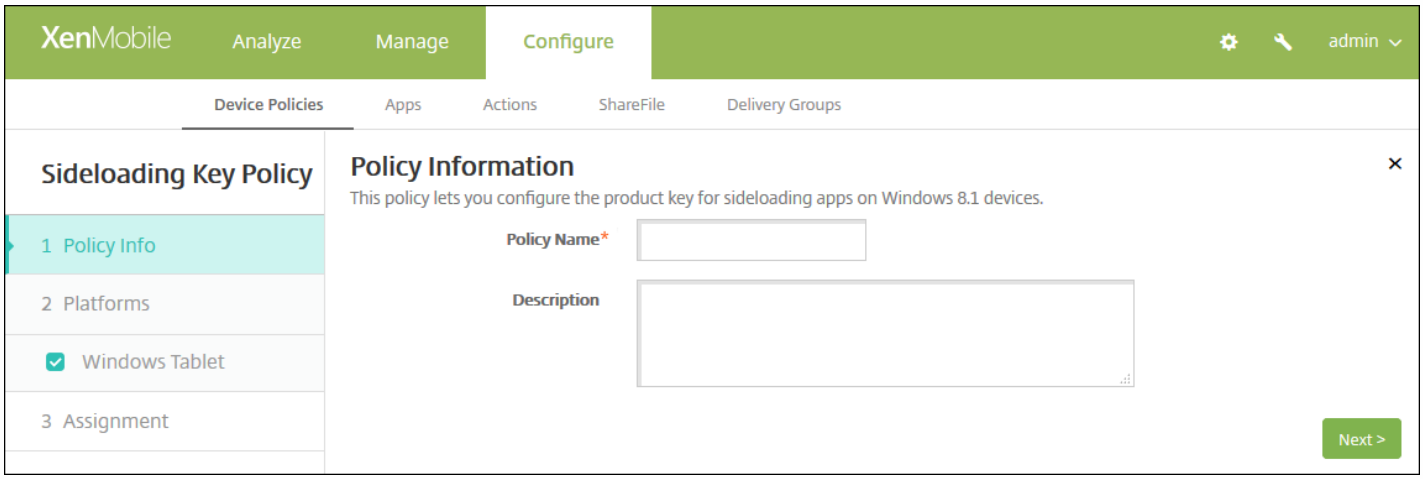
Sie benötigen zum Erstellen der Richtlinie die folgenden Informationen:

- 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 **Konfigurieren > Geräterichtlinien**. Die Seite **Geräterichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

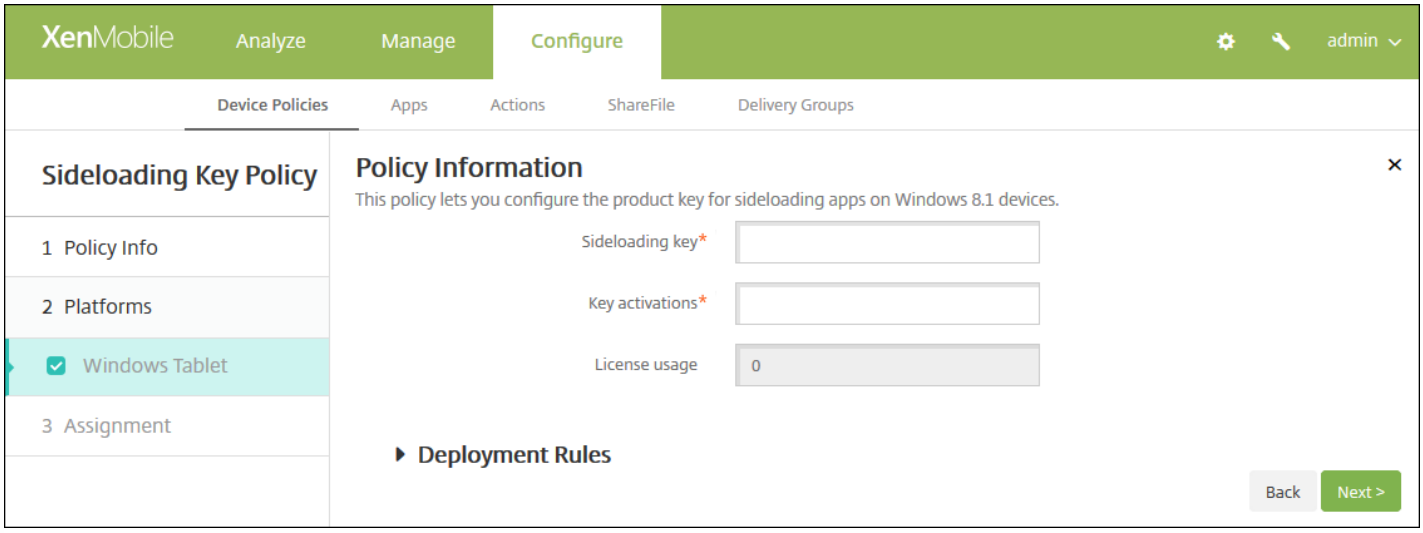
3. Erweitern Sie **Mehr** und klicken Sie dann unter **Apps** auf **Sideloadingschlüssel**. Die Seite **Sideloadingschlüssel** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Informationsseite zur Windows Tablet-Plattform wird angezeigt.

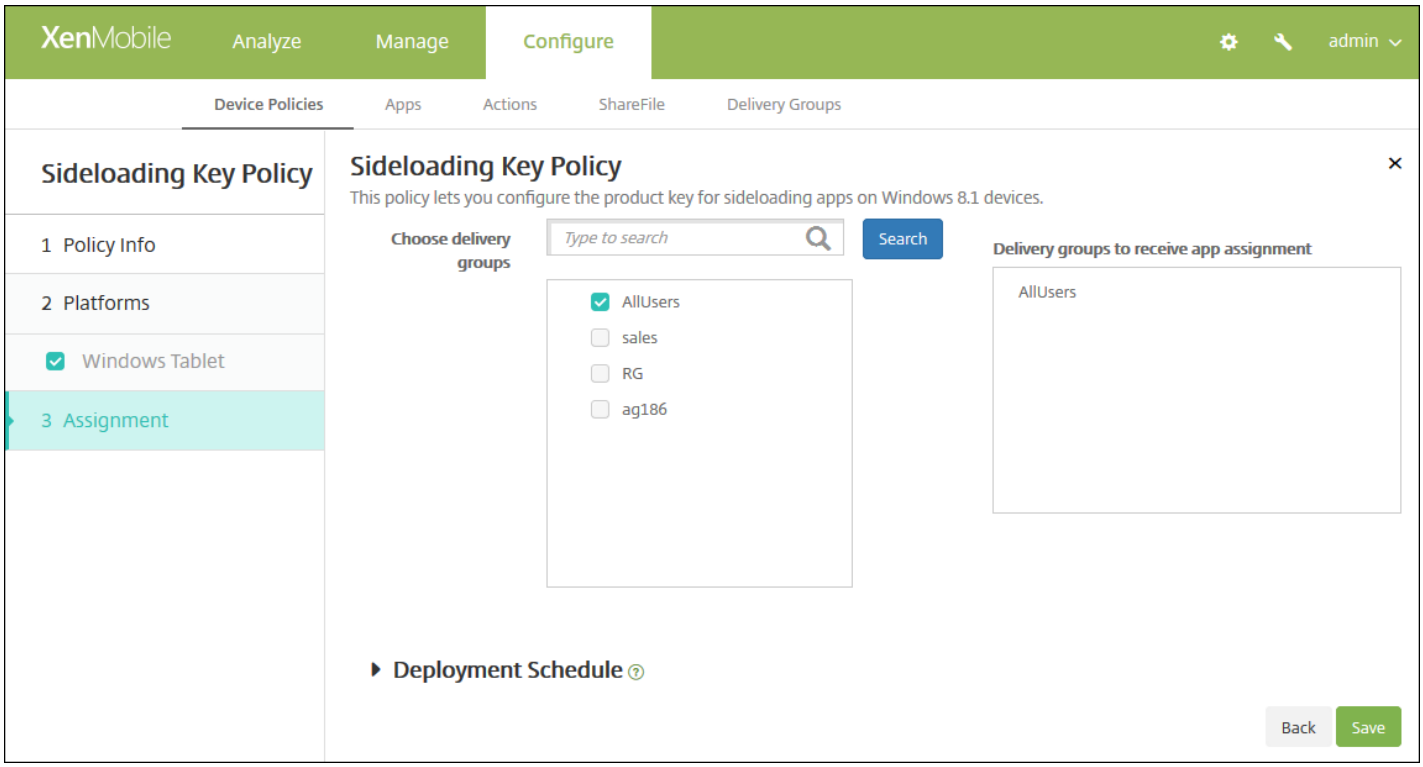


6. Konfigurieren Sie die folgenden Einstellungen:

- **Sideloadingschlüssel**: Geben Sie den Sideloadingschlüssel ein, den Sie vom Microsoft Volume Licensing Service Center erhalten haben.
- **Schlüsselaktivierungen**: Geben Sie die Schlüsselaktivierung ein, die Sie für den Sideloadingschlüssel erstellt haben.
- **Lizenzverwendung**: XenMobile berechnet diesen Wert abhängig von der Zahl angemeldeter Tablets. Sie können dieses Feld nicht ändern.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Sideloadingschlüsselrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie "Bereitstellungszeitplan" und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Geräterichtlinie für Signaturzertifikate

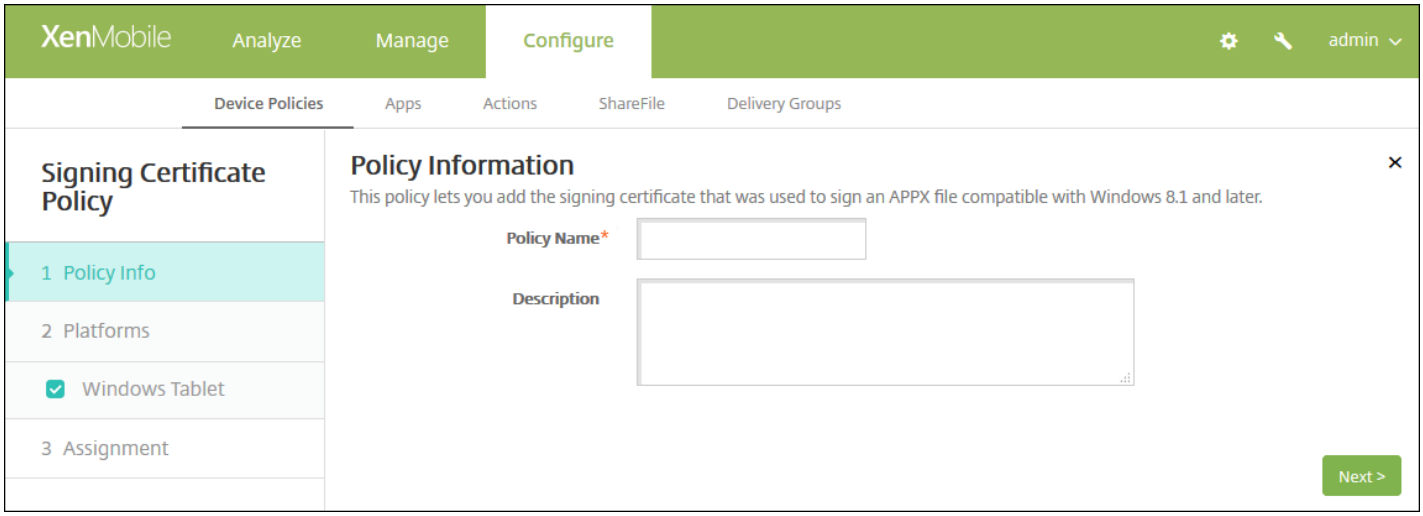
Jul 28, 2016

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-Tablets installieren können.

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

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

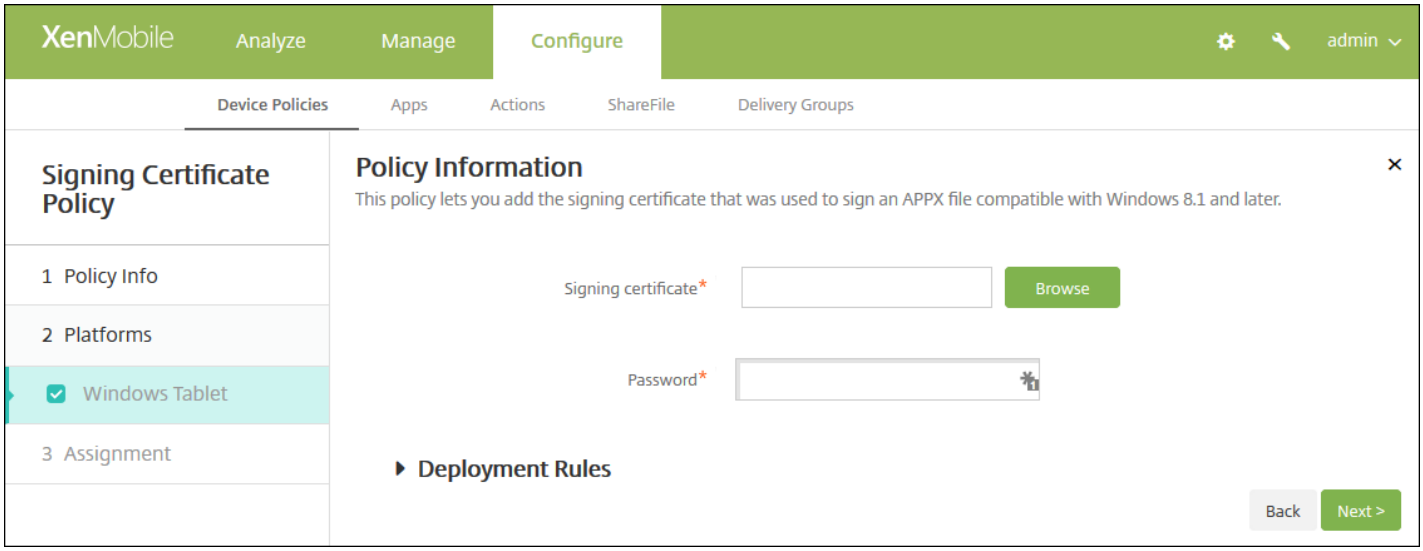
3. Klicken Sie auf **Mehr** und dann unter **Apps** auf **Signaturzertifikat**. Die Seite **Signaturzertifikat** wird angezeigt.



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

- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.
- **Beschreibung**: Geben Sie optional eine Beschreibung für die Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Plattformseite für Windows Tablet wird angezeigt.

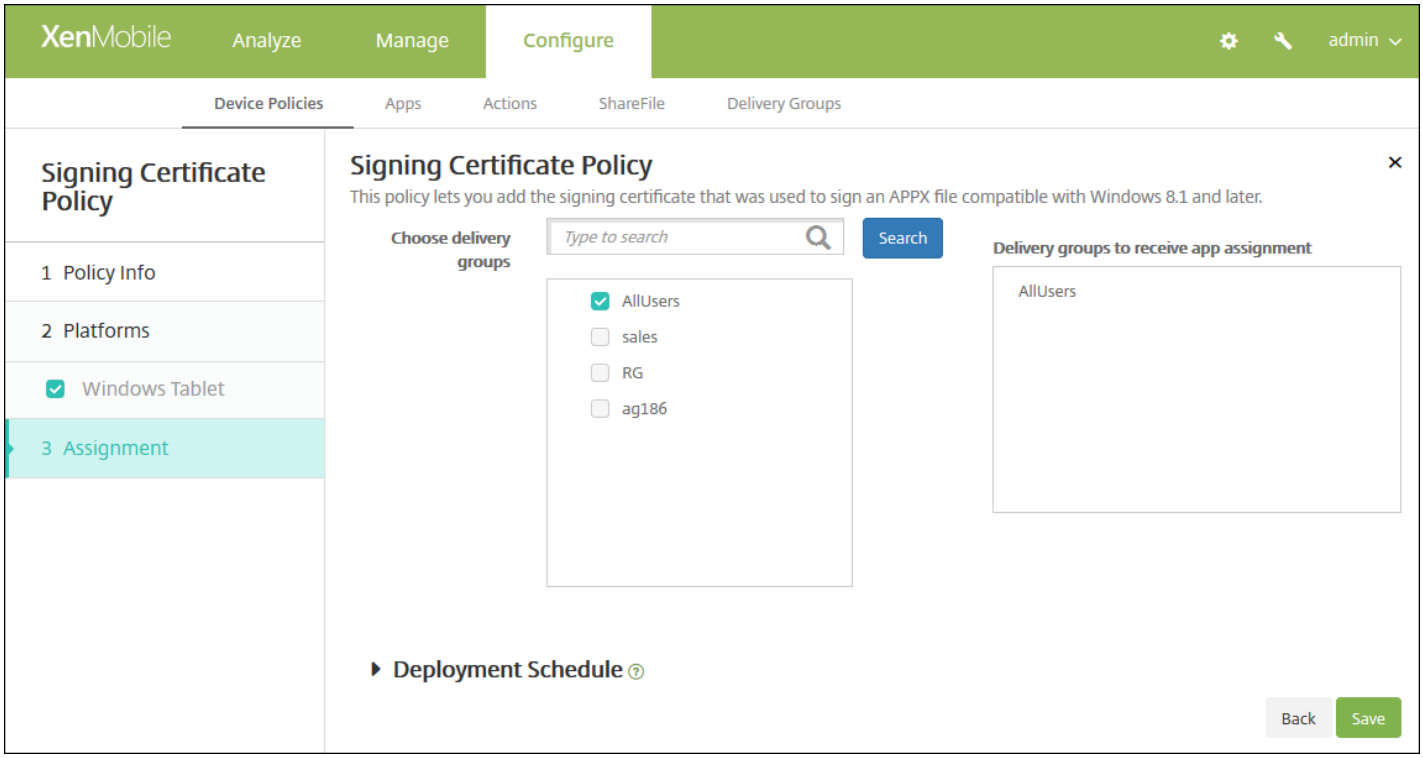


6. Konfigurieren Sie die folgenden Einstellungen:

- **Signaturzertifikat**: Klicken Sie auf **Durchsuchen**, navigieren Sie zum Speicherort des Zertifikats, das zum Signieren der APPX-Datei verwendet wurde, und wählen Sie es aus.
- **Kennwort**: Geben Sie das Kennwort für den Zugriff auf das Signaturzertifikat ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Signaturzertifikat** wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:
- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen gemachten Änderungen werden auf alle Plattformen angewendet. Ausnahme bildet die Einstellung **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

Single Sign-On-Kontorichtlinien

Jul 28, 2016

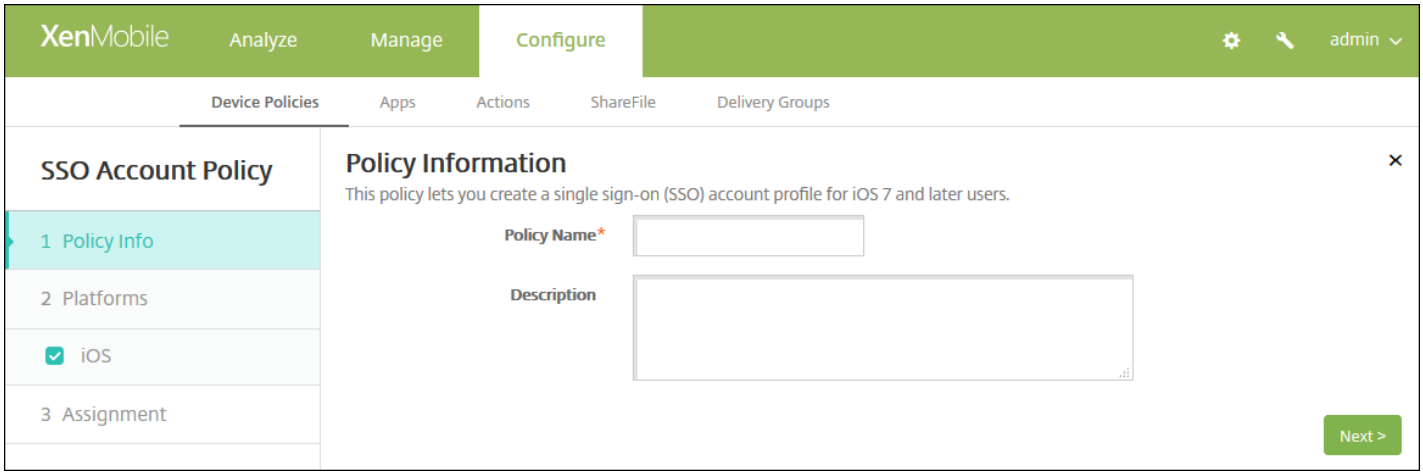
Sie erstellen Single Sign-On-Konten (SSO) in XenMobile, damit Benutzer nach einmaliger Anmeldung auf XenMobile und interne Unternehmensressourcen von unterschiedlichen Apps aus zugreifen können. Sie müssen keine Anmeldeinformationen auf dem Gerät speichern. Die Unternehmensanmeldeinformationen des SSO-Kontos 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 **Konfigurieren > Geräterichtlinien**. Die Seite **Geräterichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

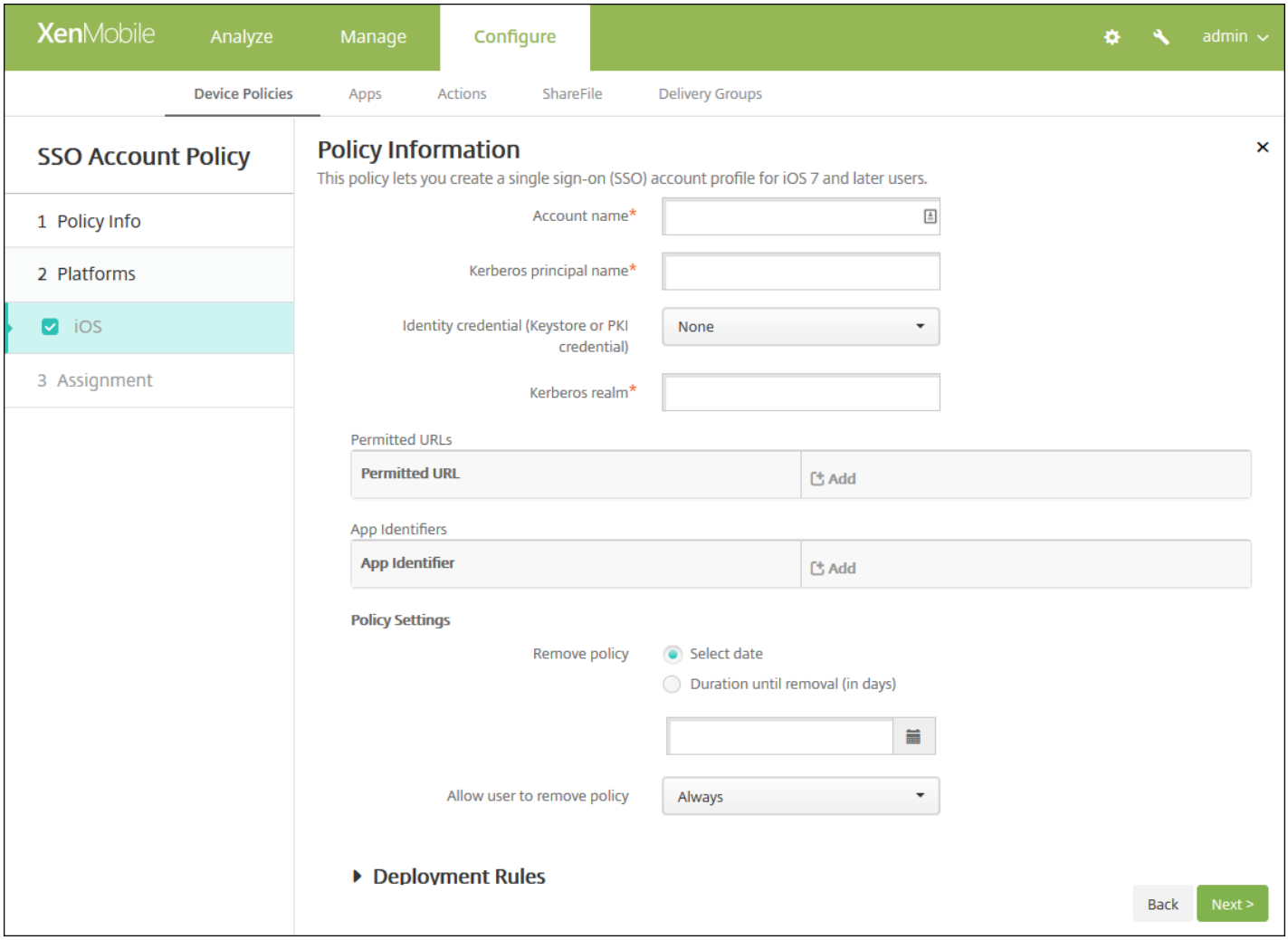
3. Klicken Sie auf **Mehr** und dann unter **Endbenutzer** auf **SSO-Konto**. Die Seite für die Richtlinieninformationen der Richtlinie **SSO-Konto** wird angezeigt.



4. Geben Sie auf der Seite **Richtlinieninformationen** die folgenden Informationen ein:

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

5. Klicken Sie auf **Weiter**. Die Seite für iOS wird angezeigt.



6. Konfigurieren Sie die folgenden Einstellungen:

- **Kontoname**: Geben Sie den Kerberos-SSO-Kontonamen ein, der auf dem Benutzergerät angezeigt wird. Diese Angabe ist erforderlich.
- **Kerberos-Prinzipalname**: Geben Sie den Kerberos-Prinzipalnamen ein. Diese Angabe ist erforderlich.
- **Identitätsanmeldeinformationen (Schlüsselspeicher oder PKI-Anmeldeinformationen)**: Klicken Sie in der Liste auf optionale Anmeldeinformationen zum Verlängern der Kerberos-Anmeldeinformationen ohne Benutzereingriff.
- **Kerberos-Bereich**: Geben Sie den Kerberos-Bereich für die Richtlinie ein. Dies ist normalerweise der Domänenname in Großbuchstaben (z. B. EXAMPLE.COM). Diese Angabe ist erforderlich.
- **Zulässige URLs**: Für jede URL, die SSO erfordern soll, klicken Sie auf **Hinzufügen** und führen Sie folgende Schritte aus:
  - **Zulässige 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.
  - Klicken Sie auf **Hinzufügen**, um die URL hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

- **App-IDs**: Klicken Sie für jede App, bei der die Verwendung von SSO zulässig sein soll, auf **Hinzufügen** und führen Sie die folgenden Schritte aus:
  - **App-ID**: Geben Sie eine App-ID für eine App ein, bei der die Verwendung der Anmeldung zulässig sein soll. Wenn Sie keine App-ID angeben, gilt die Anmeldung für **alle** App-IDs.
  - Klicken Sie auf **Hinzufügen**, um die App-ID hinzuzufügen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

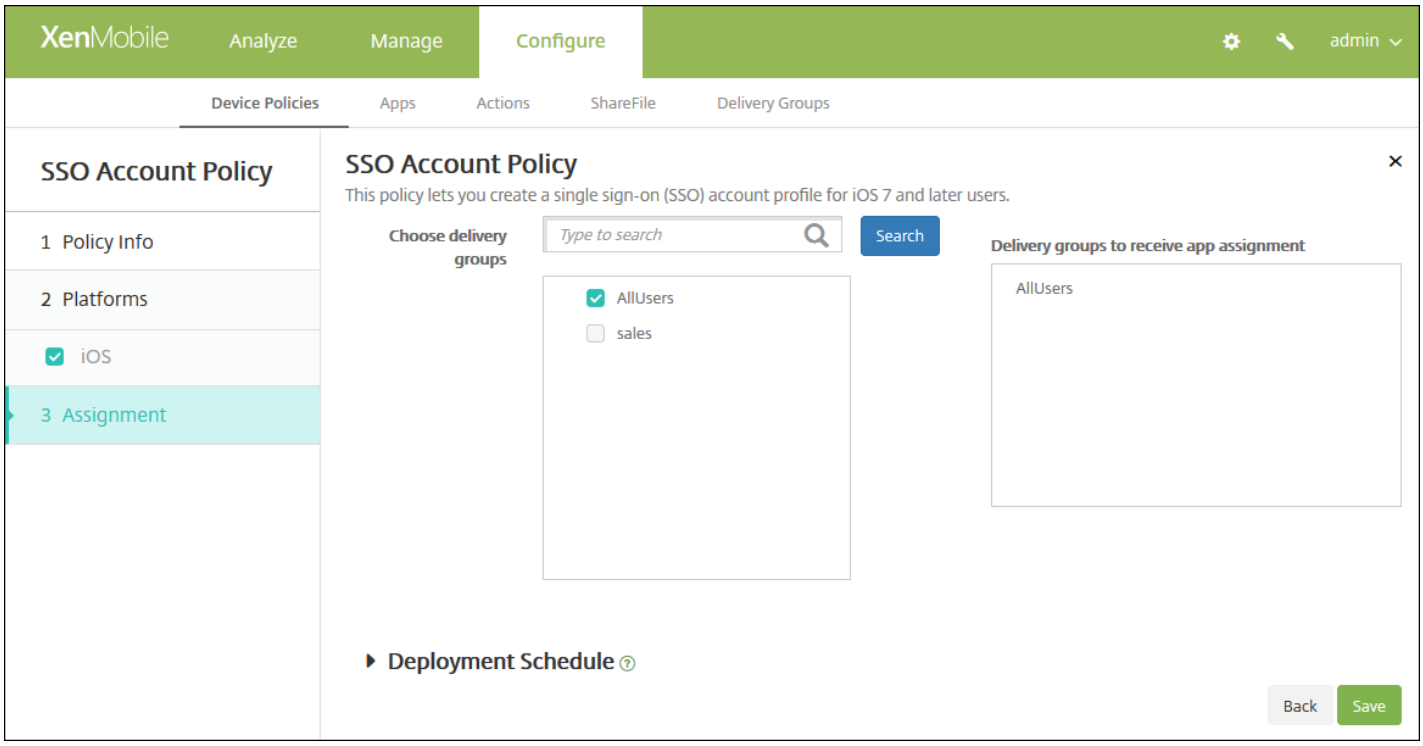
    Hinweis: Zum Löschen vorhandener URLs oder App-IDs zeigen Sie auf deren Zeile und klicken Sie auf das Papierkorbsymbol auf der rechten Seite. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie auf "Löschen" zum Löschen des Eintrags oder auf "Bearbeiten", um ihn beizubehalten.

    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 "Speichern", um die Änderungen zu speichern oder auf "Abbrechen", um den Vorgang abzubrechen.

- **Richtlinieneinstellungen**
  - Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die SSO-Kontorichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

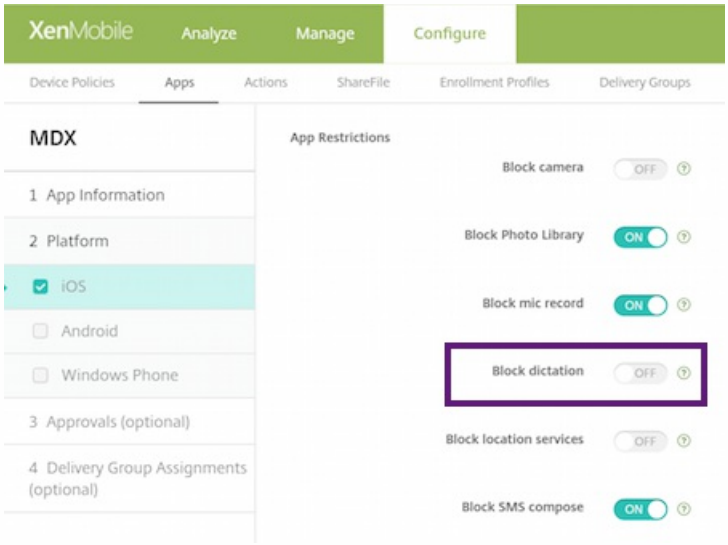
Richtlinien für Siri und die Diktierfunktion

Jul 28, 2016

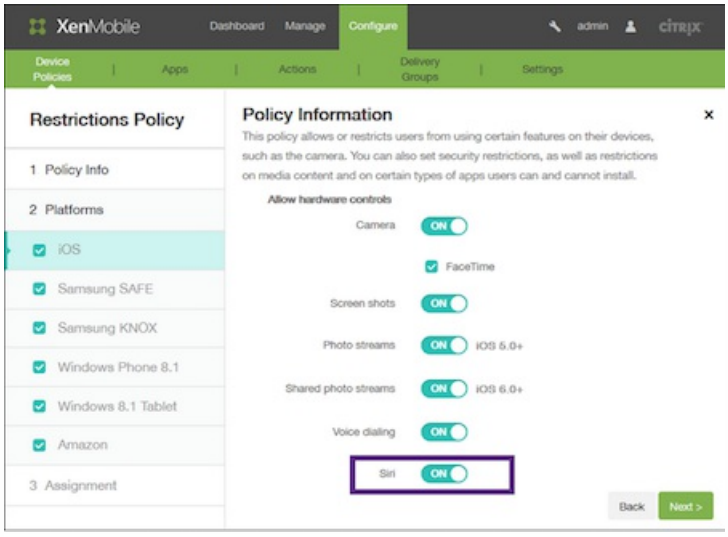
Wenn Benutzer auf einem iOS-Gerät Siri eine Frage stellen oder Text diktieren, werden die Sprachdaten von Apple zur Verbesserung von Siri gesammelt. Die Sprachdaten werden über die cloudbasierten Dienste von Apple gesendet und verlassen somit den sicheren XenMobile-Container. Diktierter Text verbleibt dagegen im Container.

Über XenMobile können Sie, falls Ihre Sicherheitsrichtlinien dies erfordern, Siri und die Diktierfunktion deaktivieren.

In MAM-Bereitstellungen ist die Richtlinie **Diktat blockieren** für jede App standardmäßig auf **Ein** festgelegt, wodurch das Mikrofon deaktiviert wird. Wenn Sie die Diktierfunktion zulassen möchten, legen Sie die Richtlinie auf **Aus** fest. Die Richtlinie können Sie auf der XenMobile-Konsole unter **Konfigurieren > Apps** aufrufen. Wählen Sie die App, klicken Sie auf **Bearbeiten** und klicken Sie dann auf **iOS**.



In MDM-Bereitstellungen können Sie Siri außerdem über die Siri-Richtlinie unter **Konfigurieren > Geräterichtlinien > Einschränkungen > iOS** deaktivieren. Die Verwendung von Siri ist standardmäßig zugelassen.



Bei der Entscheidung, ob Sie Siri und die Diktierfunktion zulassen, sollten Sie Folgendes erwägen:

- Gemäß von Apple veröffentlichten Informationen speichert Apple Sprachclips von Siri und der Diktierfunktion zwei Jahre lang. Den Daten wird eine zufällig gewählte Nummer zugewiesen, die den Benutzer repräsentiert. Weitere Informationen finden Sie in dem Wired-Artikel Apple reveals how long Siri keeps your data.
- Die Apple-Datenschutzrichtlinie können Sie auf jedem iOS-Gerät über **Einstellungen > Allgemein > Tastaturen** und Tippen auf den Link unter **Diktierfunktion aktivieren** aufrufen.

Speicherverschlüsselungsrichtlinie für Geräte

Jul 28, 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 Phone- und Android-Sony-Geräte erstellen. Jede Plattform erfordert andere Werte. Diese werden im vorliegenden Artikel detailliert beschrieben.

Samsung SAFE-Einstellungen

Windows Phone-Einstellungen

Android Sony-Einstellungen

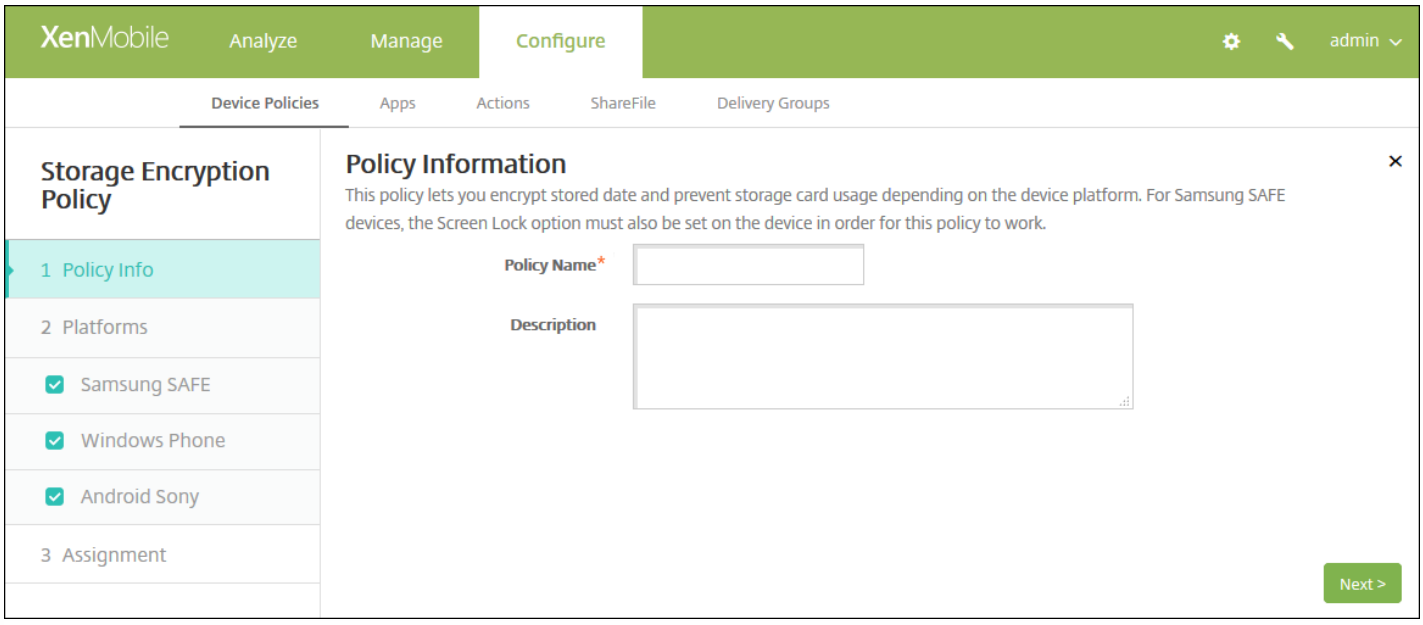
Hinweis: Vergewissern Sie sich vor der Konfiguration dieser Richtlinie, dass bei Samsung SAFE-Geräten die folgenden Anforderungen erfüllt sind:

- 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 **Konfigurieren > Gerätерichtlinien**. Die Seite **Gerätерichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

3. Klicken Sie auf **Mehr** und dann unter **Sicherheit** auf **Speicherverschlüsselung**. Die Seite **Verschlüsselung des Speichers** wird angezeigt.



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

- **Richtlinienname**: Geben Sie einen aussagekräftigen Namen für die Richtlinie ein.

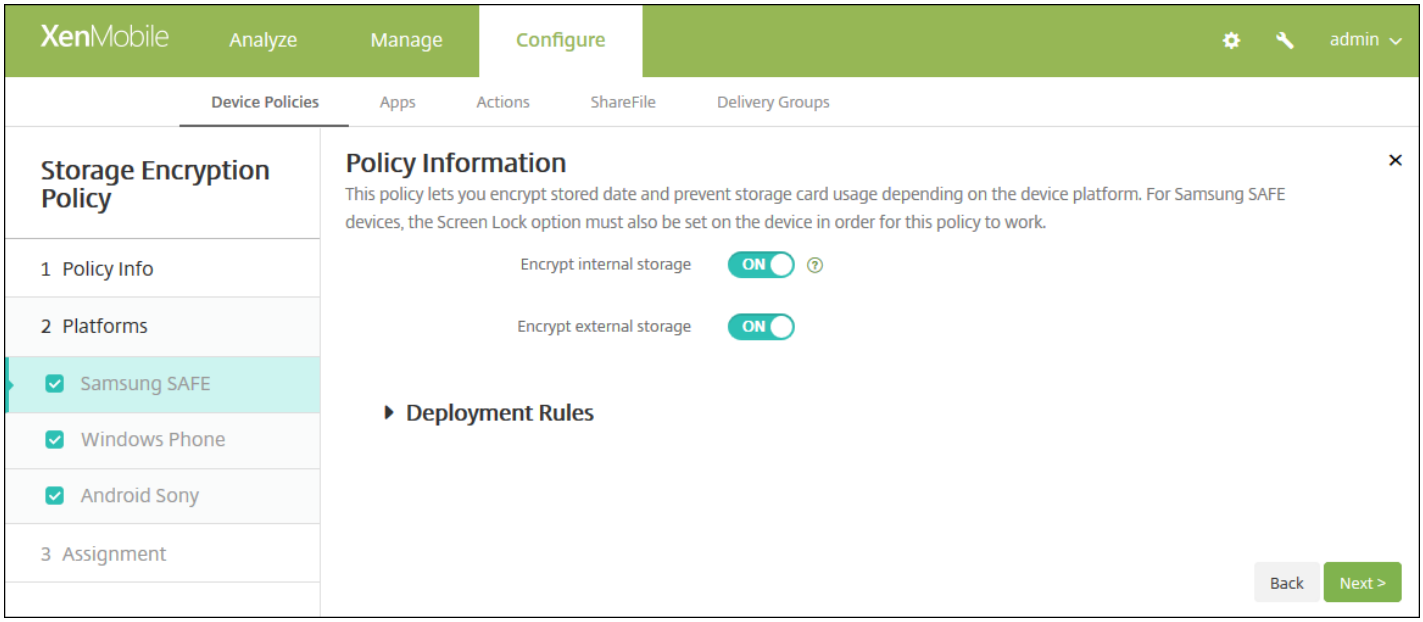
- **Beschreibung**: Geben Sie optional eine Beschreibung der Richtlinie ein.

5. Klicken Sie auf **Weiter**. Die Seite **Plattformen** wird angezeigt.

6. Wählen Sie unter **Plattformen** die gewünschten Plattformen aus. Wenn Sie nur eine Plattform konfigurieren, deaktivieren Sie die anderen.

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

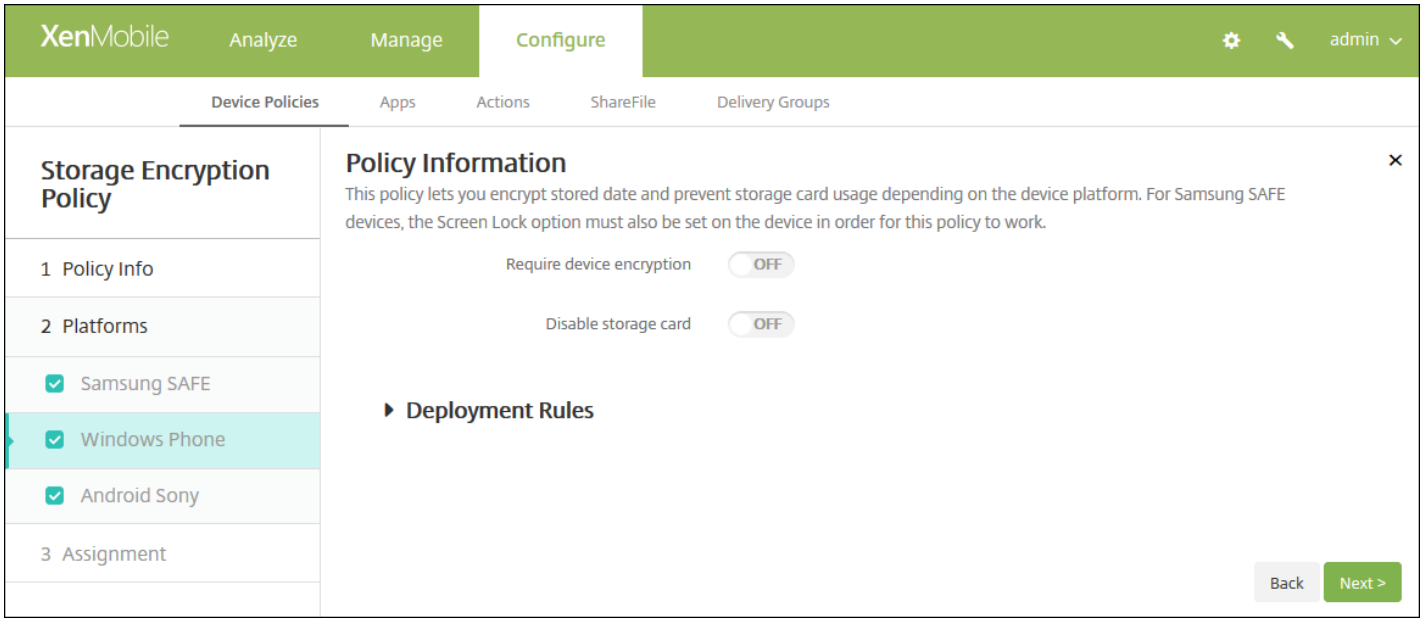
Konfigurieren der Samsung SAFE-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Internen Speicher verschlüsseln**: Wählen Sie aus, ob der interne Speicher auf Geräten verschlüsselt werden soll. Zum internen Speicher gehört auch der Gerätespeicher. Die Standardeinstellung ist **EIN**.
- **Externen Speicher verschlüsseln**: Wählen Sie aus, ob der externe Speicher auf Geräten verschlüsselt werden soll. Die Standardeinstellung ist **EIN**.

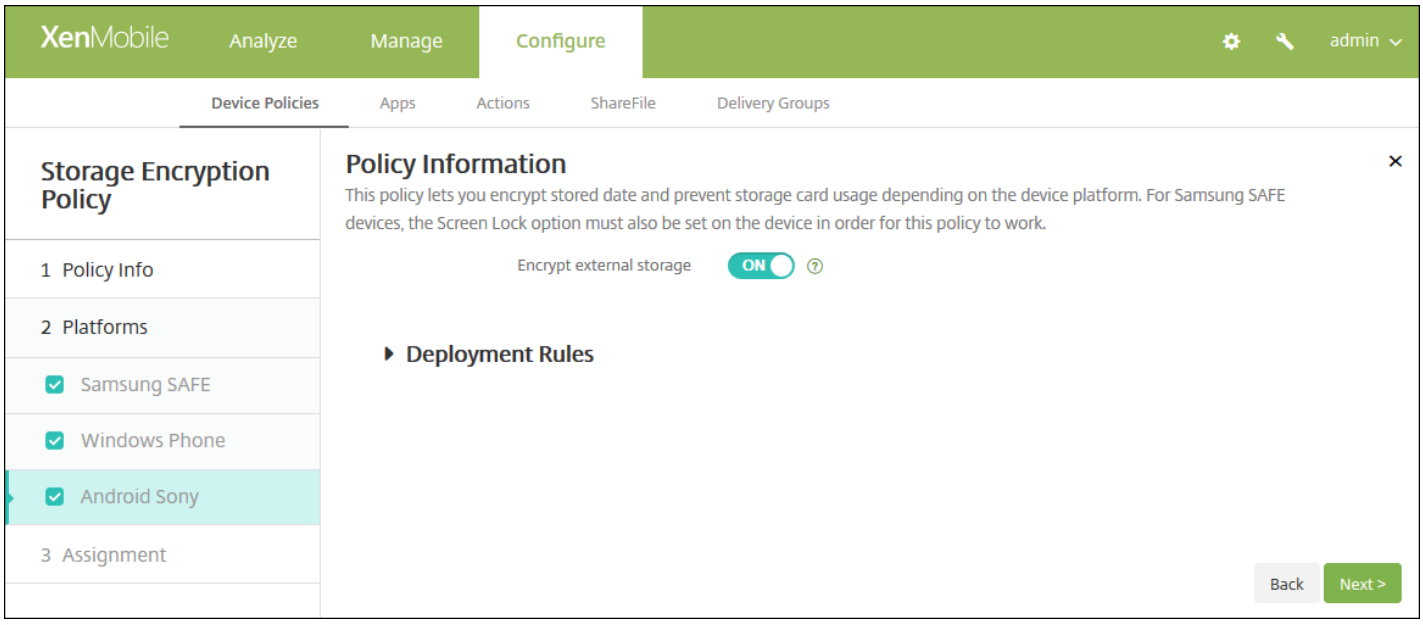
Konfigurieren von Windows Phone-Einstellungen



Konfigurieren Sie folgende Einstellungen:

- **Geräteverschlüsselung erforderlich**: Wählen Sie aus, ob die Geräte der Benutzer verschlüsselt werden sollen. Der Standardwert ist **AUS**.
- **Speicherkarte deaktivieren**: Wählen Sie aus, ob die Verwendung der Speicherkarte der Geräte unterbunden werden soll. Der Standardwert ist **AUS**.

Konfigurieren von Android Sony-Einstellungen

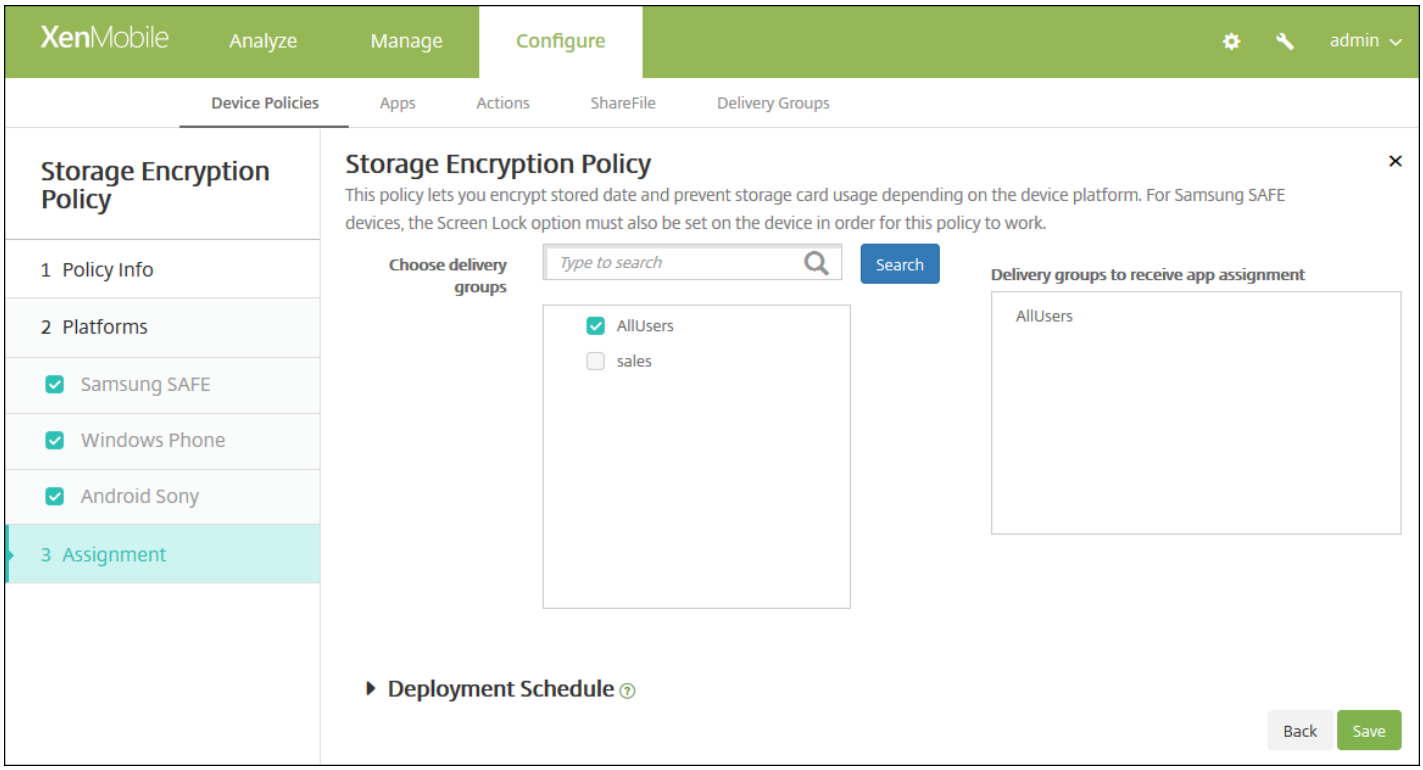


Konfigurieren Sie folgende Einstellung:

- **Externen Speicher verschlüsseln**: Wählen Sie 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 **EIN**.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Speicherrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

11. Klicken Sie auf **Speichern**.

Richtlinie für abonnierte Kalender

Jul 28, 2016

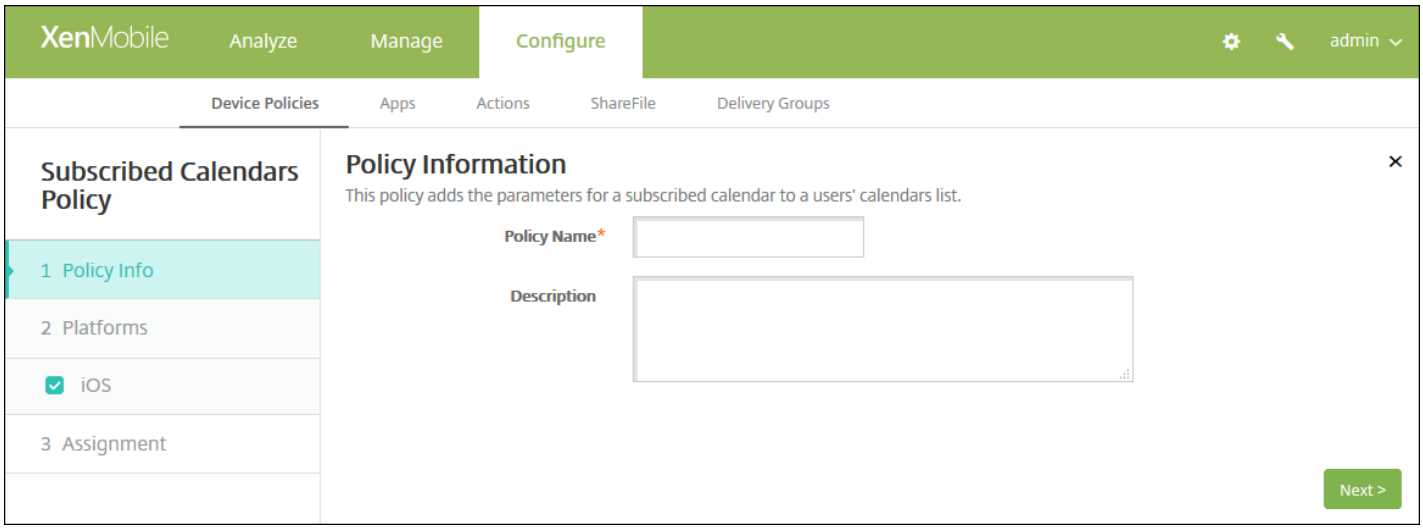
Sie können in XenMobile eine Richtlinie einrichten, mit der ein abonnierter Kalender der Liste der Kalender auf iOS-Geräten hinzugefügt wird. Die Liste der öffentlichen Kalender, die zum Abonnieren verfügbar sind, finden Sie unter www.apple.com/downloads/macosx/calendars.

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 **Konfigurieren > Gerätерichtlinien**. Die Seite **Gerätерichtlinien** wird angezeigt.

2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Neue Richtlinie hinzufügen** wird angezeigt.

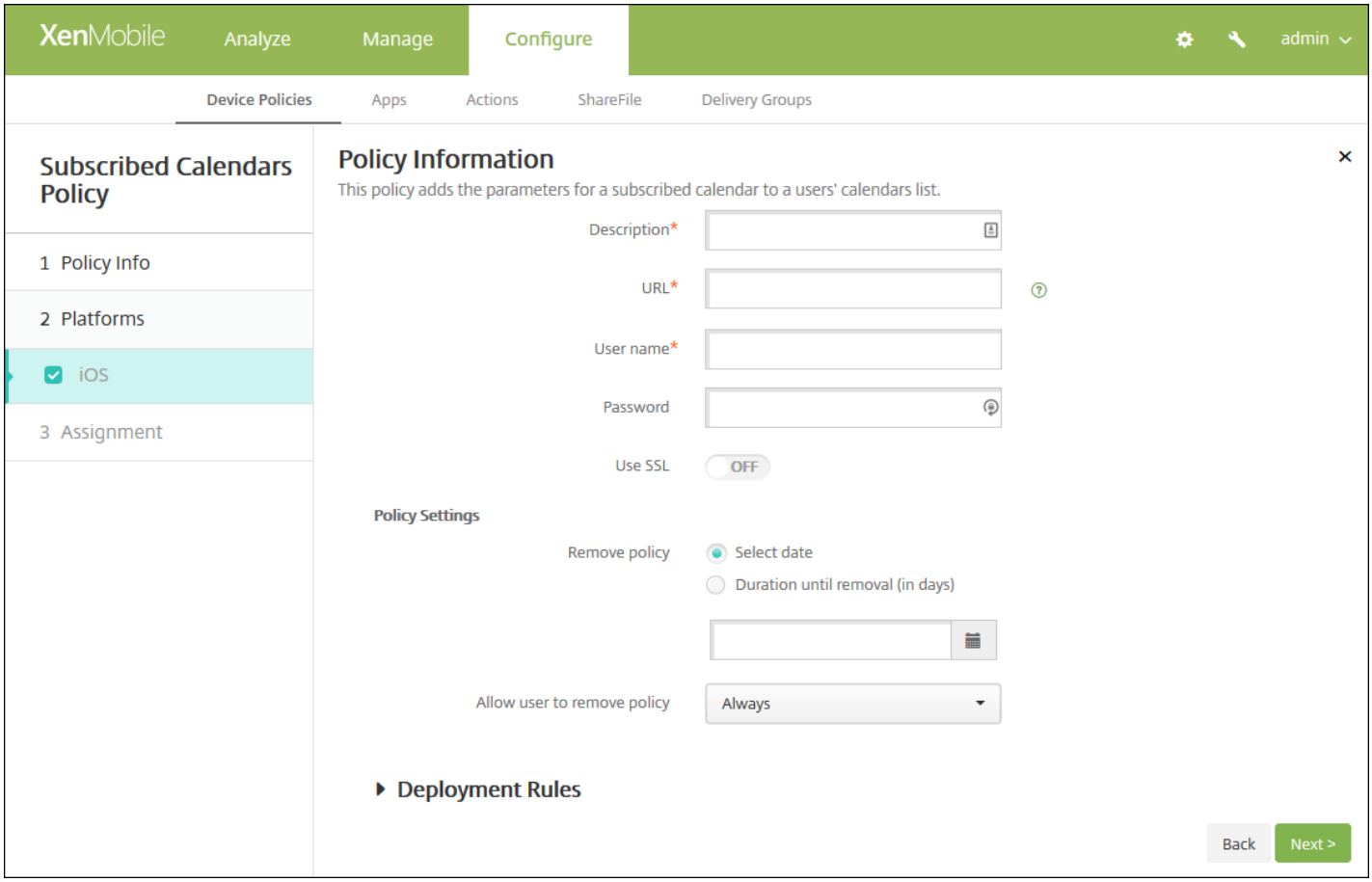
3. Klicken Sie auf **Mehr** und dann unter **Endbenutzer** auf **Abonnierte Kalender**. Die Seite für die Richtlinieninformationen der Richtlinie **Abonnierte Kalender** wird angezeigt.



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

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

5. Klicken Sie auf **Weiter**. Die Seite mit den Plattforminformationen für **iOS** wird angezeigt.

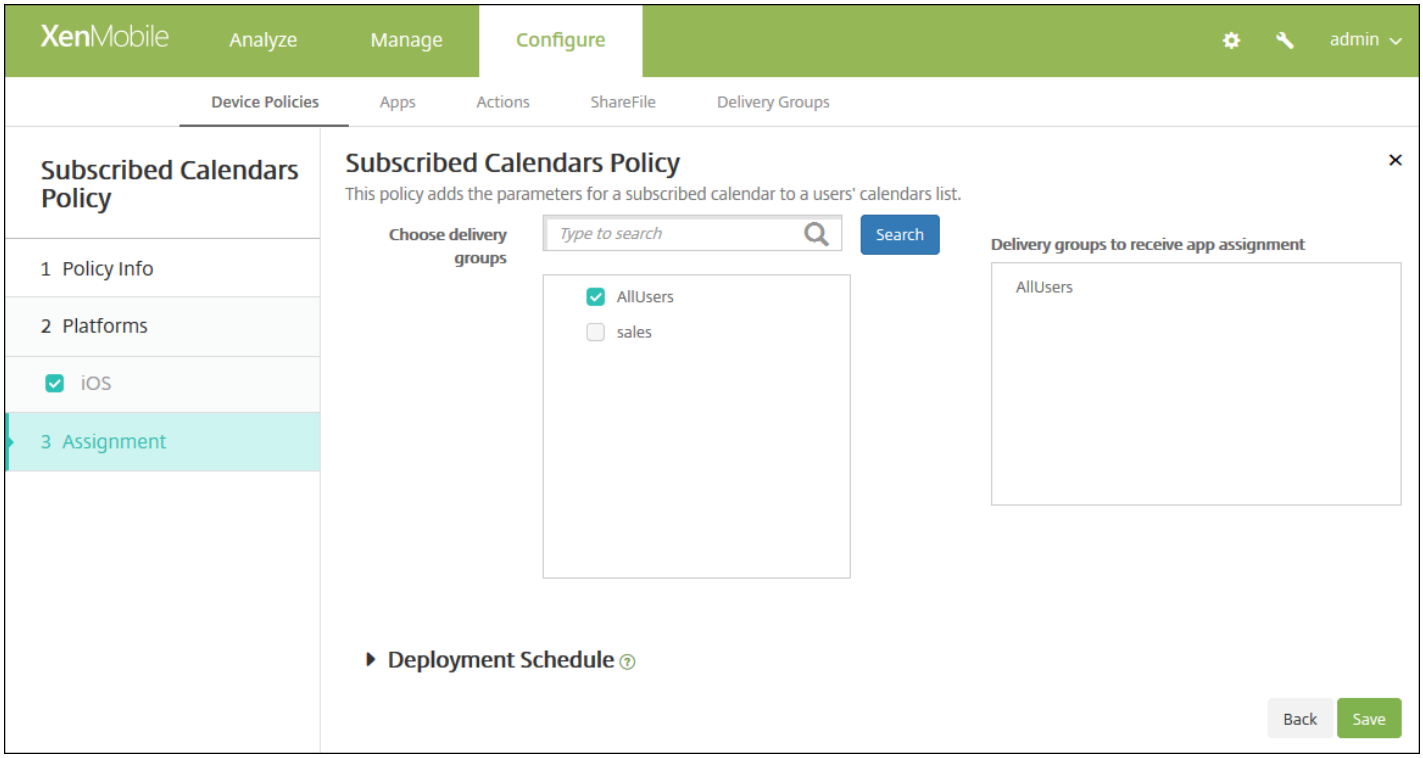


6. Konfigurieren Sie die folgenden Einstellungen:

- **Beschreibung:** Geben Sie eine Beschreibung des Kalenders ein. Diese Angabe ist erforderlich.
- **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.
- **Benutzername**: Geben Sie den Anmeldenamen des Benutzers ein. Diese Angabe ist erforderlich.
- **Kennwort**: Geben Sie ein optionales Benutzerkennwort ein.
- **SSL verwenden**: Wählen Sie aus, ob für die Verbindung mit dem Kalender Secure Socket Layer verwendet werden soll. Der Standardwert ist "Aus".
- **Richtlinieneinstellungen**
  - Klicken Sie neben **Richtlinie entfernen** auf **Datum auswählen** oder **Zeit bis zum Entfernen (in Tagen)**.
  - Bei Auswahl von **Datum auswählen** klicken Sie auf den Kalender, um das Datum für das Entfernen anzugeben.
  - Klicken Sie in der Liste **Benutzer darf Richtlinie entfernen** auf **Immer**, **Passcode erforderlich** oder **Nie**.
  - Bei Auswahl von **Passcorde erforderlich** geben Sie für **Passcode zum Entfernen** den Passcode ein.

7. Konfigurieren der Bereitstellungsregeln

8. Klicken Sie auf **Weiter**. Die Seite **Zuweisung** für die Kalenderrichtlinie wird angezeigt.



9. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

10. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

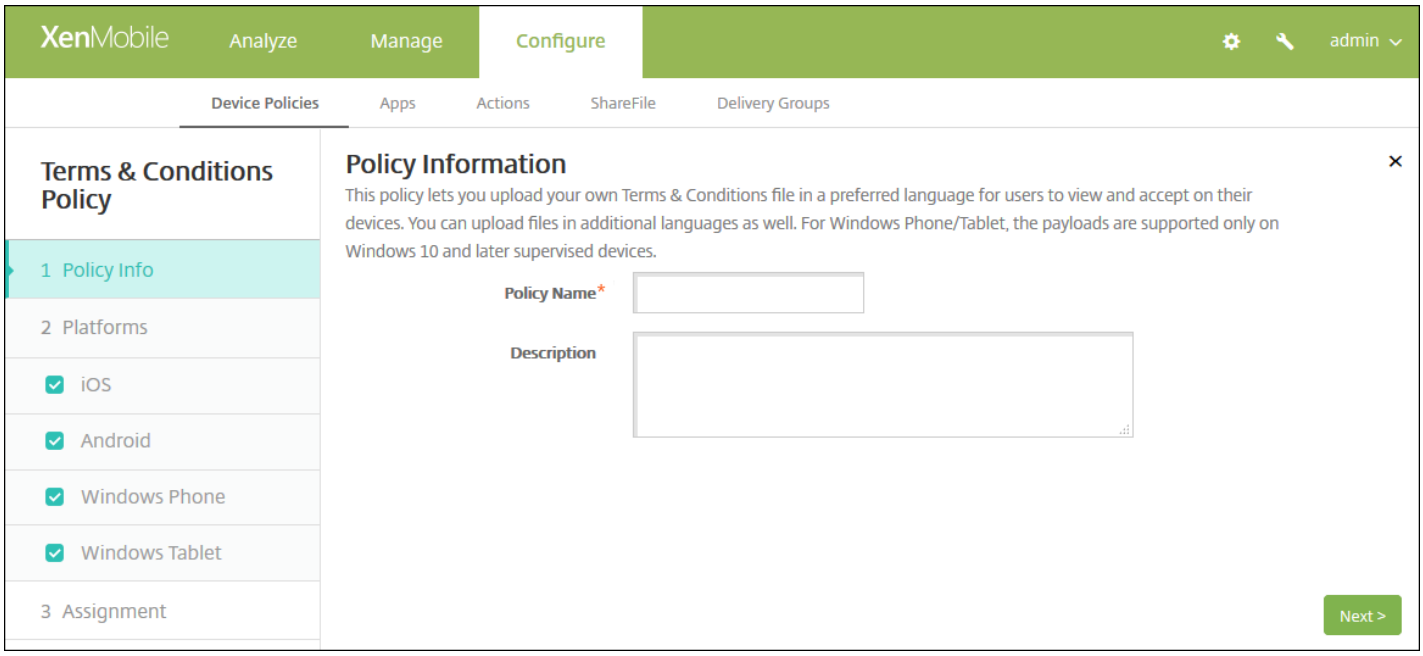
- Klicken Sie neben **Bereitstellen** auf **EIN**, um die Bereitstellung zu planen, oder auf **AUS**, um die Bereitstellung zu verhindern. Die Standardeinstellung ist **EIN**. Wenn Sie **AUS** auswählen, müssen keine anderen Optionen konfiguriert werden.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**.

Hinweis:

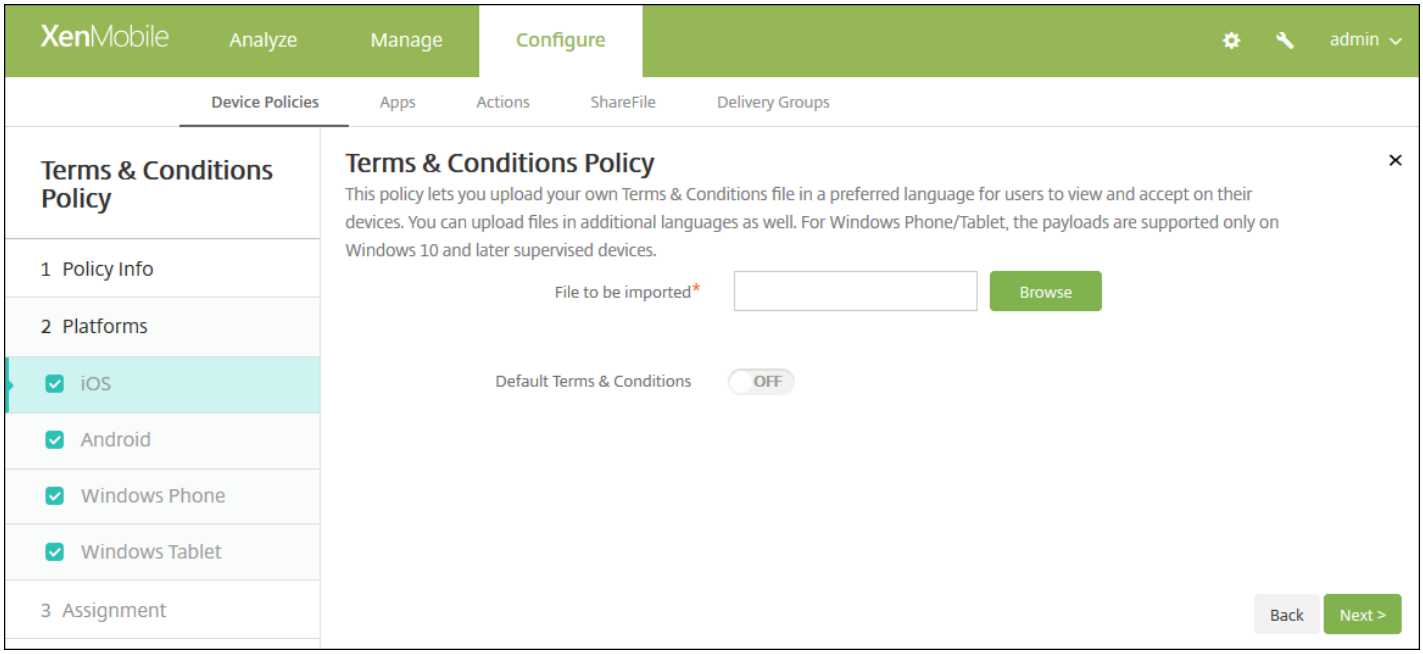
- Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- Der Bereitstellungsplan gilt für alle Plattformen. Alle von Ihnen vorgenommenen Änderungen gelten für alle Plattformen, mit Ausnahme von **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

11. Klicken Sie auf **Speichern**.

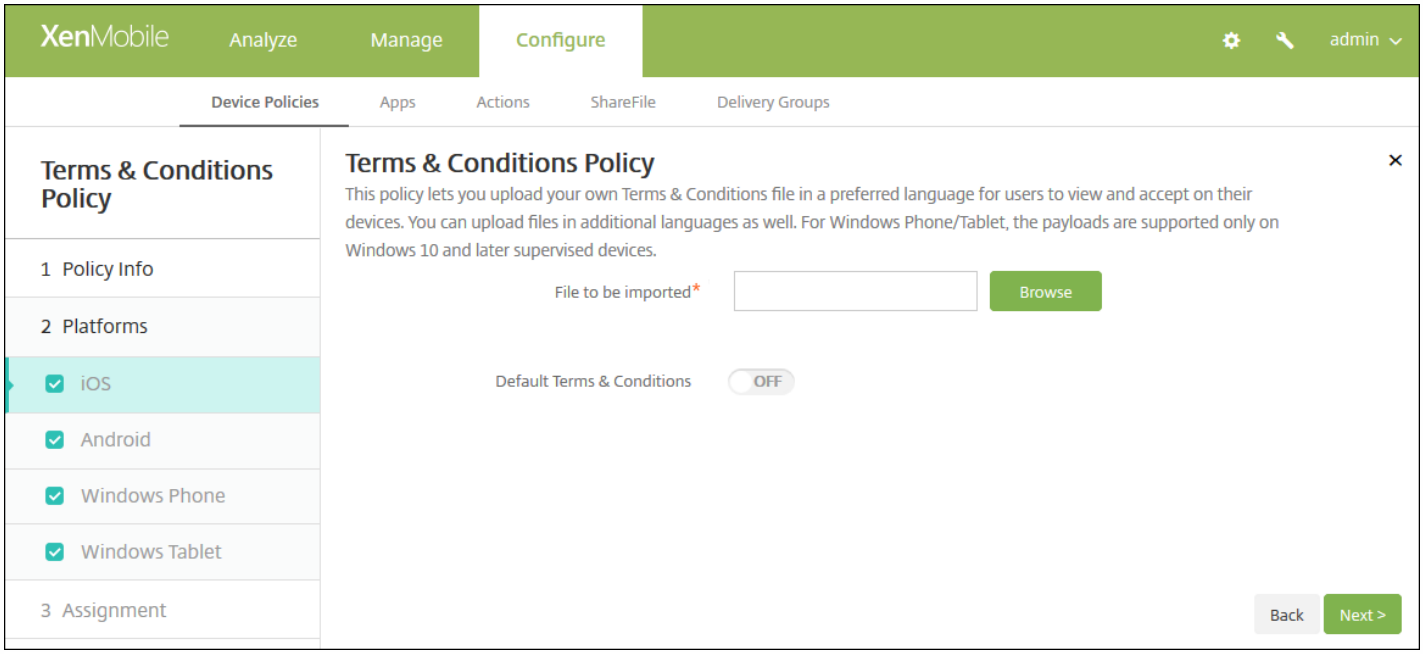
AGB-Geräterichtlinien



-
-

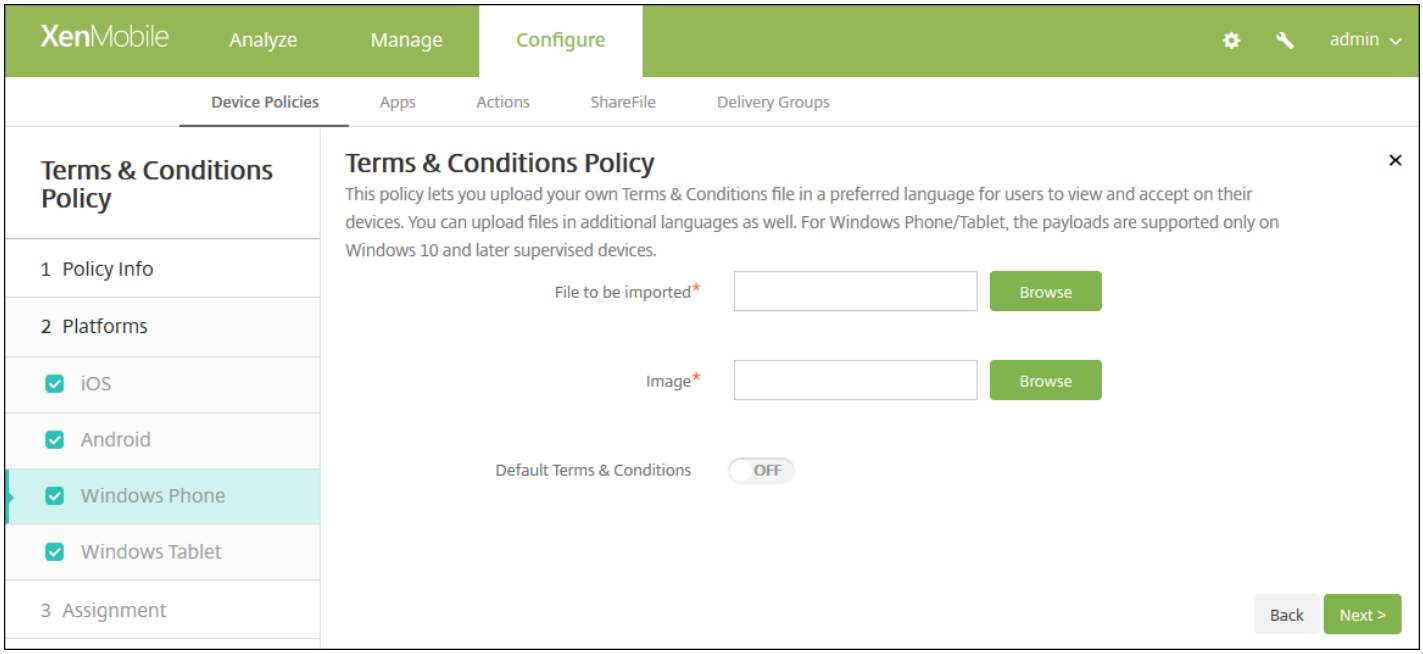


iOS- und Android-Einstellungen

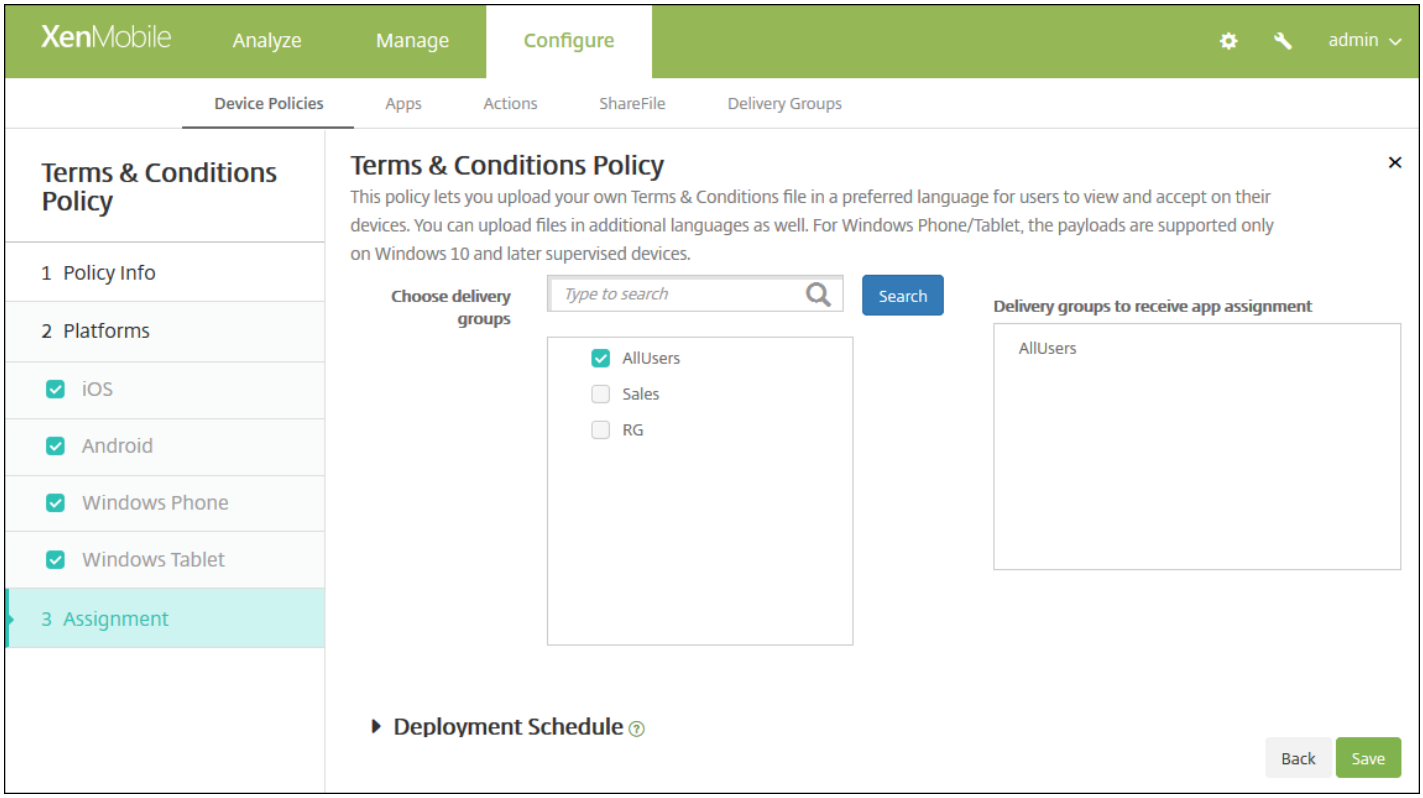


-
-

Windows Phone- und Windows Tablet-Einstellungen



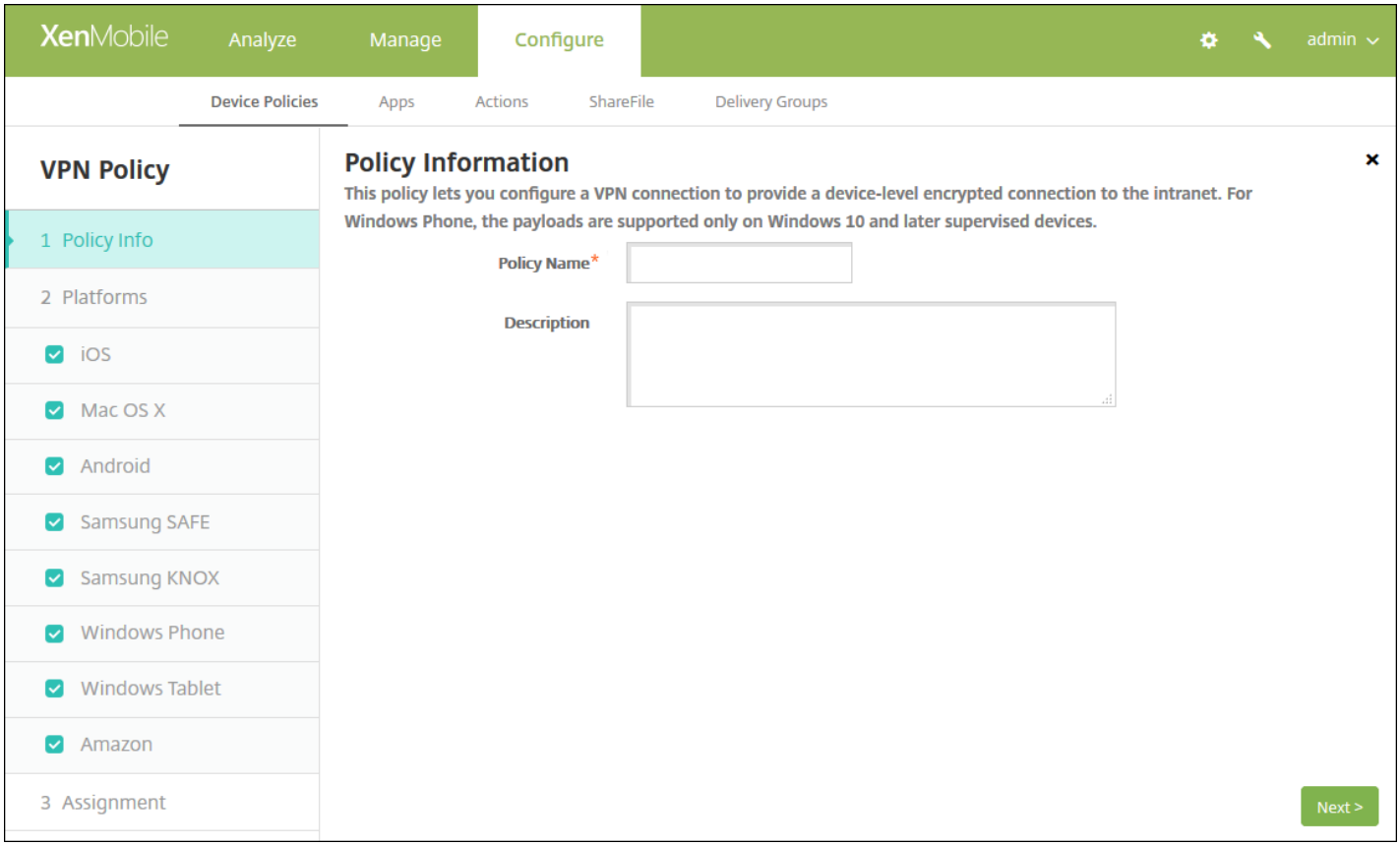
-
-
-



Versetzen eines iOS-Geräts mit dem Apple Configurator in den betreuten Modus

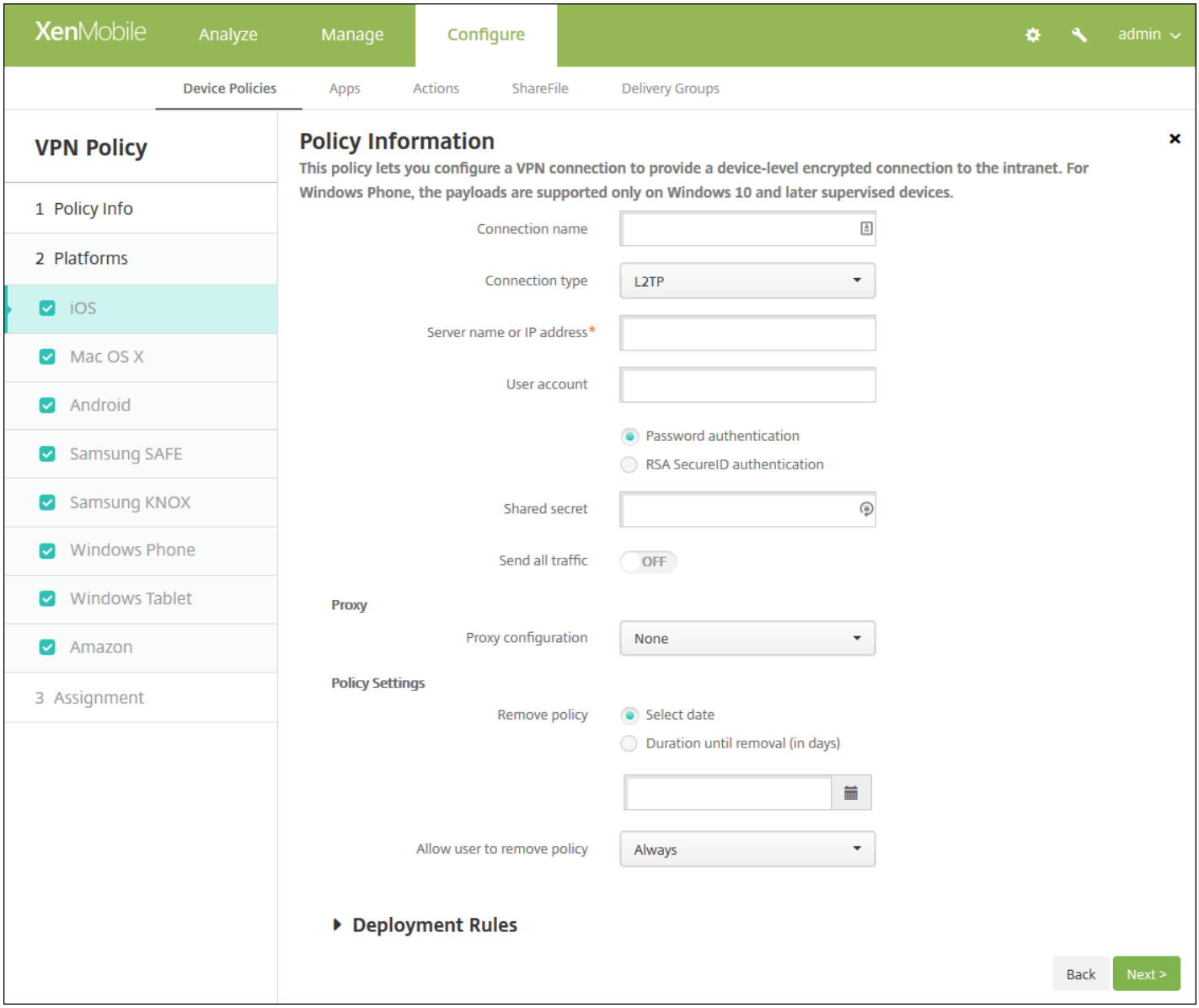
> Important

VPN-Geräterichtlinien



-
-

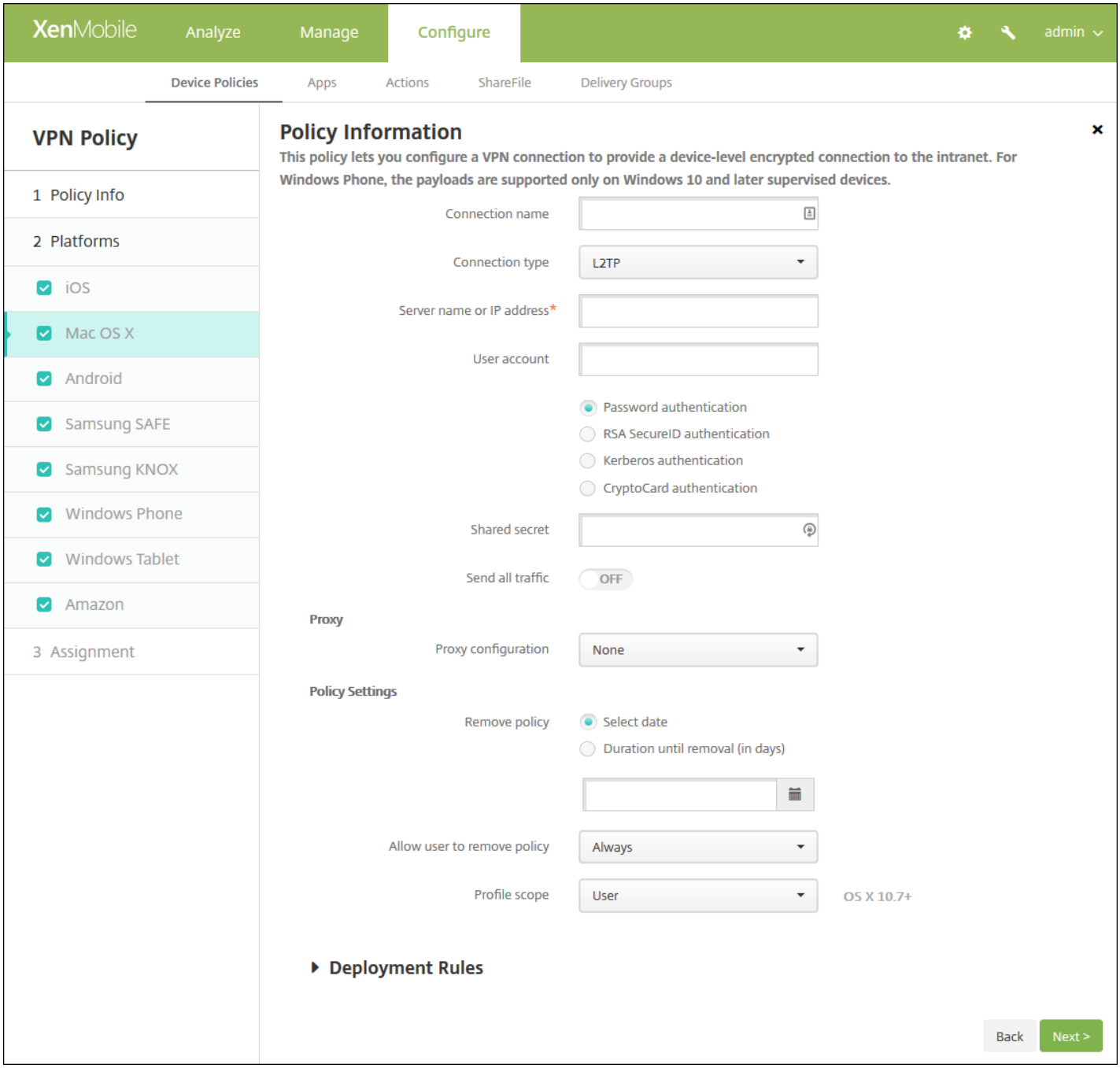
Konfigurieren von iOS-Einstellungen



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

- Konfigurieren von L2TP
- Konfigurieren von PPTP-Protokoll
- Konfigurieren von IPsec
- Konfigurieren von Cisco AnyConnect
- Konfigurieren von Juniper SSL
- Konfigurieren von F5 SSL
- Konfigurieren von SonicWALL
- Konfigurieren von Ariba VIA
- Konfigurieren von IKEv2
- Konfigurieren von Citrix VPN-Protokoll
- Konfigurieren des benutzerdefinierten SSL-Protokolls
- Konfigurieren der Einstellungen für VPN bei Bedarf

Konfigurieren von Mac OS X-Einstellungen



-
-
  -
  -
  -
  -
  -
  -

-
-
-
-

Konfigurieren von L2TP

Konfigurieren von PPTP-Protokoll

Konfigurieren von IPsec

Konfigurieren von Cisco AnyConnect

Konfigurieren von Juniper SSL

Konfigurieren von F5 SSL

Konfigurieren von SonicWALL

Konfigurieren von Ariba VIA

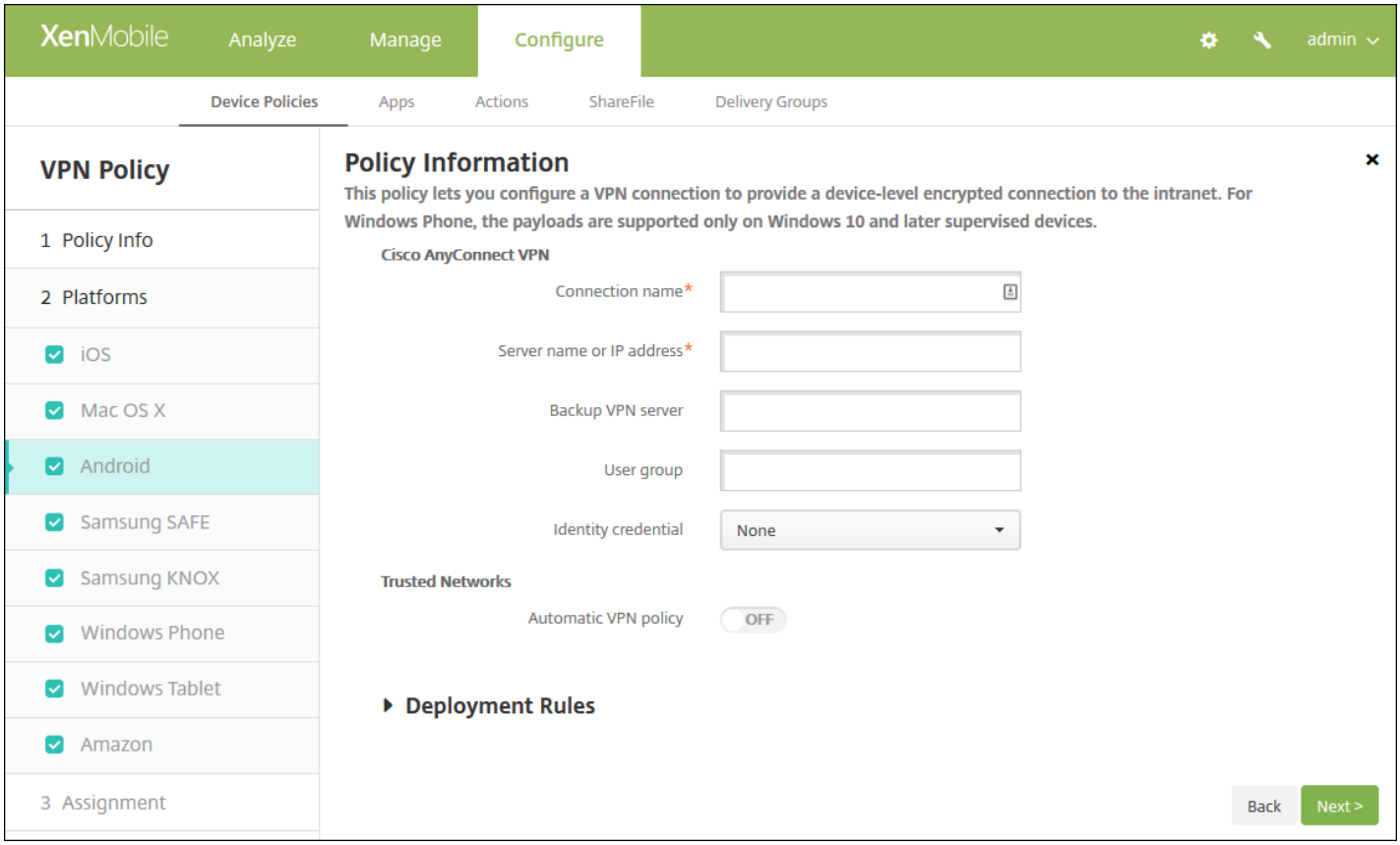
Konfigurieren von Citrix VPN-Protokoll

Konfigurieren des benutzerdefinierten SSL-Protokolls

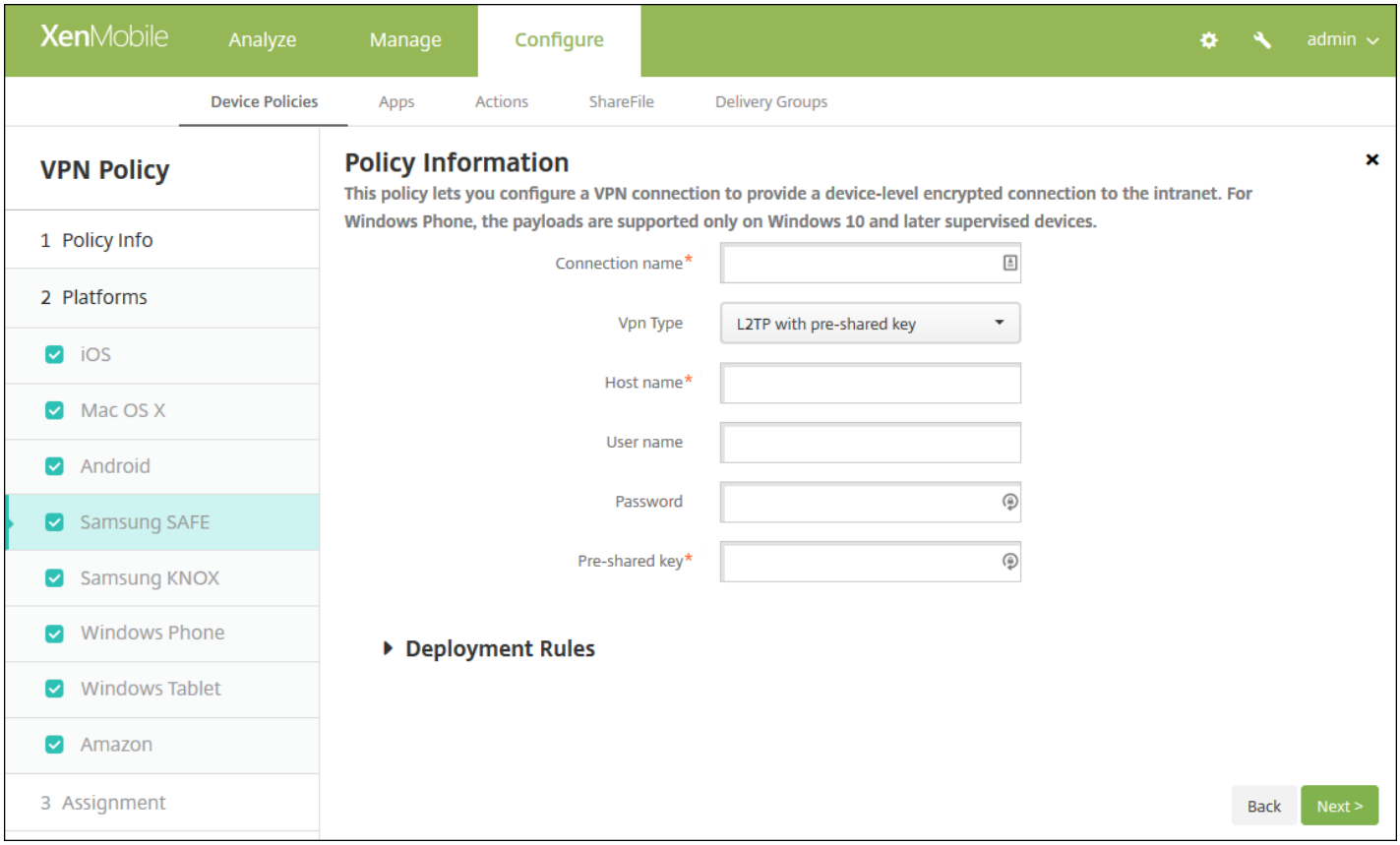
Konfigurieren der Einstellungen für VPN bei Bedarf

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

Konfigurieren von Android-Einstellungen



Konfigurieren der Samsung SAFE-Einstellungen



-
-

  -

-
-
-
-

Konfigurieren von L2TP mit vorinstalliertem Schlüssel

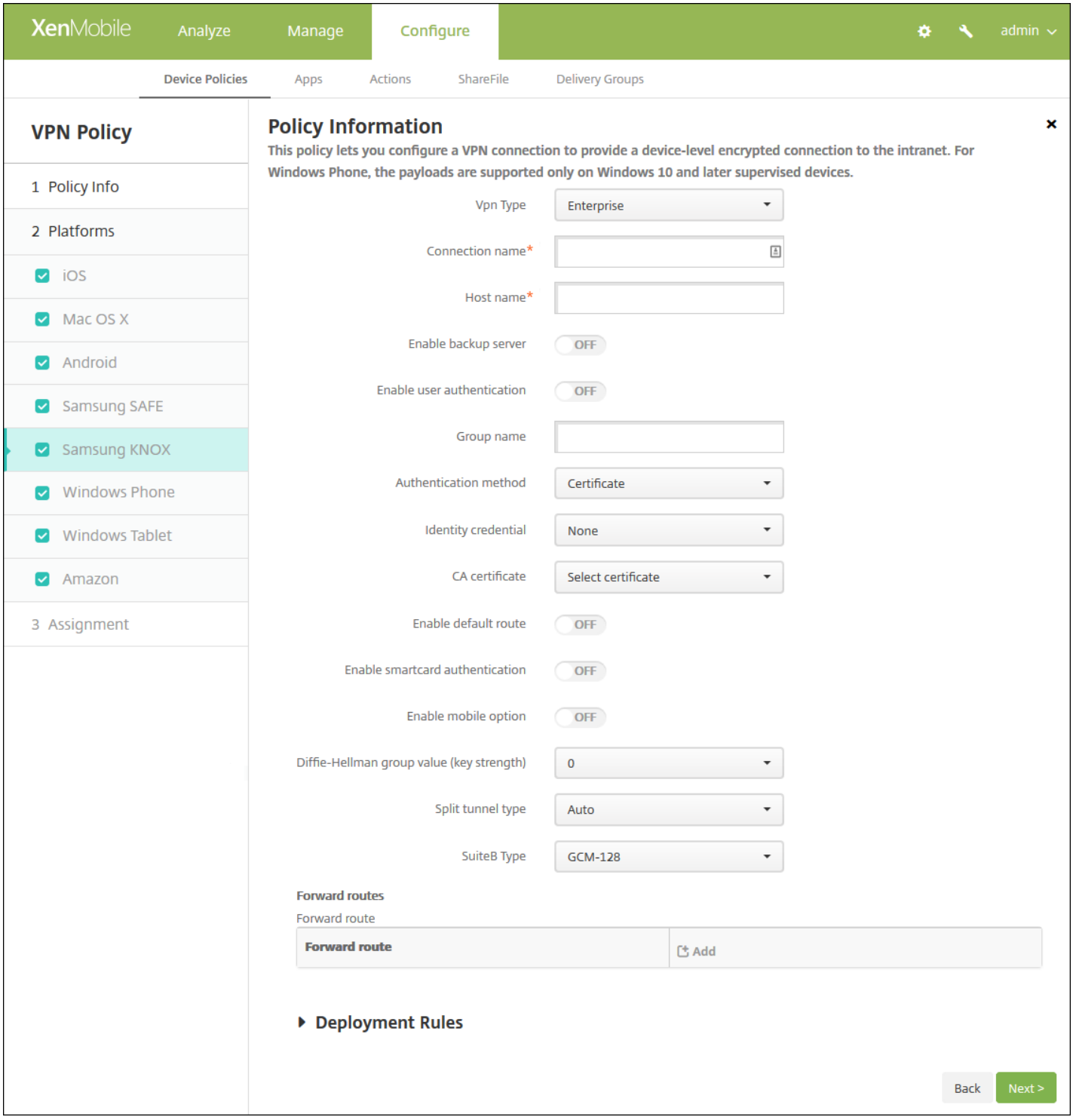
Konfigurieren von L2TP mit Zertifikat

Konfigurieren von PPTP

Konfigurieren des Enterprise-Protokolls

Konfigurieren des generischen Protokolls

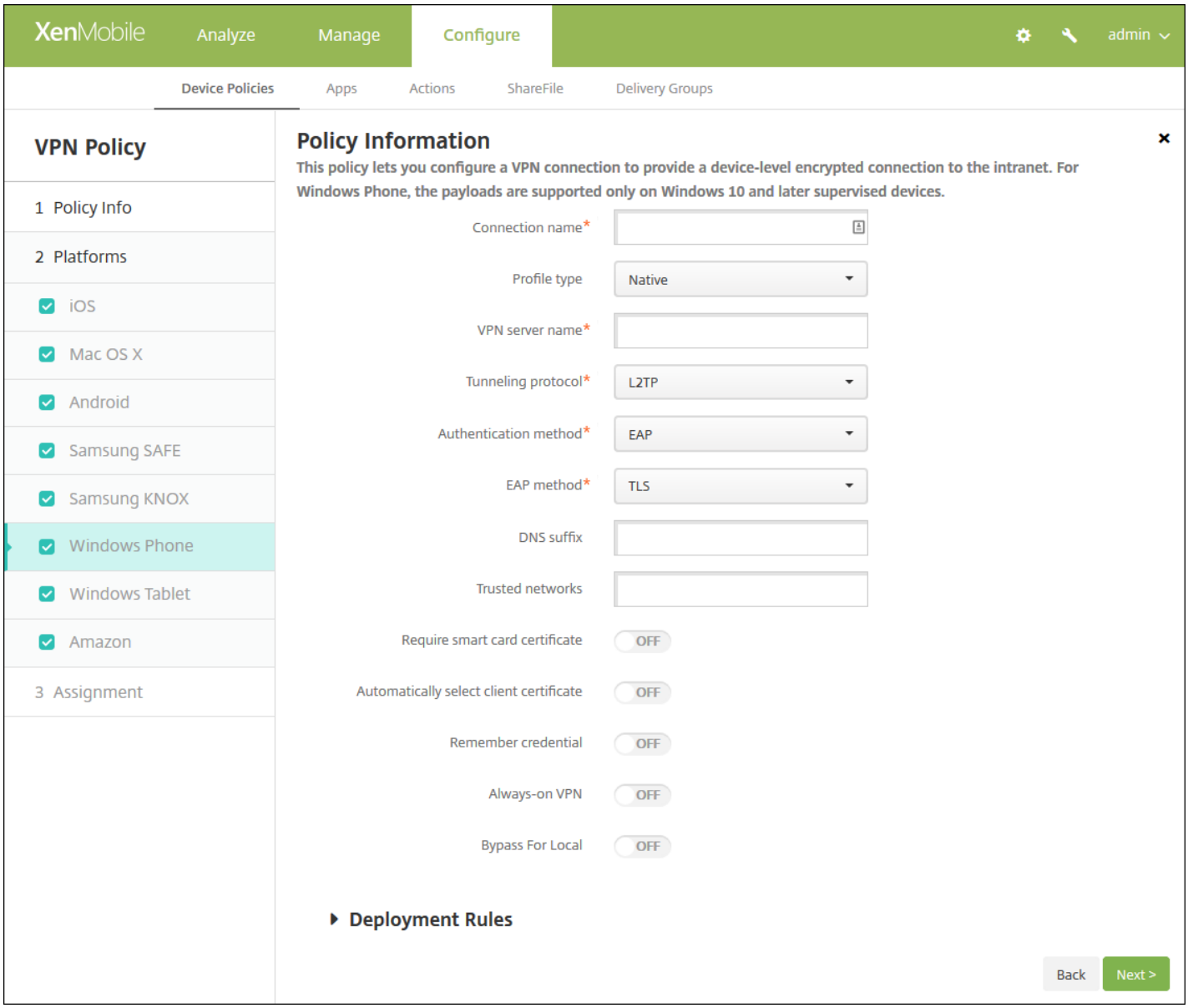
Konfigurieren der Samsung KNOX-Einstellungen



Konfigurieren des Enterprise-Protokolls

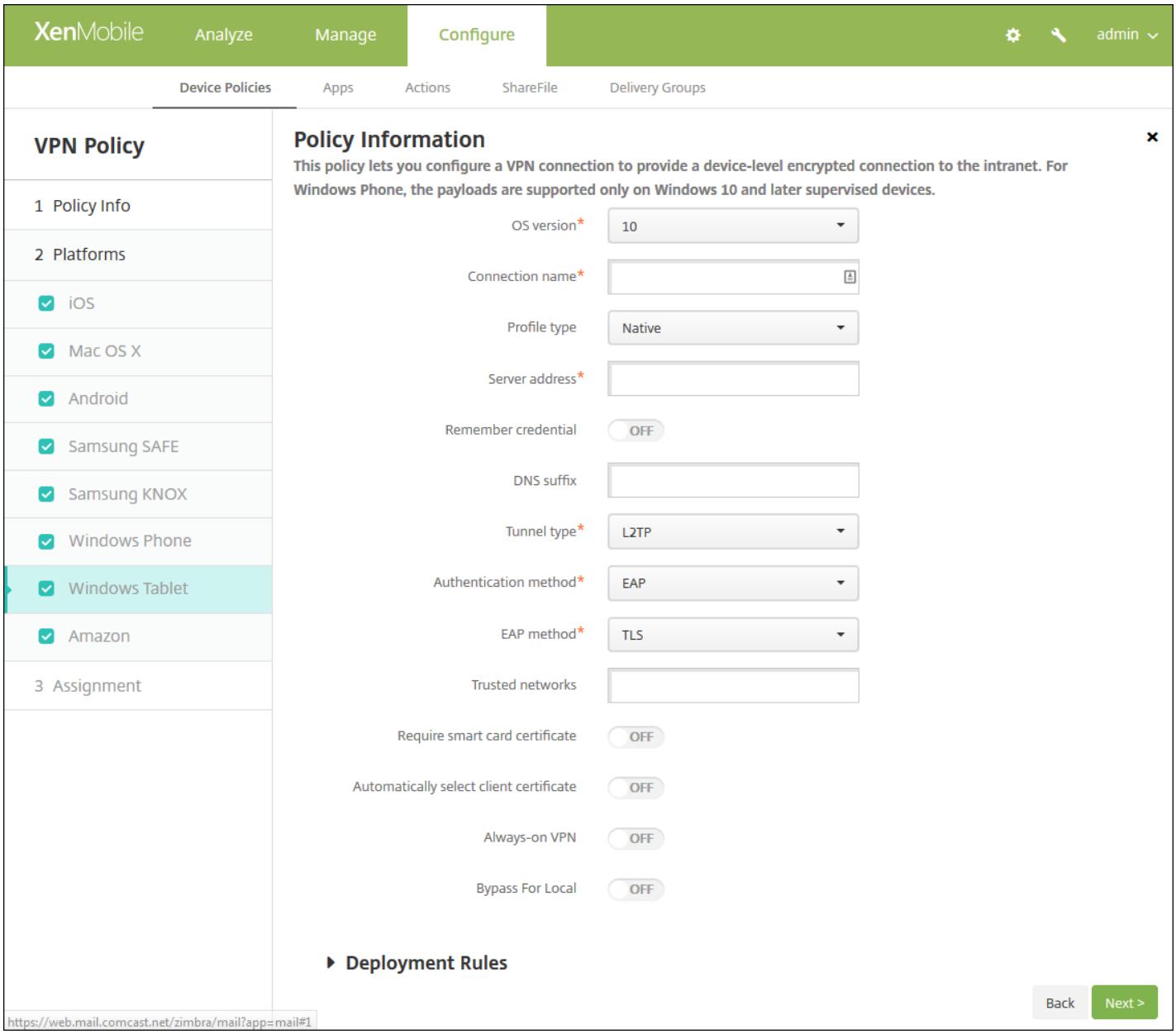
Konfigurieren des generischen Protokolls

Konfigurieren von Windows Phone-Einstellungen



-

Konfigurieren von Windows Tablet-Einstellungen

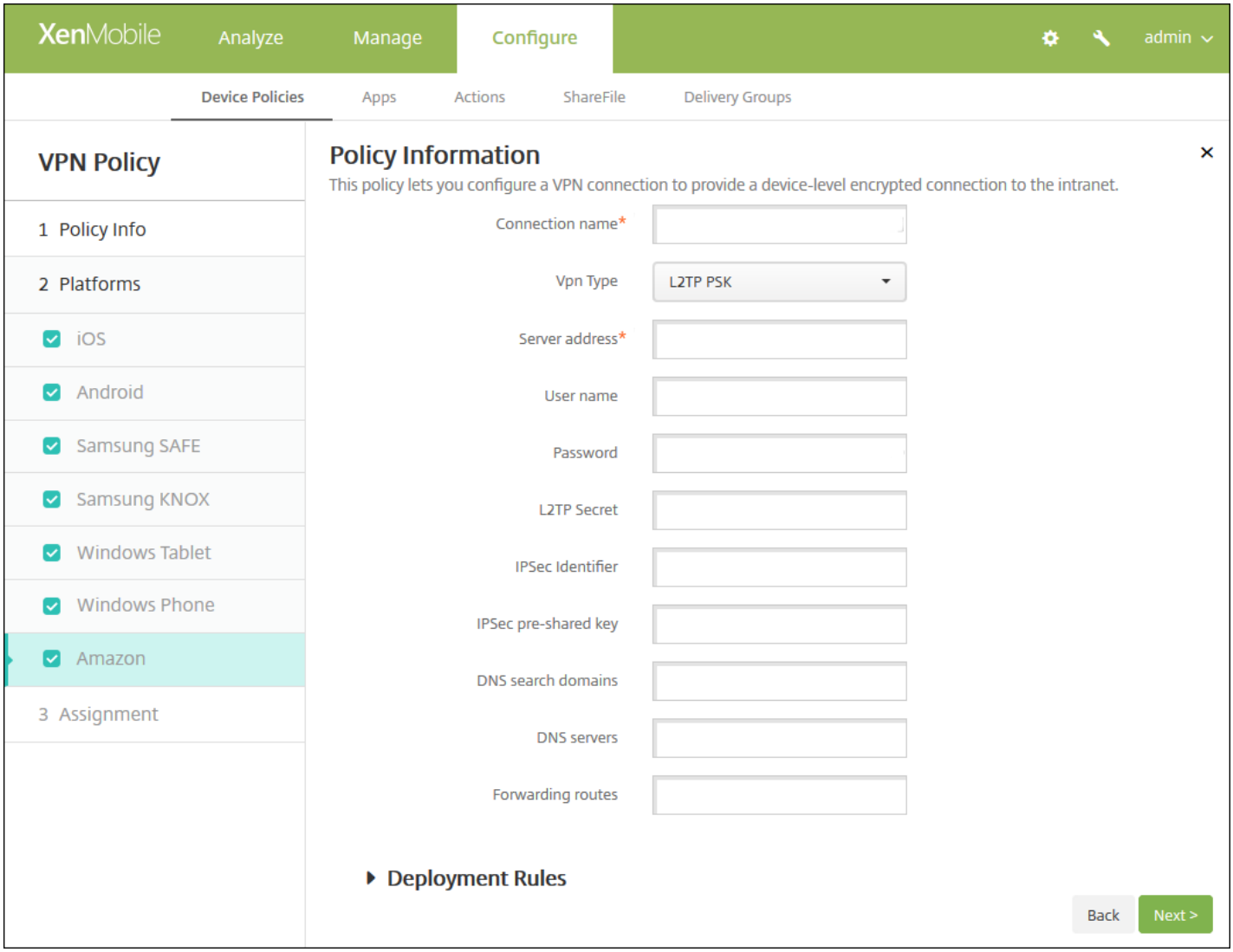


-

Konfigurieren von Windows 10-Einstellungen

Konfigurieren von Windows 8.1-Einstellungen

Konfigurieren von Amazon-Einstellungen



-
-
  -
    -
    -
    -
    -

Konfigurieren der L2TP PSK-Einstellungen

Konfigurieren der L2TP RSA-Einstellungen

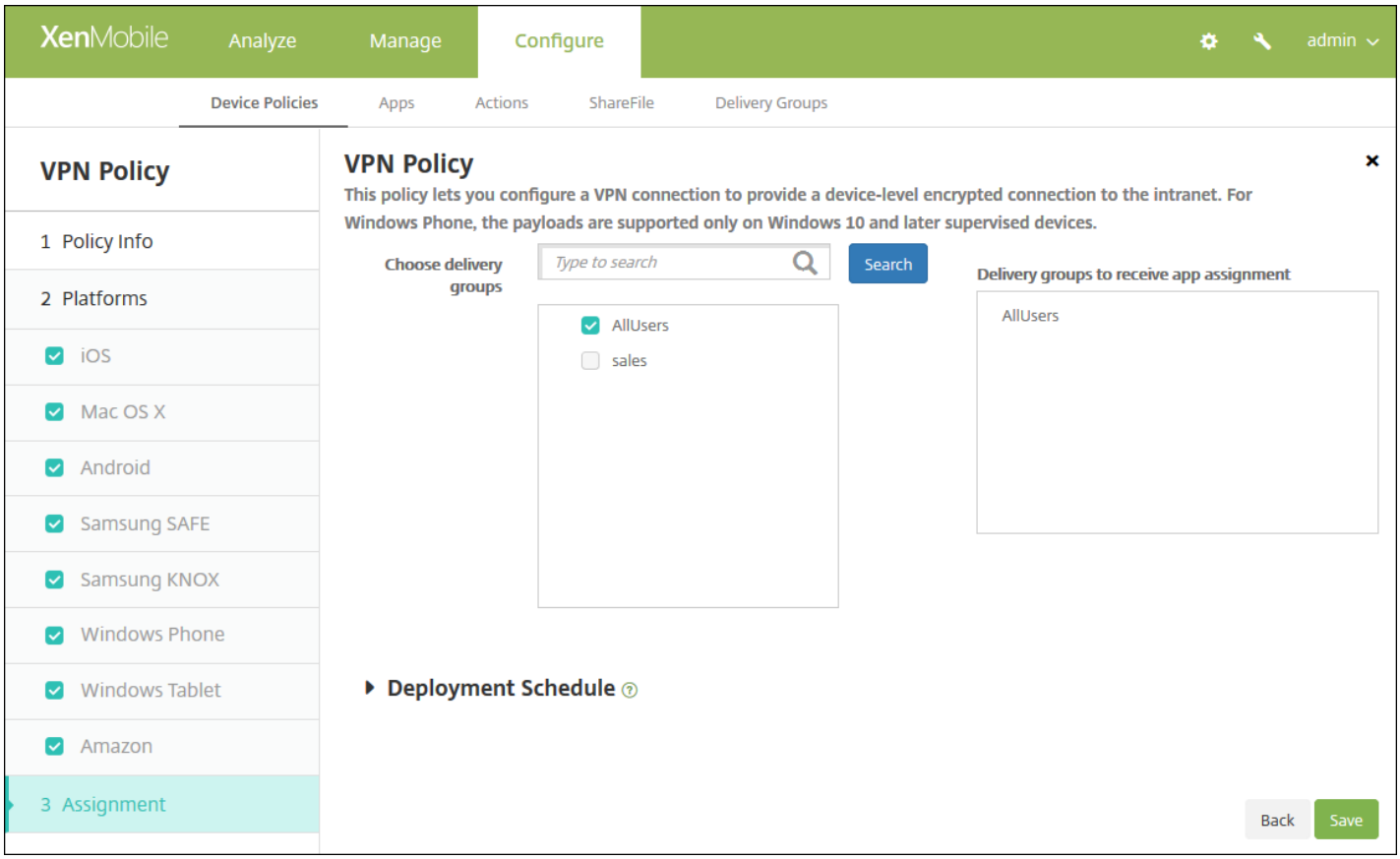
Konfigurieren der IPSEC XAUTH PSK-Einstellungen

Konfigurieren der IPSEC XAUTH RSA-Einstellungen

Konfigurieren der IPSEC HYBRID RSA-Einstellungen

Konfigurieren der PPTP-Einstellungen

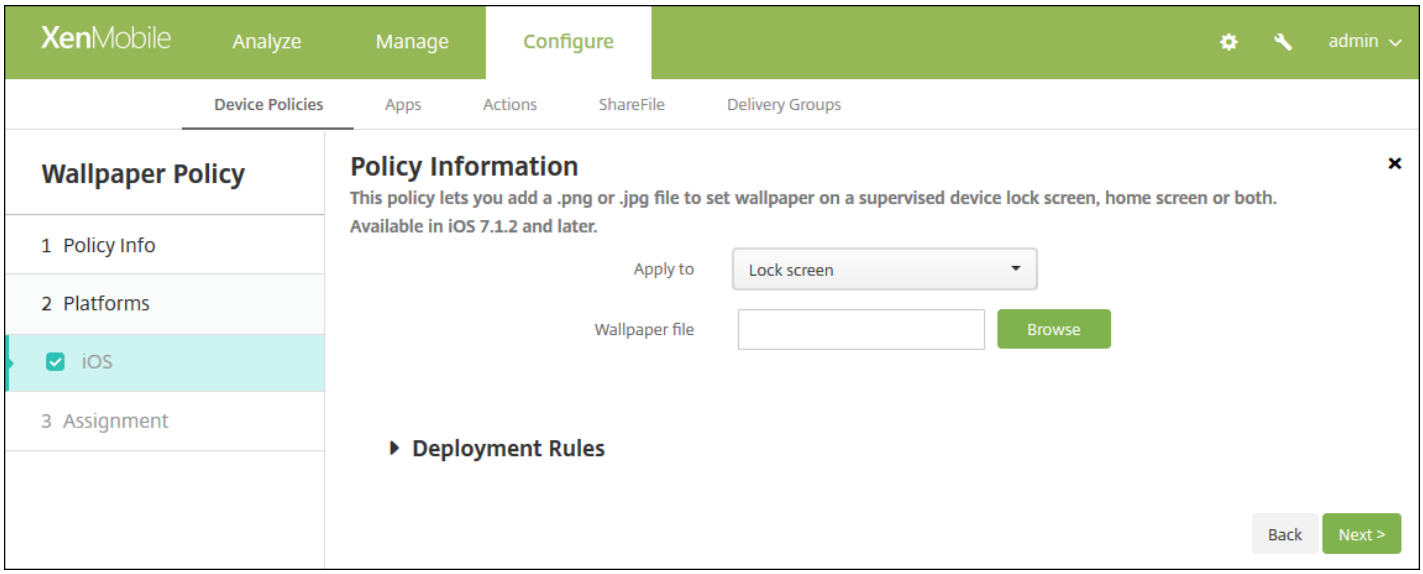
7. Konfigurieren der Bereitstellungsregeln



-
-
-

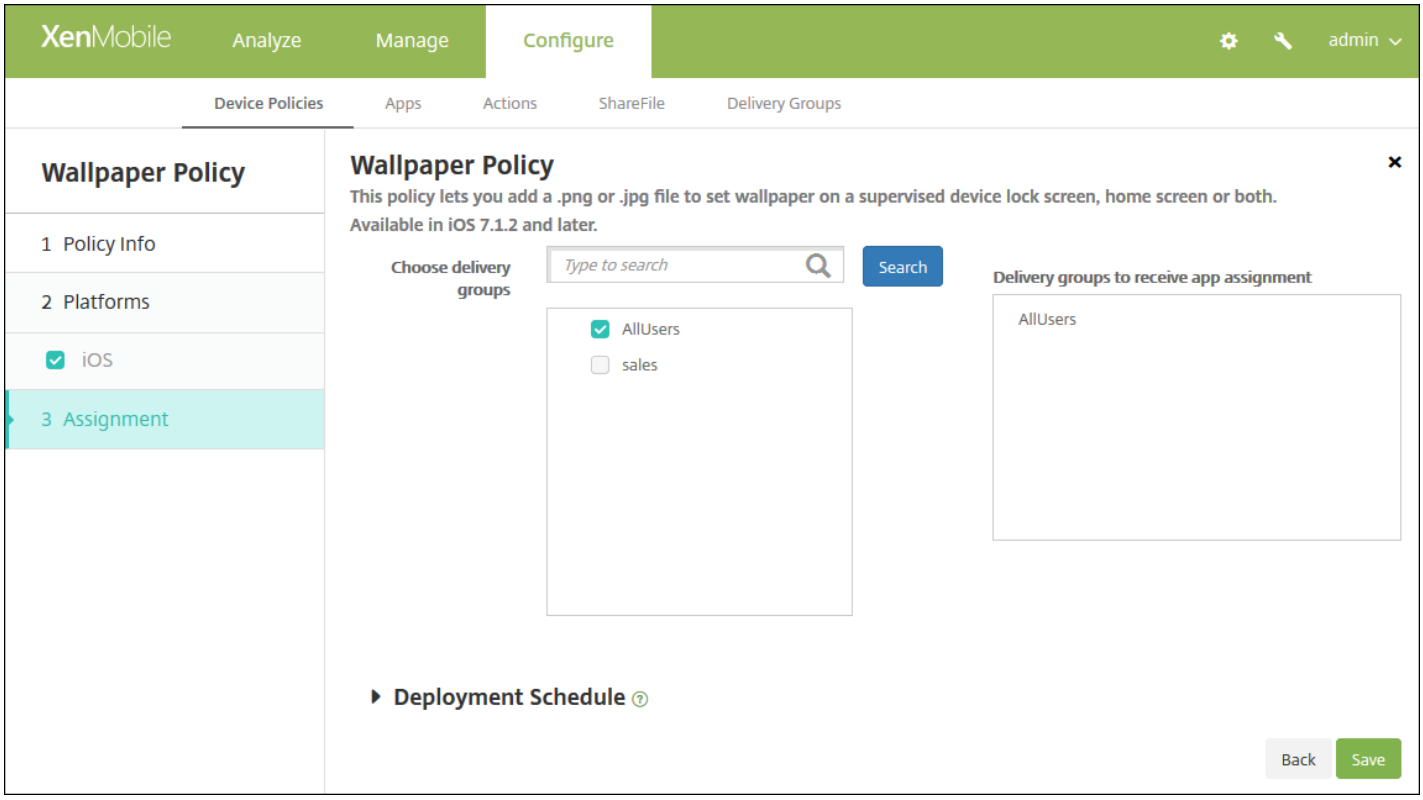
Hintergrundbild-Geräterichtlinie

-
-



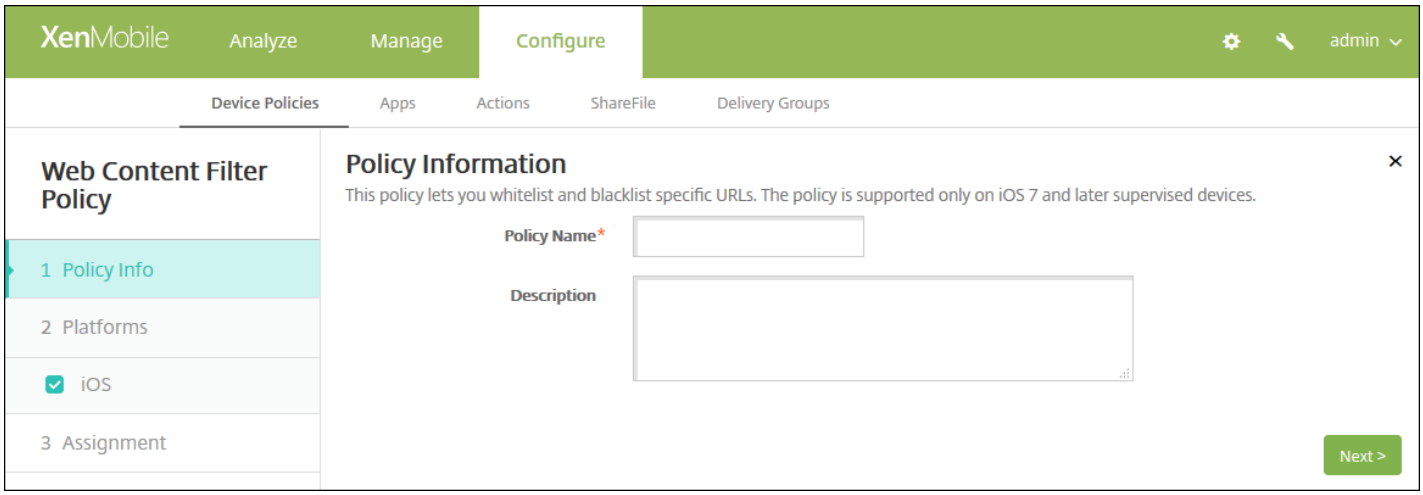
-
-

7. Konfigurieren der Bereitstellungsregeln

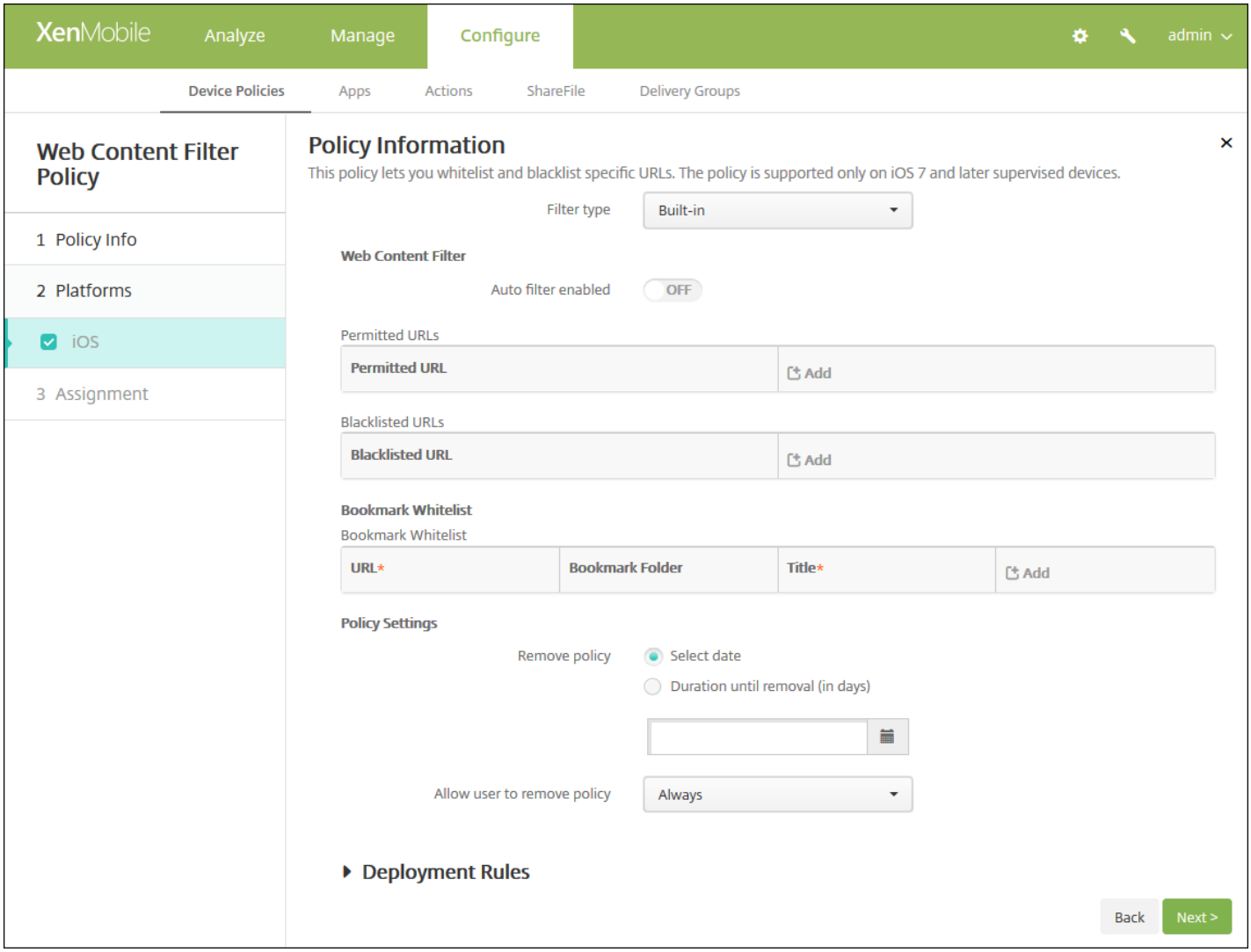


-
-
-
-
-
-
-

Geräterichtlinie für Webinhalt



-
-



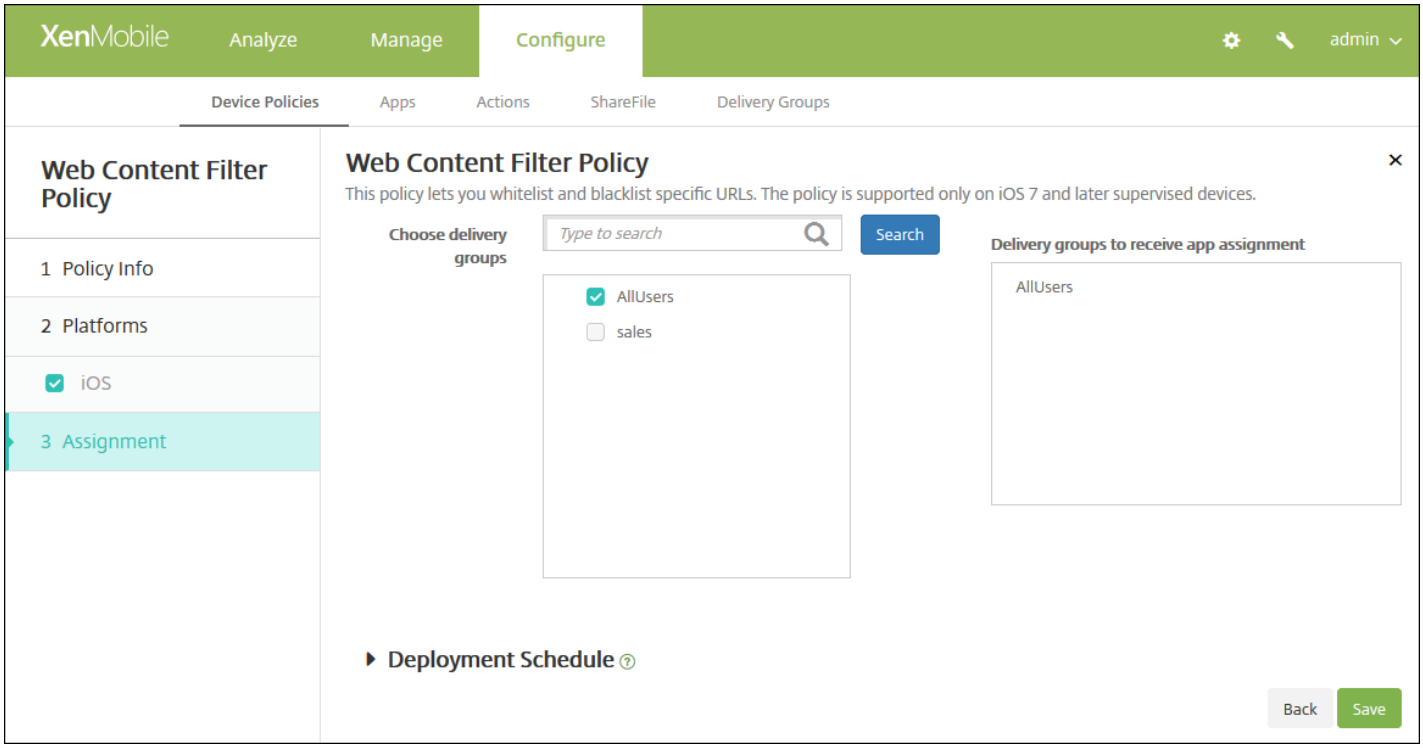
-

Einstellungen für integrierte Filter

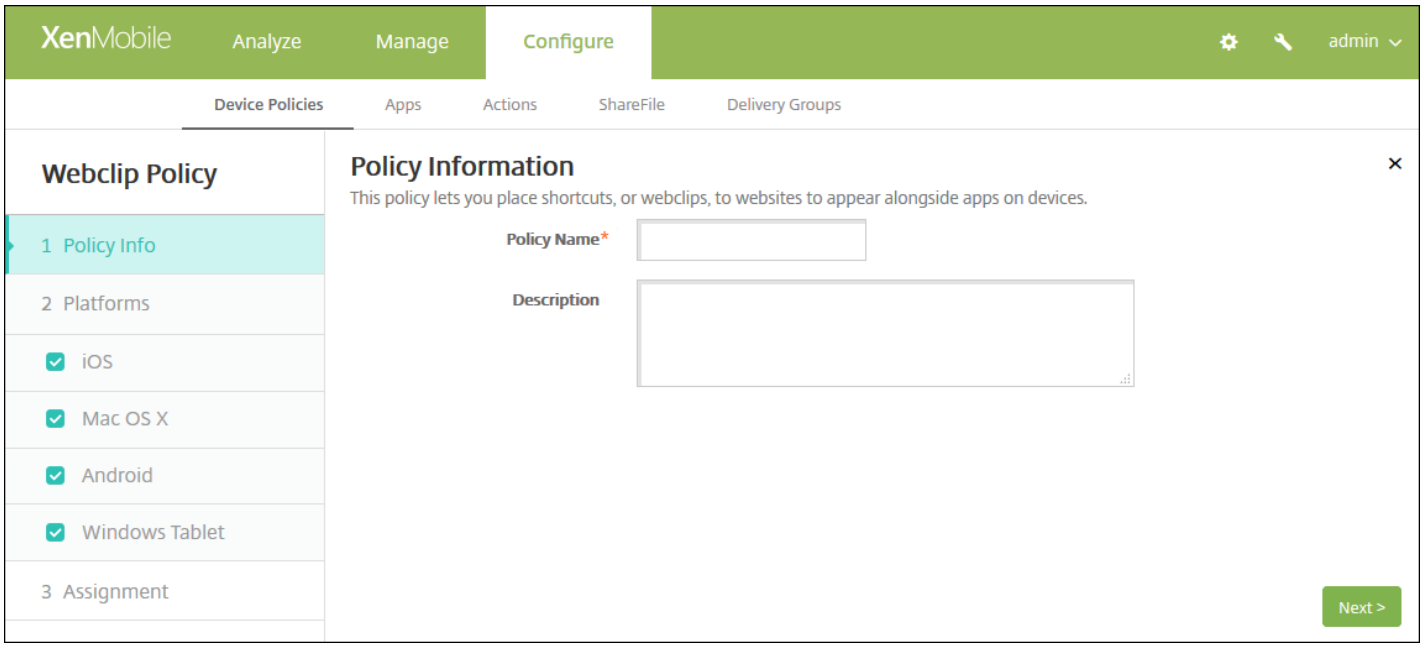
Einstellungen für Plug-In-Filter

-
  -
  -
  -
  -

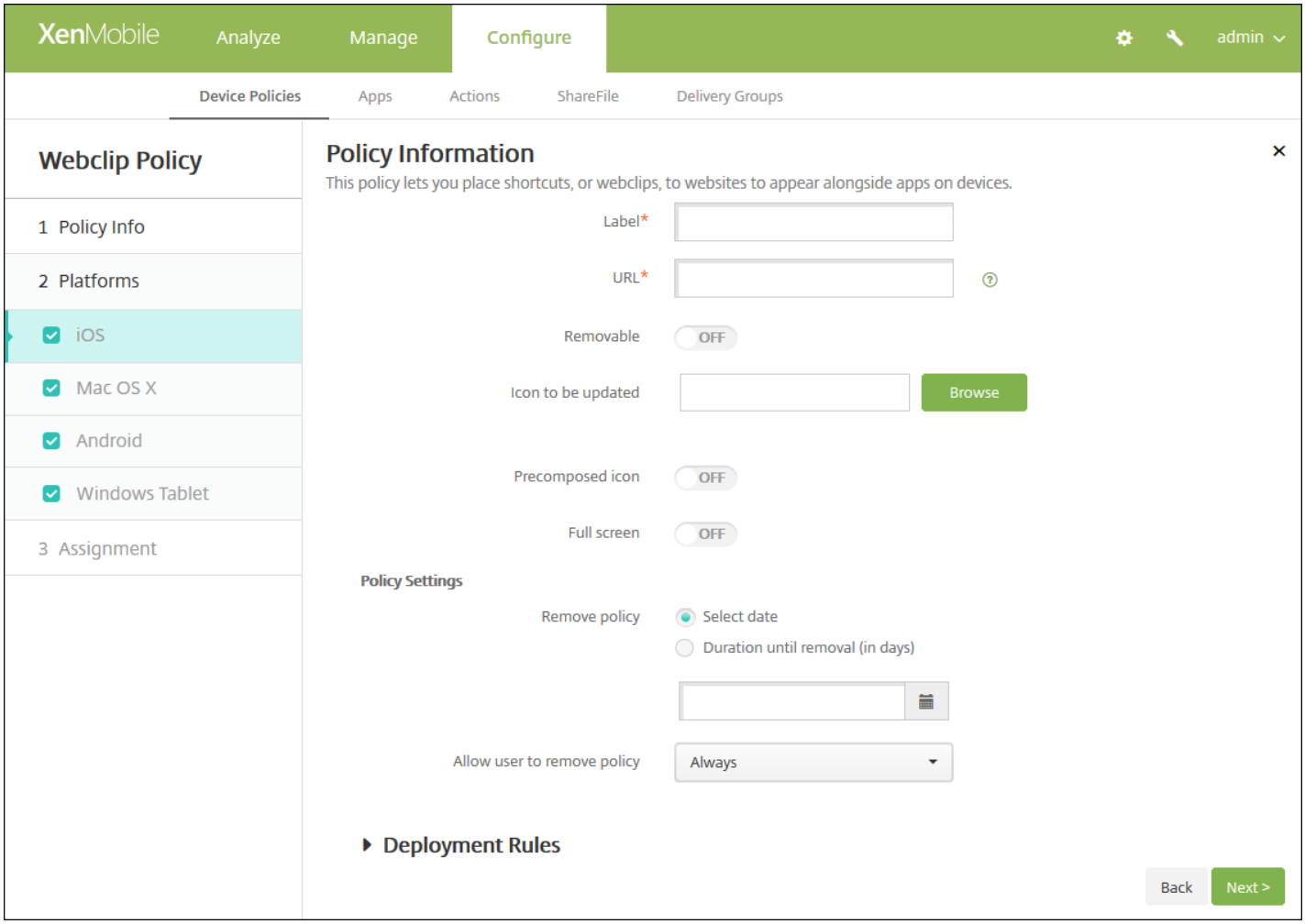
7. Konfigurieren der Bereitstellungsregeln



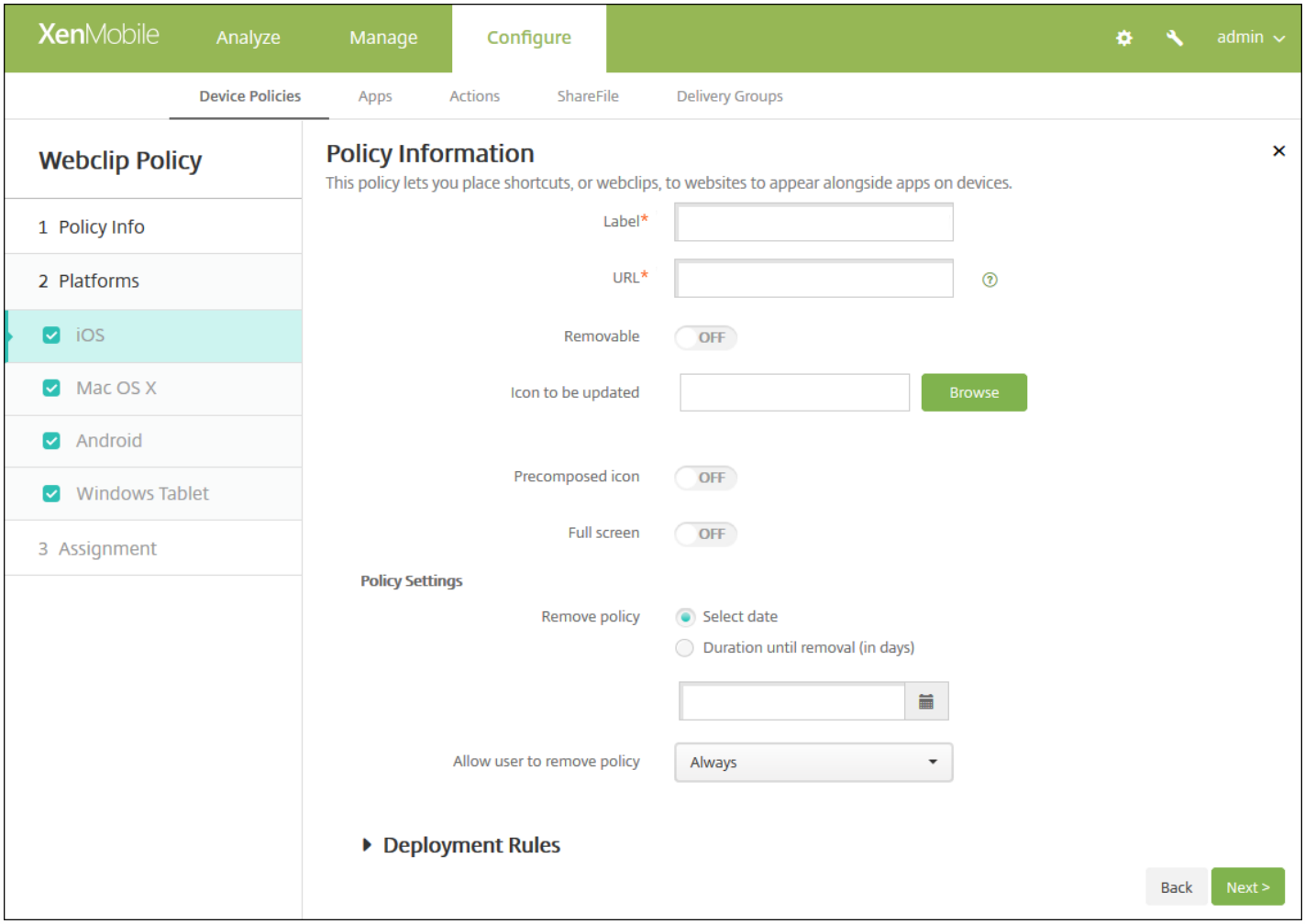
Webclip-Geräterichtlinien



-
-

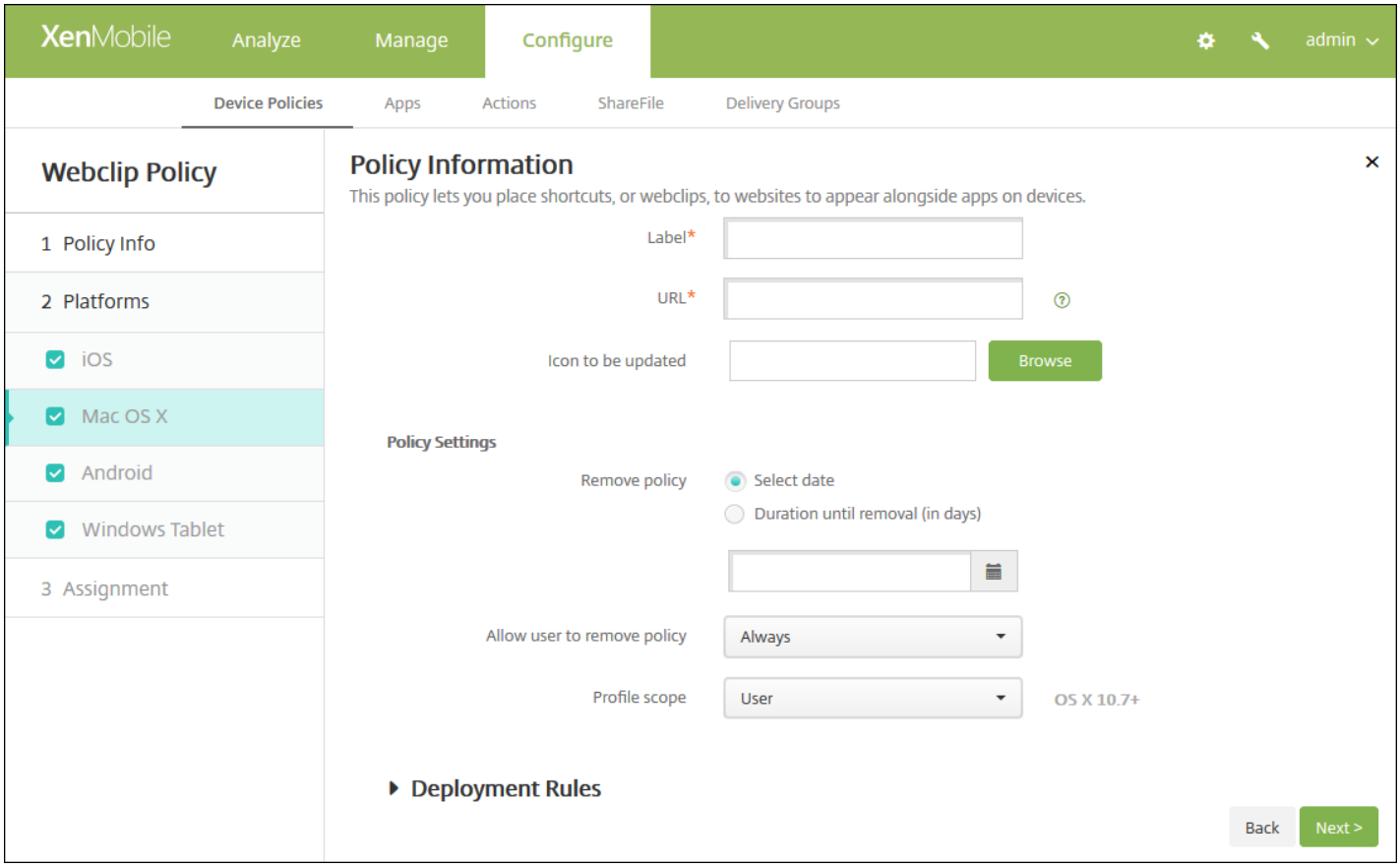


Konfigurieren von iOS-Einstellungen



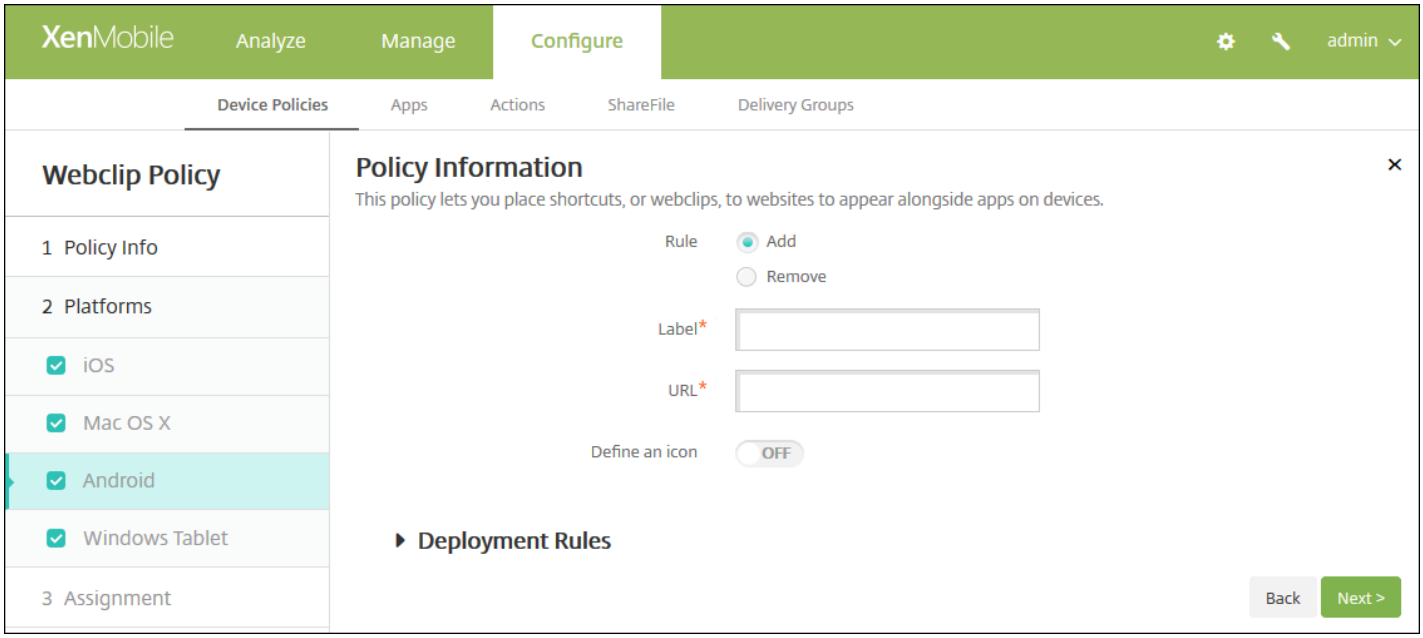
-
-
-
-
-
-
-
  -
  -
  -
  -

Konfigurieren von Mac OS X-Einstellungen



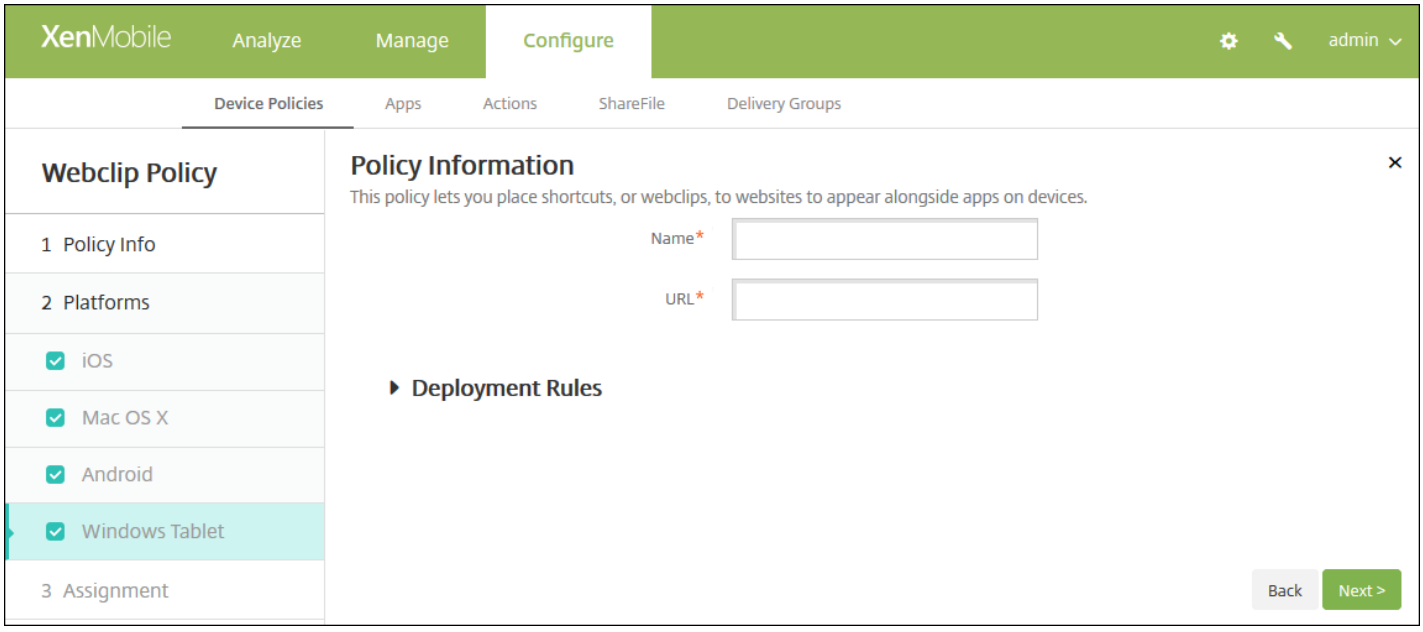
-
-
-
-
  -
  -
  -
  -
  -

Konfigurieren von Android-Einstellungen



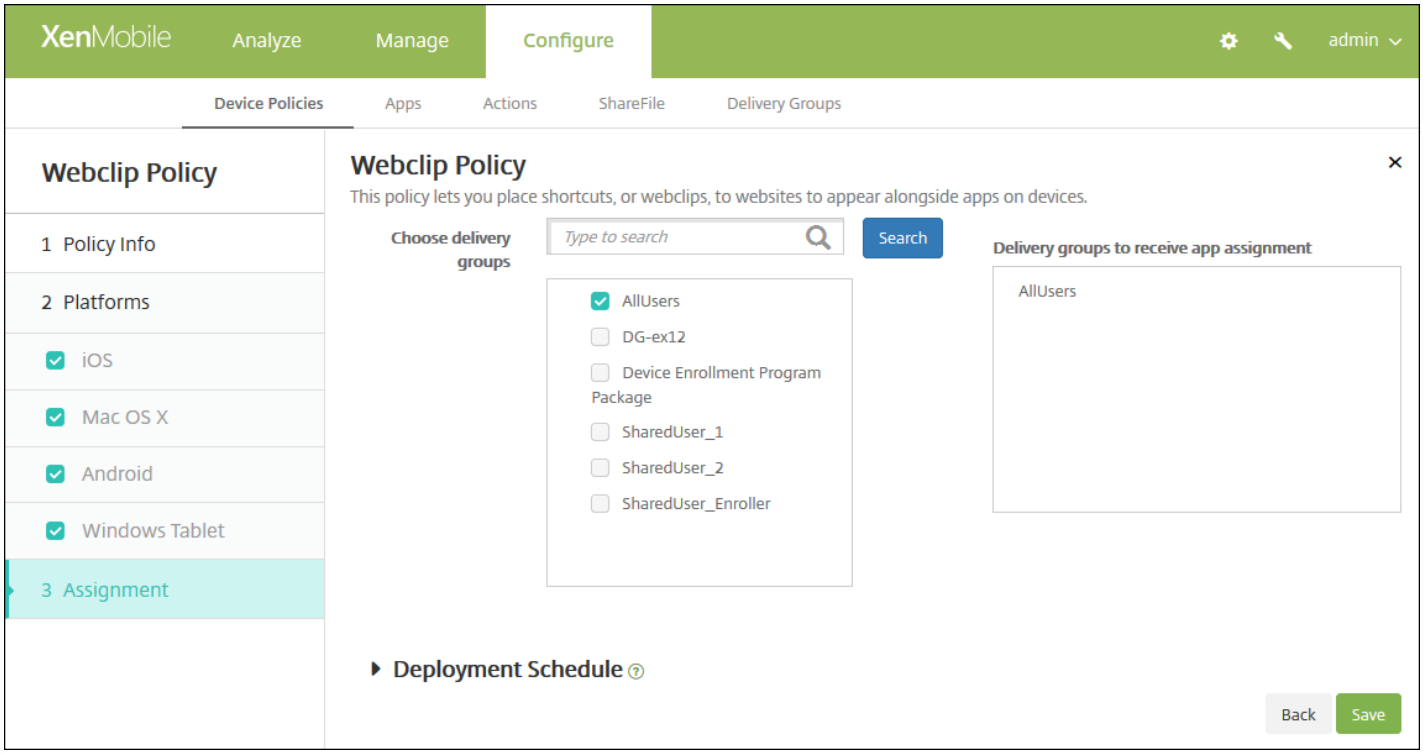
-
-
-
-
-

Konfigurieren von Windows Tablet-Einstellungen



-
-

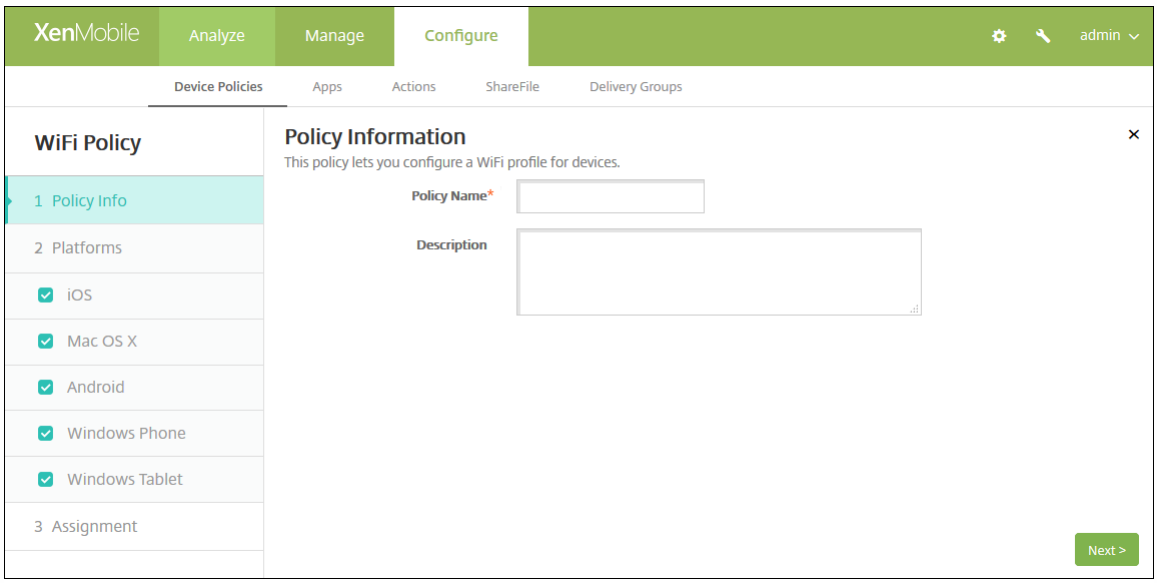
7. Konfigurieren der Bereitstellungsregeln



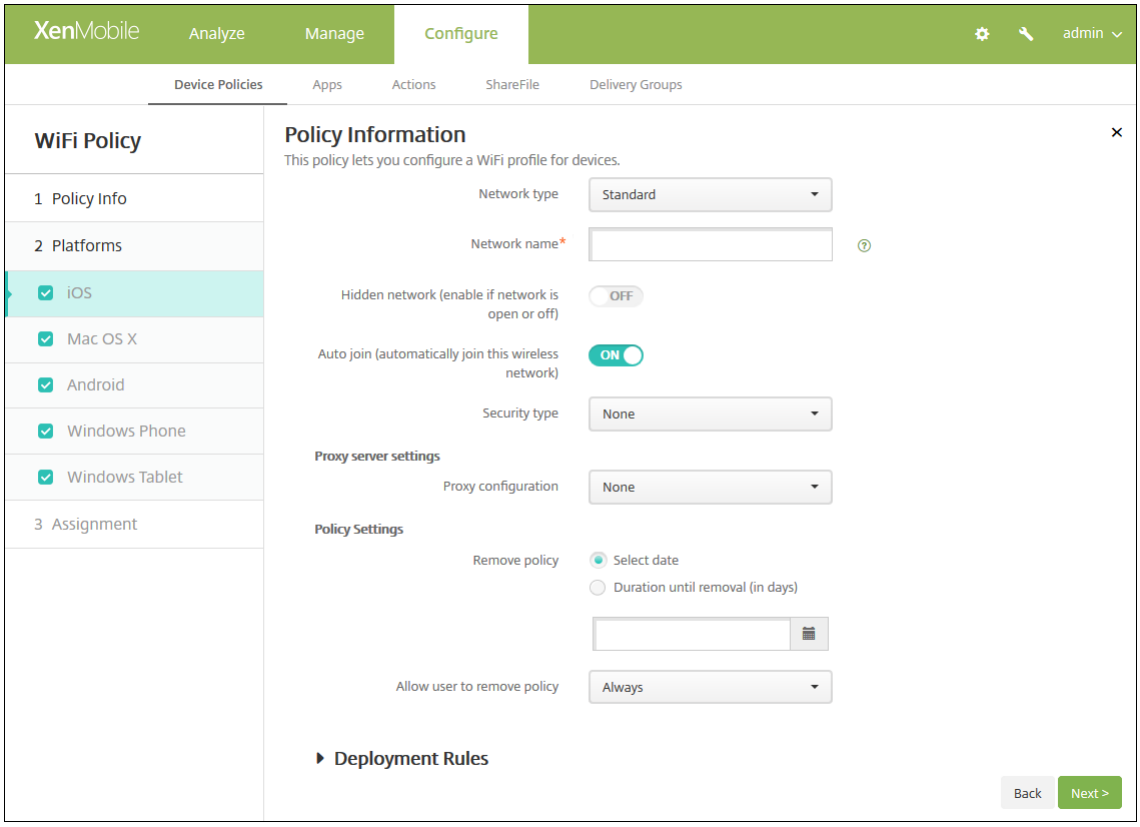
-
-
-
-
-
-
-

WiFi-Richtlinien für Geräte

Important



Konfigurieren von iOS-Einstellungen



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

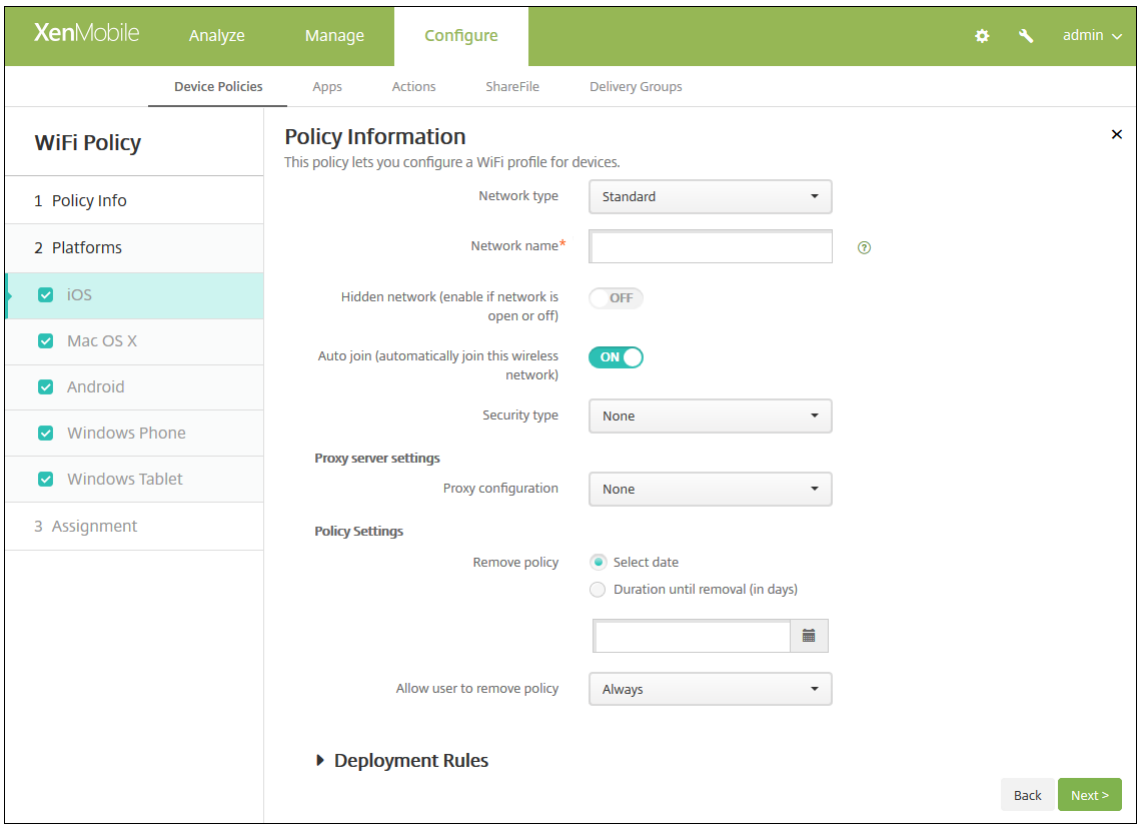
WPA, WPA Persönlich, Beliebig (Persönlich)

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Beliebig (Unternehmen)

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

-
  -
  -
  -
  -

Konfigurieren von Mac OS X-Einstellungen



-
-
-
-

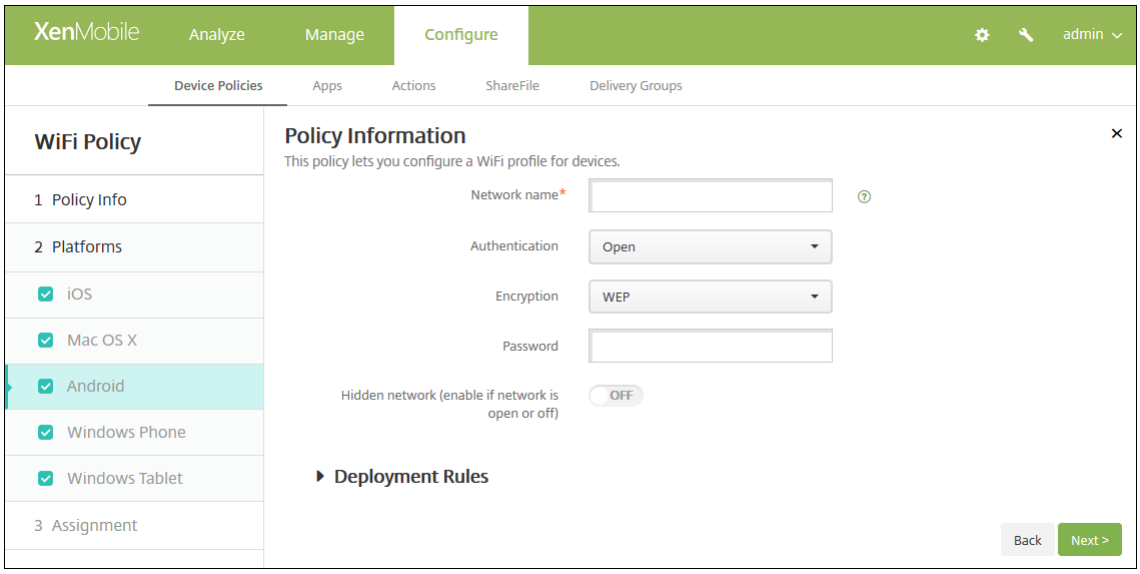
-
  -
  -
  -
  -
  -
  -
  -

WPA, WPA Persönlich, WPA 2 Persönlich, Beliebig (Persönlich)

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Beliebig (Unternehmen)

-
-
  -
  -
    -
    -
    -
    -

Konfigurieren von Android-Einstellungen

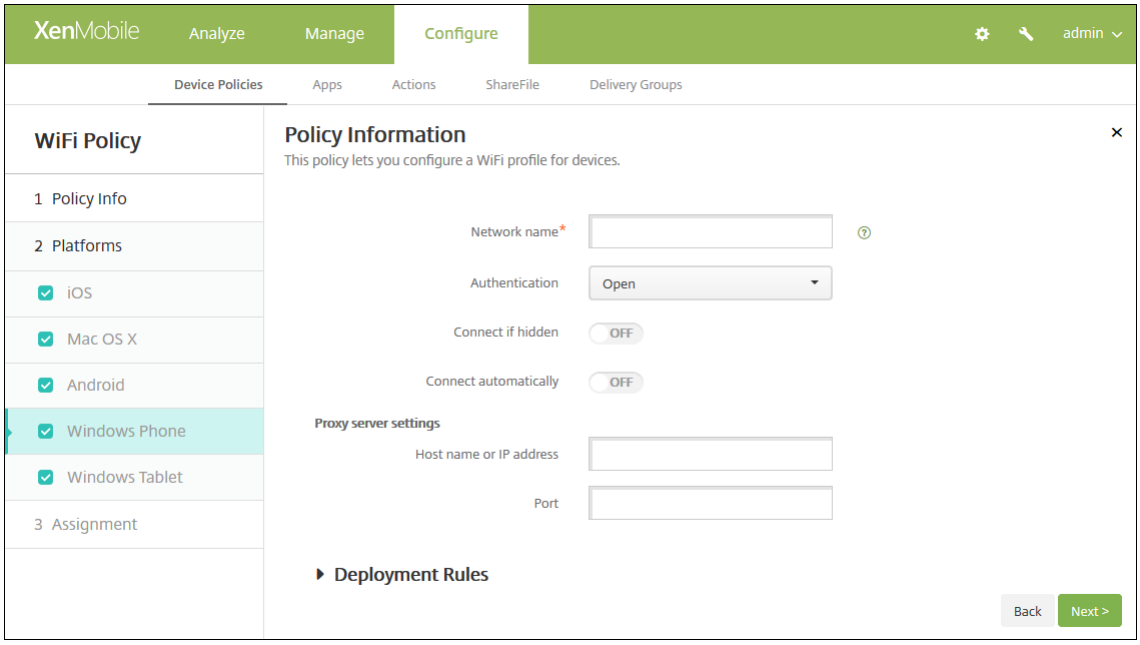


Offen, freigegeben

WPA, WPA-PSK, WPA2, WPA2-PSK

802.1x

Konfigurieren von Windows Phone-Einstellungen



-
-
  -
  -
  -
  -
  -

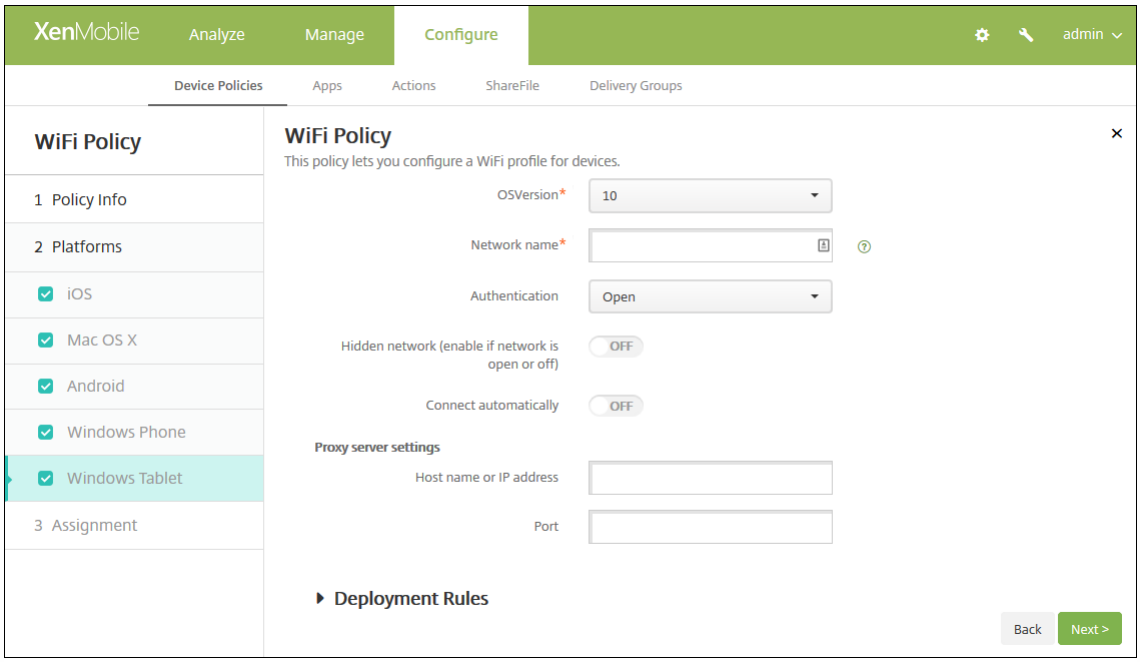
Offen

WPA (Persönlich), WPA-2 (Persönlich)

WPA-2 (Unternehmen)

-
  -
  -

Konfigurieren von Windows Tablet-Einstellungen



-

Windows 10-Einstellungen

-
  -
  -
  -
  -
  -

Offen

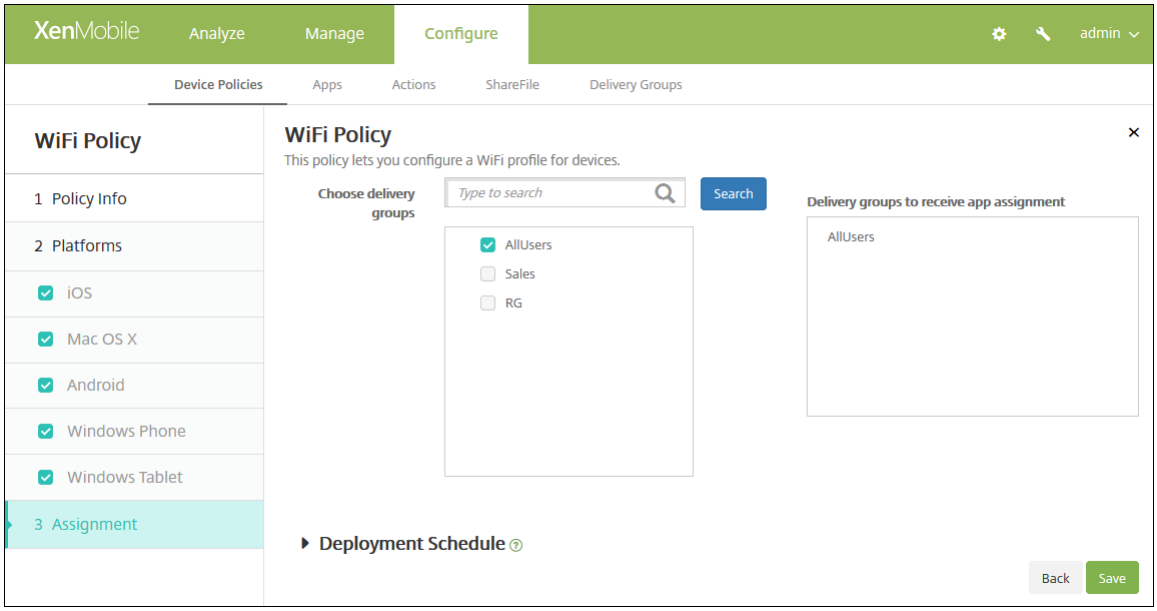
WPA (Persönlich), WPA-2 (Persönlich)

WPA-2 (Unternehmen)

Windows 8.1-Einstellungen

-
-
  -
  -
  -
  -
  -
-
-

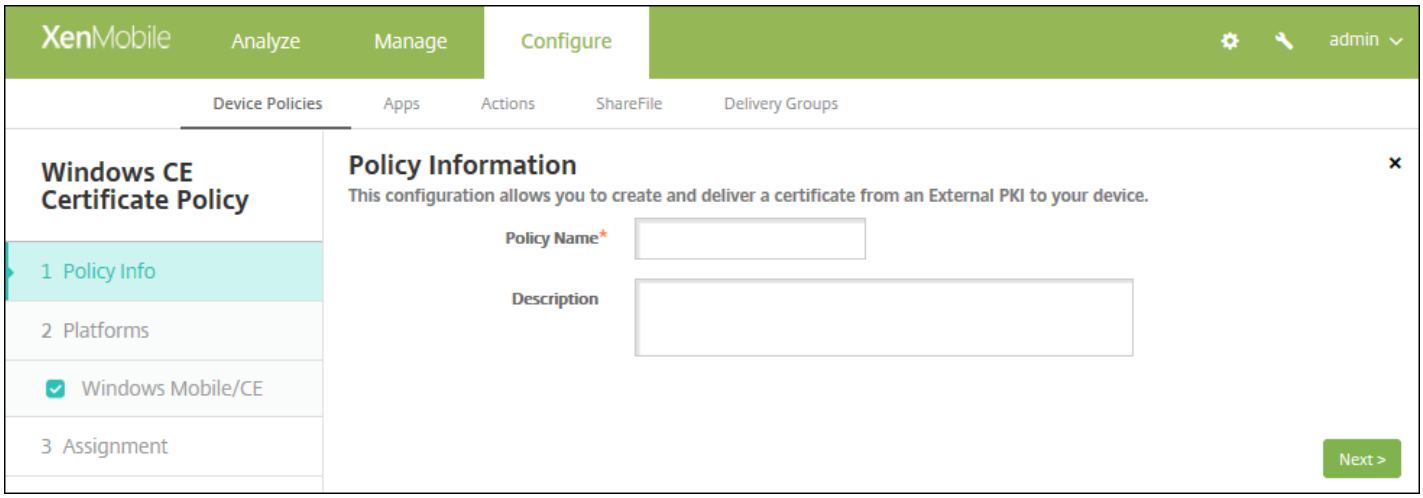
7. Konfigurieren der Bereitstellungsregeln



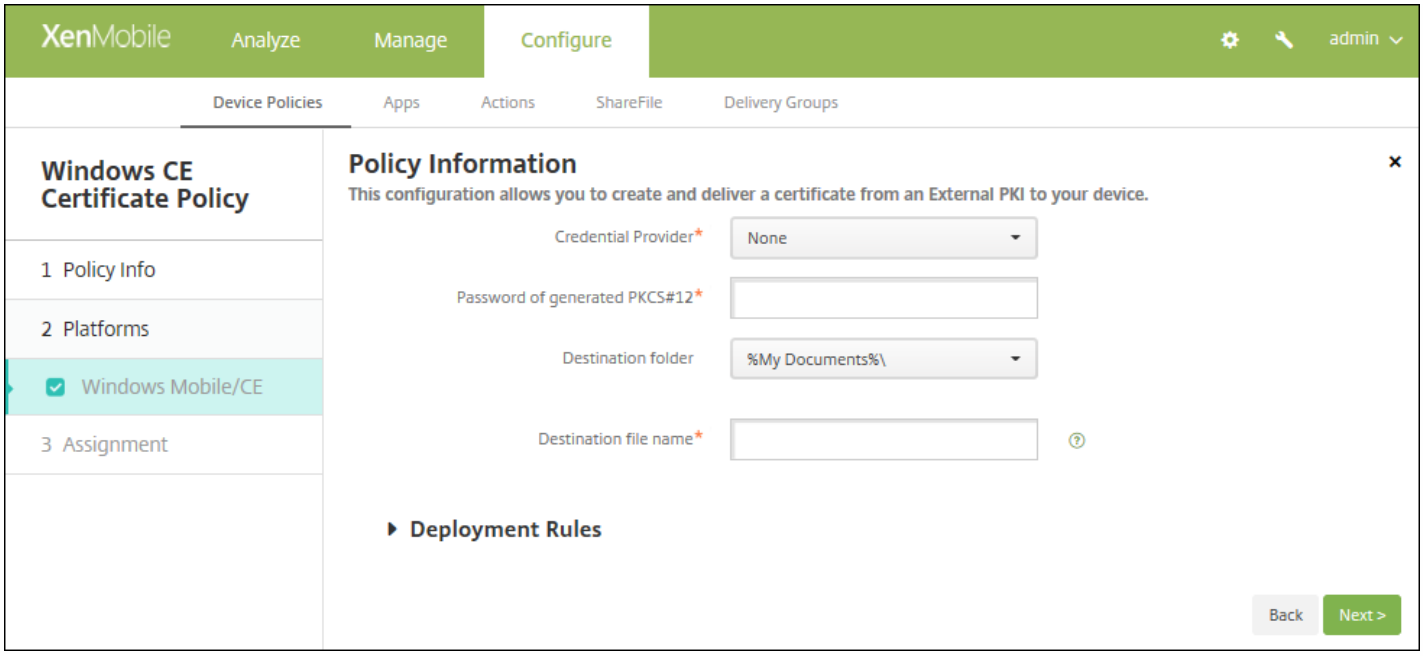
-
-
-
-
-

-
-

Windows CE-Geräterichtlinie für Zertifikate

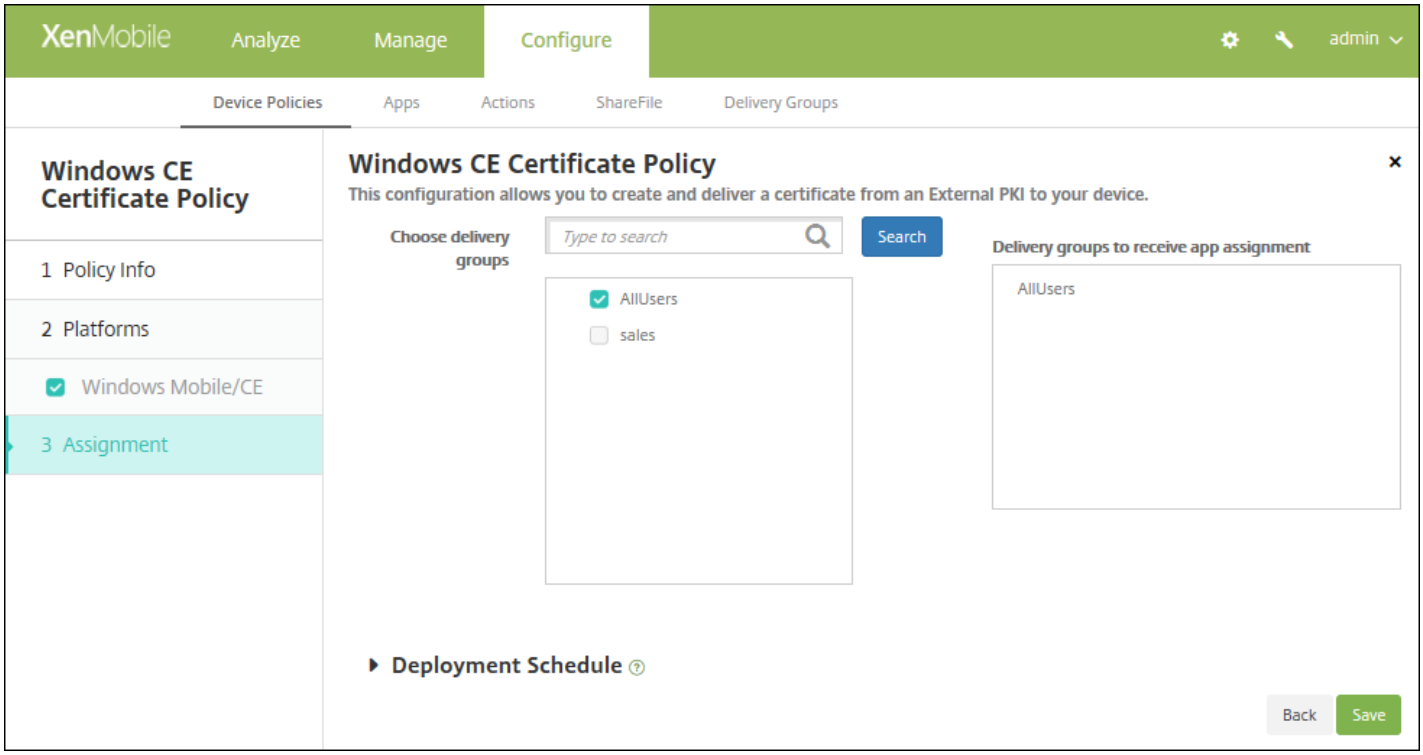


-
-



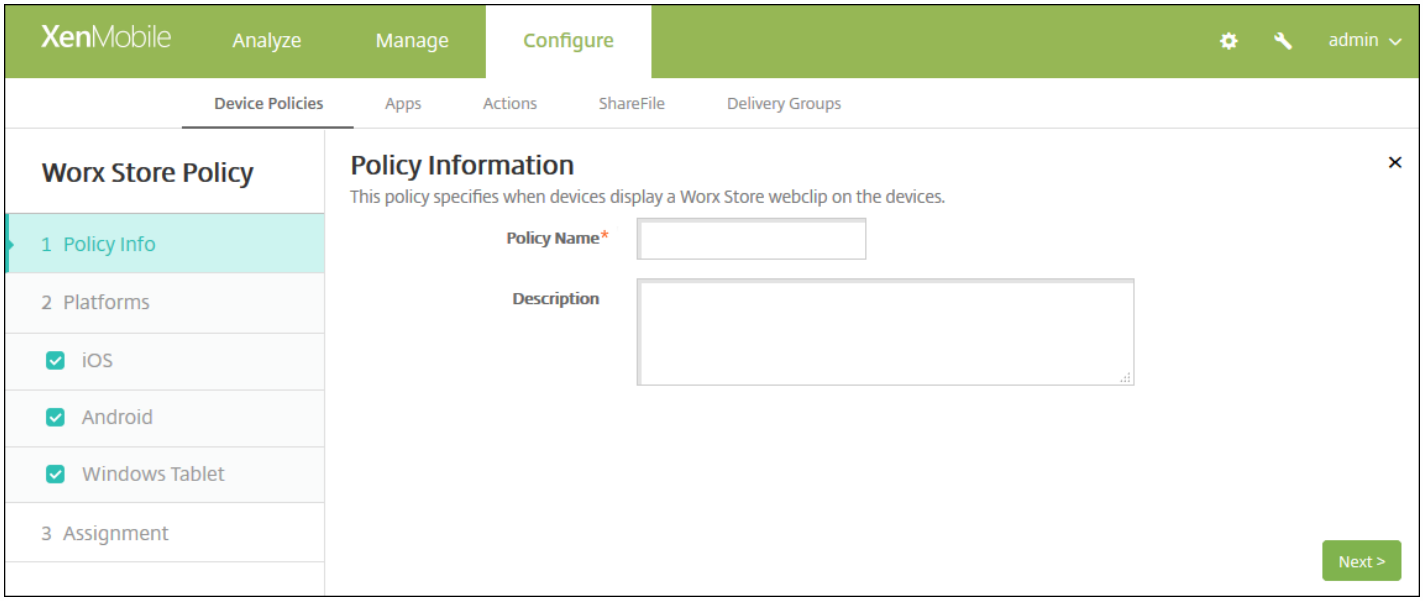
-
-
-
  -
  -
  -
  -
  -
-

7. Konfigurieren der Bereitstellungsregeln

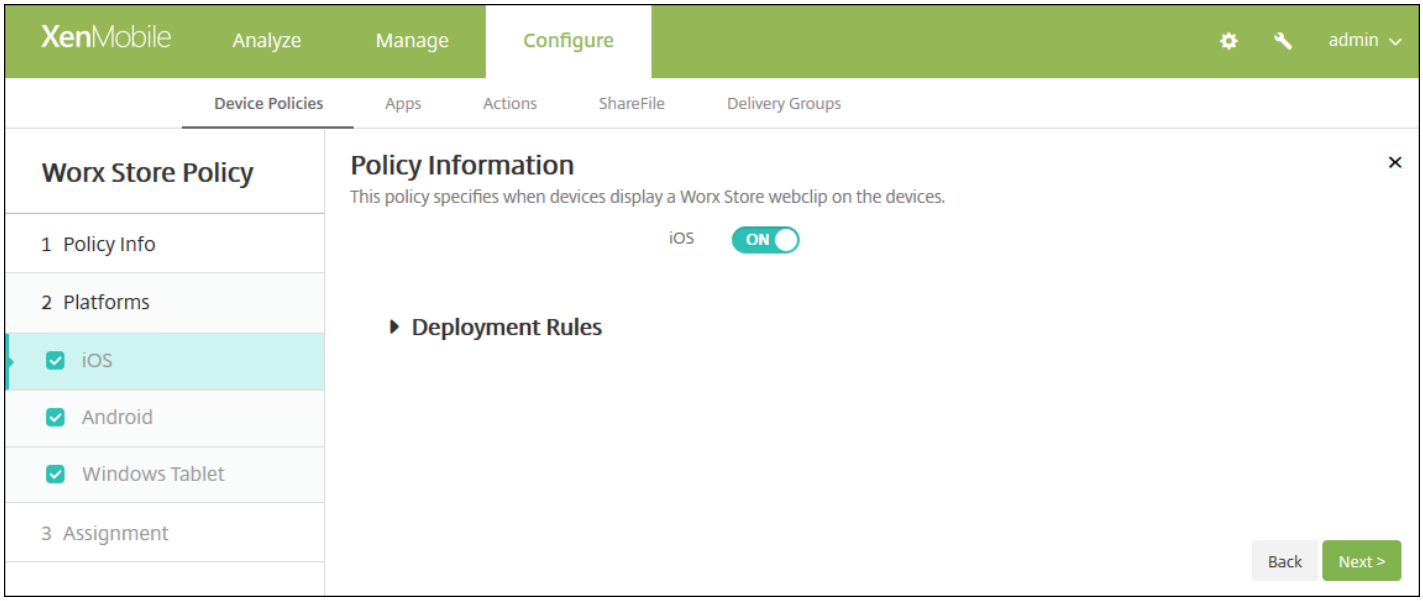


-
-
-
-
-
-
-

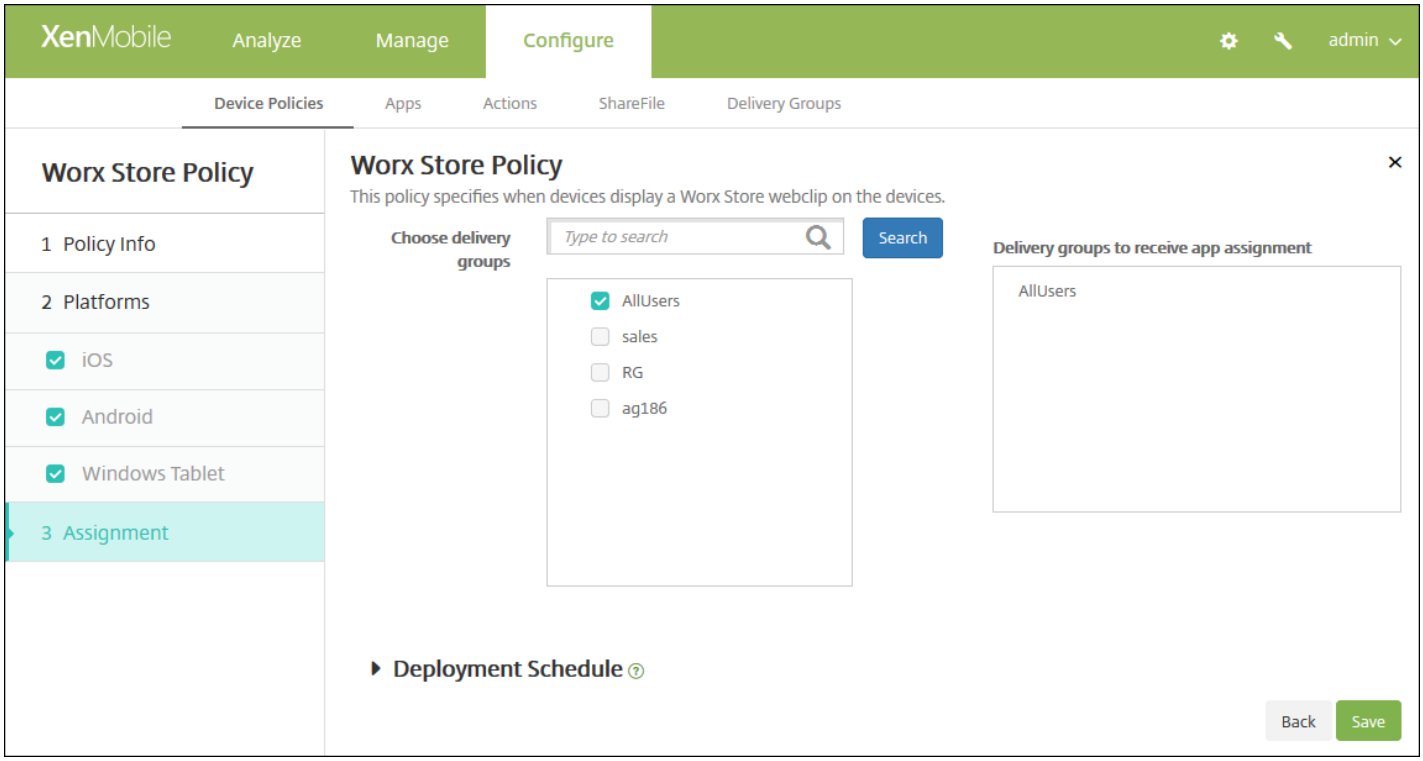
Worx Store-Geräterichtlinie



-
-

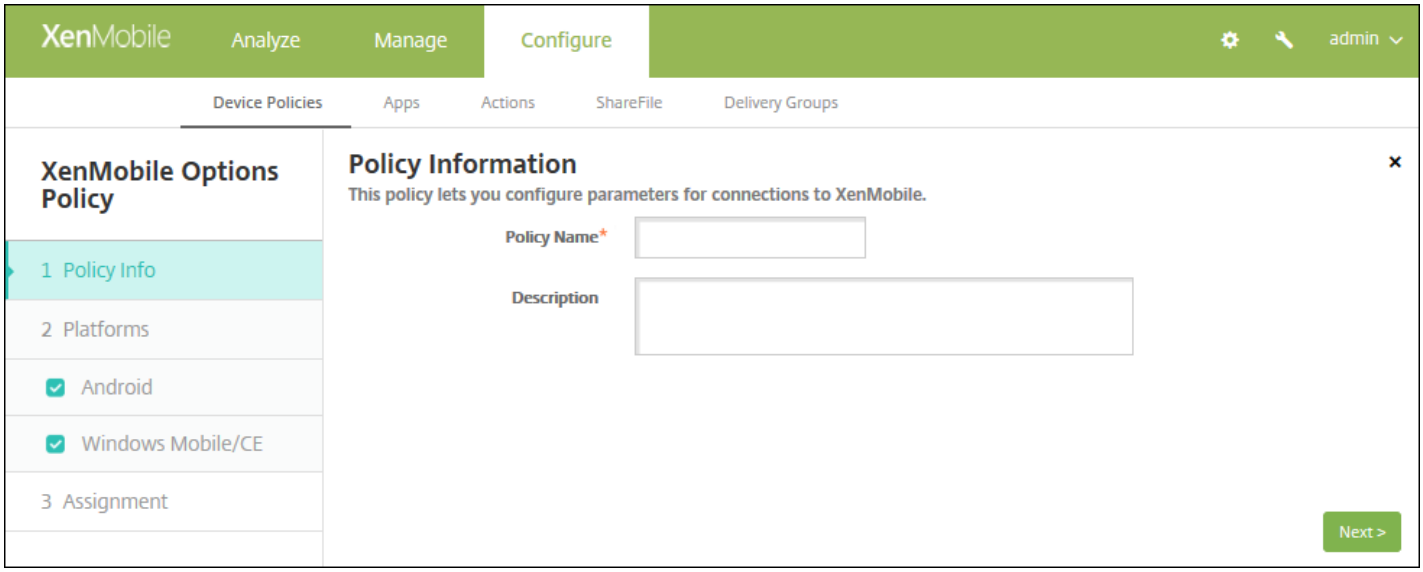


8. Konfigurieren der Bereitstellungsregeln



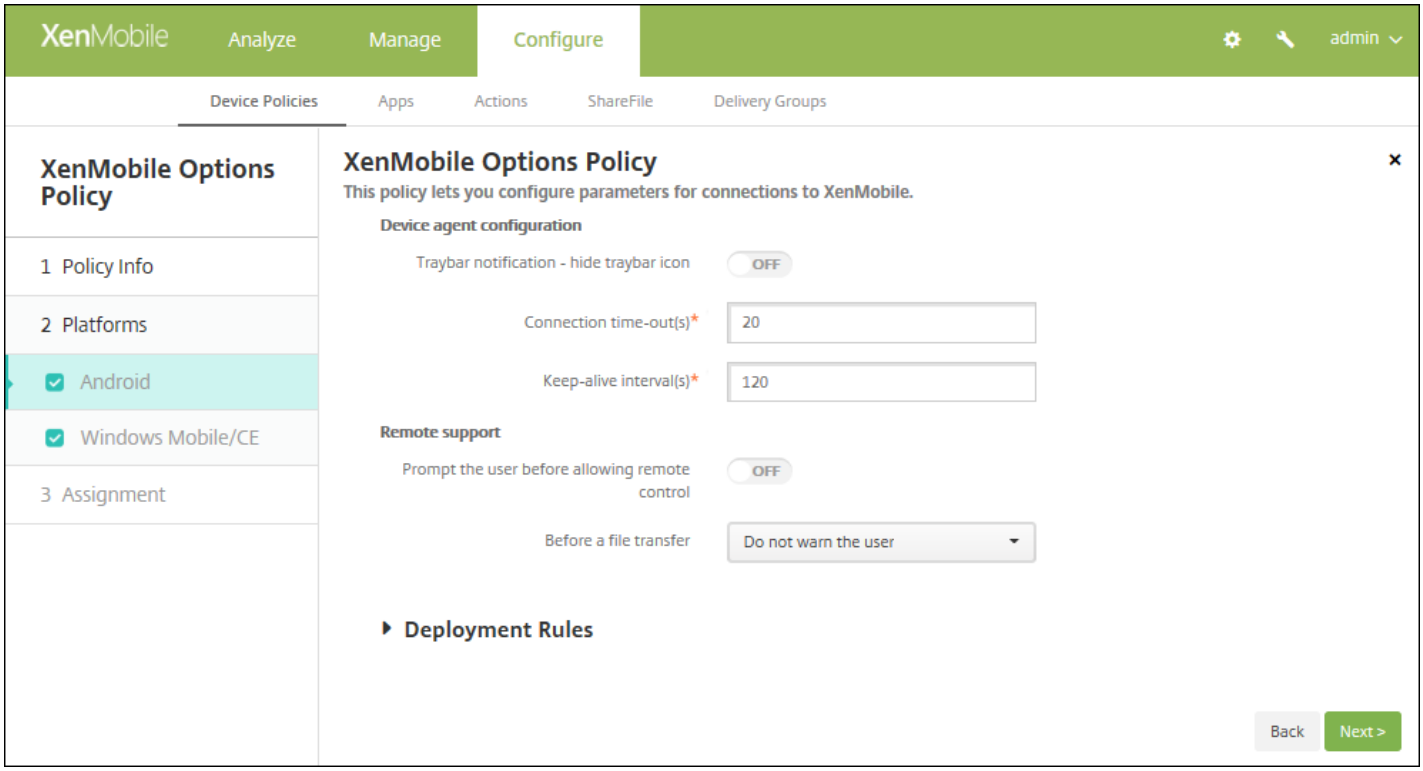
-
-
-
-
-
-
-

XenMobile-Optionsrichtlinien für Geräte



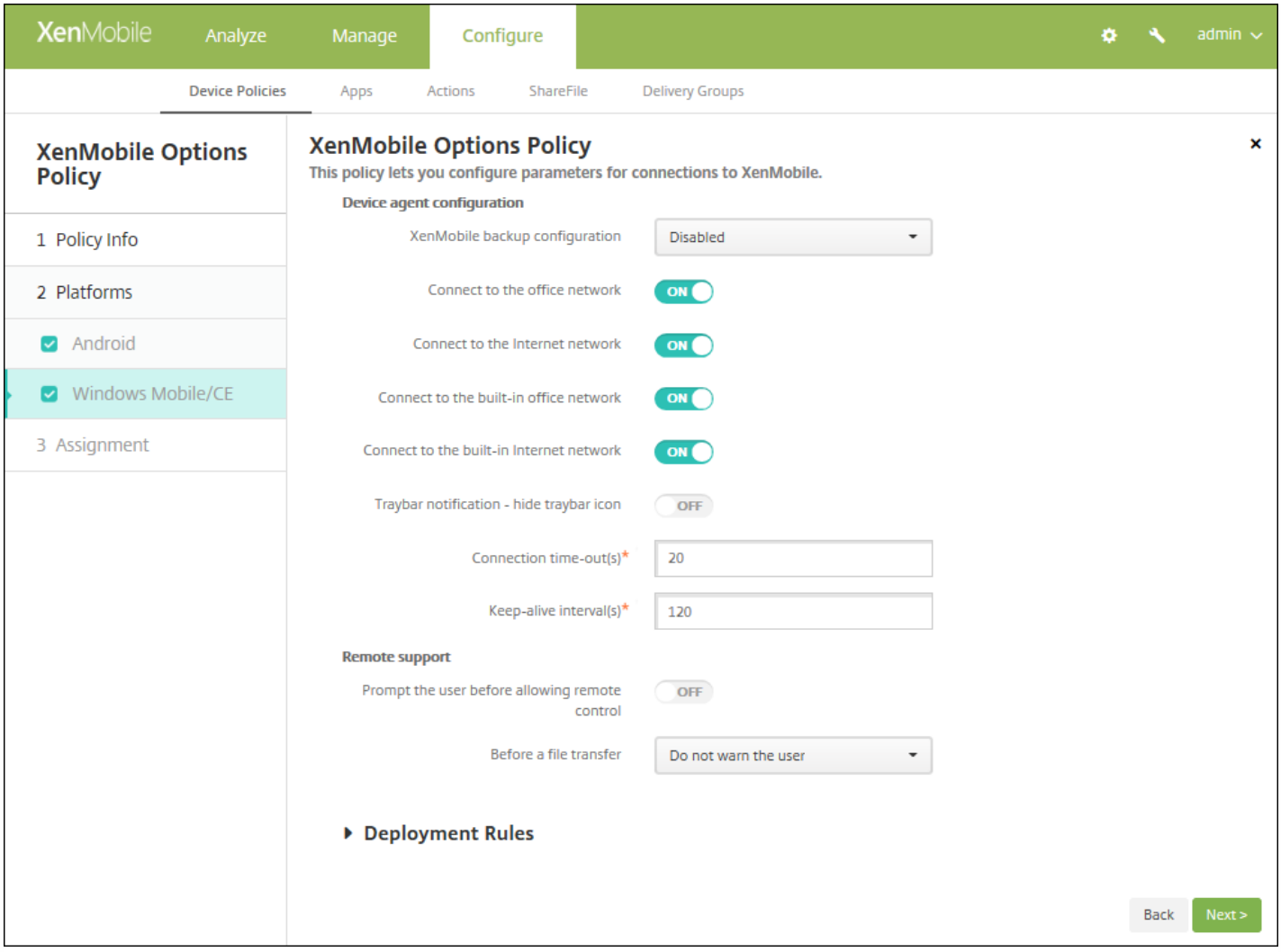
-
-

Konfigurieren von Android-Einstellungen



-
-
-
-
-

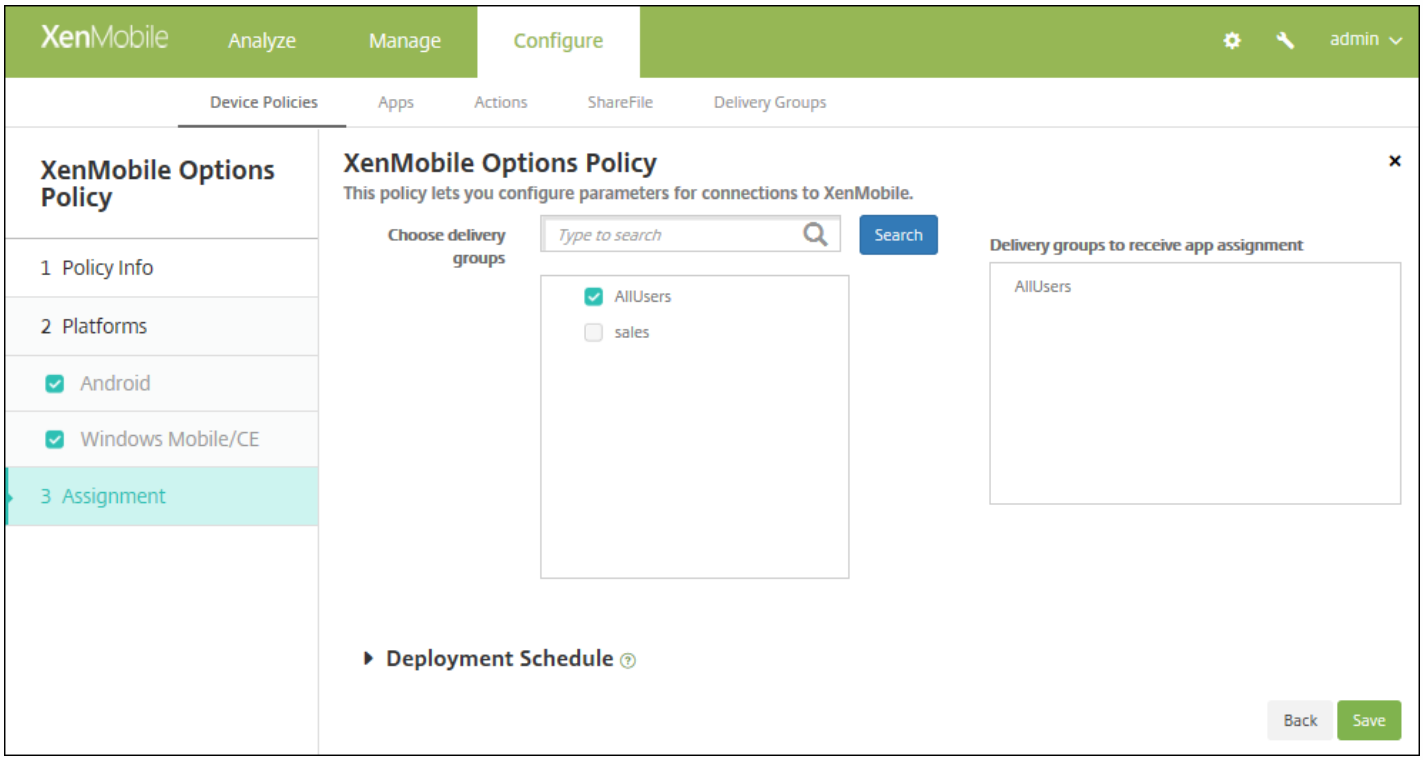
Konfigurieren von Windows Mobile-/CE-Einstellungen



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

-
-

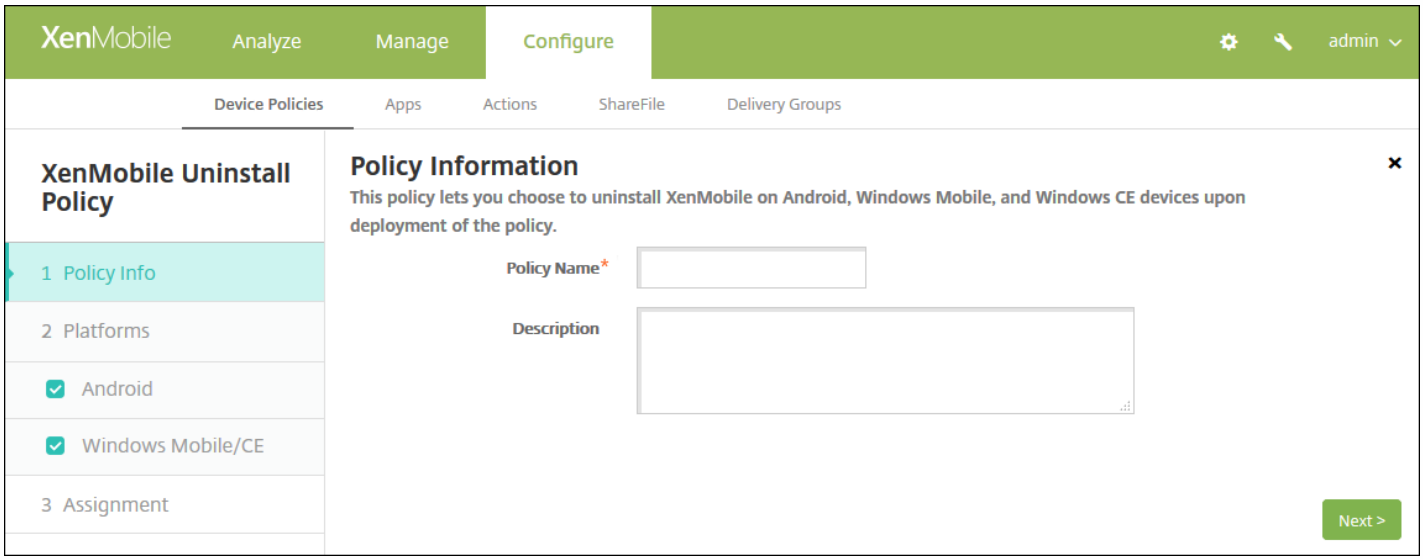
7. Konfigurieren der Bereitstellungsregeln



-
-
-
-
-

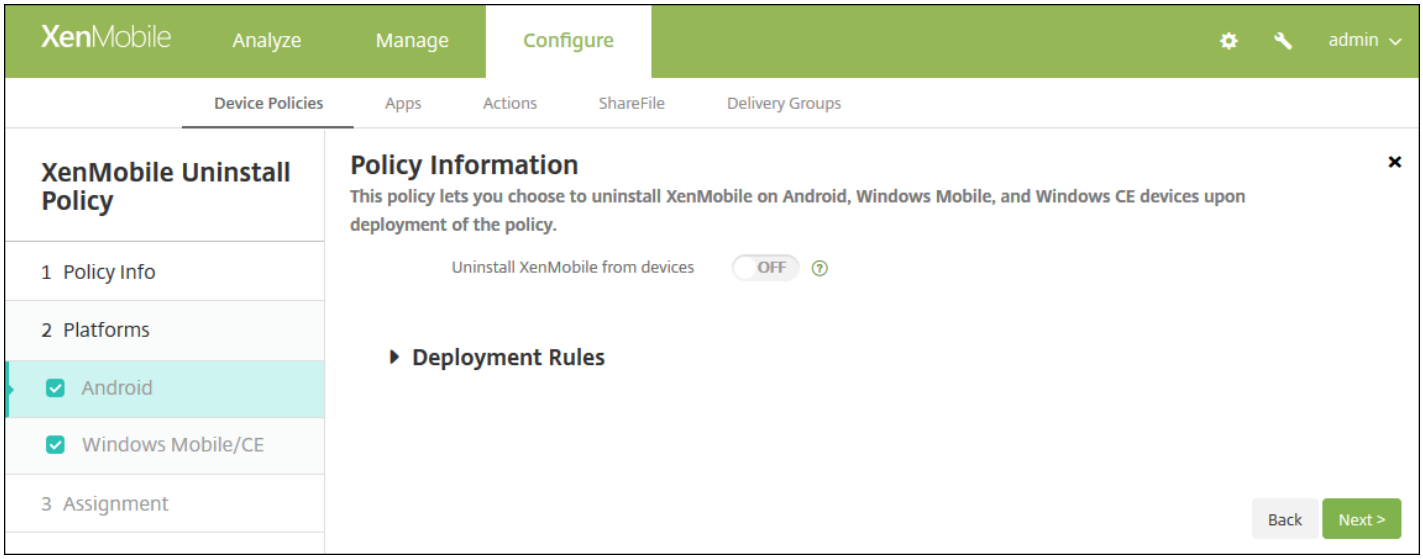
-
-

XenMobile-Deinstallationsrichtlinie



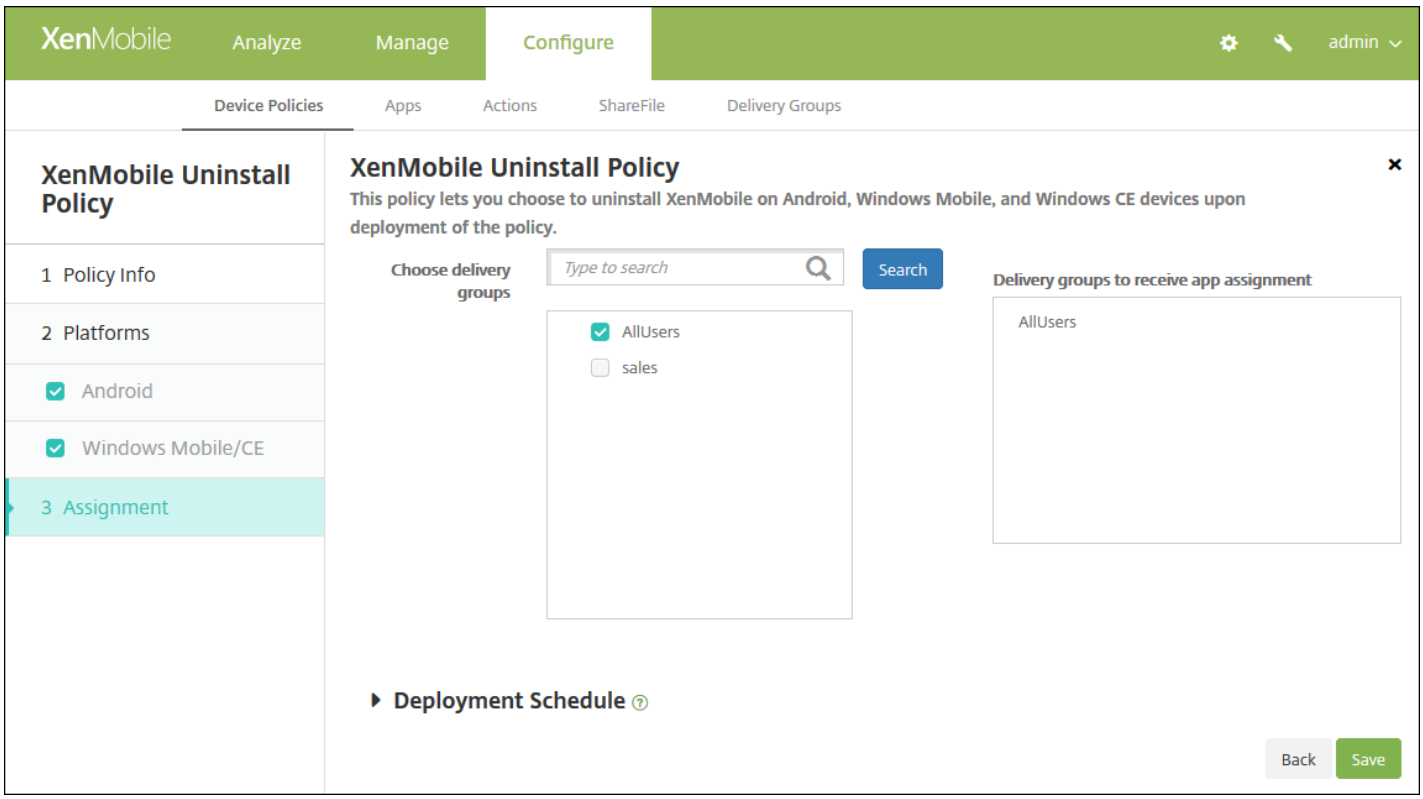
-
-

Konfigurieren von Android- und Windows Mobile-/CE-Einstellungen



-

7. Konfigurieren der Bereitstellungsregeln



-
-
-
-
-
-
-

Hinzufügen von Apps in XenMobile

-
-
-
-
-

> Hinweis
>
> -
> -

Funktionsweise von mobilen Apps und MDX-Apps

-
-

Funktionsweise von Web- und SAAS-Apps

Funktionsweise von Unternehmensapps

Funktionsweise des öffentlichen App Store

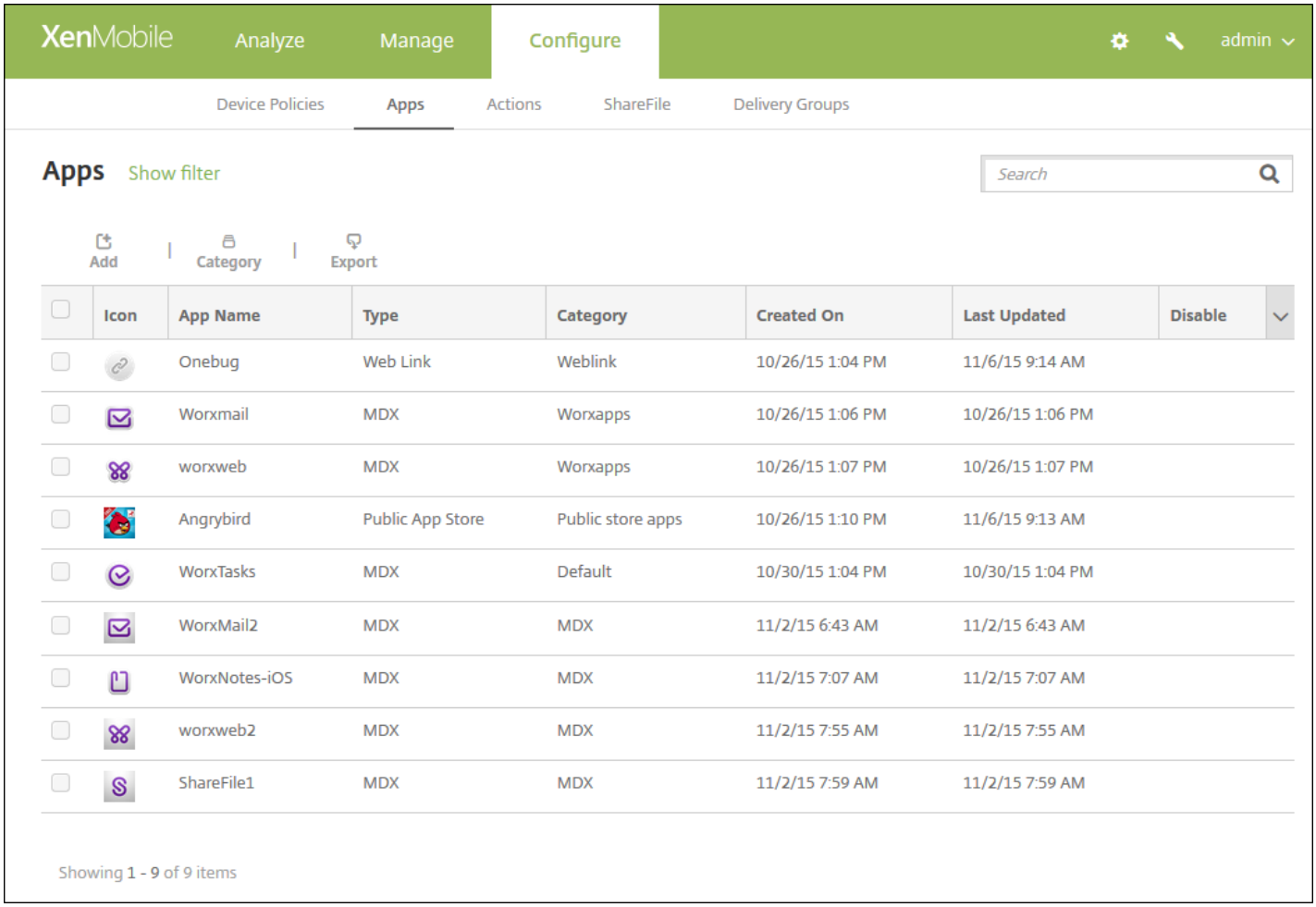
Funktionsweise von Weblinks

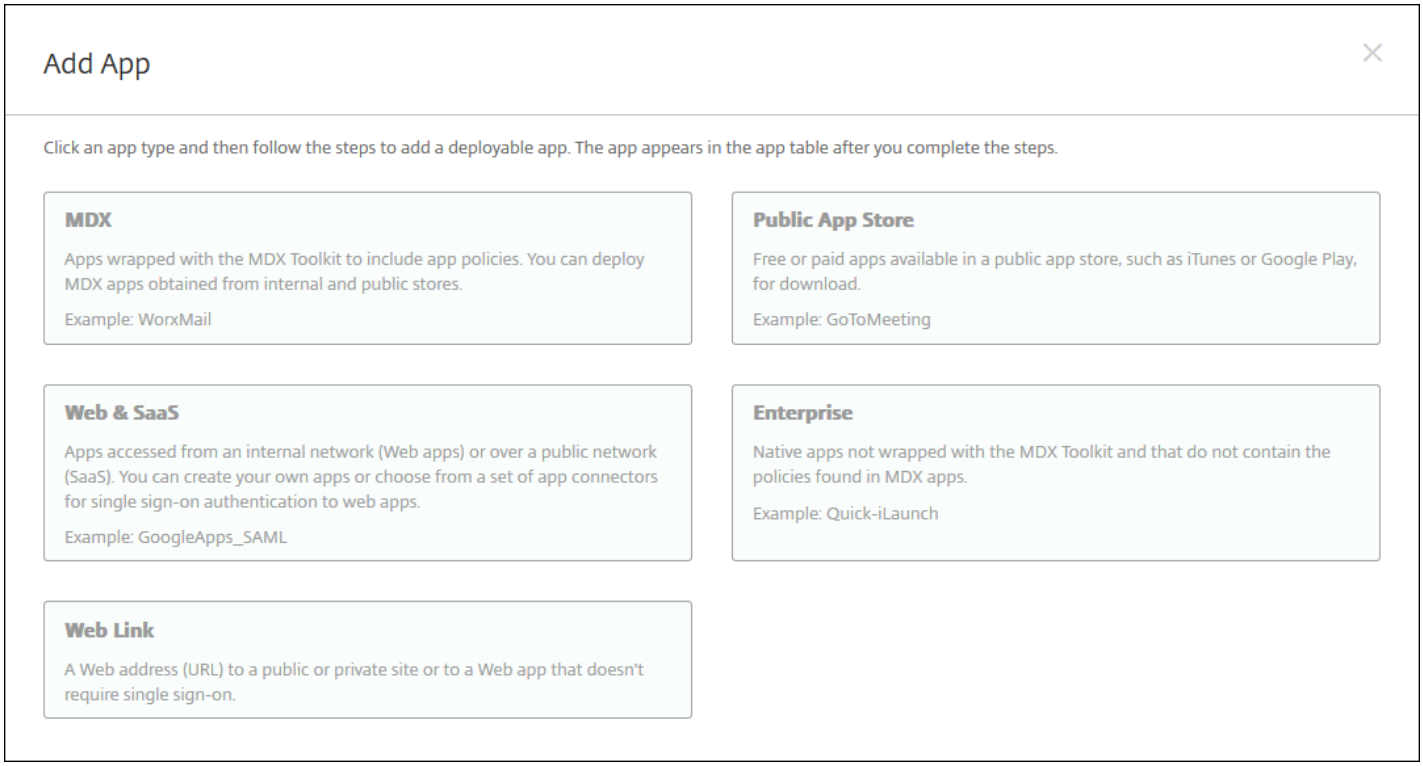
-
-
-
-

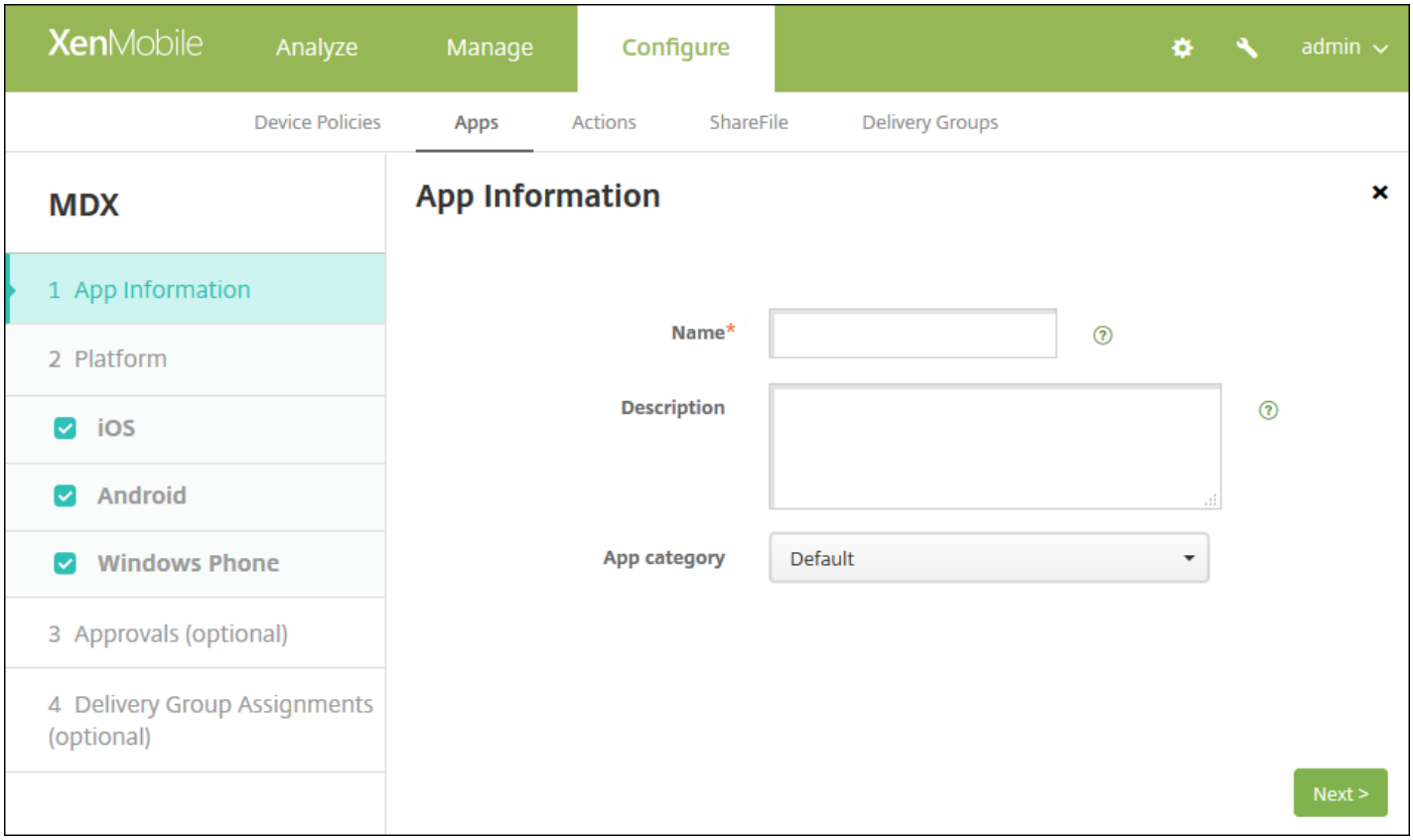
-
-
-
-
-

Hinweis

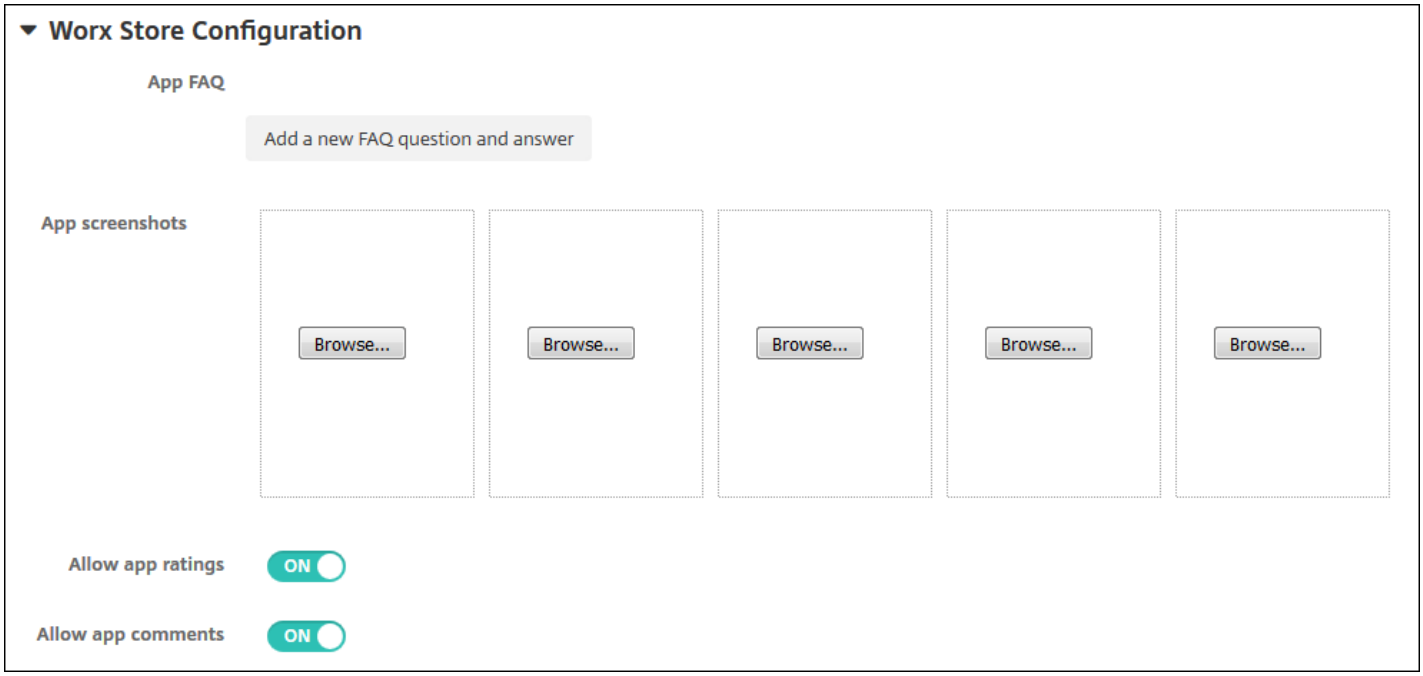
Hinzufügen von MDX-Apps zu XenMobile



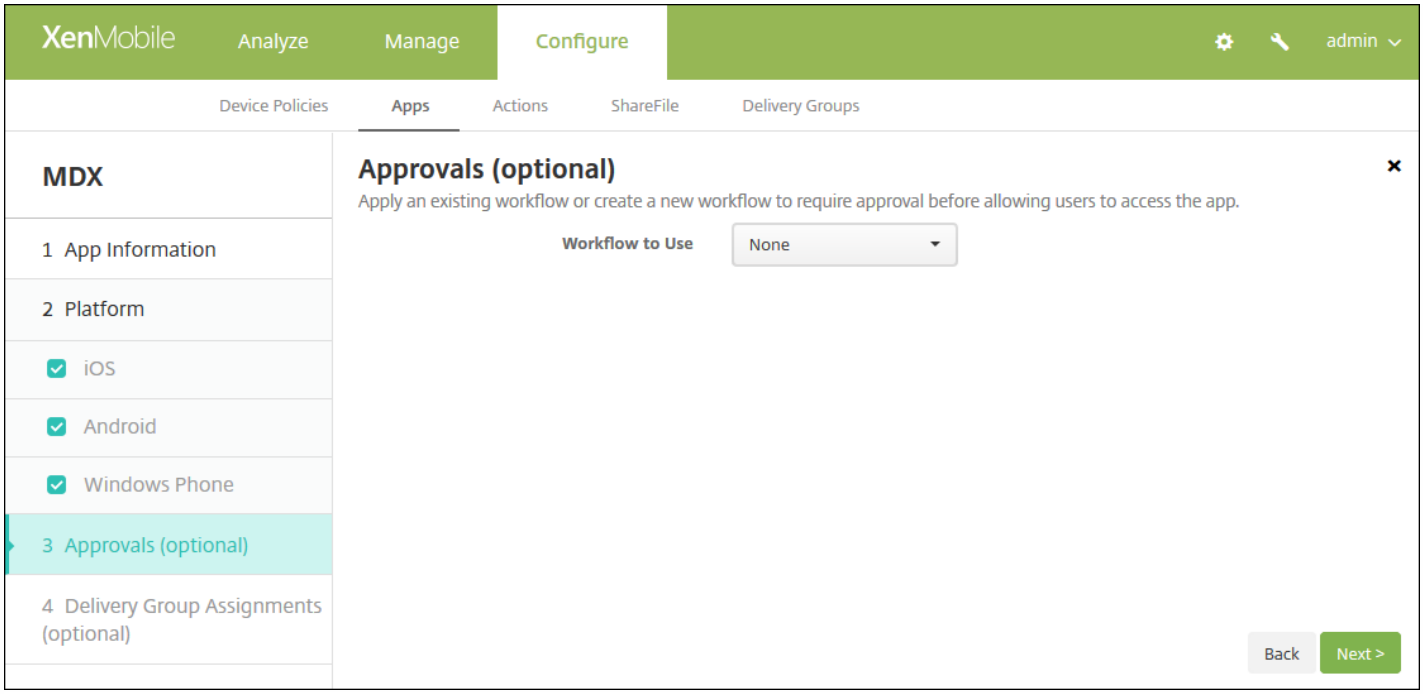




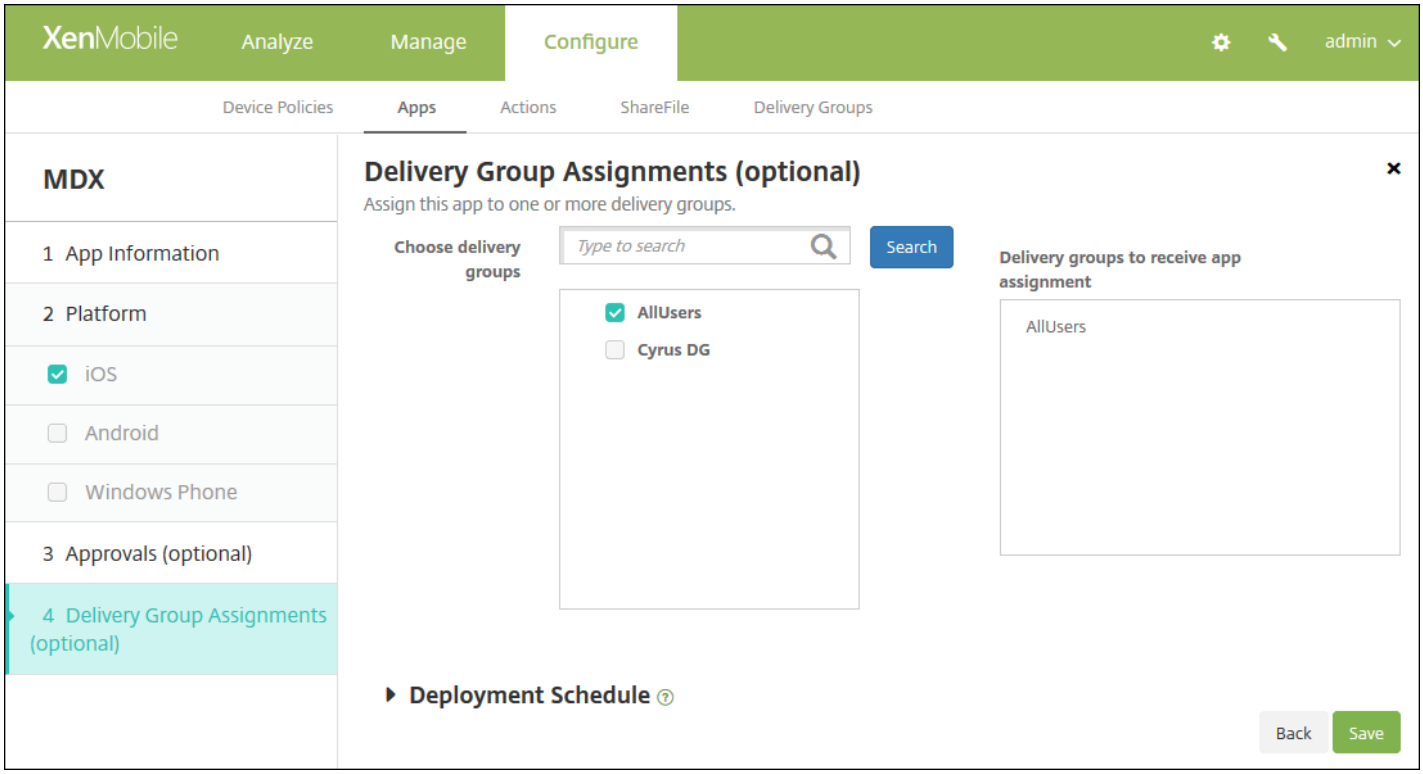
11. Konfigurieren der Bereitstellungsregeln



-
  -
  -
  -
  -

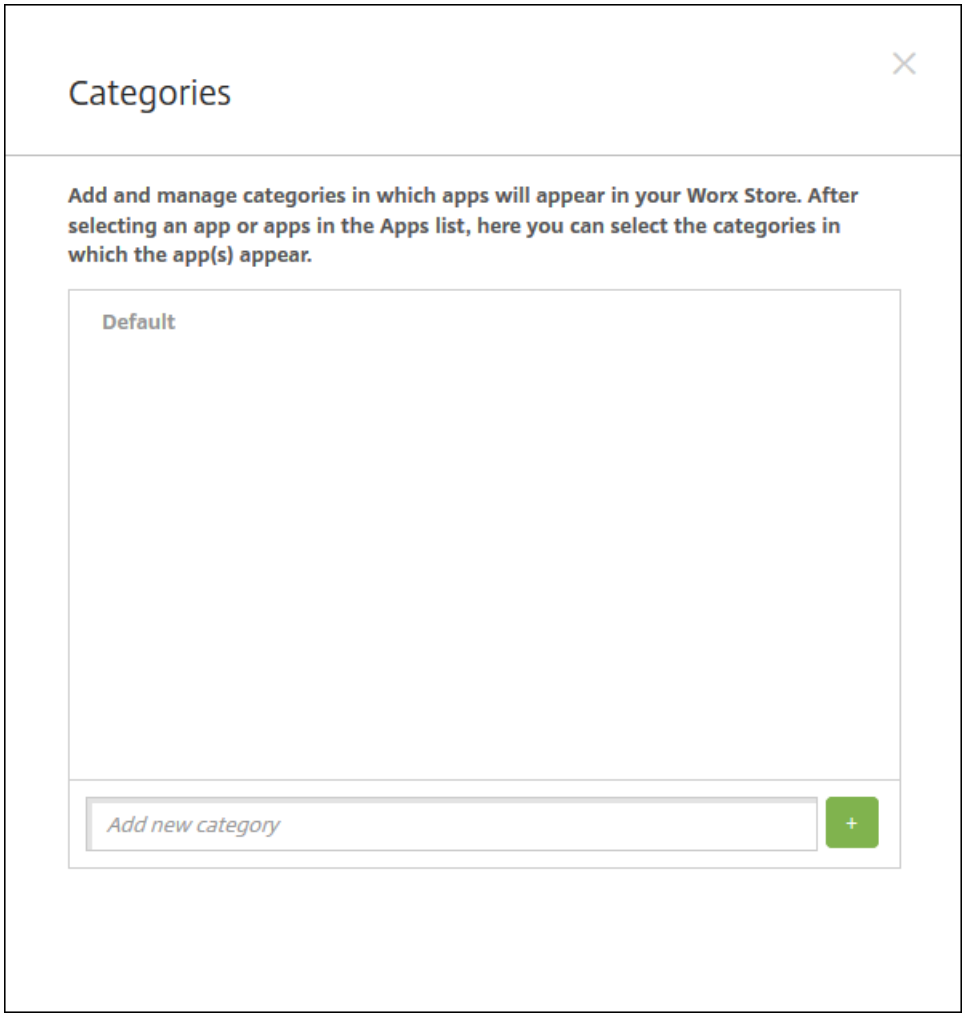


-
-
  -
  -
  -
  -
    -
    -
    -
    -
  -
  -
  -
    -
      -

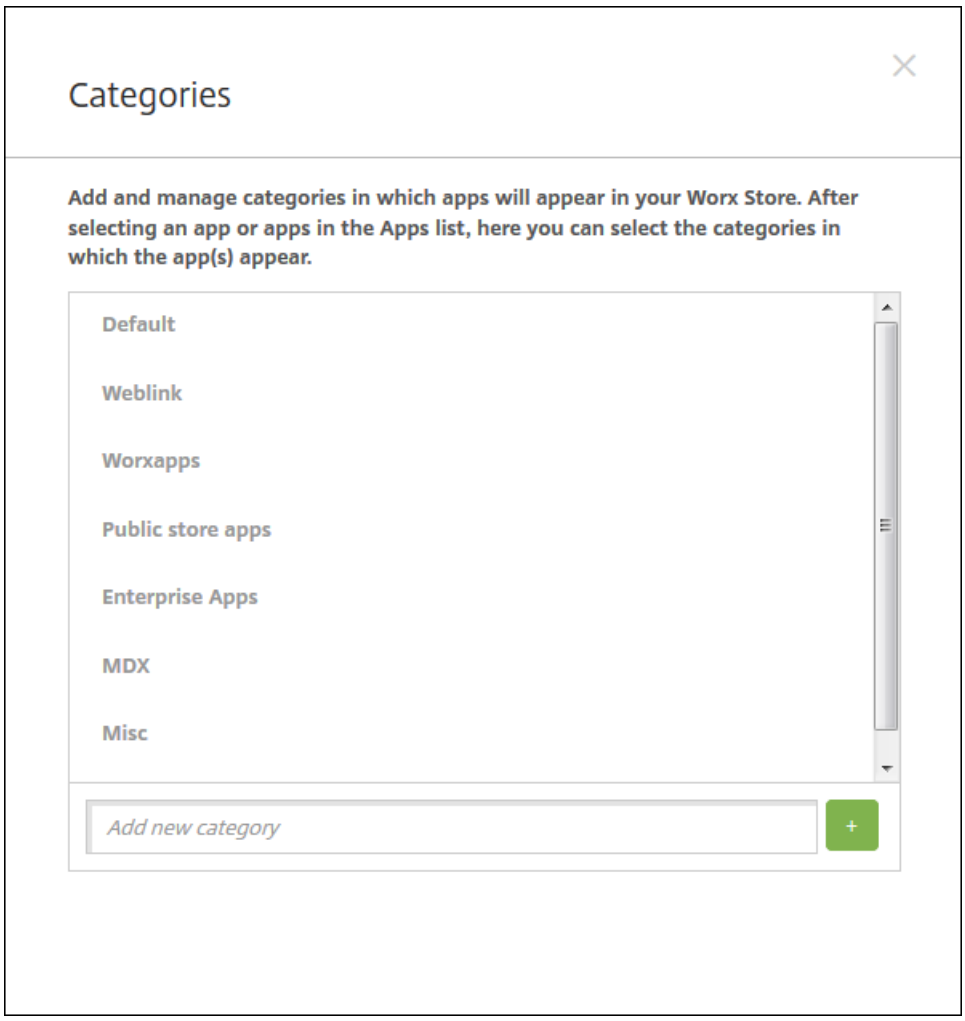


-

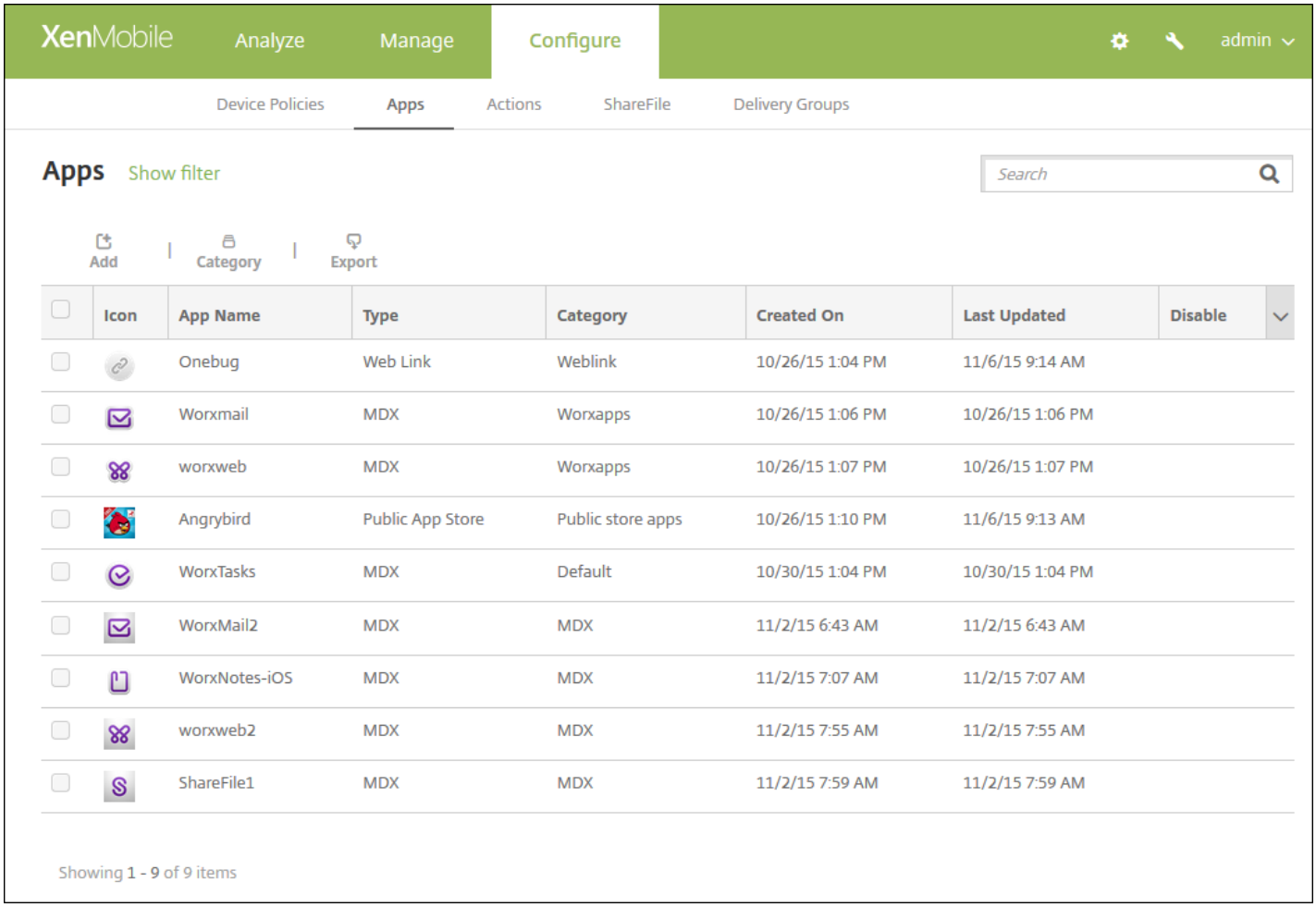
Erstellen von App-Kategorien in XenMobile

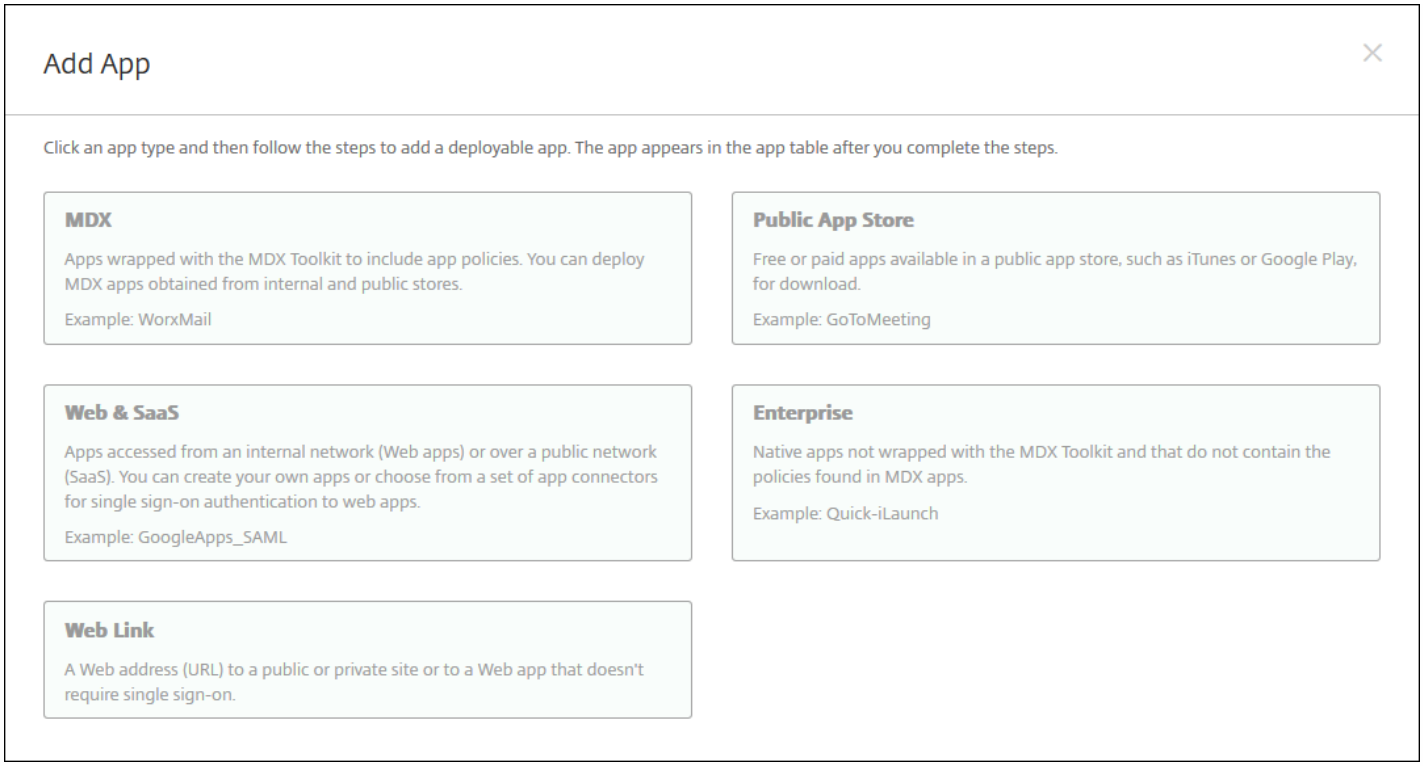


-

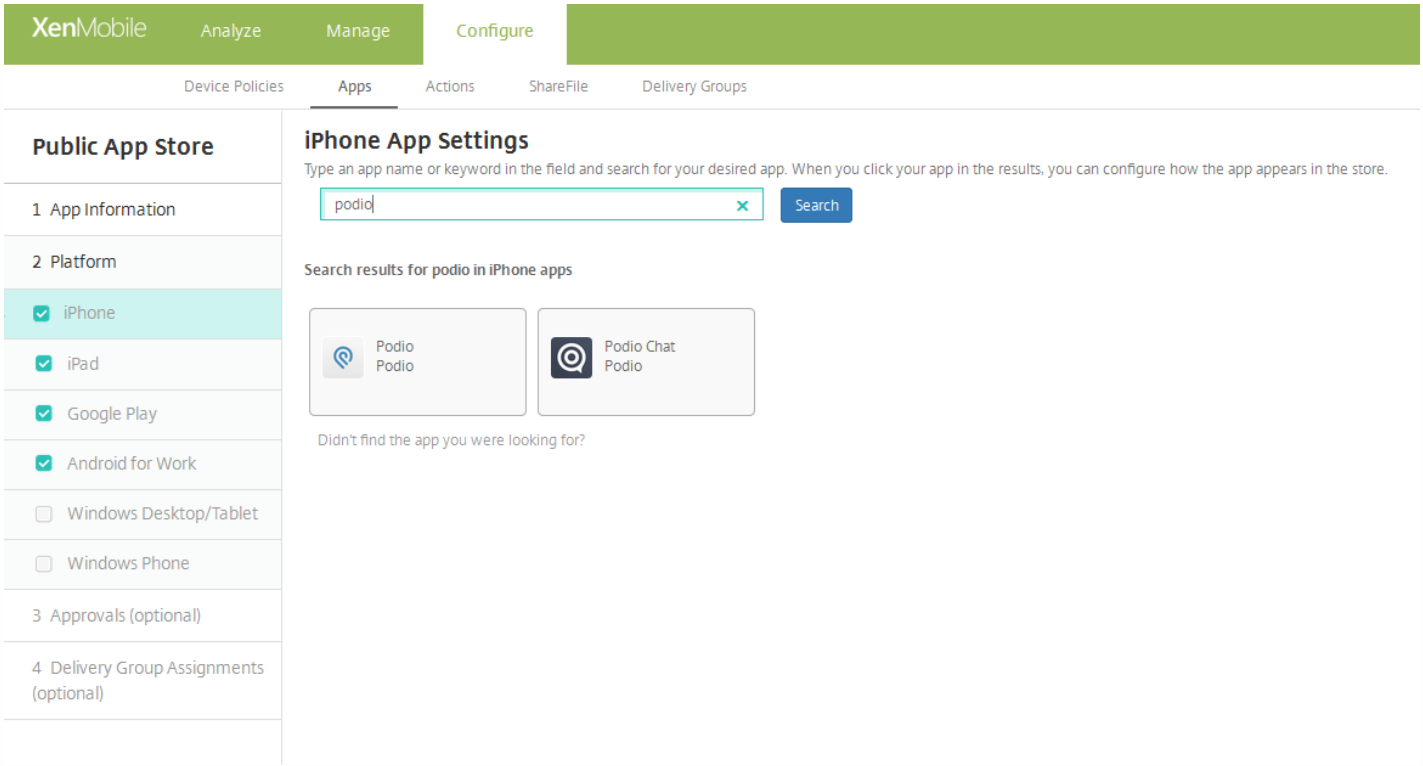


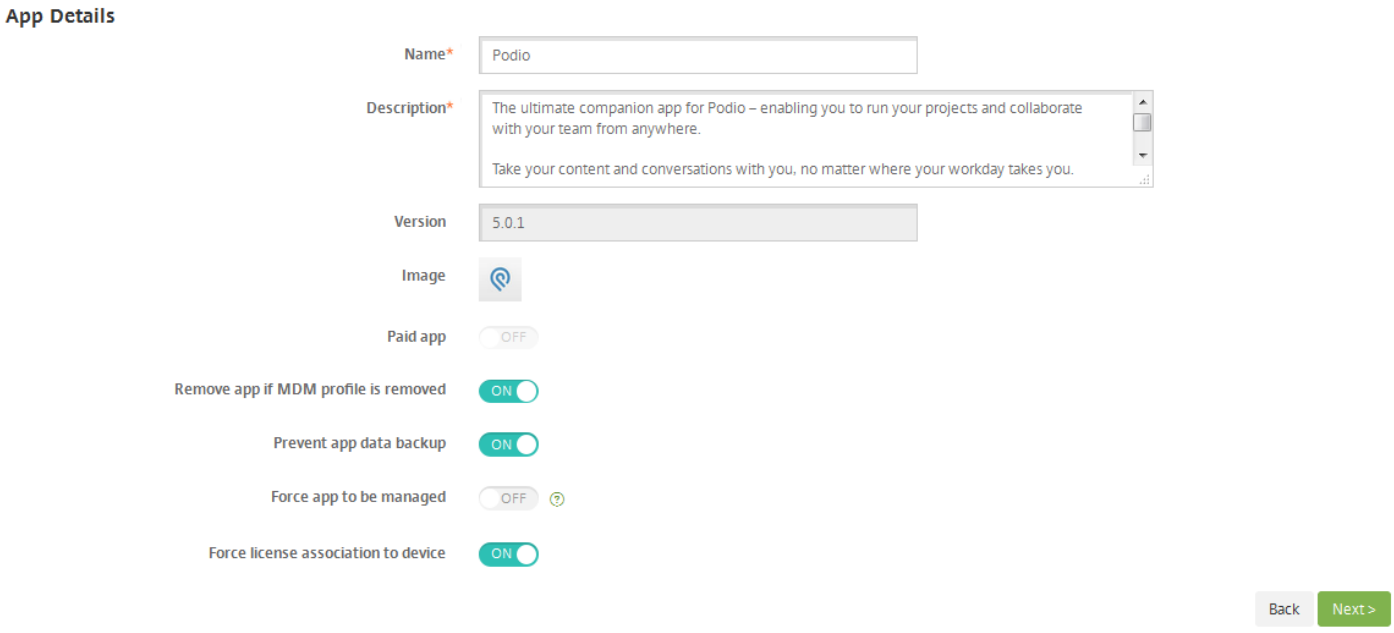
Hinzufügen von Apps aus einem öffentlichen App-Store zu XenMobile





-
-
-

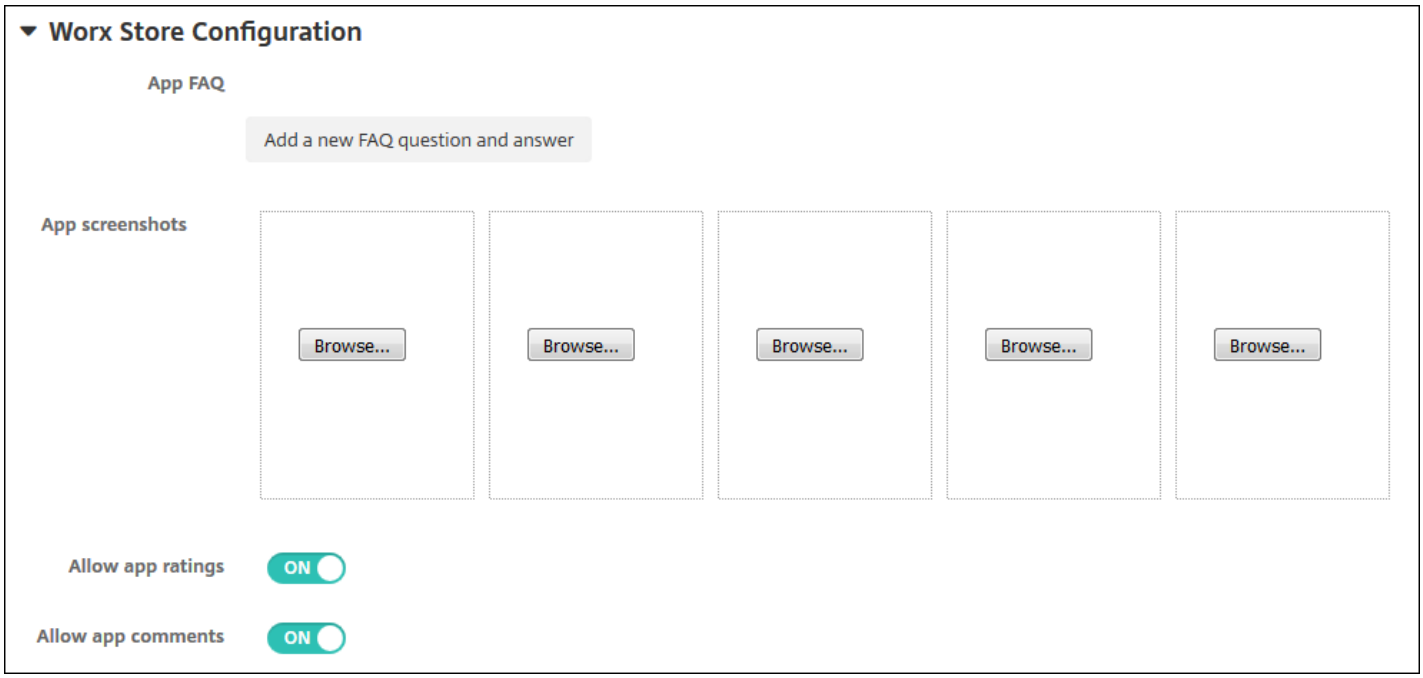




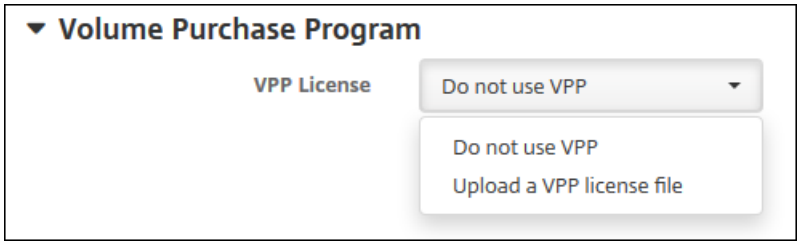
-
-

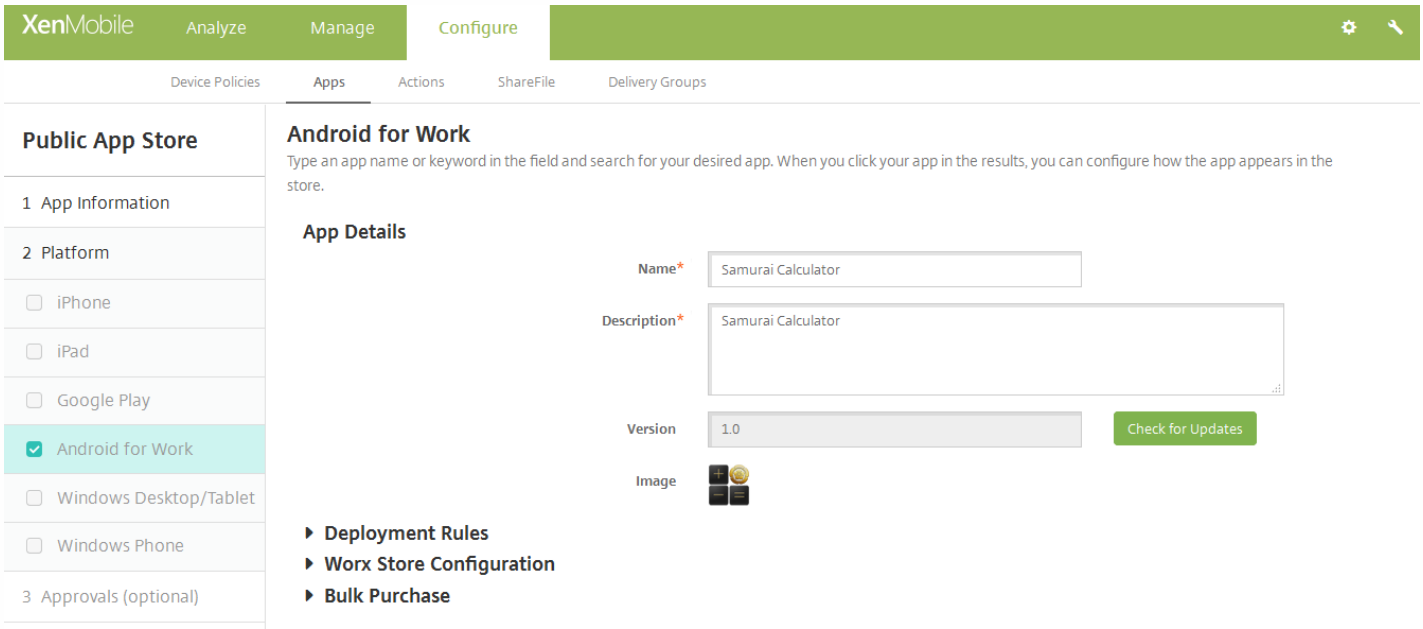
-
-
-
-

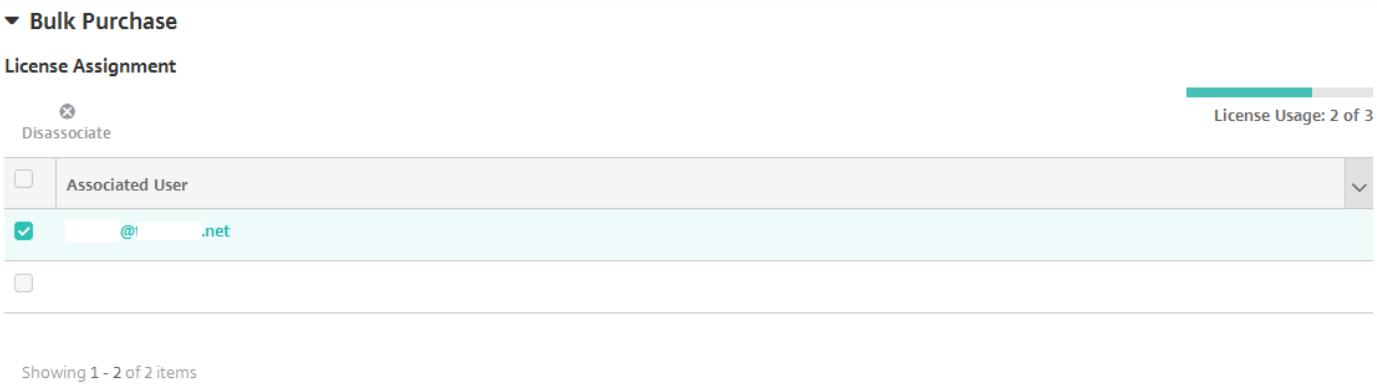
10. Konfigurieren der Bereitstellungsregeln



-
  -
  -
  -
  -

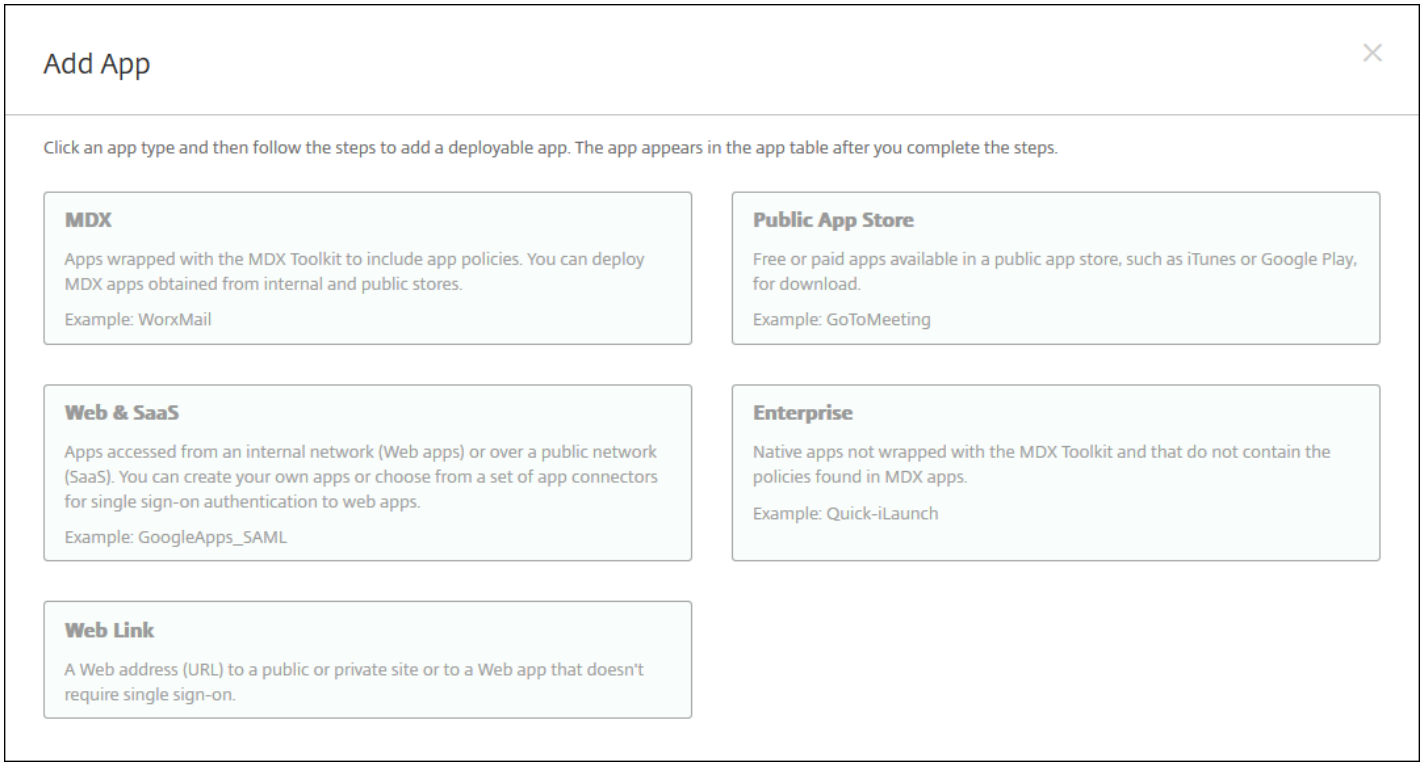


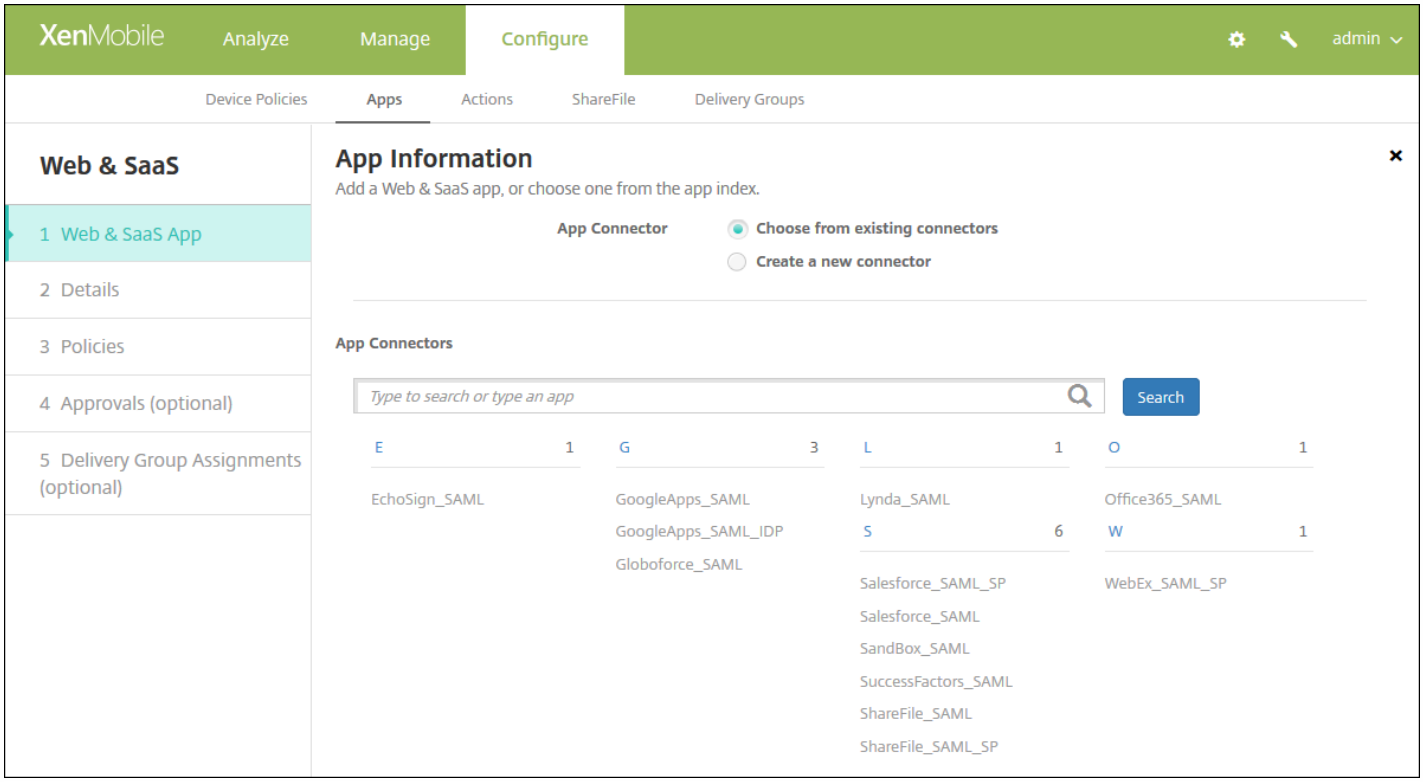


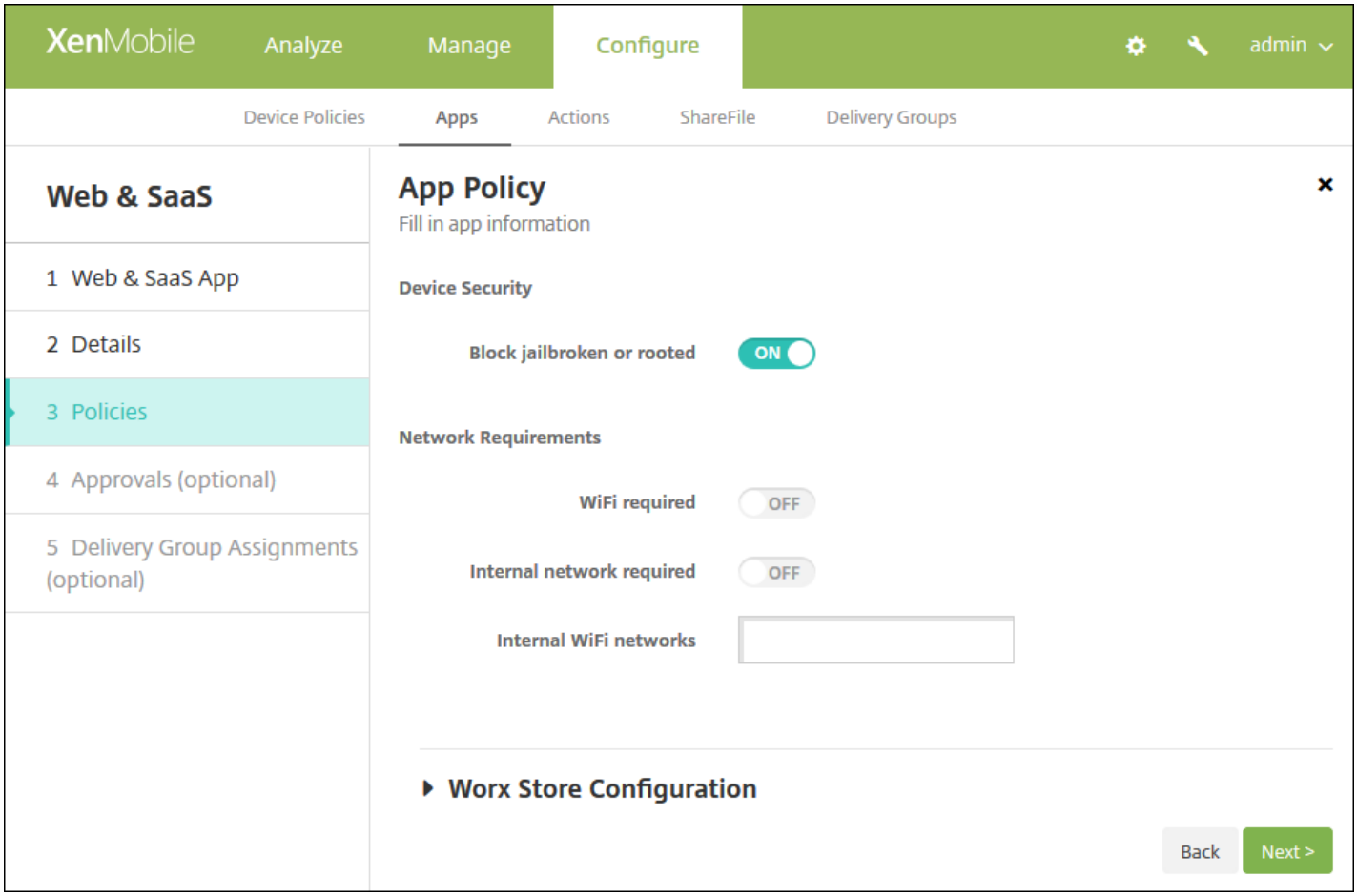


-
-
-
-
-

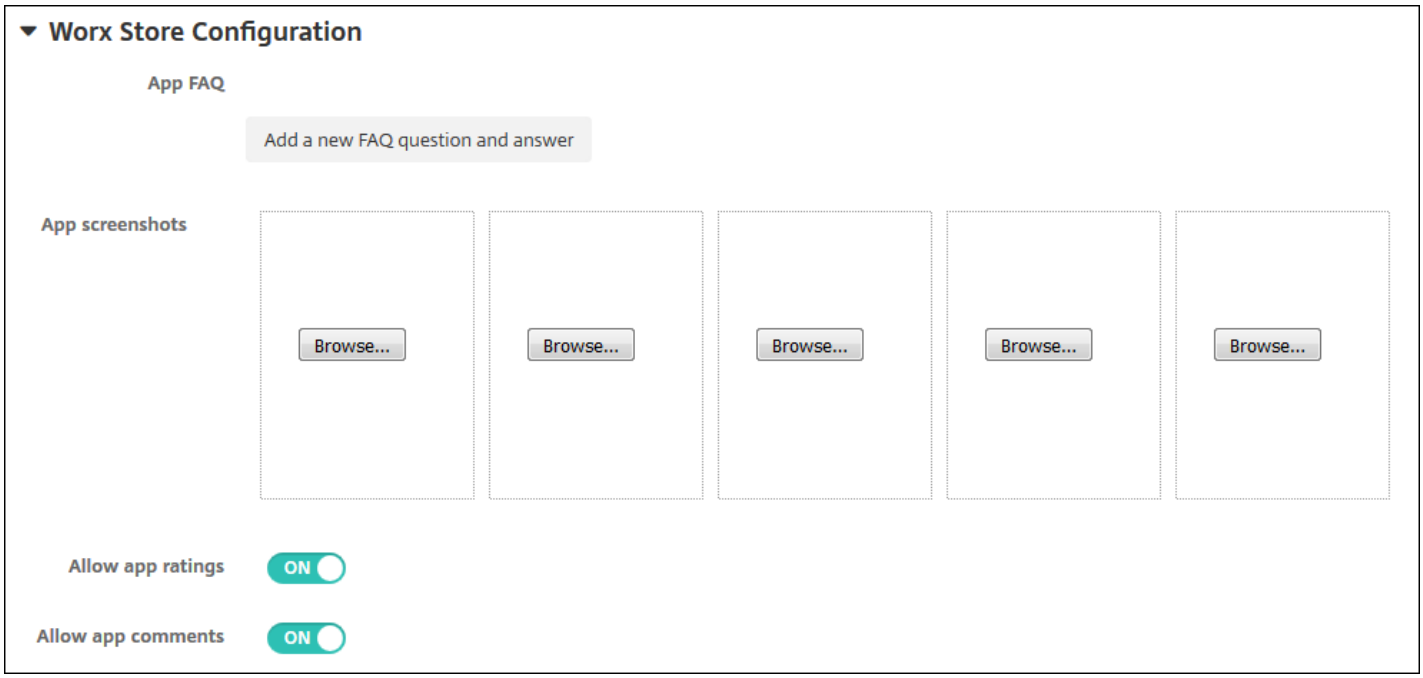
Hinzufügen von Web- und SaaS-Apps zu XenMobile



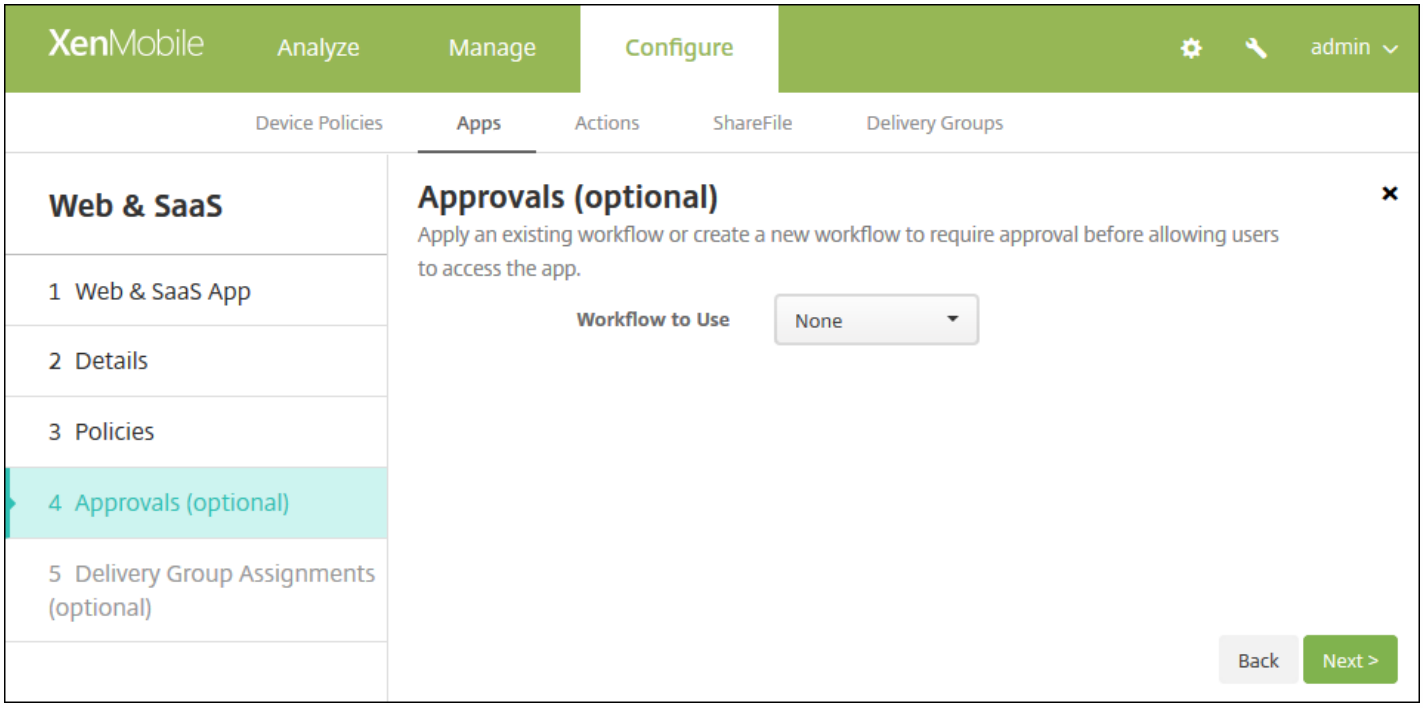




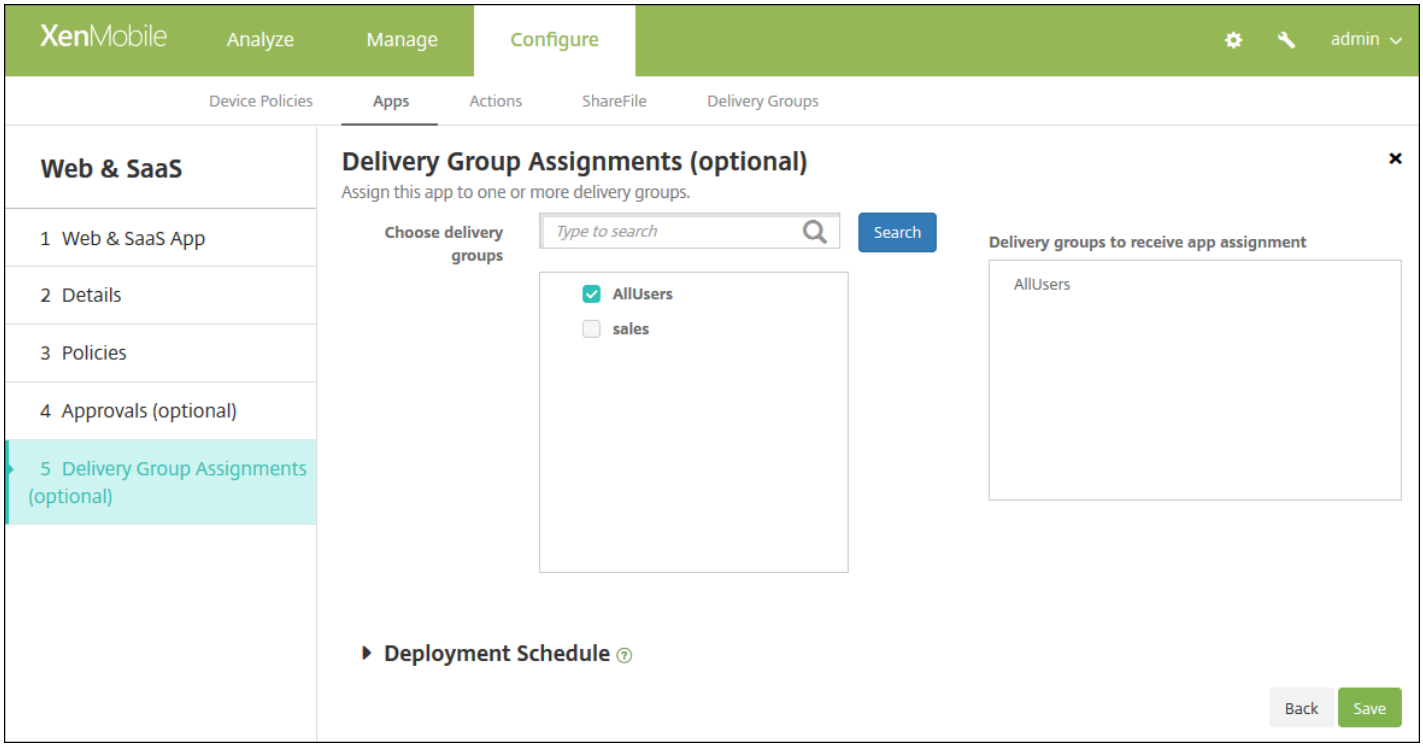
-
-
  -
  -
  -



-
  -
  -
  -
  -



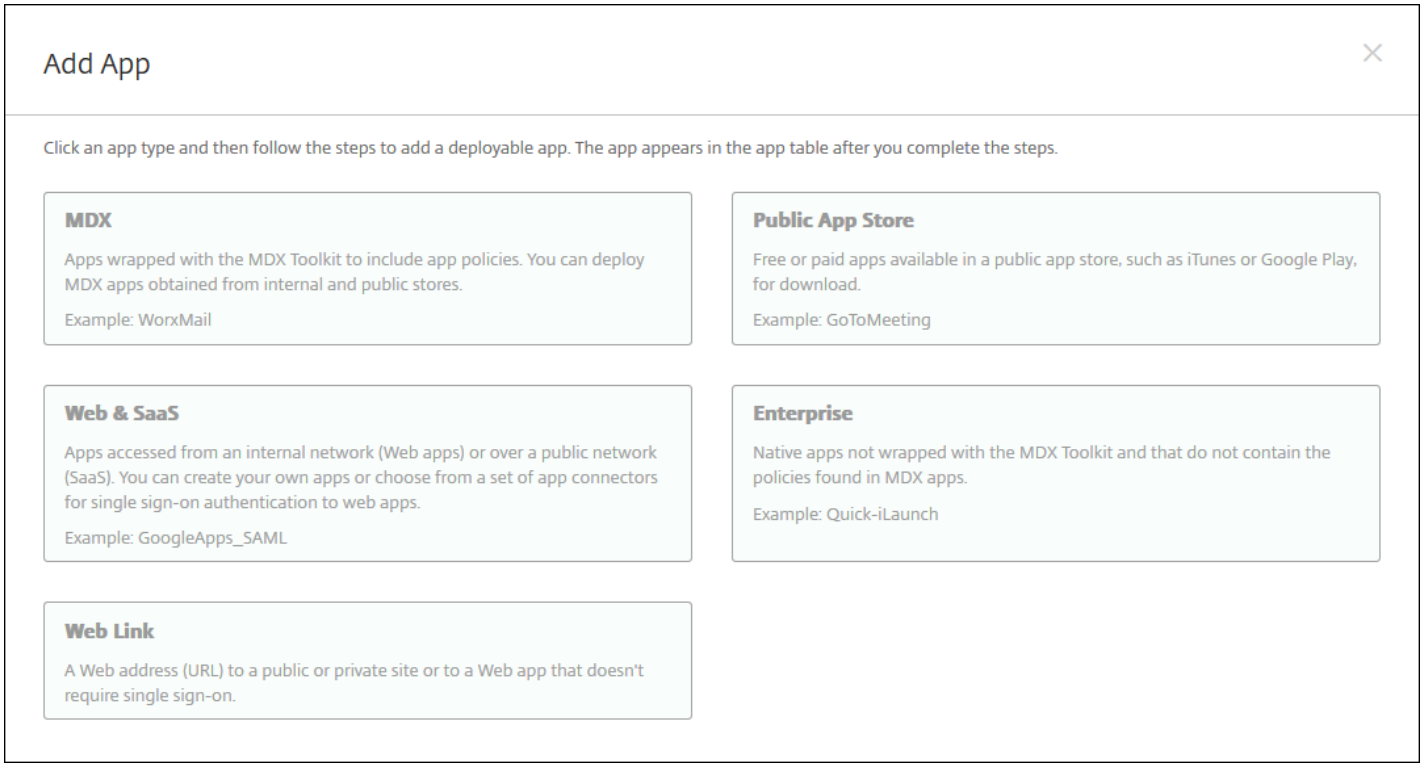
-
-
  -
  -
  -
  -
    -
    -
    -
    -
  -
  -
  -
    -
      -

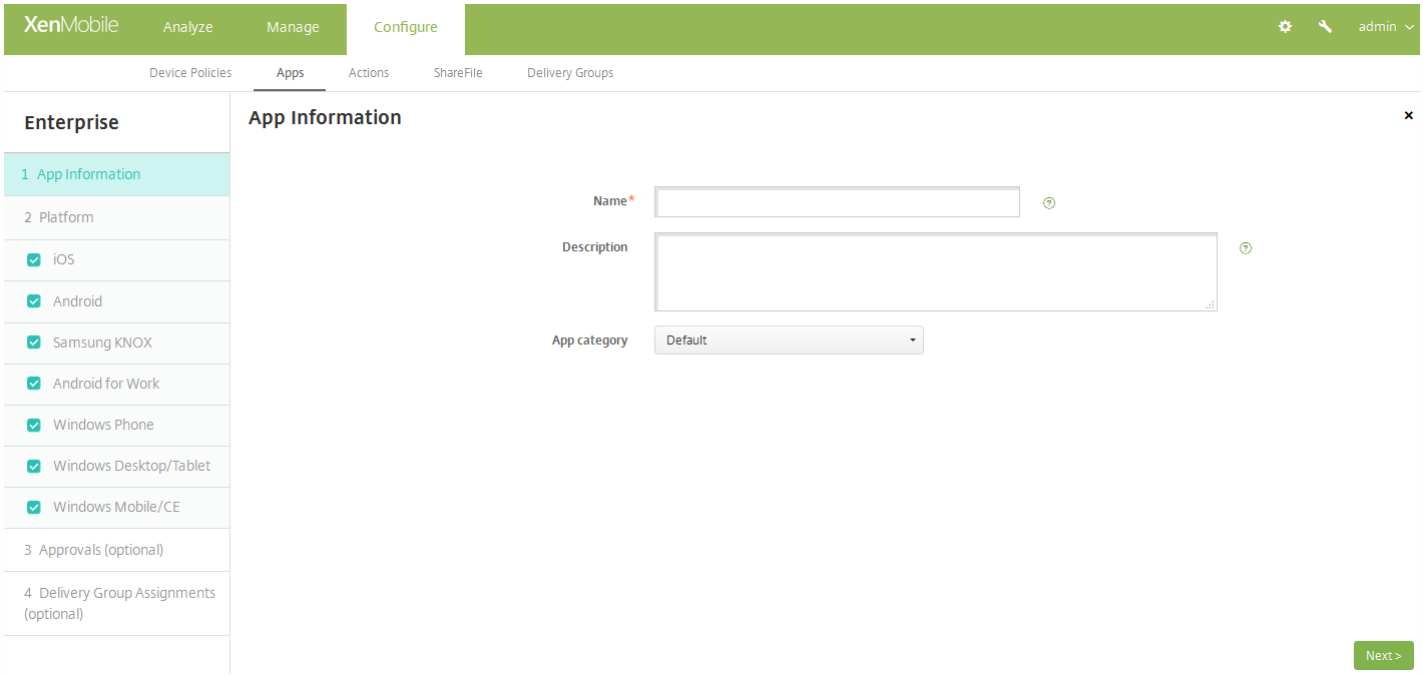


-

Liste der Anwendungsconnectortypen

Hinzufügen von Unternehmensapps zu XenMobile

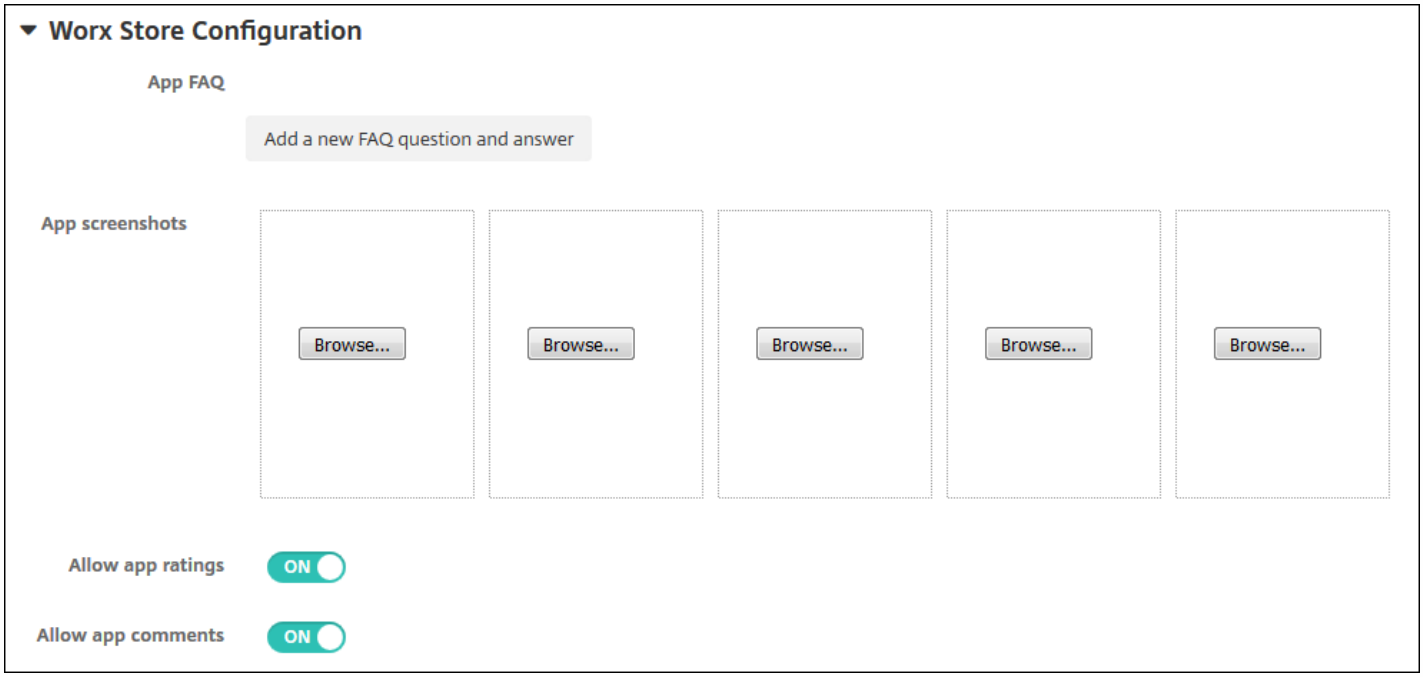




-
-
-
-
-
-
-
-
-
-

-
-

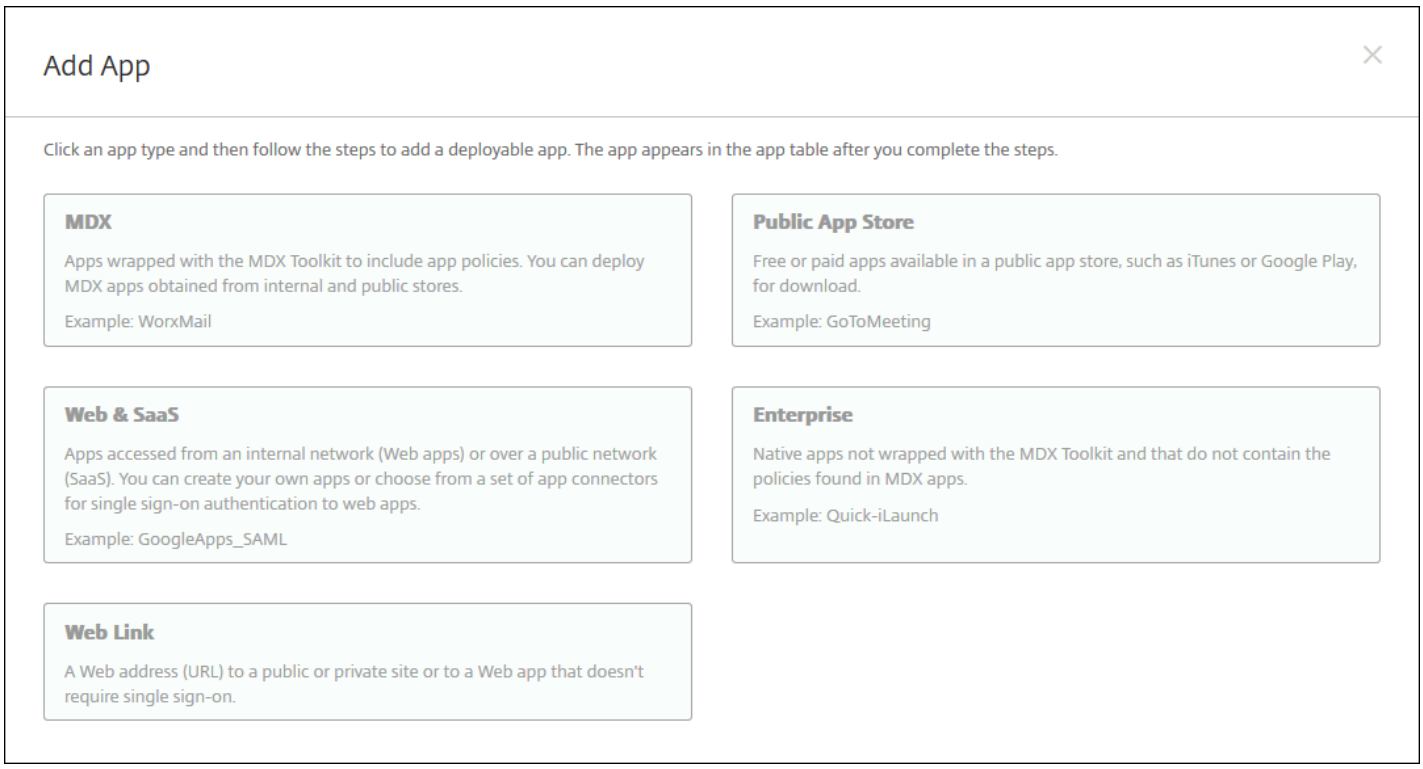
10. Konfigurieren der Bereitstellungsregeln

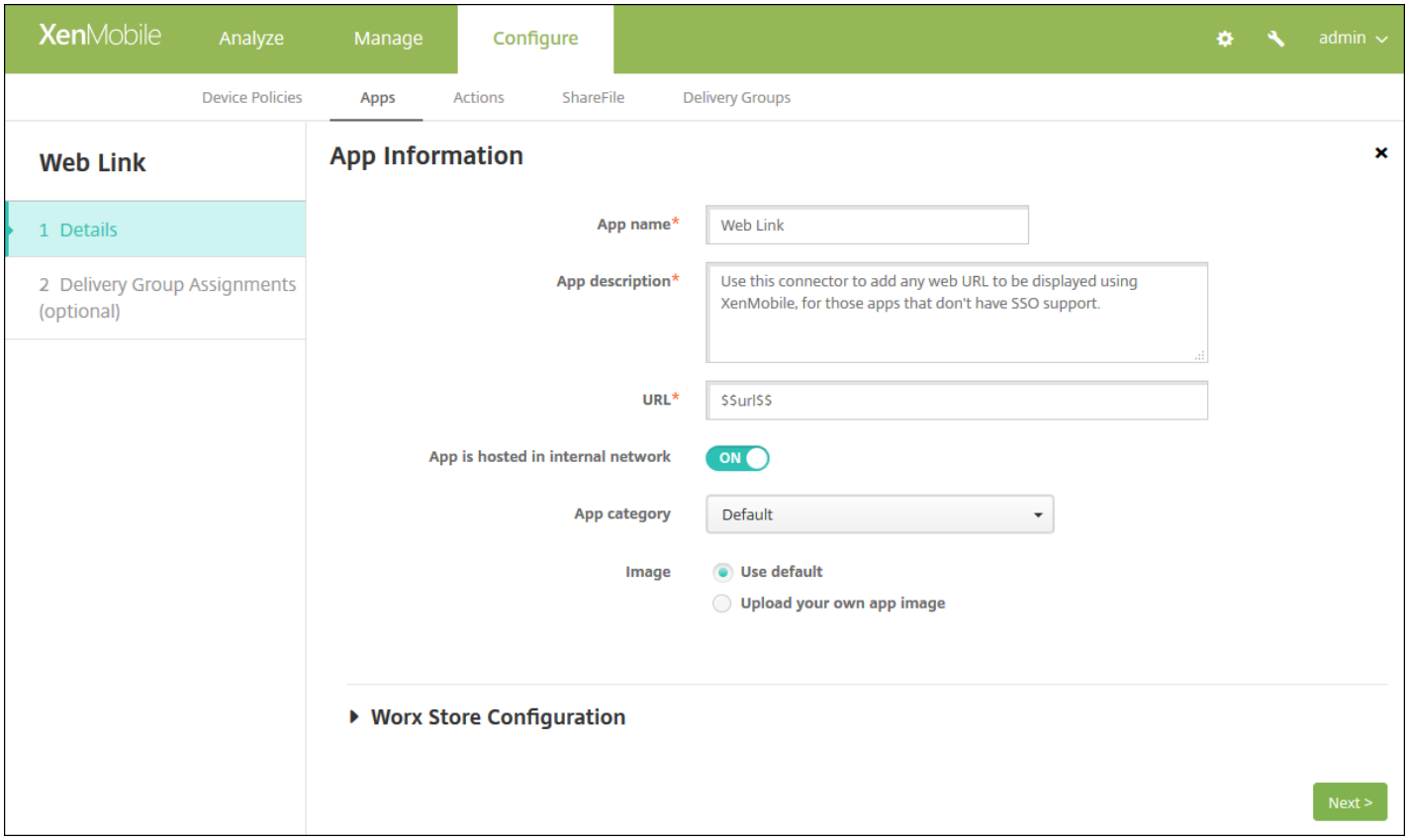


-
  -
  -
  -
  -
-

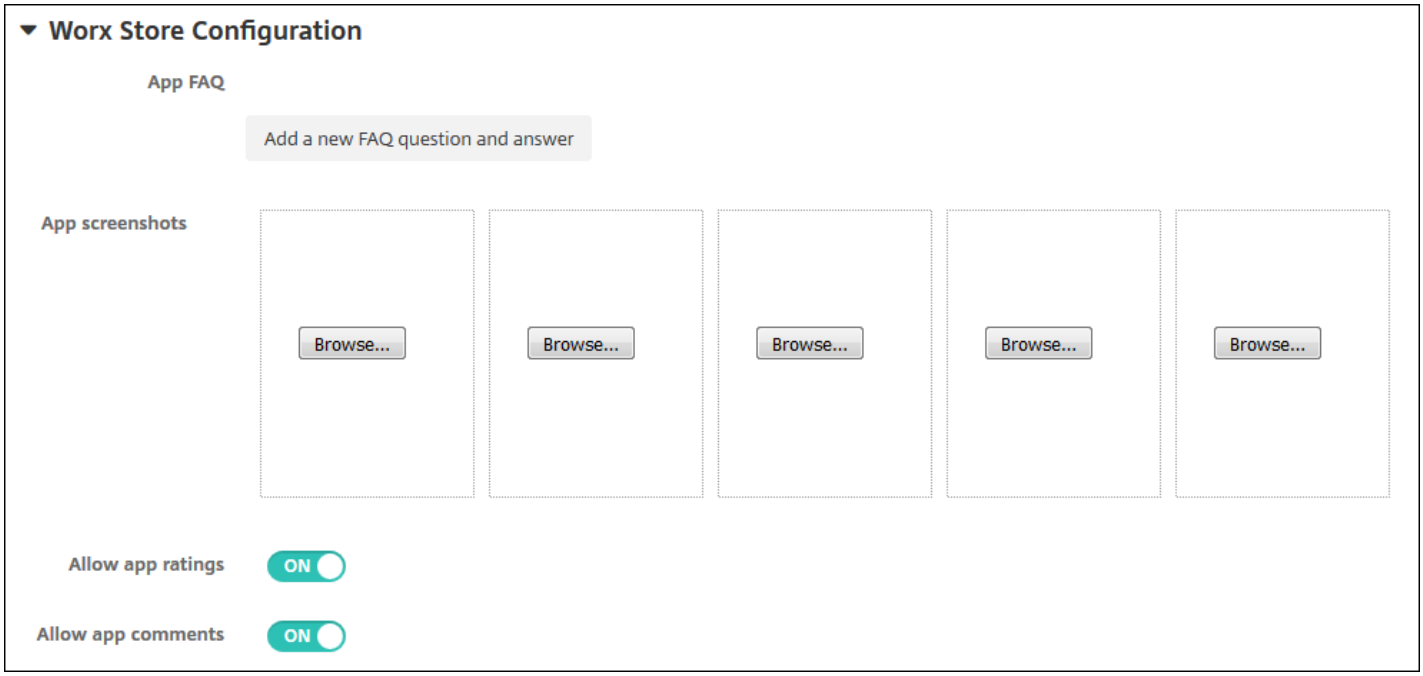
-

Hinzufügen von Weblink-Apps zu XenMobile

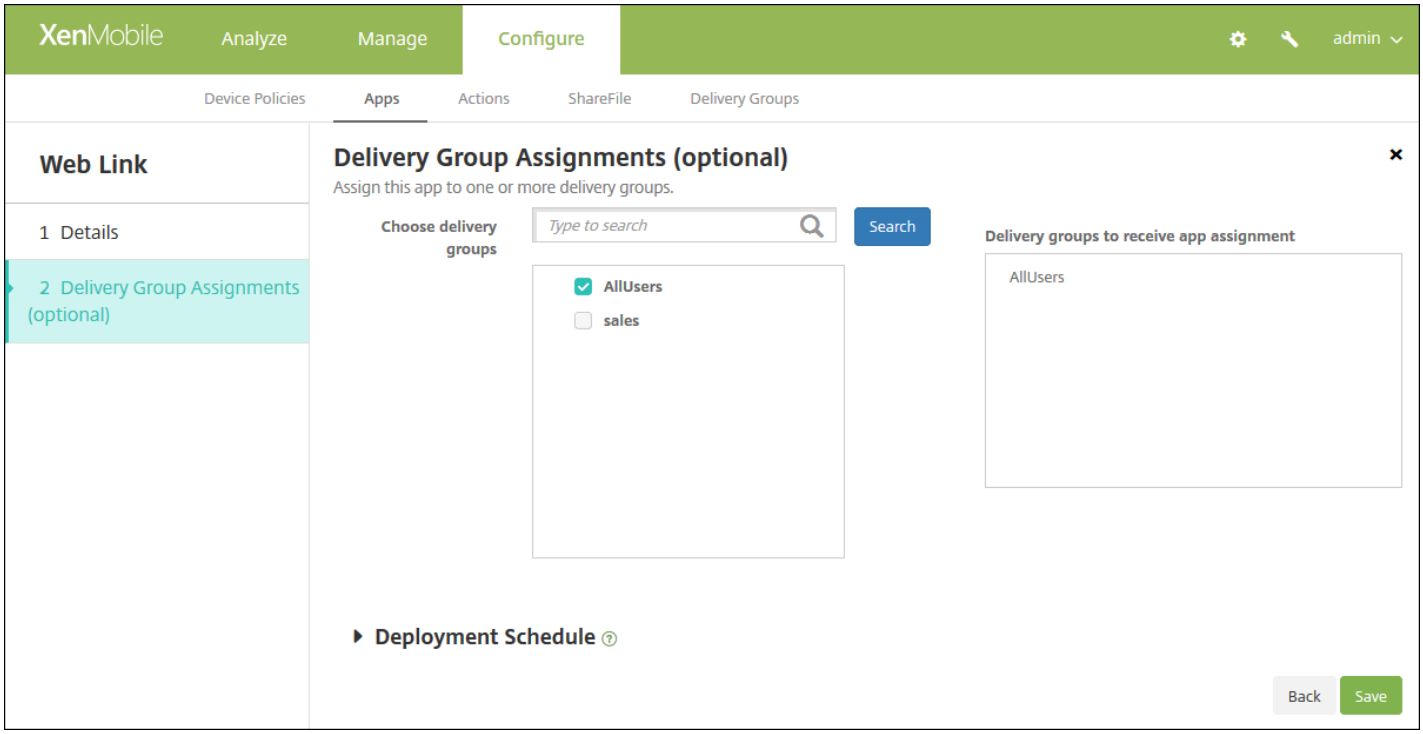




-
-
-
-
-
-
-



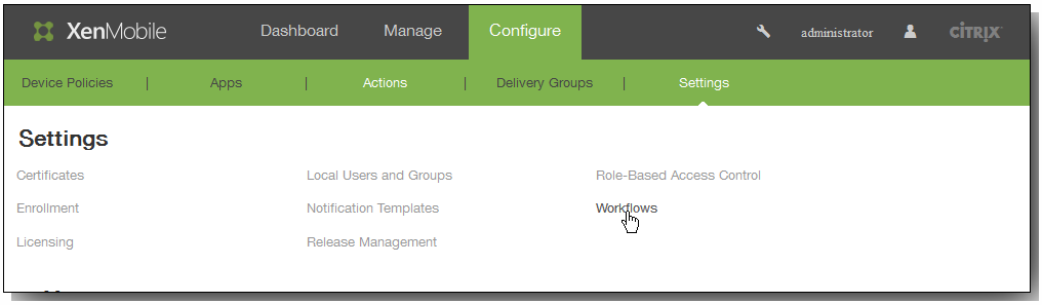
-
  -
  -
  -
  -

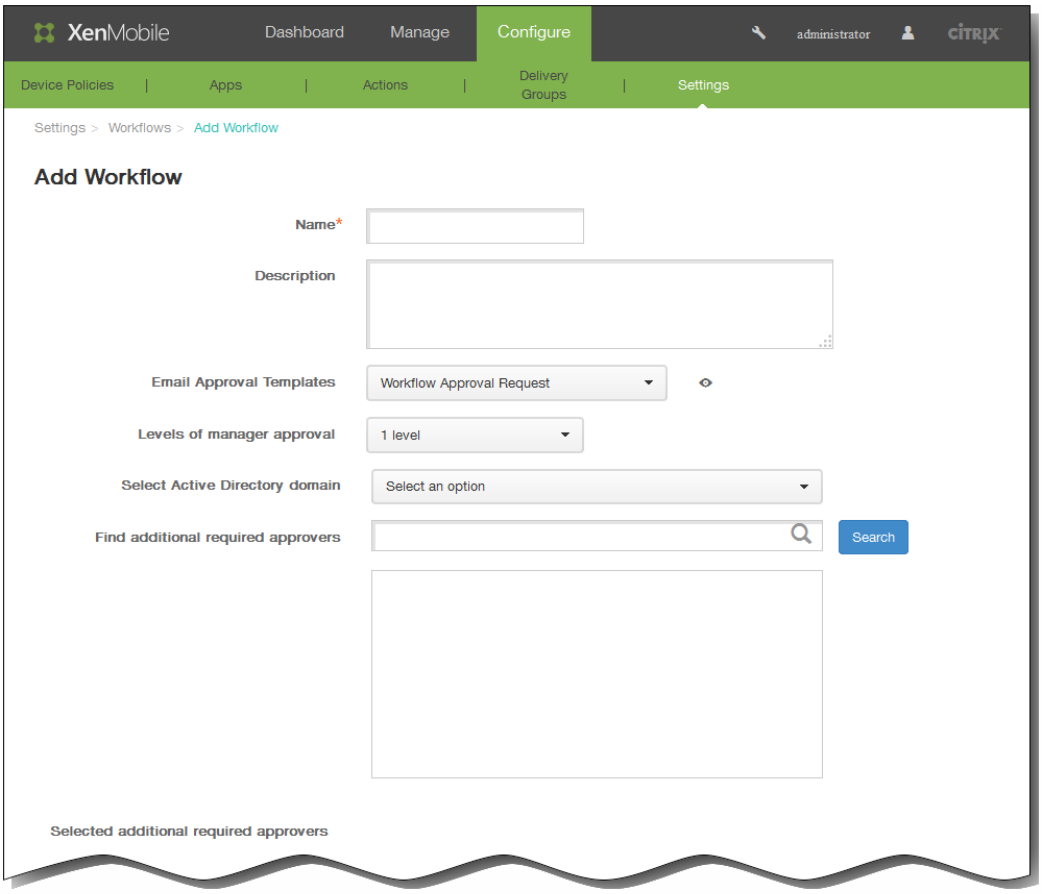


-
-
-
-
-
-
-

Erstellen und Verwalten von Workflows in XenMobile

-
-





-
-

Anzeigen von Details und Löschen eines Workflows

Aktualisieren von MDX- und Unternehmensapps in XenMobile

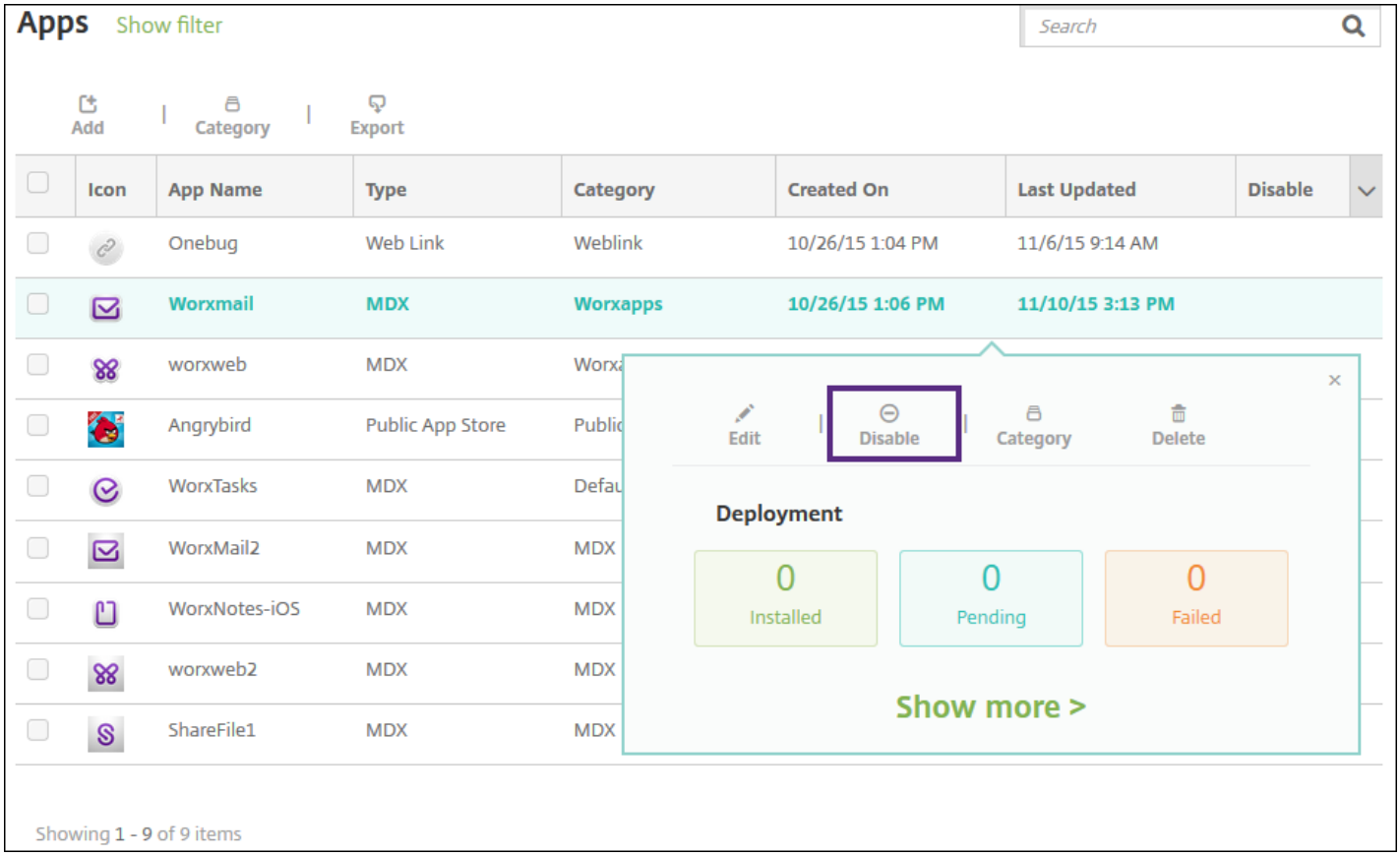
Jul 28, 2016

Zum Aktualisieren einer MDX- oder Unternehmensapp in XenMobile deaktivieren Sie diese in der XenMobile-Konsole und laden die neue App-Version hoch.

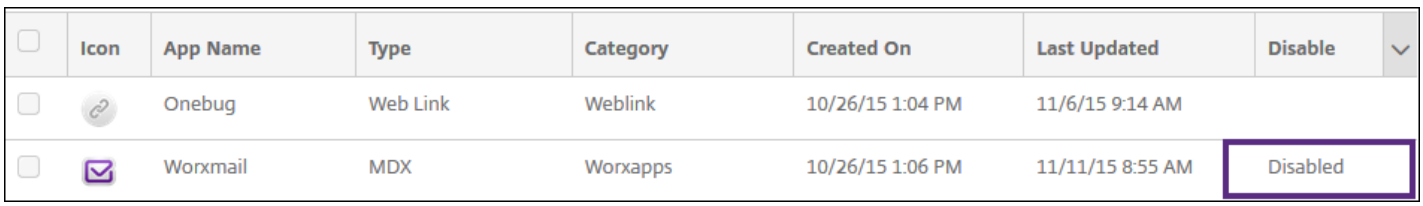
1. Klicken Sie in der XenMobile-Konsole auf **Konfigurieren** > **Apps**. Die Seite **Apps** wird angezeigt.

2. Fahren Sie bei verwalteten, d. h. bei XenMobile für die Mobilgeräteverwaltung registrierten Geräten mit Schritt 4 fort. Führen Sie für nicht verwaltete, d. h. bei XenMobile nur zum Zweck der App-Verwaltung registrierten Geräten die folgenden Schritte aus:

- Klicken Sie in der App-Tabelle auf das Kontrollkästchen neben der App, die aktualisiert werden soll, oder auf deren Zeile.
- Klicken Sie in dem daraufhin angezeigten Menü auf **Deaktivieren**. Das Dialogfeld **Deaktivieren** wird angezeigt.



- Klicken Sie in dem Dialogfeld auf **Deaktivieren**. In der Spalte **Deaktivieren** der App wird nun *Deaktiviert* 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, es wird aber 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.

4. Klicken Sie in der App-Tabelle auf das Kontrollkästchen neben der App, die aktualisiert werden soll, oder auf deren Zeile.

5. Klicken Sie im angezeigten Menü auf **Bearbeiten**. Die Seite **App-Informationen** wird angezeigt, die ursprünglich für die App ausgewählte Plattform ist ausgewählt.

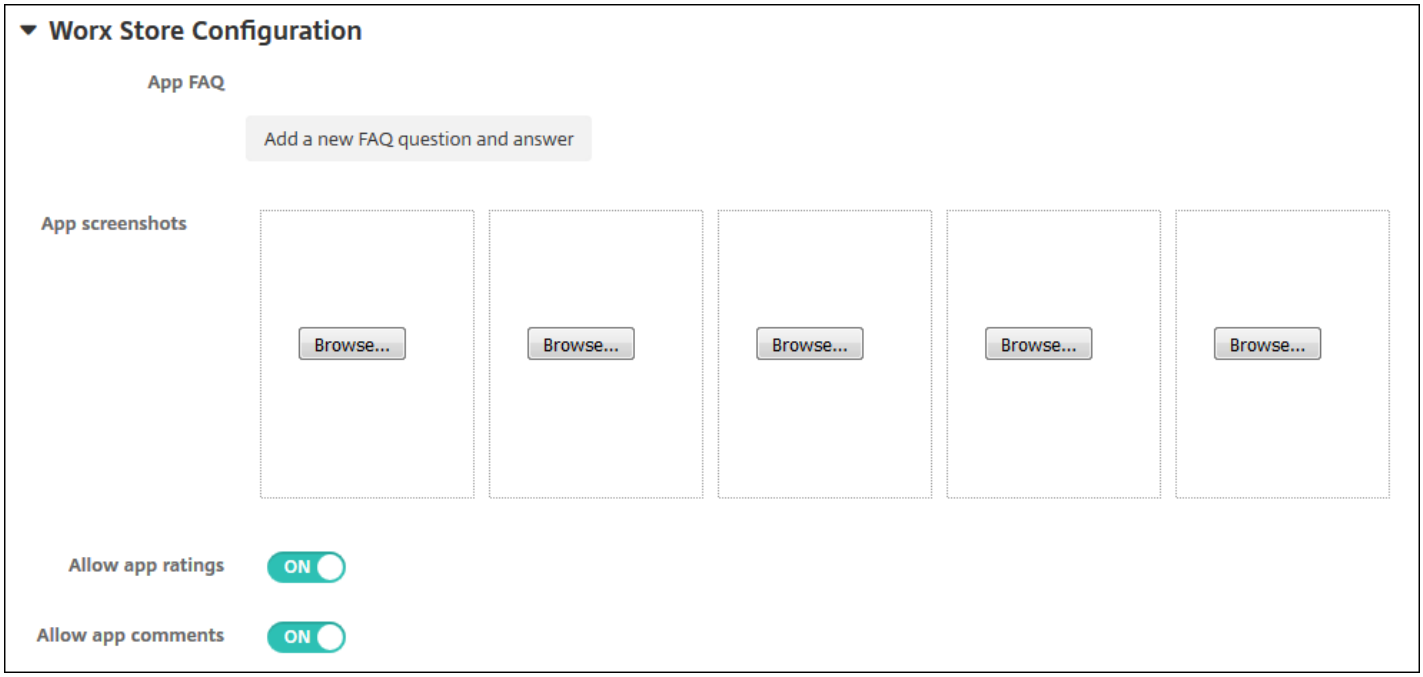
6. Konfigurieren Sie die folgenden Einstellungen:

- **Name**: Ändern Sie optional den Namen der App.
- **Beschreibung**: Ändern Sie optional die App-Beschreibung.
- **App-Kategorie**: Ändern Sie optional die App-Kategorie.

7. Klicken Sie auf **Weiter**. Die Seite der ersten ausgewählten Plattform wird angezeigt. Führen Sie für jede ausgewählte Plattform die folgenden Schritte aus:

- Wählen Sie die Datei aus, die Sie hochladen möchten, indem Sie auf **Upload** klicken und zu der Datei navigieren. Die Anwendung wird in XenMobile hochgeladen.
- Falls gewünscht, können Sie die App-Details und Richtlinieneinstellungen für die Plattform ändern.
- Konfigurieren Sie, falls gewünscht, Bereitstellungsregeln (siehe Schritt 7) und Worx Store-Konfigurationen (siehe Schritt 8).

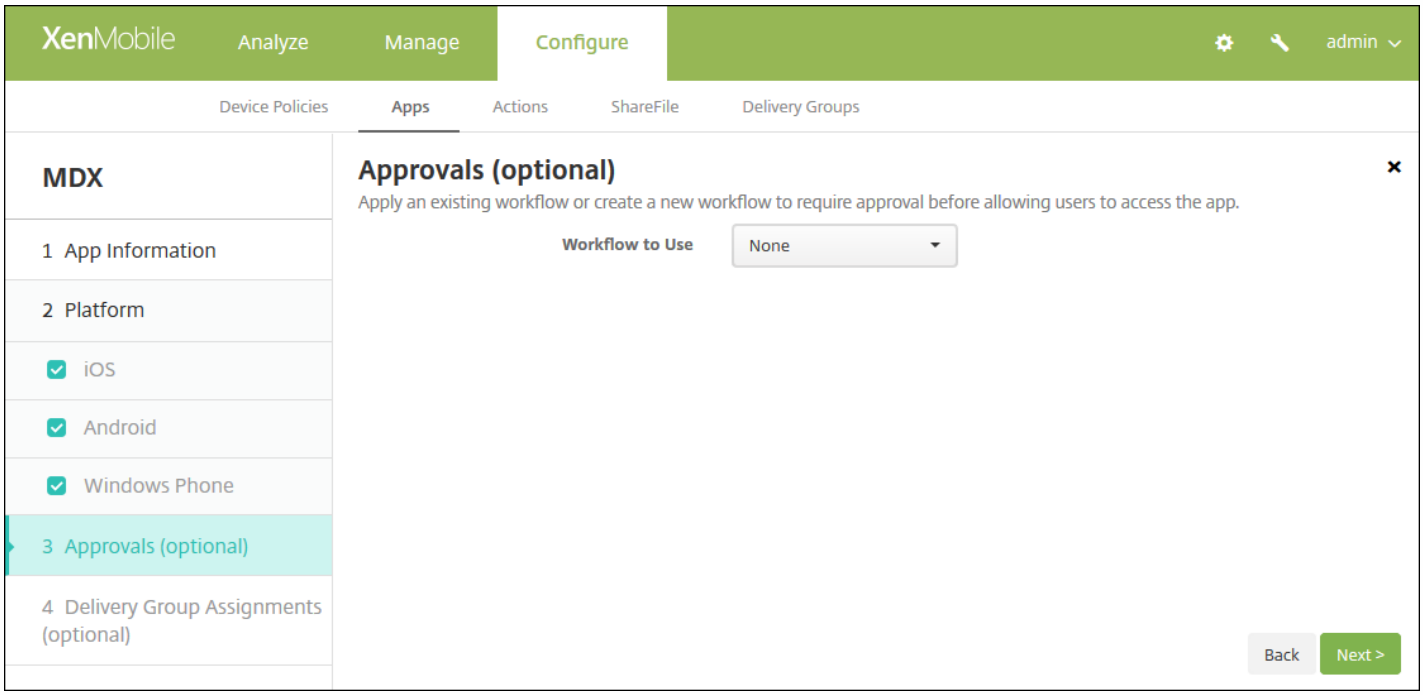
9. Erweitern Sie **Worx Store-Konfiguration**.



Sie können optional FAQ oder Screenshots für die App zur Anzeige im Worx Store hinzufügen. Sie können außerdem festlegen, ob Benutzer die App bewerten oder kommentieren können.

- Konfigurieren Sie folgende Einstellungen:
  - **App FAQ**: Fügen Sie häufig gestellte Fragen und Antworten für die App hinzu.
  - **App-Screenshots**: Fügen Sie Screenshots zur Klassifizierung der App im Worx Store hinzu. Die hochgeladene Grafikdatei muss das Format PNG haben. Sie können keine GIF- oder JPEG-Bilder hochladen.
  - **App-Bewertungen zulassen**: Wählen Sie aus, ob eine Bewertung der App durch die Benutzer zugelassen werden soll. Die Standardeinstellung ist **EIN**.
  - **App-Kommentare zulassen**: Wählen Sie aus, ob eine Kommentierung der App durch die Benutzer zugelassen werden soll. Die Standardeinstellung ist **EIN**.

10. Klicken Sie auf **Weiter**. Die Seite **Genehmigungen** wird angezeigt.



11. Wenn für das Erstellen von Benutzerkonten eine Genehmigung erforderlich ist, verwenden Sie Workflows. Wenn Sie keine Genehmigungsworkflows einrichten müssen, fahren Sie mit Schritt 12 fort.

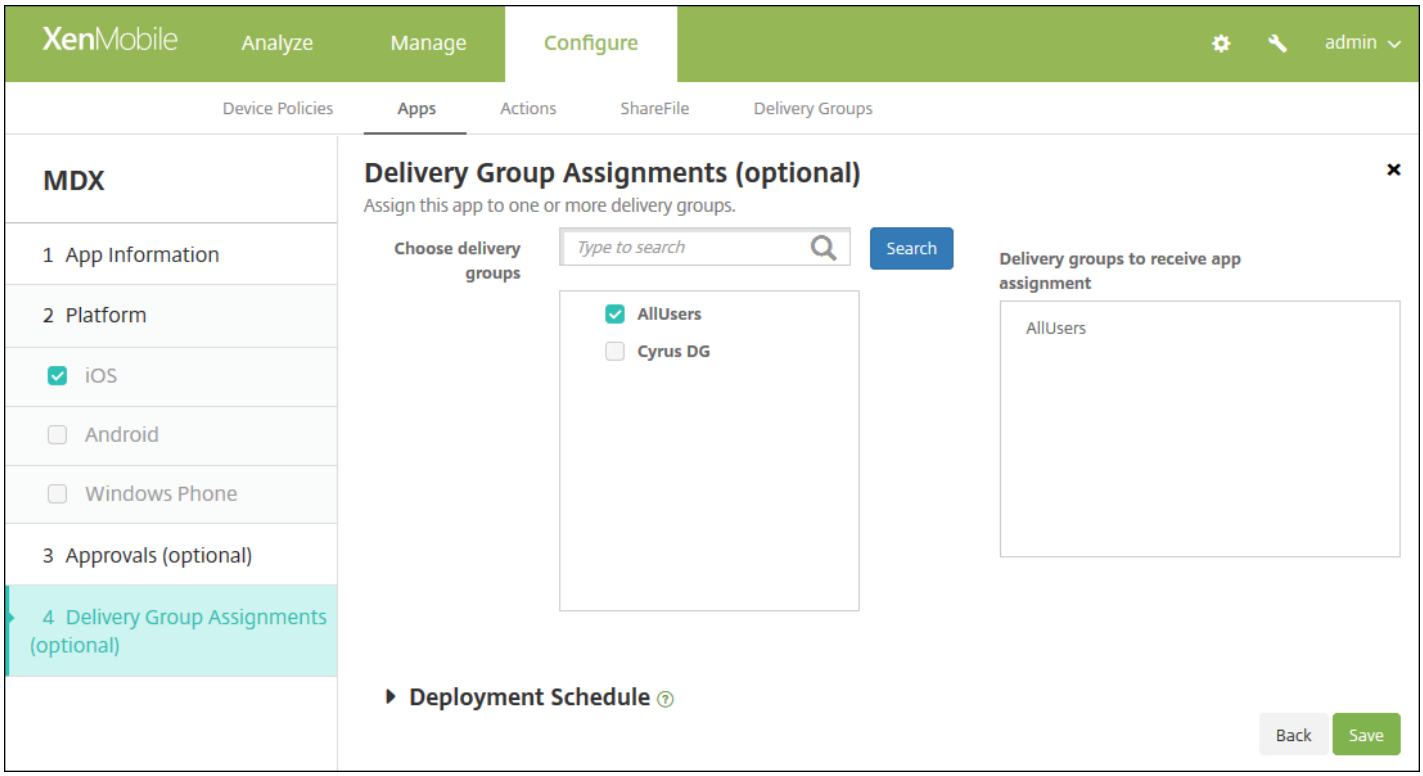
Konfigurieren Sie folgende Einstellung, wenn Sie einen Workflow erstellen oder zuweisen müssen:

- **Verwendete Workflows**: Klicken Sie in der Liste auf einen Workflow oder klicken Sie auf **Neuen Workflow erstellen**. Der Standardwert ist "Ohne".
- Wenn Sie **Neuen Workflow erstellen** ausgewählt haben, konfigurieren Sie die folgenden Einstellungen:
  - **Name**: Geben Sie einen aussagekräftigen Namen für den Workflow ein.
  - **Beschreibung**: Geben Sie optional eine Beschreibung für den Workflow ein.
  - **Vorlagen für E-Mail-Genehmigung**: Wählen Sie die E-Mail-Genehmigungsvorlage aus, die zugewiesen werden soll. Wenn Sie auf das Augensymbol rechts neben dem Feld klicken, wird ein Dialogfeld zur Vorschau der ausgewählten Vorlage angezeigt.
  - **Ebenen für Managergenehmigung**: Wählen Sie in der Liste die Anzahl der Managergenehmigungsebenen für den Workflow aus. Der Standardwert ist **1 Ebene**. Mögliche Optionen:

- Nicht erforderlich
- 1 Ebene
- 2 Ebenen
- 3 Ebenen

- **Active Directory-Domäne wählen**: Wählen Sie in der Liste die für den Workflow zu verwendende Active Directory-Domäne aus.
- **Weitere erforderliche Freigabeberechtigte suchen**: Geben Sie den Namen der zusätzlich erforderlichen Person in das Suchfeld ein und klicken Sie dann auf **Suchen**. Für die Namen wird Active Directory verwendet.
- 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 **Ausgewählte zusätzliche erforderliche Freigabeberechtigte** angezeigt.
- Zum Entfernen einer Person aus der Liste "Ausgewählte zusätzliche erforderliche Freigabeberechtigte" führen Sie einen der folgenden Schritte aus:
  - Klicken Sie auf **Suchen**, 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 **Suchen**, um das Suchergebnis einzuschränken.
  - Die Namen der Personen in der Liste **Ausgewählte zusätzliche erforderliche Freigabeberechtigte** sind im Suchergebnis mit einem Häkchen gekennzeichnet. Navigieren Sie durch die Liste und deaktivieren Sie die Kontrollkästchen aller Personen, die Sie entfernen möchten.

12. Klicken Sie auf **Weiter**. Die Seite **Zuweisungen für Bereitstellungsgruppen** wird angezeigt.



13. Machen Sie neben **Bereitstellungsgruppen wählen** eine Eingabe, um eine Bereitstellungsgruppe zu suchen, oder wählen Sie in der Liste eine oder mehrere Bereitstellungsgruppen für die Zuweisung aus. Diese ausgewählten Gruppen werden in der Liste **Bereitstellungsgruppen für App-Zuweisung** angezeigt.

14. Erweitern Sie **Bereitstellungszeitplan** und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben "Bereitstellen für immer aktive Verbindungen" auf EIN oder AUS. Die Standardeinstellung ist AUS.

Hinweis:

- Diese Option gilt, wenn Sie unter **Einstellungen > Servereigenschaften** den Schlüssel für die Bereitstellung im Hintergrund konfiguriert haben. Die Option "immer aktiv" ist für iOS-Geräte nicht verfügbar.
- 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.

15. Klicken Sie auf **Speichern**. Die Seite **Apps** wird angezeigt.

16. Wenn Sie die App in Schritt 2 deaktiviert haben, führen Sie folgende Schritte aus:

- Klicken Sie in der Apps-Tabelle auf die App, die Sie aktualisiert haben, und klicken Sie in dem nun angezeigten Menü auf **Aktivieren**.
- Klicken Sie in dem daraufhin angezeigten Dialogfeld auf **Aktivieren**. Die Benutzer können jetzt auf die App zugreifen und erhalten eine Benachrichtigung mit der Aufforderung, die App zu aktualisieren.

Aktivieren von Microsoft Office 365-Apps

Aug 22, 2016

Sie können den MDX-Container öffnen, um WorxMail, WorxWeb und ShareFile die Übertragung von Daten und Dokumenten an Microsoft Office 365-Apps zu ermöglichen. Weitere Informationen finden Sie unter Aktivieren der Interaktion von Office 365 mit WorxMail, WorxWeb und ShareFile.

MDX App-Richtlinien auf einen Blick

Jul 28, 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.

Konfigurieren von XenMobile und der ShareFile-App für Single Sign-On mit SAML

Oct 13, 2016

Sie können XenMobile und ShareFile so konfigurieren, dass diese mit Security Assertion Markup Language (SAML) Single Sign-On-Zugriff (SSO) für mobile ShareFile-Apps, die mit dem MDX Toolkit umschlossen wurden, sowie für nicht umschlossene ShareFile-Clients (z. B. Website, Outlook-Plug-In oder Synchronisierungsclients) bereitstellen.

- **Umschlossene ShareFile-Apps**: Benutzer, die sich bei ShareFile über die mobile ShareFile-App anmelden, werden zur Benutzerauthentifizierung und zum Abrufen eines SAML-Tokens an Worx Home weitergeleitet. Nach einer erfolgreichen Authentifizierung sendet die mobile ShareFile-App das SAML-Token an ShareFile. Nach der ersten Anmeldung können Benutzer über SSO auf die mobile ShareFile-App zugreifen und Dokumente aus ShareFile an WorxMail-E-Mails anhängen, ohne sich jedes Mal erneut anmelden zu müssen.
- **Nicht umschlossene ShareFile-Clients**: Benutzer, die sich bei ShareFile über einen Webbrowser oder einen anderen ShareFile-Client anmelden, werden zur Benutzerauthentifizierung und zum Abrufen eines SAML-Tokens an XenMobile weitergeleitet. Nach einer erfolgreichen Authentifizierung wird das SAML-Token an ShareFile gesendet. Nach der ersten Anmeldung können Benutzer auf ShareFile-Clients über SSO ohne erneute Anmeldung zugreifen.

Ein detailliertes Architekturdiagramm finden Sie im Artikel Reference Architecture for On-Premises Deployments in der XenMobile-Bereitstellungsdokumentation.

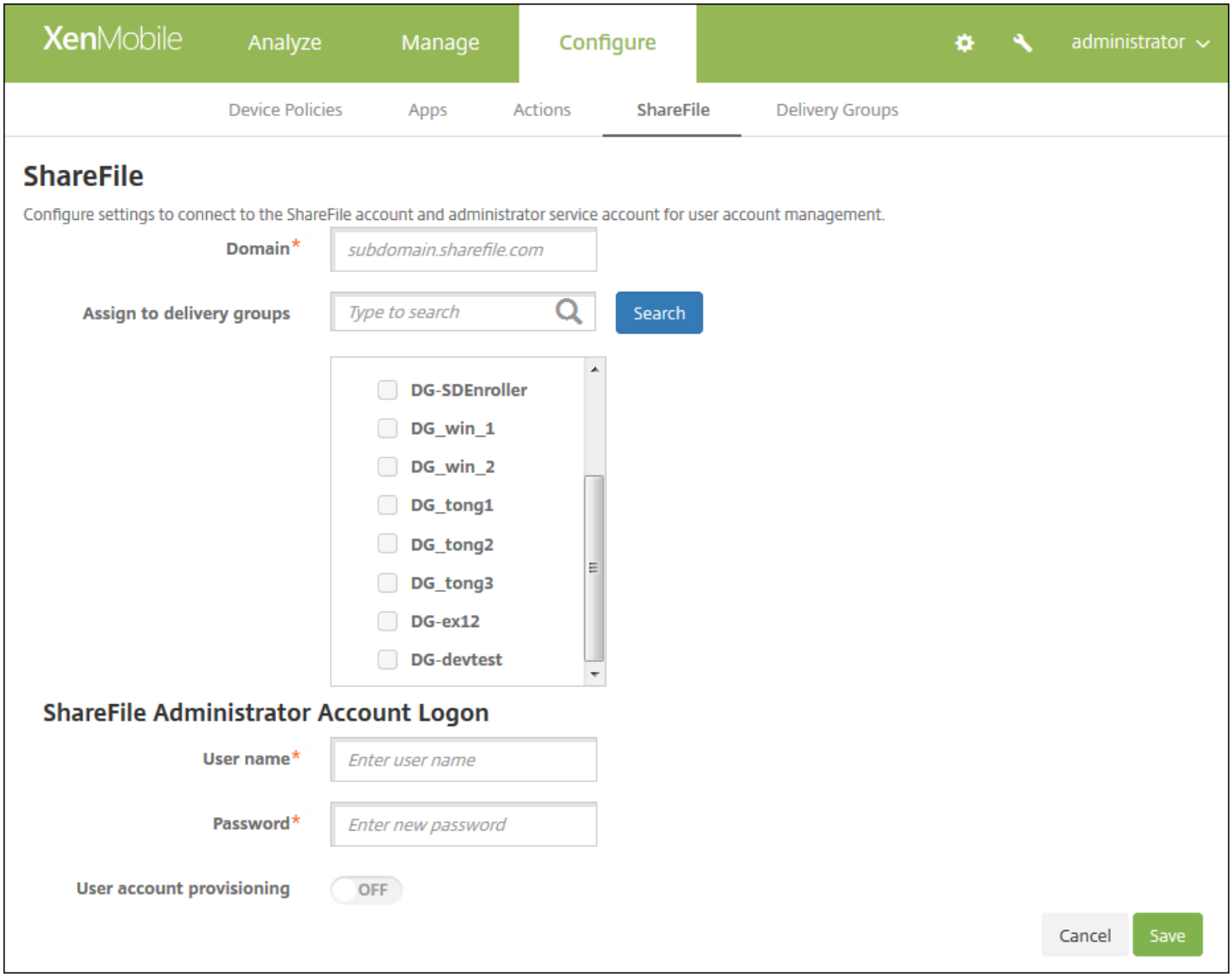
Damit Sie Single Sign-On für XenMobile und ShareFile-Apps konfigurieren können, müssen die folgenden Voraussetzungen erfüllt sein:

- MDX Toolkit Version 9.0.4 oder höher (für mobile ShareFile-Apps)
- Erforderliche mobile ShareFile-Apps:
  - ShareFile für iPhone Version 3.0.x
  - ShareFile für iPad Version 2.2.x
  - ShareFile für Android Version 3.2.x
- Worx Home 9.0 (für ShareFile Mobile-Apps): Installieren Sie die benötigte iOS- bzw. Android-Version.
- ShareFile-Administratorkonto

Stellen Sie sicher, dass XenMobile und ShareFile eine Verbindung herstellen können.

Vor der Einrichtung von SAML für ShareFile geben Sie die ShareFile-Zugriffsinformationen wie folgt an:

1. Klicken Sie in der XenMobile-Webkonsole auf **Konfigurieren > ShareFile**. Die Seite zur ShareFile-Konfiguration wird angezeigt.



2. Konfigurieren Sie die folgenden Einstellungen:

- **Domäne**: Geben Sie den Namen Ihrer ShareFile-Unterdomäne an, z. B. example.sharefile.com.
- **Bereitstellungsgruppen wählen**: Wählen Sie die Bereitstellungsgruppen aus (bzw. suchen Sie sie), für die Sie die Verwendung von SSO mit ShareFile aktivieren möchten.
- **ShareFile-Administratorkonto**
  - **Benutzername**: Geben Sie den Namen des ShareFile-Administrators ein. Dieses Benutzerkonto muss über Administratorrechte verfügen.
  - **Kennwort** Geben Sie das Kennwort des ShareFile-Administrators ein.
  - **Benutzerkontoprovisioning**: Aktivieren Sie diese Option, wenn Sie das Benutzerprovisioning in XenMobile aktivieren möchten. Wenn Sie stattdessen das ShareFile User Management Tool verwenden möchten, lassen Sie die Option deaktiviert.

    Hinweis: Enthalten die ausgewählten Rollen einen Benutzer ohne ShareFile-Konto, wird in XenMobile automatisch ein ShareFile-Konto für diesen Benutzer bereitgestellt, wenn Sie "Benutzerkontoprovisioning" aktivieren. Citrix empfiehlt die Verwendung einer Rolle mit wenigen Mitgliedern zum Testen der Konfiguration. So wird eine potenziell große Zahl von Benutzern ohne ShareFile-Konto vermieden.

3. Klicken Sie auf **Speichern**.

Die folgenden Schritte gelten für iOS- und Android-Apps und -Geräte.

1. Umschließen Sie die mobile ShareFile-App mit dem MDX Toolkit. Informationen hierzu finden Sie unter Umschließen von Apps mit dem MDX Toolkit.

2. Laden Sie in der XenMobile-Konsole die umschlossene mobile ShareFile-App in XenMobile hoch. Informationen zum Hochladen von MDX-Apps finden Sie unter Hinzufügen von MDX-Apps zu XenMobile.

3. Überprüfen Sie die SAML-Einstellungen, indem Sie sich bei ShareFile mit den Anmeldeinformationen des Administrators, die Sie beim Konfigurieren des ShareFile-Zugriffs festgelegt haben, anmelden.

4. Vergewissern Sie sich, dass ShareFile und XenMobile für dieselbe Zeitzone konfiguriert sind.

Hinweis: Stellen Sie sicher, dass in XenMobile die Uhrzeit der konfigurierten Zeitzone angezeigt wird. Wenn nicht, kann das SSO fehlschlagen.

Überprüfen der mobilen ShareFile-App

1. Falls noch nicht geschehen, installieren und konfigurieren Sie Worx Home auf dem Benutzergerät.

2. Laden Sie die mobile ShareFile-App aus dem Worx Store herunter und installieren Sie sie.

3. Starten Sie die mobile ShareFile-App. ShareFile wird ohne Anforderung von Benutzernamen und Kennwort gestartet.

Überprüfung über WorxMail

1. Falls noch nicht geschehen, installieren und konfigurieren Sie Worx Home auf dem Benutzergerät.

2. Laden Sie WorxMail aus dem Worx Store herunter, installieren und konfigurieren Sie es.

3. Öffnen Sie ein neues E-Mail-Formular und tippen Sie auf **Von ShareFile anfügen**. Die zum Anfügen verfügbaren Dateien werden ohne Anforderung von Benutzernamen und Kennwort angezeigt.

Wenn Sie den Zugriff für nicht umschlossene ShareFile-Clients (z. B. Website, Outlook-Plug-In oder Synchronisierungsclients) konfigurieren möchten, müssen Sie NetScaler Gateway folgendermaßen konfigurieren, damit es die Verwendung von XenMobile als SAML-Identitätsanbieter unterstützt:

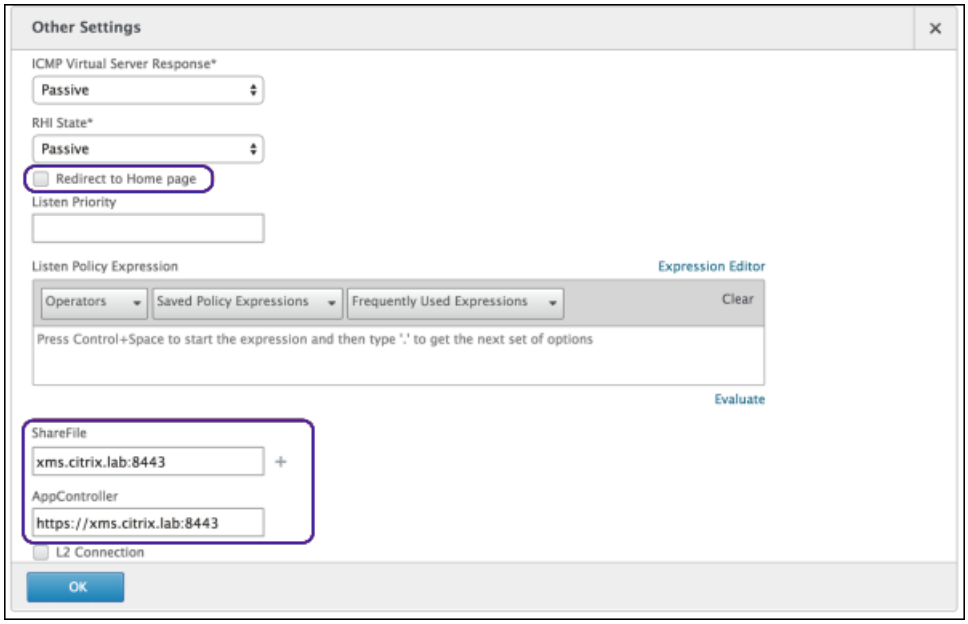
- Deaktivieren Sie die Homepageumleitung.
- Erstellen Sie eine ShareFile-Sitzungsrichtlinie und ein Profil.
- Konfigurieren Sie Richtlinien auf dem virtuellen NetScaler Gateway-Server.

Deaktivieren der Homepageumleitung

Sie müssen die Standardverarbeitung von Anforderungen, die über den /cginfra-Pfad eingehen, deaktivieren, damit den Benutzern die ursprüngliche angeforderte interne URL anstelle der konfigurierten Homepage angezeigt wird.

1. Bearbeiten Sie die Einstellungen für den virtuellen NetScaler Gateway-Server, der für XenMobile-Anmeldungen verwendet

wird. Navigieren Sie in NetScaler 10.5 zu **Other Settings** und deaktivieren Sie das Kontrollkästchen **Redirect to Home Page**.



2. Geben Sie unter **ShareFile** den internen Namen des XenMobile-Servers und die Portnummer ein.

3. Geben Sie unter **AppController** die XenMobile-URL ein.

Mit dieser Konfiguration werden Anforderungen an die über den /cginfra-Pfad eingegebene URL genehmigt.

Erstellen einer ShareFile-Sitzungsrichtlinie und eines Anforderungsprofils

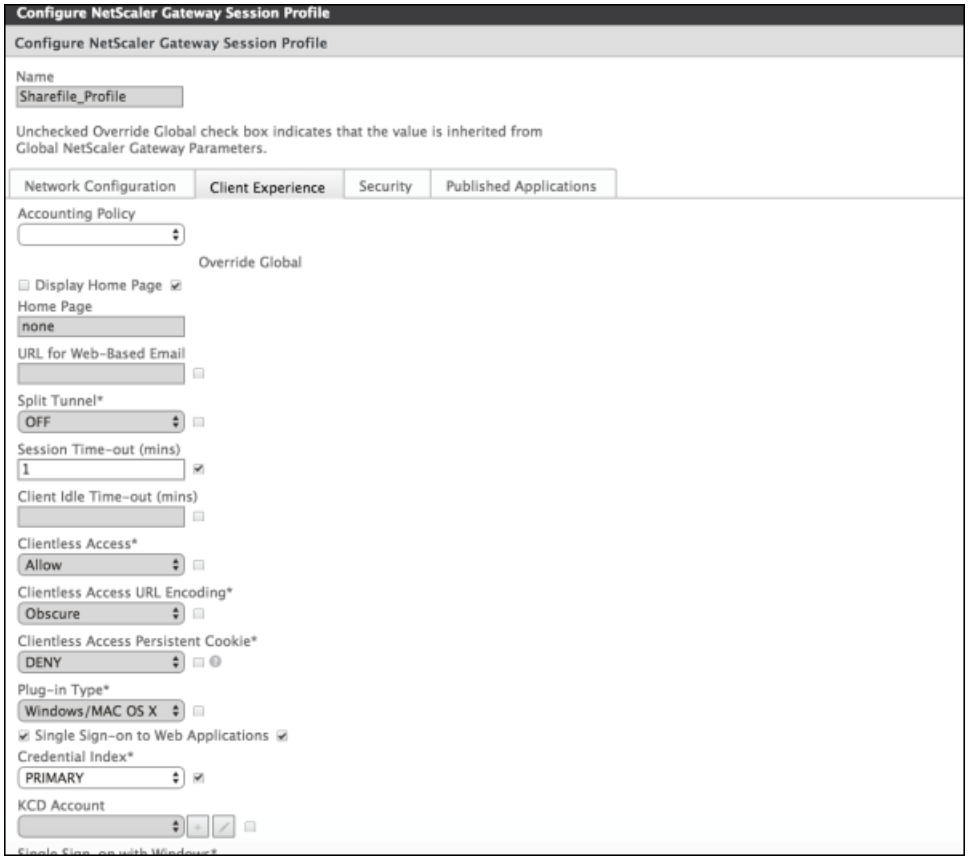
Konfigurieren Sie die folgenden Einstellungen zum Erstellen einer ShareFile-Sitzungsrichtlinie und eines Anforderungsprofils:

1. Klicken Sie im Konfigurationsprogramm für NetScaler Gateway im linken Navigationsbereich auf **NetScaler Gateway > Policies > Session**.

2. Erstellen Sie eine neue Sitzungsrichtlinie. Klicken Sie auf der Registerkarte **Policies** auf **Add**.

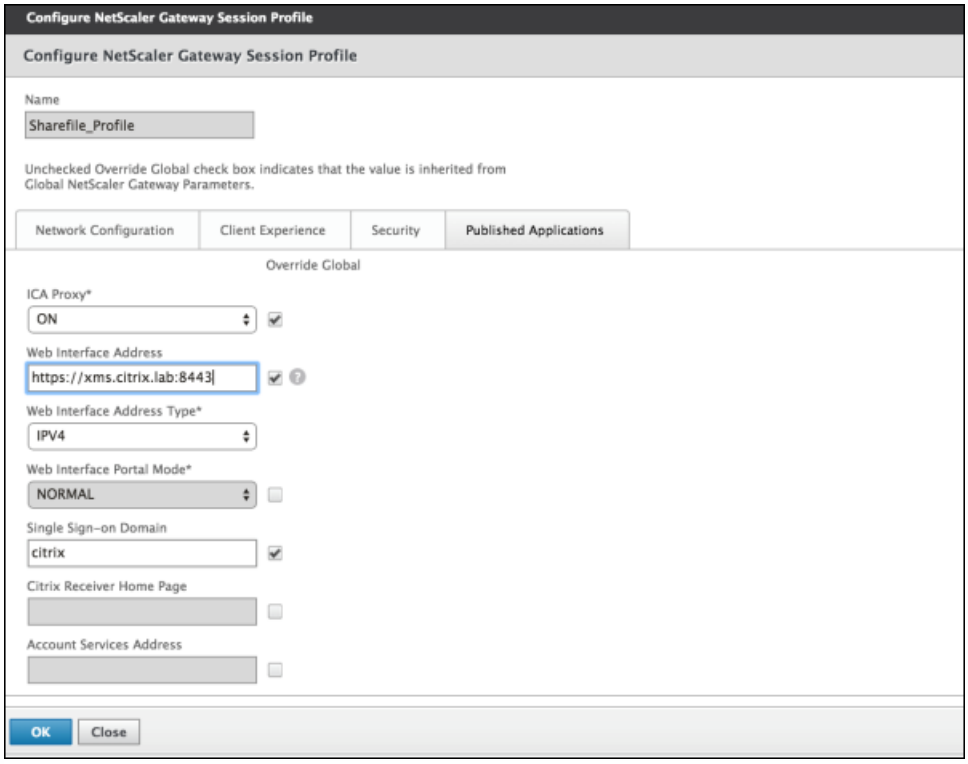
3. Geben Sie im Feld **Name** den Ausdruck **ShareFile_Policy** ein.

4. Erstellen Sie eine neue Aktion durch Klicken auf die +-Schaltfläche. Die Seite **Create NetScaler Gateway Session Profile** wird angezeigt.



Konfigurieren Sie folgende Einstellungen:

- **Name**: Geben Sie "ShareFile_Profile" ein.
- Klicken Sie auf die Registerkarte **Client Experience** und konfigurieren Sie die folgenden Einstellungen:
  - **Home Page**: Geben Sie "none" ein.
  - **Session Time-out (mins)**: Geben Sie "1" ein.
  - **Single Sign-on to Web Applications**: Wählen Sie diese Einstellung.
  - **Credential Index**: Klicken Sie in der Liste auf "PRIMARY".
- Klicken Sie auf die Registerkarte **Published Applications**.



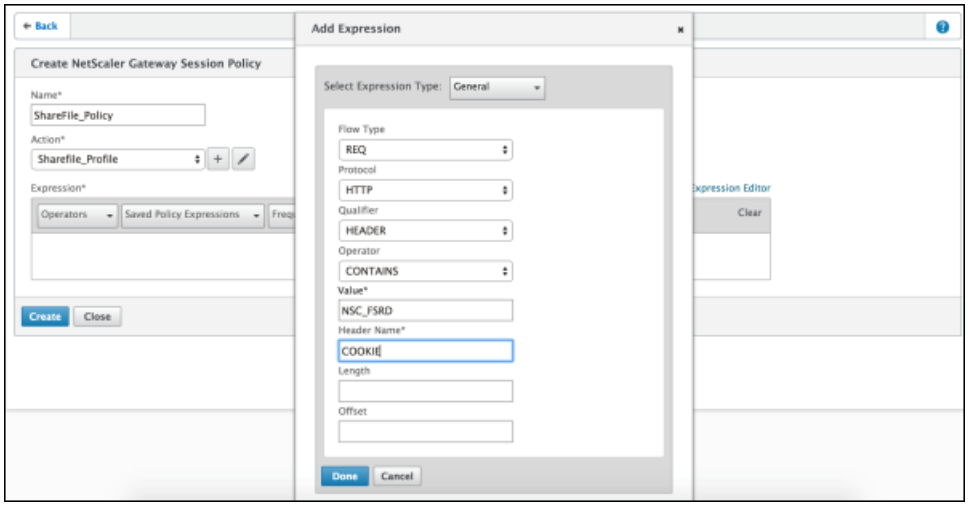
Konfigurieren Sie folgende Einstellungen:

- o **ICA Proxy**: Klicken Sie in der Liste auf **ON** aus.
- o **Web Interface Address**: Geben Sie die URL des XenMobile-Servers ein.
- o **Single Sign-on Domain**: Geben Sie den Namen Ihrer Active Directory-Domäne ein.

  Hinweis: Beim Konfigurieren des NetScaler Gateway-Sitzungsprofils muss das Domänensuffix für **Single Sign-on Domain** mit dem in LDAP festgelegten XenMobile-Domänenalias übereinstimmen.

5. Klicken Sie auf **Create**, um das Sitzungsprofil zu definieren.

6. Klicken Sie auf **Expression Editor**.



Konfigurieren Sie folgende Einstellungen:

- **Value**: Geben Sie "NSC_FSRD" ein.
- **Header Name**: Geben Sie "COOKIE" ein.
- Klicken Sie auf **Fertig**.

7. Klicken Sie auf **Create** und dann auf **Close**.

Konfigurieren von Richtlinien auf dem virtuellen NetScaler Gateway-Server

Konfigurieren Sie die folgenden Einstellungen auf dem virtuellen NetScaler Gateway-Server.

1. Klicken Sie im Konfigurationsprogramm für NetScaler Gateway im linken Navigationsbereich auf **NetScaler Gateway** > **Virtual Servers**.

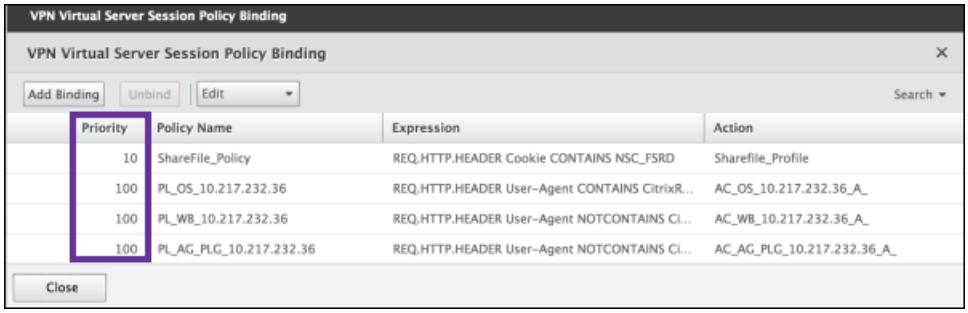
2. Klicken Sie im Bereich **Details** auf den virtuellen NetScaler Gateway-Server.

3. Klicken Sie auf **Edit**.

4. Klicken Sie auf **Configured policies** > **Session policies** und dann auf **Add binding**.

5. Wählen Sie **ShareFile_Policy** aus.

6. Bearbeiten Sie die automatisch generierte Prioritätszahl unter **Priority** für die ausgewählte Richtlinie so, dass sie die höchste Priorität (die niedrigste Zahl) vor allen anderen aufgeführten Richtlinien hat (siehe folgende Abbildung).



7. Klicken Sie auf **Done** und speichern Sie die ausgeführte NetScaler-Konfiguration.

Ermitteln Sie anhand der folgenden Schritte den internen App-Namen für die ShareFile-Konfiguration.

1. Melden Sie sich bei dem Verwaltungstool für XenMobile unter Verwendung der URL **https://:4443/OCA/admin/** an. Geben Sie dabei "OCA" unbedingt in Großbuchstaben ein.

2. Klicken Sie in der Liste **View** auf **Configuration**.

3. Klicken Sie auf **Applications > Applications** und notieren Sie den unter **Application Name** für die App angezeigten Namen mit dem unter **Display Name** angezeigten Anzeigenamen "ShareFile".

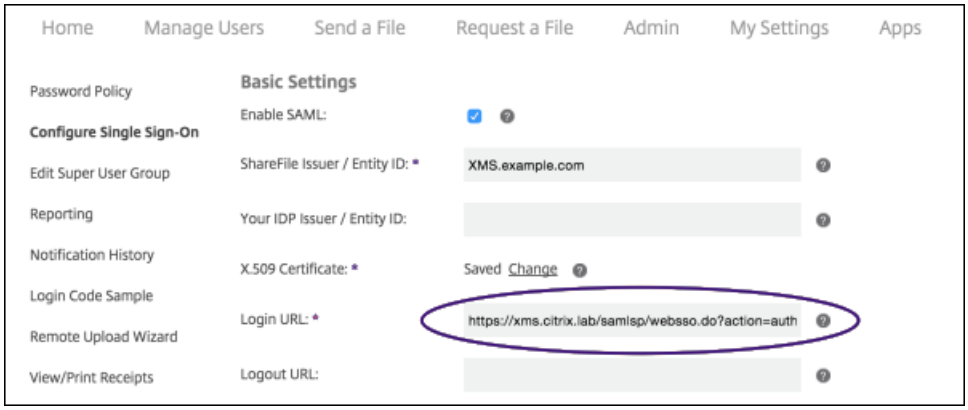
Ändern der SSO-Einstellungen für ShareFile.com

1. Melden Sie sich bei Ihrem ShareFile-Konto (https://.sharefile.com) als ShareFile-Administrator an.

2. Klicken Sie im ShareFile-Webinterface auf **Admin** und wählen Sie **Configure Single Sign-on** aus.

3. Bearbeiten Sie den Eintrag im Feld **Login URL** wie folgt:

Der Eintrag im Feld **Login URL** sollte in etwa so aussehen: https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1.



- Geben Sie den externen FQDN des virtuellen NetScaler Gateway-Servers plus "/cginfra/https/" vor dem FQDN des XenMobile-Servers und hinter dem FQDN des XenMobile-Servers "8443" ein.

  Die URL sollte nun in etwa so aussehen:
  https://**nsgateway.acme.com/cginfra/https**/xms.citrix.lab:**8443**/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1

- Ändern Sie den Parameter **&app=ShareFile_SAML_SP** auf den in Schritt 3 beim Konfigurieren von SAML für ShareFile-Apps ohne MDX festgelegten internen ShareFile-Anwendungsnamen. Der interne Name lautet standardmäßig **ShareFile_SAML**. Jedes Mal, wenn Sie die Konfiguration ändern, wird jedoch eine Zahl an den internen Namen angehängt (ShareFile_SAML_2, ShareFile_SAML_3 usw.).

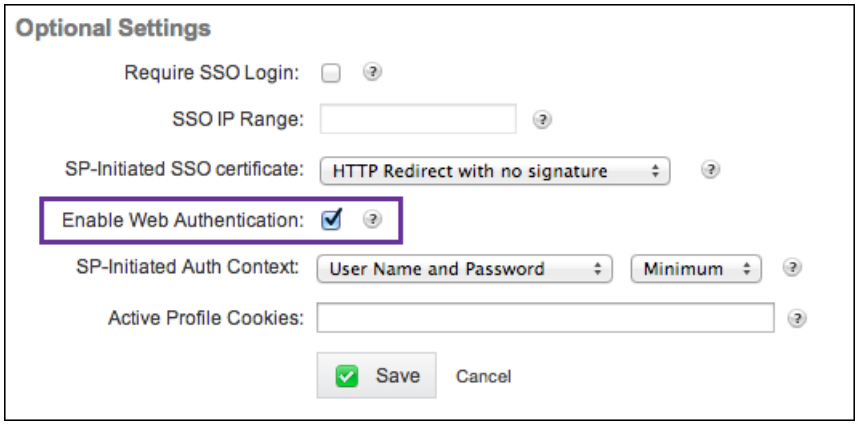
  Die URL sollte nun in etwa so aussehen:
  https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser**&app=ShareFile_SAML**&reqtype=1

- Hängen Sie "&nssso=true" an das Ende der URL an.

  Die geänderte URL sollte nun in etwa so aussehen::
  https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1**&nssso=true**.

  Wichtig: Jedes Mal, wenn Sie die ShareFile-App bearbeiten oder neu erstellen oder die ShareFile-Einstellungen in der XenMobile-Konsole ändern, wird an den internen Anwendungsnamen eine neue Zahl angehängt. Sie müssen daher die Anmelde-URL für die ShareFile-Website dem neuen Anwendungsnamen entsprechend ändern.

4. Aktivieren Sie unter **Optional Settings** das Kontrollkästchen **Enable Web Authentication**.



Überprüfen Sie die Konfiguration wie nachfolgend beschrieben.

1. Rufen Sie im Browser https://sharefile.com/saml/login auf.

Sie werden zum NetScaler Gateway-Anmeldungsformular umgeleitet. Erfolgt keine Umleitung, überprüfen Sie die oben aufgeführten Konfigurationseinstellungen.

2. Geben Sie die Anmeldeinformationen ein, die Sie für die NetScaler Gateway- bzw. XenMobile-Umgebung konfiguriert haben.

Die ShareFile-Ordner auf .sharefile.com werden angezeigt. Wenn keine ShareFile-Ordner angezeigt werden, prüfen Sie, ob Sie die richtigen Anmeldeinformationen eingegeben haben.

Automatisierte Aktionen

Oct 13, 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 **Konfigurieren** > **Aktionen**. Die Seite **Aktionen** wird angezeigt.

2. Führen Sie auf der Seite **Aktionen** einen der folgenden Schritte aus:

- Klicken Sie auf **Hinzufügen**, 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.

3. Die Seite **Aktionsinformationen** wird angezeigt.

4. Konfigurieren Sie auf der Seite **Aktionsinformationen** die folgenden Informationen:

- **Name**: Geben Sie einen Namen zur Identifizierung der Aktion ein. Diese Angabe ist erforderlich.
- **Beschreibung**: Geben Sie eine Beschreibung der Aktion ein.

5. Klicken Sie auf **Weiter**. Die Seite **Aktionsdetails** 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.

6. Konfigurieren Sie auf der Seite **Aktionsdetails** die folgenden Informationen:

- Klicken Sie in der Liste **Auslöser** auf den Auslösertyp für die Aktion. Es gibt folgende Auslöser:
  - **Ereignis**: reagiert auf ein festgelegtes Ereignis.
  - **Geräteeigenschaft**: prüft Geräte im MDM-Modus auf ein Attribut und reagiert entsprechend.
  - **Benutzereigenschaft**: reagiert auf ein Benutzerattribut, in der Regel aus Active Directory.
  - **Name der installierten App**: reagiert auf die Installation einer App. Dies gilt nicht im Nur-MAM-Modus. Hierfür muss die App-Bestandsrichtlinie auf dem Gerät aktiviert sein. Die App-Bestandsrichtlinie ist auf allen Plattformen standardmäßig aktiviert. Weitere Informationen finden Sie unter Hinzufügen von App-Bestandsrichtlinien für Geräte.

7. Klicken Sie in der nächsten Liste auf die Reaktion auf den Auslöser.

8. Klicken Sie in der Liste **Aktion** auf die Aktion, die ausgeführt werden soll, wenn das Auslöserkriterium erfüllt wird. Mit Ausnahme von **Benachrichtigung senden** 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. Folgende Aktionen sind verfügbar:

- **Gerät selektiv löschen**: Löschen aller Unternehmensdaten und -Apps von einem Gerät, private Daten und Apps bleiben erhalten.
- **Gerät vollständig löschen**: Löschen aller Daten und Apps von einem Gerät und, sofern vorhanden, dessen Speicherkarten.
- **Gerät widerrufen**: Verhindern der Herstellung einer Verbindung zwischen einem Gerät und XenMobile.
- **App-Sperre**: Verhindern des Zugriffs auf alle Apps auf einem Gerät. Benutzer von Android-Geräten haben überhaupt keinen Zugriff auf XenMobile. Benutzer von iOS-Geräten können sich anmelden, aber sie haben keinen Zugriff auf Apps.
- **App löschen**: Diese Option löscht auf Android-Geräten das XenMobile-Konto von Benutzern. Auf iOS-Geräten wird der Verschlüsselungsschlüssel gelöscht, den Benutzer für den Zugriff auf XenMobile-Features benötigen.
- **Geräte als nicht richtlinientreu markieren**: Das Gerät wird als nicht richtlinientreu markiert.
- **Benachrichtigung senden**: Senden Sie eine Nachricht an den Benutzer.

Bei den restlichen Schritten dieses Verfahrens wird erläutert, wie Sie eine Benachrichtigung senden.

9. 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 Einstellungen 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 Erstellen und Aktualisieren von Benachrichtigungsvorlagen in XenMobile.

Hinweis: Nach Auswahl der Vorlage können Sie eine Vorschau davon anzeigen indem Sie auf "Vorschau für Benachrichtigung" klicken.

10. 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.

11. Vergewissern Sie sich unter **Zusammenfassung**, dass die automatisierte Aktion wie gewünscht konfiguriert wurde.

12. Nach dem Konfigurieren der Aktion können Sie für jede Plattform separat Bereitstellungsregeln festlegen. Führen Sie hierfür Schritt 13 für jede gewünschte Plattform aus.

14. Nach dem Konfigurieren der Bereitstellungsregeln für die Aktion klicken Sie auf **Weiter**. Die Seite **Zuweisung** für Aktionen wird angezeigt, auf der Sie die Aktion Bereitstellungsgruppen bzw. Gruppen zuweisen können. Dieser Schritt ist optional.

15. Machen Sie neben **Bereitstellungsgruppen wählen** 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.

16. Erweitern Sie "Bereitstellungszeitplan" und konfigurieren Sie folgende Einstellungen:

- 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.
- Klicken Sie neben **Bereitstellungszeitplan** auf **Jetzt** oder **Später**. Die Standardeinstellung ist **Jetzt**.
- Wenn Sie auf **Später** klicken, klicken Sie auf das Kalendersymbol und wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- Klicken Sie neben **Bereitstellungsbedingung** auf **Bei jeder Verbindung** oder auf **Nur bei Fehler in der vorherigen Bereitstellung**. Die Standardeinstellung ist **Bei jeder Verbindung**.
- Klicken Sie neben **Bereitstellen für immer aktive Verbindungen** auf **EIN** oder **AUS**. Die Standardeinstellung ist **AUS**. **Hinweis:** Diese Option gilt, wenn Sie unter **Einstellungen** > **Servereigenschaften** 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 **Bereitstellen für immer aktive Verbindungen**, denn diese Option gilt nicht für iOS.

17. Klicken Sie auf **Weiter**. Die Seite **Zusammenfassung** wird angezeigt, auf der Sie die Konfiguration der Aktion überprüfen können.

18. Klicken Sie auf **Speichern**, um die Aktion zu speichern.

Makros in XenMobile

Jul 28, 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:

- loginname (username und domainname)
- username (loginname 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.

XenMobile-Clienteinstellungen

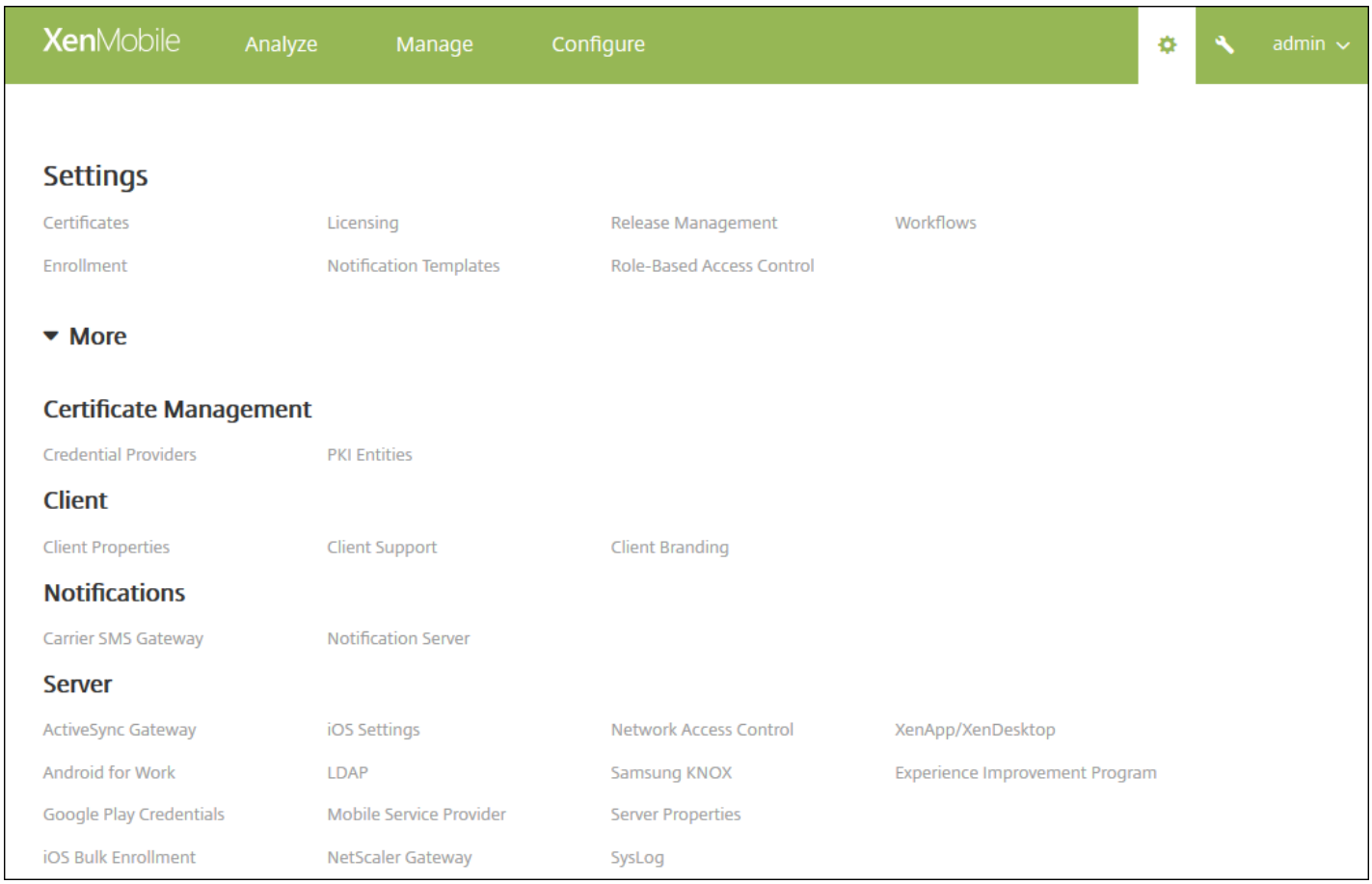
Jul 28, 2016

In der XenMobile-Konsole werden folgende XenMobile-Servereinstellungen konfiguriert:

- Clienteigenschaften
- Clientsupport
- Clientbranding

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

3. Klicken Sie unter **Client** auf die Option, die Sie konfigurieren möchten.



Erstellen von angepasstem Worx Store-Branding für iOS-Geräte

Oct 13, 2016

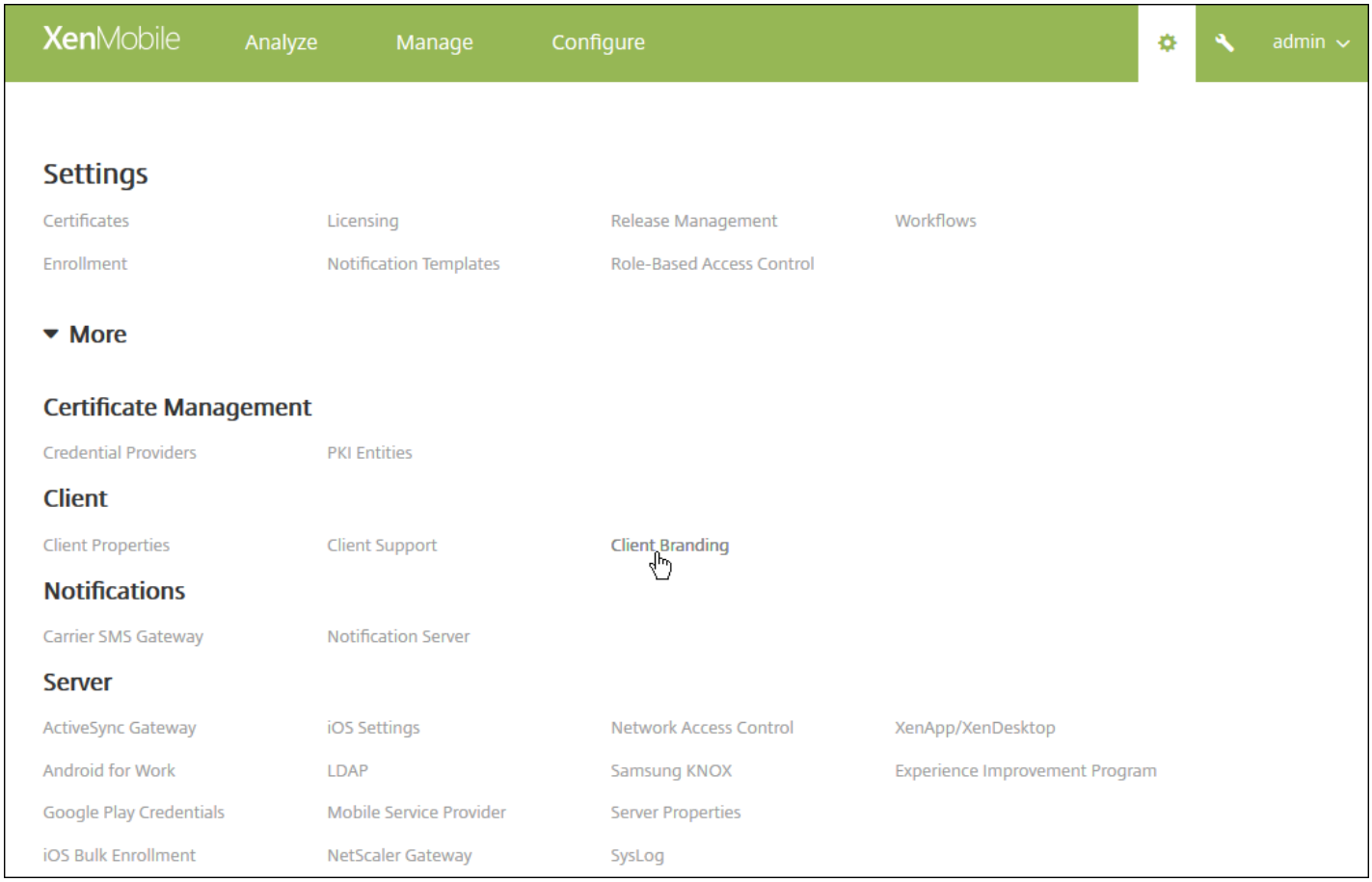
Sie können festlegen, wie Apps im XenMobile angezeigt werden und Secure Hub und dem XenMobile Store für mobile iOS- und Android-Geräte ein Logo hinzufügen.

Hinweis: Stellen Sie zu Beginn des Arbeitsgangs sicher, dass das benutzerdefinierte Bild bereitsteht.

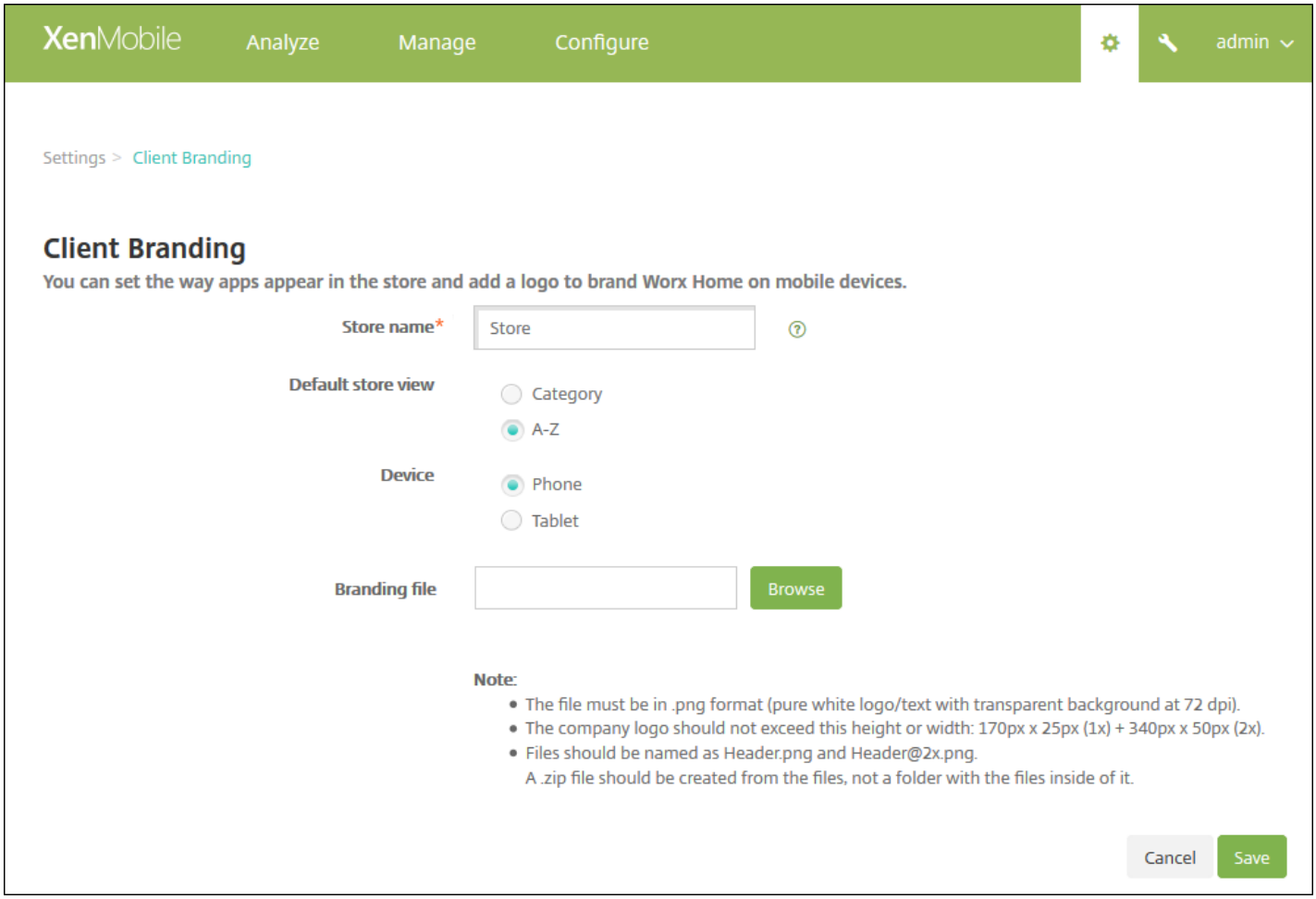
Das benutzerdefinierte Bild muss folgende Anforderungen erfüllen:

- 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 x 25 px (1x) und 340 x 50 px (2x).
- Benennen Sie die Dateien 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 das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.



2. Klicken Sie unter **Client** auf **Clientbranding**. Die Seite **Clientbranding** wird angezeigt.



Konfigurieren Sie die folgenden Einstellungen:

- **Storename**: Der Storename wird mit den Kontoinformationen des Benutzers angezeigt. Das Ändern des Namens ändert auch die URL, die für den Zugriff auf Storedienste verwendet wird. Sie müssen in der Regel den Standardnamen nicht ändern.
- **Standardstoreansicht**: Wählen Sie die Option **Kategorie** oder **A-Z** aus. Die Standardeinstellung ist **A-Z**.
- **Gerät**: Wählen Sie **Telefon** oder **Tablet** aus. Der Standardwert ist **Telefon**.
- **Brandingdatei**: Wählen Sie eine Bilddatei oder eine ZIP-Datei mit Bildern aus, indem Sie auf **Durchsuchen** klicken und zu deren Speicherort navigieren.

3. Klicken Sie auf **Speichern**.

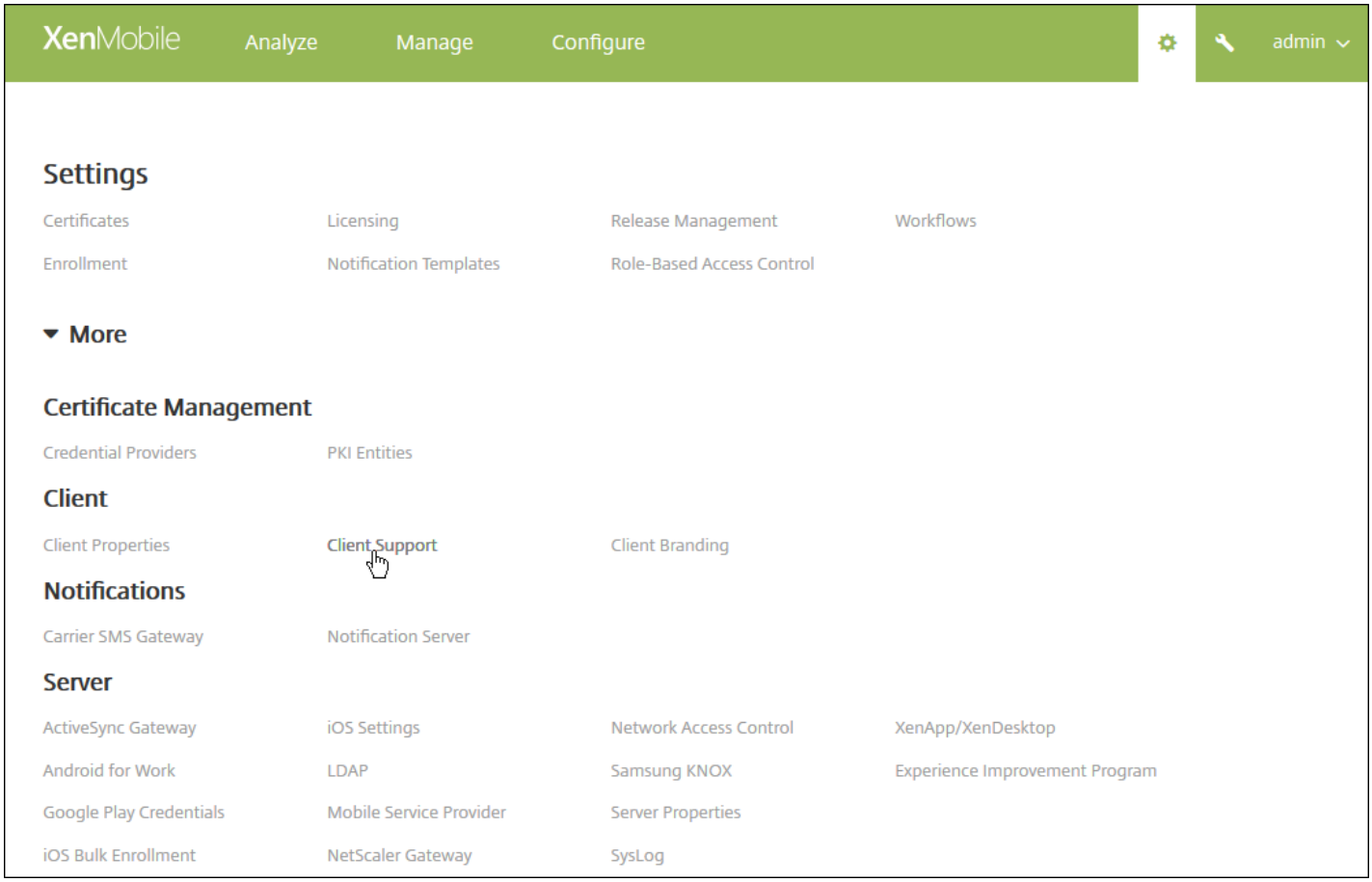
Zum Bereitstellen dieses Pakets auf Geräten müssen Sie ein Bereitstellungspaket erstellen und auf den Geräten der Benutzer bereitstellen.

Erstellen von Supportoptionen für Worx Home und GoToAssist

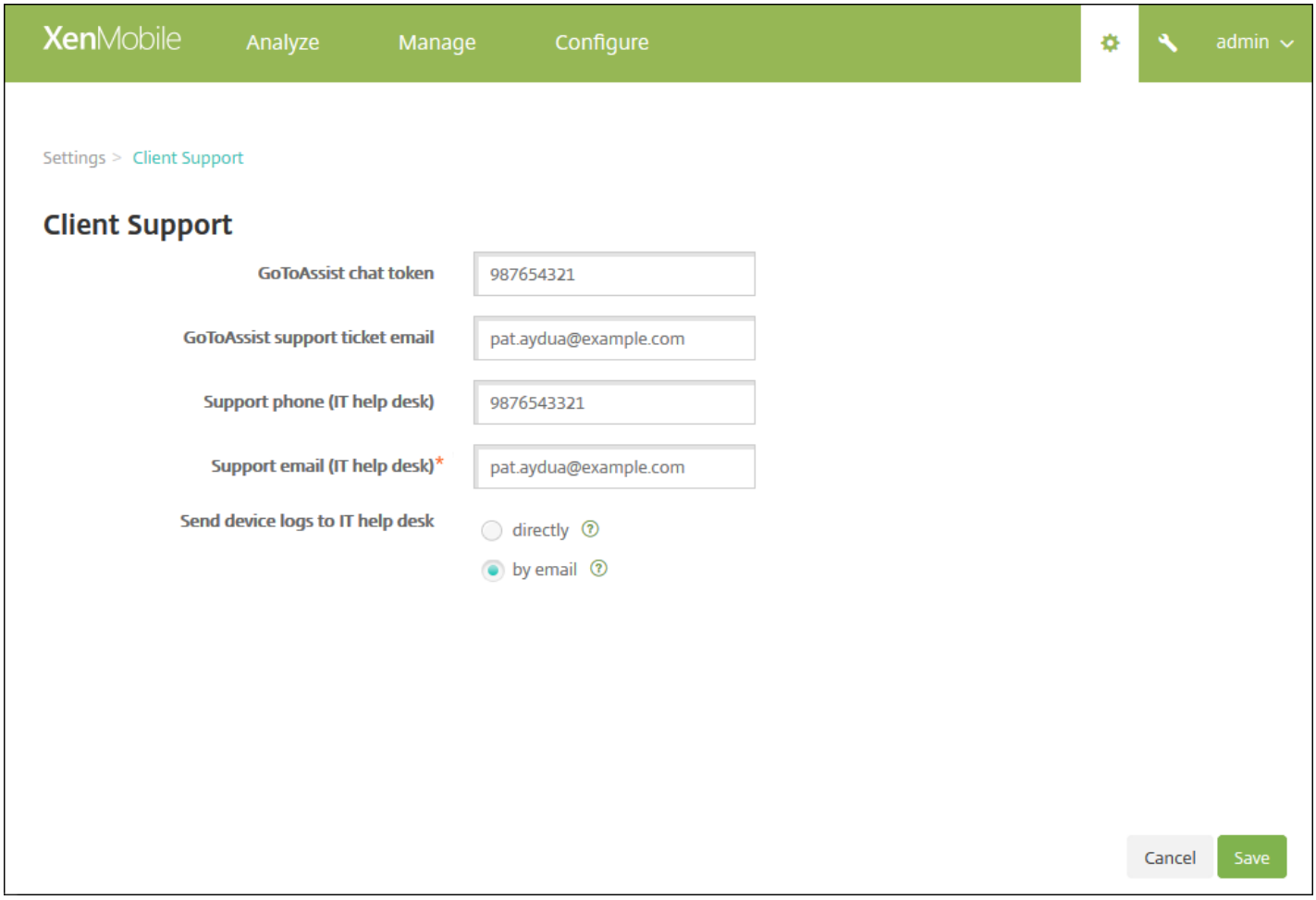
Oct 13, 2016

Sie können den Benutzern verschiedene Möglichkeiten der Kontaktaufnahme mit dem Support mittels E-Mail-Adressen, Telefonnummern und GoToAssist-Token anbieten. Wenn die Benutzer von ihrem Gerät aus Unterstützung anfordern, sehen sie die Optionen, die Sie festgelegt haben.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.



2. Klicken Sie unter **Client** auf **Clientsupport**. Die Seite **Clientsupport** wird angezeigt.



3. Konfigurieren Sie die folgenden Einstellungen:

- **GoToAssist-Chattoken**: Geben Sie das Token ein, das Benutzer zum Herstellen einer GoToAssist-Sitzung erhalten.
- **E-Mail für GoToAssist-Supportticket**: Geben Sie die E-Mail-Adresse zur Verwendung für GoToAssist-Supporttickets ein.
- **Supporttelefon (IT-Helpdesk):** Geben Sie die Telefonnummer des IT-Helpdesks ein.
- **Support-E-Mail (IT-Helpdesk)**: Geben Sie die E-Mail-Adresse des IT-Helpdesks ein.
- **Geräteprotokolle an IT-Helpdesk senden**: Wählen Sie aus, ob Geräteprotokolle direkt oder per E-Mail gesendet werden sollen. Der Standardwert ist **Per E-Mail**.
  - Wenn Sie **Direkt** aktivieren, werden Einstellungen für "Protokolle in ShareFile speichern" angezeigt. Wenn Sie "Protokolle in ShareFile speichern" aktivieren, werden die Protokolle direkt an ShareFile gesendet; ansonsten werden sie an XenMobile und dann per E-Mail an den IT-Helpdesk gesendet. Außerdem wird die Option **E-Mail verwenden, wenn Direktübertragung fehlschlägt** angezeigt. Diese ist standardmäßig aktiviert. Sie können diese Option deaktivieren, wenn Sie nicht möchten, dass Protokolle im Fall eines Problems mit dem Server über die Client-E-Mail gesendet werden. Wenn Sie diese Option deaktivieren und es tritt ein Serverproblem auf, werden keine Protokolle gesendet.
  - Wenn Sie **Per E-Mail** aktivieren, wird immer die Client-E-Mail für den Versand von Protokollen verwendet.

4. Klicken Sie auf **Speichern**.

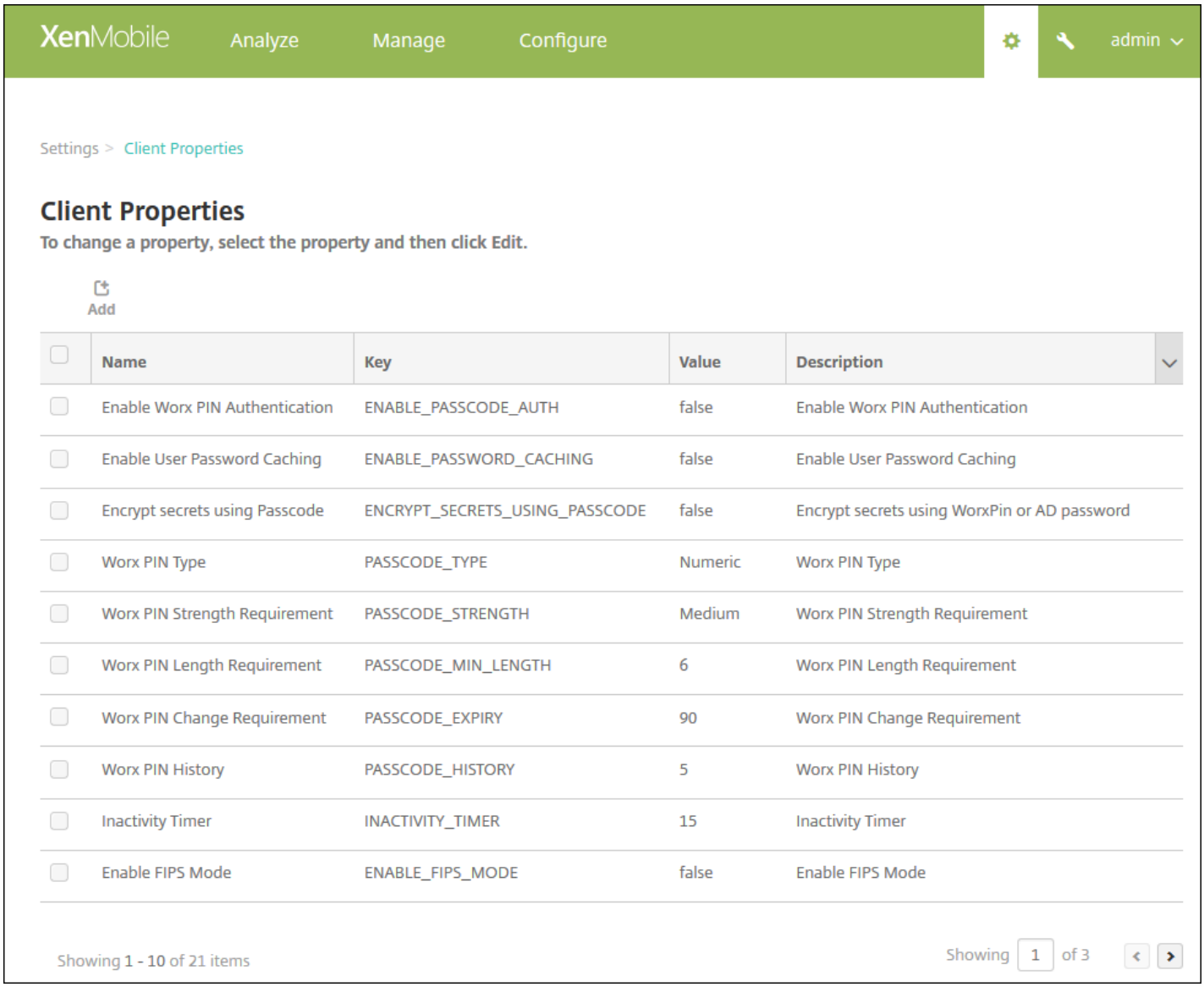
Erstellen, Bearbeiten und Löschen von Clienteigenschaften

Jul 28, 2016

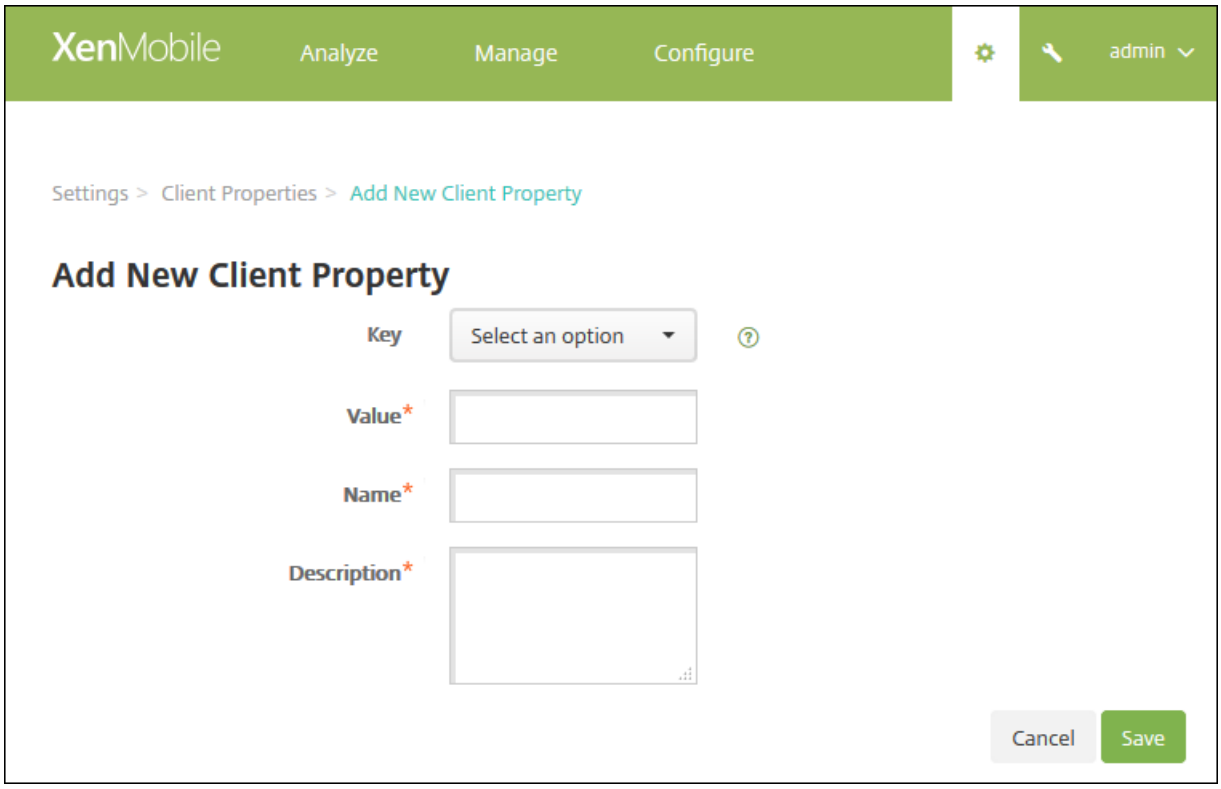
Clienteigenschaften enthalten Informationen, die direkt in Worx Home auf den Geräten der Benutzer bereitgestellt werden. Mit diesen Eigenschaften können Sie erweiterte Einstellungen, z. B. die Worx-PIN, konfigurieren. Clienteigenschaften sind beim Citrix Support erhältlich.

Clienteigenschaften können sich bei jedem neuen Release von Client-Apps, insbesondere Worx Home, ändern. Weitere Informationen zu Clienteigenschaften finden Sie unter Referenz der Clienteigenschaften.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.
2. Klicken Sie unter **Client** auf **Clienteigenschaften**. Die Seite **Clienteigenschaften** wird angezeigt. Auf dieser Seite können Sie Clienteigenschaften hinzufügen, bearbeiten und löschen.



1. Klicken Sie auf **Hinzufügen**. Die Seite **Clienteigenschaft hinzufügen** wird angezeigt.



2. Konfigurieren Sie die folgenden Einstellungen:

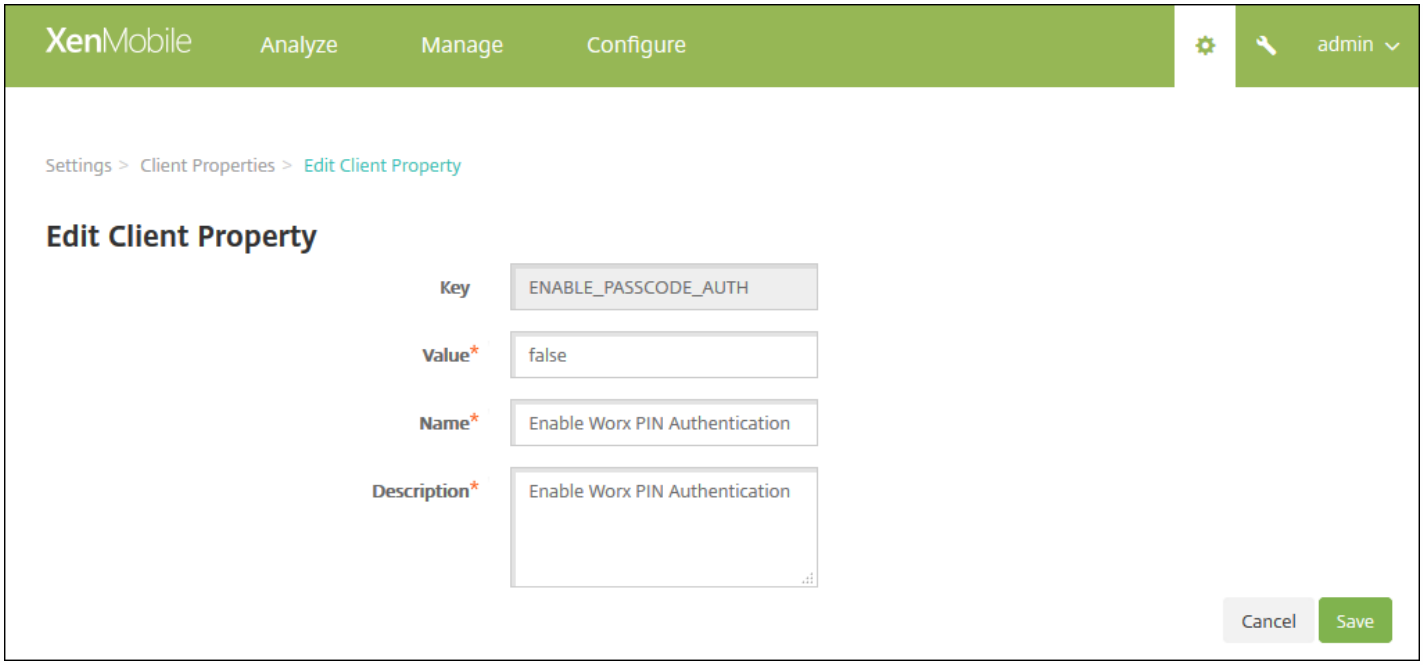
- **Schlüssel**: Klicken Sie in der Liste auf den Eigenschaftsschlüssel, den Sie hinzufügen möchten. **Wichtig:** Wenden Sie sich an den Citrix Support, bevor Sie Änderungen vornehmen, oder fordern Sie einen speziellen Schlüssel an, um eine Änderung auszuführen.
- **Wert**: Geben Sie den Wert der ausgewählten Eigenschaft ein.
- **Name**: Geben Sie einen Namen für die Eigenschaft ein.
- **Beschreibung**: Geben Sie eine Beschreibung für die Eigenschaft ein.

3. Klicken Sie auf **Speichern**.

1. Wählen Sie in der Tabelle **Clienteigenschaften** 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 **Bearbeiten**. Die Seite **Clienteigenschaft bearbeiten** wird angezeigt.



3. Ändern Sie nach Bedarf die folgenden Informationen:

- **Schlüssel**: Sie können dieses Feld nicht ändern.
- **Wert**: Wert der ausgewählten Eigenschaft.
- **Name**: Name der Eigenschaft.
- **Beschreibung**: Beschreibung der Eigenschaft.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um die Clienteigenschaft unverändert zu lassen.

1. Wählen Sie in der Tabelle **Clienteigenschaften** die gewünschte Clienteigenschaft aus.

Hinweis: Sie können mehrere Eigenschaften auswählen, indem Sie die Kontrollkästchen daneben aktivieren.

2. Klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie noch einmal auf **Löschen**.

Referenz der Clienteigenschaften

Jul 28, 2016

Die vordefinierten XenMobile-Clienteigenschaften und deren Standardeinstellungen sind wie folgt:

CONTAINER_SELF_DESTRUCT_PERIOD

Anzeigename: Self-Destruct

"Self-destruct" verhindert den Zugriff auf WorxHome und verwaltete Apps nach einer bestimmten Zeit der Inaktivität (in Tagen). Nach Ablauf der Zeit können Apps nicht mehr verwendet werden und die Registrierung des Geräts auf dem XenMobile-Server wird aufgehoben. Die Datenlöschung umfasst die App-Daten jeder App, die Daten im App-Cache und die Benutzerdaten. Als Zeit der Inaktivität gilt die Zeit, während derer der Server keine Authentifizierungsanforderung für den Benutzer erhält. Beispiel: Wenn Sie 30 Tage für die Richtlinie festlegen und der Benutzer Worx Home oder andere Apps 30 Tage lang nicht verwendet, wird die Richtlinie wirksam.

Diese globale Sicherheitsrichtlinie gilt für iOS und Android und ist eine Erweiterung der bestehenden Richtlinien zum Sperren von Apps und Löschen von Daten.

Zum Konfigurieren dieser globalen Richtlinie navigieren Sie zu **Einstellungen > Clienteigenschaften** und fügen Sie den benutzerdefinierten Schlüssel CONTAINER_SELF_DESTRUCT_PERIOD hinzu.

Wert: Anzahl der Tage

ENABLE_WORXHOME_CEIP

Anzeigename: Enable Worx Home CEIP

Dieser Schlüssel aktiviert das Programm zur Verbesserung der Benutzerfreundlichkeit. Hiermit werden in regelmäßigen Abständen anonyme Konfigurations- und Nutzungsdaten an Citrix gesendet. Mit diesen Daten kann Citrix die Qualität, Zuverlässigkeit und Leistung von XenMobile verbessern.

Wert: true oder false

Standardwert: false

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_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
Low	Alle Ziffern, beliebige Reihenfolge zugelassen	Muss mindestens eine Ziffer und einen Buchstaben enthalten. Nicht zulässig: AAAaaa, aaaaaa, abcdef Zulässig: aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa
Medium (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, 555556, 788888	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. 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#

PASSCODE_MIN_LENGTH

Anzeigename: Worx PIN Length Requirement

Dieser Schlüssel definiert die Mindestlänge für Worx-Passcodes.

Mögliche Werte: 1-99

Standardwert: 6

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 oder höher, 1-99 wird empfohlen

Standardwert: 90

Hinweis: Wenn Benutzer ihre PINs nicht zurücksetzen sollen, legen Sie den Wert auf eine sehr hohe Zahl fest (z. B. 100.000.000.000). Wenn Sie ursprünglich einen Wert zwischen 1 und 99 Tagen für den Kennwortablauf festgelegt haben und dann in diesem Zeitraum den Wert in die hohe Zahl ändern, laufen PINs am Ende des ursprünglichen Zeitraums ab und danach nie wieder.

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

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

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)

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

DEVICE_LOGS_TO_IT_HELP_DESK

Anzeigename: Geräteprotokolle an IT-Helpdesk senden

Mit diesem Schlüssel aktivieren bzw. deaktivieren Sie die Möglichkeit zum Senden von Protokollen an den IT-Helpdesk.

Mögliche Werte: true oder false

Standardwert: false

ON_FAILURE_USE_EMAIL

Anzeigename: On failure use Email to send device logs to IT help desk.

Mit diesem Schlüssel aktivieren bzw. deaktivieren Sie die Möglichkeit zum Senden von Protokollen an den IT-Helpdesk per E-Mail.

Mögliche Werte: true oder false

Standardwert: true

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

ENABLE_TOUCH_ID_AUTH

Anzeigename: Enable Touch ID Authentication

Mit diesem Schlüssel aktivieren bzw. deaktivieren Sie die Möglichkeit zur Verwendung der Touch ID-Authentifizierung auf Geräten mit der entsprechenden Funktion. Auf den Geräten muss die Worx-PIN aktiviert und der Parameter Benutzerentropie auf "false" festgelegt sein, damit die Benutzer beim Starten einer App zur Verwendung von Touch ID aufgefordert werden.

Mögliche Werte: true oder false

Standardwert: false

ENABLE_WORXHOME_GA

Anzeigename: Enable Google Analytics in WorxHome

Mit diesem Schlüssel aktivieren oder deaktivieren Sie die Möglichkeit zum Sammeln von Daten über Google Analytics in Worx Home. Wenn Sie diese Einstellung ändern, tritt der neue Wert erst in Kraft, wenn sich der Benutzer das nächste Mal bei Worx Home anmeldet.

Mögliche Werte: true oder false

Standardwert: true

XenMobile-Servereinstellungen

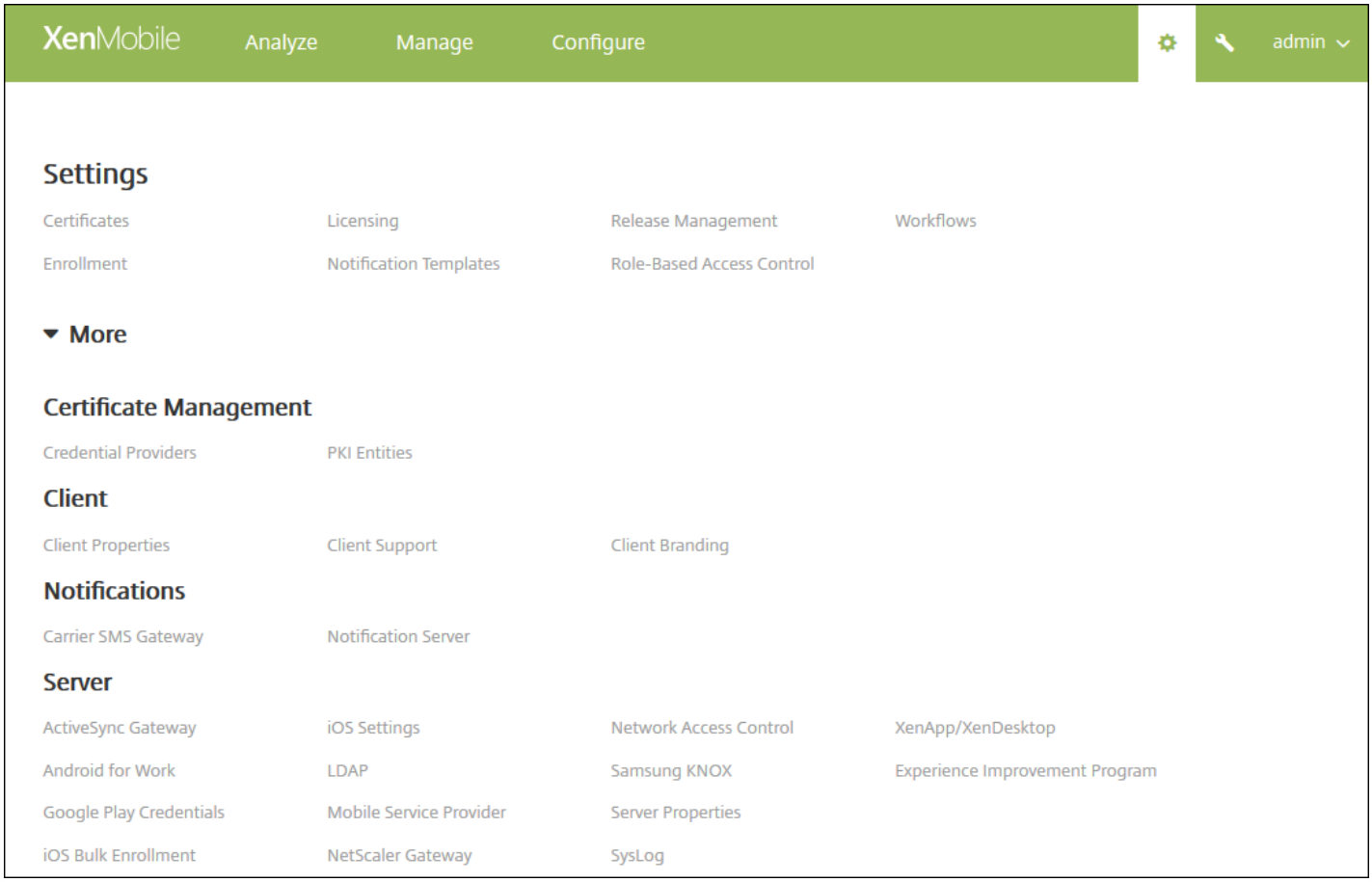
Jul 28, 2016

In der XenMobile-Konsole werden folgende XenMobile-Servereinstellungen konfiguriert:

- ActiveSync Gateway
- Android for Work
- Programm zur Verbesserung der Benutzerfreundlichkeit
- Google Play-Anmeldeinformationen
- iOS-Massenregistrierung
- iOS-Einstellungen
- LDAP
- Microsoft Azure
- Mobilfunkanbieter
- NetScaler Gateway
- Netzwerkzugriffssteuerung (NAC)
- Samsung KNOX
- Servereigenschaften
- SysLog
- XenApp/XenDesktop

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf die Option, die Sie konfigurieren möchten.



ActiveSync Gateway in XenMobile

Jul 28, 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 "Fehlende Pflicht-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:

Anonyme Geräte: 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.

Samsung KNOX-Nachweisfehler: Prüft, ob bei einem Gerät die Abfrage des Samsung KNOX-Nachweisservers fehlgeschlagen ist.

Unzulässige Apps: Prüft, ob ein Gerät unzulässige Apps aufweist, die in einer App-Zugriffsrichtlinie definiert sind.

Implizit zulassen oder verweigern: 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".

Inaktive Geräte: Prüft, ob ein Gerät entsprechend dem unter "Schwellenwert für Tage inaktiv" in den Servereigenschaften festgelegten Wert inaktiv ist.

Fehlende Pflicht-Apps: Prüft, ob auf einem Gerät Apps fehlen, die in einer App-Zugriffsrichtlinie definiert sind.

Nicht empfohlene Apps: Prüft, ob ein Gerät nicht empfohlene Apps aufweist, die in einer App-Zugriffsrichtlinie definiert sind.

Nicht richtlinientreues Kennwort: 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.

Nicht richtlinientreue Geräte: 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.

Widerrufenstatus: Prüft, ob das Gerätezertifikat widerrufen worden ist. Ein widerrufenes Gerät kann erst erneut registriert werden, wenn es wieder autorisiert ist.

Android-Geräte mit Rooting oder iOS-Geräte mit Jailbreak: Prüft, ob auf einem Android- oder iOS-Gerät ein Jailbreak vorliegt.

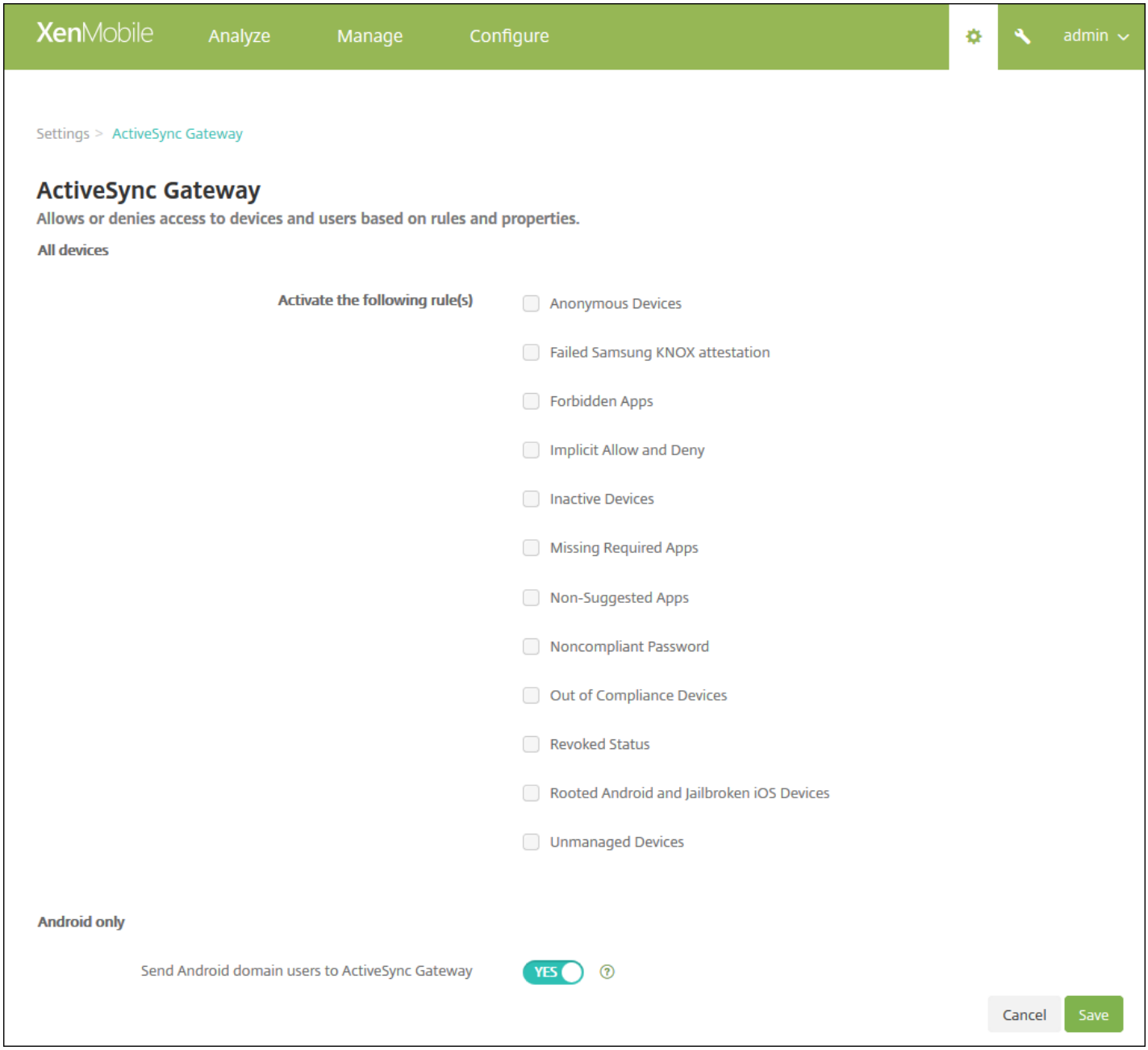
Nicht verwaltete Geräte: Prüft, ob ein Gerät verwaltet, d. h. von XenMobile kontrolliert wird. Beispielsweise ist ein Gerät im MAM-Modus oder ein nicht registriertes Gerät nicht verwaltet.

Android-Domänenbenutzer an ActiveSync-Gateway senden: Klicken Sie auf **JA**, 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.

Konfigurieren der ActiveSync-Gateway-Einstellungen

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 für **Nur Android** unter **Android-Domänenbenutzer an ActiveSync-Gateway senden** auf **JA**, um sicherzustellen, dass XenMobile Android-Geräteinformationen an das ActiveSync-Gateway sendet.

5. Klicken Sie auf **Speichern**.

Google Play-Anmeldeinformationen

Aug 22, 2016

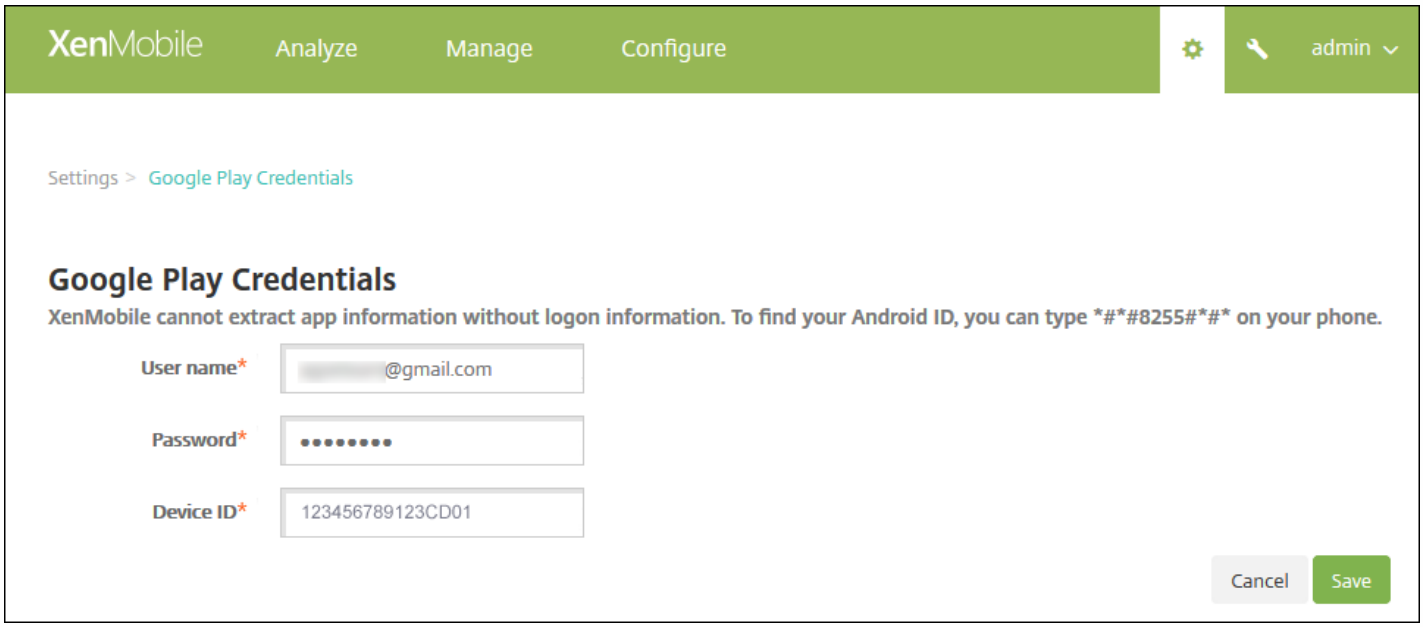
XenMobile verwendet Google Play-Anmeldeinformationen zum Extrahieren von App-Informationen für Geräte.

Hinweis: Zum Ermitteln der Android-ID geben Sie auf ihrem Telefon *#*#8255#*#* ein. Wenn Sie mit dem Code nicht die Geräte-ID Ihres Gerätetyps ermitteln können, kann die Geräte-ID möglicherweise mit einer Drittanbieter-App ermittelt werden. Sie benötigen die Google Services Framework ID mit der Bezeichnung GSF ID.

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.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **Google Play-Anmeldeinformationen**. Die Seite **Google Play-Anmeldeinformationen** wird angezeigt.



3. Konfigurieren Sie die folgenden Einstellungen:

- **Benutzername**: Geben Sie den Namen des Google Play-Kontos ein.
- **Kennwort**: Geben Sie das Benutzerkennwort ein.
- **Geräte-ID** Geben Sie in Ihre Android-ID ein.
  Zum Ermitteln der Android-ID geben Sie auf ihrem Telefon *#*#8255#*#* ein.

3. Klicken Sie auf **Speichern**.

Massenregistrierung von iOS-Geräten

Jul 28, 2016

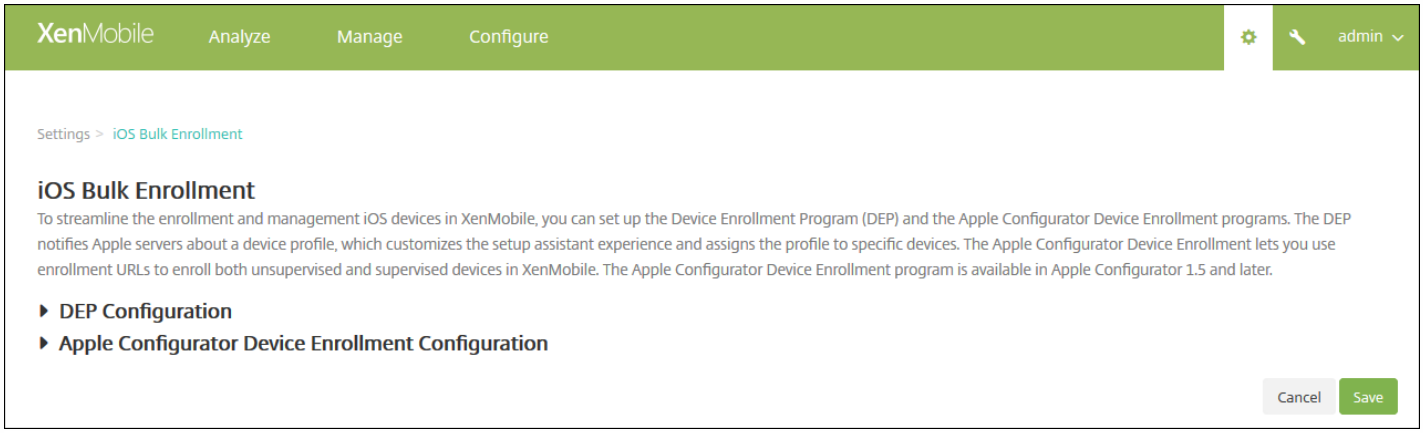
Sie können iOS-Geräte in großer Zahl bei XenMobile auf zweierlei Weise registrieren. Sie können das Registrierungsprogramm von Apple (Device Enrollment Program, DEP) verwenden, um direkt bei Apple, einem autorisierten Apple-Wiederverkäufer oder einem Netzbetreiber erworbene Geräte zu registrieren, oder Geräte unabhängig davon, wo Sie sie erworben haben, mit Apple Configurator registrieren.

Bei Verwendung des DEP brauchen Sie die Geräte nicht vorzubereiten. Sie übermitteln die Geräteseriennummern oder Bestellnummern per DEP und die Geräte werden dann konfiguriert und bei XenMobile registriert. Nachdem die Geräte registriert wurden, können Sie sie Benutzern aushändigen, die sie dann direkt verwenden können. Durch das Einrichten von Geräten per DEP können Sie außerdem einige Schritte im Setupassistenten eliminieren, die die Benutzer andernfalls beim ersten Starten ihres Geräts ausführen müssten. Weitere Informationen zum Einrichten von DEP finden Sie auf der Webseite von Apple zum Device Enrollment Program.

Mit Apple Configurator fügen Sie Geräte einem Apple-Computer mit OS X 10.7.2 oder höher und der Apple Configurator-App an. Sie verwenden Apple Configurator zum Vorbereiten der Geräte und zum Konfigurieren von Richtlinien. Nach dem Bereitstellen der Geräte mit den erforderlichen Richtlinien werden die Richtlinien beim ersten Verbindungsaufbau zwischen Gerät und XenMobile angewendet und Sie können mit dem Verwalten der Geräte beginnen. Weitere Informationen über die Verwendung von Apple Configurator finden Sie auf der Apple-Website zu Apple Configurator.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **iOS-Massenregistrierung**. Die Seite **iOS-Massenregistrierung** wird angezeigt.



Wenn Sie DEP-Einstellungen konfigurieren, lesen Sie den Abschnitt Konfigurieren von DEP-Einstellungen. Wenn Sie Apple Configurator-Einstellungen konfigurieren, lesen Sie den Abschnitt Konfigurieren von Apple Configurator-Einstellungen.

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.

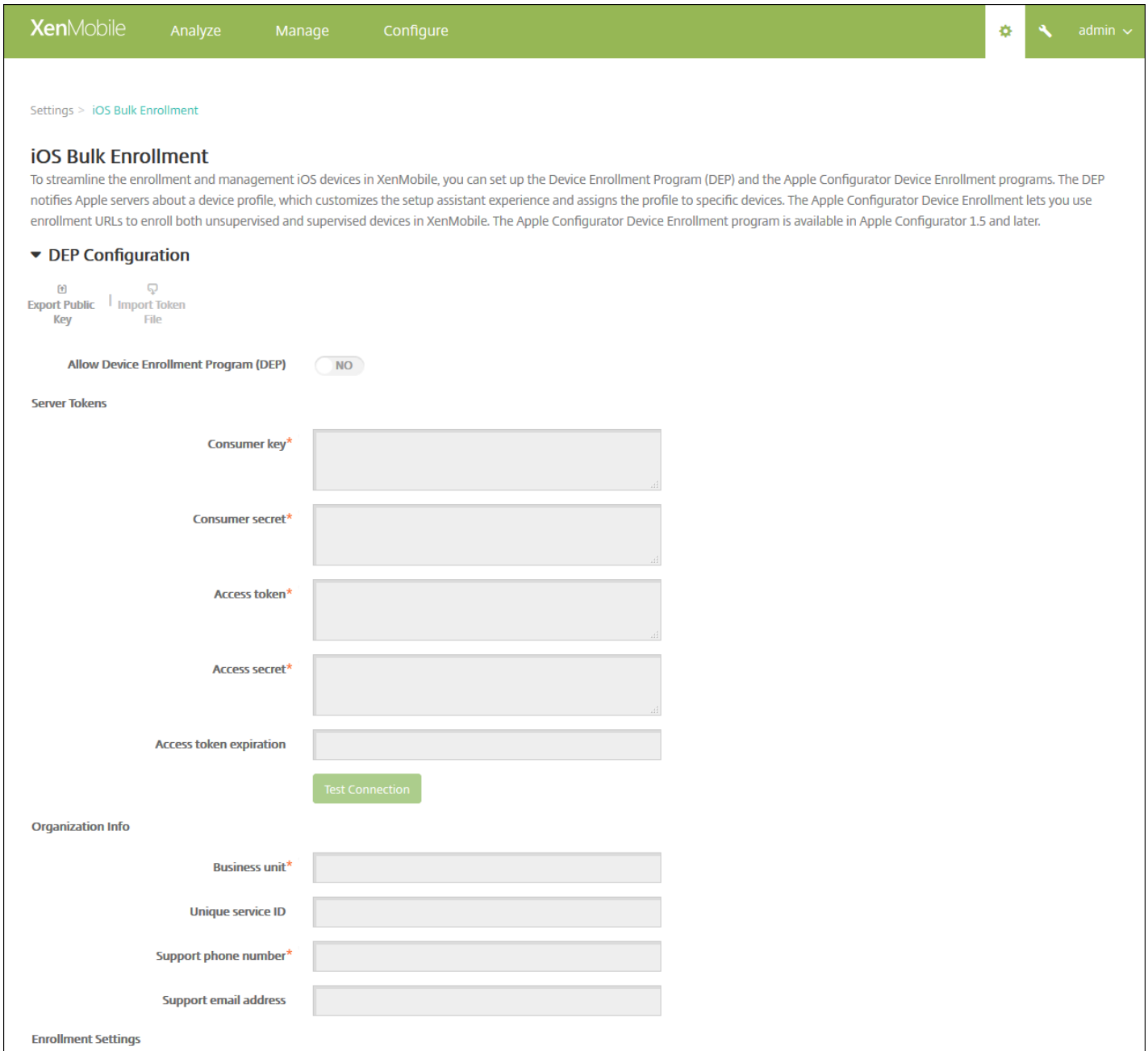
1. Um den öffentlichen Schlüssel für Apple zu erhalten, erweitern Sie auf der Seite **iOS-Massenregistrierung** die Option **DEP-Konfiguration**, klicken Sie auf **Öffentlichen Schlüssel exportieren** und speichern Sie die Datei auf Ihrem Computer.

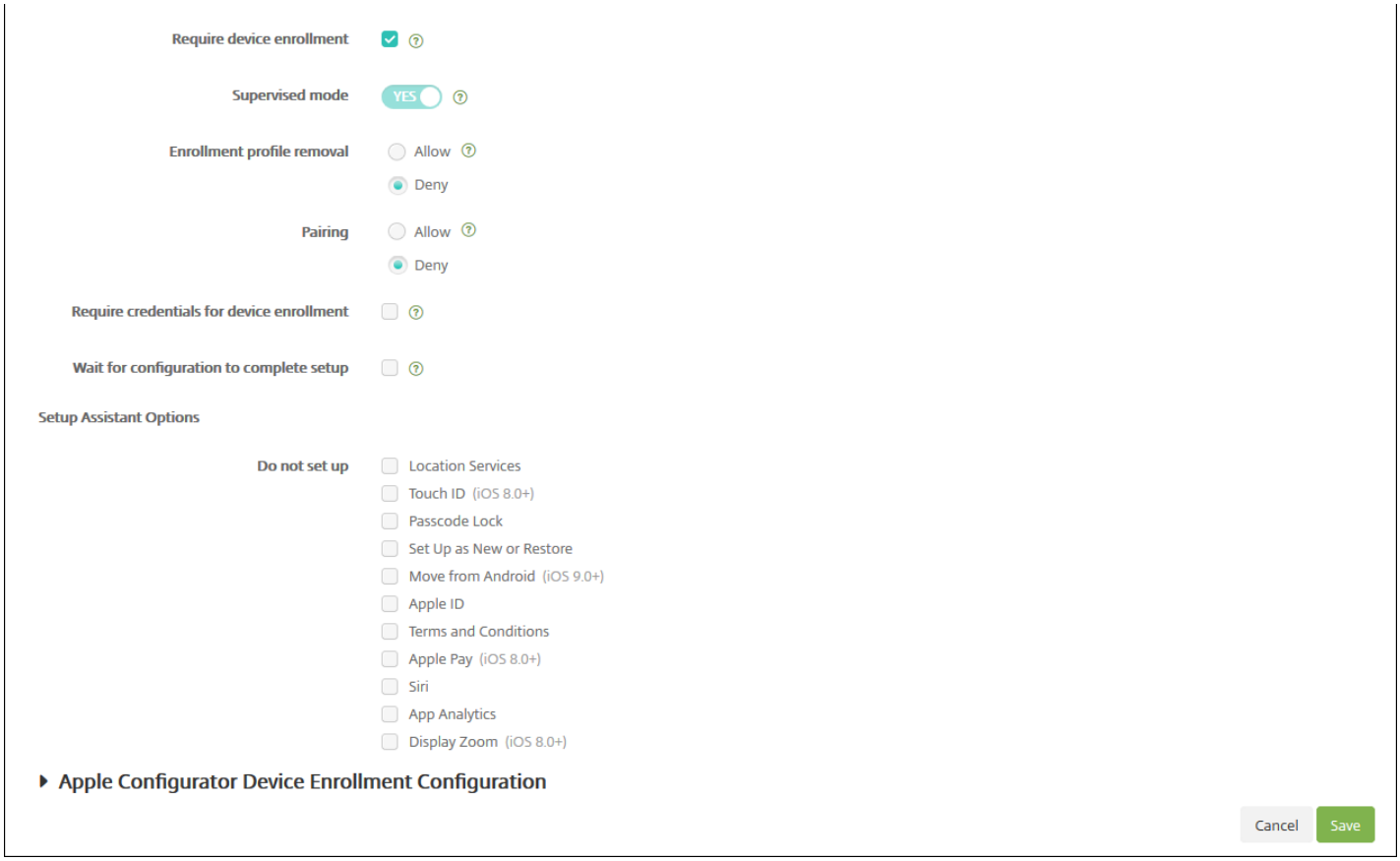
2. Navigieren Sie zu deploy.apple.com, melden Sie sich bei Ihrem DEP-Konto an und folgen Sie den Anweisungen zum Einrichten eines MDM-Servers. Im Rahmen dieses Prozesses stellt Apple ein Servertoken bereit.

3. Klicken Sie auf der Seite **iOS-Massenregistrierung** auf **Tokendatei importieren** und fügen Sie das Apple-Servertoken in XenMobile hinzu.

4. Das Feld **Servertoken** wird automatisch ausgefüllt, wenn die Tokendatei in XenMobile hochgeladen wurde.

5. Klicken Sie auf **Verbindung testen**, 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.





6. Konfigurieren Sie folgende Einstellungen für die DEP-Konfiguration:

Informationen zum Unternehmen

- **Geschäftseinheit**: Geben Sie die Unternehmenseinheit oder Abteilung ein, der das Gerät zugewiesen ist. Diese Angabe ist erforderlich.
- **Eindeutige Dienst-ID**: Geben Sie optional die eindeutige ID ein.
- **Telefonnummer vom Support**: Geben Sie die Telefonnummer ein, unter der die Benutzer beim Setup Hilfe anfordern können. Diese Angabe ist erforderlich.
- **E-Mail-Adresse vom Support**: Geben Sie optional die E-Mail-Adresse des Supports ein.

Registrierungseinstellungen

- **Geräteregistrierung erforderlich**: Wählen Sie aus, ob Benutzer Geräte registrieren müssen. In der Standardeinstellung ist dies erforderlich.
- **Betreuter Modus**: Diese Option muss auf **Ja** festgelegt werden, wenn Sie Apple Configurator zum Verwalten über DEP registrierter Geräte verwenden oder wenn **Abschluss der Konfiguration abwarten** aktiviert ist. Der Standardwert ist **Ja**. Informationen, wie Sie iOS-Geräte in den betreuten Modus versetzen, finden Sie unter Versetzen von iOS-Geräten mit dem Apple Configurator in den betreuten Modus.
- **Entfernen des Registrierungsprofils**: Wählen Sie aus, ob auf Geräten ein Profil verwendet werden darf, das remote entfernt werden kann. Der Standardwert ist **Verweigern**.
- **Kopplung**: Wählen Sie aus, ob über DEP registrierte Geräte über iTunes und Apple Configurator verwaltet werden dürfen. Der Standardwert ist **Verweigern**.
- **Anmeldeinformationen für Geräteregistrierung erforderlich**: Wählen Sie aus, ob Benutzer bei der DEP-

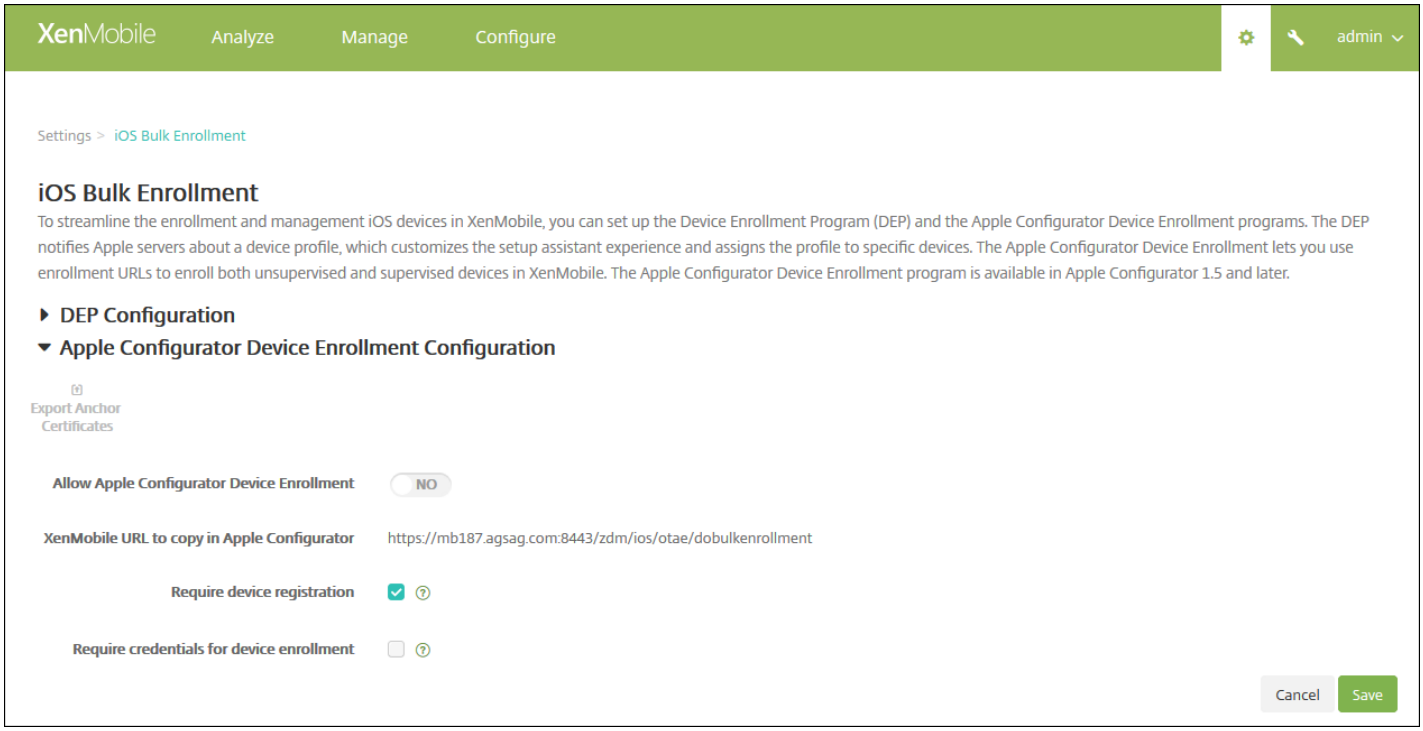
Registrierung ihre Anmeldeinformationen eingeben müssen. Diese Option ist für iOS 7.1 und höher verfügbar. **Hinweis**: Wenn Sie DEP erstmalig einrichten und diese Option nicht aktivieren, werden die DEP-Komponenten (DEP-Benutzer, Worx Home, Softwarebestand und DEP-Bereitstellungsgruppe) von Anfang an erstellt. Wenn Sie diese Option aktivieren, müssen Benutzer zur Erstellung der Komponenten erst ihre Anmeldeinformationen eingeben. Wenn Sie dann später die Option deaktivieren, können Benutzer, die ihre Anmeldeinformationen nicht eingegeben haben, die DEP-Registrierung nicht ausführen, da keine DEP-Komponenten vorhanden sind. Zum Hinzufügen von DEP-Komponenten in diesem Fall deaktivieren und reaktivieren Sie das DEP-Konto.

- **Abschluss der Konfiguration abwarten**: Wählen Sie aus, ob Geräte im Setupassistentenmodus verbleiben müssen, bis alle erforderlichen MDM-Ressourcen auf den Geräten bereitgestellt wurden. Diese Richtlinie gilt nur für iOS 9.0 und höher im betreuten Modus.
  - **Hinweis**: Laut Apple-Dokumentation funktionieren die folgenden Befehle möglicherweise nicht, wenn ein Gerät im Setupassistentenmodus ist:
    - InviteToProgram
    - InstallApplication
    - ApplyRedemptionCode
    - InstallMedia
    - RequestMirroring
    - DeviceLock

Einrichtung

Wählen Sie die Schritte im iOS-Setupassistenten aus, die Benutzer *nicht* ausführen müssen, wenn sie ihre Geräte zum ersten Mal starten.

- **Ortungsdienste**: Einrichten der Ortungsdienste auf dem Gerät
- **Touch ID**: Einrichten von Touch ID auf Geräten mit iOS 8.0 oder höher
- **Passcodesperre**: Erstellen einer Passcodesperre für das Gerät
- **Neu einrichten oder wiederherstellen**: Einrichten des Geräts als neu oder als Backup von einer iCloud oder iTunes
- **Verschieben von Android**: Aktivieren der Datenübertragung von einem Android-Gerät auf ein Gerät mit iOS 9 oder höher. Diese Option ist nur verfügbar, wenn **Neu einrichten oder wiederherstellen** aktiviert wurde (d. h. der Schritt wird ausgelassen).
- **Apple-ID**: Einrichten einer Apple-ID für das Gerät
- **AGB**: Akzeptieren der Nutzungsbedingungen für die Verwendung des Geräts
- **Apple Pay**: Einrichten von Apple Pay auf Geräten mit iOS 8.0 oder höher
- **Siri**: Auswahl, ob Siri auf dem Gerät verwendet werden soll
- **Apple Analytics**: Auswahl, ob Absturzdaten und Nutzungsstatistiken an Apple weitergegeben werden sollen
- **Anzeigezoom**: Einrichten des Anzeigezooms (Standard oder verkleinert/vergrößert) auf Geräten mit iOS 8.0 oder höher.



1. Erweitern Sie **Apple Configurator - Geräteregistrierungskonfiguration**.

2. Wählen Sie für **Apple Configurator - Geräteregistrierung aktivieren** die Einstellung **Ja**.

3. Notieren Sie sich bzw. konfigurieren Sie die folgenden Einstellungen:

- **XenMobile-URL zum Kopieren in Apple Configurator**: Dieses schreibgeschützte Feld enthält die URL des XenMobile-Servers, der mit Apple kommuniziert, und die Sie zu einem späteren Zeitpunkt in Apple Configurator einfügen müssen. In Apple Configurator 2 entspricht die Registrierungs-URL dem vollqualifizierten Domänennamen bzw. der IP-Adresse des XenMobile-Servers (z. B. mdm.server.url.com).
- **Geräteregistrierung erforderlich**: Wenn Sie diese Einstellung auswählen, müssen Sie die konfigurierten Geräte manuell oder mithilfe einer CSV-Datei auf der Registerkarte **Geräte** in XenMobile hinzufügen, bevor sie registriert werden können. Damit wird gewährleistet, dass keine unbekannten Geräte registriert werden können. In der Standardeinstellung ist das Hinzufügen von Geräten erforderlich.
- **Anmeldeinformationen für Geräteregistrierung erforderlich**: Bei Auswahl dieser Option müssen zur Registrierung von Geräten mit iOS 7.1 oder höher Anmeldeinformationen eingegeben werden. In der Standardeinstellung ist dies nicht erforderlich.

> ## Hinweis
>
> Wenn der XenMobile-Server ein vertrauenswürdiges SSL-Zertifikat verwendet, überspringen Sie den nächsten Schritt.

4. Klicken Sie auf **Ankerzertifikate exportieren** und speichern Sie die Datei certchain.pem im OS X-Schlüsselbund (Anmeldung oder System).

5. Starten Sie Apple Configurator und gehen Sie zu **Prepare -> Setup -> Configure Settings**

6. Fügen Sie unter **Device Enrollment** die URL des MDM-Servers aus Schritt 4 in das Feld **MDM server URL** ein.

7. Kopieren Sie unter **Device Enrollment** die Stammzertifizierungsstelle und die Zertifizierungsstelle des SSL-Serverzertifikats zu den **Anchor**-Zertifikaten, wenn XenMobile kein vertrauenswürdiges SSL-Zertifikat verwendet.

8. Schließen Sie Geräte mit USB-Kabel am Dock-Anschluss eines Macintosh-Computers mit Apple Configurator an, um bis zu 30 verbundene Geräte gleichzeitig zu konfigurieren. Wenn Sie keinen Dock-Anschluss haben, verwenden Sie einen oder mehrere High-Speed-USB-2.0-Hubs mit eigener Stromversorgung, um die Geräte anzuschließen.

9. Klicken Sie auf **Prepare**. Weitere Informationen zur Vorbereitung von Geräten mit Apple Configurator finden Sie der Seite Prepare devices der Apple Configurator-Hilfe.

10. Konfigurieren Sie in Apple Configurator die benötigten Geräterichtlinien.

11. Schalten Sie zur Vorbereitung jedes Gerät ein, um den iOS-Setupassistenten zu starten, der es für die erste Verwendung vorbereitet.

Wenn das XenMobile SSL-Zertifikat (Secure Sockets Layer) erneuert wird, laden Sie ein neues Zertifikat in der XenMobile-Konsole unter **Einstellungen** > **Zertifikate** hoch. Klicken Sie im Dialogfeld "Importieren" unter **Verwenden als** auf **SSL-Listener**, damit das Zertifikat für SSL verwendet wird. Nach dem Neustart des Servers verwendet XenMobile das neue SSL-Zertifikat. Weitere Informationen über Zertifikate in XenMobile finden Sie unter Hochladen von Zertifikaten in XenMobile.

Es ist nicht erforderlich, die Vertrauensstellung zwischen Apple DEP und XenMobile neu zu erstellen, wenn Sie das SSL-Zertifikat erneuern oder aktualisieren. Sie können jedoch die DEP-Einstellungen jederzeit mit den in diesem Abschnitt beschriebenen Schritten neu konfigurieren.

Weitere Informationen zu Apple DEP finden Sie in der Dokumentation von Apple.

Weitere Informationen über ein bekanntes Problem und einen Workaround für diese Konfiguration finden Sie unter Bekannte Probleme bei XenMobile Server 10.3.

Bereitstellen von iOS-Geräten mit Apple DEP

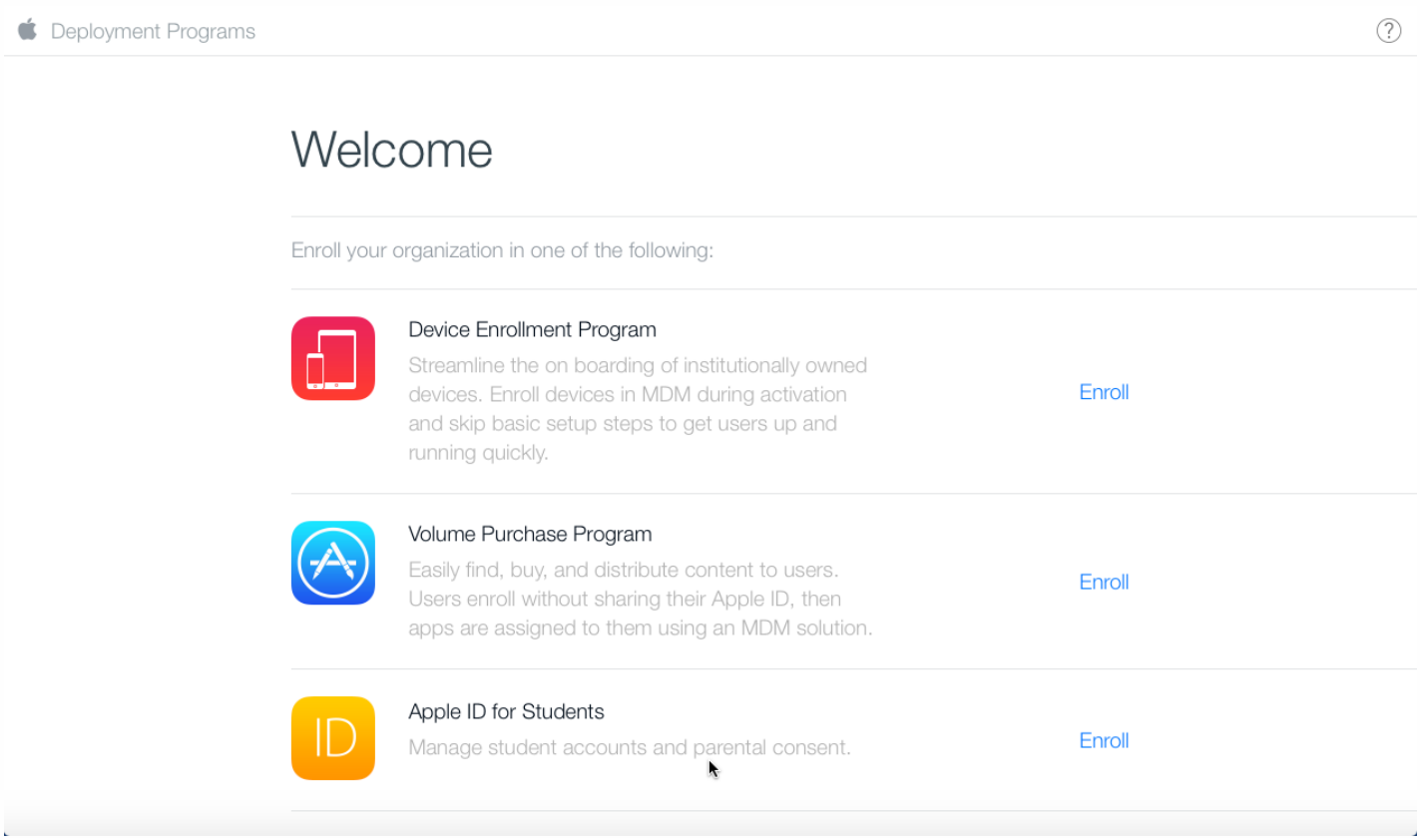
Jul 28, 2016

Wenn Sie die Vorteile des Apple Developer Enterprise Program (DEP) für die Registrierung und Verwaltung von iOS-Geräten in XenMobile nutzen möchten, benötigen Sie ein Apple DEP-Konto. Für die Anmeldung am Apple DEP müssen Organisationen folgende Informationen bereithalten.

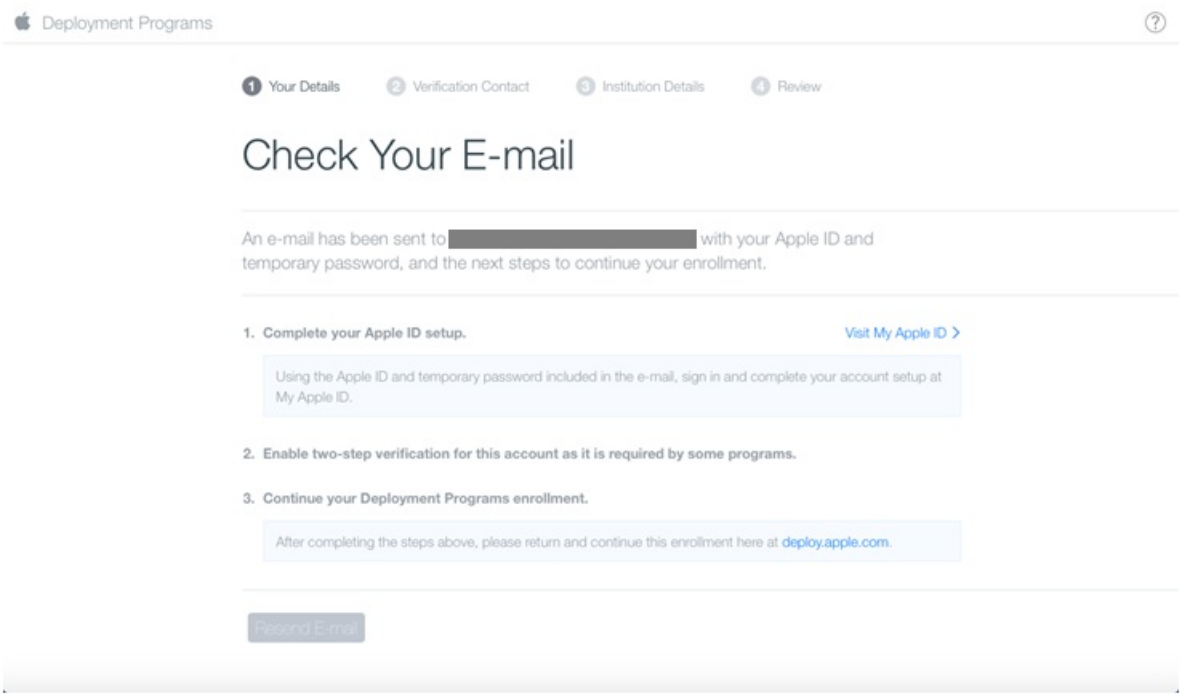
- Telefonnummer und E-Mail-Adresse der Firma oder der Organisation
- Verifizierungskontakt
- Unternehmens- oder Organisationsinformationen (D-U-N-S-Nummer/Steuernummer)
- Apple Kundennummer

Weitere Informationen zum Apple DEP finden Sie in dieser PDF von Apple. Das Apple DEP ist nur für Organisationen verfügbar, nicht für Einzelpersonen. Berücksichtigen Sie, dass zum Erstellen eines Apple DEP-Kontos viele Unternehmensdetails und -informationen angegeben werden müssen, daher kann das Anfordern eines Kontos bis hin zur Genehmigung länger dauern.

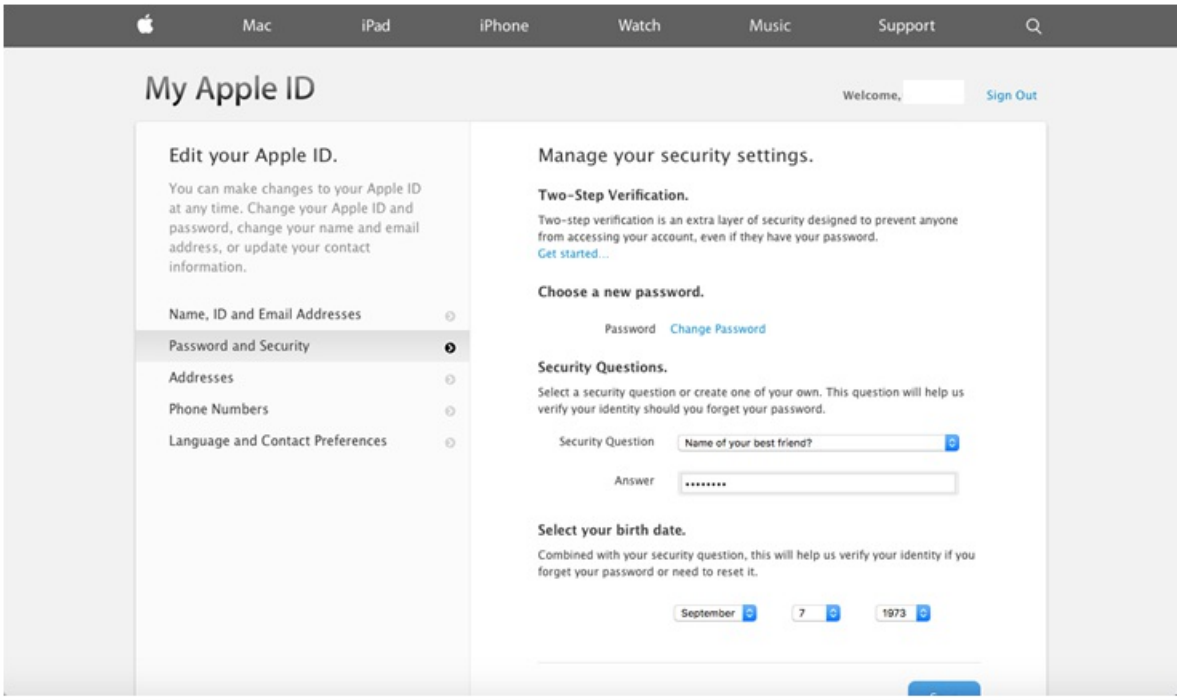
Beim Beantragen eines DEP-Kontos verwenden Sie am besten eine E-Mail-Adresse, die mit der Organisation verbunden ist, z. B. dep@company.com.



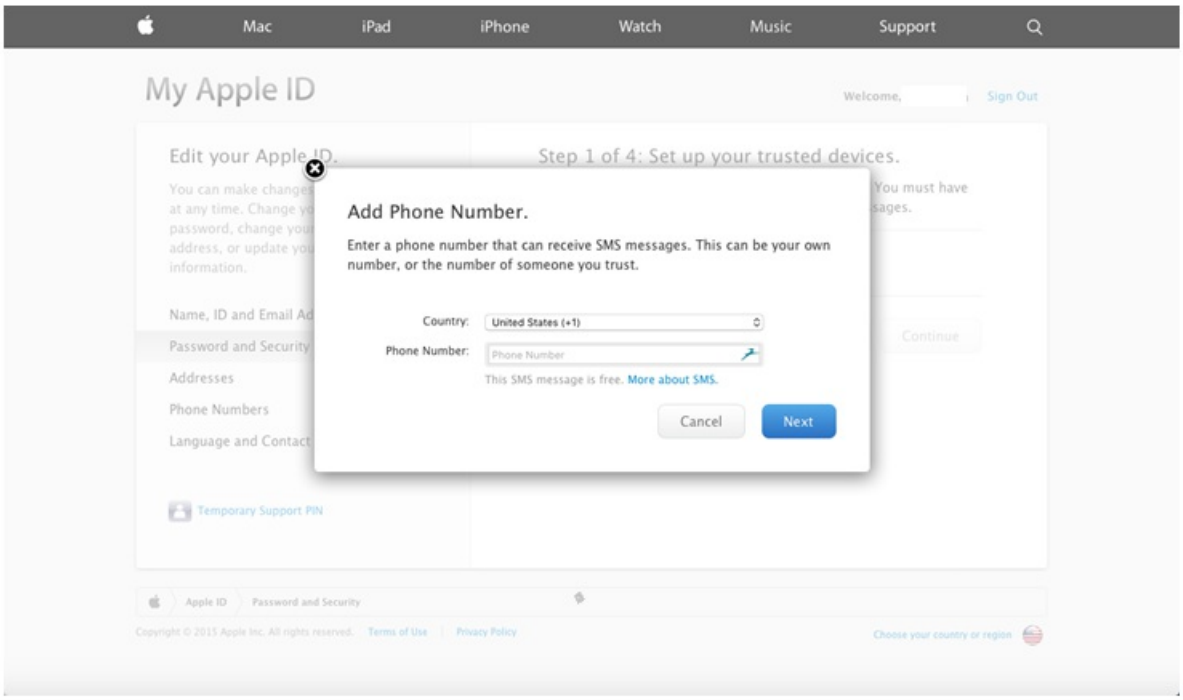
1. Wenn Sie die Organisationsinformationen angegeben haben, erhalten Sie per E-Mail ein temporäres Kennwort für die neue Apple-ID.



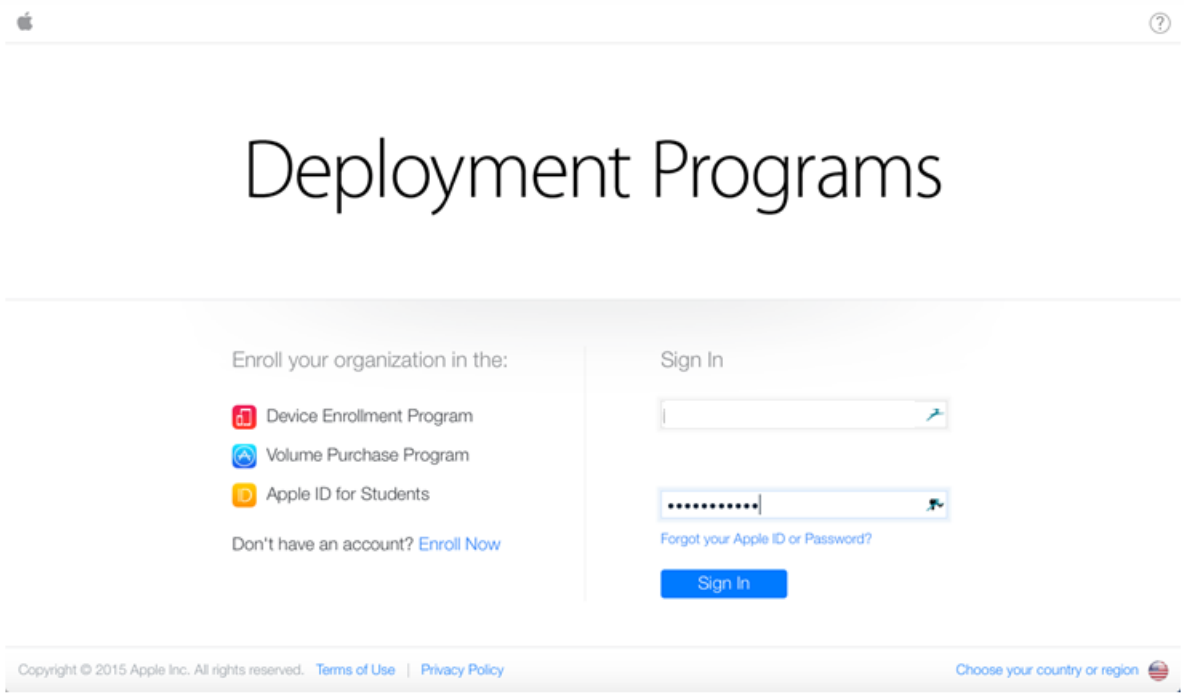
2. Melden Sie sich mit der Apple-ID an und legen Sie die Sicherheitseinstellungen für das Konto fest.



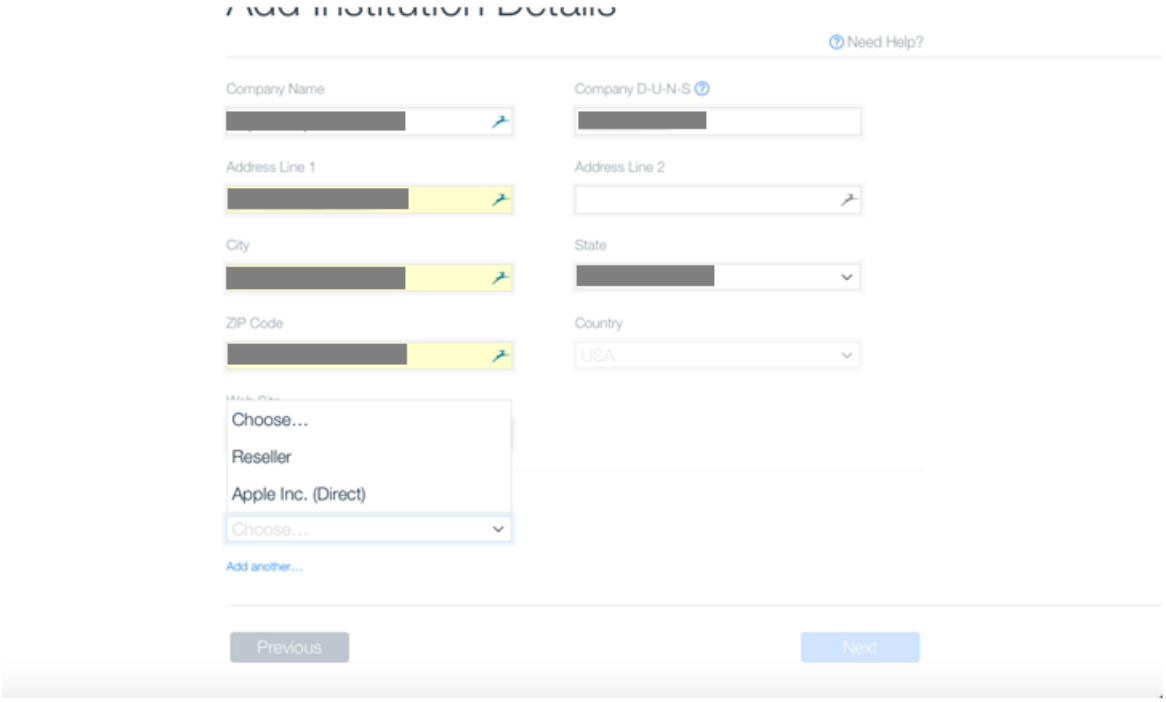
3. Konfigurieren und aktivieren Sie die Überprüfung in zwei Schritten, die für das DEP-Portal erforderlich ist. Bei diesen Schritten fügen Sie eine Telefonnummer hinzu, über die Sie die 4-stellige PIN für die Überprüfung in zwei Schritten erhalten.



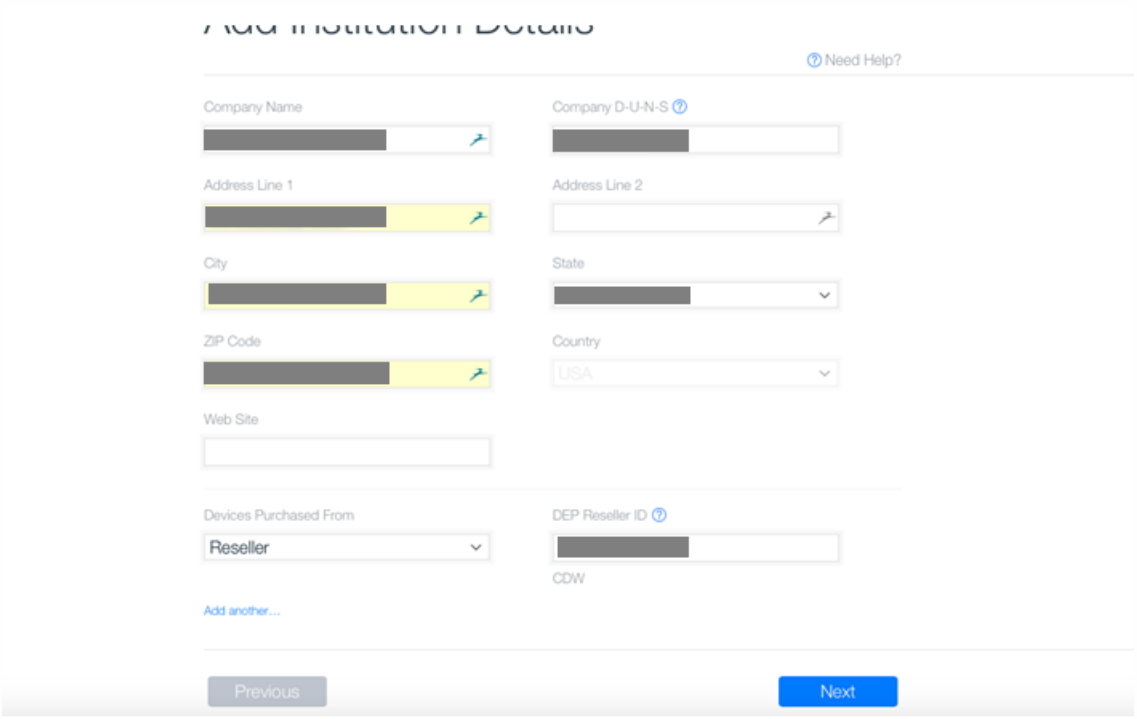
4. Melden Sie sich mit der Überprüfung in zwei Schritten beim DEP-Portal an und schließen Sie die Kontokonfiguration ab.

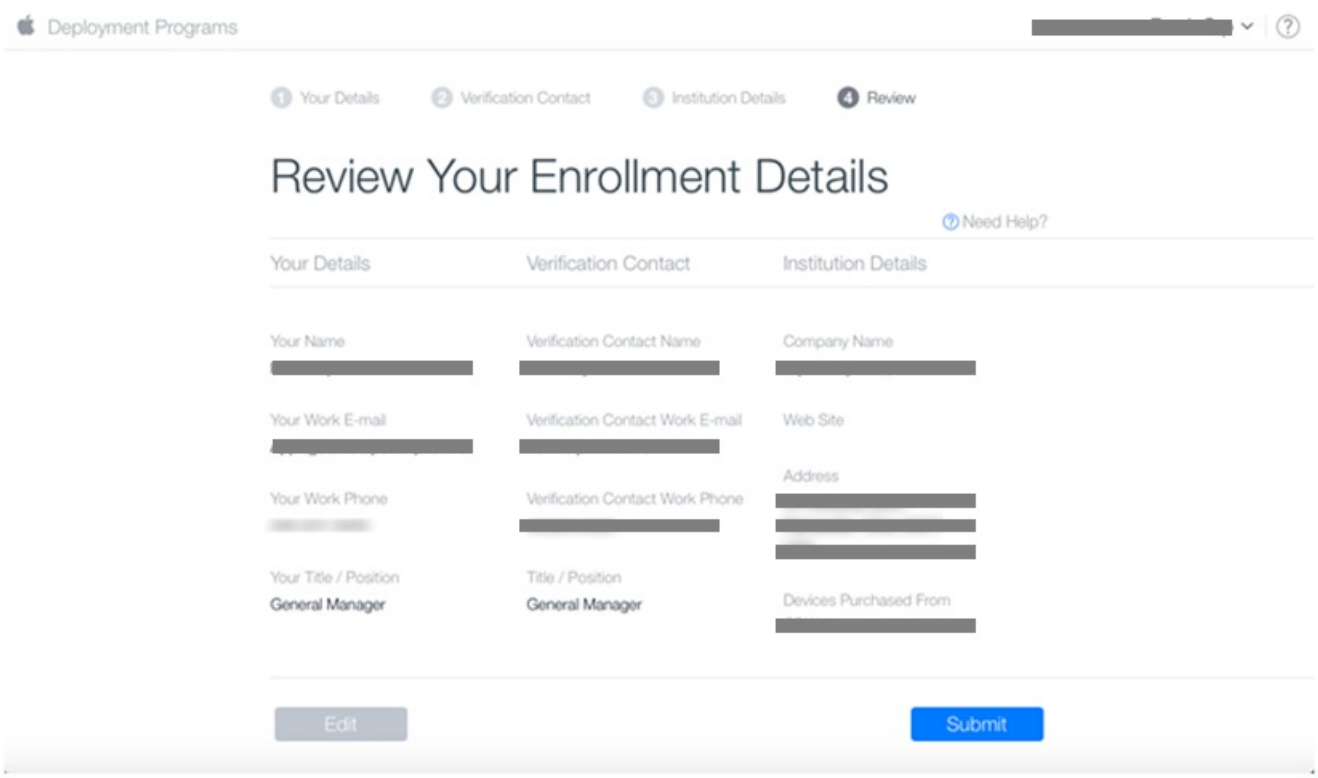


5. Fügen Sie die Details Ihres Unternehmens hinzu und wählen Sie aus, wo Sie Ihre Geräte erwerben. Details zu Erwerbsoptionen finden Sie im nächsten Abschnitt unter Bestellen von DEP-aktivierten Geräten.

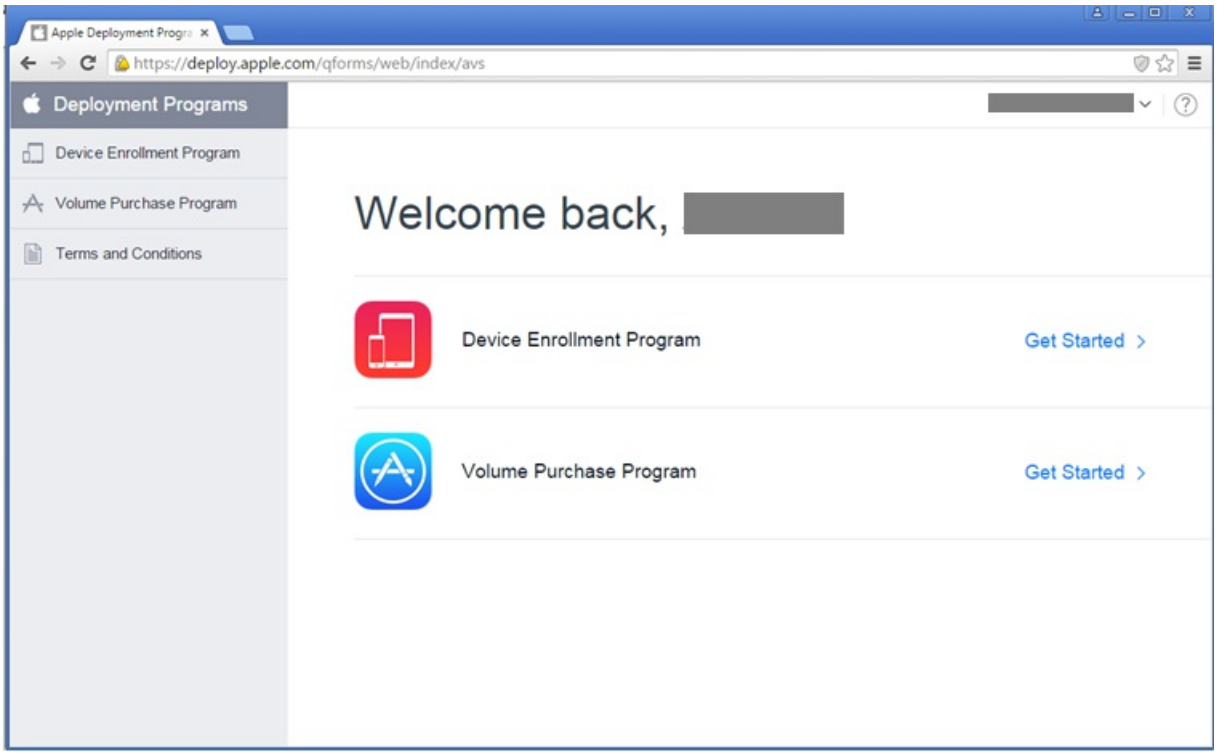


6. Fügen Sie die Apple-Kundennummer oder die DEP-Wiederverkäufer-ID hinzu und überprüfen Sie Ihre Registrierungsdetails. Warten Sie dann darauf, dass Apple Ihr Konto genehmigt.



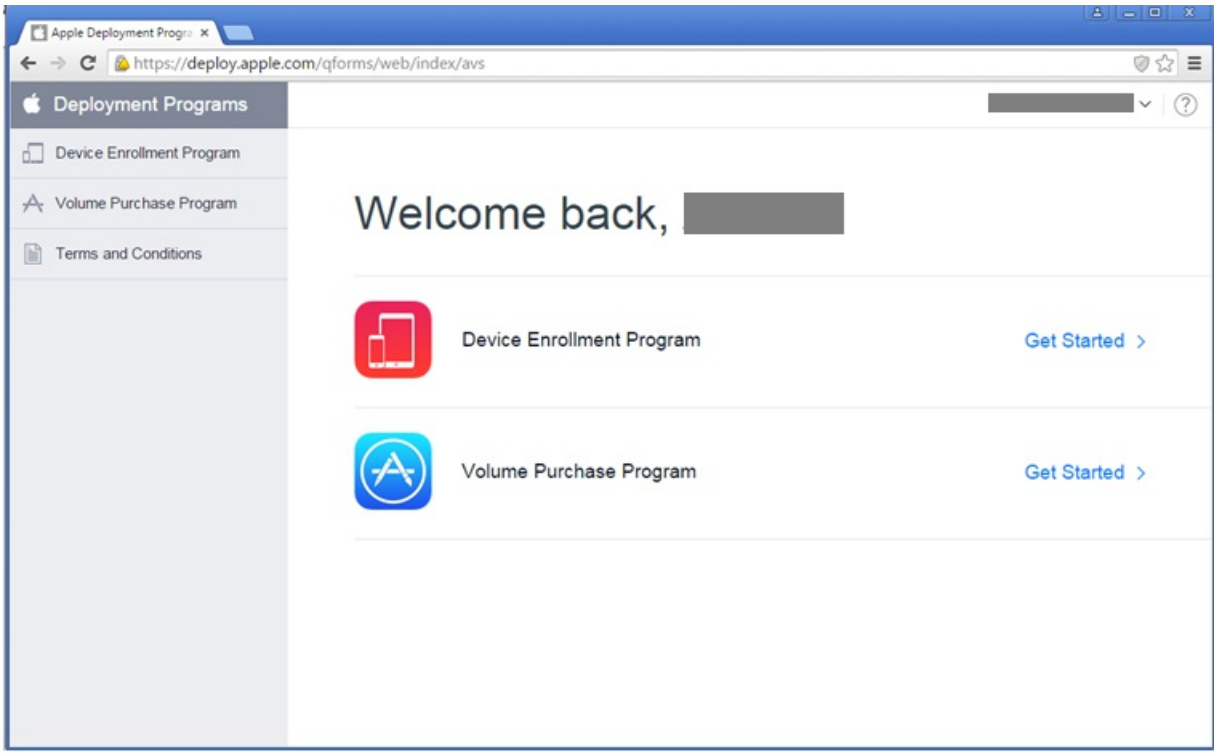


7. Wenn Sie Ihre Anmeldeinformationen von Apple erhalten haben, melden Sie sich beim Apple DEP-Portal an. Führen Sie dann die Schritte im nächsten Abschnitt aus, um Ihre Konto mit XenMobile zu verbinden.

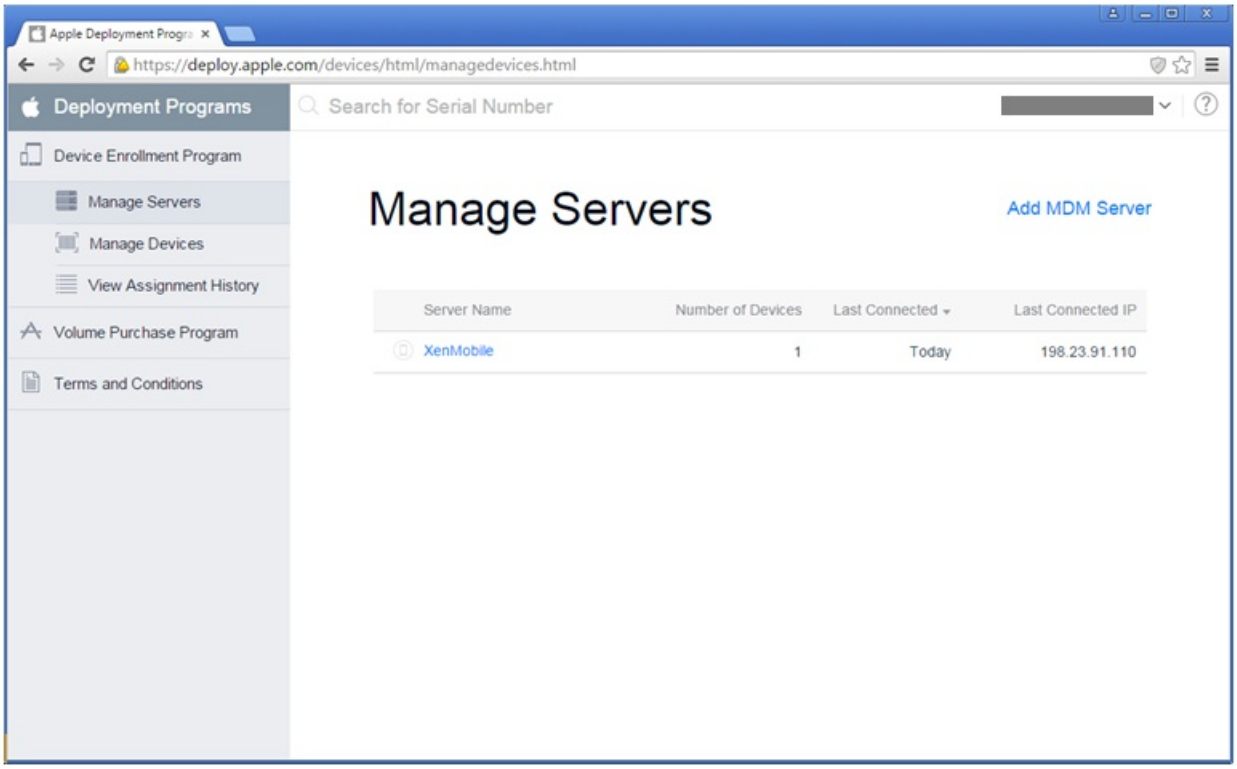


Befolgen Sie die Anleitungen in diesem Abschnitt, um Ihr Apple DEP-Konto mit Ihrer XenMobile-Serverbereitstellung zu verbinden.

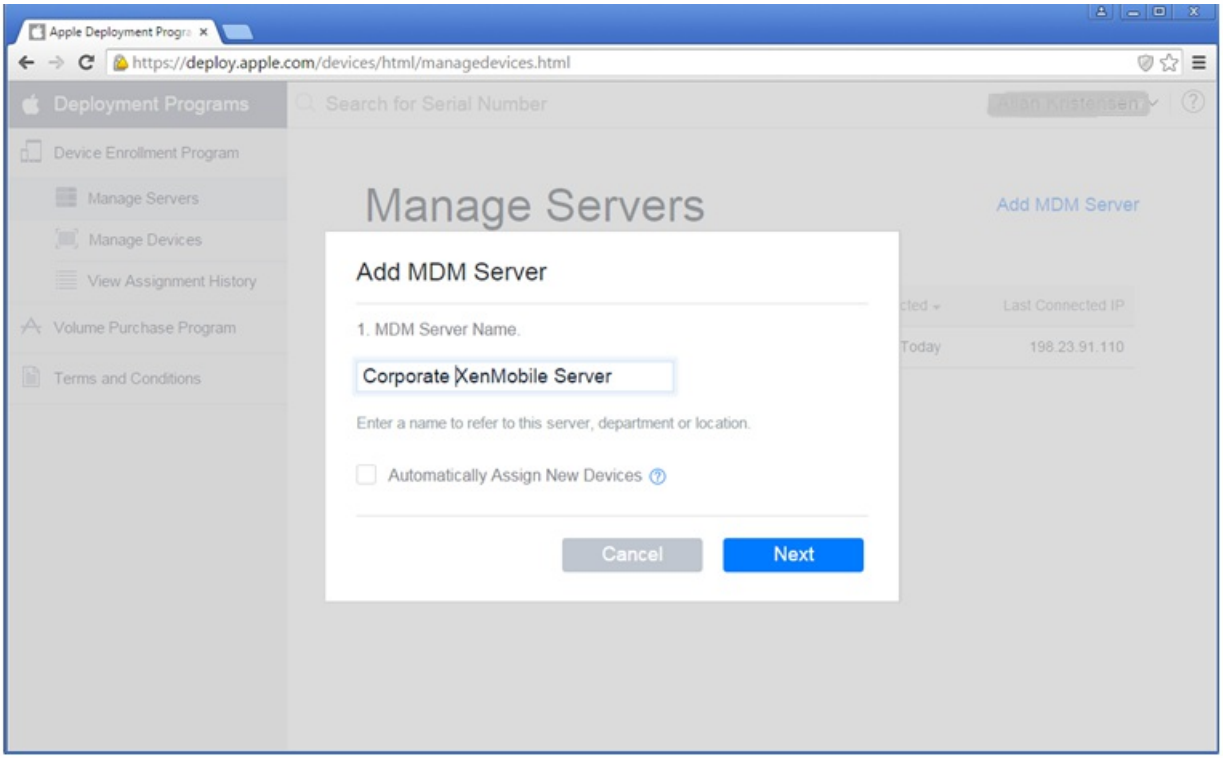
1. Klicken Sie links im Apple DEP-Portal auf **Device Enrollment Program**.



2. Klicken Sie auf **Manage Servers** und dann rechts auf **Add MDM Server**.



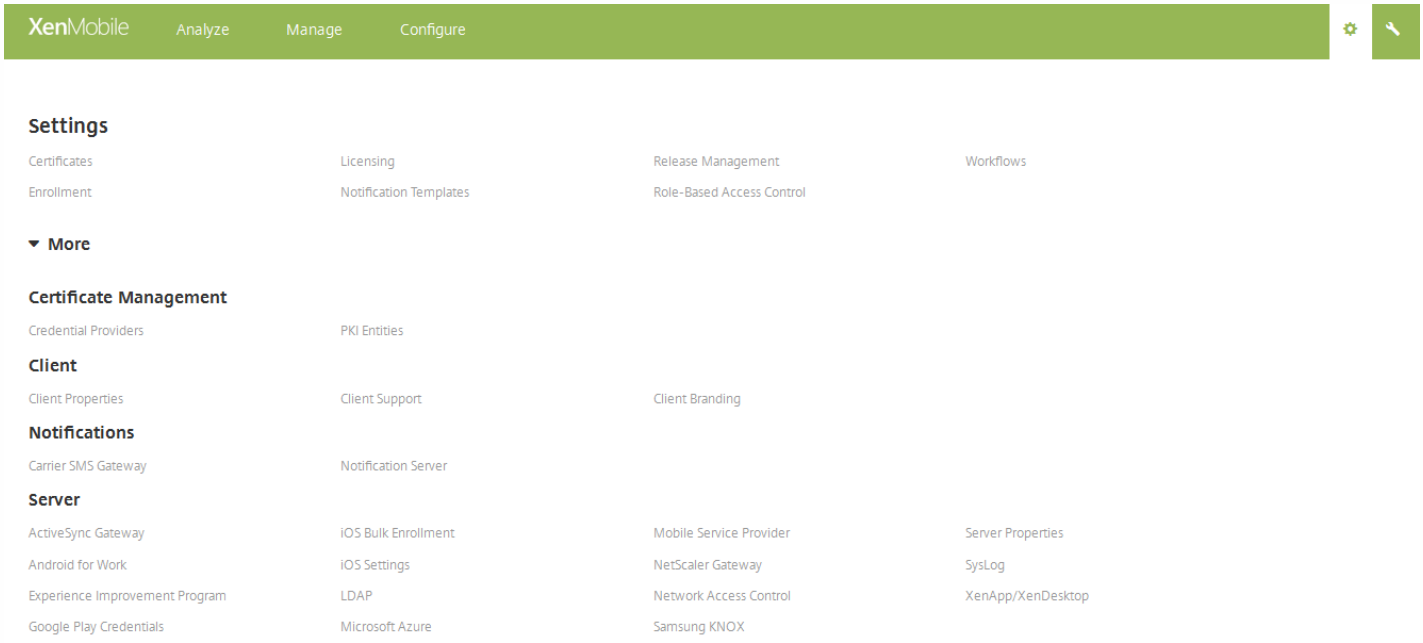
3. Geben Sie im Fenster **Add MDM Server** einen Namen für Ihren XenMobile-Server ein und klicken Sie auf **Next**.



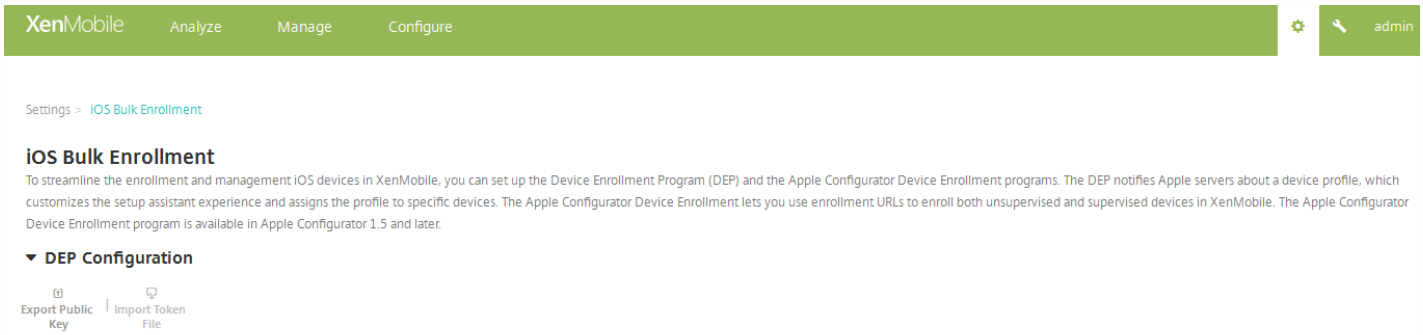
4. Laden Sie einen öffentlichen Schlüssel vom XenMobile-Server hoch. Generieren des Schlüssels in XenMobile:

   a. Melden Sie sich an der XenMobile-Konsole an und klicken Sie auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

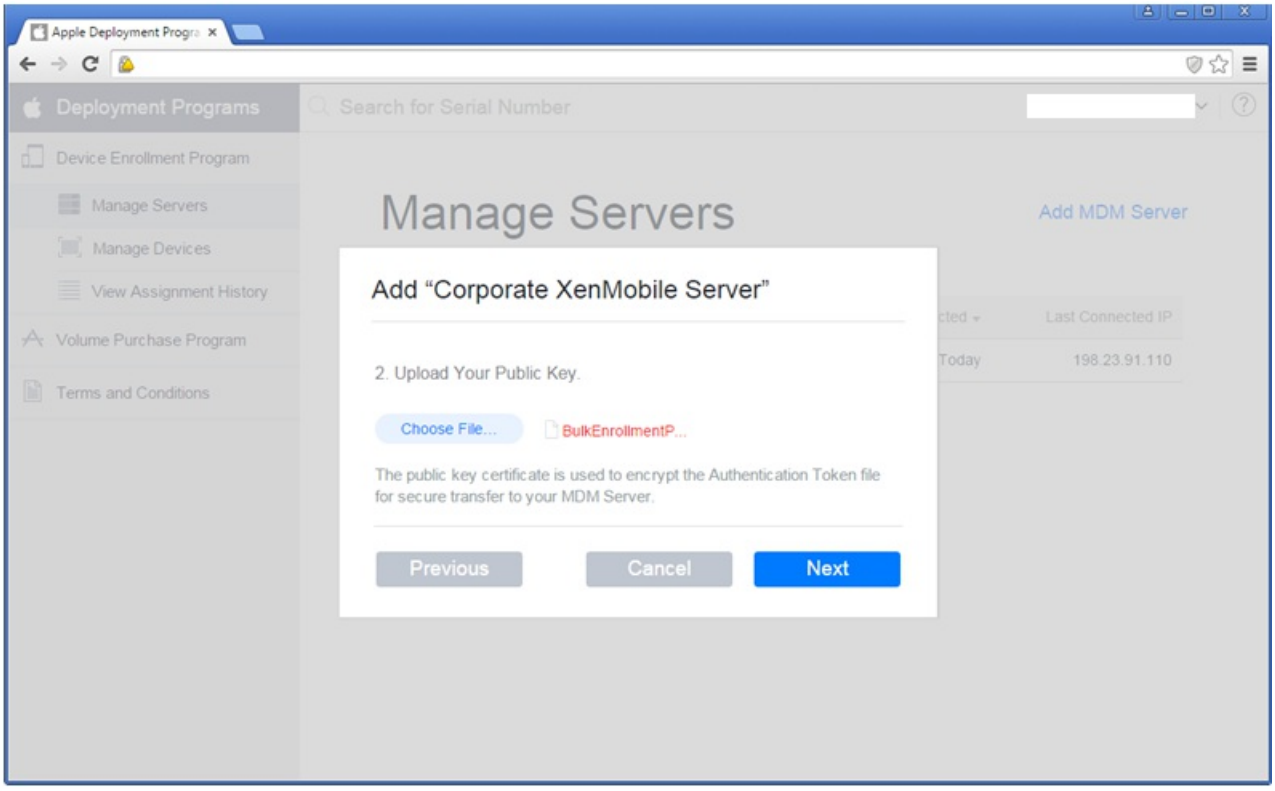
   b. Klicken Sie unter **Mehr** auf **iOS-Massenregistrierung**.



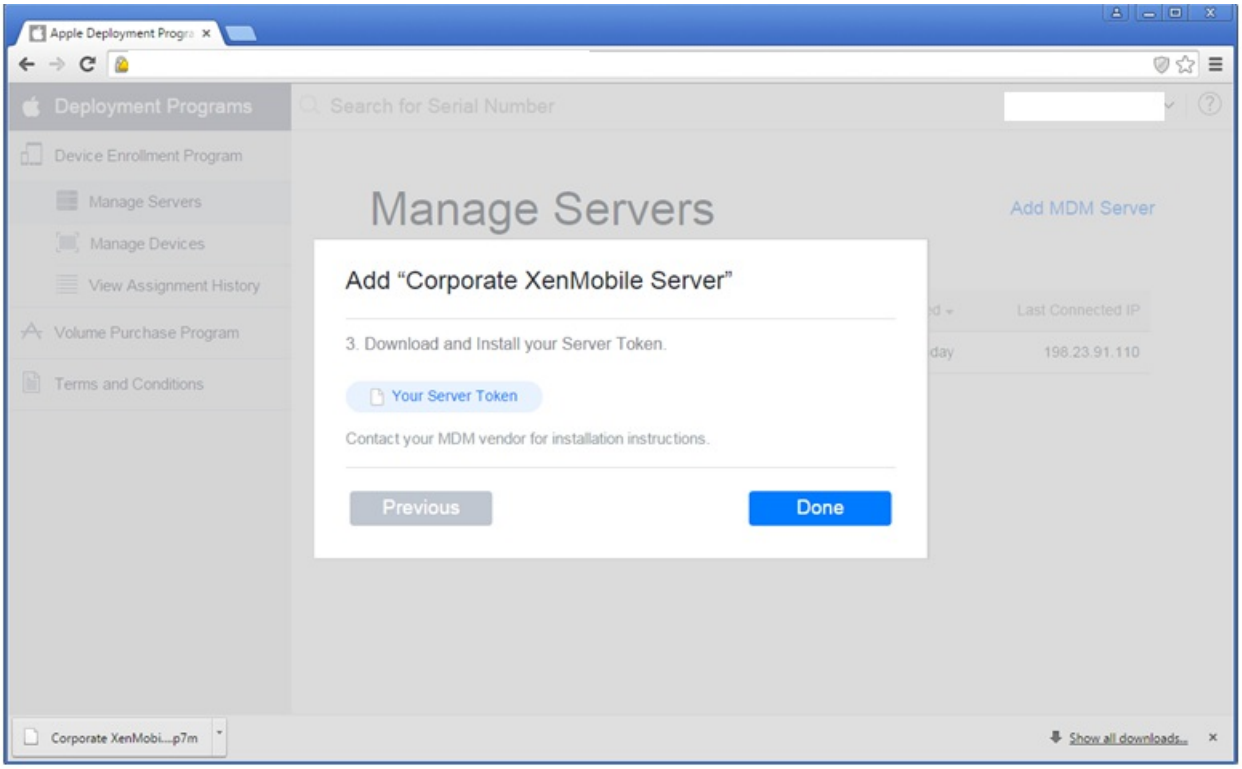
b. Erweitern Sie **DEP-Konfiguration** auf der Seite **iOS-Massenregistrierung** und klicken Sie auf **Öffentlichen Schlüssel exportieren**. Der öffentliche Schlüssel wird heruntergeladen.



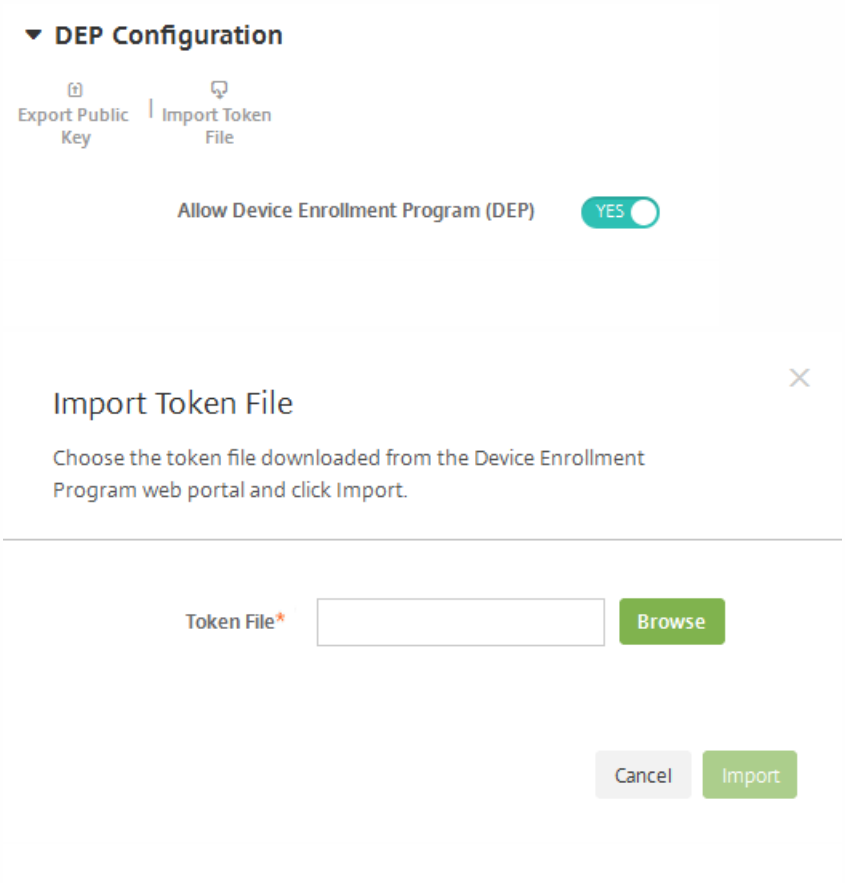
5. Klicken Sie im Apple DEP-Portal auf **Choose file**, wählen Sie den öffentlichen Schlüssel, den Sie heruntergeladen haben, und klicken Sie dann auf **Next**.



6. Klicken Sie auf **Your Server Token**, um einen Servertoken zu generieren, der vom Browser heruntergeladen wird, und klicken Sie dann auf **Done**.

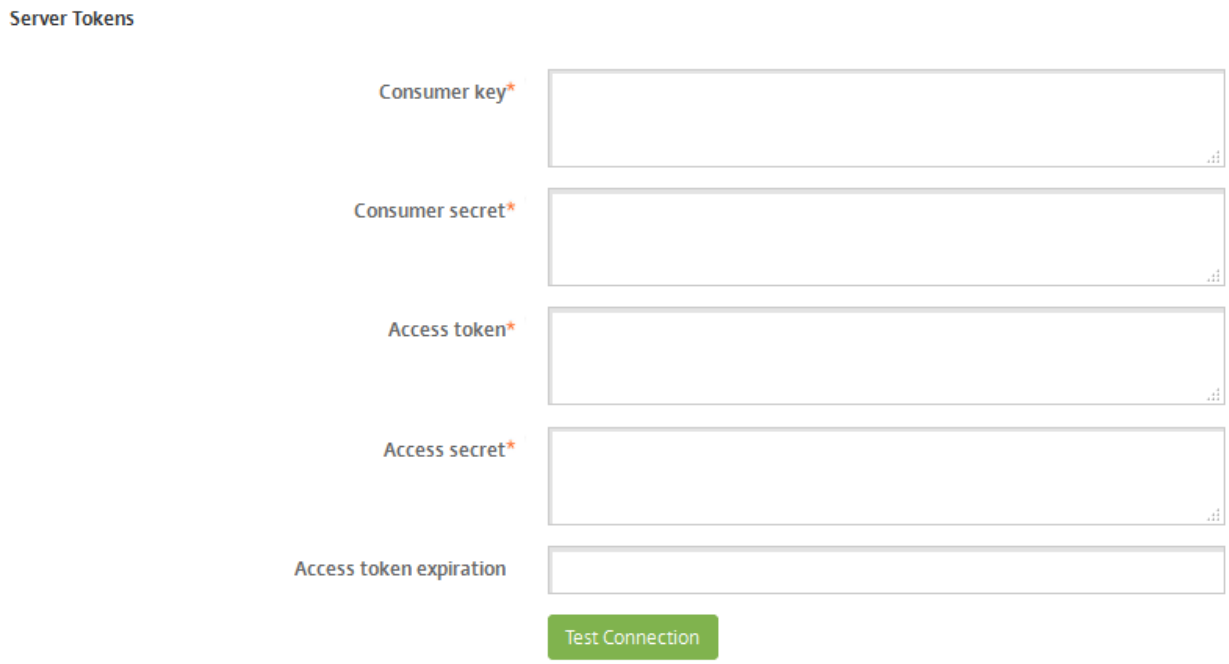


7. Klicken Sie in der XenMobile-Konsole auf der Seite **iOS-Massenregistrierung** neben **Device Enrollment Program (DEP) zulassen** auf "Ja", klicken Sie dann auf **Tokendatei importieren** und laden Sie die Tokendatei hoch, die Sie im vorherigen Schritt heruntergeladen haben.



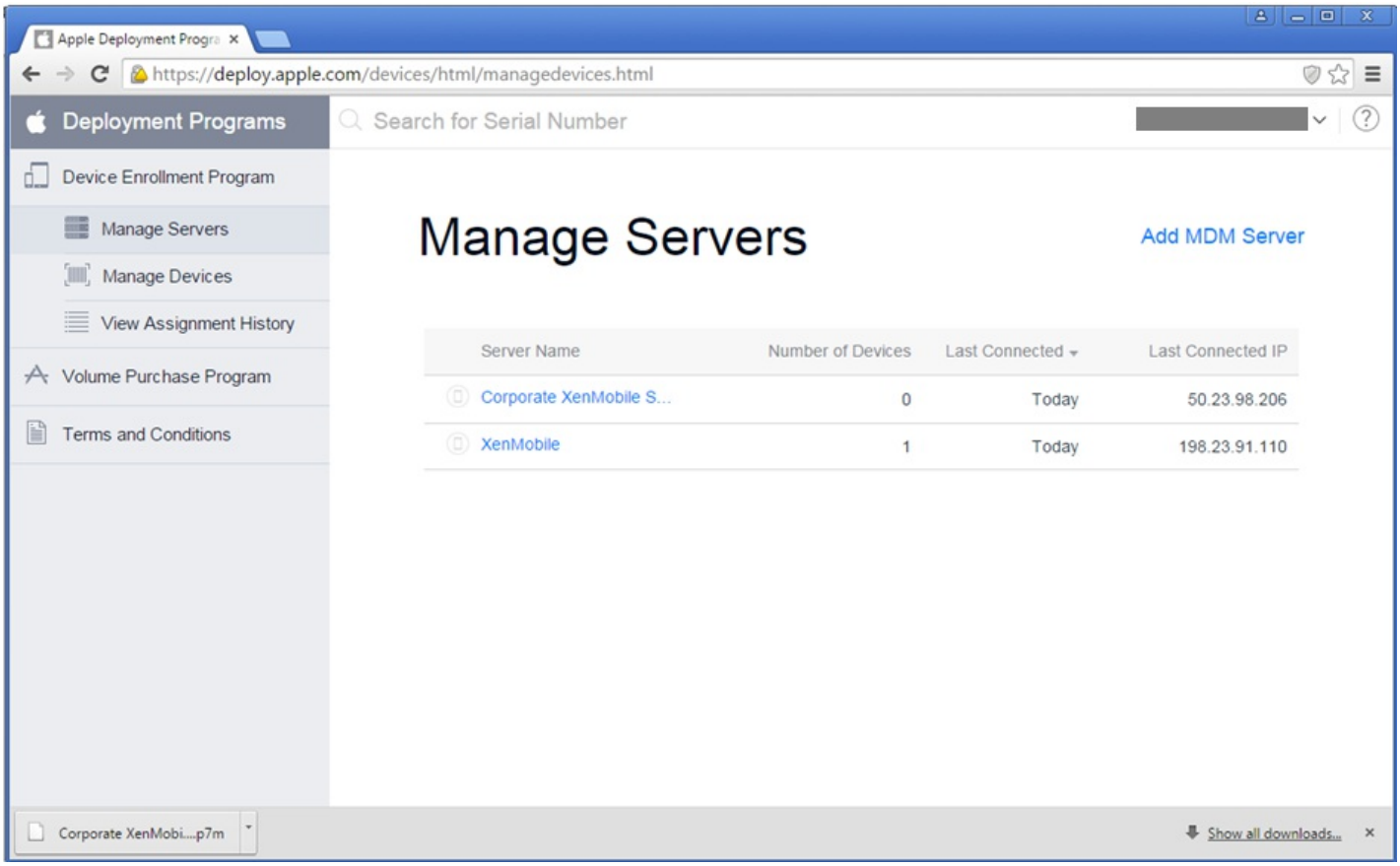
Nach dem Import der Tokendatei werden Ihre Apple DEP-Tokeninformationen in der XenMobile-Konsole angezeigt.

8. Klicken Sie auf **Test Connection**, um die Verbindung zwischen Apple DEP und XenMobile zu überprüfen.



9. Legen Sie auf der Seite **iOS Bulk Enrollment** die zusätzlichen Einstellungen fest, wählen Sie die Apple DEP-Steuerelemente und -Richtlinien aus, die Sie für die Apple DEP-Geräte implementieren möchten, und klicken Sie auf **Save**.

Der XenMobile-Server wird im Apple DEP-Portal angezeigt.



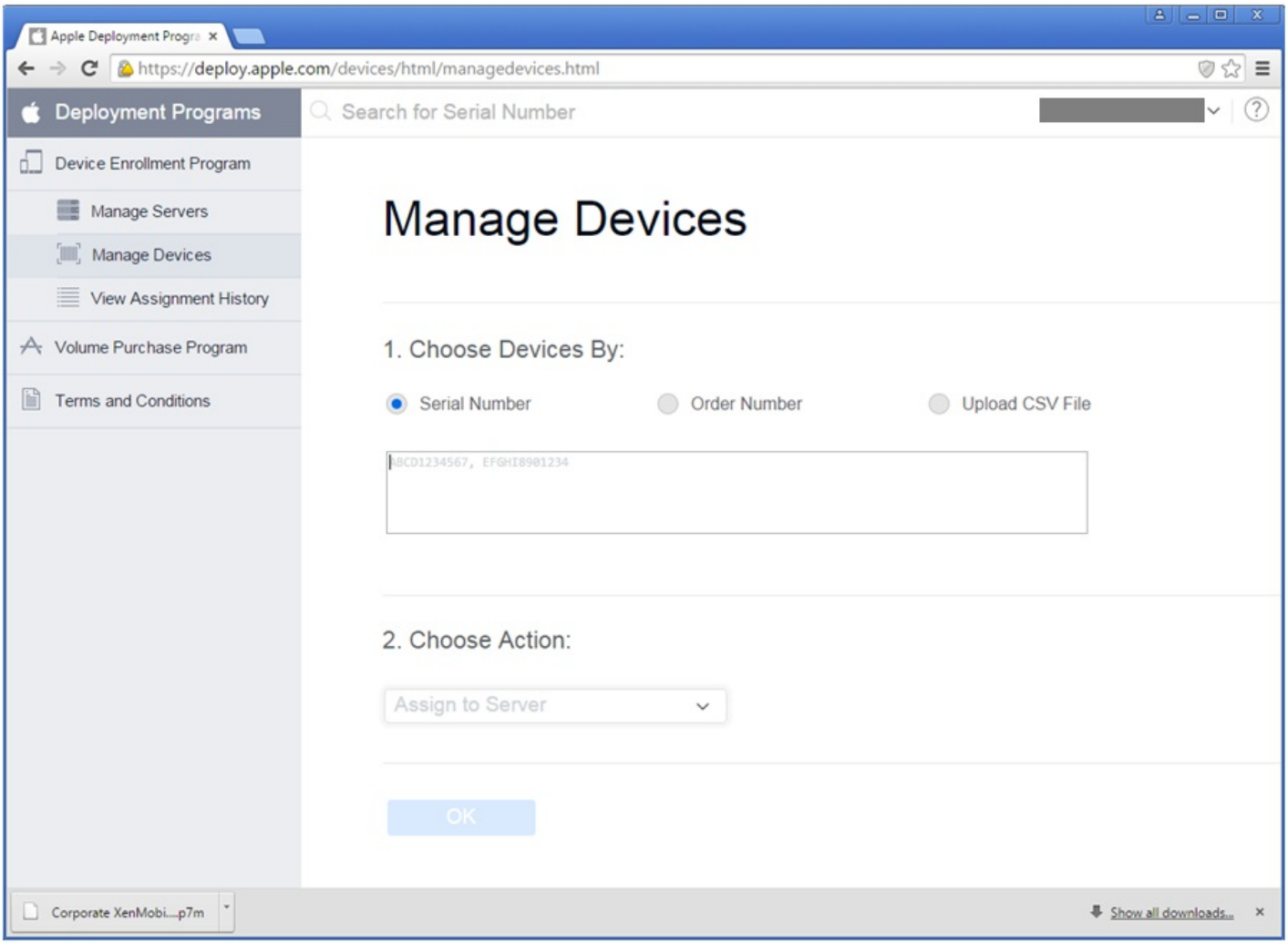
Sie können DEP-aktivierte Geräte direkt bei Apple oder für DEP autorisierten Wiederverkäufern und Netzbetreibern bestellen. Wenn Sie bei Apple bestellen, müssen Sie Ihre Apple Kunden-ID im Apple DEP-Portal angeben, damit Apple das gekaufte Gerät Ihrem Apple DEP-Konto zuordnen kann.

Wenn Sie bei einem Wiederverkäufer oder Netzbetreiber bestellen, fragen Sie Ihren Apple Wiederverkäufer oder Netzbetreiber, ob sie am Apple DEP teilnehmen. Fragen Sie beim Kauf der Geräte nach der Apple DEP-ID des Wiederverkäufers. Sie benötigen diese Informationen, um Ihren Apple DEP-Wiederverkäufer Ihrem Apple DEP-Konto hinzuzufügen. Wenn Sie die Apple DEP-ID des Wiederverkäufers hinzugefügt haben, erhalten Sie bei Genehmigung eine DEP-Kunden-ID. Geben Sie die DEP-Kunden-ID an den Wiederverkäufer weiter, der mit der ID Informationen über die von Ihnen gekauften Geräte an Apple übermittelt. Weitere Informationen finden Sie auf der Website von Apple.

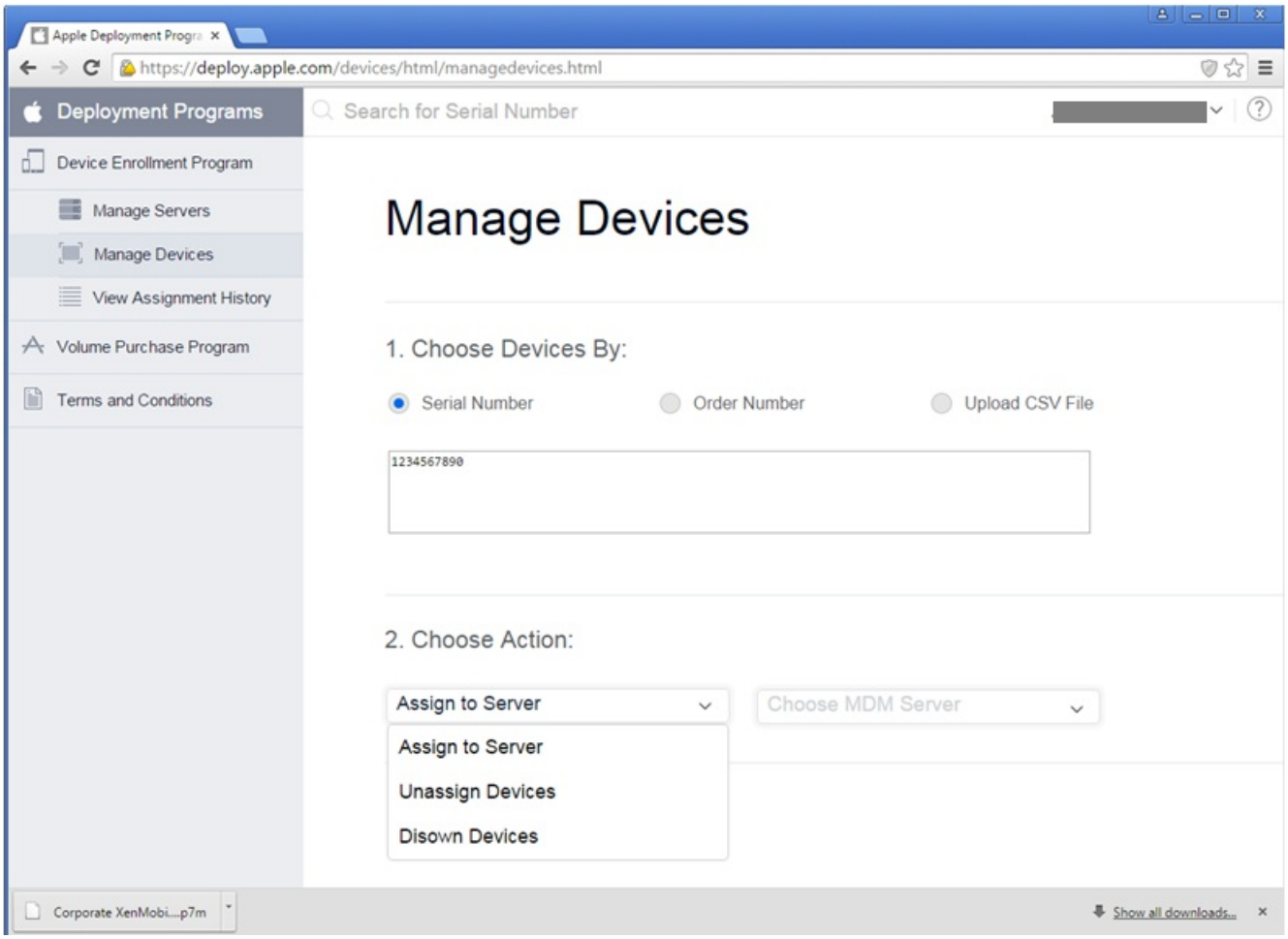
Mit den folgenden Schritten ordnen Sie Geräte in Ihrem Apple DEP-Konto über das DEP-Portal Ihrem XenMobile-Server zu.

1. Melden Sie sich beim Apple DEP-Portal an.

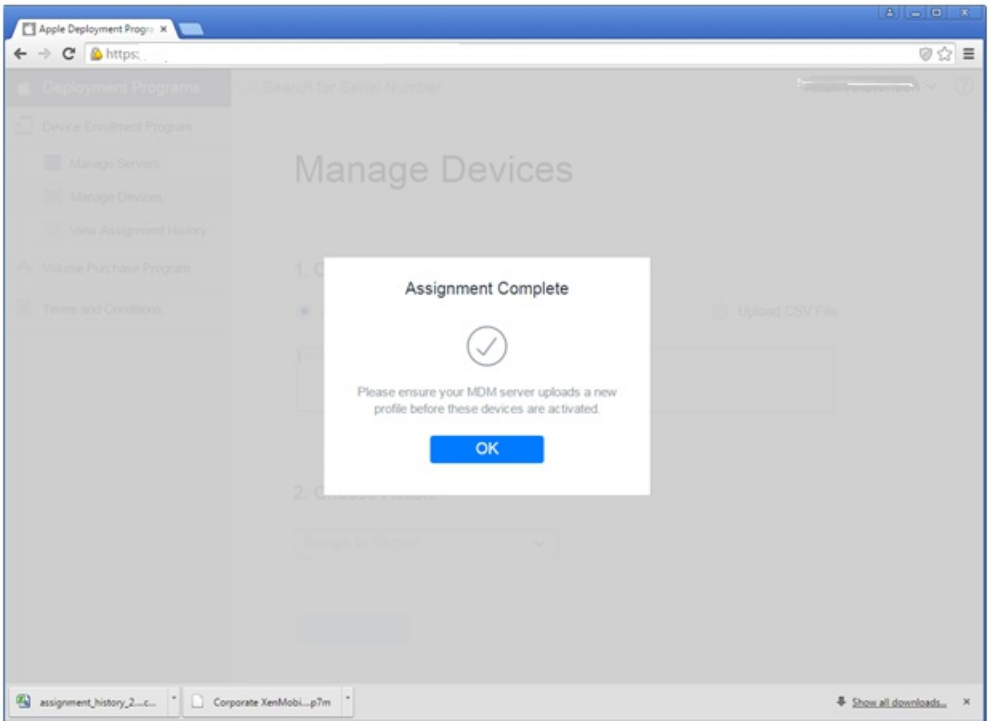
2. Klicken Sie auf **Device Enrollment Program**, klicken Sie auf **Manage Devices** und wählen Sie dann in **Choose Devices By** die Option aus, für die Sie Ihre Apple DEP-aktivierten Geräte hochladen und definieren möchten: **Serial Number**, **Order Number** oder **Upload CSV File**.



3. Zum Zuweisen der Geräte zu einem XenMobile-Server klicken Sie unter **Choose Action** auf **Assign to Server**, klicken Sie dann in der Liste auf den Namen Ihres XenMobile-Servers und dann auf **OK**.



Ihre Apple DEP-Geräte sind nun dem ausgewählten XenMobile-Server zugewiesen.



Benutzer registrieren ein Apple DEP-aktiviertes Gerät mit den folgenden Schritten.

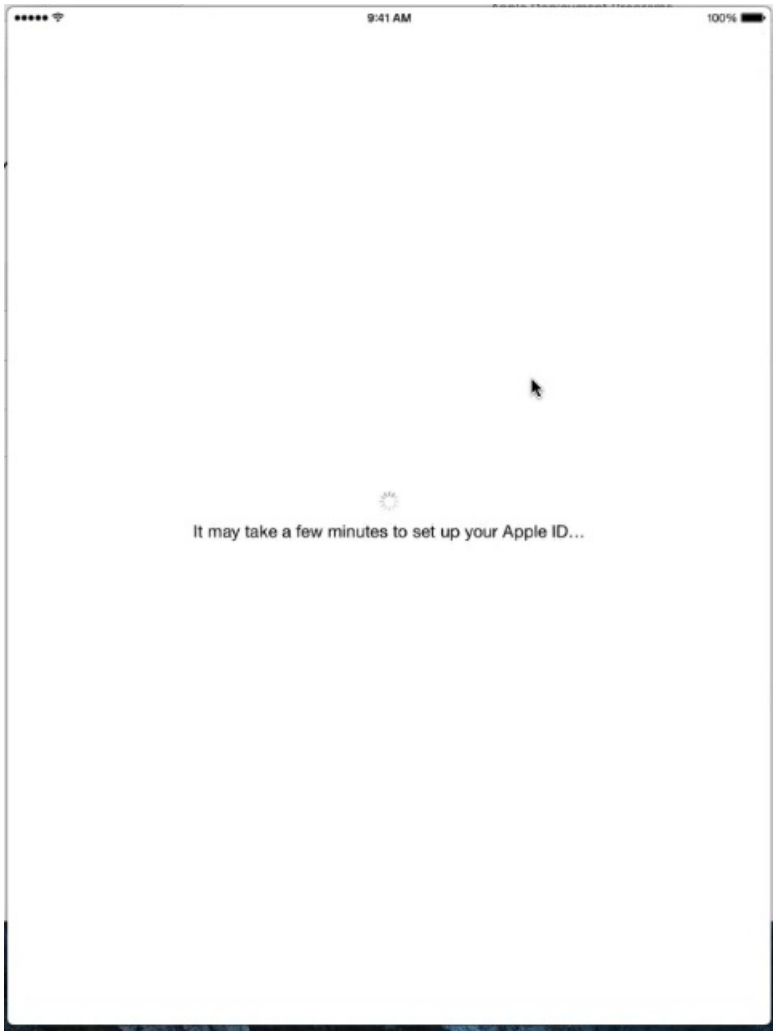
1. Benutzer starten ihr Apple DEP-aktiviertes Gerät.

2. Mit dem Konfigurationsassistenten konfigurieren Benutzer die Anfangseinstellungen auf ihrem iOS-Gerät.

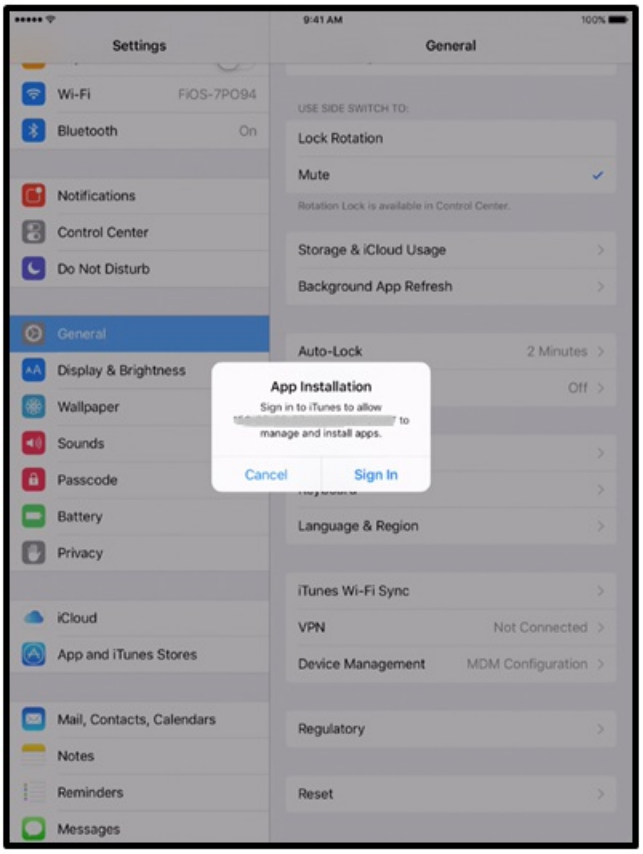
3. Das Gerät startet automatisch die XenMobile-Geräteregistrierung. Der Assistent führt Benutzer durch die Registrierung des Geräts beim XenMobile-Server, der dem Apple DEP-aktivierten Gerät zugeordnet ist.

Der Apple DEP-Registrierungsvorgang beginnt automatisch als Teil der iOS-Erstkonfiguration für Apple DEP-aktivierte Geräte.

4. Die Apple DEP-Konfiguration, die Sie in der XenMobile-Konsole konfiguriert haben, wird für das Apple DEP-aktivierte Gerät bereitgestellt. Der Assistent führt die Benutzer durch die Konfiguration des Geräts.



5. Benutzer werden u. U. aufgefordert, sich bei iTunes anzumelden, sodass Worx Home heruntergeladen werden kann.



6. Dazu öffnen Benutzer Worx Home und geben ihre Anmeldeinformationen ein. Entsprechend der Richtlinie müssen Benutzer u. U. eine Worx-PIN erstellen und verifizieren.

Die übrigen erforderlichen Apps werden per Push auf dem Gerät bereitgestellt.

iOS-Programm für Volumenlizenzen

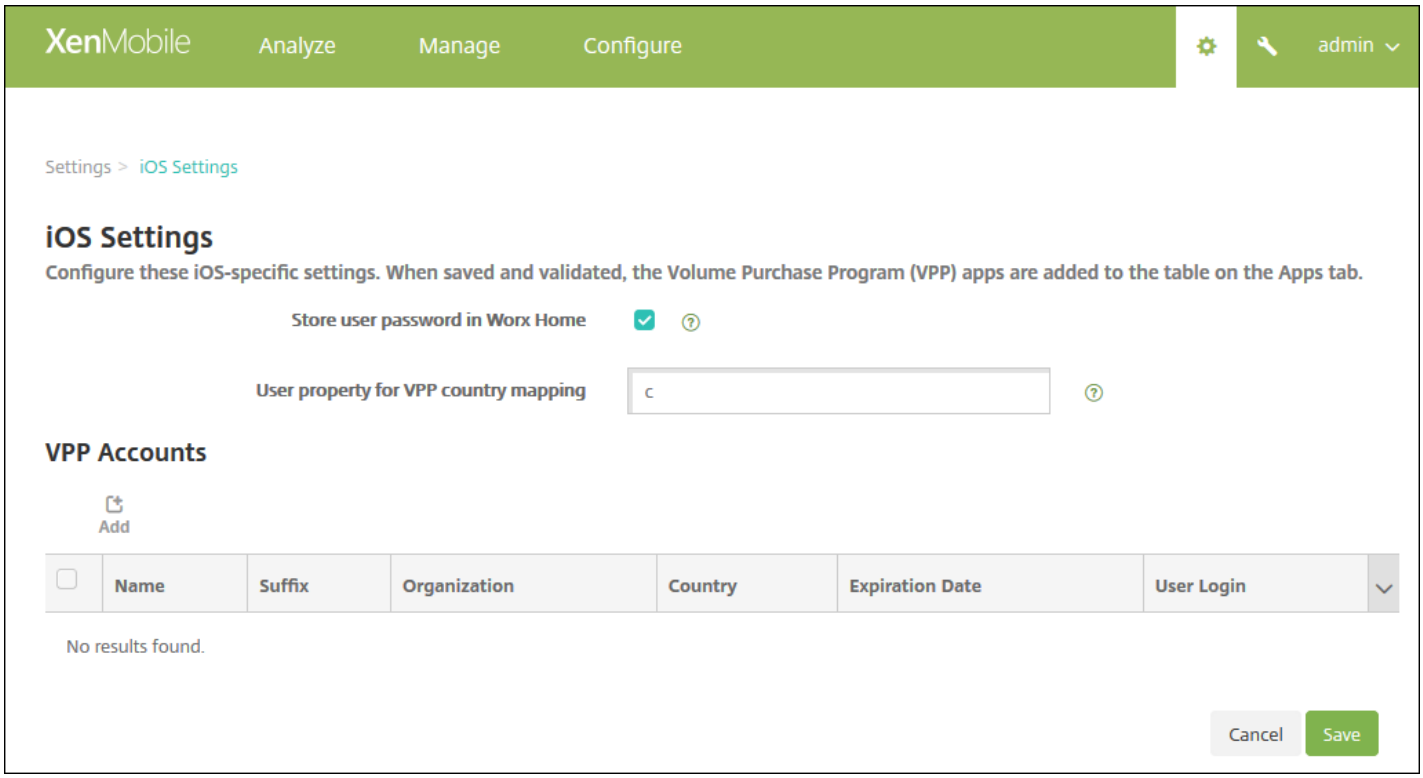
Jul 28, 2016

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.

1. Klicken Sie in der XenMobile-Webkonsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **iOS-Einstellungen**. Die Seite **iOS-Einstellungen** wird angezeigt.



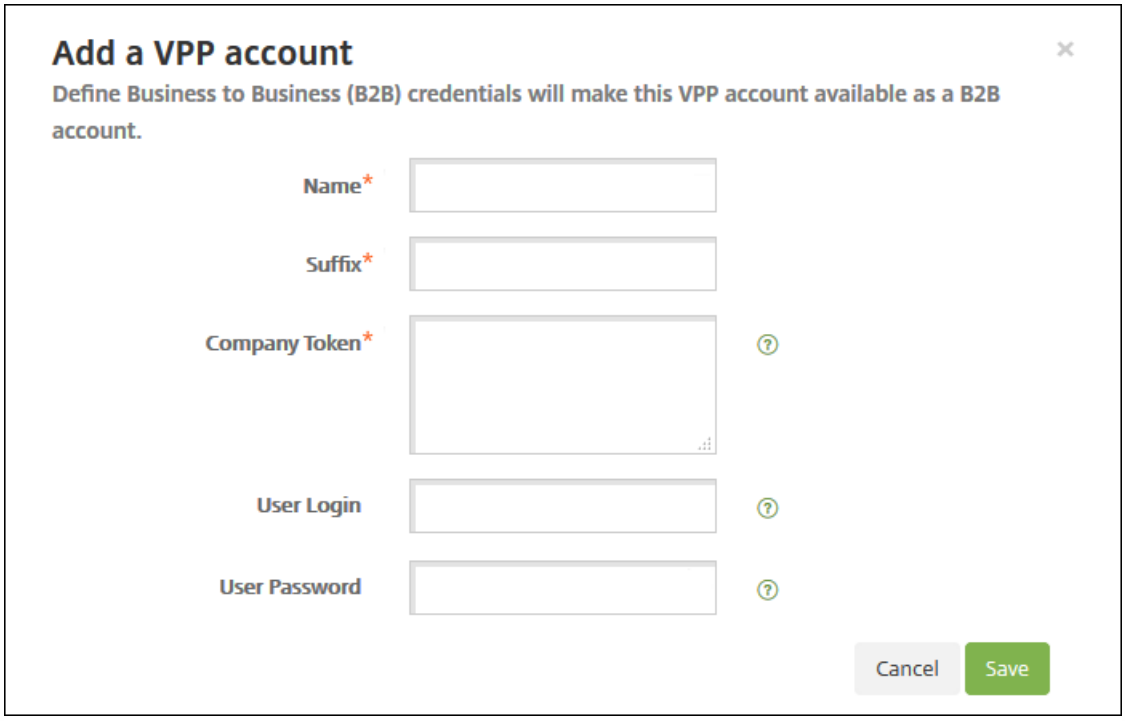
3. Konfigurieren Sie die folgenden Einstellungen:

- **Benutzerkennwort in Worx Home speichern**: Wählen Sie aus, ob ein Benutzername mit Kennwort in Worx Home für die XenMobile-Authentifizierung gespeichert werden soll. Standardmäßig werden die Anmeldeinformationen gespeichert.
- **Benutzereigenschaft für VPP-Länderzuordnung**: Geben Sie 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.

VPP-Konten

- Klicken Sie für jedes VPP-Konto, das Sie hinzufügen möchten, auf **Hinzufügen**. Das Dialogfeld **VPP-Konto hinzufügen** wird angezeigt.



Konfigurieren Sie folgende Einstellungen für jedes hinzugefügte Konto:

- **Name**: Geben Sie einen Namen für das VPP-Konto ein.
- **Suffix**: Geben Sie das für Apps Suffix ein, die über das VPP-Konto erworben wurden.
- **Unternehmenstoken**: Geben Sie das von Apple erhaltene VPP-Diensttoken ein oder kopieren Sie es und fügen Sie es ein. Zum Anfordern des Tokens klicken Sie auf der Seite mit der Kontoübersicht im Apple-VPP-Portal auf die Schaltfläche "Herunterladen" zum Erstellen und Herunterladen der VPP-Datei. Die Datei enthält das Diensttoken und andere Informationen wie etwa den Ländercode und das Ablaufdatum. Speichern Sie die Datei in einem sicheren Speicherort.
- **Benutzeranmeldung**: Geben Sie optional den Benutzernamen eines autorisierten VPP-Kontos an.
- **Benutzerkennwort**: Geben Sie optional ein Benutzerkennwort des VPP-Kontos an.

5. Klicken Sie auf **Speichern**, um das Dialogfeld zu schließen.

6. Klicken Sie auf **Speichern**, um die iOS-Einstellungen zu speichern.

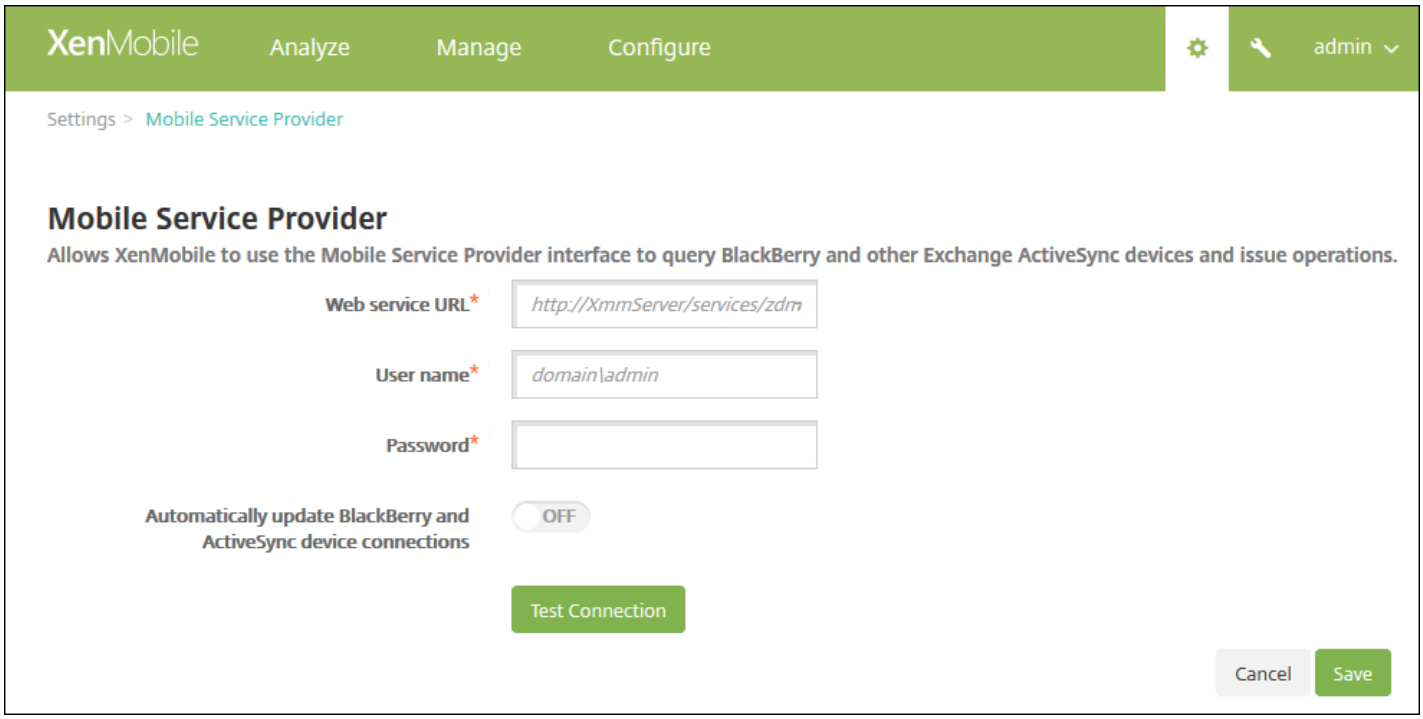
Mobilfunkanbieter

Jul 28, 2016

Sie können XenMobile für die Verwendung der Mobilfunkanbieter-Schnittstelle zum Abfragen von BlackBerry- und anderen Exchange ActiveSync-Geräten und Auslösen von Vorgängen konfigurieren.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **Mobilfunkanbieter**. Die Seite **Mobilfunkanbieter** wird angezeigt.



3. Konfigurieren Sie die folgenden Einstellungen:

- Geben Sie unter **Webdienst-URL** die URL des Webdiensts ein, z. B. http://XmmServer/services/xdmservice.
- Benutzername: Geben Sie den Benutzernamen im Format "domäne\admin" ein.
- **Kennwort**: Geben Sie das Kennwort ein.
- **Automatisch BlackBerry- und ActiveSync-Geräteverbindungen aktualisieren**: Wählen Sie aus, ob Geräteverbindungen automatisch aktualisiert werden sollen. Der Standardwert ist **EIN**.
- Klicken Sie auf **Verbindung testen**, um die Verbindung zu prüfen.

4. Klicken Sie auf **Speichern**.

Netzwerkzugriffssteuerung (NAC)

Jul 28, 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:

Anonyme Geräte: 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.

Samsung KNOX-Nachweisfehler: Prüft, ob bei einem Gerät die Abfrage des Samsung KNOX-Nachweisservers fehlgeschlagen ist.

Unzulässige Apps: Prüft, ob ein Gerät unzulässige Apps aufweist, die in einer App-Zugriffsrichtlinie definiert sind.

Implizit zulassen oder verweigern: 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 "Implizit zulassen".

Inaktive Geräte: Prüft, ob ein Gerät entsprechend dem unter "Schwellenwert für Tage inaktiv" in den Servereigenschaften festgelegten Wert inaktiv ist.

Fehlende Pflicht-Apps: Prüft, ob auf einem Gerät Apps fehlen, die in einer App-Zugriffsrichtlinie definiert sind.

Nicht empfohlene Apps: Prüft, ob ein Gerät nicht empfohlene Apps aufweist, die in einer App-Zugriffsrichtlinie definiert sind.

Nicht richtlinientreues Kennwort: 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.

Nicht richtlinientreue Geräte: 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.

Widerrufenstatus: Prüft, ob das Gerätezertifikat widerrufen worden ist. Ein widerrufenes Gerät kann erst erneut registriert werden, wenn es wieder autorisiert ist.

Android-Geräte mit Rooting oder iOS-Geräte mit Jailbreak: Prüft, ob auf einem Android- oder iOS-Gerät ein Jailbreak vorliegt.

Nicht verwaltete Geräte: 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.

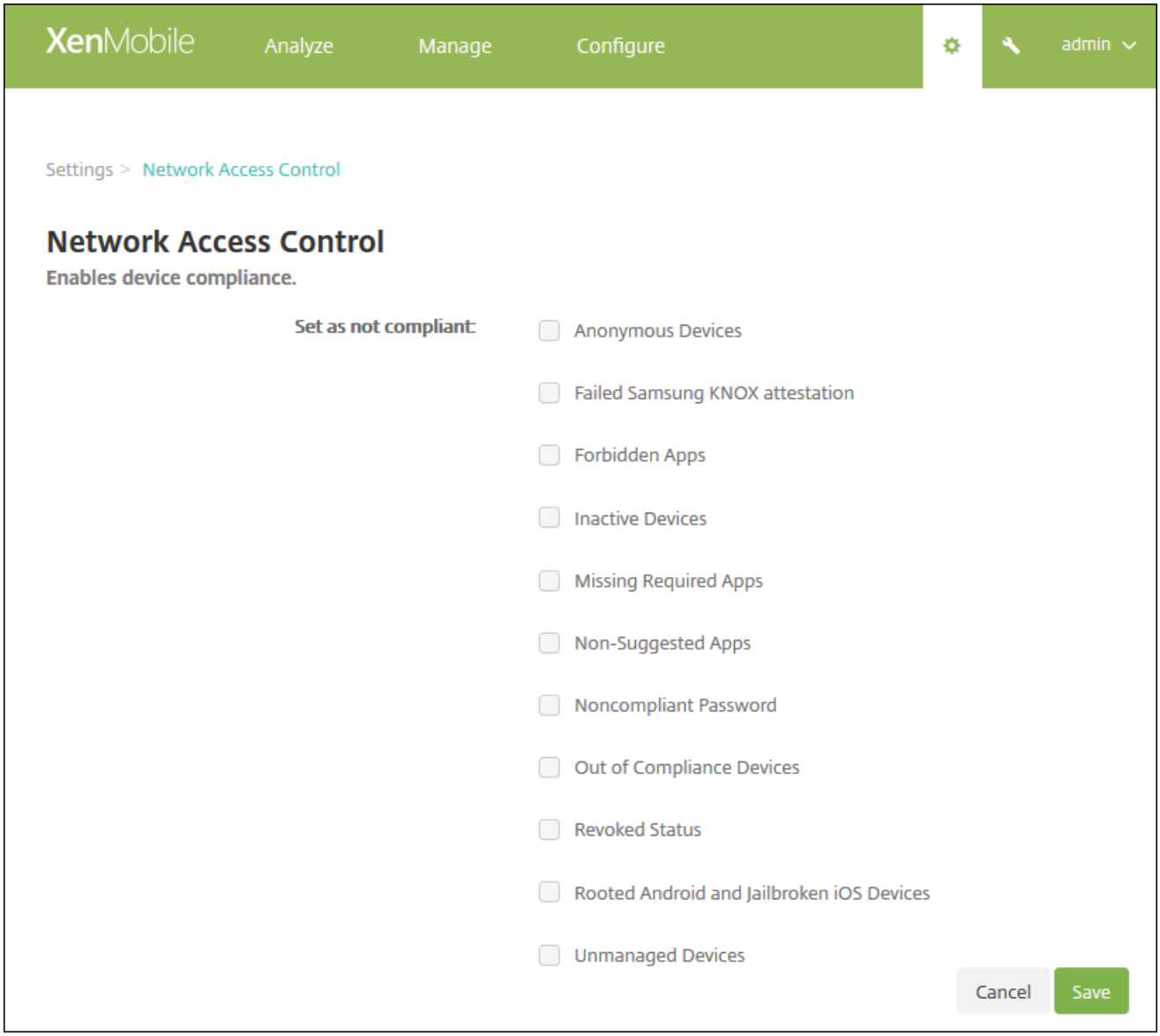
Android-Domänenbenutzer an ActiveSync-Gateway senden: Klicken Sie auf **JA**, damit XenMobile Android-Geräteinformationen an das ActiveSync-Gateway sendet. Durch Aktivieren dieser Option wird sichergestellt, dass XenMobile Android-Geräteinformationen an das ActiveSync-Gateway für den Fall sendet, dass 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.

Konfigurieren der Netzwerkzugriffssteuerung

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **Netzwerkzugriffssteuerung**. Die Seite **Netzwerkzugriffssteuerung** wird angezeigt.



3. Aktivieren Sie die Kontrollkästchen für die gewünschten Filter unter **Als nicht richtlinientreu einstellen**.

4. Klicken Sie auf **Speichern**.

Samsung KNOX

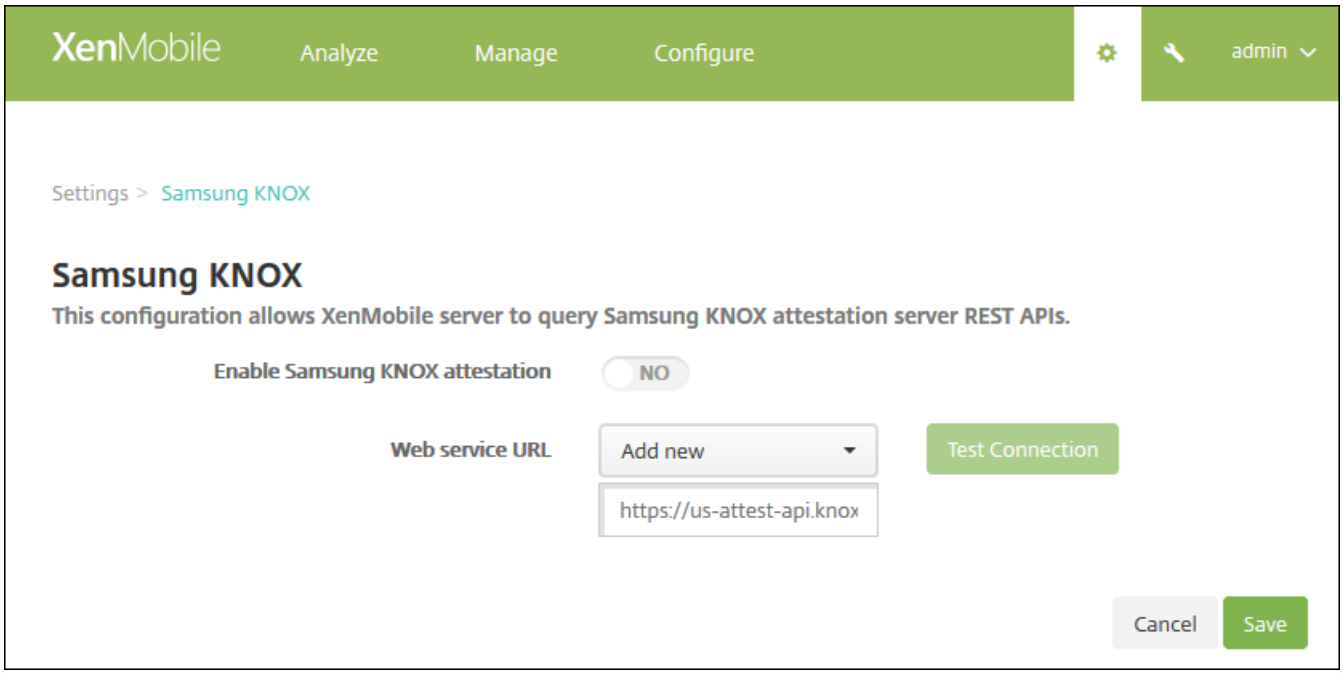
Jul 28, 2016

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.

1. Klicken Sie in der XenMobile-Webkonsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **Samsung KNOX**. Die Seite **Samsung KNOX** wird angezeigt.



3. Konfigurieren Sie die folgenden Einstellungen:

- **Samsung KNOX-Nachweis aktivieren**: Wählen Sie aus, ob der Samsung KNOX-Nachweis aktiviert werden soll. Der Standardwert ist **NEIN**. Wenn Sie **Samsung KNOX-Nachweis aktivieren** aktivieren, wird die Option **Webdienst-URL** aktiviert.
- Wählen Sie in der Liste den gewünschten Nachweisserver aus.

4. Klicken Sie auf **Verbindung testen**, um die Verbindung zu prüfen.

5. Klicken Sie auf **Speichern**.

> ## Hinweis
>
> Verwenden Sie Samsung KNOX Mobile Enrollment, um mehrere Samsung KNOX-Geräte in XenMobile (oder einem beliebigen Manager für mobile Geräte) zu registrieren, ohne Geräte einzeln manuell zu konfigurieren. Weitere Informationen finden Sie unter

Samsung KNOX Massenregistrierung.

Erstellen, Bearbeiten und Löschen von Servereigenschaften

Jul 28, 2016

XenMobile bietet über 100 Eigenschaften für serverweite Vorgänge. In diesem Abschnitt werden einige der wichtigsten Servereigenschaften und Informationen zum Hinzufügen, Bearbeiten und Löschen von Servereigenschaften erläutert.

Servereigenschaften – Definitionen

Ausführungszeit der Auditprotokollbereinigung

Die Startzeit der Auditprotokollbereinigung im Format HH:MM AM/PM. Beispiel: 04:00 AM. Standardwert: **02:00 AM**.

Auditprotokoll-Bereinigungsintervall (Tage)

Die Anzahl der Tage, die der XenMobile-Server das Auditprotokoll aufbewahrt. Standardwert: **1**.

Auditprotokollierung

Beim Einstellen von **Falsch** werden Benutzeroberflächenereignisse nicht erfasst. Der Standardwert ist **Falsch**.

Auditprotokollaufbewahrung (Tage)

Die Anzahl der Tage, die der XenMobile-Server das Auditprotokoll aufbewahrt. Standardwert: **7**.

Bereitstellungsprotokollbereinigung (Tage)

Die Anzahl der Tage, die der XenMobile-Server das Bereitstellungsprotokoll aufbewahrt. Standardwert: **7**.

Deaktivieren der SSL-Serverüberprüfung

Beim Einstellen von **Wahr** wird die SSL-Serverzertifikatüberprüfung deaktiviert, wenn alle folgenden Bedingungen zutreffen: Sie haben die zertifikatbasierte Authentifizierung auf dem XenMobile-Server aktiviert, der Microsoft-Zertifizierungsstellenserver ist der Zertifikataussteller und das Zertifikat wurde von einer internen Zertifizierungsstelle signiert, deren Stammzertifikat der XenMobile-Server nicht vertraut. Die Standardeinstellung ist **Wahr**.

Inaktivitätstimeout in Minuten

Die Anzahl der Minuten, nach denen ein inaktiver Administrator abgemeldet wird, der mit der öffentlichen API des XenMobile-Servers auf die XenMobile-Konsole oder eine Drittanbieteranwendung zugreift. Ein Timeoutwert von **0** bedeutet, dass ein inaktiver Benutzer angemeldet bleibt. Standardwert: **5**.

Single Sign-On für NetScaler

Beim Einstellen von **Falsch** ist das Rückruffeature von XenMobile während des Single Sign-Ons von NetScaler zum XenMobile-Server deaktiviert. Mit dem Rückruffeature wird die NetScaler Gateway-Sitzungs-ID überprüft, wenn die NetScaler Gateway-Konfiguration eine Rückruf-URL enthält. Der Standardwert ist **Falsch**.

Sitzungsprotokollbereinigung (Tage)

Die Anzahl der Tage, die der XenMobile-Server das Sitzungsprotokoll aufbewahrt. Standardwert: **7**.

Nicht authentifizierter App-Download für Android-Geräte

Beim Einstellen von **Wahr** können Sie selbstgehostete Apps auf Android-Geräte herunterladen, auf denen Android for Work ausgeführt wird. Diese Eigenschaft ist erforderlich, wenn in Android for Work die Option zum Bereitstellen einer statischen Download-URL im Google Play Store aktiviert ist. In diesem Fall dürfen Download-URLs kein Einmalticket (durch die Servereigenschaft **XAM-Einmalticket** definiert) umfassen, das den Authentifizierungstoken enthält. Der Standardwert ist **Falsch**.

Nicht authentifizierter App-Download für Windows-Geräte

Wird nur für ältere Versionen von Worx Home verwendet, die Einmaltickets nicht validieren. Beim Einstellen von **Falsch** können Sie nicht authentifizierte Apps von XenMobile auf Windows-Geräte herunterladen. Der Standardwert ist **Falsch**.

XAM-Einmalticket

Die Anzahl Millisekunden, die ein Einmalauthentifizierungstoken für den Download einer App gültig ist. Diese Eigenschaft wird zusammen mit den Eigenschaften **Nicht authentifizierter App-Download für Android-Geräte** und **Nicht authentifizierter App-Download für Windows-Geräte** verwendet, die festlegen, ob nicht authentifizierte App-Downloads zulässig sind. Standardwert: **3600000**.

Maximales Inaktivitätsintervall (in Minuten) für das XenMobile MDM-Selbsthilfeportal

Die Anzahl der Minuten, nach denen ein inaktiver Benutzer vom XenMobile-Selbsthilfeportal abgemeldet wird. Ein Timeoutwert von **0** bedeutet, dass ein inaktiver Benutzer angemeldet bleibt. Standardwert: **30**.

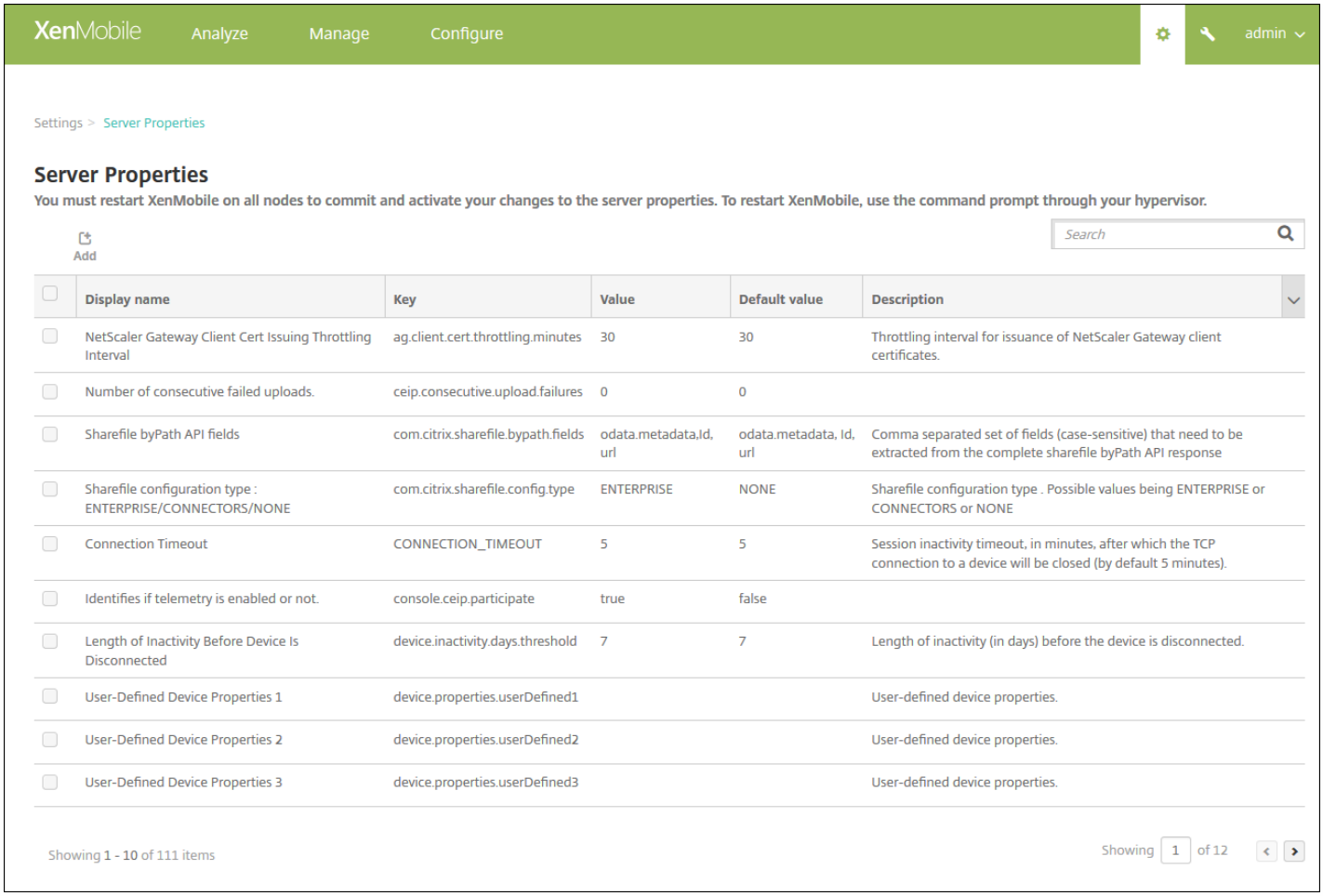
Hinzufügen, Bearbeiten oder Löschen von Servereigenschaften

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.

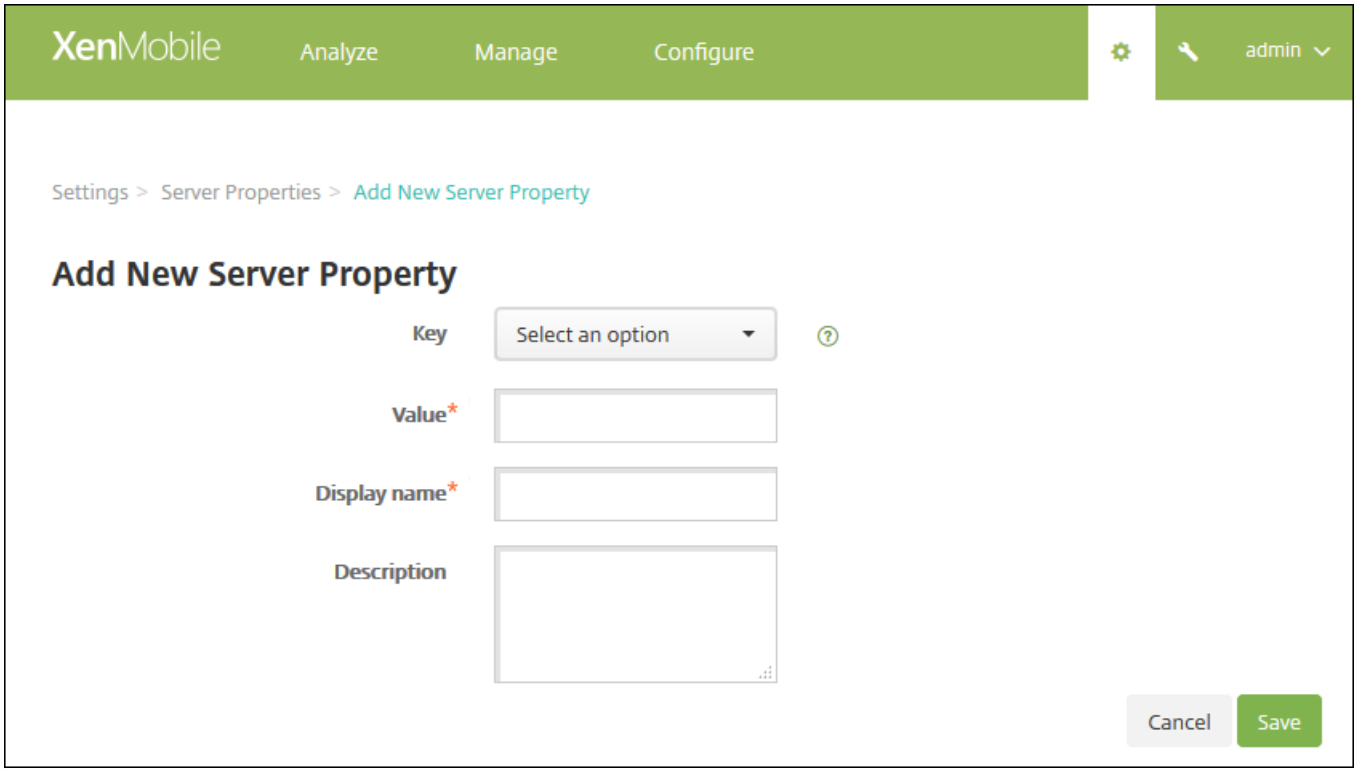
1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **Servereigenschaften**. Die Seite **Servereigenschaften** wird angezeigt. Auf dieser Seite können Sie Servereigenschaften hinzufügen, bearbeiten und löschen.



Hinzufügen von Servereigenschaften

1. Klicken Sie auf **Hinzufügen**. Die Seite **Neue Servereigenschaft hinzufügen** wird angezeigt.



2. Konfigurieren Sie die folgenden Einstellungen:

- **Schlüssel**: Wählen Sie in der Liste den geeigneten Schlüssel aus. Bei Schlüsseln wird Groß- und Kleinschreibung unterschieden. Bevor Sie Änderungen vornehmen, müssen Sie sich an den Citrix Support wenden oder einen speziellen Schlüssel anfordern.
- **Wert**: Geben Sie einen Wert ein, je nachdem, welchen Schlüssel Sie ausgewählt haben.
- **Anzeigename**: Geben Sie einen Namen für die neue Eigenschaft ein, der in der Tabelle **Servereigenschaften** angezeigt werden soll**.**
- **Beschreibung**: Geben Sie optional eine Beschreibung für die Servereigenschaft ein.

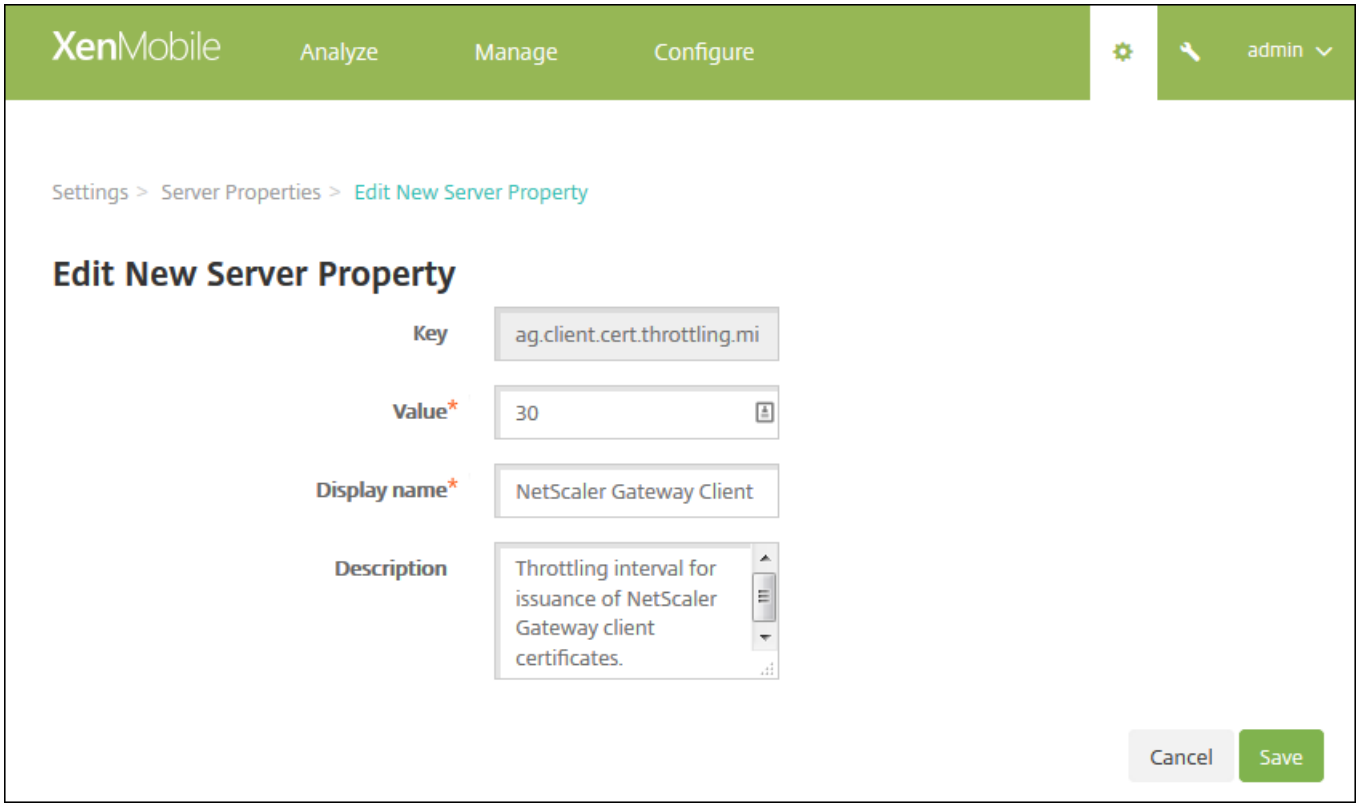
3. Klicken Sie auf **Speichern**.

Bearbeiten von Servereigenschaften

1. Wählen Sie in der Tabelle **Servereigenschaften** die gewünschte Eigenschaft aus.

> **Hinweis:** Wenn Sie das Kontrollkästchen neben einer Servereigenschaft auswählen, wird das Menü mit den Optionen oberhalb der Liste der Servereigenschaften eingeblendet. Wenn Sie auf eine andere Stelle im Eintrag klicken, wird es rechts neben dem Eintrag eingeblendet.

2. Klicken Sie auf **Bearbeiten**. Die Seite **Neue Servereigenschaft bearbeiten** wird angezeigt.



3. Ändern Sie nach Bedarf die folgenden Informationen:

- **Schlüssel**: Sie können dieses Feld nicht ändern.
- **Wert**: Wert der ausgewählten Eigenschaft.
- **Anzeigename**: Name der Eigenschaft.
- **Beschreibung**: Beschreibung der Eigenschaft.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern oder auf **Abbrechen**, um die Eigenschaft unverändert zu lassen.

Löschen von Servereigenschaften

1. Wählen Sie in der Tabelle **Servereigenschaften** die gewünschte Eigenschaft aus.

> **Hinweis:** Sie können mehrere Eigenschaften auswählen, indem Sie die Kontrollkästchen daneben aktivieren.

2. Klicken Sie auf **Löschen**. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie noch einmal auf **Löschen**.

Konfigurieren des effektiven Servermodus in XenMobile

Jul 28, 2016

Der XenMobile-Servermodus ist ein Wert, der unter "Servereigenschaften" festgelegt wird. Sie können den Wert auf MAM, MDM oder ENT festlegen, je nachdem, ob er für Anwendungsverwaltung, Geräteverwaltung oder Anwendungs- und Geräteverwaltung eingestellt wird. Legen Sie die Eigenschaft "Server Mode" entsprechend dem Modus fest, in dem Geräte registriert werden sollen, siehe Tabelle unten. Der Servermodus ist unabhängig vom Lizenztyp standardmäßig auf ENT festgelegt.

Weitere Informationen zum Festlegen des Servermodus finden Sie unter Hinzufügen, Bearbeiten und Löschen von Servereigenschaften.

In der folgenden Tabelle ist aufgeführt, welcher Servermodus für einen bestimmten Lizenztyp und gewünschten Gerätemodus verwendet werden sollte:

Ihre Lizenzen sind für Edition	**Geräte in diesem Modus registrieren**	**Servermodus festlegen auf**
ENT / ADV / MDM	MDM-Modus	MDM
ENT / ADV	MAM-Modus (bzw. ausschließlicher MAM-Modus)	MAM
ENT / ADV	MDM+MAM-Modi	ENT Benutzer, die die Geräteverwaltung ablehnen, verwenden den Legacy-MAM-Modus.

Der *effektive Servermodus* ist eine Kombination aus Lizenztyp und Servermodus. Bei einer MDM-Lizenz ist der effektive Servermodus immer MDM, unabhängig von der Einstellung für den Servermodus. Wenn Sie eine Lizenz für die MDM Edition haben, wird durch Festlegen des Servermodus auf MAM oder ENT die Anwendungsverwaltung nicht aktiviert. Bei Enterprise- und Advanced-Lizenzen ist der effektive Servermodus gleich dem Servermodus.

Der Servermodus wird dem Serverprotokoll jedes Mal hinzugefügt, wenn eine Lizenz aktiviert oder gelöscht wird und wenn der Servermodus unter "Servereigenschaften" geändert wird. Weitere Informationen zum Erstellen und Anzeigen von Protokolldateien finden Sie unter Support und Wartung von XenMobile.

SysLog

Jul 28, 2016

Sie können XenMobile zum Senden von Protokolldateien an einensyslog-Serverkonfigurieren. 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. Administratorereignisse und Benutzerereignisse werden aufgezeichnet.

Sie können den Server zum Sammeln folgender Datentypen konfigurieren:

- Systemprotokolle mit Aktionen, die von XenMobile ausgeführt wurden
- 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:

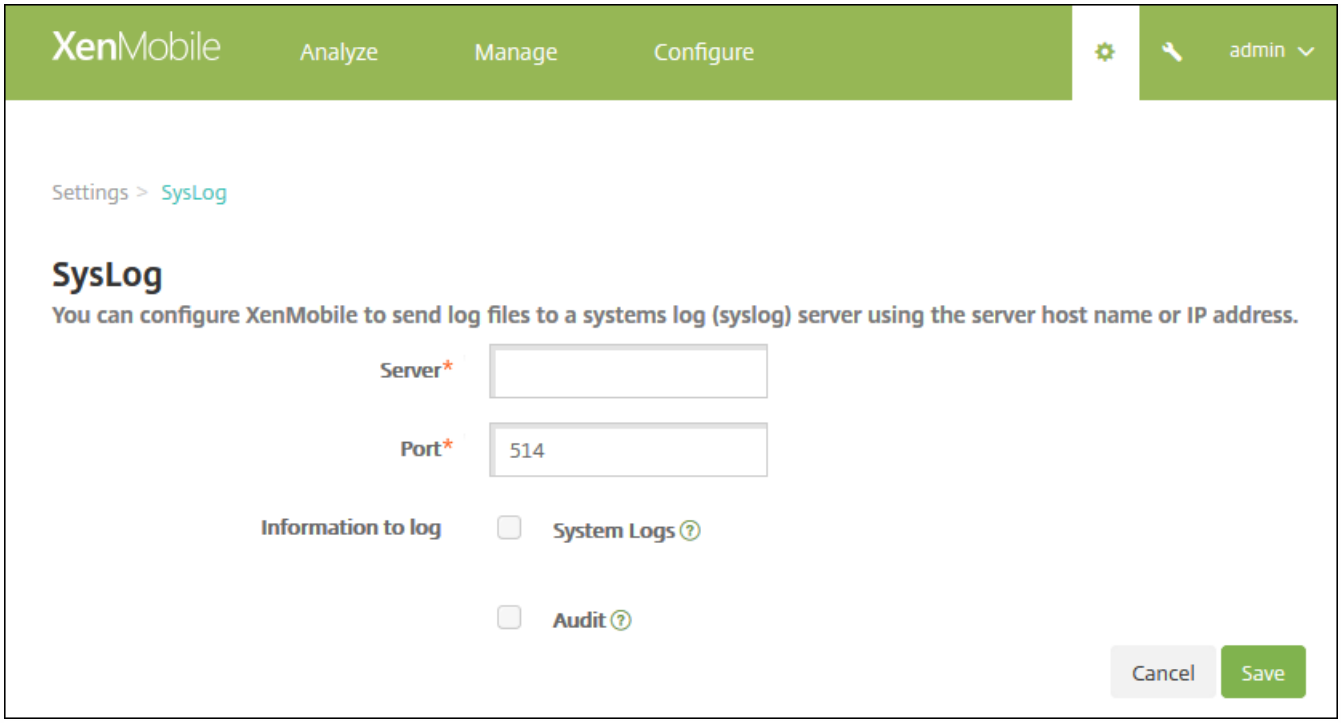
- IP-Adresse des Geräts, das die Protokollmeldung generiert hat
- Zeitstempel
- Meldungstyp
- Dringlichkeitsstufe des Ereignisses (Critical, Error, Notice, Warning, Informational, Debug, Alert, or Emergency)
- Meldungstext

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 **Alle herunterladen**. Weitere Informationen finden Sie unter Anzeigen und Analysieren von Protokolldateien in XenMobile.

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie auf **Syslog**. Die Seite **Syslog** wird angezeigt.



3. Konfigurieren Sie die folgenden Einstellungen:

- **Name**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) des syslog-Servers ein.
- **Port**: Geben Sie die Portnummer ein. In der Standardeinstellung ist dieser Port auf 514 eingestellt.
- **Informationen für Protokollierung**: Aktivieren oder deaktivieren Sie nach Bedarf die Optionen **Systemprotokolle** und **Audit**.
  - Systemprotokolle enthalten Aktionen von XenMobile.
  - Überwachungsprotokolle enthalten eine chronologische Auflistung der Systemaktivitäten im Zusammenhang mit XenMobile.

4. Klicken Sie auf **Speichern**.

So konfigurieren Sie XenApp und XenDesktop

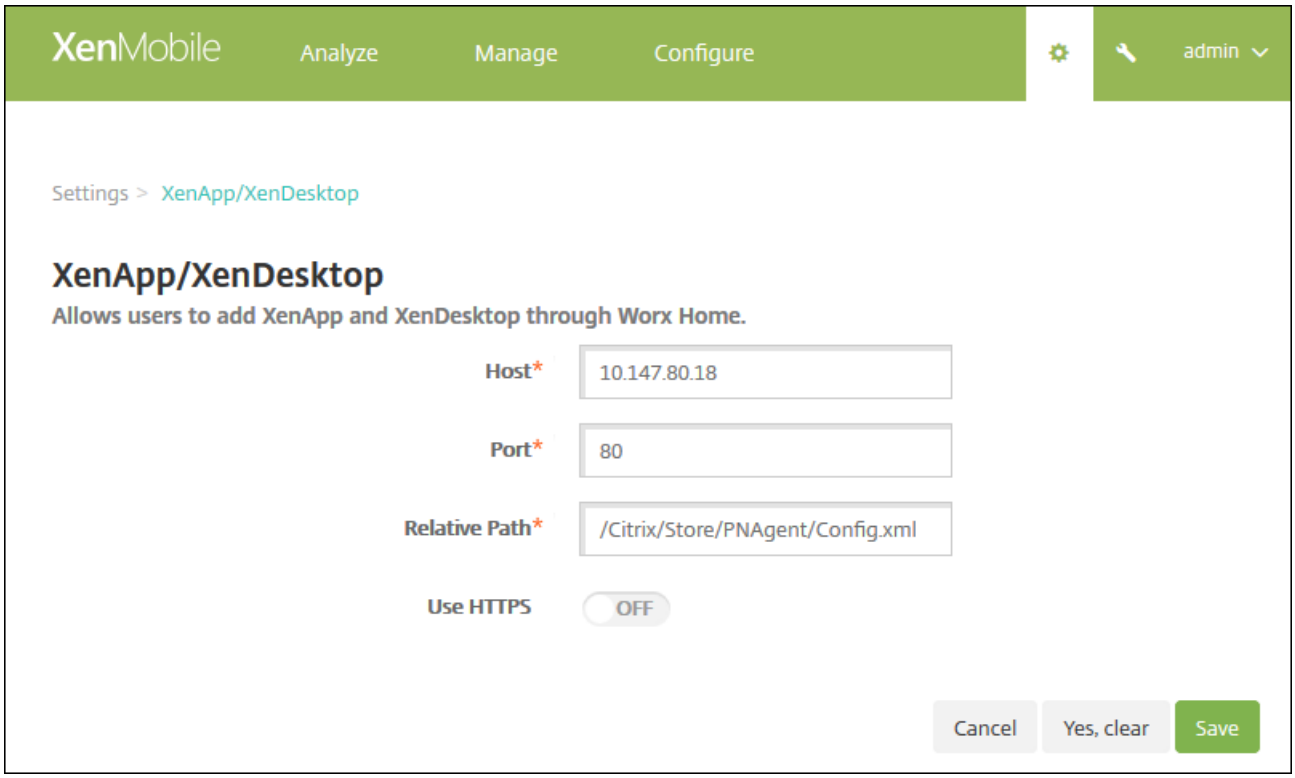
Jul 28, 2016

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 der Webinterface-Site oder von StoreFront.

1. Klicken Sie in der XenMobile-Webkonsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie auf **XenApp/XenDesktop**. Die Seite **XenApp/XenDesktop** wird angezeigt.



3. Konfigurieren Sie die folgenden Einstellungen:

- **Host**: Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse der Webinterface-Site oder von StoreFront ein.
- **Port**: Geben Sie die Portnummer der Webinterface-Site oder von StoreFront ein. Der Standardwert ist 80.
- **Relativer Pfad**: Geben Sie den Pfad ein. Beispiel: /Citrix/PNAgent/config.xml
- **HTTPS verwenden**: Wählen Sie aus, ob die sichere Authentifizierung zwischen Webinterface-Site bzw. StoreFront und dem Clientgerät aktiviert werden soll. Der Standardwert ist **AUS**.

4. Klicken Sie auf **Speichern**.

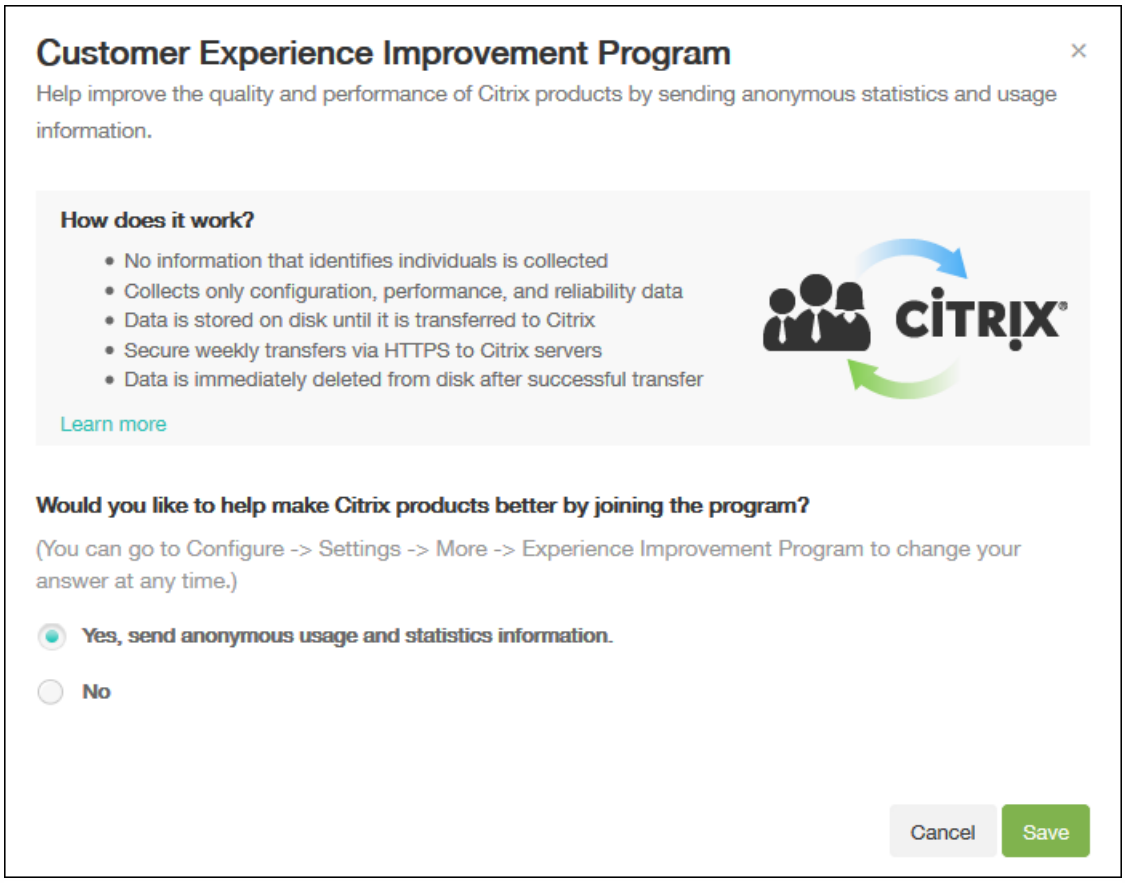
Programm zur Verbesserung der Benutzerfreundlichkeit

Jul 28, 2016

Durch das Citrix Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) werden anonyme Konfigurations- und Verwendungsdaten aus XenMobile gesammelt und automatisch an Citrix gesendet. Mit diesen Daten kann Citrix die Qualität, Zuverlässigkeit und Leistung von XenMobile verbessern. Die Teilnahme am CEIP ist freiwillig. Bei der ersten Installation von XenMobile und wenn Sie ein Update installieren, erhalten Sie Möglichkeit beim CEIP teilzunehmen. Wenn Sie sich für eine Teilnahme entscheiden, werden Daten normalerweise wöchentlich gesammelt, Leistungs- und Verwendungsdaten werden stündlich gesammelt. Die Daten werden auf Datenträgern gespeichert und einmal in der Woche sicher über HTTPS an Citrix übertragen. Sie können die Einstellung zur Teilnahme am CEIP ändern. Weitere Informationen zum CEIP finden Sie unter Citrix Programm zur Verbesserung der Benutzerfreundlichkeit.

CEIP beim Installieren oder Aktualisieren von XenMobile

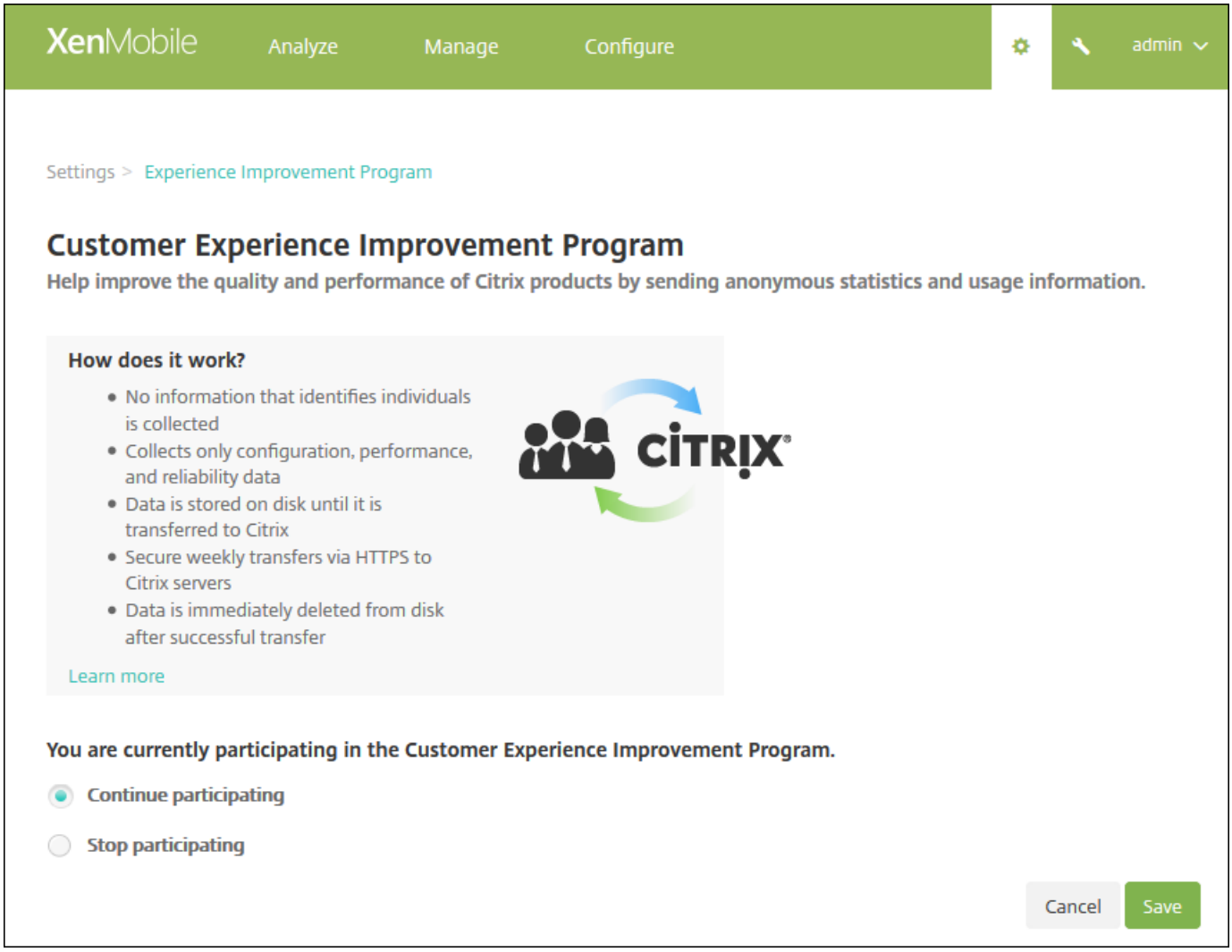
Bei der ersten Installation von XenMobile oder wenn Sie ein Update durchführen, wird das folgende Dialogfeld angezeigt, in dem Sie auswählen, ob Sie teilnehmen möchten und dann auf **Speichern** klicken.



Ändern der Einstellung zur Teilnahme am CEIP

1. Zum Ändern der Einstellungen Ihrer Teilnahme am CEIP klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben, um die Seite **Einstellungen** zu öffnen.

2. Klicken Sie unter **Server** auf **Programm zur Verbesserung der Benutzerfreundlichkeit**. Die Seite **Programm zur Verbesserung der Benutzerfreundlichkeit** wird angezeigt. Wie die Seite genau aussieht, hängt davon ab, ob Sie zu dem Zeitpunkt am CEIP teilnehmen.



3. Wenn Sie aktuell am CEIP teilnehmen und die Teilnahme beenden möchten, klicken Sie auf **Nicht mehr teilnehmen**.

4. Wenn Sie aktuell nicht am CEIP teilnehmen und die Teilnahme beginnen möchten, klicken Sie auf **Teilnehmen**.

5. Klicken Sie auf **Speichern**.

Microsoft Azure-Einstellungen

Jul 28, 2016

Geräte mit Windows 10 werden mit Microsoft Azure als Active Directory-Verbundauthentifizierung registriert. Sie können Microsoft Azure AD Windows 10-Geräte mit einem der folgenden Verfahren hinzufügen:

- Registrierung bei MDM im Rahmen des Standardbeitritts zu Azure AD beim ersten Einschalten des Geräts
- Registrierung bei MDM im Rahmen des Beitritts zu Azure AD unter Verwendung der Seite "Windows-Einstellungen" nach dem Konfigurieren des Geräts

Sie benötigen eine Lizenz für Microsoft Azure Active Directory Premium, um XenMobile in Microsoft Azure zu integrieren. Die Lizenz ist für die MDM-Integration in Azure AD erforderlich, damit Windows 10-Geräte mit Azure AD registriert werden können. Informationen zum Erwerb der Premium-Lizenz finden Sie unter Microsoft Azure. Die entsprechenden Preise finden Sie unter Azure Active Directory – Preise.

Bevor Windows-Geräte bei Azure registriert werden können, müssen Sie die Microsoft Azure-Servereinstellungen in XenMobile konfigurieren und eine AGB-Richtlinie für Windows-Geräte einrichten. In diesem Artikel wird die Konfiguration der Microsoft Azure-Einstellung behandelt. Informationen zum Einrichten einer AGB-Richtlinie für Windows-Geräte finden Sie unter AGB-Geräterichtlinien

Vor dem Festlegen der Microsoft Azure-Servereinstellungen in XenMobile müssen Sie sich beim Azure AD-Portal anmelden und folgende Schritte ausführen:

1. Registrieren Sie die benutzerdefinierte Domäne und lassen Sie sie prüfen. Weitere Informationen finden Sie unter Hinzufügen eines eigenen Domänennamens zu Azure Active Directory.

2. Erweitern Sie Ihr lokales Verzeichnis auf Azure Active Directory mit Tools zur Verzeichnisintegration. Weitere Informationen finden Sie unter Verzeichnisintegration.

3. Machen Sie MDM zum zuverlässigen Eintrag in Azure AD. Klicken Sie hierzu auf **Azure Active Directory** > **Anwendungen** und dann auf **Hinzufügen**. Wählen Sie **Anwendung hinzufügen** aus dem Katalog aus. Wechseln Sie zu **Verwaltung mobiler Geräte**, wählen Sie **On-premise MDM application** und speichern Sie die Einstellungen.

4. Konfigurieren Sie in der Anwendung die XenMobile-Server-Discovery, AGB-Endpunkte und APP-ID-URI:

- MDM-Discovery-URL: https://:8443/zdm/wpe
- MDM-AGB-URL: https://:8443/zdm/wpe/tou
- APP-ID-URI: https://:8443/

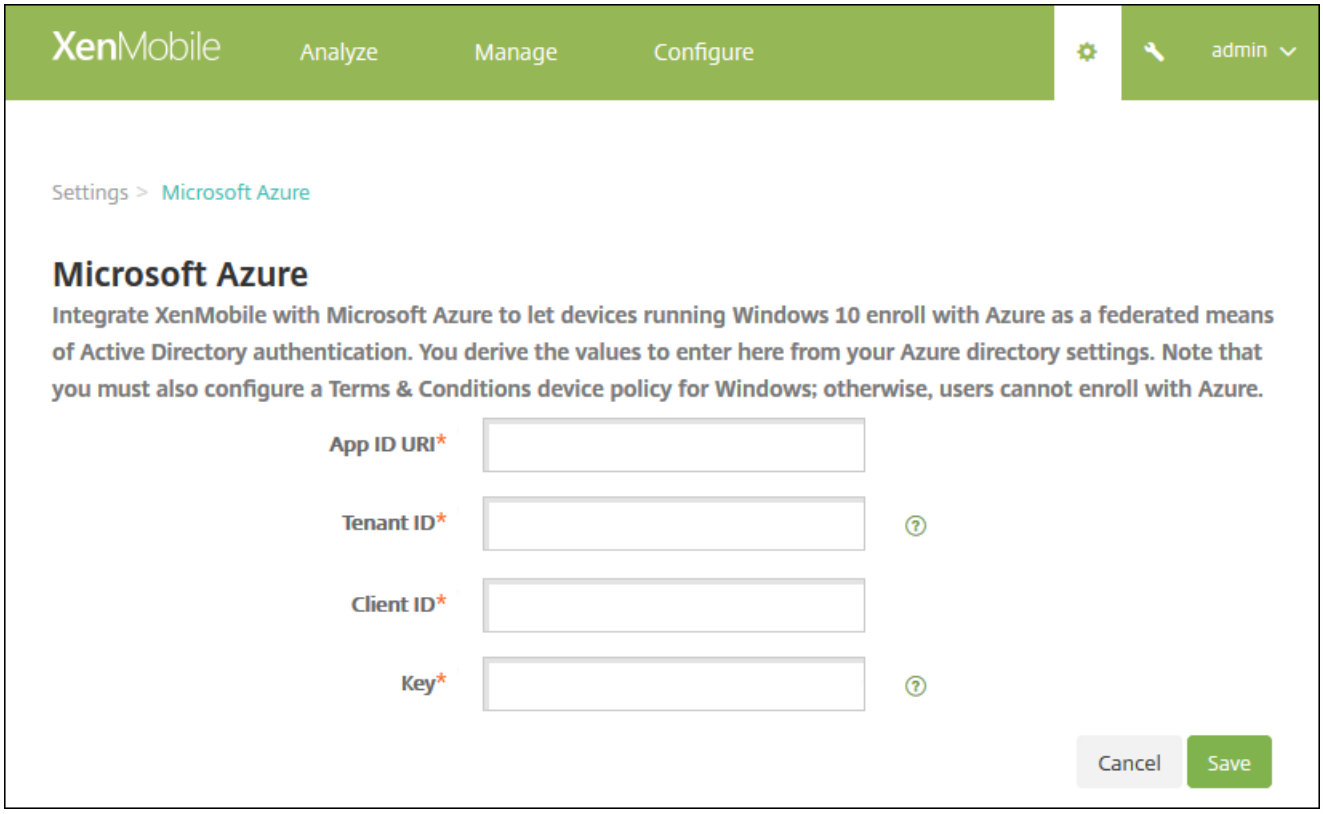
5. Wählen Sie die in Schritt 3 erstellte lokalen MDM-Anwendung aus und aktivieren Sie die Option **Geräte für diese Benutzer verwalten**, um MDM für alle Benutzer oder bestimmte Benutzergruppen zu aktivieren.

Sie benötigen die folgenden Informationen von Ihrem Microsoft Azure-Konto zum Konfigurieren der Einstellungen in der XenMobile-Konsole:

- App-ID-URI: URL des Servers, auf dem XenMobile ausgeführt wird
- Mandanten-ID: von der Azure-Seite mit den Anwendungseinstellungen
- Client-ID: eindeutiger Bezeichner Ihrer App
- Schlüssel: von der Azure-Seite mit den Anwendungseinstellungen

1. Klicken Sie in der XenMobile-Konsole auf das Zahnradsymbol rechts oben. Die Seite **Einstellungen** wird angezeigt.

2. Klicken Sie unter **Server** auf **Microsoft Azure**. Die Seite **Microsoft Azure** wird angezeigt.



3. Konfigurieren Sie die folgenden Einstellungen:

- **App-ID-URI**: Geben Sie die URL des Servers mit XenMobile ein, die Sie beim Konfigurieren der Azure-Einstellungen eingegeben haben.
- **Mandanten-ID**: Kopieren Sie den Wert von der Azure-Seite mit den Anwendungseinstellungen. Kopieren Sie in der Adressleiste des Browsers den Abschnitt aus Zahlen und Buchstaben. Beispiel: Die Mandanten-ID von https://manage.windowszaure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem ... ist *abc123-abc123-abc123*.
- **Client-ID**: Kopieren Sie den Wert von der Azure-Seite "Konfigurieren". Dies ist der eindeutige Bezeichner Ihrer App.
- **Schlüssel**: Kopieren Sie den Wert von der Azure-Seite mit den Anwendungseinstellungen. Wählen Sie unter **Schlüssel** eine Zeitdauer aus und speichern Sie die Einstellung. Sie können den Schlüssel dann kopieren und in das Feld einfügen. Ein Schlüssel ist erforderlich, wenn Apps Daten in Microsoft Azure AD lesen und schreiben.

4. Klicken Sie auf **Speichern**.

Important

Wenn Benutzer auf ihren Windows-Geräten Azure AD beitreten, sind die WorxStore- und Weblink-Geräterichtlinien, die Sie in XenMobile konfiguriert haben, nur für Benutzer von Azure AD, aber nicht für lokale Benutzer verfügbar. Damit lokale Benutzer die Richtlinien verwenden können, müssen sie die folgenden Schritte ausführen:

1. Azure AD im Namen eines Azure-Benutzers unter **Einstellungen** > **Info** > **Azure AD beitreten** beitreten.
2. Abmelden von Windows und Anmelden mit einem Azure AD-Konto.

Google Cloud Messaging

Jul 28, 2016

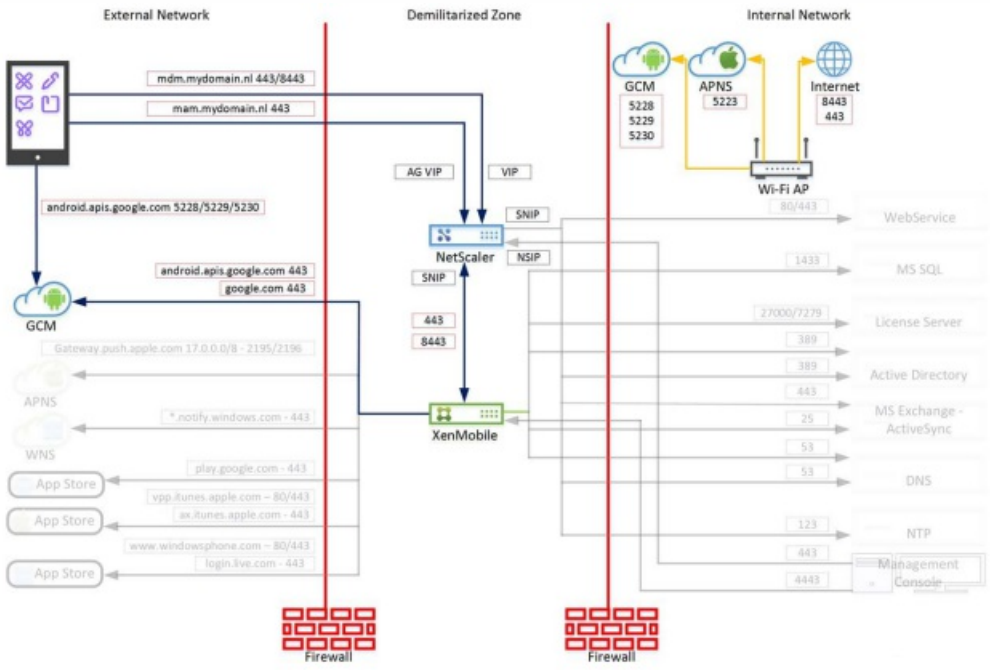
Als Alternative zur MDX-Richtlinie **Aktives Abfrageintervall** können Sie mit Google Cloud Messaging (GCM) steuern, wie und wann Android-Geräte eine Verbindung mit XenMobile herstellen müssen. Bei der in diesem Artikel beschriebenen Konfiguration lösen Sicherheitsaktionen oder Bereitstellungsbefehle eine Pushbenachrichtigung an Worx Home aus, sodass der Benutzer aufgefordert wird, eine Verbindung mit dem XenMobile-Server herzustellen.

Voraussetzungen

- XenMobile 10.3.x
- Aktueller Worx Home-Client
- Anmeldeinformationen für Google Developer-Konto
- Öffnen Sie in XenMobile Port 443 für Android.apis.google.com und Google.com.

Architektur

In diesem Diagramm ist der Kommunikationsfluss für GCM im externen und internen Netzwerk dargestellt.

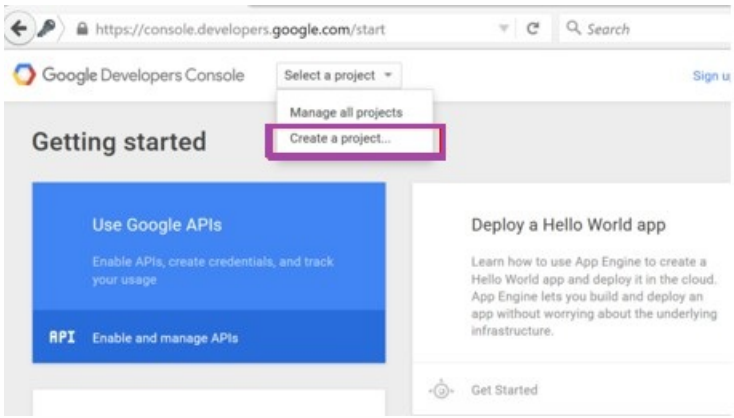


Konfigurieren Ihres Google-Kontos für GCM

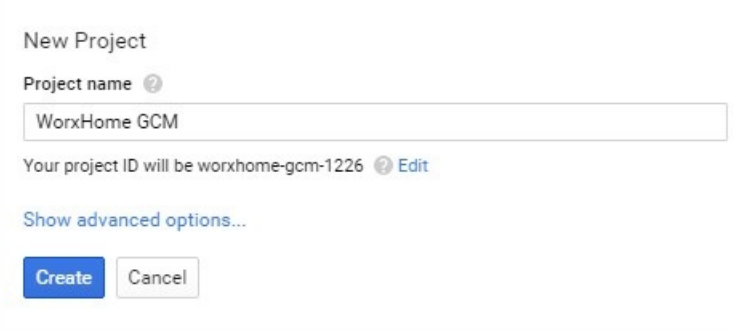
1. Melden Sie sich an der folgenden URL mit den Anmeldeinformationen für Ihr Google Developer-Konto an:

   https://console.developers.google.com

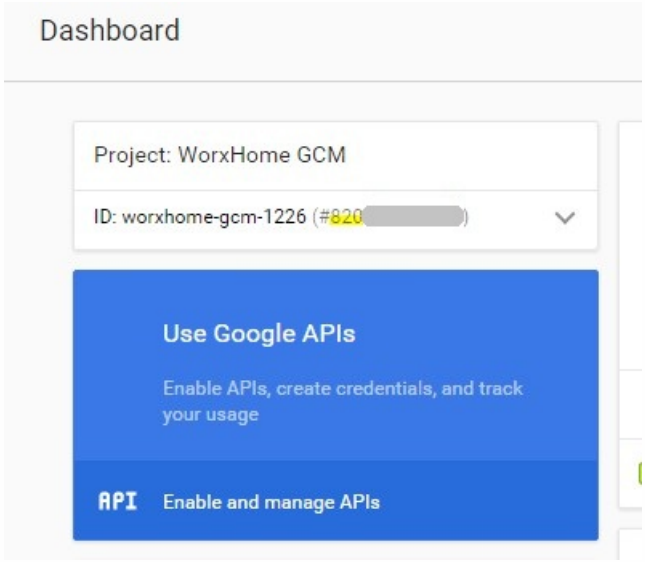
2. Wählen Sie unter **Select a project** die Option **Create a project**.



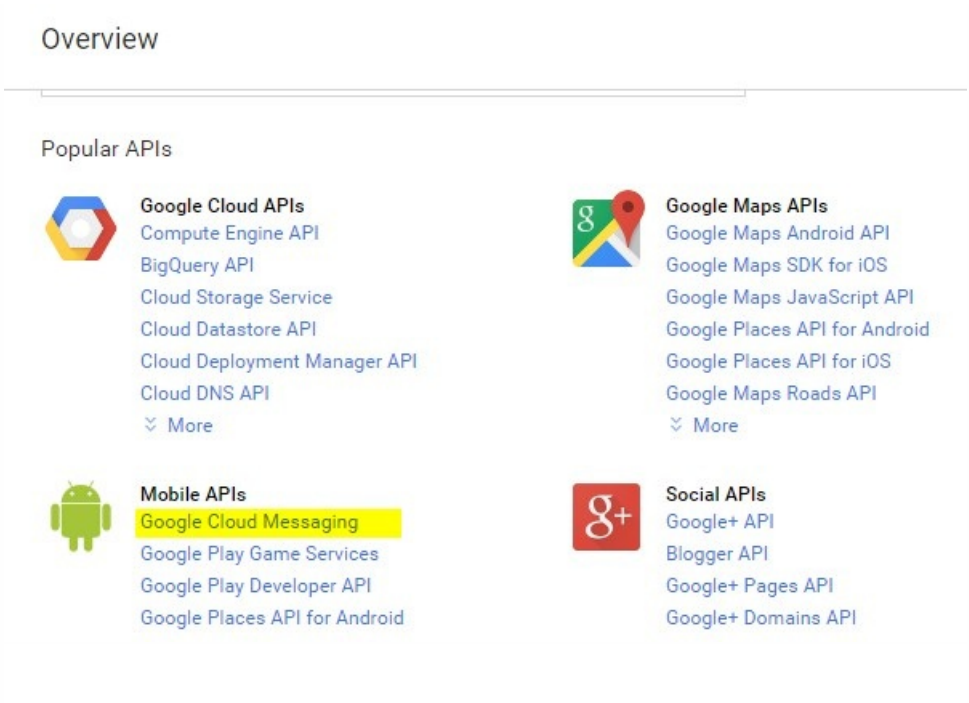
3. Geben Sie einen Namen unter **Project name** ein und klicken Sie auf **Create**.



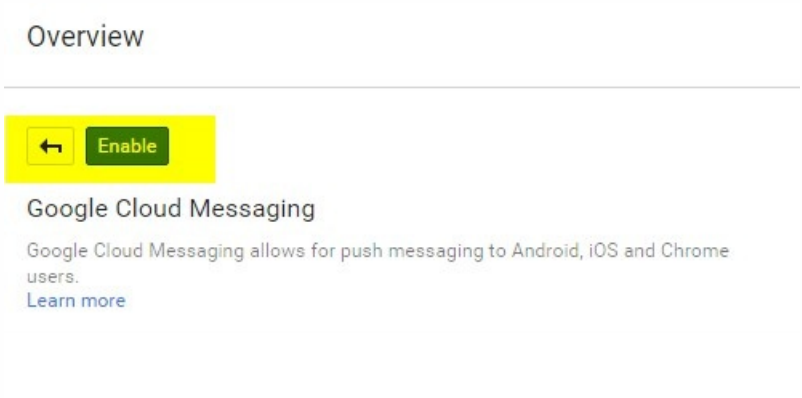
4. Im Dashboard wird Ihre Absender-ID (unten markiert) neben der Projekt-ID angezeigt. Notieren Sie die Absender-ID, da Sie sie später in den XenMobile-Servereinstellungen eingeben müssen. Klicken Sie auf **Use Google APIs**.



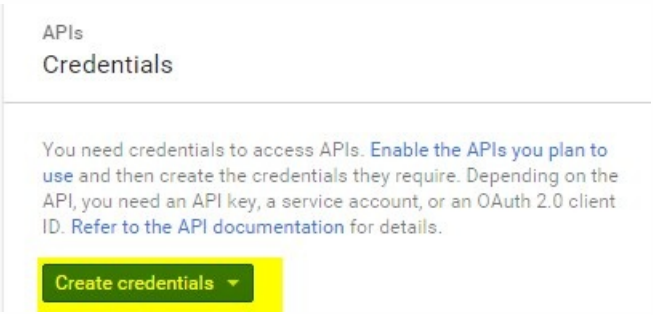
5. Klicken Sie im Bereich **Mobile APIs** auf **Google Cloud Messaging**.



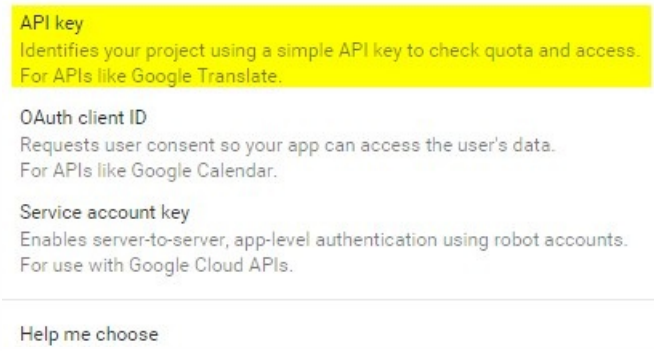
6. Klicken Sie auf **Enable**.



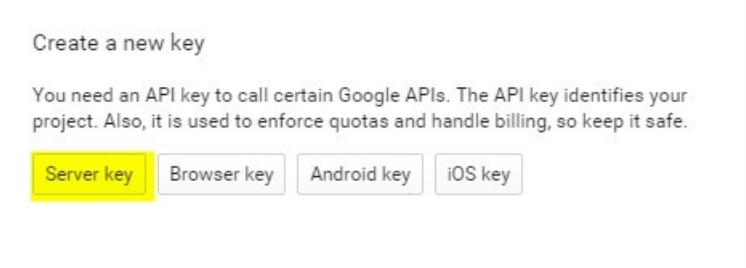
7. Klicken Sie unter **Credentials** auf **Create credentials**.



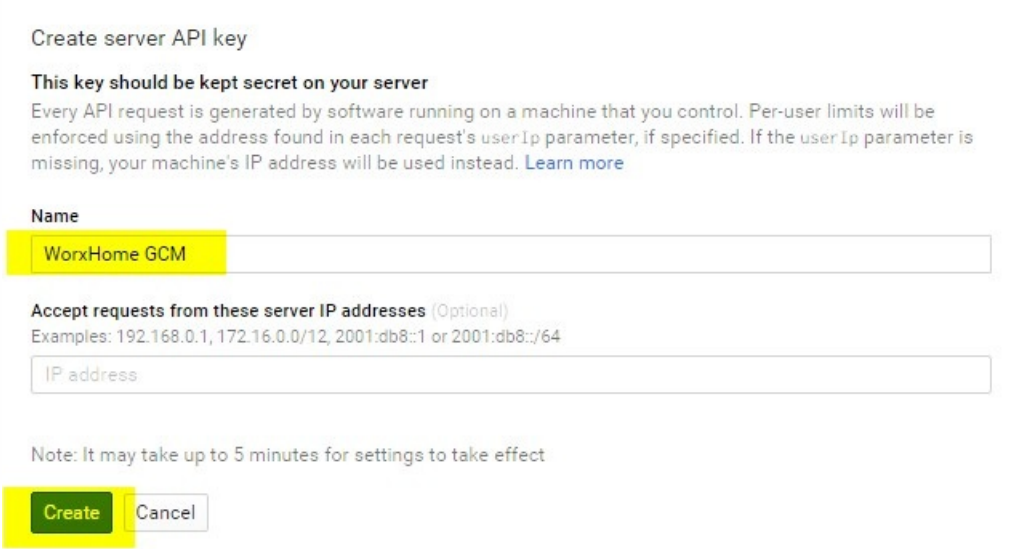
8. Klicken Sie auf **API key**.



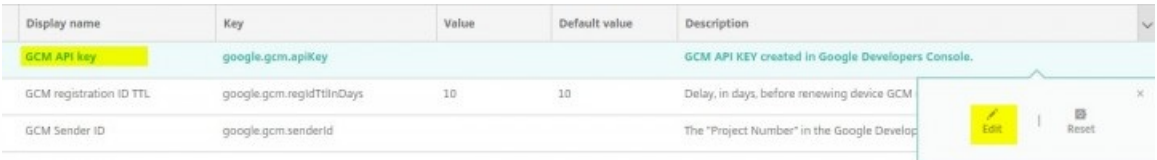
9. Klicken Sie unter **Create a new key** auf **Server key**.



10. Geben Sie in **Create server API key** einen Namen ein (im Beispiel wurde ein Projektname verwendet) und klicken Sie dann auf **Create**.



11. Notieren Sie den API-Schlüssel. Sie benötigen ihn zum Konfigurieren von XenMobile.



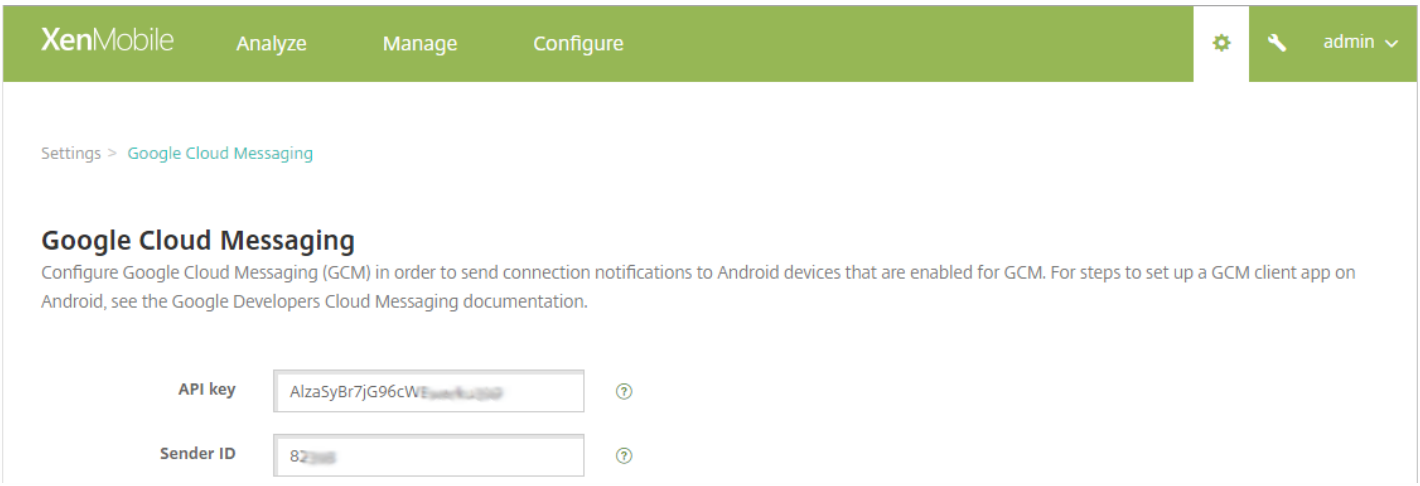
Konfigurieren von XenMobile für GCM

1. Melden Sie sich an der XenMobile-Verwaltungskonsole an und klicken Sie auf **Einstellungen > Google Cloud Messaging**.

   a. Geben Sie im Feld **API-Schlüssel** den GCM API-Schlüssel ein, den Sie im letzten Schritt der GCM-Konfiguration notiert haben.

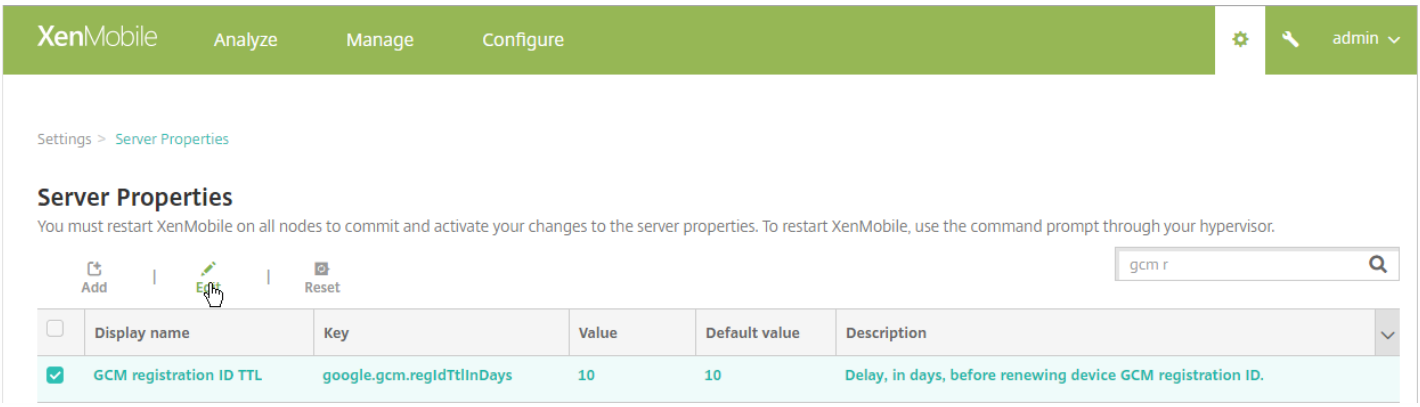
   b. Geben Sie in **Absender-ID** die Absender-ID ein, die Sie im vorherigen Vorgang notiert haben, und klicken Sie auf **Speichern**.

   Hinweis: Die Seite **Einstellungen > Google Cloud Messaging** ist neu in XenMobile 10.3.6. Wenn Sie nicht das aktuelle XenMobile-Release verwenden, gehen Sie zu **Einstellungen > Server** und aktualisieren Sie den **API-Schlüssel** (google.gcm.apiKey) und die **Absender-ID** (google.gcm.senderid).



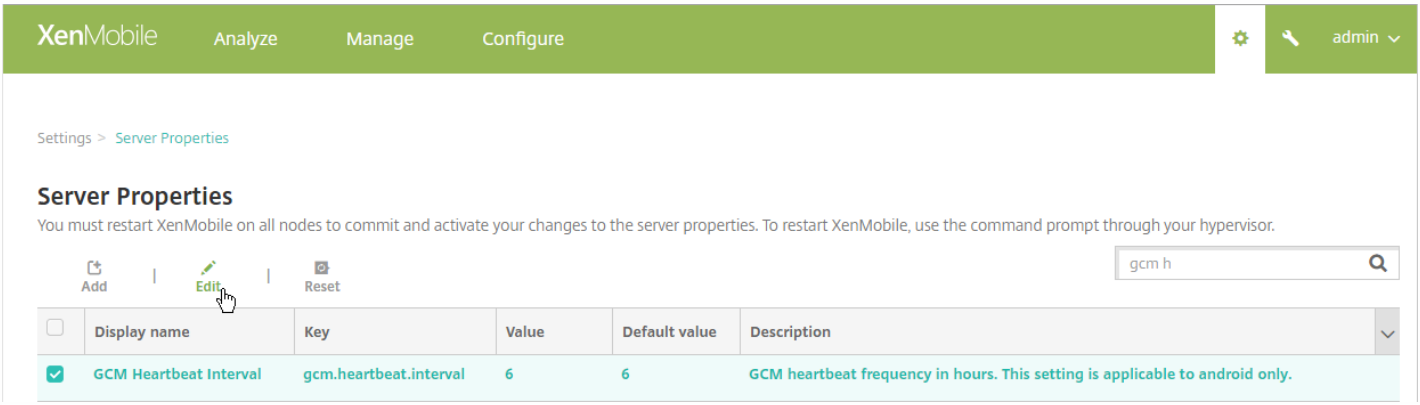
2. Wenn Sie die Standardeinstellungen für die folgenden Eigenschaften ändern müssen, klicken Sie auf **Einstellungen > Servereigenschaften**.

- **GCM Registration ID TTL:** Die Standardfrist bis zum Erneuern der GCM-Registrierungs-ID für das Gerät ist **10** Tage. Wenn Sie den Wert ändern möchten, geben Sie **gcm r** in das Suchfeld ein, klicken Sie auf **GCM Registration ID TTL** und dann auf **Bearbeiten**.



- **GCM Heartbeat Interval:** Die Standardfrequenz, mit der XenMobile mit dem GCM-Server kommuniziert, ist **6** Stunden.

Wenn Sie den Wert ändern möchten, geben Sie **gcm h** in das Suchfeld ein und klicken Sie auf **GCM Heartbeat Interval** und dann auf **Bearbeiten**.



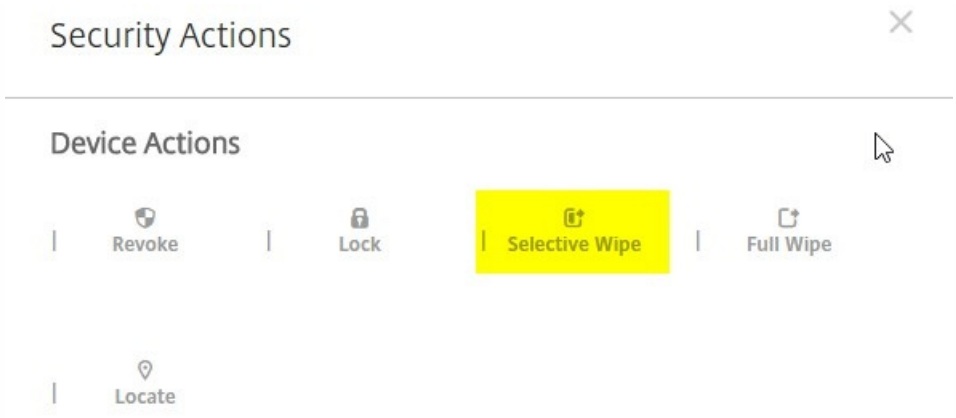
Testen der Konfiguration

1. Registrieren Sie ein Android-Gerät.

2. Lassen Sie das Gerät eine Zeit lang inaktiv, sodass die Verbindung mit dem XenMobile-Server getrennt wird.

3. Melden Sie sich bei der XenMobile-Verwaltungskonsole an, klicken Sie auf **Verwalten**, wählen Sie das Android-Gerät aus und klicken Sie auf **Sicherheit**.

4. Klicken Sie unter **Geräteaktionen** auf **Selektiv löschen**.



Bei erfolgreicher Konfiguration wird auf dem Gerät ein selektiver Löschvorgang ausgeführt, ohne dass das Gerät die Verbindung mit XenMobile wiederherstellt.

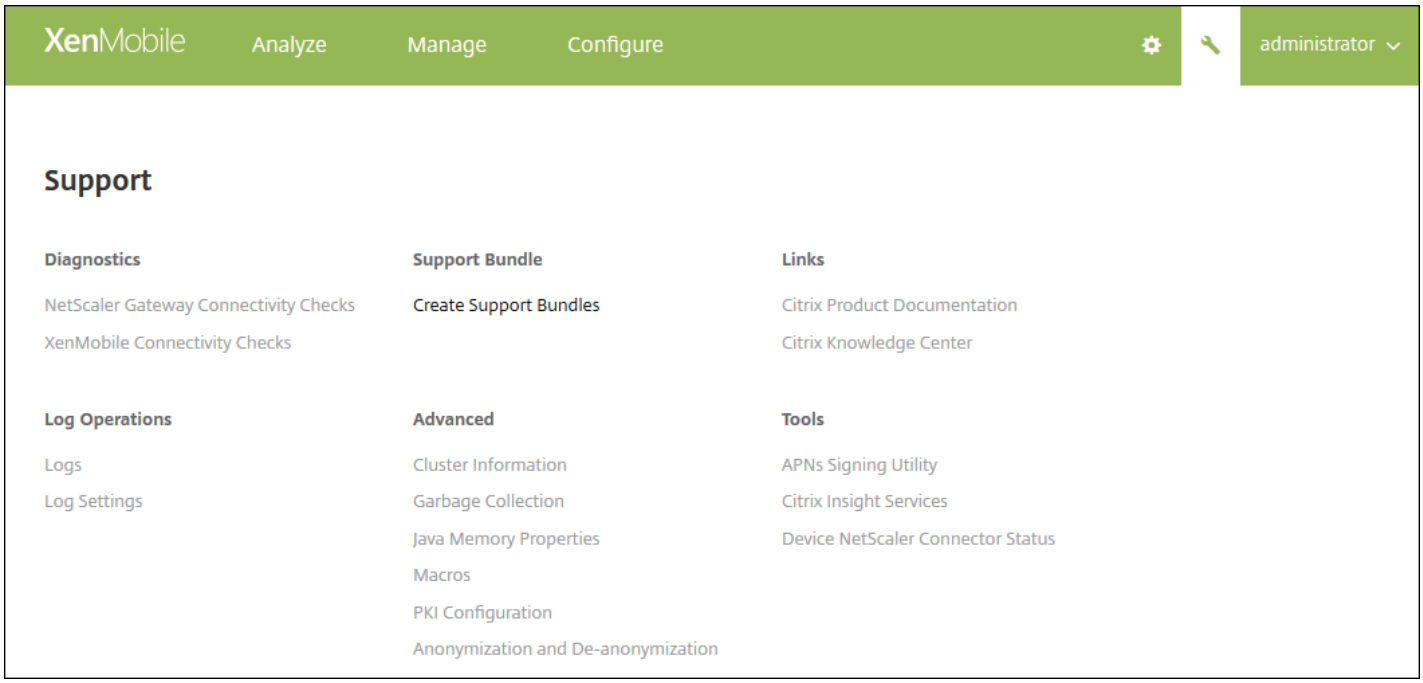
Support und Wartung von XenMobile

Jul 28, 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.

Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben.

Die Seite Support wird angezeigt.



Verwenden Sie die Seite **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

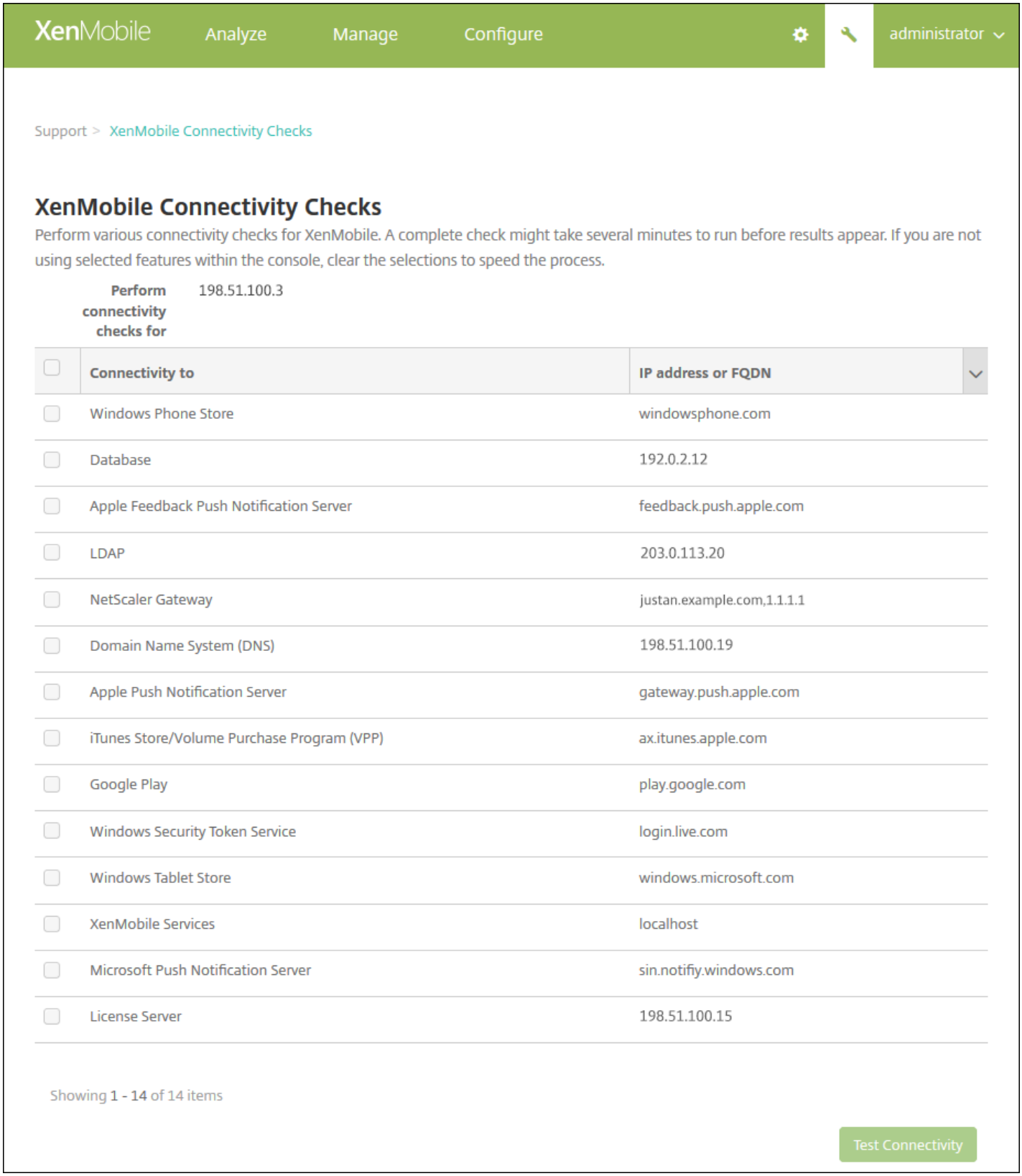
Jul 28, 2016

Über die Seite **Support** können Sie die Verbindung zwischen XenMobile und NetScaler Gateway sowie anderen Servern und Speicherorten prüfen.

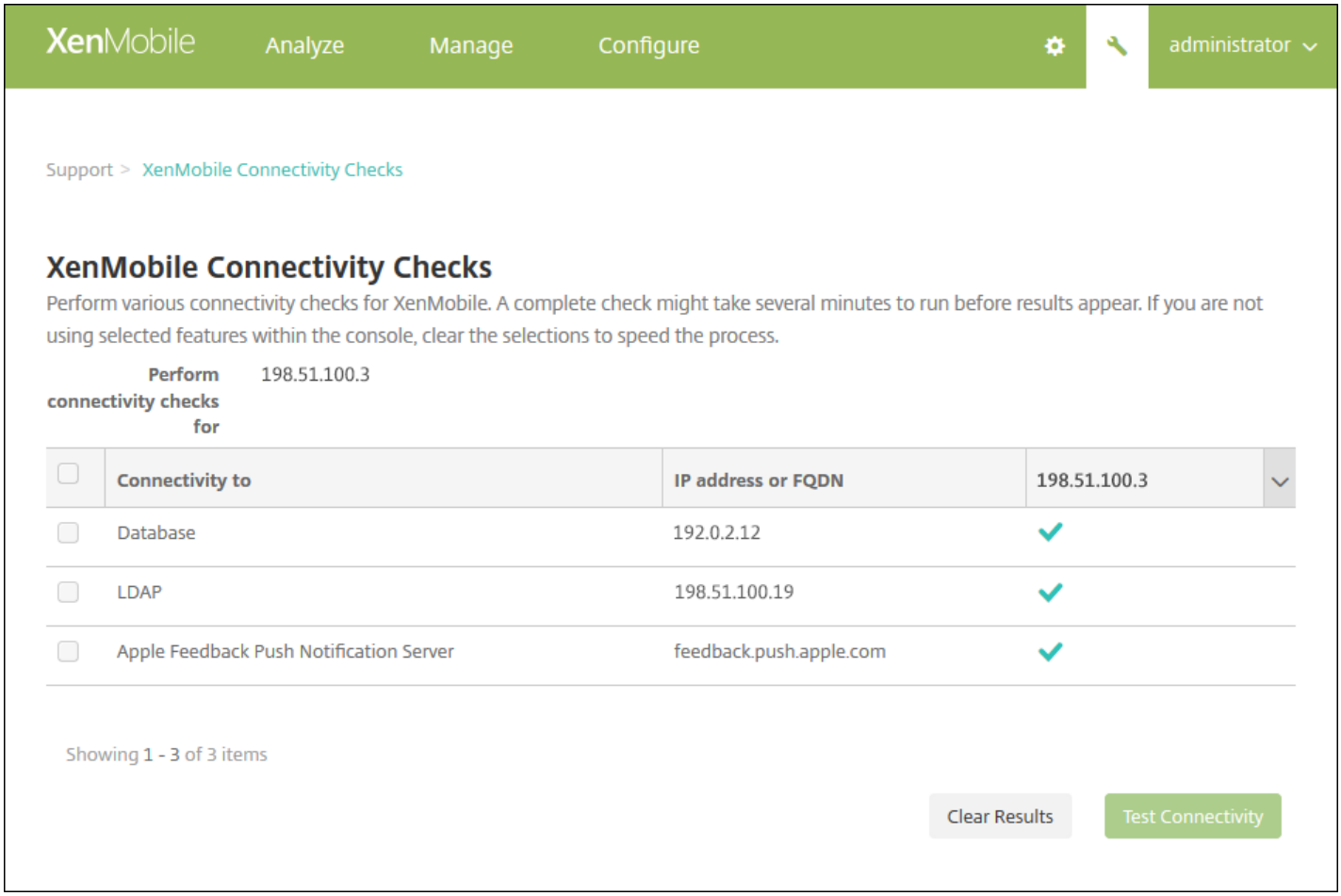
Prüfen von XenMobile-Verbindungen

1. Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben. Die Seite **Support** wird angezeigt.

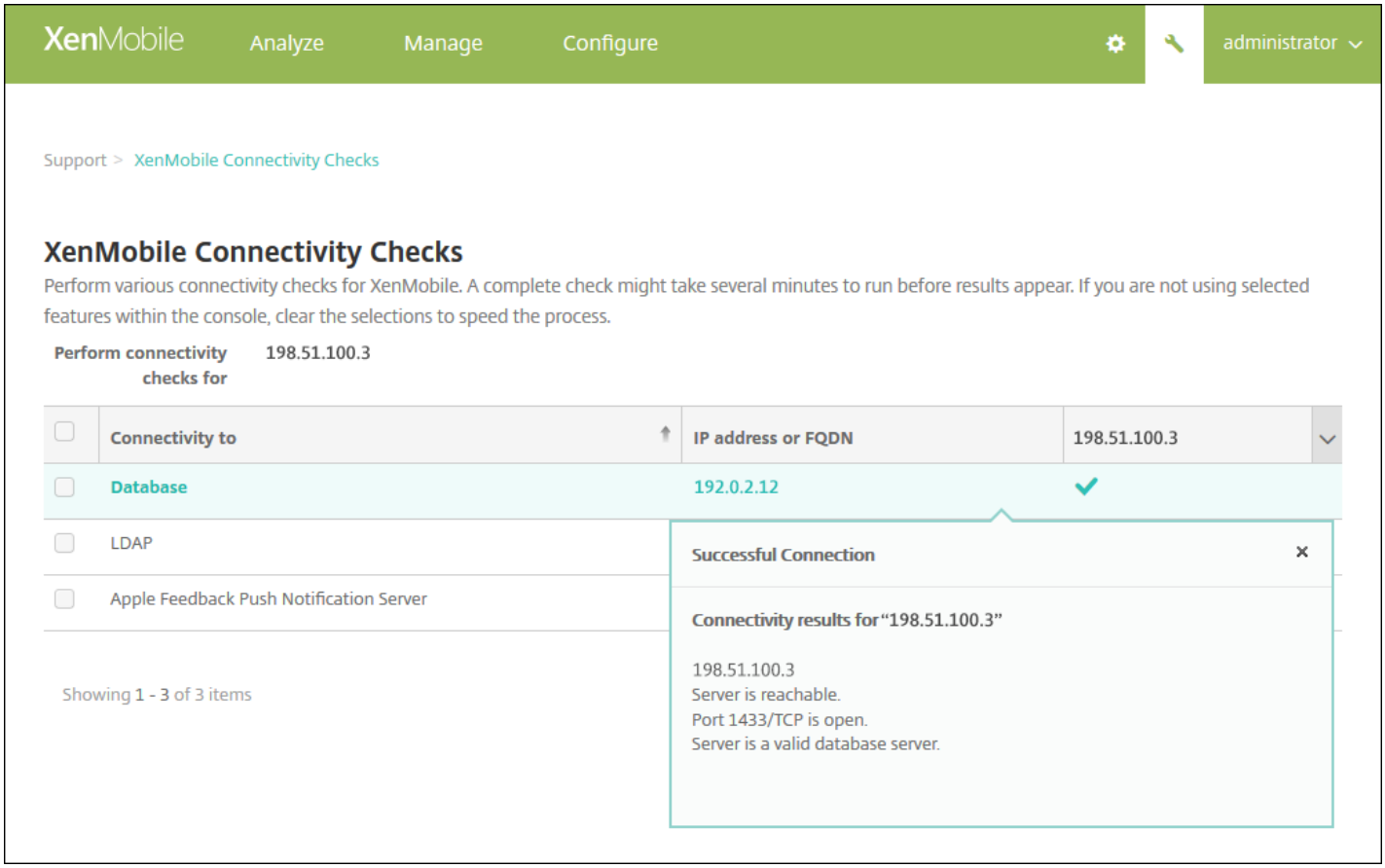
2. Klicken Sie unter **Diagnose** auf **XenMobile-Konnektivitätsprüfung**. Die Seite **XenMobile-Konnektivitätsprüfung** wird angezeigt. Wenn die XenMobile-Umgebung Clusterknoten enthält, werden alle Knoten angezeigt.



2. Wählen Sie die Server aus, deren Verbindung geprüft werden soll, und klicken Sie auf **Konnektivität testen**. Das Testergebnis wird angezeigt.

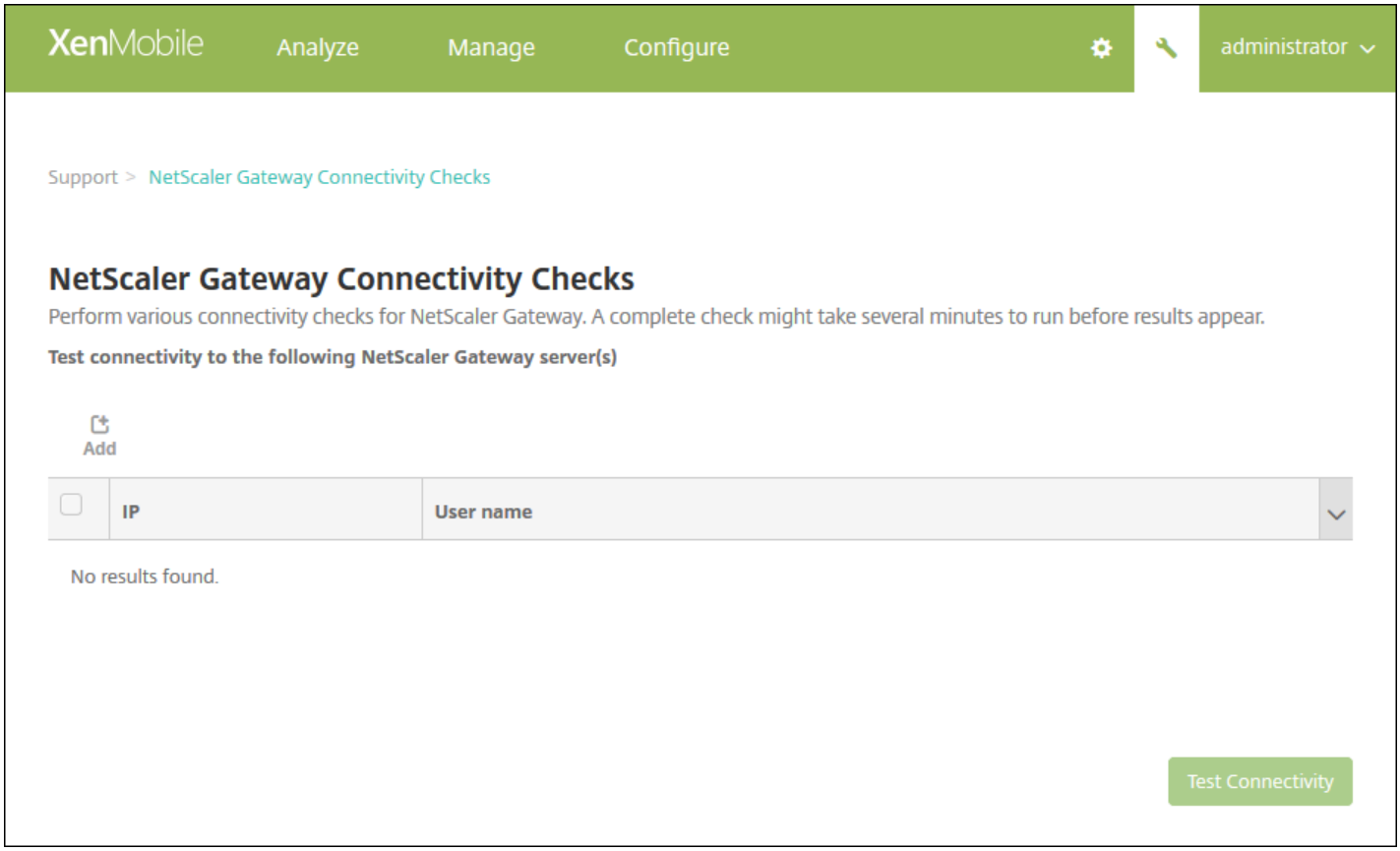


3. Wählen Sie einen Server in der Tabelle mit dem Testergebnis aus, um detaillierte Angaben für ihn anzuzeigen.

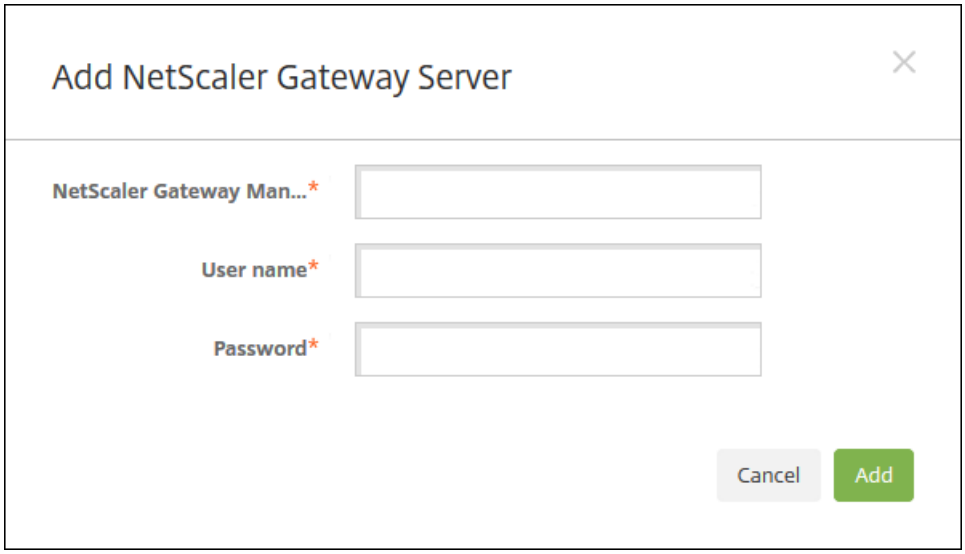


Prüfen von NetScaler Gateway-Verbindungen

1. Klicken Sie auf der Seite **Support** unter **Diagnose** auf **NetScaler Gateway-Konnektivitätsprüfung**. Die Seite **NetScaler Gateway-Konnektivitätsprüfung** wird angezeigt. Die Tabelle ist leer, wenn Sie keine NetScaler Gateway-Server hinzugefügt haben.



2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **NetScaler Gateway-Server hinzufügen** 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 **Hinzufügen**. Das NetScaler Gateway wird der Tabelle auf der Seite **NetScaler Gateway-Konnektivitätsprüfung** hinzugefügt.

6. Klicken Sie auf **Konnektivität testen**. Das Ergebnis wird in einer Tabelle angezeigt.

7. Wählen Sie einen Server in der Tabelle mit dem Testergebnis aus, um detaillierte Angaben für ihn anzuzeigen.

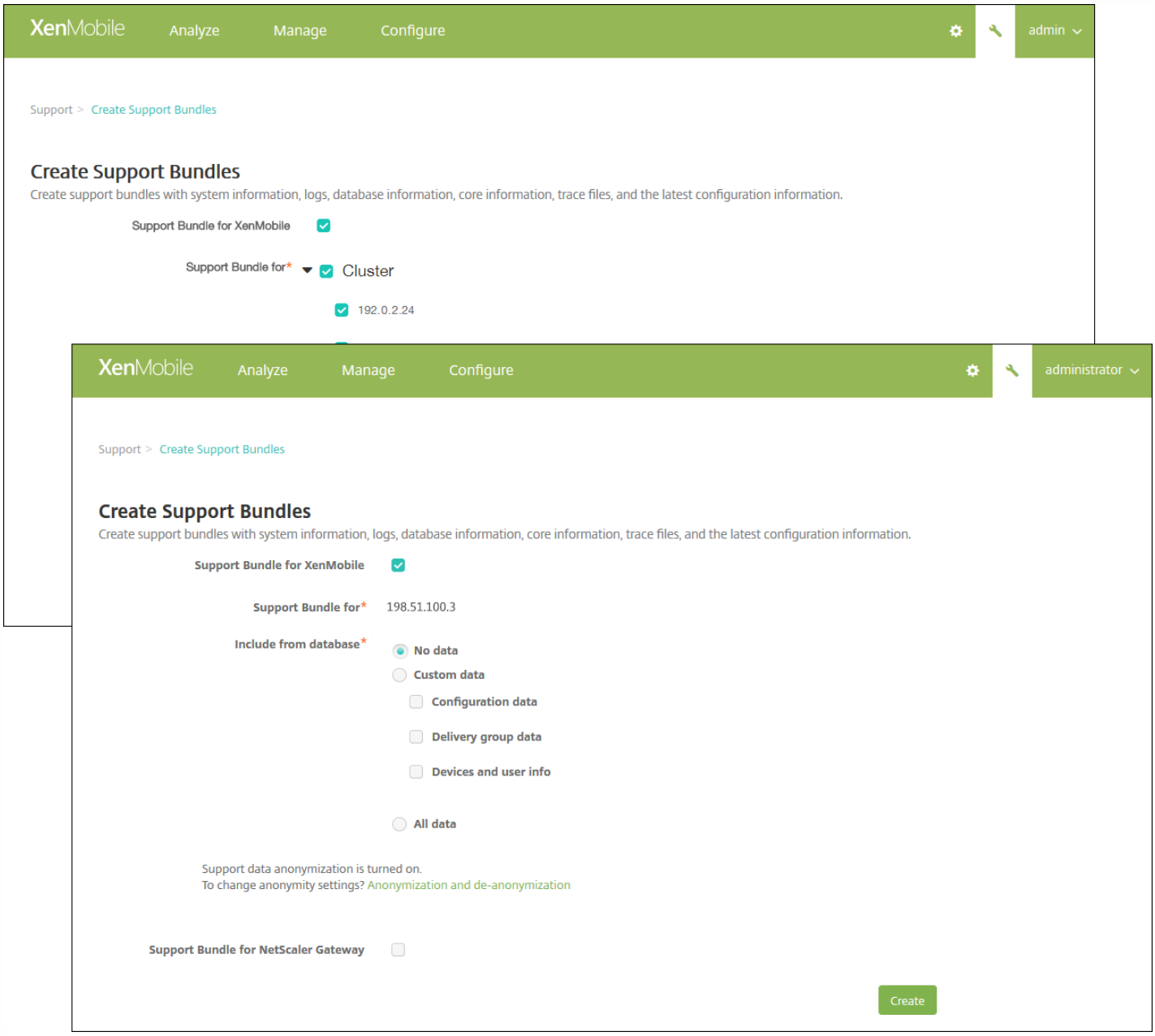
Erstellen von Supportpaketen in XenMobile

Jul 28, 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. Die Seite **Support** wird angezeigt.

2. Klicken Sie auf der Seite **Support** auf **Supportpakete erstellen**. Die Seite **Supportpakete erstellen** wird angezeigt. Wenn die XenMobile-Umgebung Clusterknoten enthält, werden alle Knoten angezeigt.



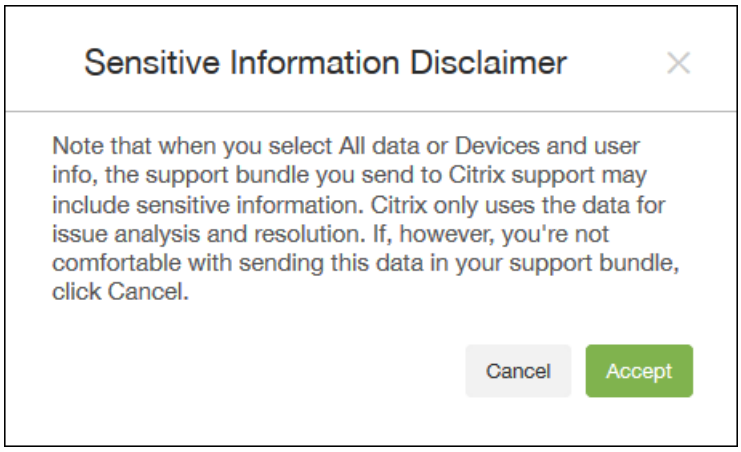
3. Stellen Sie sicher, dass das Kontrollkästchen **Supportpaket für XenMobile** aktiviert ist.

4. Wenn die XenMobile-Umgebung Clusterknoten enthält, können Sie unter **Supportpaket für** beliebige oder alle Knoten für die Datensammlung auswählen.

5. Führen Sie unter **Aus Datenbank einschließen** einen der folgenden Schritte aus:

- Klicken Sie auf **Keine Daten**.
- Klicken Sie auf **Benutzerdefinierte Daten** und wählen Sie nach Bedarf die gewünschten Daten aus:
  - **Konfigurationsdaten**: umfasst Zertifikatkonfigurationen und Device Manager-Richtlinien.
  - **Bereitstellungsgruppendaten**: umfasst Informationen zu App-Bereitstellungsgruppen mit App-Typen und Details zur App-Bereitstellungsrichtlinie.
  - **Geräte- und Benutzerinfo**: umfasst Geräterichtlinien, Apps, Aktionen und Bereitstellungsgruppen.
- Klicken Sie auf **Alle Daten**.

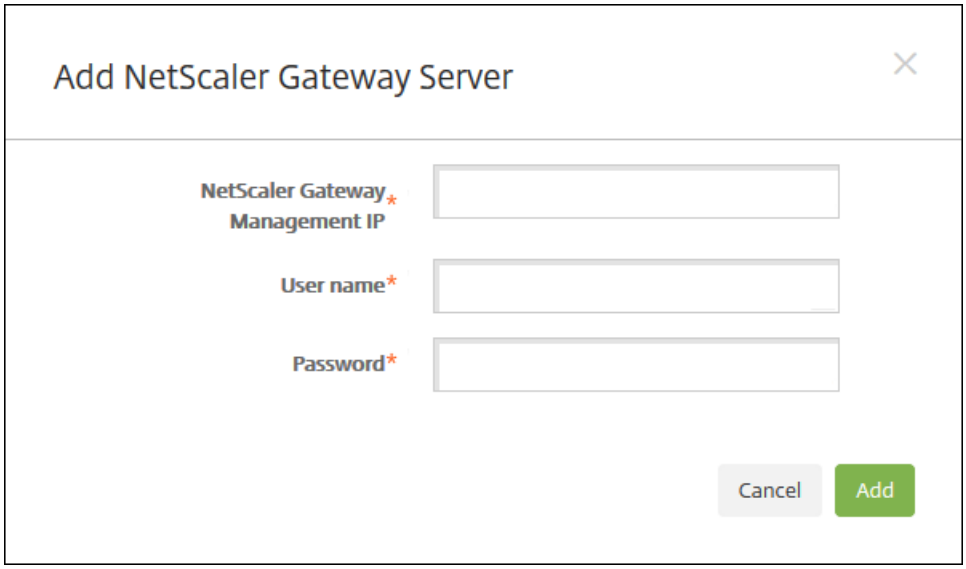
Hinweis: Wenn Sie **Geräte- und Benutzerinfo** oder **Alle Daten** auswählen und dies Ihr erstes Supportpaket ist, wird das Dialogfeld **Haftungsausschluss für vertrauliche Informationen** angezeigt. Lesen Sie den Haftungsausschluss und klicken Sie dann auf **Akzeptieren** oder **Abbrechen**. Wenn Sie auf **Abbrechen** klicken, kann das Supportpaket nicht an Citrix hochgeladen werden. Wenn Sie auf **Akzeptieren** klicken, können Sie das Supportpaket an Citrix hochladen. Der Haftungsausschluss wird das nächste Mal, wenn Sie ein Supportpaket mit Geräte- oder Benutzerdaten erstellen, nicht wieder angezeigt.



6. Unterhalb von **Aus Datenbank einschließen** steht ein Vermerk darüber, ob vertrauliche Benutzer-, Server- und Netzwerkdaten in Supportpaketen anonymisiert werden. (In der Standardeinstellung ist die Anonymisierung aktiviert.) Sie können diese Einstellung über den Link **Anonymisierung und Deanonymisierung** ändern. Weitere Informationen finden Sie unter Anonymisierung von Daten in Supportpaketen.

6. Wählen Sie **Supportpaket für NetScaler Gateway** aus, wenn Sie Supportpakete von NetScaler Gateway einschließen möchten, und führen Sie die folgenden Schritte aus:

- Klicken Sie auf **Hinzufügen**. Das Dialogfeld **NetScaler Gateway-Server hinzufügen** wird angezeigt.



- 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.

- Geben Sie unter **Benutzername** und **Kennwort** die Anmeldeinformationen für den Zugriff auf den Server ein, auf dem NetScaler Gateway ausgeführt wird.

  Hinweis: Wenn Sie ein Paket von einem NetScaler Gateway-Server erstellen, der bereits hinzugefügt wurde, wird der Benutzername bereitgestellt.

7. Klicken Sie auf **Hinzufügen**. Das neue NetScaler Gateway-Supportpaket wird der Tabelle hinzugefügt.

8. Wiederholen Sie Schritt 7 zum Hinzufügen weiterer NetScaler Gateway-Supportpakete nach Bedarf.

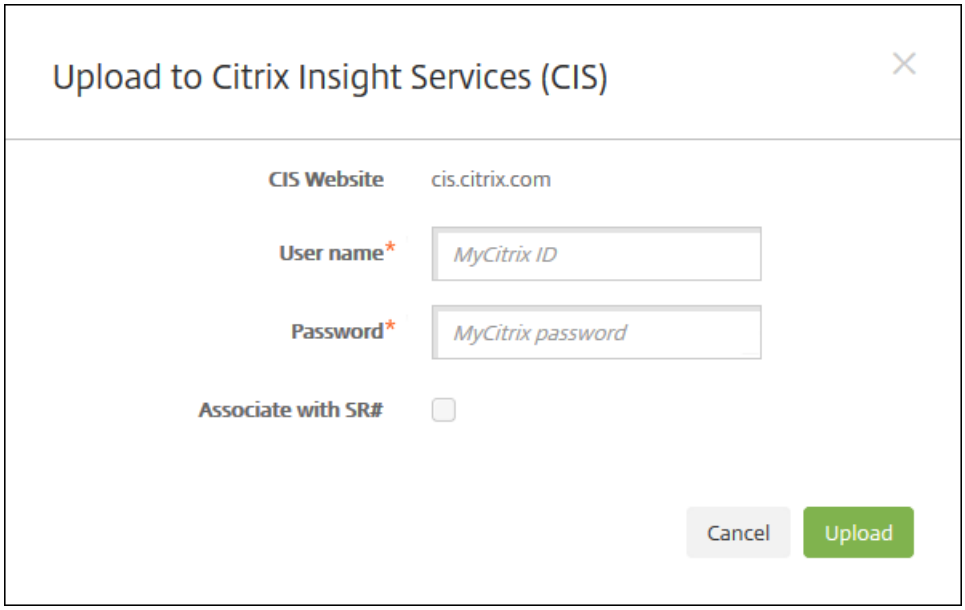
9. Klicken Sie auf **Erstellen**. Das Supportpaket wird erstellt und zwei neue Schaltfläche werden angezeigt: **Upload zu CIS** und **Zu Client herunterladen**.

Fahren Sie mit dem Abschnitt 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. Sie benötigen eine MyCitrix-ID mit Kennwort für den Upload an CIS.

1. Klicken Sie auf der Seite **Supportpakete erstellen** auf **Upload zu CIS**. Das Dialogfeld **Upload zu Citrix Insight Services (CIS)** wird angezeigt.



2. Geben Sie unter **Benutzername** Ihre MyCitrix-ID ein.

3. Geben Sie unter **Kennwort** Ihr MyCitrix-Kennwort ein.

4. Wenn Sie das Paket mit einer vorhandenen Dienstanforderung verbinden möchten, wählen Sie das Kontrollkästchen **SR-Nr. zuordnen** aus und geben Sie in die beiden neu angezeigten Felder Folgendes ein:

- Geben Sie unter **SR-Nr.** die achtstellige Dienstanforderungsnummer ein, der Sie das Paket zuordnen möchten.
- Geben Sie unter **SR-Beschreibung** eine Beschreibung der Dienstanforderung ein.

5. Klicken Sie auf **Upload**.

Wenn Sie zum ersten Mal ein Supportpaket an CIS hochladen und noch kein CIS-Konto über ein anderes Produkt erstellt und die Bestimmungen zu Datensammlung und Datenschutz akzeptiert haben, wird das folgende Dialogfeld angezeigt. Sie müssen die Bestimmungen akzeptieren, damit ein Upload möglich ist. Wenn Sie ein CIS-Konto haben und die Bestimmungen zuvor akzeptiert haben, erfolgt der Upload des Supportpakets sofort.

6. Lesen Sie die Bestimmungen und klicken Sie auf **Zustimmen und Upload**. Das Supportpaket wird 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.

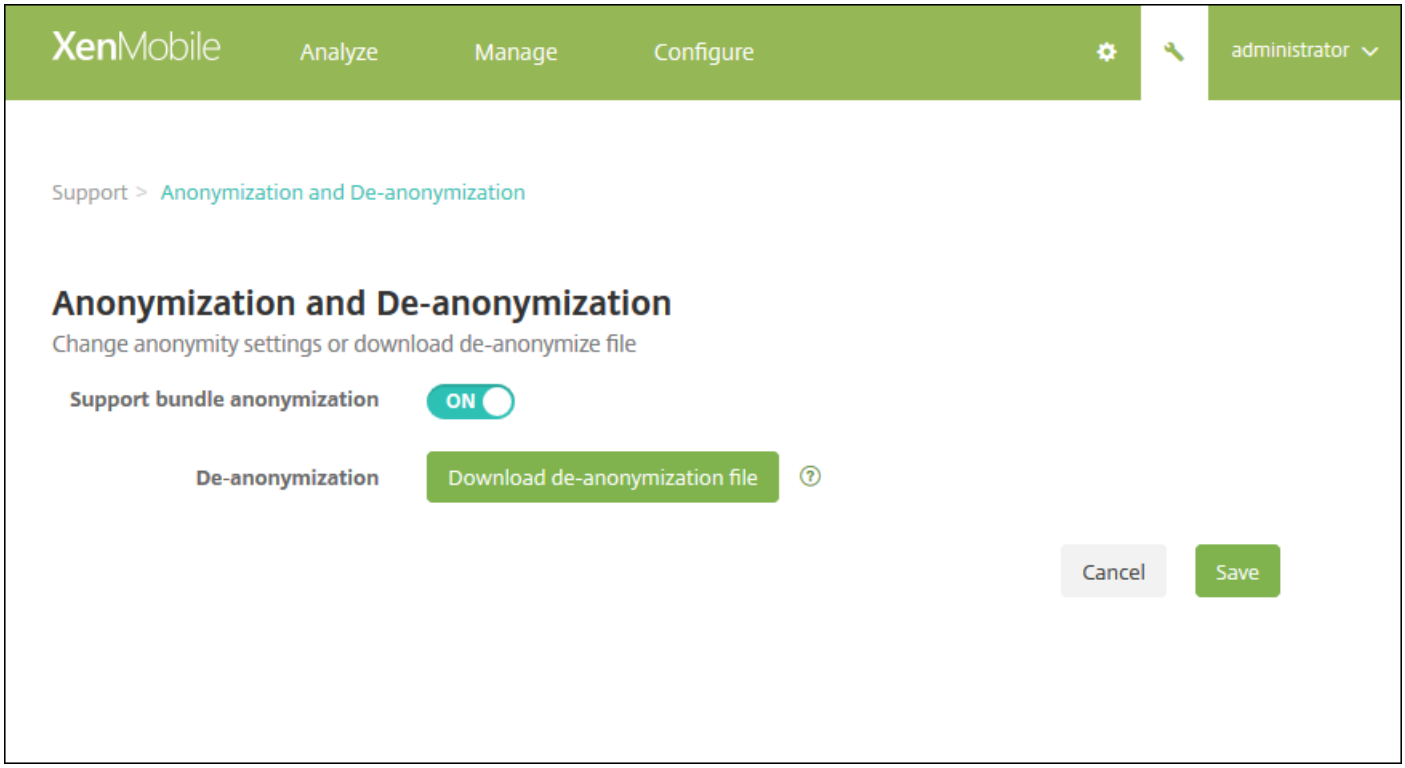
Anonymisierung von Daten in Supportpaketen

Jul 28, 2016

Beim Erstellen von Supportpaketen in XenMobile werden vertrauliche Benutzer-, Server- und Netzwerkdaten standardmäßig anonymisiert. Sie können dieses Verhalten auf der Seite "Anonymisierung und Deanonymisierung" ändern. Sie können auch eine Zuordnungsdatei herunterladen, die XenMobile beim Anonymisieren von Daten speichert. Der Citrix Support fordert diese Datei u. U. an, um für die Suche nach einem Problem bei einem bestimmten Benutzer oder Gerät die Anonymisierung von Daten rückgängig zu machen.

1. Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben. Die Seite **Support** wird angezeigt.

2. Klicken Sie auf der Seite **Support** unter **Erweitert** auf **Anonymisierung und Deanonymisierung**. Die Seite **Anonymisierung und Deanonymisierung** wird angezeigt.



3. Wählen Sie unter **Supportpaketanonymisierung** aus, ob die Daten anonymisiert werden sollen. Die Standardeinstellung ist **EIN**.

4. Klicken Sie neben **Deanonymisierung** auf **Deanonymisierungsdatei herunterladen**, um die Zuordnungsdatei an den Citrix Support zu senden, wenn dieser spezifische Geräte- oder Benutzerinformationen zur Problemdiagnose benötigt.

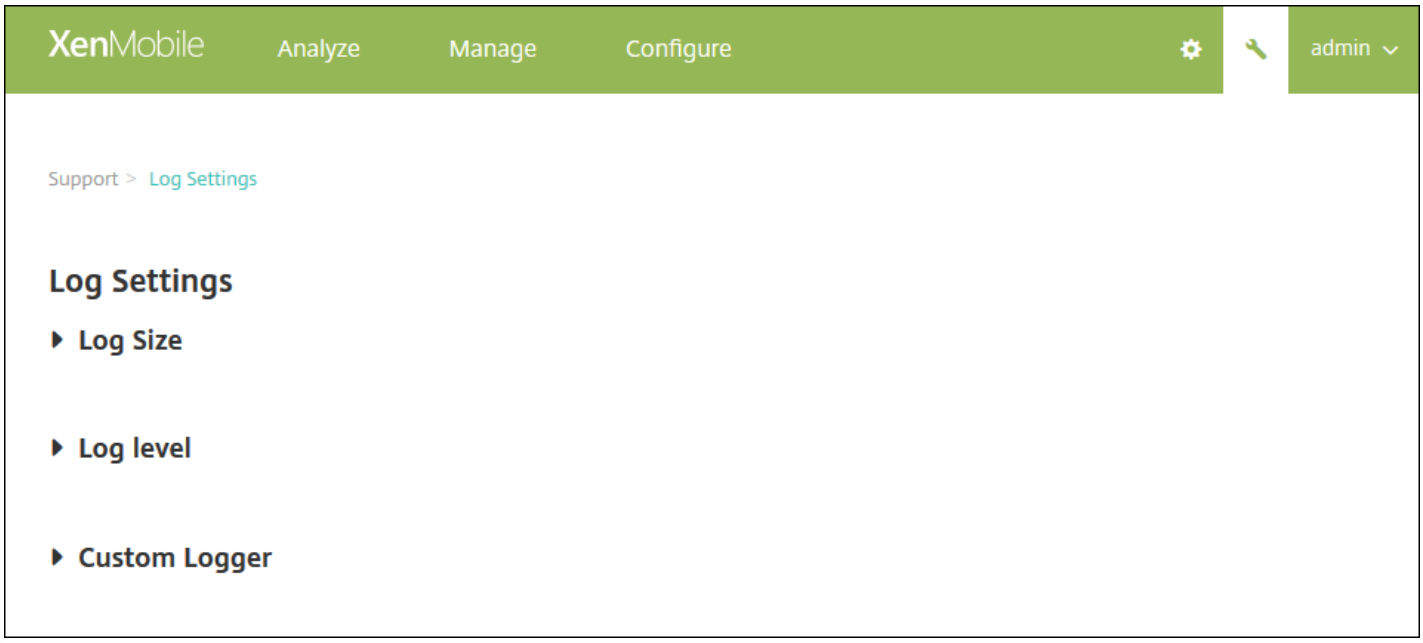
Konfigurieren der Protokolleinstellungen

Jul 28, 2016

Sie können Protokolleinstellungen konfigurieren, um die Ausgabe der von XenMobile generierten Protokolle anzupassen. Wenn Sie XenMobile-Servercluster haben, werden Protokolleinstellungen, die Sie in der XenMobile-Konsole festlegen, auf alle Server im Cluster angewendet.

1. Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben. Die Seite **Support** wird angezeigt.

2. Klicken Sie unter **Protokollvorgänge** auf **Protokolleinstellungen**. Die Seite **Protokolleinstellungen** wird angezeigt.

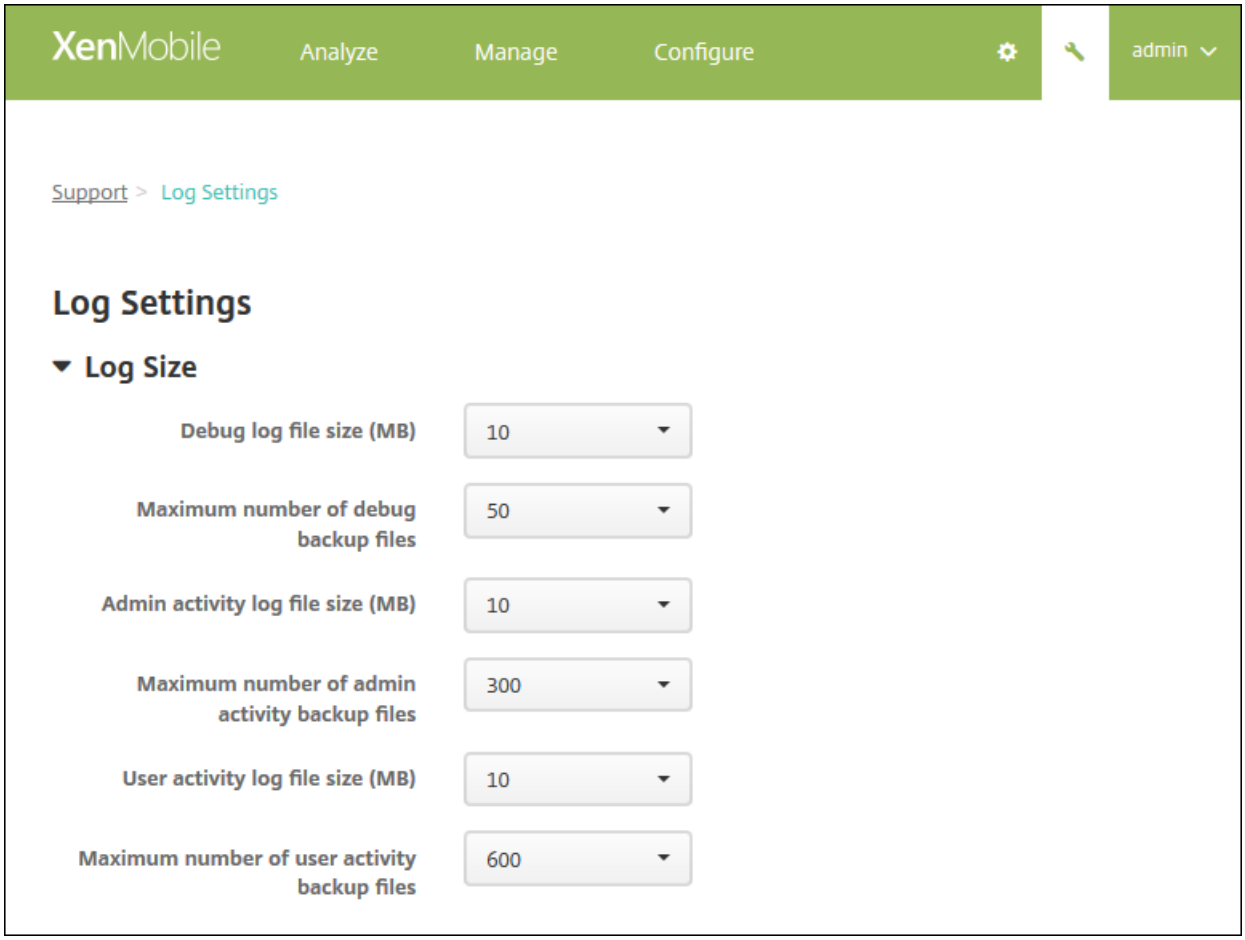


Auf der Seite **Protokolleinstellungen** können Sie folgende Einstellungen ändern:

- **Protokollgröße**: 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).
- **Protokollebene**: Mit dieser Option ändern Sie die Protokollebene oder behalten die Einstellungen bei.
- **Benutzerdefinierte Protokollierung**: Verwenden Sie diese Option zum Erstellen einer benutzerdefinierten Protokollierung. Benutzerdefinierte Protokolle erfordern einen Klassennamen und eine Protokollebene.

Konfigurieren der Protokollgrößenoptionen

1. Erweitern Sie **Protokollgröße** auf der Seite **Protokolleinstellungen**.



2. Konfigurieren Sie die folgenden Einstellungen:

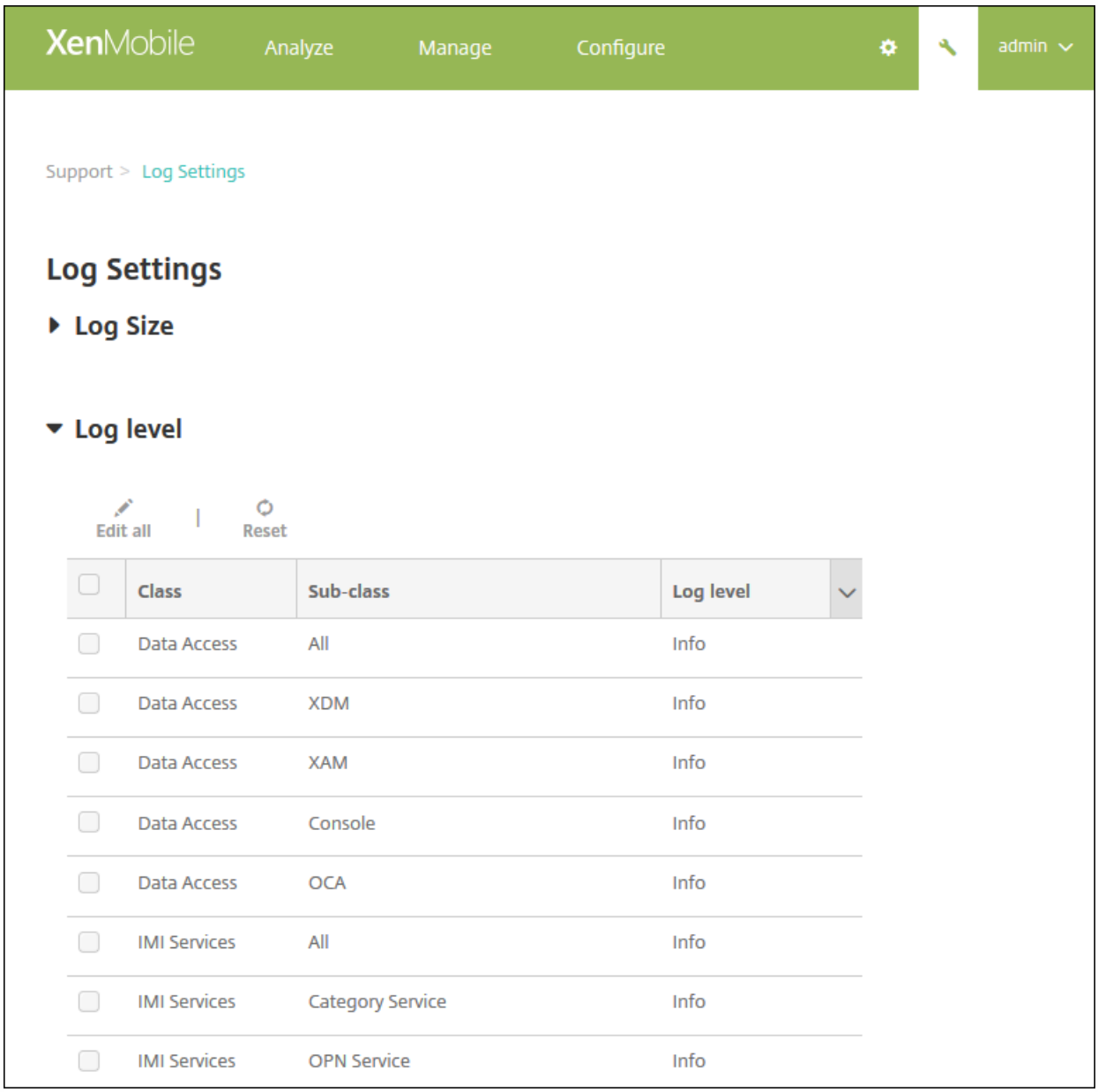
- **Dateigröße des Debugprotokolls (MB)**: Klicken Sie in der Liste auf eine Größe zwischen 5 MB und 20 MB, um die maximale Größe der Debugdatei zu ändern. Die Standarddateigröße ist **10 MB**.
- **Maximale Anzahl der Debugbackupdateien**: Wählen Sie in der Liste aus, wie viele Sicherungskopien der Debugdatei maximal auf dem Server gespeichert werden sollen. Standardmäßig werden von XenMobile 50 Sicherungsdateien auf dem Server gespeichert.
- **Dateigröße des Administratoraktivitätsprotokolls (MB)**: Klicken Sie in der Liste auf eine Größe zwischen 5 MB und 20 MB, um die maximale Größe der Administratoraktivitätsprotokolldatei zu ändern. Die Standarddateigröße ist **10 MB**.
- **Maximale Anzahl der Administratoraktivitätsbackupdateien**: Wählen Sie in der Liste aus, wie viele Sicherungskopien der Administratoraktivitätsprotokolldatei maximal auf dem Server gespeichert werden sollen. Standardmäßig werden von XenMobile 300 Sicherungsdateien auf dem Server gespeichert.
- **Dateigröße des Benutzeraktivitätsprotokolls (MB)**: Klicken Sie in der Liste auf eine Größe zwischen 5 MB und 20 MB, um die maximale Größe der Benutzeraktivitätsprotokolldatei zu ändern. Die Standarddateigröße ist **10 MB**.
- **Maximale Anzahl der Benutzeraktivitätsbackupdateien**: Wählen Sie in der Liste aus, wie viele Sicherungskopien der Benutzeraktivitätsprotokolldatei maximal auf dem Server gespeichert werden sollen. Standardmäßig werden von XenMobile 300 Sicherungsdateien auf dem Server gespeichert.

Konfigurieren der Protokollebene

Mit den Einstellungen für die Protokollebene können Sie angeben, welche Art von Informationen XenMobile im Protokoll sammelt. Sie können die gleiche Ebene für alle Klassen festlegen oder Sie können bestimmte Ebenen für einzelne Klassen

auswählen.

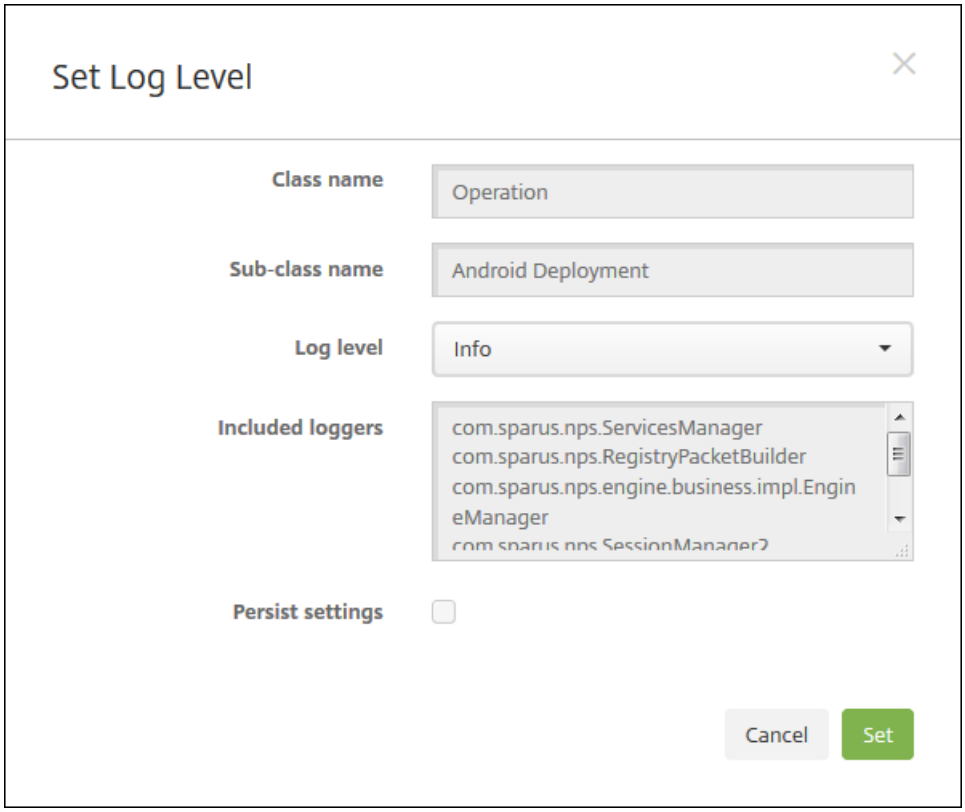
1. Erweitern Sie **Protokollebene** auf der Seite **Protokolleinstellungen**. Die Tabelle mit allen Protokollklassen wird angezeigt.



2. Führen Sie einen der folgenden Schritte aus:

- Aktivieren Sie das Kontrollkästchen neben einer Klasse und klicken Sie dann auf **Ebene einstellen**, um die Protokollebene nur für diese Klasse zu ändern.
- Klicken Sie auf **Alle bearbeiten**, um die Änderung der Protokollebene auf alle Klassen in der Tabelle anzuwenden.

Das Dialogfeld **Protokollebene einstellen** wird angezeigt, in dem Sie die Protokollebene festlegen und auswählen können, ob die ausgewählte Protokollebene beim Neustart des XenMobile-Servers weiterhin gelten soll.

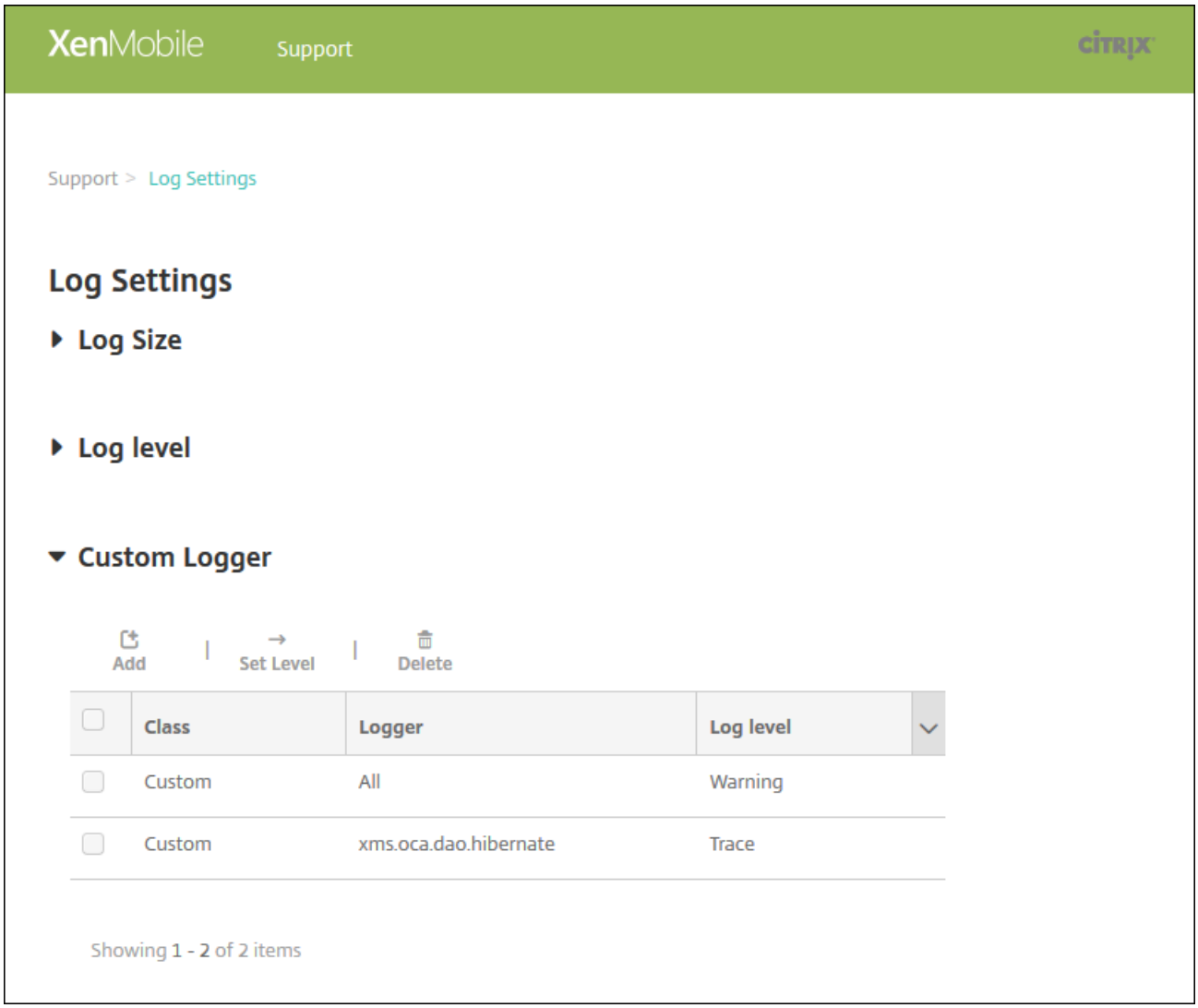


- **Klassenname**: Wenn Sie die Auswahl für alle Klassen ändern, wird in diesem Feld All angezeigt, ansonsten werden die einzelnen Klassennamen angezeigt. Das Feld kann nicht bearbeitet werden.
- **Unterklassenname**: Wenn Sie die Protokollebene für alle Klassen ändern, wird in diesem Feld "Alle" angezeigt, ansonsten werden die einzelnen Unterklassennamen angezeigt. Das Feld kann nicht bearbeitet werden.
- **Protokollebene**: Wählen Sie in der Liste eine Protokollebene aus. Die unterstützten Protokollebenen umfassen:
  - Schwerwiegend
  - Fehler
  - Warnung
  - Info
  - Debug
  - Trace
  - Aus
- **Enthaltene Protokollierung**: Wenn Sie die Protokollebene für alle Klassen ändern, ist dieses Feld leer, ansonsten wird der Name der aktuell konfigurierten Protokollierung für eine einzelne Klasse angezeigt. Das Feld kann nicht bearbeitet werden.
- **Persistente Einstellungen**: Wenn Sie die Protokollebeneneinstellungen beim Neustart des Servers beibehalten möchten, aktivieren Sie dieses Kontrollkästchen. Wenn Sie dieses Kontrollkästchen nicht aktivieren, werden die Protokollebeneneinstellungen beim Neustart des Servers auf die Standardwerte zurückgesetzt.

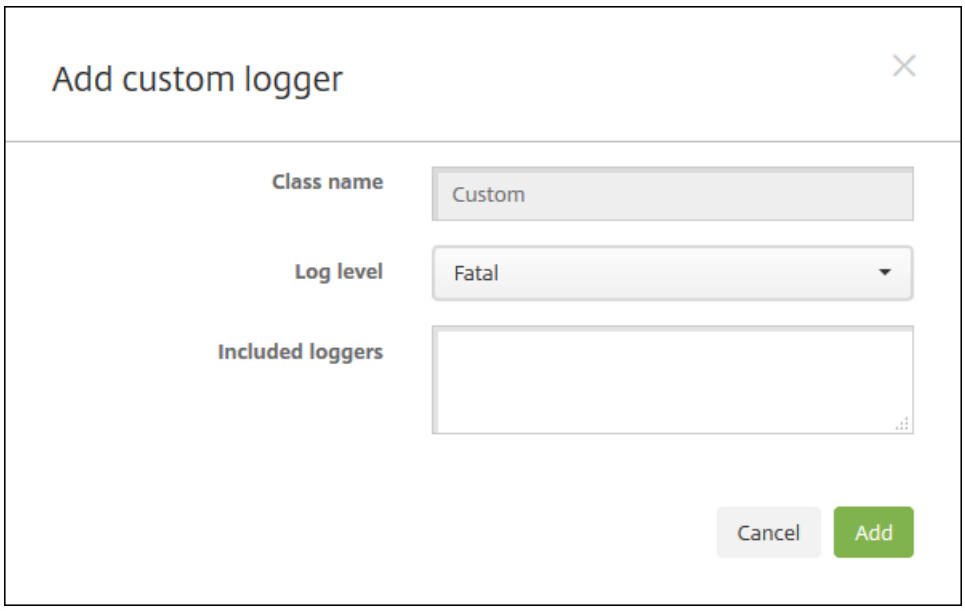
3. Klicken Sie auf **Festlegen**, um die Änderungen zu übergeben.

Hinzufügen einer benutzerdefinierten Protokollierung

1. Erweitern Sie **Benutzerdefinierte Protokollierung** auf der Seite **Protokolleinstellungen**. Die Tabelle **Benutzerdefinierte Protokollierung** wird angezeigt. Wenn Sie noch keine benutzerdefinierte Protokollierung hinzugefügt haben, ist die Tabelle zunächst leer.



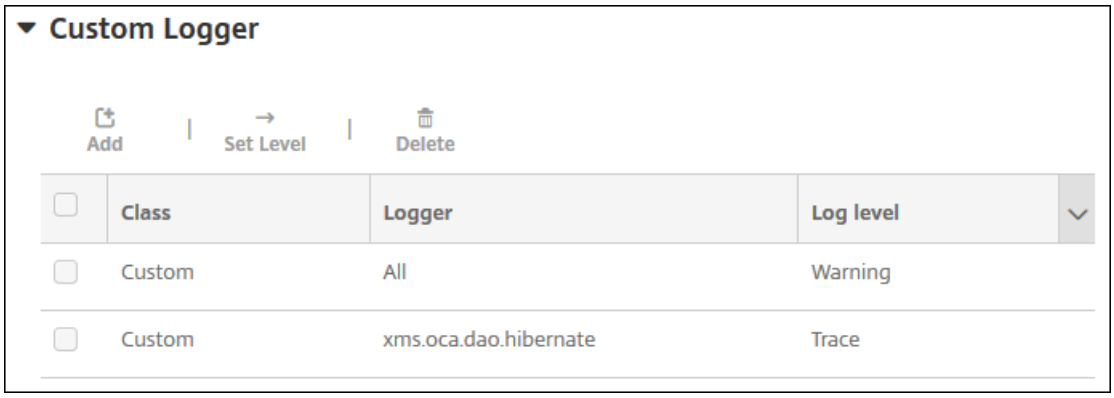
2. Klicken Sie auf **Hinzufügen**. Das Dialogfeld **Benutzerdefinierte Protokollierung hinzufügen** wird angezeigt.



3. Konfigurieren Sie die folgenden Einstellungen:

- **Klassenname**: Im Feld wird **Benutzerdefiniert** angezeigt und es kann nicht bearbeitet werden.
- **Protokollebene**: Wählen Sie in der Liste eine Protokollebene aus. Die unterstützten Protokollebenen umfassen:
  - Schwerwiegend
  - Fehler
  - Warnung
  - Info
  - Debug
  - Trace
  - Aus
- **Enthaltene Protokollierung**: Geben Sie die Protokollierungen ein, die Sie in der benutzerdefinierten Protokollierung einschließen möchten, oder lassen Sie das Feld leer, um alle Protokollierungen einzuschließen.

4. Klicken Sie auf **Hinzufügen**. Die benutzerdefinierte Protokollierung wird der Tabelle **Benutzerdefinierte Protokollierung** hinzugefügt.



Löschen einer benutzerdefinierten Protokollierung

1. Erweitern Sie **Benutzerdefinierte Protokollierung** auf der Seite **Protokolleinstellungen**.

2. Wählen Sie die benutzerdefinierte Protokollierung aus, die Sie löschen möchten.

3. Klicken Sie auf **Löschen**. In einem Dialogfeld werden Sie gefragt, ob Sie die benutzerdefinierte Protokollierung wirklich löschen möchten. Klicken Sie auf **OK**.

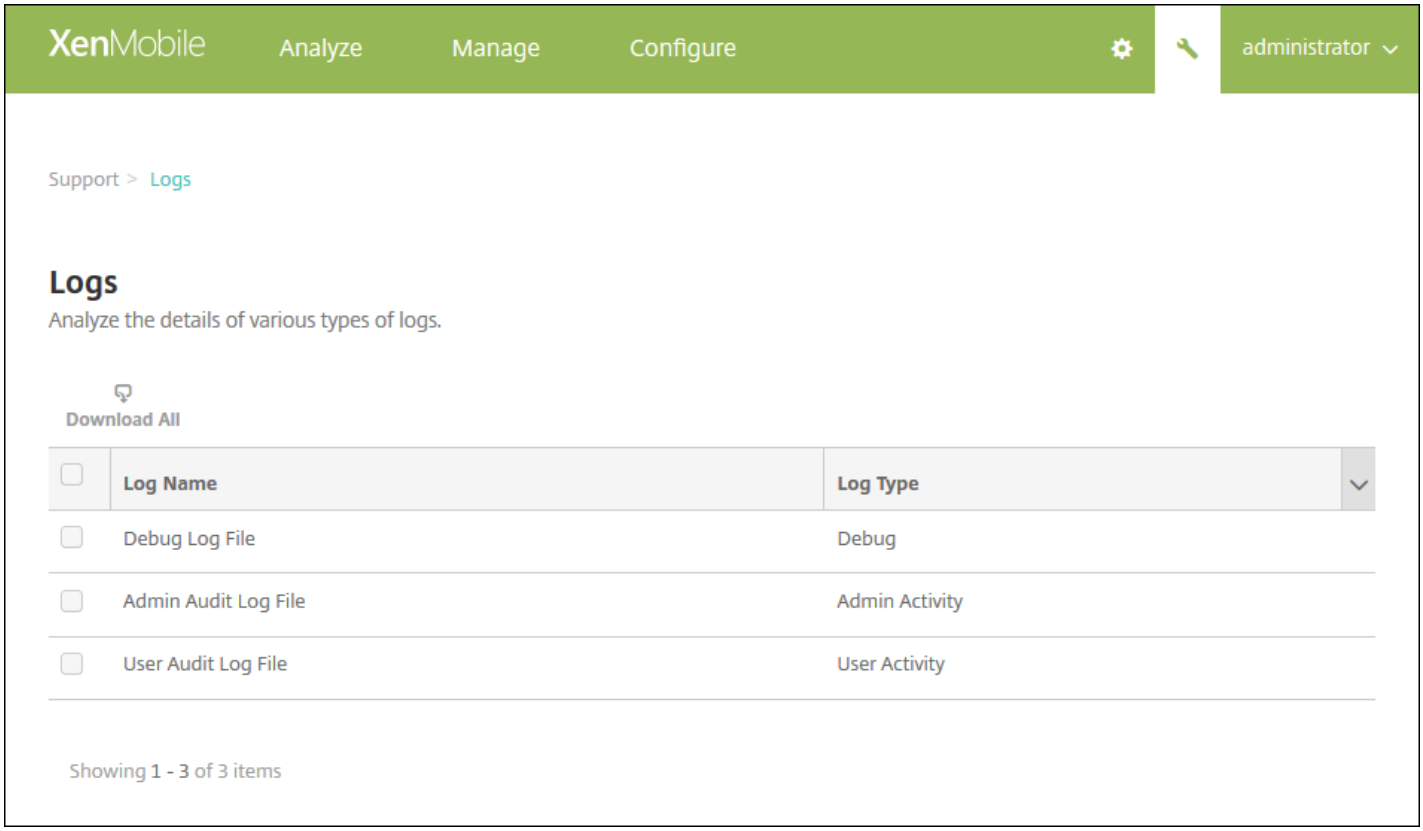
Wichtig: Sie können diesen Vorgang nicht rückgängig machen.

Anzeigen und Analysieren von Protokolldateien in XenMobile

Jul 28, 2016

1. Klicken Sie in der XenMobile-Konsole auf das Schraubenschlüsselsymbol rechts oben. Die Seite **Support** wird geöffnet.

2. Klicken Sie unter **Protokollvorgänge** auf **Protokolle**. Die Seite **Protokolle** wird angezeigt. Einzelne Protokolle werden in einer Tabelle angezeigt.



3. Wählen Sie das Protokoll aus, das Sie anzeigen möchten:

- Debugprotokolle enthalten nützliche Informationen für den Citrix Support, z. B. Fehlermeldungen und serverbezogene Aktionen.
- Administratorüberwachungsprotokolle enthalten Auditinformationen über Aktivitäten auf der XenMobile-Konsole.
- Benutzerüberwachungsprotokolle enthalten Informationen über konfigurierte Benutzer.

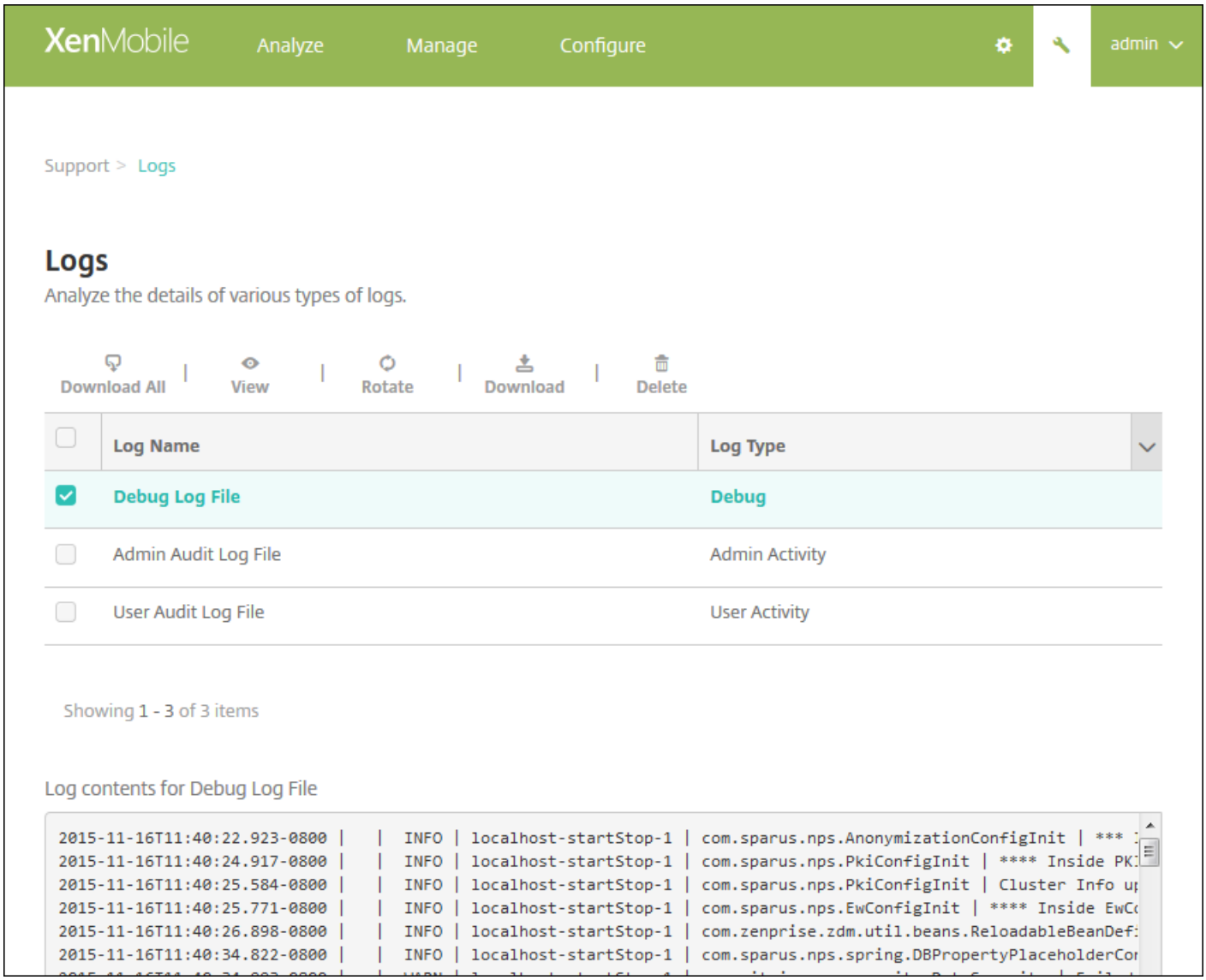
4. Verwenden Sie die Aktionen oberhalb der Tabelle zum Herunterladen aller oder einzelner Protokolle und zum Anzeigen, Archivieren und Löschen des ausgewählten Protokolls.

Hinweis:

- Wenn Sie mehr als eine Protokolldatei auswählen, sind nur die Aktionen **Alle herunterladen** und **Löschen** verfügbar.
- Wenn Sie XenMobile-Servercluster haben, können Sie nur die Protokolle für den Server anzeigen, mit dem Sie verbunden sind. Zum Anzeigen von Protokollen für die anderen Server verwenden Sie eine der Downloadoptionen.

5. Führen Sie einen der folgenden Schritte aus:

- **Alle herunterladen**: Es werden alle Protokolle im System (Debug-, Admin-Audit-, Benutzer-Audit-, Serverprotokolle usw.) heruntergeladen.
- **Anzeigen**: Zeigt den Inhalt des ausgewählten Protokolls unterhalb der Tabelle an.
- **Archivieren**: 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 **Archivieren**, um fortzufahren.
- **Herunterladen**: Die Konsole lädt nur den ausgewählten Protokolldateityp herunter und alle archivierten Protokolle dieses Typs.
- **Löschen**: Löscht die ausgewählten Protokolldateien dauerhaft.



Remote Support

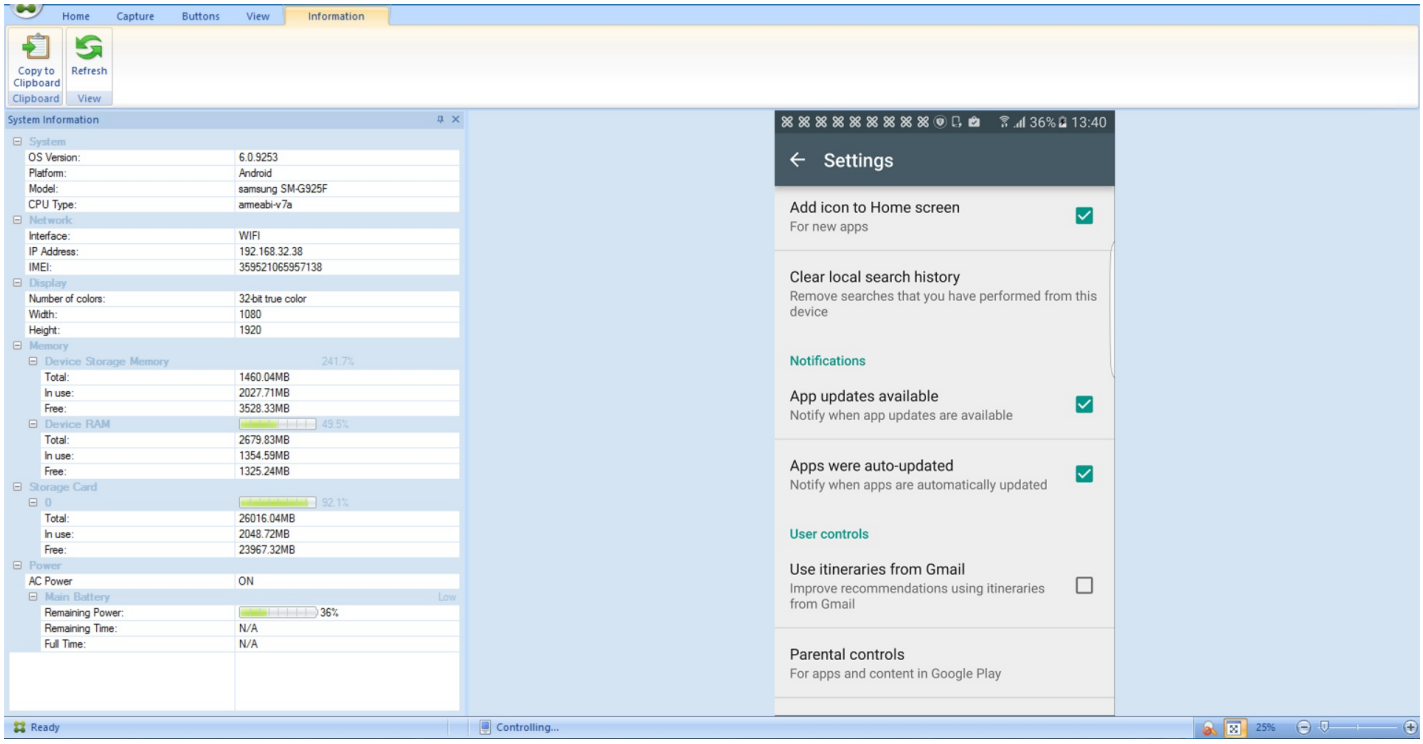
Jul 28, 2016

Durch Remote Support können Helpdesk-Mitarbeiter die Steuerung verwalteter Windows- und Android-Mobilgeräte übernehmen. Remote Support ist auf allen Windows-Mobilgeräten und auf Android Samsung SAFE-Geräten verfügbar. Die Remotesteuerung von iOS-Geräten wird nicht unterstützt.

> ## Hinweis
>
> XenMobile Remote Support ist in XenMobile Cloud-Versionen 10.x nicht verfügbar.

Während einer Remotesteuerungssitzung:

- Benutzern wird auf ihrem Mobilgerät durch ein Symbol angezeigt, dass eine Remotesteuerungssitzung aktiv ist.
- Remote Support-Mitarbeiter sehen das Remote Support-Anwendungsfenster und ein Remotesteuerungsfenster mit einer Darstellung des gesteuerten Geräts.



Remote Support bietet die folgenden Funktionen:

- Remoteanmeldung an dem Mobilgerät eines Benutzers und Steuerung des Bildschirms. Benutzer können sehen, was Sie auf dem Bildschirm machen. Dies kann auch für Schulungszwecke genutzt werden.
- Navigieren und Reparieren von Remotegeräten in Echtzeit. Sie können die Konfigurationen eines Geräts ändern, Betriebssystemprobleme behandeln und problematische Anwendungen und Prozesse deaktivieren oder beenden.
- Isolieren und Eindämmen von Bedrohungen, bevor sie andere mobile Geräte befallen, indem der Netzwerkzugriff deaktiviert, schadhafte Prozesse beendet und Apps oder Malware entfernt wird.

- Geräte können per Remotesteuerung zum Klingeln gebracht bzw. angerufen werden, damit Benutzer es wiederfinden. Wenn ein Benutzer sein Gerät nicht finden kann, können Sie die Daten darauf löschen, um sicherzustellen, dass die vertraulichen Daten nicht gestohlen werden.

Remote Support ermöglicht Supportmitarbeitern Folgendes:

- Anzeigen einer Liste aller mit XenMobile-Servern verbundenen Geräte
- Anzeigen von Systeminformationen einschließlich Gerätemodell, Betriebssystemversion, Seriennummer und IMEI (International Mobile Station Equipment Identity)-Nummer, Speicher- und Batteriestatus sowie Konnektivität.
- Anzeigen der Benutzer und Gruppen der XenMobile-Server.
- Ausführen des Task-Managers des Geräts, in dem aktive Prozesse angezeigt und beendet sowieso das Mobilgerät neu gestartet werden kann
- Ausführen von Remotedateiübertragungen, mit denen Dateien in beide Richtungen zwischen Mobilgeräten und einem zentralen Dateiserver übertragen werden
- Herunterladen und Installieren von Softwareprogrammen als Batchvorgang auf einem oder mehreren Mobilgerät(en)
- Konfigurieren von Remote-Registrierungsschlüsseleinstellungen auf dem Gerät
- Optimieren der Reaktionszeit in Mobilfunknetzen mit geringer Bandbreite durch Verwendung von Echtzeit-Gerätebildschirmremotesteuerung
- Anzeigen der Geräteskin für die meisten Mobilgerätemarken und -modelle. Anzeigen eines Skin-Editors, um neue Gerätemodelle hinzuzufügen und physische Tasten zuzuordnen.
- Aktivieren der Funktionen zur Aufnahme des Gerätebildschirms, Aufzeichnung und Wiedergabe, sodass Aktionsfolgen auf dem Gerät aufgenommen und in einer AVI-Videodatei gespeichert werden können
- Durchführen von Live-Besprechungen, bei denen ein gemeinsames Whiteboard, Chat und VoIP-basierte Sprachübertragung zwischen dem Mobilgerätebenutzer und Supportmitarbeitern eingesetzt werden können

Systemanforderungen für Remote Support

Für die Installation der Remote Support-Software müssen Windows-basierte Computer die folgenden Anforderungen erfüllen. Informationen zu den Portanforderungen finden Sie unter Portanforderungen.

Unterstützte Plattformen

- Intel Xeon/Pentium 4, 1 GHz mindestens (Computer der Klasse Arbeitsstation)
- mindestens 512 MB RAM
- Mindestens 100 MB freier Speicherplatz auf dem Datenträger

Unterstützte Betriebssysteme

- Microsoft Windows 2003 Server Standard Edition bzw. Enterprise Edition SP1 oder höher
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 oder höher
- Microsoft Windows Vista SP1 oder höher
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

Installieren der Remote Support-Software

1. Damit Sie das Installationsprogramm für Remote Support von der XenMobile 10-Downloadseite herunterladen können, müssen Sie sich mit Ihrem Konto anmelden.
2. Erweitern Sie **Tools** und laden Sie XenMobile Remote Support v9 herunter.
   Der Remote Support-Dateiname ist zurzeit XenMobileRemoteSupport-9.0.0.35265.exe.
3. Doppelklicken Sie auf das Remote Support-Installationsprogramm und folgen Sie den Anweisungen im Installationsassistenten.

Installieren von Remote Support von der Befehlszeile aus:

Führen Sie den folgenden Befehl aus:

RemoteSupport.exe /S

wobei *RemoteSupport* der Name des Installationsprogramms ist. Beispiel:

XenMobileRemoteSupport-9.0.0.35265.exe /S

Beim Installieren der Remote Support-Software können Sie die folgenden Variablen verwenden:

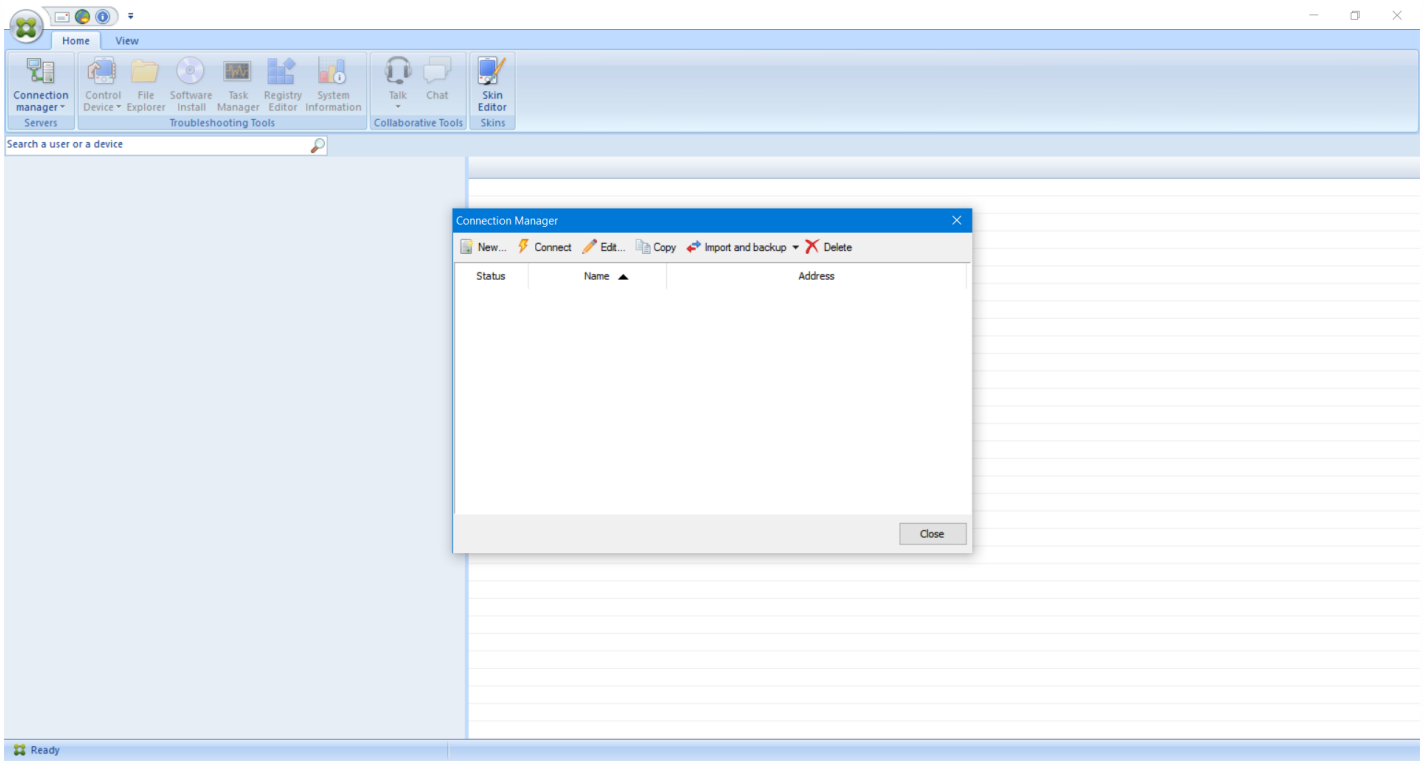
- /S: zur automatischen Installation der Remote Support-Software mit den Standardparametern
- /D=dir: zum Angeben eines benutzerdefinierten Installationsverzeichnisses

Herstellen einer Verbindung zwischen Remote Support und XenMobile

Um Remotesupportverbindungen mit verwalteten Geräten herzustellen, müssen Sie eine Verbindung von Remote Support zu den XenMobile-Servern herstellen, die die Geräte verwalten. Diese Verbindung erfolgt über einen App-Tunnel, der in der Tunnelrichtlinie definiert wird. Die Tunnelrichtlinie ist eine Richtlinie für Android- und Windows Mobile-/CE-Geräte. Der App-Tunnel muss wie unter App-Tunnelrichtlinien für Geräte definiert werden, bevor Sie eine Verbindung zwischen Remote Support und XenMobile herstellen können.

1. Starten Sie die Remote Support-Software und melden Sie sich mit Ihren XenMobile-Anmeldeinformationen an.

2. Klicken Sie im **Verbindungs-Manager** auf **New**.



3. Geben Sie im Dialogfeld **Connection Configuration** auf der Registerkarte **Server** folgende Werte ein:

   Geben Sie in **Configuration name** einen Namen für die Konfiguration ein.

   Geben Sie in **Server IP address or name** die IP-Adresse oder den DNS-Namen des XenMobile-Servers ein.

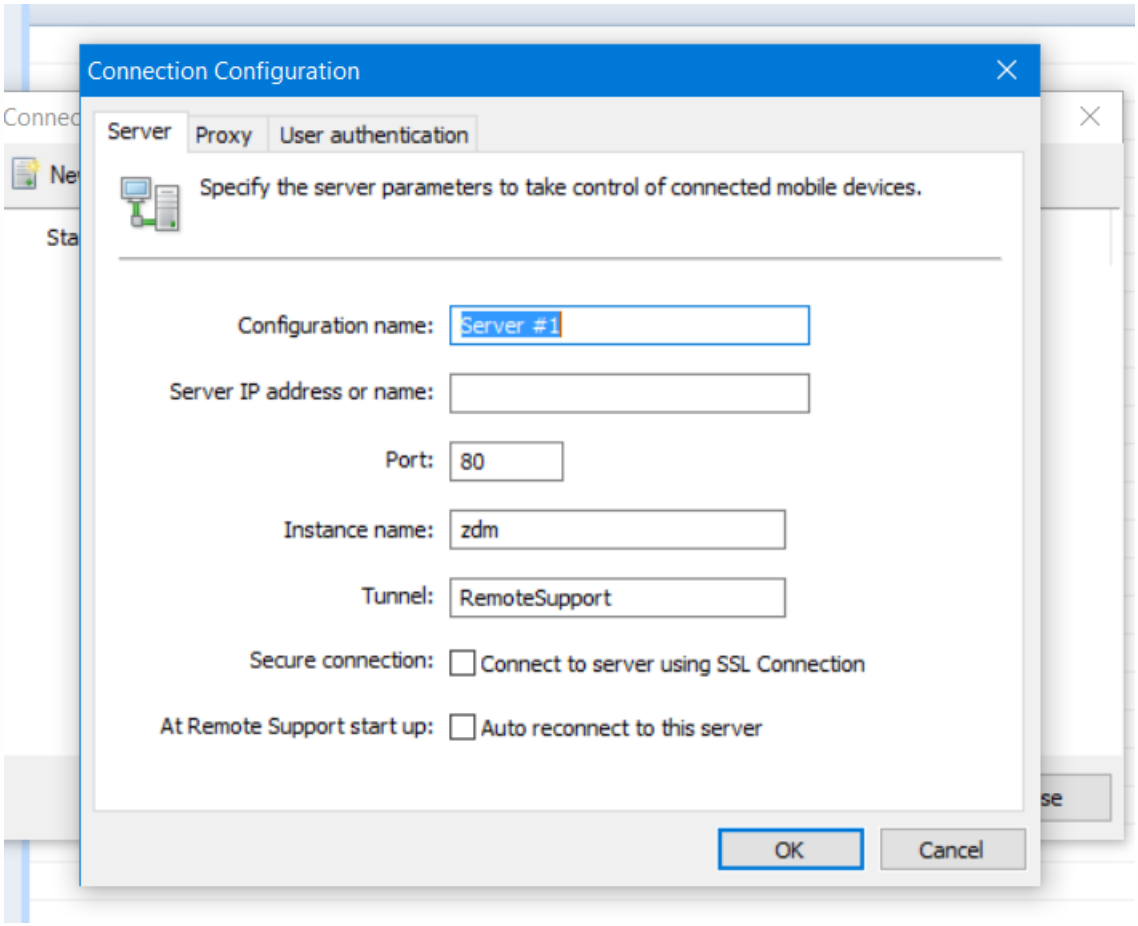
   Geben Sie in **Port** eine TCP-Portnummer gemäß der XenMobile-Serverkonfiguration ein.

   Geben Sie in **Instance name** einen Instanznamen ein, wenn XenMobile Teil einer Bereitstellung mit mehreren Mandanten ist.

   Geben Sie in **Tunnel** den Namen der Tunnelrichtlinie ein.

   Aktivieren Sie das Kontrollkästchen **Connect to server using SSL Connection**.

   Aktivieren Sie das Kontrollkästchen **Auto reconnect to this server**, damit beim Start der Remote Support-Anwendung immer eine Verbindung zu dem konfigurierten XenMobile-Server hergestellt wird.



4. Aktivieren Sie auf der Registerkarte **Proxy** die Option **Use a http proxy server** und geben Sie die folgenden Informationen ein:

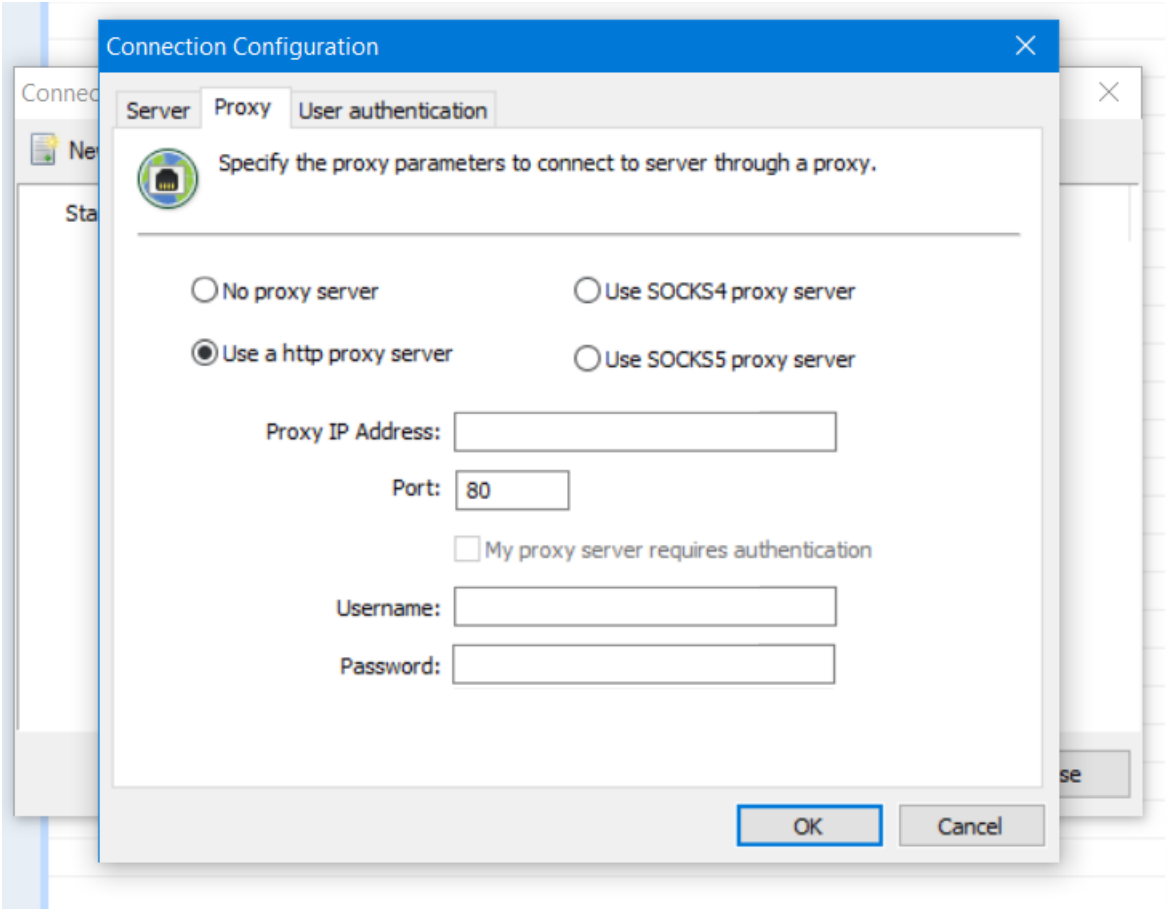
Geben Sie in **Proxy IP Address** die IP-Adresse des Proxyservers ein.

Geben Sie in **Port** die Nummer des TCP-Ports des Proxyservers ein.

Aktivieren Sie das Kontrollkästchen **My proxy server requires authentication**, wenn der Proxyserver eine Authentifizierung erfordert, um Verkehr zuzulassen.

Geben Sie in **Username** den Benutzernamen für die Authentifizierung auf dem Proxyserver ein.

Geben Sie in **Password** das Kennwort für die Authentifizierung auf dem Proxyserver ein.



5. Aktivieren Sie auf der Registerkarte **User Authentication** das Kontrollkästchen **Remember my login and password** und geben Sie die Anmeldeinformationen ein.

6. Klicken Sie auf **OK**.

Zum Herstellen einer Verbindung mit XenMobile doppelklicken Sie auf die Verbindung, die Sie erstellt haben, und geben Sie dann den für die Verbindung konfigurierten Benutzernamen und das Kennwort ein.

Aktivieren von Remotesupport für Samsung Knox-Geräte

Sie erstellen eine Remotesupportrichtlinie in XenMobile, um Remotezugriff auf Samsung

KNOX-Geräte zu erhalten. Sie können Support zweierlei Art konfigurieren:

- Einfacher Remotesupport: 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.
- Premiumremotesupport: 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.

Weitere Informationen zur Konfiguration der Remotesupportrichtlinie finden Sie unter Geräterichtlinie für Remotesupport.

Verwenden einer Remote Support-Sitzung

Wenn Sie Remote Support gestartet haben, werden im linken Bereich des Anwendungsfensters von Remote Support XenMobile-Benutzergruppen so angezeigt, wie sie in der XenMobile-Verwaltungskonsole definiert wurden. Standardmäßig werden nur Gruppen angezeigt, die derzeit verbundene Benutzer enthalten. Sie können das Gerät für jeden Benutzer neben dem Benutzereintrag sehen.

1. Zum Anzeigen aller Benutzer erweitern Sie jede Gruppe in der linken Spalte.
   Die derzeit mit dem XenMobile-Server verbundenen Benutzer sind durch ein grünes Symbol gekennzeichnet.
2. Zum Anzeigen aller Benutzer, einschließlich der derzeit nicht verbundenen, klicken Sie auf **View** und wählen Sie **Non-connected devices**.
   Nicht verbundene Benutzer werden ohne grünes Symbol angezeigt.

Geräte mit einer Verbindung mit dem XenMobile-Server, die keinem Benutzer zugewiesen sind, sind als anonym gekennzeichnet. (Die Zeichenfolge **Anonymous** wird in der Liste angezeigt.) Sie können diese Geräte genauso wie die Geräte angemeldeter Benutzer steuern.

Sie steuern ein Gerät, indem Sie auf die Zeile des Geräts und dann auf **Control Device** klicken. Eine Darstellung des Geräts wird im Remotesteuerungsfenster angezeigt. Mit den folgenden Methoden können Sie mit einem gesteuerten Gerät interagieren:

- Remotesteuerung des Gerätebildschirms einschließlich Steuerung mit Farben im Hauptfenster oder in einem eigenen, unverankerten Fenster
- Erstellen einer VoIP-Sitzung zwischen Helpdesk und Benutzer Konfigurieren von VoIP-Einstellungen
- Erstellen eines Chats mit dem Benutzer
- Zugreifen auf den Task-Manager des Geräts zum Verwalten von Objekten, wie Speicher- und CPU-Auslastung und den ausgeführten Anwendungen
- Durchsuchen der lokalen Verzeichnisse des Mobilgeräts Übertragen von Dateien
- Bearbeiten der Registrierung auf Windows Mobilgeräten
- Anzeigen von Gerätesysteminformationen und der installierten Software
- Aktualisieren des Status der Verbindung zwischen Mobilgerät und XenMobile-Server

Optionen für die XenMobile-Befehlszeilenschnittstelle

Jul 28, 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 Analyzer

Oct 13, 2016

XenMobile Analyzer ist ein cloudbasiertes Tool, mit dem Sie mit XenMobile zusammenhängende Installationsprobleme und Probleme mit anderen Features diagnostizieren und beheben können. Das Tool überprüft Ihre XenMobile-Umgebung auf Probleme bei der Registrierung und Authentifizierung von Geräten und Benutzern.

Damit die Prüfungen ausgeführt werden, müssen Sie das Tool konfigurieren, sodass es auf den XenMobile-Server verweist, und Sie müssen Informationen angeben, z. B. Serverbereitstellungstyp, mobile Plattform, Authentifizierungstyp und die Anmeldeinformationen des Benutzers für den Test. Das Tool stellt dann eine Verbindung mit dem Server her und scannt die Umgebung auf Konfigurationsprobleme. Wenn XenMobile Analyzer Probleme erkennt, gibt das Tool Empfehlungen zum Beheben der Probleme.

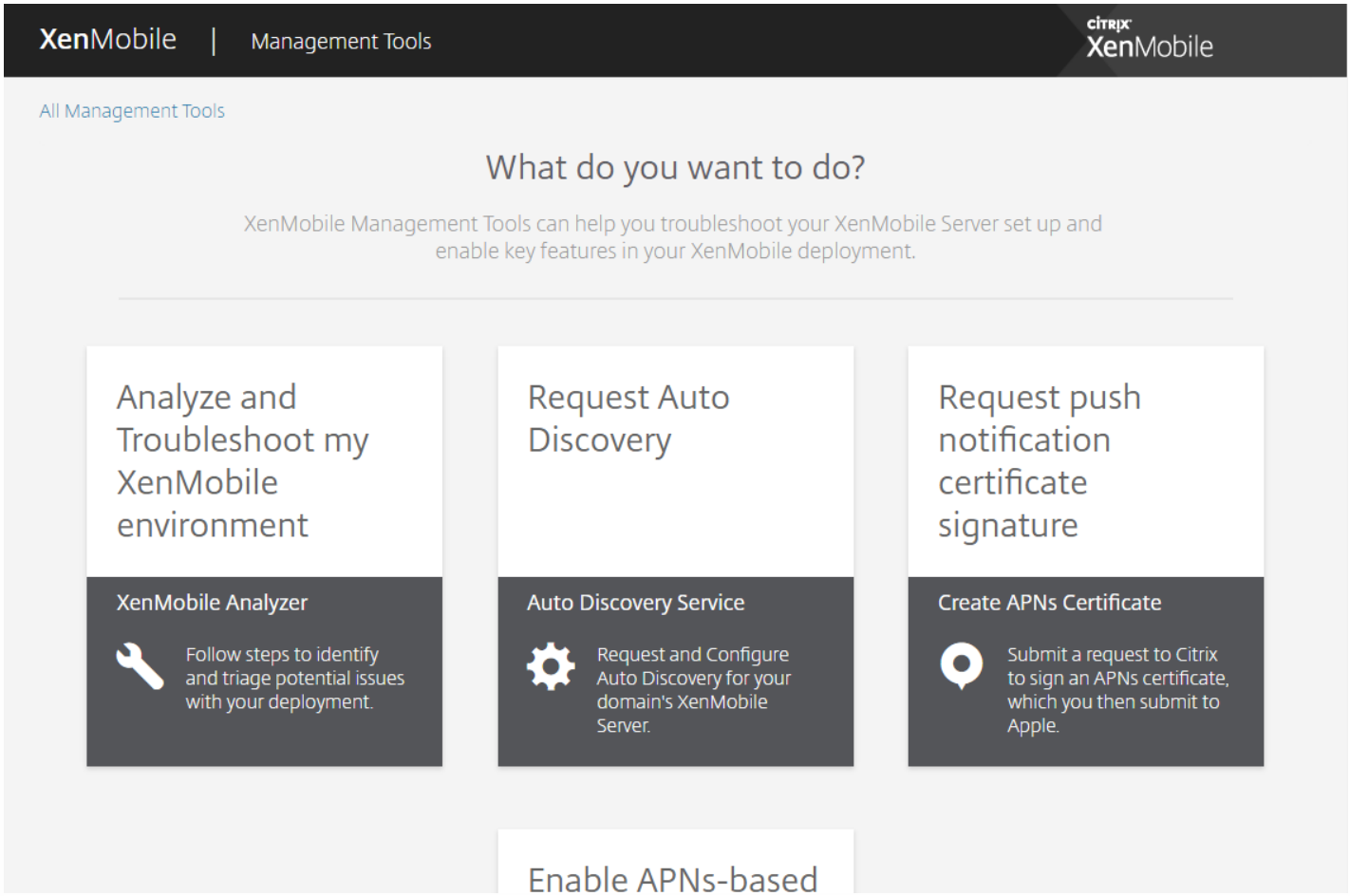
XenMobile Analyzer – Hauptfeatures

- Sicherer, cloudbasierter Dienst zur Behandlung von mit XenMobile verbundenen Problemen.
- Zielgenaue Empfehlungen bei XenMobile-Konfigurationsproblemen.
- Reduzierte Anzahl von Supportanrufen und schnellere Problembehandlung in XenMobile-Umgebungen.
- Zero-Day-Support für Releases von XenMobile Server.
- Aktivierung benutzerdefinierter iOS-Registrierung: benutzerdefinierte Portunterstützung für XenMobile (auf anderen Ports als 8443).
- Anzeige eines Zertifikatannahmedialogfelds für nicht vertrauenswürdige oder unvollständige Serverzertifikate.
- Automatische Ermittlung von zweistufigen Authentifizierungsszenarios.
- WorxWeb-Tests für Erreichbarkeit von Intranetsites.
- WorxMail Auto Discovery Service-Prüfungen.
- ShareFile Single Sign-On-Prüfungen.
- Benutzerdefinierte Portunterstützung für NetScaler.
- Unterstützung für nicht englischsprachige Browser.

Voraussetzungen

Produkt	Unterstützte Version
XenMobile-Server	10.3.0 - 10.3.6
NetScaler Gateway	10.5 - 11.1
Simulation der Clientregistrierung	iOS und Android

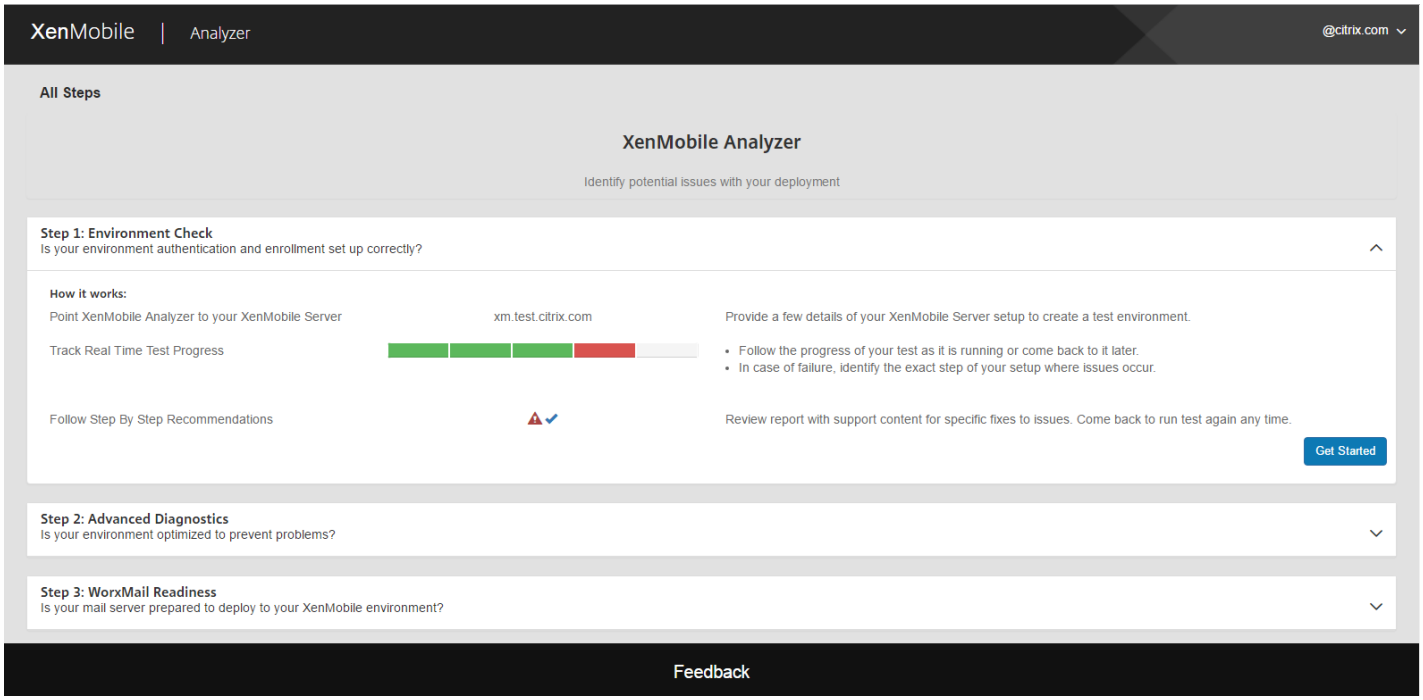
Mit Ihren Citrix Anmeldeinformationen können Sie auf das Tool unter https://xenmobiletools.citrix.com zugreifen. Die XenMobile-Seite für Verwaltungstools wird geöffnet. Klicken Sie hier auf **Analyze and Troubleshoot my XenMobile Environment**, um XenMobile Analyzer zu starten.



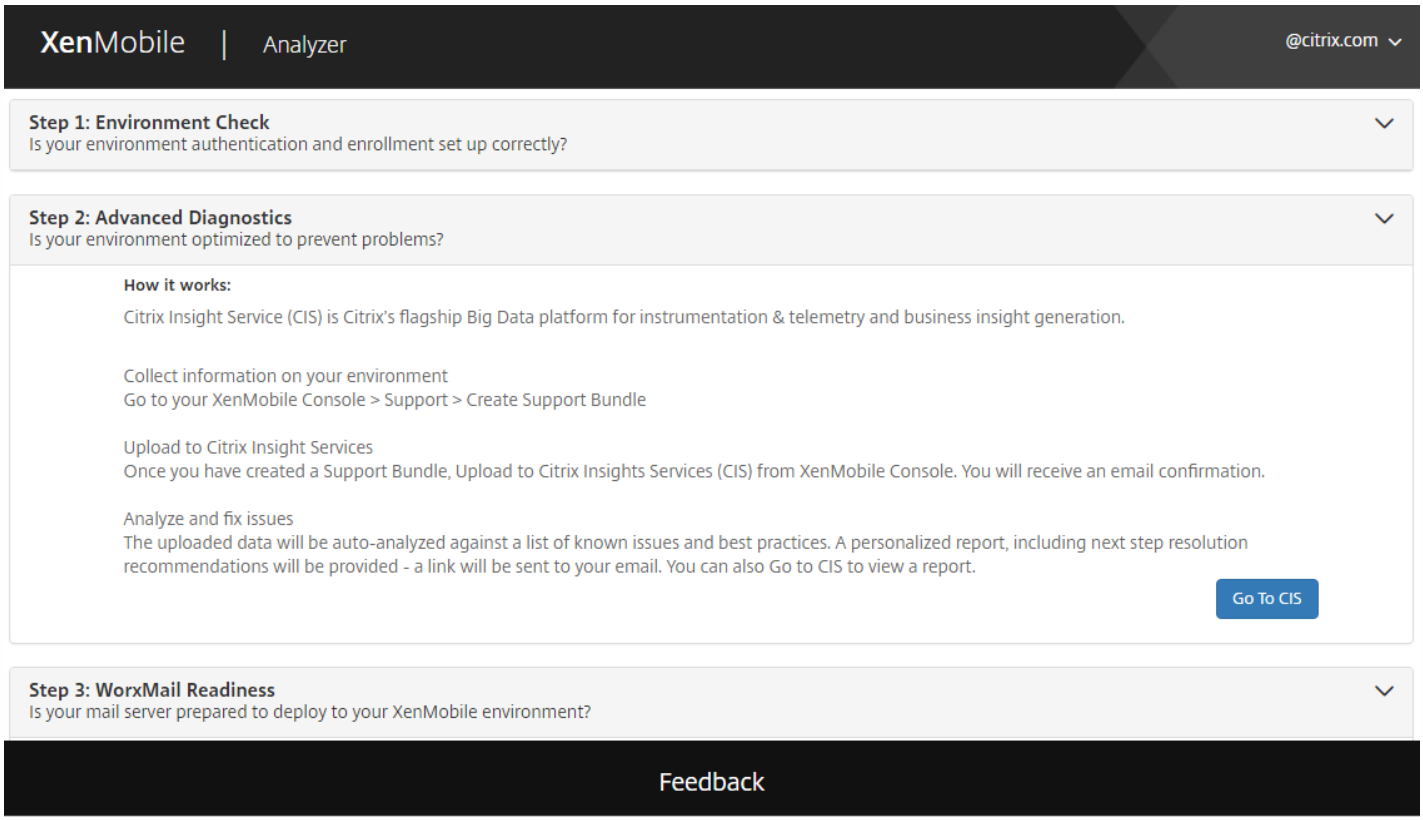
XenMobile Analyzer umfasst fünf Hauptschritte, die Sie durch den Selektierungsvorgang führen. Auf diese Weise lässt sich die Anzahl an Supporttickets reduzieren, wodurch sich die Kosten verringern.

Führen Sie die folgenden Schritte aus:

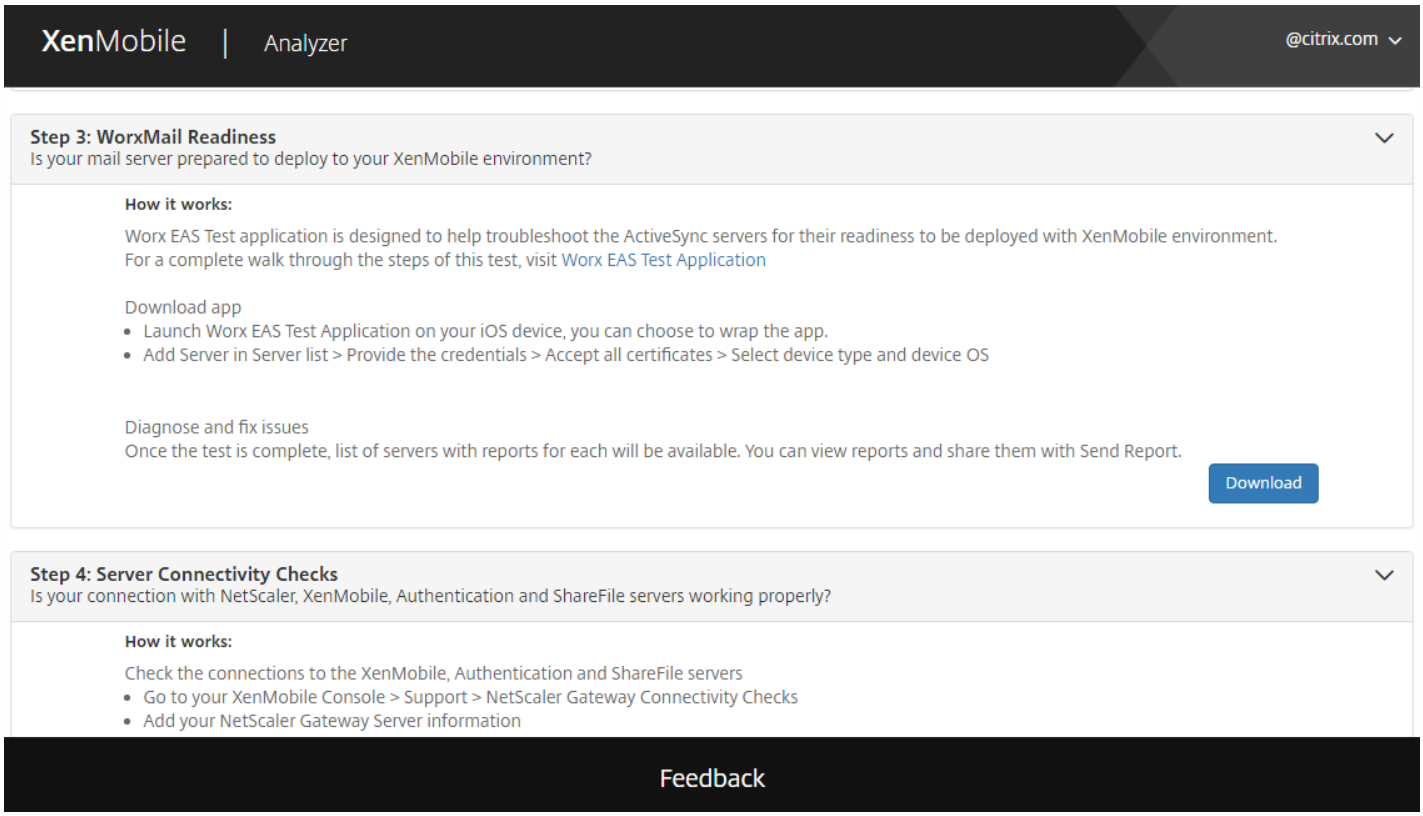
1. **Environment Check**: In diesem Schritt richten Sie Tests ein, um das Setup auf Probleme zu prüfen. Der Schritt bietet auch Empfehlungen und Lösungen zu Problemen bei der Registrierung und Authentifizierung von Geräten und Benutzern.



2. **Advanced Diagnostics**: In diesem Schritt erhalten Sie Informationen zur Verwendung von Citrix Insight Services, um weitere Probleme zu finden, die beim Überprüfen der Umgebung möglicherweise nicht gefunden wurden.

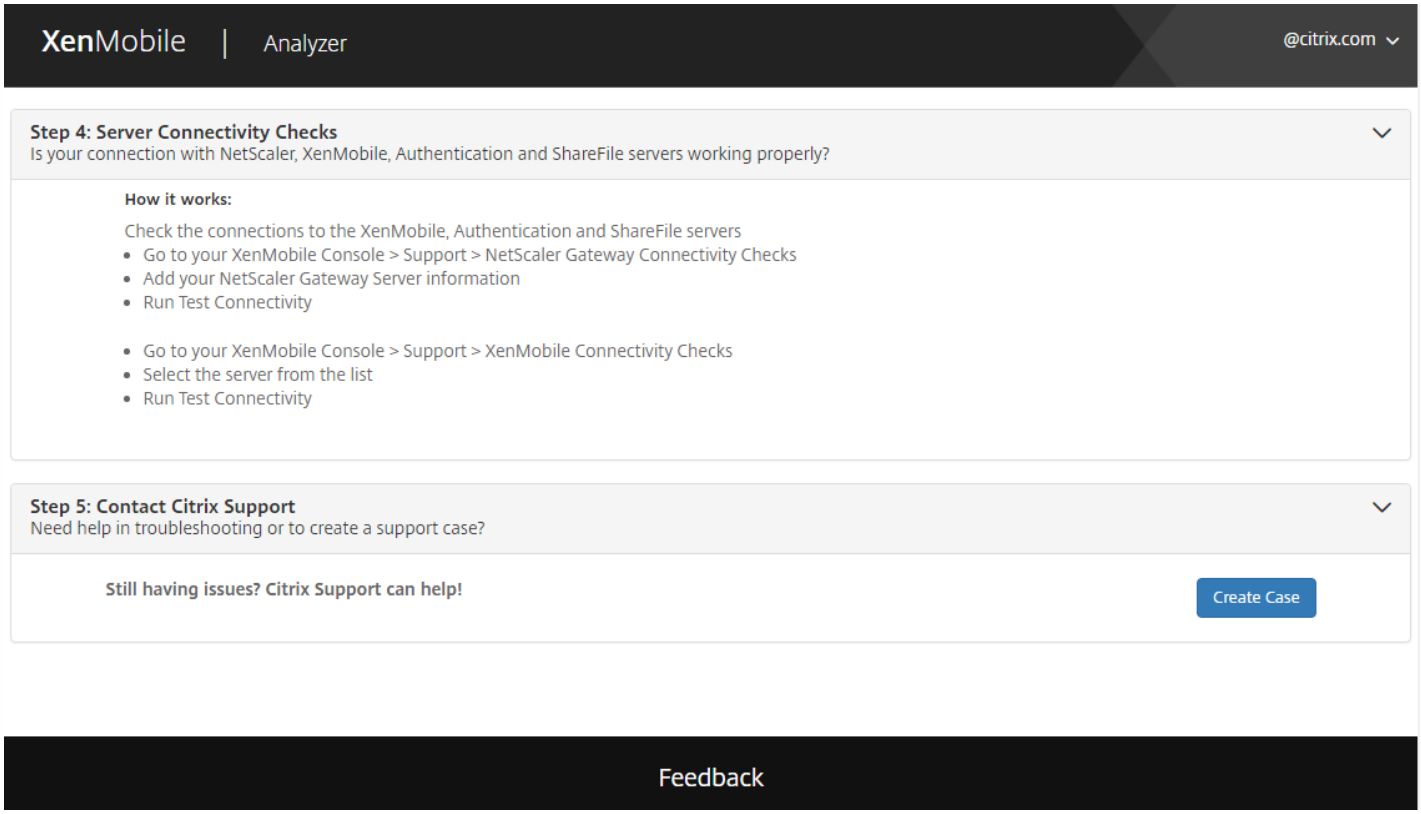


3. **WorxMail Readiness**: In diesem Schritt werden Sie zum Download der Worx Exchange ActiveSync Test-Anwendung geleitet. Die Anwendung unterstützt Sie bei den Vorbereitungen, damit sichergestellt ist, dass die ActiveSync-Server für die Bereitstellung mit einer XenMobile-Umgebung bereit sind.



4: **Server Connectivity Checks**: In diesem Schritt testen Sie die Konnektivität Ihrer Server.

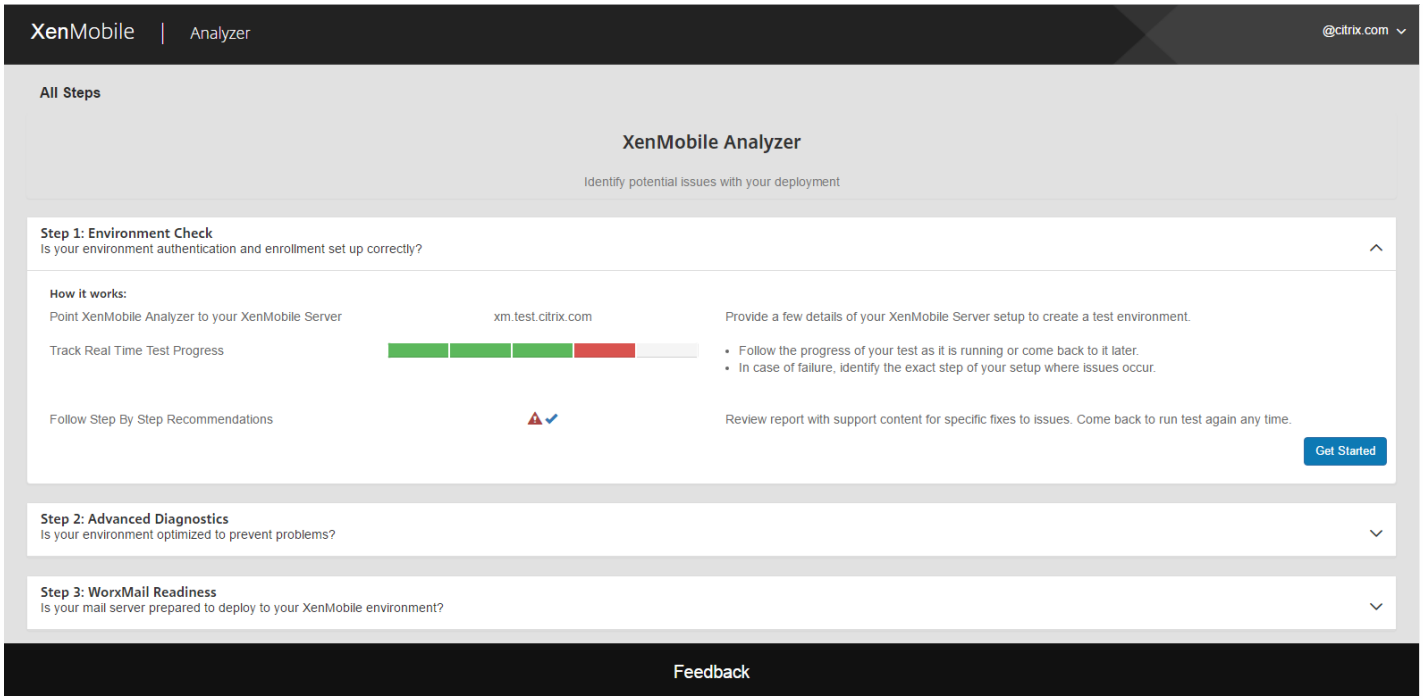
5. **Contact Citrix Support**: In diesem Schritt werden Sie zur Supportsite weitergeleitet, wo Sie einen Citrix Supportfall erstellen können, wenn Sie immer noch Probleme haben.



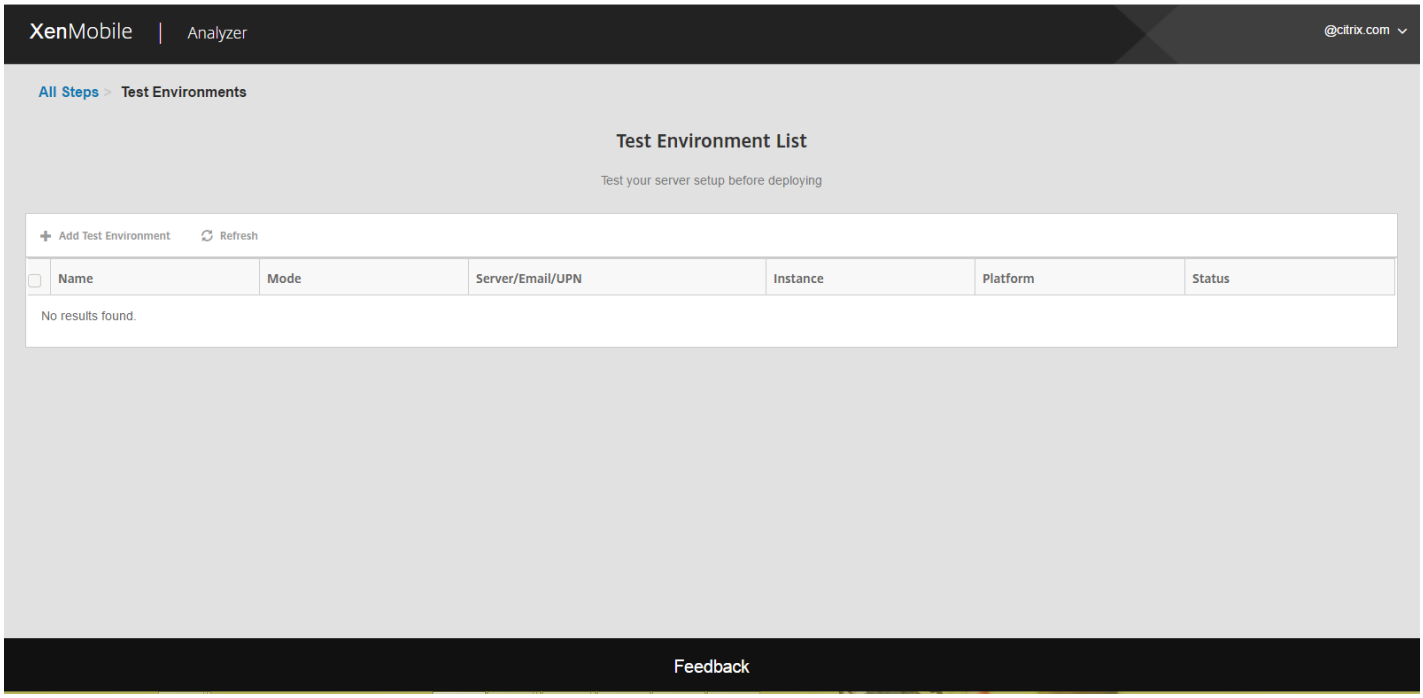
In den folgenden Abschnitten werden die Schritte detailliert erläutert.

Ausführen einer Umgebungsprüfung

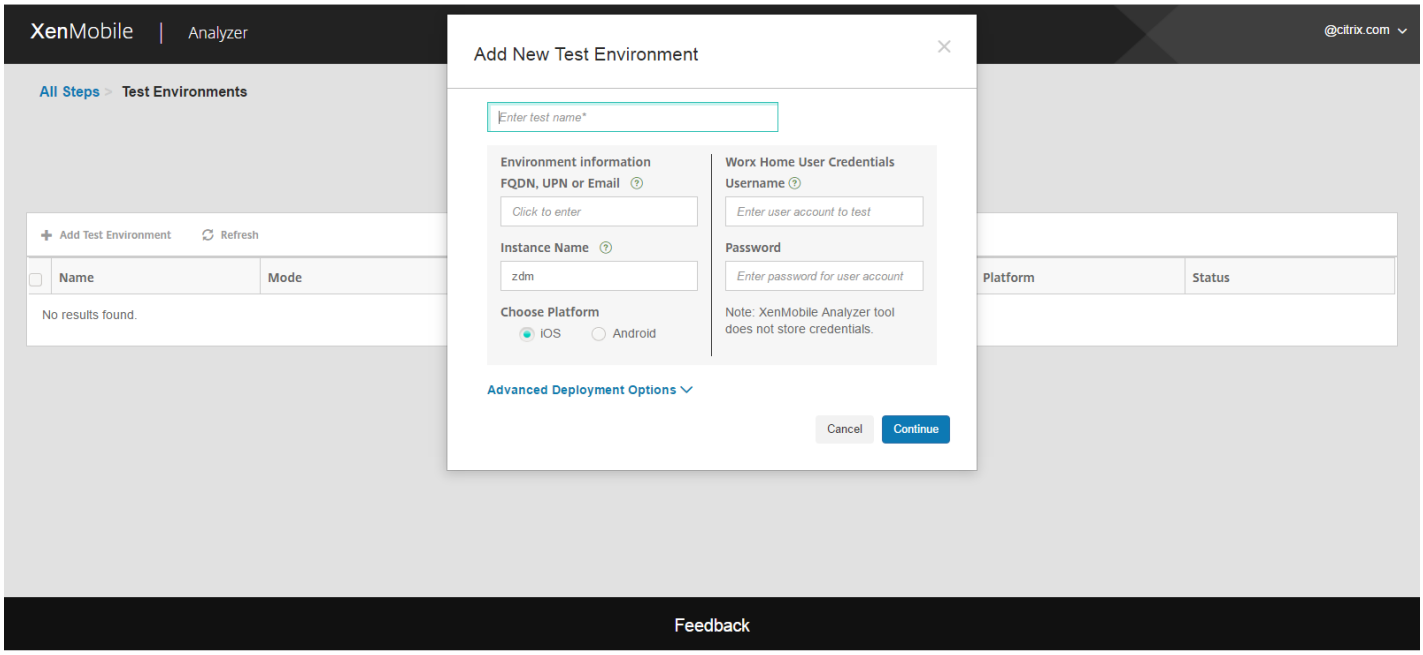
1. Melden Sie sich beim XenMobile Analyzer an und klicken Sie auf **Step 1: Environment Checks**.
2. Klicken Sie auf **Get Started**.



3. Klicken Sie auf **Add Test Environment**.



4. Führen Sie im Dialogfeld **Add Test Environment** die folgenden Schritte aus:



a. Geben Sie einen eindeutigen Namen für den Test ein, damit Sie den Test zukünftig leicht identifizieren können.

b. Wenn Sie eine Einladungs-URL für die Registrierung haben, klicken Sie auf **Advanced Deployment Options**. Wenn die Bereitstellungsoptionen angezeigt werden, aktivieren Sie das Kontrollkästchen **Do you have invitation URL** und geben Sie die URL an. Wenn Sie das Feld leer lassen, ermittelt das Tool den XenMobile-Server, Benutzernamen und andere Informationen automatisch.

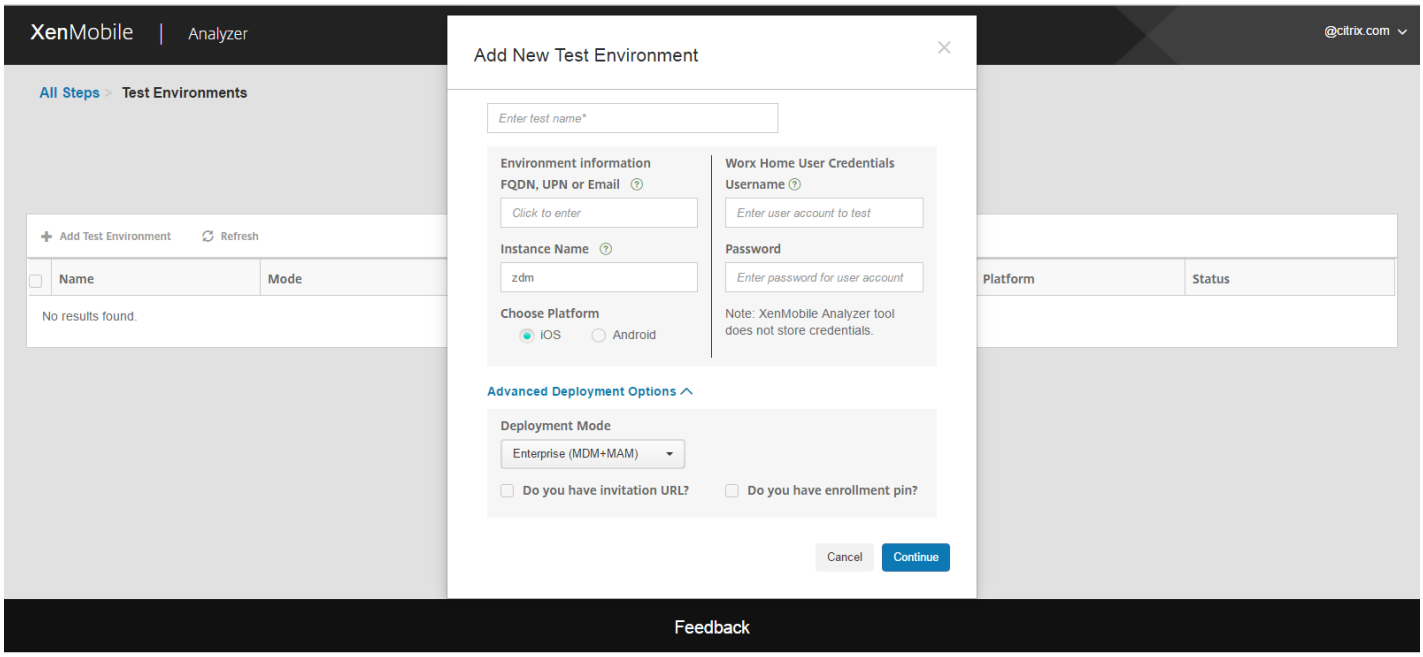
c. Wenn Sie keine Einladungs-URL haben, geben Sie die Serverinformationen manuell ein.

d. Wählen Sie in der Liste **Deployment Mode** den XenMobile-Bereitstellungsmodus aus.

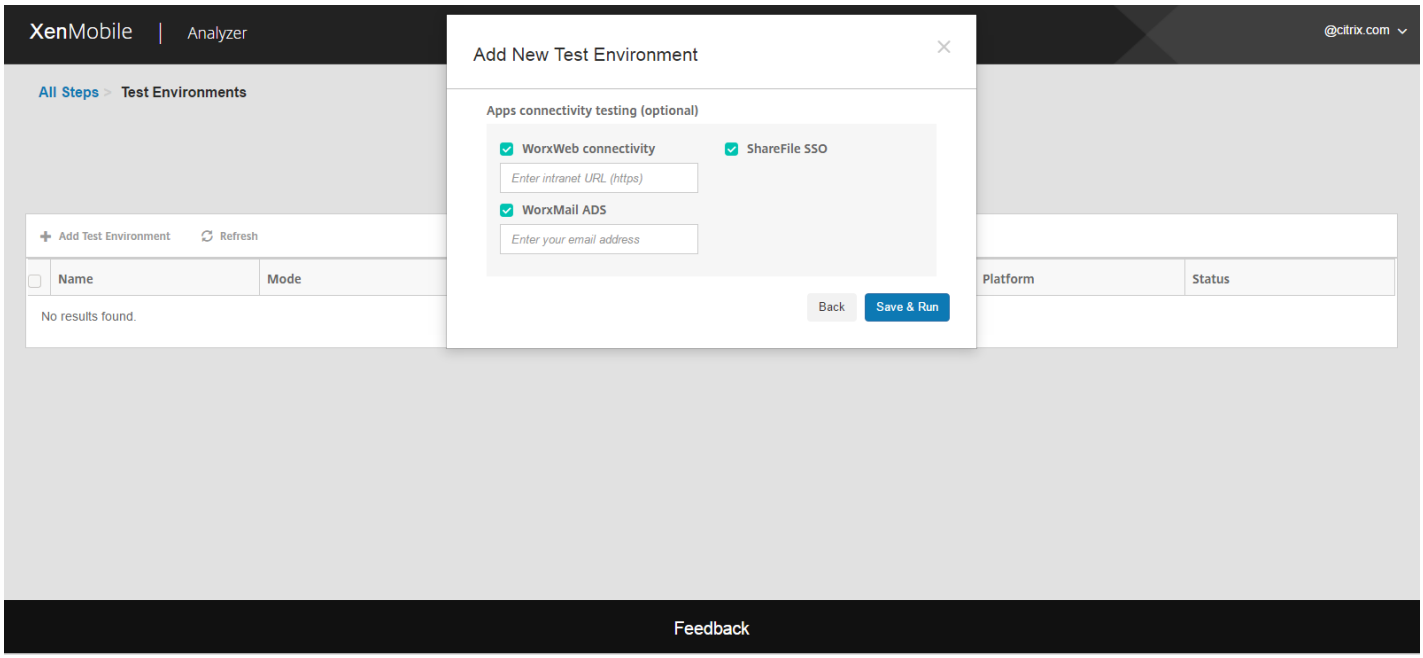
e. Wenn Sie eine benutzerdefinierte Instanz verwenden, geben Sie den Wert in **Instance Name** ein.

f. Wählen Sie unter **Choose Platform** entweder **iOS** oder **Android** als Plattform für die Tests aus.

g. Geben Sie in **Username** und **Password** den Benutzernamen und das Kennwort für die Authentifizierung ein. Wenn Ihre Umgebung für die zweistufige Authentifizierung konfiguriert ist, aktivieren Sie das Kontrollkästchen **Two Factor Authentication** und geben Sie das zweite Kennwort an.



5. Klicken Sie auf **Weiter**.



6. Sie können Tests auf Anwendungsebene ausführen. Wählen Sie mindestens einen der folgenden Tests.

   a. WorxWeb Connectivity: Geben Sie eine Intranet-URL an. Das Tool testet die Erreichbarkeit der URL. Auf diese Weise wird getestet, ob Verbindungsprobleme vorliegen, die beim Herstellen einer Verbindung mit Intranet-URLs in der WorxWeb-App auftreten können.

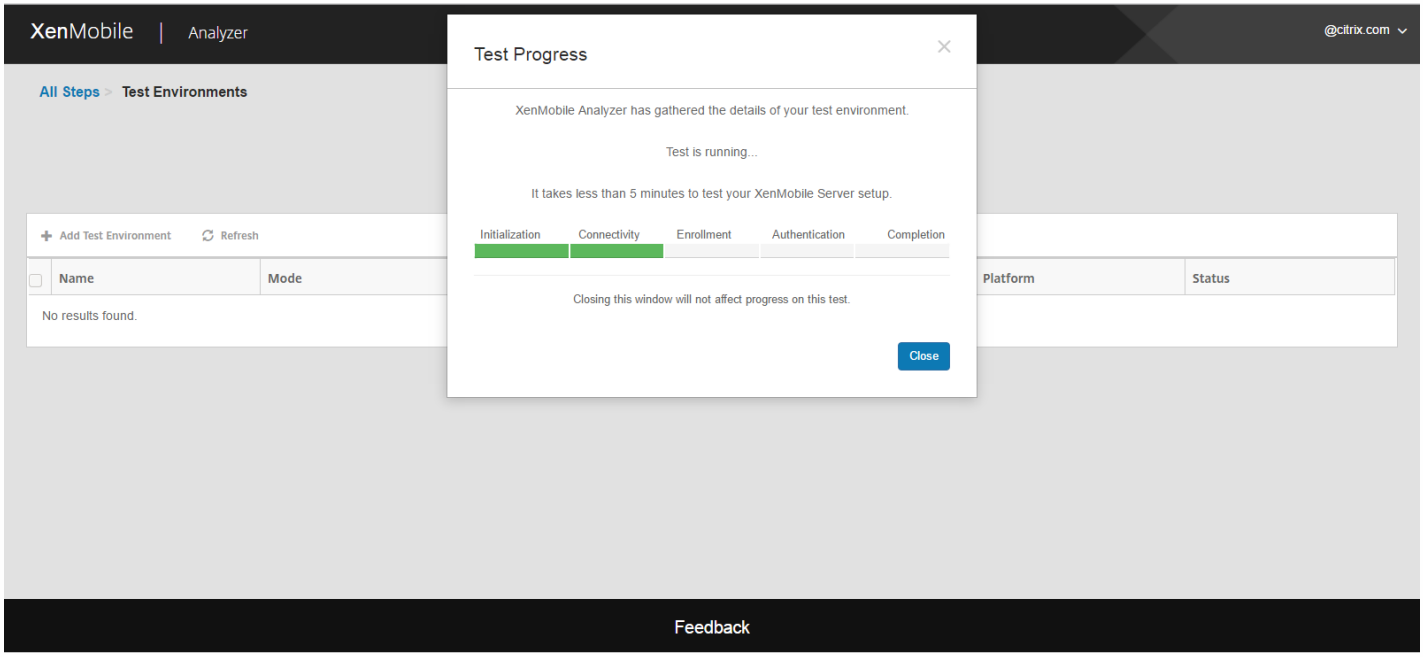
   b. WorxMail ADS: Geben Sie die E-Mail-Adresse eines Benutzers an. Hiermit wird die Autodiscovery-Funktion des Microsoft Exchange Servers in Ihrer XenMobile-Umgebung getestet. Auf diese Weise werden Probleme mit WorxMail Auto Discovery erkannt.

c. ShareFile SSO: Bei der Auswahl testet XenMobile Analyzer, ob die ShareFile DNS-Auflösung erfolgreich ausgeführt wird und ob ShareFile Single Sign-On (SSO) mit den angegebenen Benutzeranmeldeinformationen funktioniert.

7. Klicken Sie auf **Save & Run**, um die Tests zu starten.

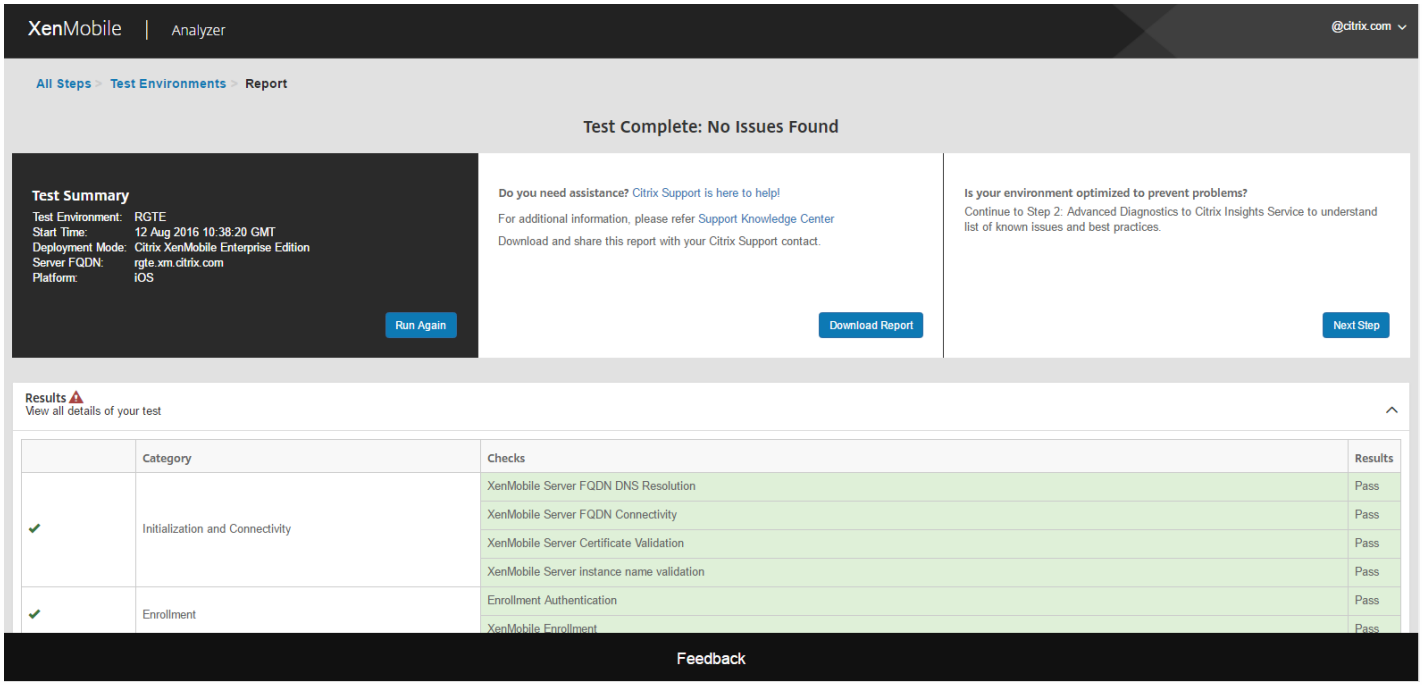
Eine Statusanzeige wird angezeigt. Sie können das Statusdialogfeld offen lassen oder schließen, die Tests werden fortgesetzt.

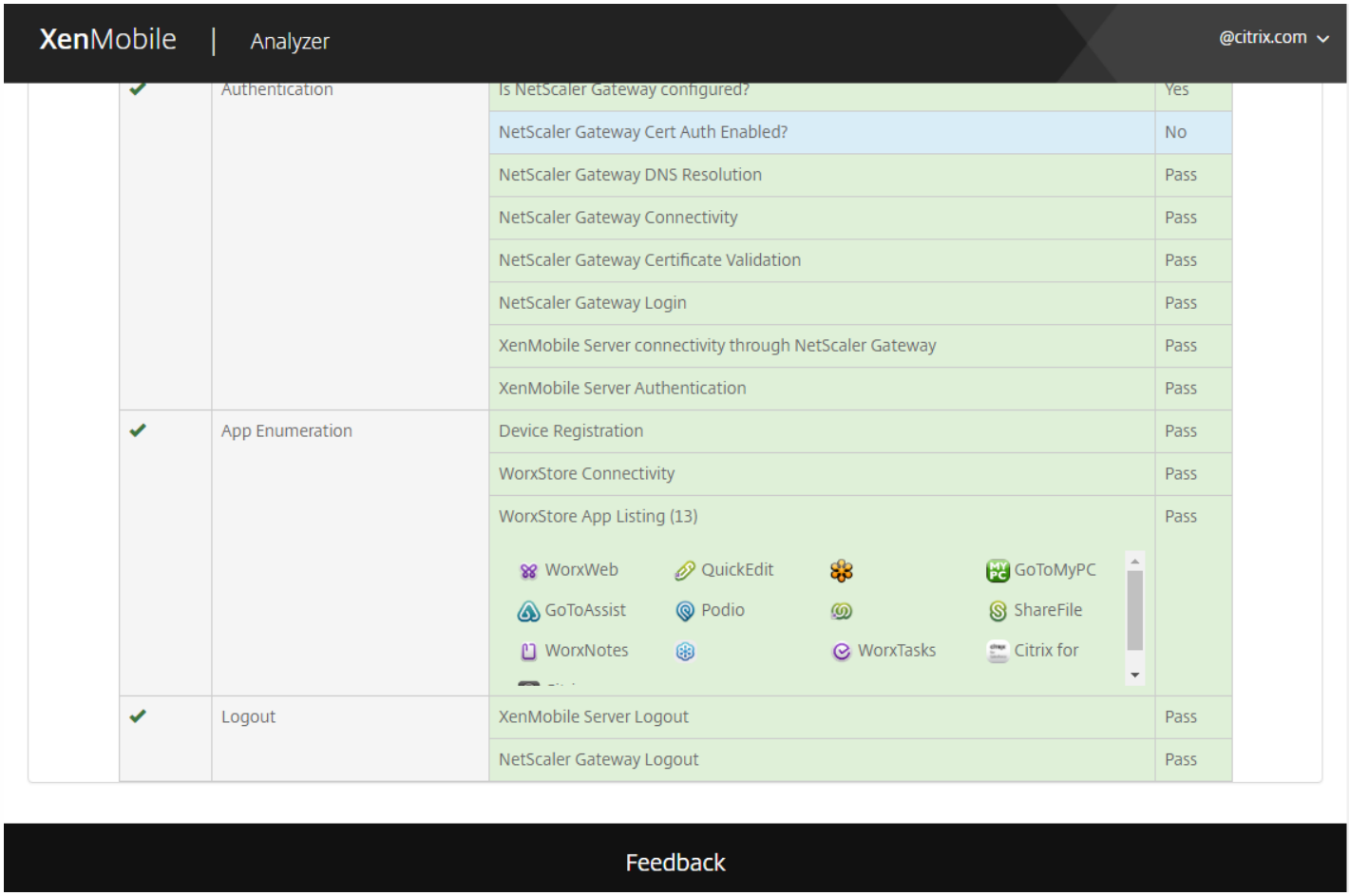
Bestandene Tests werden grün angezeigt. Nicht bestandene Tests werden rot angezeigt.



8. Wenn Sie das Statusdialogfeld schließen, können Sie jederzeit zur Seite **Test Environments List** zurückkehren und auf das Symbol **View Report** klicken, um die Ergebnisse zu sehen.

Auf der Seite **Results** werden Testdetails, Empfehlungen und Ergebnisse angezeigt.





Wenn Empfehlungen mit Citrix Knowledge Base-Artikeln verknüpft sind, werden die Artikel auf dieser Seite aufgeführt.

9. Klicken Sie auf die Registerkarte **Results**, um die einzelnen Kategorien und Tests anzuzeigen, die das Tool

ausgeführt hat, sowie die Ergebnisse.

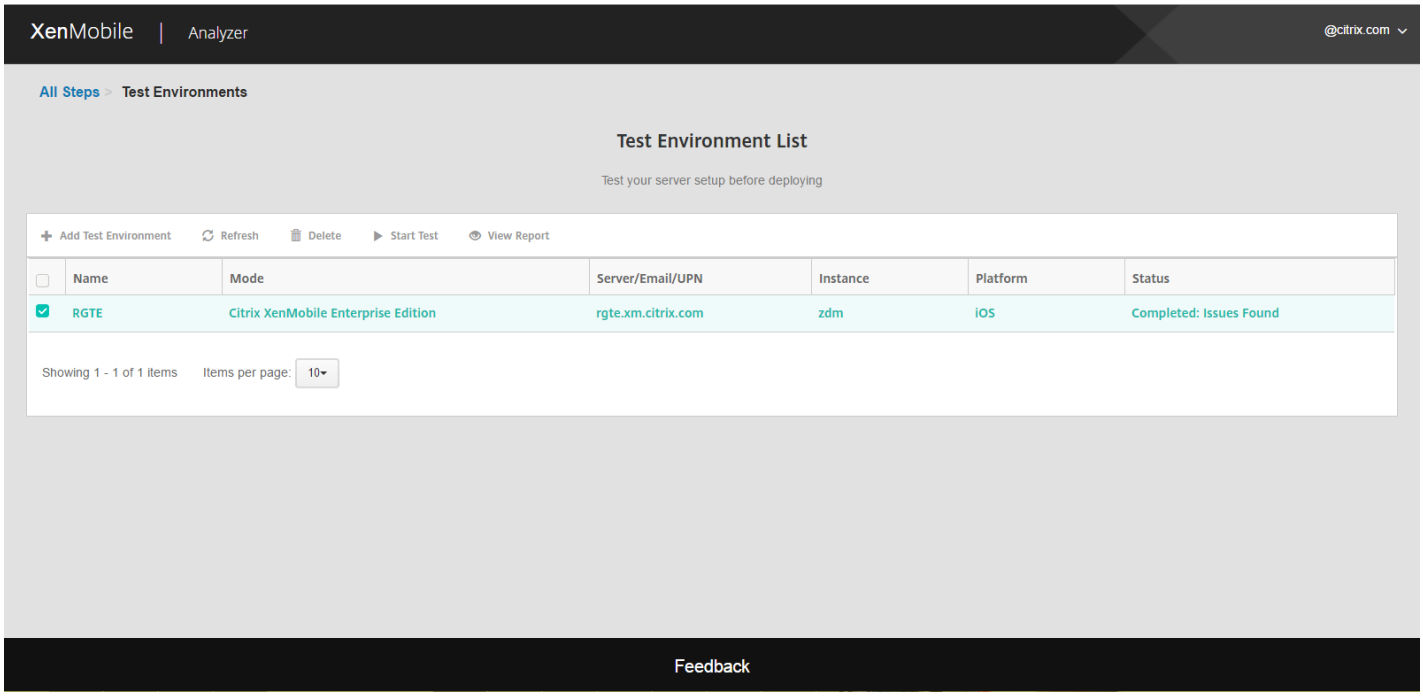
a. Durch Klicken auf **Download Report** laden Sie den Bericht herunter.

b. Wenn Sie zur Liste mit den Testumgebungen zurückkehren möchten, klicken Sie auf **Test Environments**.

c. Um den Test erneut auszuführen, klicken Sie auf **Run Again**.

d. Wenn Sie einen anderen Test ausführen möchten, gehen Sie zu **Test Environments**, wählen Sie den Test aus und klicken Sie auf **Start Test**.

e. Gehen Sie zum nächsten Schritt in XenMobile Analyzer, indem Sie auf **Next Step** klicken.



Ausführen der Schritte 2 bis 5 in XenMobile Analyzer

In dem Schritt, in dem Sie die Umgebung überprüfen, interagieren Sie mit XenMobile Analyzer direkt zum Ausführen von Tests, während die Schritte 2 bis 5 informativ sind. Alle Schritte enthalten Informationen für andere Supporttools, mit denen Sie sicherstellen können, dass die XenMobile-Umgebung richtig eingerichtet ist.

- **Step 2** - **Advanced Diagnostics**: Dieser Schritt informiert Sie über das Sammeln von Informationen über Ihre Umgebung und das Hochladen der Informationen an Citrix Insight Services. Das Tool analysiert Ihre Daten und erstellt einen personalisierten Bericht mit empfohlenen Lösungen.
- **Step 3** - **WorxMail Readiness**: Dieser Schritt führt Sie durch das Herunterladen und Ausführen der Worx Exchange ActiveSync Test-Anwendung. Die Anwendung prüft ActiveSync-Server auf ihre Eignung zur Bereitstellung mit XenMobile-Umgebungen. Nachdem die Anwendung ausgeführt wurde, können Sie die Berichte anzeigen und mit anderen teilen.
- **Step 4** - **Server Connectivity Checks**: In diesem Schritt erhalten Sie Anweisungen zum Überprüfen der Verbindungen mit XenMobile-, Authentifizierungs- und ShareFile-Servern.
- **Step 5** - **Contact Citrix Support**: Wenn gar nichts hilft, können Sie ein Supportticket mit Citrix Support erstellen.

Bekannte Probleme

In XenMobile Analyzer sind die nachfolgend aufgeführten Probleme bekannt:

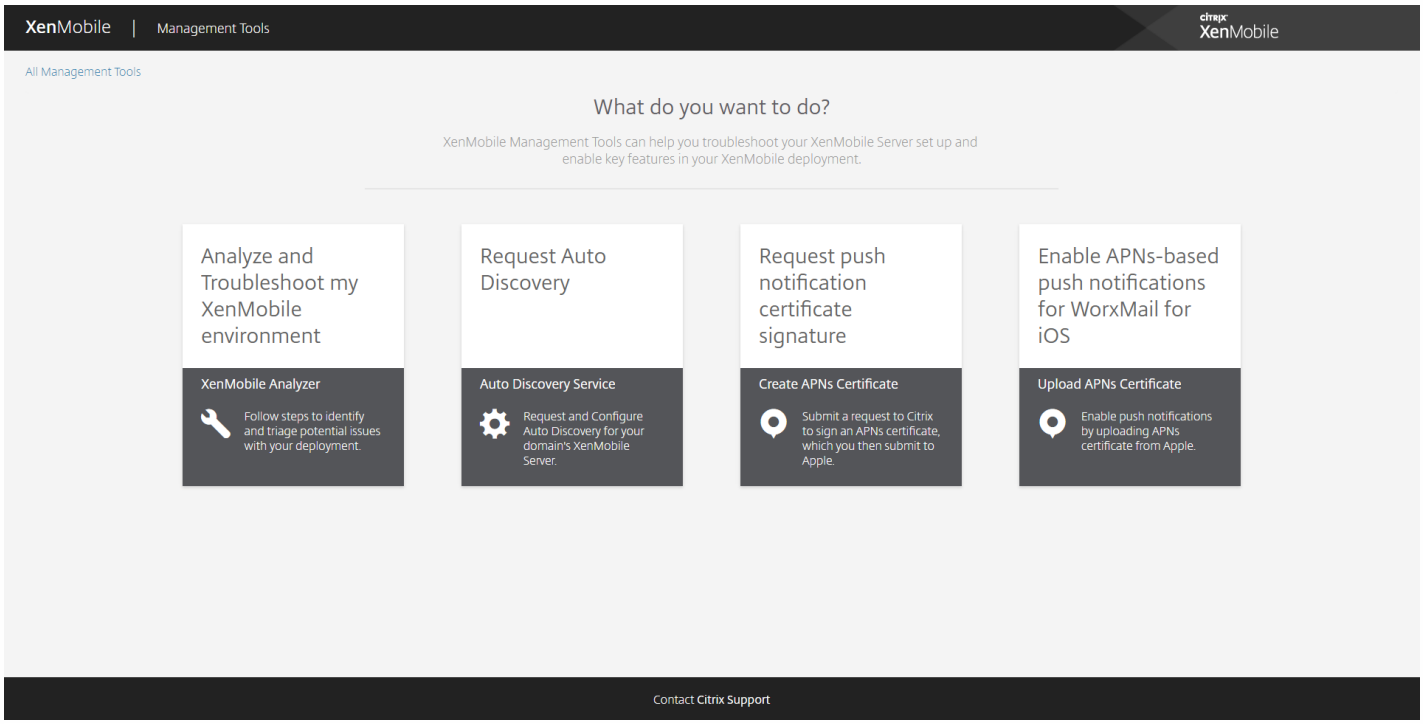
- Die Anzahl der aufgeführten Apps kann nach Client variieren, wenn auf dem XenMobile-Server die Richtlinie zur Plattformeinschränkung festgelegt ist.
- Beim Ausführen von WorxWeb Intranet-Konnektivitätstests wird die Eingabe mehrerer URLs in das Textfeld nicht unterstützt.
- Das Worx Home-Authentifizierungsfeature für gemeinsam genutzte Geräte wird nicht unterstützt.

XenMobile Autodiscovery-Dienst

Jul 28, 2016

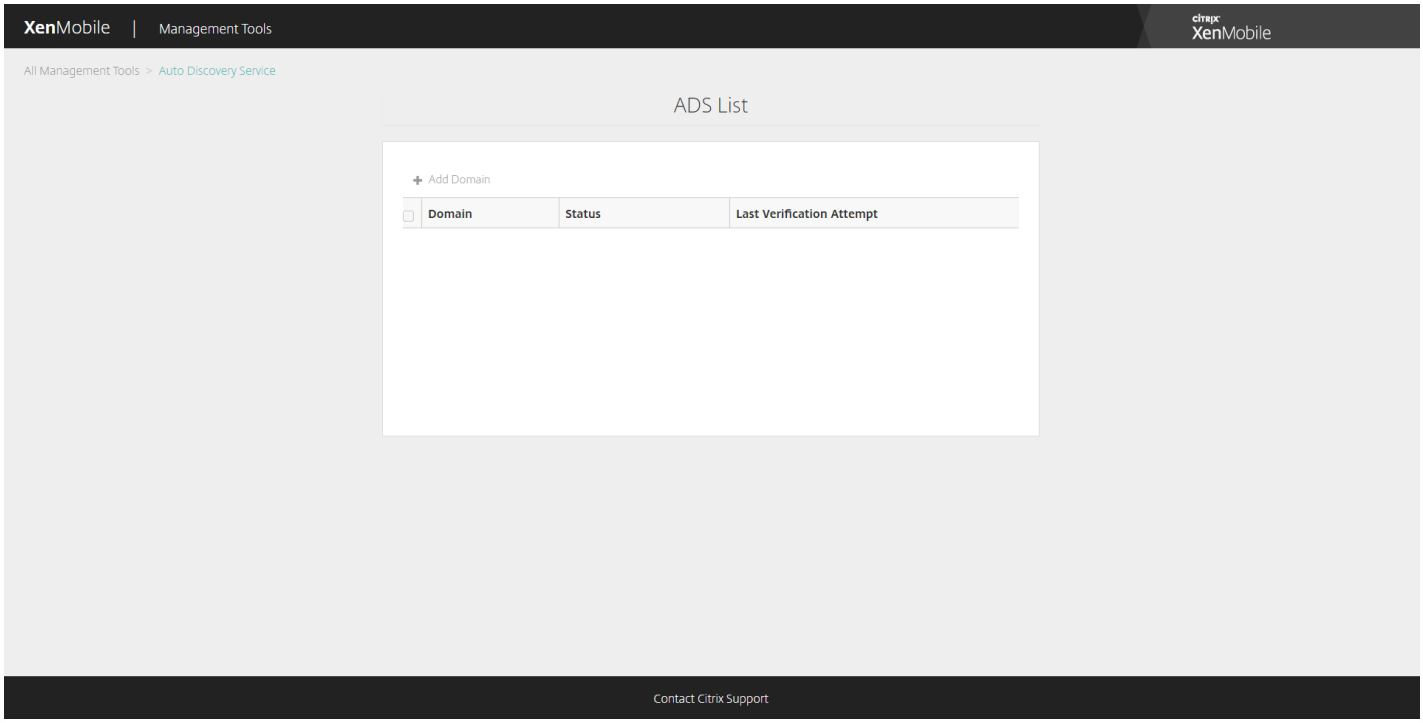
Autodiscovery ist ein wichtiger Teil vieler XenMobile-Bereitstellungen. Autodiscovery vereinfacht den Registrierungsvorgang für Benutzer. Diese können bei der Geräteregistrierung dann ihren Netzwerkbenutzernamen und ihr Active Directory-Kennwort verwenden, statt Angaben zum XenMobile-Server eingeben zu müssen. Der Benutzername wird im Benutzerprinzipalnamensformat (UPN) eingegeben, z. B. user@mycompany.com. Mit dem XenMobile Autodiscovery-Dienst können Sie einen Autodiscovery-Datensatz ohne Unterstützung durch Citrix Support erstellen und bearbeiten.

Zum Zugreifen auf den XenMobile Autodiscovery-Dienst navigieren Sie zu https://xenmobiletools.citrix.com und klicken auf **Request Auto Discovery**.

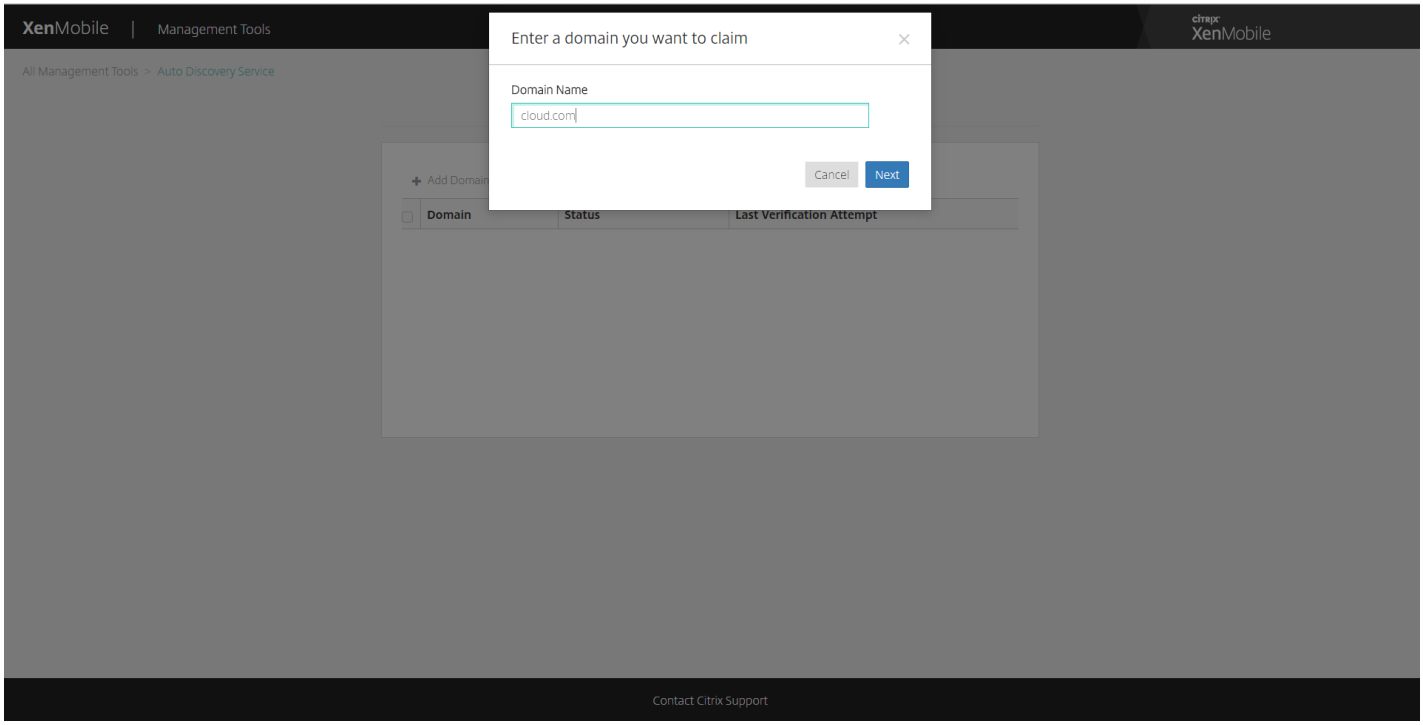


Anfordern von Autodiscovery

1. Auf der Seite des Autodiscovery-Diensts müssen Sie zunächst eine Domäne beanspruchen. Klicken Sie auf **Add Domain**.



2. Geben Sie in dem Dialogfeld, das geöffnet wird, den Domänennamen Ihrer XenMobile-Umgebung ein und klicken Sie dann auf **Next**.



3. Im nächsten Schritt wird überprüft, ob Sie tatsächlich der Eigentümer der Domäne sind.

a. Kopieren Sie das über das XenMobile Tools-Portal zur Verfügung gestellte DNS-Token.

b. Erstellen Sie einen DNS-TXT-Datensatz in der Zonendatei für Ihre Domäne über das Portal des Domänenhosting-

Anbieters.

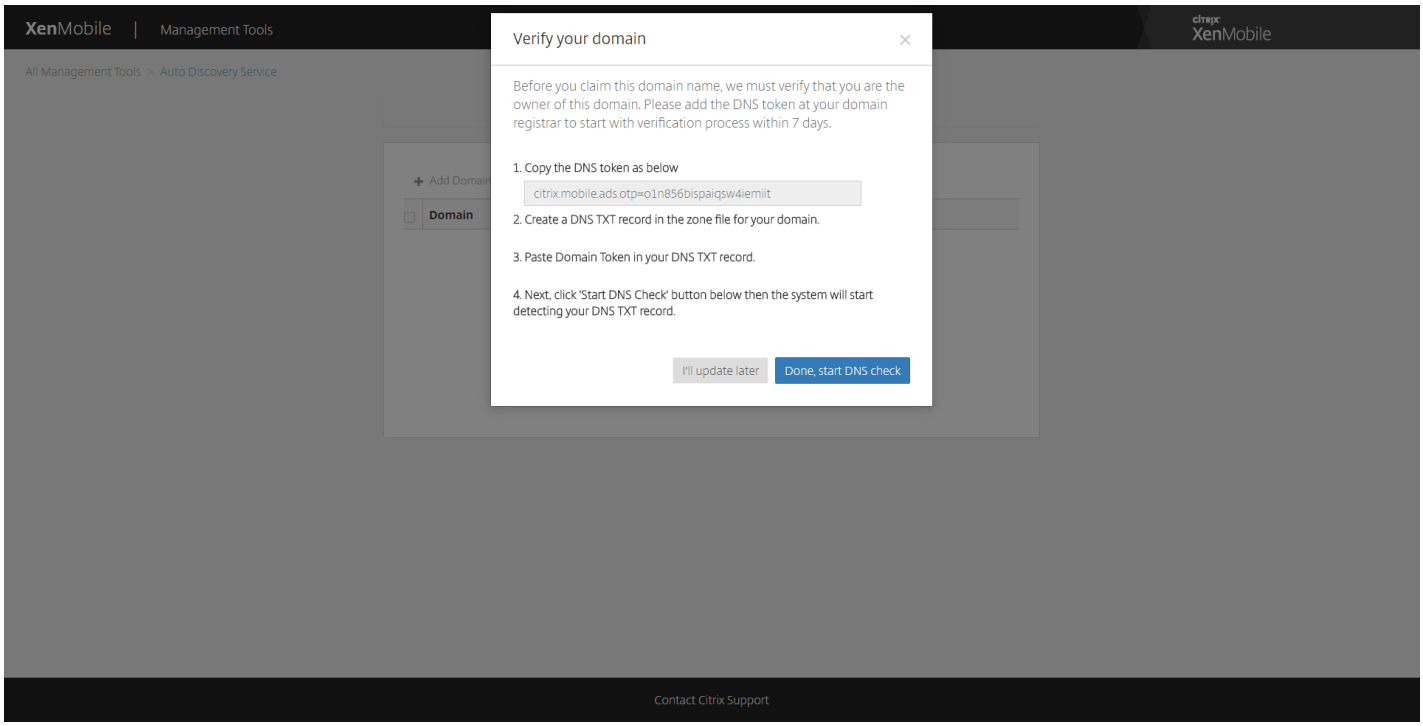
Zum Erstellen eines DNS-TXT-Datensatzes müssen Sie sich bei dem Portal des Hosting-Anbieters der Domäne anmelden, die Sie in Schritt 2 oben hinzugefügt haben. Über das Domänenhostingportal können Sie die Domänennamenserver-Datensätze bearbeiten und einen benutzerdefinierten TXT-Datensatz hinzufügen. Weiter unten finden Sie ein Beispiel für einen DNS-TXT-Eintrag auf dem Hostingportal einer Beispieldomäne "domain.com".

c. Fügen Sie das Domänentoken in Ihren DNS-TXT-Datensatz ein und speichern Sie den Domänennamenserver-Datensatz.

d. Klicken Sie im XenMobile Tools-Portal auf "Done, start DNS check".

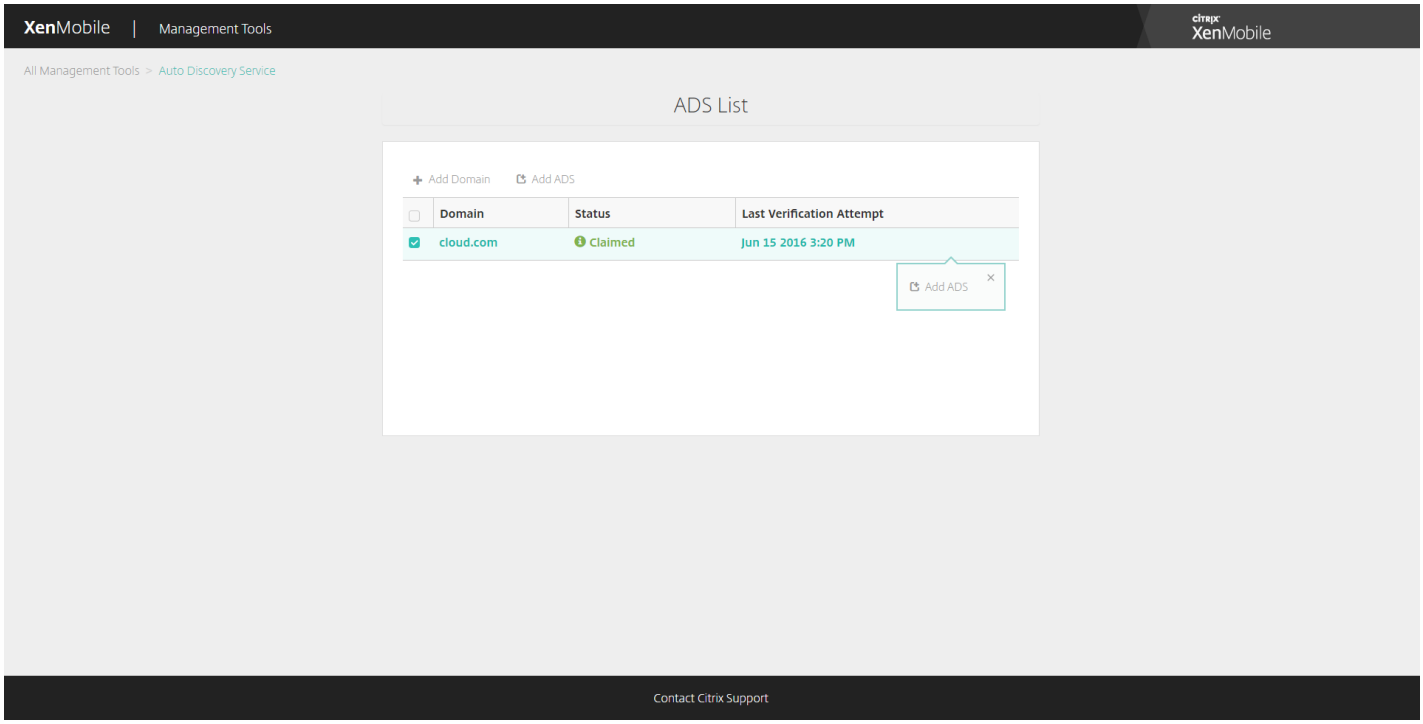
Das System erkennt den DNS-TXT-Datensatz. Alternativ können Sie auf "I'll update later" klicken. Der Datensatz wird dann gespeichert. Die DNS-Prüfung wird erst gestartet, wenn Sie auf den Datensatz mit dem Status "Waiting" und dann auf "DNS Check" klicken.

Diese Prüfung dauert im Idealfall ungefähr eine Stunde, aber es kann auch bis zu zwei Tage dauern, bis eine Antwort zurückgegeben wird. Darüber hinaus müssen Sie möglicherweise das Portal verlassen und wieder zurückkehren, um die Statusänderung zu sehen.

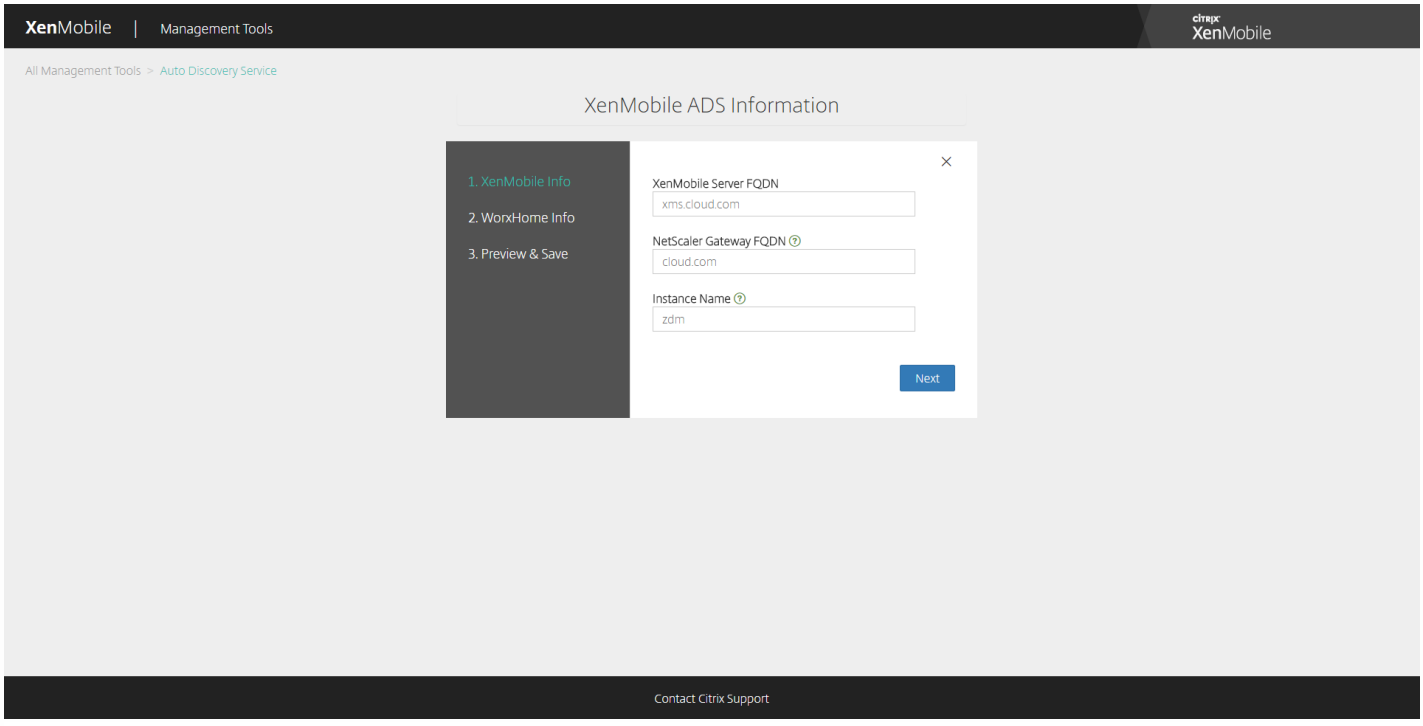


4. Nachdem Sie Ihre Domäne beansprucht haben, geben Sie Autodiscovery-Dienstinformationen ein. Klicken Sie mit der rechten Maustaste auf den Domänendatensatz, für den Sie Autodiscovery anfordern, und klicken Sie auf **Add ADS**.

Wenn Ihre Domäne bereits einen Autodiscovery-Datensatz hat, öffnen Sie einen Fall beim Citrix Support, um diesen nach Bedarf zu ändern.



5. Nehmen Sie Eingaben in **XenMobile Server FQDN**, **NetScaler Gateway FQDN** und **Instance Name** vor und klicken Sie auf **Next**. Wenn Sie nicht sicher sind, fügen Sie eine Standardinstanz "zdm" hinzu.



6. Geben Sie die folgenden Informationen für Worx Home ein und klicken Sie dann auf **Next**.

a. **User ID Type**: Wählen Sie für den ID-Typ, mit dem Benutzer sich anmelden, **E-mail address** oder **UPN** aus.

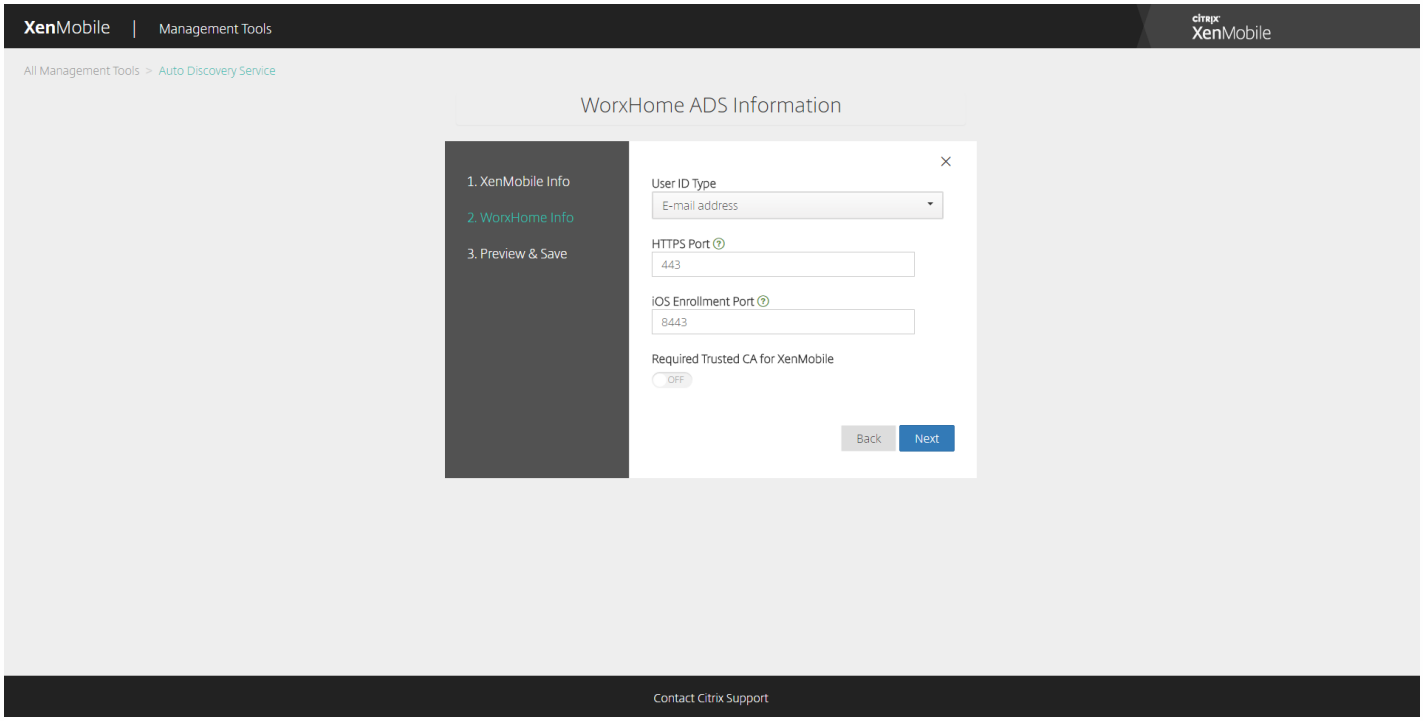
UPN wird verwendet, wenn der UPN (userPrincipalName) des Benutzers mit seiner E-Mail-Adresse übereinstimmt.

Bei beiden Methoden erfolgt die Suche der Serveradresse anhand der eingegebenen Domäne. Bei der Methode **E-Mail-Adresse** werden die Benutzer aufgefordert, den Benutzernamen und das Kennwort einzugeben, bei der Methode **UPN** müssen sie ihr Kennwort eingeben.

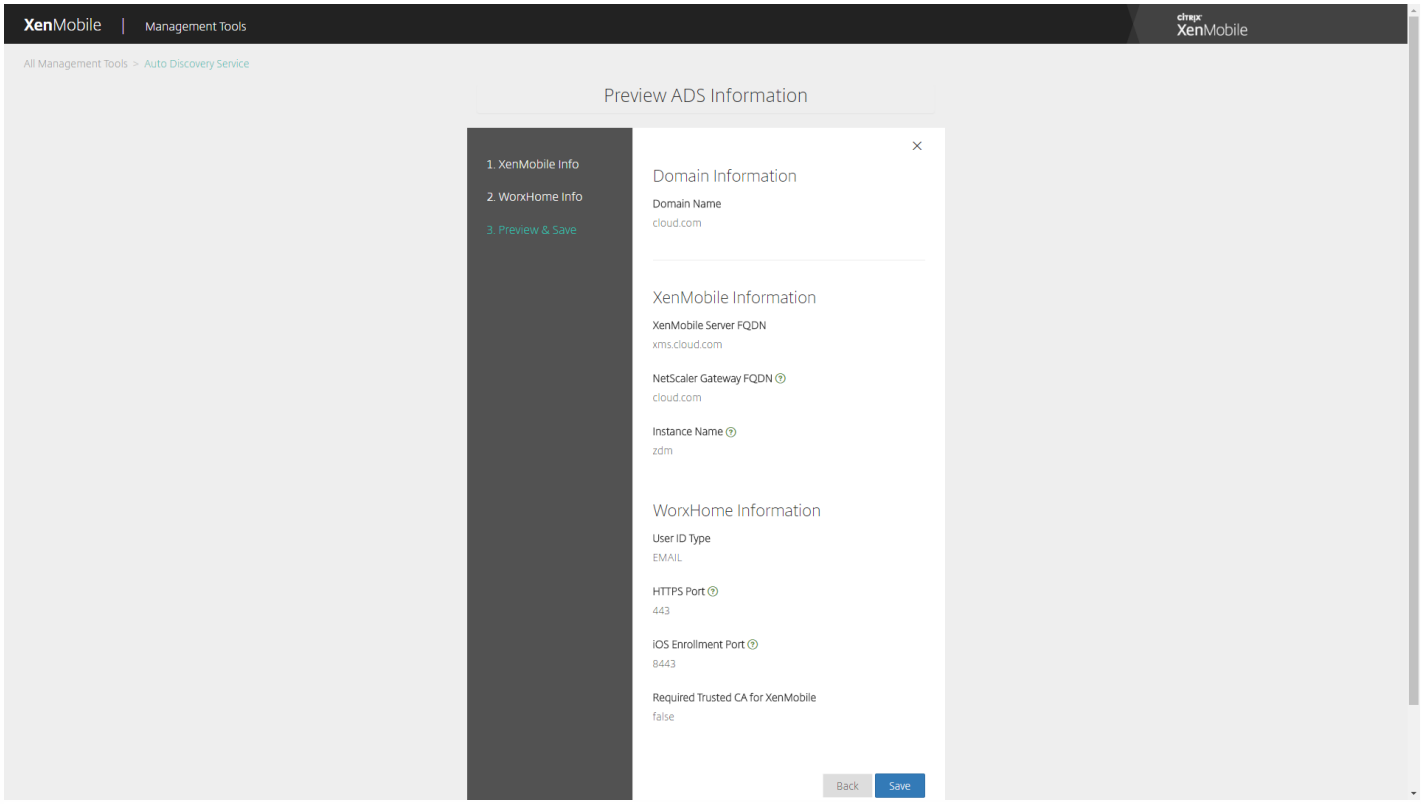
b. **HTTPS Port**: Geben Sie den Port an, über den auf Worx Home über HTTPS zugegriffen wird. Normalerweise ist dies Port 443.

c. **iOS Enrollment Port**: Geben Sie den Port an, über den auf Worx Home für die iOS-Registrierung zugegriffen wird. Normalerweise ist dies Port 8443.

d. **Required Trusted CA for XenMobile**: Geben Sie an, ob für den Zugriff auf XenMobile ein vertrauenswürdiges Zertifikat erforderlich ist. Diese Option kann auf **ON** oder **OFF** festgelegt werden. Derzeit kann kein Zertifikat für dieses Feature hochgeladen werden. Wenn Sie dieses Feature verwenden möchten, wenden Sie sich an den Citrix Support und lassen Sie Autodiscovery vom Support einrichten. Weitere Informationen über das Zertifikatpinning finden Sie in dem Abschnitt zum Zertifikatpinning des Artikels Worx Home. Informationen zu den für das Zertifikatpinning erforderlichen Ports finden Sie im Support-Artikel XenMobile Port Requirements for ADS Connectivity.



7. Auf einer Zusammenfassungsseite werden alle in den oben beschriebenen Schritten eingegebenen Informationen angezeigt. Stellen Sie sicher, dass die Daten richtig sind, und klicken Sie dann auf **Save**.



Referenz zur XenMobile REST-API

Jul 28, 2016

Mit der XenMobile-REST-API können Sie Dienste aufrufen, die über die XenMobile-Konsole verfügbar gemacht werden. Sie können REST-Dienste über einen beliebigen REST-Client aufrufen. Die API erfordert zum Aufrufen der Dienste keine Anmeldung bei der XenMobile-Konsole.

Eine umfassende aktuelle Liste der verfügbaren APIs finden Sie in der PDF-Datei Referenz zur XenMobile REST-API. Dieser Artikel enthält nicht den vollständigen API-Satz.

Berechtigungen für den Zugriff auf die REST-API

Sie benötigen eine der folgenden Berechtigungen für den Zugriff auf die REST-API:

- Zugriffsberechtigung auf die öffentliche API, die als Teil der Konfiguration des rollenbasierten Zugriffs festgelegt wurde (weitere Informationen zum Einrichten des rollenbasierten Zugriffs finden Sie unter Konfigurieren von Rollen mit RBAC)
- Superuser-Benutzerberechtigung

Aufrufen von REST-API-Diensten

Sie können REST-API-Dienste über den REST-Client oder CURL-Befehle aufrufen. Die folgenden Beispiele verwenden den Advanced REST-Client für Chrome.

> **Hinweis**
>
> Ändern Sie für die folgenden Beispiele den Hostnamen und die Portnummer gemäß Ihrer Umgebung.

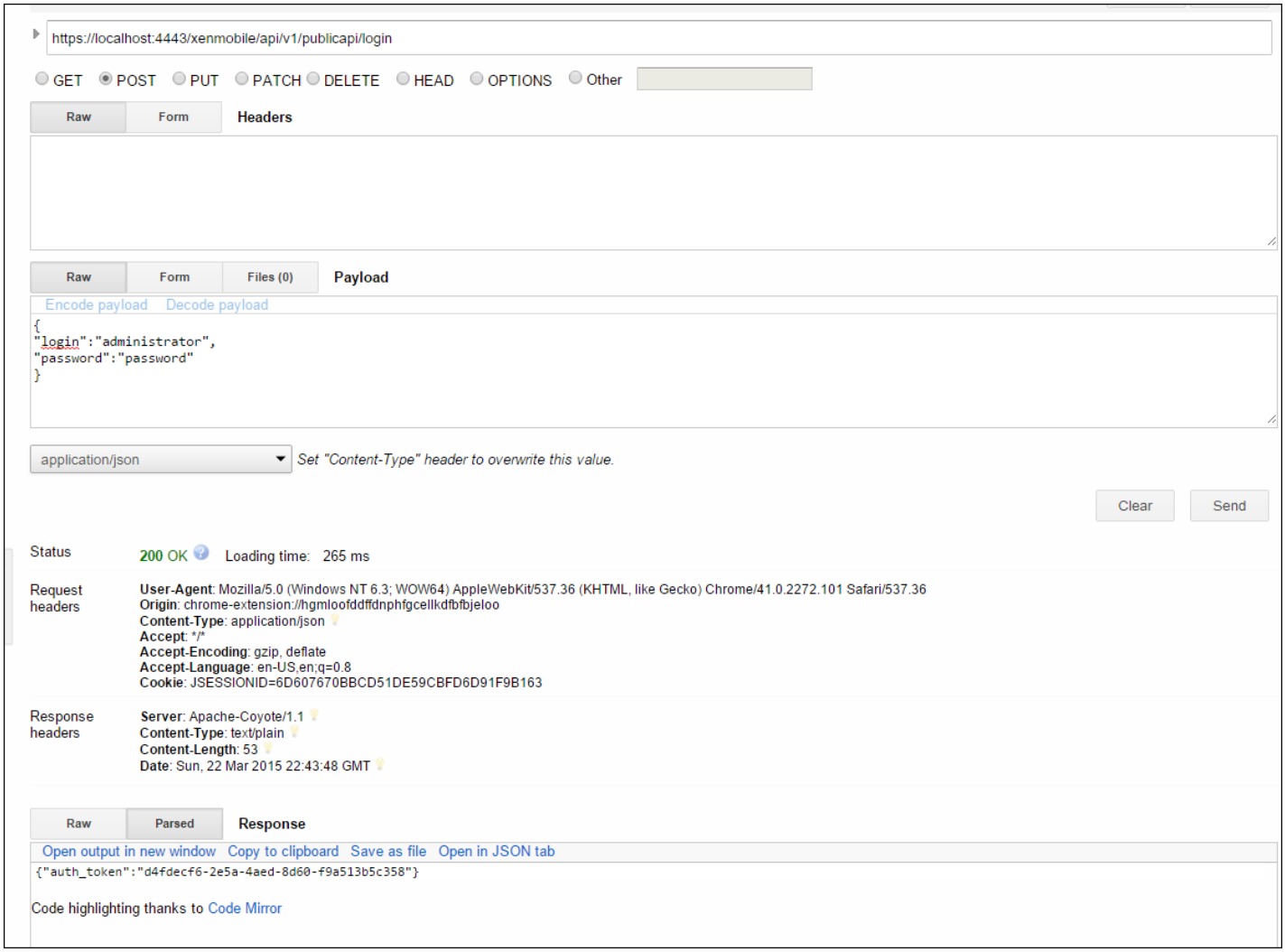
Login

URL: https://:/xenmobile/api/v1/authentication/login

Anforderung: { "login":"administrator", "password":"password" }

Methodentyp: POST

Inhaltstyp: application/json



Abruf von Bereitstellungsgruppen per Filter

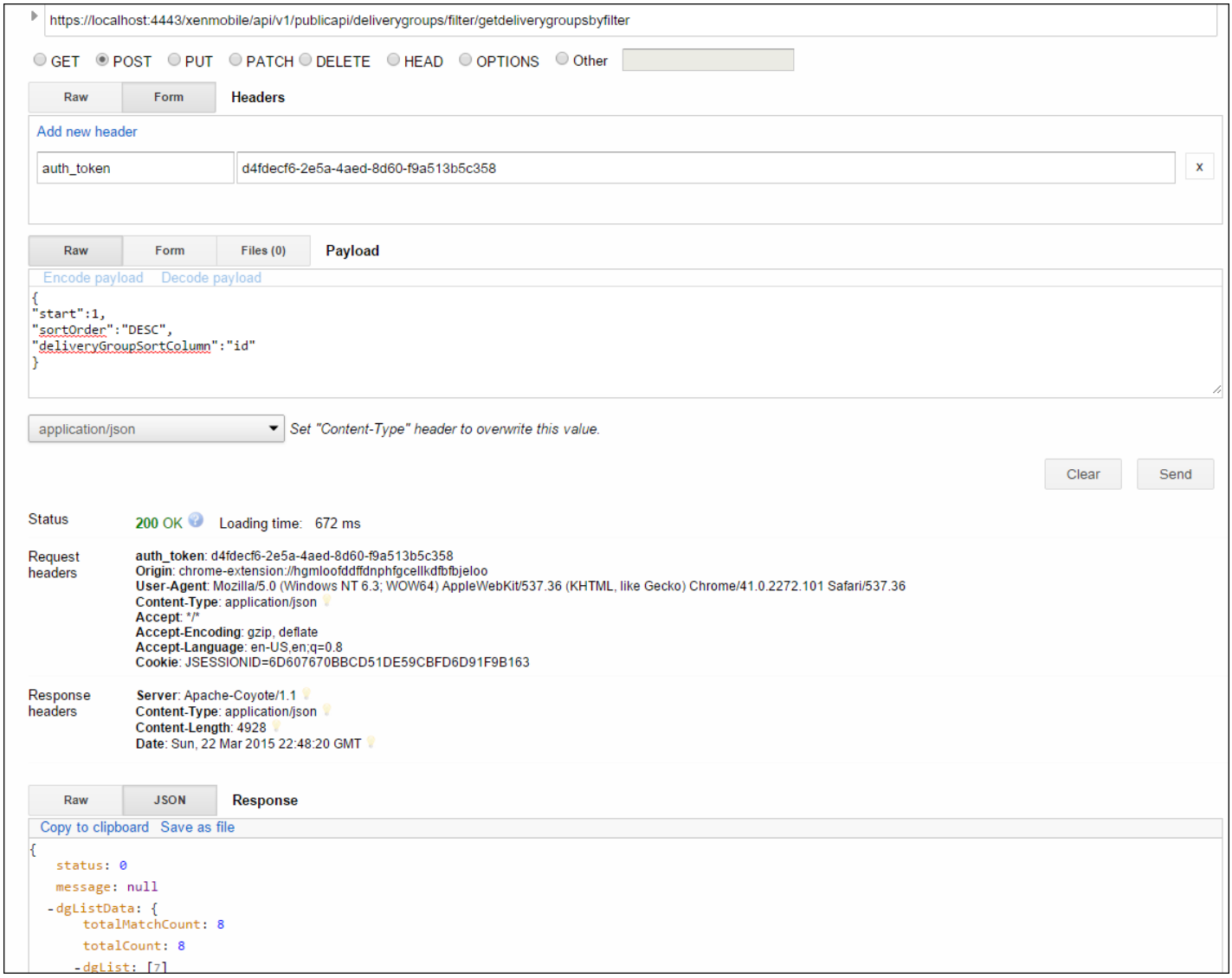
URL: /xenmobile/api/v1/deliverygroups/filter

Anforderung: KOPIEREN

```
{

        "start": 1,

        "sortOrder": "DESC",

        "deliveryGroupSortColumn":"id",

        "search":"add"

}
```

Methodentyp: POST

Inhaltstyp: application/json



REST-API-Definitionen

In den folgenden Abschnitten werden einige der in der PDF aufgeführten APIs erläutert. Die vollständige Dokumentation zu APIs finden Sie in der PDF-Datei.

Nicht vergessen: Ändern Sie für die folgenden Beispiele den Hostnamen und die Portnummer gemäß Ihrer Umgebung.

Anmelden bei der öffentlichen API

Akzeptiert die Benutzeranmeldeinformationen und verwendet den vorhandenen Authentifizierungsmanager für die Authentifizierung des Benutzers. Bei der ersten Authentifizierung eines Benutzers durch den Authentifizierungsmanager wird ein Authentifizierungstoken generiert, das im Anforderungsheader eingefügt wird.

URL: https://:4443/xenmobile/api/v1/authentication/login

Anforderungstyp: POST

Anforderungsparameter KOPIEREN

```
{ "login":"administrator", "password":"password" }
```

Beispielantwort KOPIEREN

```
{

    "auth-token":"q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"

}
```

Anmelden bei der öffentlichen API über Workspace Cloud

Akzeptiert die Benutzeranmeldeinformationen und verwendet den vorhandenen Authentifizierungsmanager für die Authentifizierung des Benutzers. Bei der ersten Authentifizierung eines Benutzers durch den Authentifizierungsmanager wird ein Authentifizierungstoken generiert, das im Anforderungsheader eingefügt wird.

URL: https://:/xenmobile/api/v1/authentication/cwclogin

Anforderungstyp: POST

Anforderungsheader: Authorization – CWSAuth service=

Anforderungsparameter KOPIEREN

```
{“context”:”customer or cloud”, “customerId”:”customer ID”}
```

Beispielantwort KOPIEREN

```
{

    "auth-token":"authentication token"

}
```

Abmelden von der öffentlichen API

Entfernt das bei der Anmeldung generierte Authentifizierungstoken und meldet den aktuellen Benutzer ab. Erfordert den Benutzernamen und das Authentifizierungstoken.

URL: https://:/xenmobile/api/v1/authentication/logout

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Anforderungsparameter KOPIEREN

```
{“login”:”administrator”}
```

Beispielantwort KOPIEREN

```
{"Status":"user administrator logged out successfully."}
```

Verwalten von Zertifikaten

Vorgänge der Zertifikatverwaltung ermöglichen das Anzeigen, Löschen, Importieren und Hinzufügen von Zertifikaten über die öffentliche API.

Get all certificates

Gibt alle Zertifikate in der Datenbank zurück.

URL: https://:/xenmobile/api/v1/certificates

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Anforderungsparameter: keine

Beispielantwort KOPIEREN


```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": null,
    "certificate": [
        {
            "name": "ent-root-ca",
            "description": "test description server 1",
            "validFrom": "2012-02-22",
            "validTo": "2017-02-21",
            "type": "chain",
            "isActive": false,
            "privateKey": "false",
            "ca": null,
            "id": 4656,
            "certDetails": {
```



```
"signatureAlgo": "SHA1WithRSAEncryption",

"version": null,

"serialNum": "348237881800118418457268346483687164l3",

"issuerName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,

    "locality": null,

    "state": null,

    "country": null,

    "description": null

},

"subjectName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,
```



```
                        "locality": null,
                        "state": null,
                        "country": null,
                        "description": null
                    }
                }
            }
        ],
        "apnsCheckObj": {
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
        }
}
```


Delete certificates

Löscht die angegebenen Zertifikate. Erfordert die Zertifikat-ID für jedes Zertifikat, das gelöscht werden soll.

URL: https://:/xenmobile/api/v1/publicapi/certificates

Anforderungstyp: DELETE

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Anforderungsparameter KOPIEREN

```
{“certificateIds”:[“<certificate_id_1>”,”<certificate_id_2>”, ..., "<certificate_id_n>"]}
```

Import certificate as SAML certificate

Importiert das angegebene Zertifikat als SAML-Zertifikat.

URL: https://:/xenmobile/api/v1/certificates/import/certificate/saml

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: Multipart/form-data

Anforderungsparameter KOPIEREN

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'saml',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

Beispielantwort KOPIEREN

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {
```

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```

Import certificate as server certificate

Importiert das angegebene Zertifikat als Serverzertifikat.

URL: https://:/xenmobile/api/v1/certificates/import/certificate/server

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: Multipart/form-data

Anforderungsparameter KOPIEREN

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'none',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

Beispielantwort KOPIEREN

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {
```

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```

Import certificate as listener certificate

Importiert das angegebene Zertifikat als SSL-Listener-Zertifikat.

URL: https://:/xenmobile/api/v1/certificates/import/certificate/listener

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: Multipart/form-data

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'listener',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
```

```
        "apnsCheck": {

                "topicNameMismatch": false,

                "certExpired": false,

                "certNotYetValid": false,

                "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

                "topicNameMismatch": false,

                "certExpired": false,

                "certNotYetValid": false,

                "malformed": false

        }

}
```

Create certificate

Erstellt ein selbstsigniertes Zertifikat oder eine Zertifikatsignieranforderung (CSR), das bzw. die eine Zertifizierungsstellensignatur erfordert.

URL: https://:/xenmobile/api/v1/certificates/csr

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: Application/form_url_encoded

Anforderungsparameter KOPIEREN

```
{
    "isSelfSign":true,
    "csrRequest":{
    "commonName":"your certificate name",
    "description":"certificate description",
    "org":"organization",
    "orgUnit":"organization unit",
    "locality":"location",
    "state":"CA",
    "country":"US",
    "isSelfSign":true
    },
"validDays":"60",
"keyLength":"1024",
"useAs":"none"
}
```

Beispielantwort KOPIEREN

```
{
    status: 0
    message: "Success"
    csrRequest: ""
    apnsCheck: null
    certificate: null
    apnsCheckObj:
    {
    topicNameMismatch: false
    certExpired: false
    certNotYetValid: false
    malformed: false
    }
}
```

Export certificate

Lädt das angegebene Zertifikat herunter. In der folgenden Tabelle finden Sie die Parameter für diesen Vorgang.

Parameter	Erforderlich	Beschreibung

id	Ja	Numerische Zertifikat-ID
dürfen Kennwort		Kennwort für das Zertifikat, das exportiert wird.
exportPrivateKey		Kennzeichen, das angibt, ob der private Schlüssel exportiert werden soll.

URL: https://:/xenmobile/api/v1/certificates/export

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{
    "id": "300",
    "password": "1111",
    "exportPrivateKey": true
}
```

Beispielantwort: zeigt die Zertifikatzeichenfolge bei einer erfolgreichen Anforderung an.

Verwalten von Schlüsselspeichern

Sie können Schlüsselspeicher über die öffentliche API importieren.

Import a server keystore

Importiert einen Server-Schlüsselspeicher.

URL: https://:/xenmobile/api/v1/certificates/import/keystore/server

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: Multipart/form-data

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
```

```
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Import SAML keystore

Importiert einen SAML-Schlüsselspeicher.

URL: https://:/xenmobile/api/v1/certificates/import/keystore/saml

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: Multipart/form-data

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
}
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
```

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Import APNs keystore

Importiert einen APNS-Schlüsselspeicher.

URL: https://:/xenmobile/api/v1/certificates/import/keystore/apns

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: Multipart/form-data

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':apns,
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
```

```
        "message": "Success",
        "csrRequest": null,
        "apnsCheck": {
                "topicNameMismatch": false,
                "certExpired": false,
                "certNotYetValid": false,
                "malformed": false
        },
        "certificate": null,
        "apnsCheckObj": {
                "topicNameMismatch": false,
                "certExpired": false,
                "certNotYetValid": false,
                "malformed": false
        }
}
```


Import SSL listener keystore

Importiert einen SSL-Listener-Schlüsselspeicher.

URL: https://:/xenmobile/api/v1/certificates/import/keystore/listener

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: Multipart/form-data

Anforderungsparameter KOPIEREN

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':"listener",
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

Beispielantwort KOPIEREN

```
{
```

```
        "status": 0,

        "message": "Success",

        "csrRequest": null,

        "apnsCheck": {

                "topicNameMismatch": false,

                "certExpired": false,

                "certNotYetValid": false,

                "malformed": false

        },

    "certificate": null,

    "apnsCheckObj": {

                "topicNameMismatch": false,

                "certExpired": false,

                "certNotYetValid": false,

                "malformed": false

        }

    }
```


Sie können über die öffentliche API Lizenzen verwalten.

Get license information

Listet Informationen über alle Lizenzen auf.

URL: https://:/xenmobile/api/v1/licenses

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
    status: 0
    message: "Success"
    cpLicenseServer: {
        serverAddress: "192.0.2.20"
        localPort: 0
        remotePort: 27000
        serverType: "remote"
        licenseType: "none"
        isServerConfigured: true
        gracePeriodLeft: 0
        isRestartLpeNeeded: null
        isScheduleNotificationNeeded: null
            licenseList: []
```

```
{
        sadate: "2015.1210"
        notice: "Example Systems Inc."
        vendorString: ";LT=Retail;GP=720;UDM=U;LP=90;CL=STD,ADV,ENT;SA=1;ODP=0"
        licensesInUse: 0
        licensesAvailable: 102
        overdraftLicenseCount: 2
        p_E_M: "CXM_ENTU_UD"
        serialNumber: "cxmretailent1000user"
        licenseType: "Retail"
        expirationDate: "01-DEC-2015"
}
licenseNotification:
{
        id: 1
        notificationEnabled: false
        notifyFrequency: 7
        notifyNumberDaysBeforeExpire: 60
        recepientList: ""
```

```
                emailContent: "License expiry notice"

            }

        }

}
```

Save license information

Speichert alle Lizenzinformationen.

URL: https://:/xenmobile/api/v1/licenses

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{

    "serverAddress": "192.0.2.20",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": "remote",

    "licenseType": "none",

    "isServerConfigured": true,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": true,
```

```
    "isScheduleNotificationNeeded": true,
    "licenseList": [],
    "licenseNotification": {
        "id": 1,
        "notificationEnabled": true,
        "notifyFrequency": 20,
        "notifyNumberDaysBeforeExpire": 60,
        "recepientList": "justa.name123@example.com",
        "emailContent": "Licenseexpirynotice"
    }
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success"
}
```

Upload license file

Lädt die angegebene Lizenzdatei hoch.

URL: https://:/xenmobile/api/v1/licenses/upload

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: Multipart/form-data

Anforderungsparameter: uploadFile =

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success"
}
```

Activate license

Aktiviert die angegebene Lizenz.

URL: https://:/xenmobile/api/v1/licenses/activate/{license type}

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter: Lizenztyp zur Aktivierung der Lizenz-URL anfügen.

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success"
    "cpLicenseServer": null
}
```

Remove all licenses

Entfernt alle Lizenzen.

URL: https://:/xenmobile/api/v1/licenses/remove

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "isConnected": null
}
```

Test license server

Führt einen Verbindungstest auf dem Lizenzserver durch.

URL: https://:/xenmobile/api/v1/licenses/testserver/

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{
    "serverAddress": "192.0.2.7",
    "localPort": 0,
    "remotePort": 27000,
    "serverType": null,
    "licenseType": null,
    "isServerConfigured": null,
    "gracePeriodLeft": 0,
    "isRestartLpeNeeded": null,
    "isScheduleNotificationNeeded": null,
    "licenseList": [],
    "licenseNotification": null
}
```


Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "isConnected": true
}
```

Get earliest expiration date

Sucht die Lizenz mit dem frühesten Ablaufdatum.

URL: https://:/xenmobile/api/v1/licenses/getexpirationdate

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{

    "status": 0,

    "message": "Success",

    "expiredDate": 1448956800000,

    "daysBeforeExpire": 229,

    "daysInPOC": 0

}
```


Verwalten von LDAP-Konfigurationen

In der folgenden Tabelle finden Sie die Parameter für LDAP-Konfigurationsvorgänge.

Parameter	Erforderlich	Beschreibung
primaryHost	Ja	IP-Adresse oder Hostname des primären LDAP-Servers. Eingabe als IP-Adresse oder FQDN.
secondaryHost	Nein	IP-Adresse oder Hostname des sekundären LDAP-Servers. Eingabe als IP-Adresse oder FQDN.
port	Ja	Portnummer des LDAP-Servers
username	Ja	Gültiger Benutzername für den LDAP-Server
dürfen Kennwort	Ja	Kennwort für username
userBaseDN	Ja	
lockoutLimit	Nein	

lockoutTime	Nein	
useSecure	Nein	
userSearchBy	Ja	Suche nach Benutzern über upn oder samaccount
domain	Ja	Eindeutiger Domänenname des LDAP-Servers
domainAlias	Ja	Alias für die LDAP-Domäne
globalCatalogPort	Nein	
gcRootContext	Nein	
groupBaseDN	Ja	
isDefault	Nein	Teil der GET-Antwort, die zeigt, ob es sich bei der LDAP-Konfiguration um die Standardeinstellung handelt.
name	Nein	Teil der GET-Antwort und eindeutige ID, die zum Aktualisieren oder Löschen der LDAP-Konfiguration verwendet wird.

List LDAP configuration

Listet die gesamte LDAP-Konfiguration in XenMobile auf.

URL: https://:/xenmobile/api/v1/ldap

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{

    “result”: [

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"aaa@example.com","password":"1.pwd","userBaseDN":"dc=

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"test@xmexample.com","password":"1.pwd","userBaseDN":"d

    ]

}
```

Add new LDAP configuration

Fügt eine neue LDAP-Konfiguration hinzu. Der Domänenname muss eindeutig sein und sich von dem aller anderen LDAP-Konfiguration unterscheiden.

URL: https://:/xenmobile/api/v1/ldap/msactivedirectory

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```

Beispielantwort KOPIEREN

```
{

    “status”: 0,

    “message”: “LDAP configuration created”

}
```

Edit LDAP configuration

Bearbeitet eine vorhandene LDAP-Konfiguration mit Ausnahme der Domäne, die mit "Edit" nicht geändert werden kann.

URL: https://:/xenmobile/api/v1/ldap/msactivedirectory/{name}

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{
    "primaryHost":"192.0.2.7",
    "secondaryHost":"",
    "port":"389",
    "username":"aaa@example.com",
    "password":"1.pwd",
    "userBaseDN":"dc=example,dc=com",
    "groupBaseDN":"dc=example,dc=com",
    "lockoutLimit":"0",
    "lockoutTime":"1",
    "useSecure":"false",
    "userSearchBy":"upn",
    "domain":"example.com",
    "domainAlias":"exampleAlias",
    "globalCatalogPort":"0",
    "gcRootContext":""
}
```


Set default LDAP configuration

Legt die angegebene LDAP-Konfiguration als Standard fest.

URL: https://:/xenmobile/api/v1/ldap/default/{name}

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Delete LDAP configuration

Löscht die angegebene LDAP-Konfiguration.

URL: https://:/xenmobile/api/v1/ldap/{name}

Anforderungstyp: DELETE

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Verwalten von NetScaler Gateway-Konfigurationen

Ermöglicht das Verwalten der NetScaler Gateway-Konfigurationen. In der folgenden Tabelle finden Sie die Parameter für NetScaler Gateway-Vorgänge.

Parameter	Erforderlich	Beschreibung
name	Ja	Eindeutiger Name für NetScaler Gateway
alias	Nein	
haben,	Ja	Öffentlich zugängliche URL für NetScaler Gateway
passwordRequired	Ja	
logonType	Ja	Gültige Werte: domain-only, domain-token, domain-certificate, certificate-only, certificate-token und token-only
callback	Nein	
sind	Ja	Legen Sie den Parameter auf "true" oder "false" fest, wenn Sie eine NetScaler Gateway-Konfiguration hinzufügen bzw. bearbeiten. Wenn Sie diesen Parameter nicht übergeben gilt standardmäßig "false".

id	Nein	Teil der GET-Antwort und eindeutige ID, die zum Aktualisieren oder Löschen der NetScaler Gateway-Konfiguration verwendet wird.

List all NetScaler Gateway configurations

Listet die gesamte NetScaler Gateway-Konfiguration in XenMobile auf.

URL: https://:/xenmobile/api/v1/netscaler

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{

    “result”: [

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false","id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        },

        { "name":"displayName",

        "alias":"",
```

```
            "url":"https://externalURl.com",

            "passwordRequired":"false",

            "logonType":"domain",

            "default":"false",

            "id":"",

            “callback”: [{“callbackUrl”:http://example.com,

            “ip”:”192.0.2.8”}]

            }

        ]

}
```

Add new NetScaler Gateway configuration

Fügt eine neue NetScaler Gateway-Konfiguration hinzu.

URL: https://:/xenmobile/api/v1/netscaler

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{

    "name":"displayName",

    "alias":"",

    “default”:true, "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “callback”: [{“callbackUrl”:http://example.com,

    “ip”:”192.0.2.8”}]

}
```

Edit NetScaler Gateway configuration

Bearbeitet die angegebene NetScaler Gateway-Konfiguration.

URL: https://:/xenmobile/api/v1/netscaler/{id}

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{

    "name":"displayName",

    "alias":"",

    "url":"https://externalURI.com",

    "passwordRequired":"false",

    "logonType":"domain",

    “default”: true,

    “callback”: [{“callbackUrl”:http://ag.com,

    “ip”:”192.0.2.8”}]

}
```

Delete NetScaler Gateway configuration

Löscht die angegebene NetScaler Gateway-Konfiguration.

URL: https://:/xenmobile/api/v1/netscaler/{id}

Anforderungstyp: DELETE

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Set default NetScaler Gateway configuration

Legt die angegebene NetScaler Gateway-Konfiguration als Standard fest.

URL: https://:/xenmobile/api/v1/netscaler/default/{id}

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Verwalten der Konfiguration des SMS- und des SMTP-Benachrichtigungsservers

Sie können Konfigurationen der SMS- und SMTP-Benachrichtigungsserver aktivieren (als Standardeinstellung festlegen), hinzufügen, bearbeiten und löschen. In der folgenden Tabelle finden Sie die Parameter für Konfigurationsvorgänge am SMS- und am SMTP-Server.

Parameter	Erforderlich	Beschreibung
name	Ja	Eindeutiger Name der SMS-/SMTP-Konfiguration.
serverType	Nein	Benachrichtigungsservertyp (SMS oder SMTP), der vom Server in der GET-Anforderung übermittelt wird
active	Nein	Gibt an, ob der Server für Benachrichtigungen verwendet wird. Es kann nur ein Server für jeden Typ aktiv sein.
id	Nein	Eindeutige Kennung, die zum Aktualisieren, Löschen oder Aktivieren des Servers verwendet wird
description	Nein	Beschreibung des Servers
SMS-Parameter		
key	Ja	
secret	Ja	
virtualPhoneNumber	Ja	Muss im Telefonnummernformat vorliegen.
https	Ja	Standardwert ist "false".
country	Ja	
carrierGateway	Ja	Standardwert ist "false".
SMTP-Parameter		
secureChannelProtocol	Ja	Typ des verwendeten Sicherheitsprotokolls. Gültige Werte: Ohne, SSL

		und TLS. Standardwert ist "Ohne".
port	Ja	
authentication	Ja	Gibt an, ob die Authentifizierung verwendet werden soll. Gültige Werte sind "true" und "false".
username	Ja, wenn authentication = true	
dürfen Kennwort	Ja, wenn authentication = true	
msSecurePasswordAuth	Ja	Standardwert ist "false".
fromName	Ja	
fromEmail	Ja	
numOfRetries	Nein	Eine Ganzzahl. Der Standardwert ist 5.
timeout	Nein	Eine Ganzzahl. Der Standardwert ist 30.
maxRecipients	Nein	Eine Ganzzahl. Der Standardwert ist 100.

List all SMS and SMTP servers

Listet alle SMS- und SMTP-Server in XenMobile auf.

URL: https://:/xenmobile/api/v1/notificationserver

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Accept: application/json

Beispielantwort KOPIEREN

```
{

    “result”: [

        { "name":"serverName","serverType":"SMS,"active":"true","id":"10"},

        { "name":"serverName2","serverType":"SMTP,"active":"true","id":"10"},

        { "name":"serverName3","serverType":"SMS,"active":"false","id":"10"}

    ]

}
```

Get server details

Ruft Informationen über die Server nach Server-ID ab.

URL: https://:/xenmobile/api/v1/notificationserver/{id}

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Accept: application/json

Beispielantwort SMS KOPIEREN

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false",

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Beispielantwort SMTP KOPIEREN

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.12",

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Add SMS server configuration

Fügt eine SMS-Serverkonfiguration hinzu.

URL: https://:/xenmobile/api/v1/notificationserver/sms

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false",

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Edit SMS server configuration

Bearbeitet die SMS-Serverkonfiguration.

URL: https://:/xenmobile/api/v1/notificationserver/sms/{id}

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{
    "name":"displayName",
    "description":"",
    "server":"192.0.2.9",
    "carrierGateway":"true",
    "country":"+93",
    "https":"false",
    “key”: “123456”,
    "secret":"secretKey",
    "virtualPhoneNumber":"4085552222",
    "carrierGateway":"true"
}
```

Add SMTP server configuration

Fügt eine SMTP-Serverkonfiguration hinzu.

URL: https://:/xenmobile/api/v1/notificationserver/smtp

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false",

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Edit SMTP configuration

Bearbeitet die SMTP-Serverkonfiguration.

URL: https://:/xenmobile/api/v1/notificationserver/smtp/{id}

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{
    name":"displayName",
    "description":"Edited description",
    "server":"192.0.2.9"
    "secureChannelProtocol":"true",
    "port":"345",
    "authentication":"false",
    “username”: “test”,
    “password”: “testPassword”,
    "msSecurePasswordAuth":"true",
    "fromName":"Email name",
    "fromEmail":test@example.com,
    "numOfRetries":5,
    "timeout":30,
    "maxRecipients":100
}
```

Delete server configuration

Löscht die angegebene SMS- oder SMTP-Serverkonfiguration.

URL: https://:/xenmobile/api/v1/notificationserver/{id}

Anforderungstyp: DELETE

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Set default SMS configuration

Legt die angegebene SMS-Serverkonfiguration als Standard fest.

URL: https://:/xenmobile/api/v1/notificationserver/activate/sms/{id}

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Set default SMTP configuration

Legt die angegebene SMTP-Serverkonfiguration als Standard fest.

URL: https://:/xenmobile/api/v1/notificationserver/activate/smtp/{id}

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Verwalten der lokalen Benutzer und Gruppen

Sie können lokale Benutzer und Gruppen mit den folgenden Diensten verwalten.

Get all users

Ruft alle lokalen Benutzer auf.

URL: https://:/xenmobile/api/v1/localusersgroups

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
```

```
"status": 0,

"message": "Success",

"result": [

    {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"

        },

        "role": "ADMIN",

        "roles": null,

        "createdOn": "1/10/15 11:42 AM",

        "lastAuthenticated": "1/10/15 11:42 AM",

        "domainName": null,

        "adUser": false,

        "vppUser": false

    }
```



```
    ]

}
```

Get one user

Ruft den angegebenen lokalen Benutzer auf.

URL: https://:/xenmobile/api/v1/localusersgroups/{name}

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{

    "status": 0,

    "message": "Success",

    "result": {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"
```

```
                company": "example"

            },

            "role": "ADMIN",

            "roles": null,

            "createdOn": "1/10/15 11:42 AM",

            "lastAuthenticated": "1/10/15 11:42 AM",

            "domainName": null,

            "adUser": false,

            "vppUser": false

        }

}
```

Add user

Fügt einen Benutzer mit den angegebenen Attributen hinzu.

URL: https://:/xenmobile/api/v1/localusersgroups

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{

    "attributes": {

            "badpwdcount": "4",

            "asuseremail": "justa.name@example.com",

            "company": "example",

            "mobile": "4695557854"

            },

    "groups": [

            "MSP"

            ],

    "role": "USER",

    "username": "justaname_XX",

    "password": "password"

}
```

Beispielantwort KOPIEREN

```
{

    "status": 0,
```

```
"message": "Success",
"user": {
    "userid": 0,
    "username": "justaname_XX",
    "password": "password",
    "confirmPassword": null,
    "groups": [
        "MSP"
    ],
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
    },
    "role": "USER",
    "roles": null,
    "createdOn": null,
    "lastAuthenticated": null,
    "domainName": null,
```



```
            "adUser": false,

            "vppUser": false

        }

}
```

Update user

Aktualisiert die Benutzerattribute.

URL: https://:/xenmobile/api/v1/localusersgroups

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{

    "attributes": {

            "badpwdcount": "4",

            "asuseremail": "justa.name@example.com",

            "company": "example",

            "mobile": "4695557854"

            },

    "groups": [

            "MSP"

            ],

    "role": "USER",

    "username": "justaname_XX",

    "password": "password"

}
```

Beispielantwort KOPIEREN

```
{

    "status": 0,
```

```
"message": "Success",
"user": {
    "userid": 108,
    "username": "justaname_XX",
    "password": null,
    "confirmPassword": null,
    "groups": [
        "MSP"
    ],
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
    },
    "role": "USER",
    "roles": null,
    "createdOn": "3/27/15 1:10 PM",
    "lastAuthenticated": "3/27/15 1:10 PM",
    "domainName": null,
```



```
            "adUser": false,

            "vppUser": false

        }

}
```

Change user password

Setzt das Kennwort eines Benutzers zurück. Sie können das Kennwort eines Benutzers auch über den Aufruf "update local user" ändern.

URL: https://:/xenmobile/api/v1/localusersgroups/resetpassword

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{

    "username": “administrator”,

    “password”: “newPassword”

}
```

Beispielantwort KOPIEREN

```
Response Errors:

1250 – User id not found

1252 – Failed to reset the password

Password can also be changed in the update local user call.
```

Delete users

Löscht die angegebenen Benutzer.

URL: https://:/xenmobile/api/v1/localusersgroups/resetpassword

Anforderungstyp: DELETE

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{ justaname XX }
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Delete one user

Löscht den angegebenen Benutzer.

URL: https://:/xenmobile/api/v1/localusersgroups/

Anforderungstyp: DELETE

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Import provisioning file

Lädt eine Datei mit den Daten lokaler Benutzer hoch. Die Datei muss im CSV-Format vorliegen. Weitere Informationen zu Provisioningdateien finden Sie unter Provisioningdateiformate.

URL: https://:/xenmobile/api/v1/localusersgroups/importprovisioningfile

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
importdata={"fileType:"user"}

uploadfile=<file to be uploaded.csv>
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

So verwalten Sie Apps

Sie können Apps mit den folgenden Diensten verwalten.

Get all apps by filter

Ruft die Apps nach den angegebenen Filterparametern auf.

URL: https://:/xenmobile/api/v1/application/filter

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)
Inhaltstyp: application/json

Beispiel für Anforderungsdaten KOPIEREN

```
{
    "start": 0,
    "limit": 10,

    "applicationSortColumn": "name",
    "sortOrder": "DESC",
    "enableCount": false,
    "search": "Worx",
    "filterIds":"['application.deliverygroup#<DG_Name>@_fn_@app.dg','application.deliverygroup#<DG_Name>@_fn_@app.dg']"
}
```

Beispiel für Antwortdaten KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "applicationListData": {
        "totalMatchCount": 2,
        "totalCount": 2,
        "appList": [{
            "id": 2,
            "name": "WorxNotes",
            "description": "Worx Notes Application",
            "createdOn": "6/7/16 3:55 PM",
            "lastUpdated": "6/7/16 5:11 PM",
            "disabled": false,
            "nbSuccess": 0,
            "nbFailure": 0,
            "nbPending": 0,
            "schedule": null,
            "permitAsRequired": true,
            "iconData": "iVBORw0KGgoAAAANSUhEUgAAAHgAAAB4CAYAAAA5ZDbSAAA.....",
            "appType": "MDX",
```



```
    "categories": ["Default"],
    "roles": null,
    "workflow": null,
    "vppAccount": null
  }, {
    "id": 1,
    "name": "Angry Bird",
    "description": "",
    "createdOn": "6/7/16 3:53 PM",
    "lastUpdated": "6/7/16 3:54 PM",
    "disabled": false,
    "nbSuccess": 0,
    "nbFailure": 0,
    "nbPending": 0,
    "schedule": null,
    "permitAsRequired": true,
    "iconData": "/9j/4AAQSkZJRgABAQEAAQABAAD/2wBDAAYEBQYFBAYGBQYHBwYIChA...",
    "appType": "App Store App",
    "categories": ["Default"],
    "roles": null,
```



```
            "workflow": null,
            "vppAccount": null
        }]
    }
}
```

Get mobile apps by container

Ruft mobile Apps in dem angegebenen Container auf.

URL: https://:/xenmobile/api/v1/application/mobile/{containerId}

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "result": {
        "id": 14,
        "name": "testApp",
        "description": "",
```

```
"createdOn": null,
"lastUpdated": null,
"disabled": false,
"nbSuccess": 0,
"nbFailure": 0,
"nbPending": 0,
"schedule": {
    "enableDeployment": true,
    "deploySchedule": "NOW",
    "deployScheduleCondition": "EVERYTIME",
    "deployDate": null,
    "deployTime": null,
    "deployInBackground": false
},
"iconData": "",
"appType": "MDX",
"categories": [
    "Default"
],
"roles": [],
```



```
"workflow": null,
"ios": {
"displayName": "GoToMeeting",
"description": "G2MW_IOS_5.3.3_075_01",
"paid": false,
"removeWithMdm": true,
"preventBackup": true,
"appVersion": "5.3.3.075",
"minOsVersion": "",
"maxOsVersion": "",
"excludedDevices": "",
"avppParams": null,
"avppTokenParams": null,
"rules": null,
"appType": "mobile_ios",
"uuid": "8e69d397-48bb-4f29-a95c-dd7b16665c1c",
"id": 0,
"store": {
"rating": {
"rating": 0,
```



```
            "reviewerCount": 0
        },
        "screenshots": [],
        "faqs": [],
        "storeSettings": {
            "rate": true,
            "review": true
        }
    },
    "policies": [
        {
            "policyName": "ReauthenticationPeriod",
            "policyValue": "480",
            "policyType": "integer",
            "policyCategory": "Authentication",
            "title": "Reauthentication period (minutes)",
            "description": "\nDefines the period before a user is challenged to authenticate again. ",
            "units": "minutes",
            "explanation": null
        },
```



```
{
        "policyName": "BlockJailbrokenDevices",
        "policyValue": "true",
        "policyType": "boolean",
        "policyCategory": "Device Security",
        "title": "Block jailbroken or rooted",
        "description": "\nIf On, the application is locked when the device is jailbroken or rooted.",
        "units": null,
        "explanation": null
},
{
        "policyName": "CertificateLabel",
        "policyValue": "",
        "policyType": "string",
        "policyCategory": "Network Access",
        "title": "Certificate label",
        "description": "\nThe label for the certificate.\n                                                    Default value is empty.\n
        "units": null,
        "explanation": null
}
```



```
                    ]
                },
                "android": null,
                "android_knox": null,
                "android_work": null,
                "windows": null,
                "windows_tab": null
            }
        }
```


Get public store apps by container

Ruft öffentliche Store-Apps in dem angegebenen Container auf.

URL: https://:/xenmobile/api/v1/application/mobile/appstore/{containerId}

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Delete app container

Löscht den angegebenen App-Container.

URL: https://:/xenmobile/api/v1/application/{containerId}

Anforderungstyp: DELETE

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Verwalten der Bereitstellungsgruppenkonfigurationen

Sie können Bereitstellungsgruppenkonfigurationen mit den folgenden Diensten verwalten.

Get delivery groups by filter

Ruft Bereitstellungsgruppen nach den angegebenen Filterparametern auf.

URL: https://:/xenmobile/api/v1/deliverygroups/filter

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
{
    "start": 1,
    "sortOrder": "DESC",
    "deliveryGroupSortColumn": "id",
    “limit”:10,
    "search": "add"
}
```

Beispielantwort KOPIEREN

```
{
        "status": 0,
        "message": "Success",
```

```
"dgListData": {

"totalMatchCount": 7,

"totalCount": 10,

"dgList": [

{

"id": null,

"name": "add delivery group 6.0",

"description": "testing add delivery group 6.0",

"groups": [[{

{

"id": 1null,

"userListId": 1null,

"name": "MSPTESTLOCALGROUP",

"uniqueName": "MSPTESTLOCALGROUP",

"uniqueId": "MSPTESTLOCALGROUP",

"domainName": "local",

"primaryToken": 0null,

}"objectSid": null

],},

{
```



```
            "id": null,

            "userListId": null,

            "name": "AC08EP61S75",

            "uniqueName": "AC08EP61S75",

            "uniqueId": "AC08EP61S75",

            "domainName": "local",

            "primaryToken": null,

            "objectSid": null

        }],

        "users": [{

            "uniqueName": null,

            "domainName": "local",

            "name": null,

            "objectId": "shankar",

            "customProperties": {

                "name": "value",

                "name1": "value1"

            },

            "uniqueId": "shankar"

        }],
```



```
"zoneId": null,

"zoneDomain": null,

"rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\":\"001-restri

"disabled": false,

"lastUpdated": 1427144713353,

"anonymousUser": true,

"roledefLangVersionId": 1,

"applications": [

        {

                "name": "Web Link",

                "required": false

        },

        {

                "name": "GoogleApps_SAML",

                "required": true

        }

],

"devicePolicies": [

        "test terms conditions"

]
```



```
        ],
        "smartActions": [
            "shankar ganesh"
        ],
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    },
    {
        "id": null,
        "name": "add delivery group 5.0",
        "description": "testing add delivery group 5.0",
        "groups": [
            {
                "id": 1,
                "userListId": 1,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP",
                "domainName": "local",
```



```
                "primaryToken": 0

            }

        ],

        "zoneId": null,

        "zoneDomain": null,

        "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\":\"001-restri

        "disabled": false,

        "lastUpdated": 1426891345698,

        "anonymousUser": true,

        "roledefLangVersionId": 1,

        "applications": [

            {

                "name": "GoogleApps_SAML",

                "required": true

            },

            {

                "name": "Web Link",

                "required": false

            }

        ],
```



```
                    "devicePolicies": [

                        "test terms conditions"

                    ],

                    "smartActions": [

                        "shankar ganesh"

                    ],

                    "nbSuccess": 0,

                    "nbFailure": 0,

                    "nbPending": 0

                }

            ]

        }


}
```


Get delivery group by name

URL: https://:/xenmobile/api/v1/deliverygroups/{name}

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": null,
        "name": "AllUsers",
        "description": "default role",
        "groups": [],
        "zoneId": null,
        "zoneDomain": null,
        "rules": null,
        "disabled": false,
        "lastUpdated": null,
        "anonymousUser": false,
        "roledefLangVersionId": 1,
        "applications": [
            {
                "name": "test mdx",
                "required": false
            },
```



```
        {
            "name": "test all",
            "required": false
        },
        {
            "name": "justa test",
            "required": false
        },
        {
            "name": "test enterprise",
            "required": false
        },
        {
            "name": "name test",
            "required": false
        }
    ],
    "devicePolicies": [
        "test terms conditions"
    ]
```



```
            ],
            "smartActions": [
                "justa name"
            ],
            "nbSuccess": 0,
            "nbFailure": 0,
            "nbPending": 0
        }
}
```

Edit delivery group

URL: https://:/xenmobile/api/v1/deliverygroups

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
{
    "name": "temp3",
    "description": "temp3 desc",
    "applications": [
```

```
{

                "name": "TESTAPP",

                 "priority": -1,

                 "required": false

                        }       ],
      "devicePolicies": [
         {
                "name":"test terms conditions",
                "priority":-1
          }
      ],
      "smartActions": [
         {
            "name":"Smart Action Name 1",
            "priority":-1
          }
      ],
   "groups": [

      {

  "uniqueName": "AC08EP61S75",

          "domainName": "local",

          "name": "AC08EP61S75",

          "objectSid": "AC08EP61S75",
```



```
"uniqueId": "AC08EP61S75",

"customProperties": {

        "gr1": "gr1",

        "gr2": "gr2"

    }

        }

    ],

    "users": [

        {

            "uniqueName": "testuser",

            "domainName": "local",

            "name": " testuser ",

            "objectId": " testuser "

        }

    ],

    "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\" testuser@citrix.co

}
```


Beispielantwort KOPIEREN


```
{
        "status": 0,
        "message": "Success",
"role": {
                "id": null,
                "name": "temp4",
                "description": "temp4 desc",
                "zoneId": null,
                "zoneDomain": null,
                "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\"tempuser
                "disabled": false,
                "lastUpdated": null,
                "anonymousUser": false,
                "roledefLangVersionId": null,
                "applications": [
                        {
                        "name": "TESTAPP2",
                        "priority": -1,
```



```
                "required": false
            },
{
                "name": "TESTAPP2",
                "priority": -1,
                "required": false
            }
            ],
            "devicePolicies": [
                {
                "name": "TestPolicy1",
                "priority": -1
            },
{
                "name": "TestPolicy",
                "priority": -1
            }
            ],
            "smartActions": [
```



```
{
                "name": "TestAction2",
                "priority": -1
            },
{
                "name": "TestAction3",
                "priority": -1
            }
        ],
            "nbSuccess": 0,
            "nbFailure": 0,
            "nbPending": 0,
            "groups": [{
                "uniqueName": "AC08EP61S75",
                "domainName": "local",
                "name": "AC08EP61S75",
                "objectSid": "AC08EP61S75",
                "uniqueId": "AC08EP61S75",
                "customProperties": {
                    "gr1": "gr1",
```



```
                    "gr2": "gr2"

                }

            }],

            "users": [{

                "uniqueName": " tempuser ",

                "domainName": "local",

                "name": " tempuser ",

                "objectId": " tempuser ",

                "customProperties": null,

                "uniqueId": " tempuser "

            }]


    }
```

Add delivery group

Fügt eine Bereitstellungsgruppe hinzu.

URL: https://:/xenmobile/api/v1/deliverygroups

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
{

    "name": "temp3",

    "description": "temp3 desc",

    "applications": [

{

                "name": "TESTAPP",

                 "priority": -1,

                 "required": false

                        }      ],

      "devicePolicies": [

         {

              "name":"test terms conditions",

              "priority":-1

          }

      ],

      "smartActions": [

         {

            "name":"Smart Action Name 1",

            "priority":-1

          }

      ],

    "groups": [

      {
```



```
    "uniqueName": "AC08EP61S75",
            "domainName": "local",
            "name": "AC08EP61S75",
            "objectSid": "AC08EP61S75",
"uniqueId": "AC08EP61S75",
"customProperties": {
        "gr1": "gr1",
        "gr2": "gr2"
    }}
    ],
    "users": [
        {
            "uniqueName": "testuser",
            "domainName": "local",
            "name": " testuser ",
            "objectId": " testuser "
        }
    ],
    "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\" testuser@citrix.co
```



```
}
```

Beispielantwort KOPIEREN


```
{
        "status": 0,
        "message": "Success",
"role": {
                "id": null,
                "name": "temp4",
                "description": "temp4 desc",
                "zoneId": null,
                "zoneDomain": null,
                "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\"shankar.g
                "disabled": false,
                "lastUpdated": null,
                "anonymousUser": false,
                "roledefLangVersionId": null,
                "applications": [
                        {
                        "name": "TESTAPP2",
```



```
                "priority": -1,
                "required": false
            },
{
                "name": "TESTAPP2",
                "priority": -1,
                "required": false
            }
            ],
            "devicePolicies": [
                {
                "name": "TestPolicy1",
                "priority": -1
            },
{
                "name": "TestPolicy",
                "priority": -1
            }
            ],
```



```
                "smartActions": [
{
                        "name": "TestAction2",
                        "priority": -1
                },
{
                        "name": "TestAction3",
                        "priority": -1
                }
        ],
                "nbSuccess": 0,
                "nbFailure": 0,
                "nbPending": 0,
                "groups": [{
                        "uniqueName": "AC08EP61S75",
            "domainName": "local",
            "name": "AC08EP61S75",
            "objectSid": "AC08EP61S75",
"uniqueId": "AC08EP61S75",
"customProperties": {
```



```
        "gr1": "gr1",

        "gr2": "gr2"

    }           }],

                "users": [{

                        "uniqueName": " tempuser ",

                        "domainName": "local",

                        "name": " tempuser ",

                        "objectId": " tempuser ",

                        "customProperties": null,

                        "uniqueId": " tempuser "

                }]


      }
```

Delete delivery group

Löscht die angegebenen Bereitstellungsgruppen.

URL: https://:/xenmobile/api/v1/deliverygroups

Anforderungstyp: DELETE

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
[ "add delivery group 11.0" ]
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "roleNames": [
        "add delivery group 11.0"
    ]
}
```

Enable or Disable Delivery Group

Aktiviert oder deaktiviert die angegebenen Bereitstellungsgruppen.

URL: https://:/xenmobile/api/v1/deliverygroups/{bereitstellungsgruppennuame}/{enable/disable}

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "roleName": "AllUsers"
}
```

Verwalten von Servereigenschaften

Sie können XenMobile-Servereigenschaften mit folgenden Diensten verwalten.

Get all server properties

Ruft alle aktuellen XenMobile-Servereigenschaften auf.

URL: https://:/xenmobile/api/v1/serverproperties

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": [
        {
            "id": 1,
            "name": "ios.mdm.pki.ca-root.certificatefile",
```

```
        "value": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayName": "ios.mdm.pki.ca-root.certificatefile",

        "description": "",

        "defaultValue": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayFlag": false,

        "editFlag": true,

        "deleteFlag": false,

        "markDeleted": false

    } ,

    {

        "id": 2,

        "name": "ios.mdm.https.host",

        "value": "192.0.2.4",

        "displayName": "ios.mdm.https.host",

        "description": "",

        "defaultValue": "192.0.2.4",

        "displayFlag": false,

        "editFlag": false,

        "deleteFlag": false,
```



```
                "markDeleted": false

            },

            {

                "id": 3,

                "name": "ios.mdm.enrolment.checkRemoteAddress",

                "value": "false",

                "displayName": "iOS Device Management Enrollment - Check Remote Address",

                "description": "",

                "defaultValue": "false",

                "displayFlag": true,

                "editFlag": true,

                "deleteFlag": false,

                "markDeleted": false

            },

        ]

}
```


Get server properties by filter

Ruft die Servereigenschaften nach den angegebenen Filterparametern auf.

URL: https://:/xenmobile/api/v1/serverproperties/filter

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{
    "start": 0,
    "limit": 1000,
    "orderBy": "name",
    "sortOrder": "desc",
    "searchStr": "justaserver1"
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": [
        {
            "id": 154,
            "name": "justaserver123",
```

```
                "value": "justaserver1",
                "displayName": "justarserver display name",
                "description": "justaserver description",
                "defaultValue": "justaserver1",
                "displayFlag": true,
                "editFlag": true,
                "deleteFlag": true,
                "markDeleted": false
            }
        ]
    }
```

Add server property

Fügt die angegebene Servereigenschaft hinzu.

URL: https://:/xenmobile/api/v1/serverproperties

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 1",
    "description": "Description 1"
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": null
}
```

Edit server properties

Bearbeitet die angegebene Servereigenschaft.

URL: https://:/xenmobile/api/v1/serverproperties

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 2",
    "description": "Description 2"
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Reset server properties

Setzt die angegebenen Servereigenschaften zurück.

URL: https://:/xenmobile/api/v1/serverproperties/reset

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{
    "names": [,
        "justaname7"
        ]
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": null
}
```

Delete server properties

URL: https://:/xenmobile/api/v1/serverproperties

Anforderungstyp: DELETE

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Anforderungsparameter KOPIEREN

```
{
    "justaname3",
    "justaname4"
}
```

Beispielantwort KOPIEREN

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Verwalten von Geräten

Sie können Geräte in XenMobile mit folgenden Diensten verwalten.

Get Devices by Filter

URL: https://:/xenmobile/api/v1/device/filter

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Alle Anforderungsparameter sind optional.

Gültige Werte für **sortOrder** : ASC, DSC und DESC.

Gültige Werte für **sortColumn**: ID, SERIAL, IMEI, ACTIVESYNCID, WIFIMAC, BLUETOOTHMAC, OSFAMILY, SYSTEM_OEM, SYSTEM_PLATFORM, SYSTEM_OS_VERSION, DEVICE_PROPERTY, LASTAUTHDATE, INACTIVITYDAYS,ISACTIVE, LASTUSER, BLCOMPLIANT, WLCOMPLIANT, RLCOMPLIANT, MANAGED, SHAREABLE und BULKPROFILESTATUS.

Anforderungsparameter KOPIEREN

```
{

    "start": "0-999",

    "limit": "0-999",

    "sortOrder": "ASC",

    "sortColumn": "ID",

    "search": "Any search term",

    "enableCount": "false",

    "constraints": "{'constraintList':[{'constraint':'DEVICE_OS_FAMILY','parameters':[{'name':'osFamily','type':'STRING','value':'iOS'}]}]}",

    "filterIds": "['group#/group/MSP@_fn_@normal']"

}
```

Beispielantwort KOPIEREN

```
{

    "id": "1-9999999",
```

```
"jailBroken": "true/false",

"managed": "true/false",

"gatewayBlocked": "true/false",

"deployFailed": "1-999",

"deployPending": "1-999",

"deploySuccess": "1-999",

"mdmKnown": "true/false",

"mamRegistered": "true/false",

"mamKnown": "true/false",

"userName": "user name",

"serialNumber": "serial number",

"imeiOrMeid": "IMEI/MEID",

"activeSyncId": "Active sync ID",

"wifiMacAddress": "WiFi MAC address",

"blueToothMacAccress": "Bluetoothi MAC address",

"devicePlatform": "Device platform",

"osVersion": "Operating system version of the device",

"deviceModel": "Device model information",

"lastAccess": "Timestamp when the device was last accessed",

"inactivityDays": "Number of days device has been inactive",
```



```
    "shareable": "Flag indicating if the device is shareable",
    "sharedStatus": "Get shareable status of the device",
    "depRegistered": "Flag indicating if the device is DEP registered",
    "deviceName": "Name of the device",
    "deviceType": "Phone/Tablet",
    "productName": "Product name",
    "platform": "Platform of the device"
}
```

Get Devices by Device ID

URL: https://:/xenmobile/api/v1/device/{device_id}

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "device": {
    "htcMdm": true,
    "managedByZMSP": true,
```

```
"serialNumber": "string",
"id": 0,
"applications": [
  {
    "resourceType": "APP_NATIVE",
    "resourceTypeLabel": "string",
    "packageInfo": "string",
    "statusLabel": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
  }
],
"smartActions": [
  {
    "resourceType": "APP_NATIVE",
    "resourceTypeLabel": "string",
    "packageInfo": "string",
    "statusLabel": "string",
    "lastUpdate": 0
```



```
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
  }
],
"platform": "string",
"osFamily": "WINDOWS",
"nbSuccess": 0,
"nbFailure": 0,
"nbPending": 0,
"deliveryGroups": [
  {
    "statusLabel": "string",
    "linkey": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
  }
],
"lastAuthDate": 0,
```



```
"sharedStatus": "INACTIVE",

"managed": true,

"smgStatus": "ACCESS_ALLOWED",

"mdmKnown": true,

"mamKnown": true,

"mamRegistered": true,

"lastUsername": "string",

"imei": "string",

"activesyncid": "string",

"wifimac": "string",

"bluetoothmac": "string",

"inactivityDays": 0,

"shareable": true,

"bulkProfileStatus": "NO_BULK",

"deviceType": "string",

"softwareInventory": [

 {

   "version": "string",

   "blacklistCompliant": true,

   "suggestedListCompliant": true,
```



```
      "packageInfo": "string",
      "installCount": 0,
      "installTimeStamp": 0,
      "author": "string",
      "container": 0,
      "name": "string",
      "size": 0
    }
  ],
  "deviceActions": [
    {
      "actionType": "WIPE",
      "failedTime": 0,
      "doneTime": 0,
      "askedTime": 0
    }
  ],
  "managedSoftwareInventory": [
    {
      "version": "string",
```



```
      "blacklistCompliant": true,
      "suggestedListCompliant": true,
      "packageInfo": "string",
      "installCount": 0,
      "installTimeStamp": 0,
      "author": "string",
      "container": 0,
      "name": "string",
      "size": 0
    }
  ],
  "policies": [
    {
      "resourceType": "APP_NATIVE",
      "resourceTypeLabel": "string",
      "packageInfo": "string",
      "statusLabel": "string",
      "lastUpdate": 0,
      "status": "SUCCESS",
      "name": "string"
```



```
  }
],
"active": true,
"xmlId": "string",
"deviceUsers": [
  {
    "user": {
      "displayName": "string",
      "id": 0,
      "xmlId": "string",
      "properties": [
        {
          "displayName": "string",
          "id": 0,
          "b64": true,
          "group": "string",
          "name": "string",
          "value": "string"
        }
```

```
        ]

      },

      "lastAuthDate": 0,

      "prevAuthDate": 0,

      "userLogin": "string"

    }

  ],

  "packageStates": [

    {

      "packageName": "string",

      "packageId": 0,

      "statusLabel": "string",

      "date": 0,

      "status": "PENDING"

    }

  ],

  "pushState": "ENQUEUED",

  "pushStateLabel": "string",

  "lastPushDate": 0,

  "lastSentNotification": 0,
```



```
"lastRepliedNotification": 0,

"strongId": "string",

"lastSoftwareInventoryTime": 0,

"firstConnectionDate": 0,

"lastIOSProfileInventoryTime": 0,

"lastUser": {

  "displayName": "string",

  "id": 0,

  "xmlId": "string",

  "properties": [

    {

      "displayName": "string",

      "id": 0,

      "b64": true,

      "group": "string",

      "name": "string",

      "value": "string"

    }

  ]

},
```



```
"blacklistCompliant": true,

"suggestedListCompliant": true,

"requiredListCompliant": true,

"devicePropertiesTimestamp": 0,

"revoked": true,

"mamDeviceId": "string",

"deviceToken": "string",

"typeInst": 0,

"appLock": true,

"appWipe": true,

"mamReady": true,

"validCertificates": [

 {

   "credentialProviderId": "string",

   "type": "string",

   "issuerName": "string",

   "startDate": 0,

   "endDate": 0,

   "revoked": true,

   "certificateNumber": "string"
```



```
  }
],
"revokedCertificates": [
  {
    "credentialProviderId": "string",
    "type": "string",
    "issuerName": "string",
    "startDate": 0,
    "endDate": 0,
    "revoked": true,
    "certificateNumber": "string"
  }
],
"authorizeEnabled": true,
"revokeEnabled": true,
"lockEnabled": true,
"cancelLockEnabled": true,
"unlockEnabled": true,
"cancelUnlockEnabled": true,
"containerLockEnabled": true
```

```
"containerLockEnabled": true,

"cancelContainerLockEnabled": true,

"containerUnlockEnabled": true,

"cancelContainerUnlockEnabled": true,

"containerPwdResetEnabled": true,

"cancelContainerPwdResetEnabled": true,

"wipeEnabled": true,

"cancelWipeEnabled": true,

"clearRestrictionsEnabled": true,

"cancelClearRestrictionsEnabled": true,

"corpWipeEnabled": true,

"cancelCorpWipeEnabled": true,

"sdCardWipeEnabled": true,

"cancelSdCardWipeEnabled": true,

"locateEnabled": true,

"cancelLocateEnabled": true,

"enableTrackingEnabled": true,

"disableTrackingEnabled": true,

"disownEnabled": true,

"activationLockBypassEnabled": true,
```



```
"ringEnabled": true,

"cancelRingEnabled": true,

"newPinCode": "string",

"oldPinCode": "string",

"lockMessage": "string",

"resetPinCode": true,

"scanTime": "string",

"screenSharingPwd": "string",

"iosprofileInventory": [

 {

   "iosConfigInventories": [

     {

       "description": "string",

       "type": "string",

       "organization": "string",

       "identifier": "string",

       "name": "string"

     }

   ],

   "description": "string",
```



```
      "organization": "string",
      "managed": true,
      "identifier": "string",
      "receivedDate": 0,
      "encrypted": true,
      "name": "string"
    }
  ],
  "iosprovisioningProfileInventory": [
    {
      "managed": true,
      "uuid": "string",
      "expiryDate": 0,
      "name": "string"
    }
  ],
  "erasedMemoryCard": true,
  "gpsCoordinates": [
    {
      "gpsTimestamp": 0
```



```
  }
],
"lastGpsCoordinate": {
  "gpsTimestamp": 0
},
"gpsFilterStartDate": 0,
"gpsFilterEndDate": 0,
"wipePinCode": "string",
"lockPhoneNumber": "string",
"dstDevIdUsed": true,
"dstValue": "string",
"smartActionsFailure": true,
"policiesFailure": true,
"applicationsFailure": true,
"touchdownProperties": [
  {
    "category": "string",
    "name": "string",
    "value": "string"
  }
```



```
],
"appUnwipeEnabled": true,
"requestMirroringEnabled": true,
"cancelRequestMirroringEnabled": true,
"stopMirroringEnabled": true,
"cancelStopMirroringEnabled": true,
"knownByZMSP": true,
"wipeDeviceFlag": true,
"lockDeviceFlag": true,
"appWipeEnabled": true,
"appLockEnabled": true,
"appUnlockEnabled": true,
"bulkEnrolled": true,
"nbAvailable": 0,
"hasContainer": true,
"connected": true,
"properties": [
 {
   "displayName": "string",
```

```
        "id": 0,

        "b64": true,

        "group": "string",

        "name": "string",

        "value": "string"

      }

    ]

  }

}
```


Get Device Apps by Device ID

URL: https://:/xenmobile/api/v1/device/{device_id}/apps

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "applications": [
    {
      "resourceType": "APP_NATIVE",
      "resourceTypeLabel": "string",
      "packageInfo": "string",
      "statusLabel": "string",
      "lastUpdate": 0,
      "status": "SUCCESS",
      "name": "string"
    }
  ]
}
```


Get Device Actions by Device ID

URL: https://:/xenmobile/api/v1/device/{device_id}/actions

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN


```
{
  "status": 0,
  "message": "string",
  "actions": [
    {
      "resourceType": "APP_NATIVE",
      "resourceTypeLabel": "string",
      "packageInfo": "string",
      "statusLabel": "string",
      "lastUpdate": 0,
      "status": "SUCCESS",
      "name": "string"
    }
  ]
}
```


Get Device Delivery Groups by Device ID

URL: https://:/xenmobile/api/v1/device/{device_id}/deliverygroups

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN


```
{
  "status": 0,
  "message": "string",
  "deliveryGroups": [
    {
      "statusLabel": "string",
      "linkey": "string",
      "lastUpdate": 0,
      "status": "SUCCESS",
      "name": "string"
    }
  ]
}
```


Get Managed Software Inventory by Device ID

URL: https://:/xenmobile/api/v1/device/{device_id}/managedswinventory

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN


```
{
  "status": 0,
  "message": "string",
  "softwareInventory": [
    {
      "version": "string",
      "blacklistCompliant": true,
      "suggestedListCompliant": true,
      "packageInfo": "string",
      "installCount": 0,
      "installTimeStamp": 0,
      "author": "string",
      "container": 0,
      "name": "string",
      "size": 0
    }
  ]
}
```

Get Policies by Device ID

URL: https://:/xenmobile/api/v1/device/{device_id}/policies

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "policies": [
    {
      "resourceType": "APP_NATIVE",
      "resourceTypeLabel": "string",
      "packageInfo": "string",
      "statusLabel": "string",
      "lastUpdate": 0,
      "status": "SUCCESS",
      "name": "string"
    }
  ]
}
```

Get Software Inventory by Device ID

URL: https://:/xenmobile/api/v1/device/{device_id}/softwareinventory

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN


```
{
  "status": 0,
  "message": "string",
  "softwareInventory": [
    {
      "version": "string",
      "blacklistCompliant": true,
      "suggestedListCompliant": true,
      "packageInfo": "string",
      "installCount": 0,
      "installTimeStamp": 0,
      "author": "string",
      "container": 0,
      "name": "string",
      "size": 0
    }
  ]
}
```

Get GPS Coordinates by Device ID

URL: https://:/xenmobile/api/v1/device/locations/{geräte_id}

Abfrageparameter:

startDate: Startdatum für den Koordinatenfilter
endDate: Enddatum für den Koordinatenfilter

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{

  "status": 0,

  "message": "string",

  "deviceCoordinates": {

    "deviceCoordinateList": {

      "deviceCoordinateList": [

        {

          "gpsTimestamp": 0

        }

      ],

      "startDate": 0,

      "endDate": 0

    }

}
```

Send Notification to a List of Devices or Users

URL: https://:/xenmobile/api/v1/device/notify

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
{
  "smtpFrom": "Test",
  "to": [
    {
      "deviceId": "1",
      "email": "user@test.com",
      "osFamily": "iOS",
      "serialNumber": "F7NLX6WDF196",
      "smsTo": "+123456676",
      "token": {
        "type": "apns",
        "value": "dfb2fb351a4fb068e40858ecad572e317e6c39b4fa7de6fb29ea1ad7e2254499"
      }
    }
  ],
  "smtpSubject": "This is test subject",
  "smtpMessage": "This is test message",
  "smsMessage": "This is test message",
  "agentMessage": "This is test message",
  "sendAsBCC": "true",
```

```
"smtp": "true",

"sms": "true",

"agent": "true",

"templateId": "-1",

"agentCustomProps": {

  "sound": "Casino.wav"

}
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "notificationRequests": {
    "smtpNotifRequestId": 0,
    "smsNotifRequestId": 0,
    "smsGatewayNotifRequestId": 0,
    "apnsAgentNotifRequestId": 0,
    "shtpAgentNotifRequestId": 0
  }
}
```


Authorize a List of Devices

URL: https://:/xenmobile/api/v1/device/authorize

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN


```
[1,2]
```


Beispielantwort KOPIEREN


```
{

  "status": 0,

  "message": "string",

  "deviceActionMessages": {

    "devicesActionParameters": {

      "description": "string",

      "messageList": [

        {

          "id": "string",

          "message": "string"

        }

      ]

    }

  }

}
```

Apply Activation Lock Bypass on a List of Devices

URL: https://:/xenmobile/api/v1/device/activationLockBypass

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Apply App Lock on a List of Devices

URL: https://:/xenmobile/api/v1/device/appLock

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Apply App Wipe on a List of Devices

URL: https://:/xenmobile/api/v1/device/appWipe

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Apply Container Lock on a List of Devices

URL: https://:/xenmobile/api/v1/device/containerLock

Abfrageparameter: newPinCode: PIN-Code für den Android Container

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{

  "status": 0,

  "message": "string",

  "deviceActionMessages": {

    "devicesActionParameters": {

      "description": "string",

      "messageList": [

        {

          "id": "string",

          "message": "string"

        }

      ]

    }

  }

}
```

Cancel Container Lock on a List of Devices

URL: https://:/xenmobile/api/v1/device/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Apply Container Unlock on a List of Devices

URL: https://:/xenmobile/api/v1/device/containerUnlock

Abfrageparameter: newPinCode: PIN-Code für den Android Container

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{

  "status": 0,

  "message": "string",

  "deviceActionMessages": {

    "devicesActionParameters": {

      "description": "string",

      "messageList": [

        {

          "id": "string",

          "message": "string"

        }

      ]

    }

  }

}
```

Cancel Container Unlock on a List of Devices

URL: https://:/xenmobile/api/v1/device/containerUnlock/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Reset Container Password on a List of Devices

URL: https://:/xenmobile/api/v1/device/containerPwdReset

Abfrageparameter: newPinCode: PIN-Code für den Android Container

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{

  "status": 0,

  "message": "string",

  "deviceActionMessages": {

    "devicesActionParameters": {

      "description": "string",

      "messageList": [

        {

          "id": "string",

          "message": "string"

        }

      ]

    }

  }

}
```

Cancel Reset Container Password on a List of Devices

URL: https://:/xenmobile/api/v1/device/containerPwdReset/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Disown a List of Devices

URL: https://:/xenmobile/api/v1/device/disown

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{

  "status": 0,

  "message": "string",

  "deviceActionMessages": {

    "devicesActionParameters": {

      "description": "string",

      "messageList": [

        {

          "id": "string",

          "message": "string"

        }

      ]

    }

  }

}
```

Locate a List of Devices

URL: https://:/xenmobile/api/v1/device/locate

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Cancel Locating a List of Devices

URL: https://:/xenmobile/api/v1/device/locate/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Apply GPS Tracking on a List of Devices

URL: https://:/xenmobile/api/v1/device/track

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Cancel GPS Tracking on a List of Devices

URL: https://:/xenmobile/api/v1/device/track/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```


Lock a List of Devices

URL: https://:/xenmobile/api/v1/device/lock

Abfrageparameter:

newPinCode: PIN-Code muss für Android- und Symbian-Geräte zwischen 4 und 16 Zeichen lang sein. PIN-Code muss für Windows-Geräte 4 Zeichen lang sein.

resetPinCode: fügt der Sperranforderung eine Anforderung zum Zurücksetzung des PIN-Codes hinzu. Nur für Windows Phone 8.1 verfügbar
lockMessage: fügt der Sperranforderung eine Nachricht hinzu. Nur für iOS 7 und höher verfügbar.
phoneNumber: fügt der Sperranforderung eine Telefonnummer hinzu. Nur für iOS 7 und höher verfügbar.

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{

  "status": 0,

  "message": "string",

  "deviceActionMessages": {

    "devicesActionParameters": {

      "description": "string",

      "messageList": [

        {

          "id": "string",

          "message": "string"

        }

      ]

    }

  }

}
```

Cancel Locking a List of Devices

URL: https://:/xenmobile/api/v1/device/lock/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Unlock a List of Devices

URL: https://:/xenmobile/api/v1/device/unlock

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{

  "status": 0,

  "message": "string",

  "deviceActionMessages": {

    "devicesActionParameters": {

      "description": "string",

      "messageList": [

        {

          "id": "string",

          "message": "string"

        }

      ]

    }

  }

}
```

Cancel Unlocking a List of Devices

URL: https://:/xenmobile/api/v1/device/track/unlock/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Deploy a List of Devices

URL: https://:/xenmobile/api/v1/device/refresh

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{

  "status": 0,

  "message": "string",

  "deviceActionMessages": {

    "devicesActionParameters": {

      "description": "string",

      "messageList": [

        {

          "id": "string",

          "message": "string"

        }

      ]

    }

  }

}
```

Request AirPlay Mirroring on a List of Devices

URL: https://:/xenmobile/api/v1/device/requestMirroring

Abfrageparameter:

dstName: Name des Ziels (Name oder Geräte-ID)
dstDevId: MAC-Adresse des Zielgeräts (Name oder Zielgeräte-ID)

scanTime: Scandauer in Sekunden
screenSharingPwd: Kennwort für Bildschirmfreigabe

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{

  "status": 0,

  "message": "string",

  "deviceActionMessages": {

    "devicesActionParameters": {

      "description": "string",

      "messageList": [

        {

          "id": "string",

          "message": "string"

        }

      ]

    }

  }

}
```

Cancel Request for AirPlay Mirroring on a List of Devices

URL: https://:/xenmobile/api/v1/device/requestMirroring/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Stop AirPlay Mirroring on a List of Devices

URL: https://:/xenmobile/api/v1/device/stopMirroring

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{

  "status": 0,

  "message": "string",

  "deviceActionMessages": {

    "devicesActionParameters": {

      "description": "string",

      "messageList": [

        {

          "id": "string",

          "message": "string"

        }

      ]

    }

  }

}
```

Cancel Stop AirPlay Mirroring on a List of Devices

URL: https://:/xenmobile/api/v1/device/track/stopMirroring/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Clear All Restrictions on a List of Devices

URL: https://:/xenmobile/api/v1/device/track/restrictions/clear

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Cancel Clear All Restrictions on a List of Devices

URL: https://:/xenmobile/api/v1/device/track/restrictions/clear/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Revoke a List of Devices

URL: https://:/xenmobile/api/v1/device/revoke

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Ring a List of Devices

URL: https://:/xenmobile/api/v1/device/ring

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Cancel Ringing a List of Devices

URL: https://:/xenmobile/api/v1/device/track/ring/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Wipe a List of Devices

URL: https://:/xenmobile/api/v1/device/wipe

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Cancel Wipe of a List of Devices

URL: https://:/xenmobile/api/v1/device/track/wipe/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{

  "status": 0,

  "message": "string",

  "deviceActionMessages": {

    "devicesActionParameters": {

      "description": "string",

      "messageList": [

        {

          "id": "string",

          "message": "string"

        }

      ]

    }

  }

}
```

Selectivly Wipe a List of Devices

URL: https://:/xenmobile/api/v1/device/selwipe

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Cancel Selectivly Wiping a List of Devices

URL: https://:/xenmobile/api/v1/device/track/selwipe/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Wipe SD Cards on a List of Devices

URL: https://:/xenmobile/api/v1/device/sdcardwipe

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Cancel Wiping SD Cards on a List of Devices

URL: https://:/xenmobile/api/v1/device/track/sdcardwipe/cancel

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
[1,2]
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceActionMessages": {
    "devicesActionParameters": {
      "description": "string",
      "messageList": [
        {
          "id": "string",
          "message": "string"
        }
      ]
    }
  }
}
```

Get All Known Properties on a Device

URL: https://:/xenmobile/api/v1/device/knownProperties

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN


```
{
  "status": 0,
  "message": "string",
  "knownProperties": {
    "knownProperties": {
      "knownPropertyList": [
        {
          "name": "string",
          "type": "STRING",
          "displayName": "string",
          "group": "EVERYWAN",
          "groupLabel": "string"
        }
      ]
    }
  }
```


Get All Used Properties on a Device

URL: https://:/xenmobile/api/v1/device/usedProperties

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceUsedPropertiesList": {
    "deviceUsedProperties": {
      "deviceUsedPropertiesParameters": [
        {
          "name": "string",
          "type": "STRING",
          "displayName": "string"
        }
      ]
    }
  }
}
```

Get All Device Properties by Device ID

URL: https://:/xenmobile/api/v1/device/properties/{geräte-ID}

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN


```
{
  "status": 0,
  "message": "string",
  "devicePropertiesList": {
    "deviceProperties": {
      "startIndex": 0,
      "devicePropertyParameters": [
        {
          "name": "string",
          "value": "string",
          "id": 0,
          "displayName": "string",
          "group": "string",
          "b64": true
        }
      ],
```



```
    "totalCount": 0
  }
 }
}
```

Update All Device Properties by Device ID

URL: https://:/xenmobile/api/v1/device/properties/{geräte-ID}

Anforderungstyp: PUT

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
{
  "properties": [
    {
      "name": "ACTIVE_ITUNES",
      "value": "0"
    }
  ]
}
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string"
}
```

Add or Update a Device Property by Device ID

URL: https://:/xenmobile/api/v1/device/properties/{geräte-ID}

Anforderungstyp: POST

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielanforderung KOPIEREN

```
{
  "name": "PROPERTY_NAME",
  "value": "PROPERTY_VALUE"
}
```

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string"
}
```

Delete a Device Property by Device ID

URL: https://:/xenmobile/api/v1/device/properties/{geräte-ID}

Anforderungstyp: DELETE

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string"
}
```

Get iOS Device MDM Status by Device ID

URL: https://:/xenmobile/api/v1/device/mdmStatus/{geräte-ID}

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "deviceMdmStatus": {
    "deviceMdmStatusParameters": {
      "pushState": "ENQUEUED",
      "lastPushDate": 0,
      "lastRepliedNotification": 0,
      "lastSentNotification": 0,
      "pushStateLabel": "string"
    }
  }
}
```

Generate PIN Code

URL: https://:/xenmobile/api/v1/device/pincode/generate

Abfrageparameter: pinCodeLength: Länge des angeforderten PIN-Codes

Anforderungstyp: GET

Anforderungsheader: auth_token (bei der Anmeldung generiertes Authentifizierungstoken)

Inhaltstyp: application/json

Beispielantwort KOPIEREN

```
{
  "status": 0,
  "message": "string",
  "pinCode": {
    "answer": "string"
  }
}
```

XenMobile SOAP APIs

Aug 22, 2016

Sie können in XenMobile für die Mobilgeräteverwaltung die folgenden SOAP-Webdienst-APIs verwenden. APIs und SDKs für XenMobile können Sie von der XenMobile Developer Community-Website herunterladen.

WSDL-Name (Web Service Definition Language)	Aufruf
EveryWanDevice	addDevice
	addDevice
	authenticateUser
	authorize
	canCreateUser
	clearDeploymentHisto
	corporateDataWipeDevice
	createUser
	deploy
	deviceExists
	disableTrackingDevice
	enableTrackingDevice
	findDeviceByUdid
	getAllDevices
	getDeploymentHisto
	getDeploymentHisto

getDeviceInfo

getDeviceInformationForUser

getDeviceProperties

getLastUser

getManagedStatus

getMasterKeyList

getSoftwareInventory

getStrongID

getUserDevices

isEnforceSSL

isEnforceStrongAuthentication

locateDevice

lockDevice

putDeviceProperties

registerDeviceForUser

removeDevice

resetDeploymentState

revoke

unlockDevice

wipeDevice

	addDevice
CiscoISE/NAC	action/pinlock
	/mdminfo
	/devices/0/all
	/devices/0/macaddress/
	/batchdevices/0/macaddress/all
OTPServices	browseOtp
	createOtp
	getAvailableEnrollmentModes
	getOtpInfo
	revokeOtp
	triggerNotification

XenMobile Mail Manager 10

Oct 13, 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.

Zum Herunterladen von XenMobile Mail Manager navigieren Sie auf Citrix.com zum Abschnitt "Server Components" unter XenMobile 10 Server.

Neue Features in XenMobile Mail Manager 10.1

Zugriffsregeln

Im Fenster "Rule Analysis" ist ein Kontrollkästchen, bei dessen Aktivierung nur die Regeln angezeigt werden, die Konflikte, Überschreibungen, Redundanzen oder Ergänzungen sind.

Standardzugriff (Allow, Block oder Unchanged) und ActiveSync-Befehlsmodi (PowerShell oder Simulation) werden für jede in der XenMobile-Bereitstellung konfigurierte Microsoft Exchange-Umgebung separat festgelegt.

Snapshots

Sie können die maximale Anzahl Snapshots konfigurieren, die im Snapshotverlauf angezeigt wird.

Sie können zudem konfigurieren, welche Fehler bei einem größeren Snapshot ignoriert werden. Wenn bei einem größeren Snapshot Fehler zurückgegeben werden, die nicht als ignorierbar konfiguriert sind, werden die Ergebnisse des Snapshots verworfen.

Um Fehler als ignorierbar zu konfigurieren, bearbeiten Sie die Datei config.xml in einem XML-Editor:

- Wenn der Exchange Server Office 365 ist, navigieren Sie zum Knoten /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors und fügen Sie den Text, der mit dem untergeordneten Element übereinstimmen soll, im gleichen Format hinzu wie das vorhandene untergeordnete Fehlerelement. Reguläre Ausdrücke werden unterstützt.
- Wenn der Exchange Server ein lokaler Server ist, navigieren Sie zum Knoten /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors und fügen Sie den Text, der mit dem untergeordneten Element übereinstimmen soll, im gleichen Format hinzu wie das vorhandene untergeordnete Fehlerelement. Reguläre Ausdrücke werden unterstützt.
- Wenn mehr als eine Exchange-Umgebung konfiguriert ist, navigieren Sie zum Knoten /ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='ID, die mit der gewünschten Exchange-Umgebung übereinstimmt']/ExchangeServer/Specialists/PowerShell. Fügen Sie dem PowerShell-Knoten einen untergeordneten Knoten "IgnorableErrors" hinzu und fügen Sie für jeden zu ignorierenden Fehler dem Knoten "IgnorableErrors" einen untergeordneten Fehlerknoten hinzu, wobei Sie den entsprechenden Text in einem CDATA-Abschnitt speichern. Reguläre Ausdrücke werden unterstützt.

Speichern Sie die Datei config.xml und starten Sie den XenMobile Mail Manager-Dienst neu.

PowerShell und Exchange

Basierend auf der verbundenen Exchange-Version bestimmt XenMobile Mail Manager nun dynamisch, welche Cmdlets verwendet werden. Beispielsweise wird für Exchange 2010 Get-ActiveSyncDevice verwendet, während für Exchange 2013 und Exchange 2016 Get-MobileDevice verwendet wird.

Exchange-Konfiguration

Exchange Server-Konfigurationen können bearbeitet und aktualisiert werden, ohne dass der XenMobile Mail Manager-Dienst neu gestartet werden muss.

Zwei neue Spalten auf der Registerkarte mit der Exchange-Umgebungsübersicht zeigen die Befehlsmodi der Umgebungen an (PowerShell oder Simulation) sowie den Zugriffsmodus (Allow, Block oder Unchanged).

Problembehandlung und Diagnose

PowerShell-Dienstprogramme zur Problembehandlung sind im Order Support\PowerShell verfügbar.

Beim Konnektivitätstest mit dem Exchange-Dienst, den Sie mit der Schaltfläche "Test Connectivity" im Konfigurationsfenster der Konsole starten, werden alle schreibgeschützten Cmdlets ausgeführt, die der Dienst verwendet. Darüber hinaus werden für den konfigurierten Benutzer RBAC-Berechtigungstests auf dem Exchange Server ausgeführt und alle Fehler und Warnungen werden farbkodiert (blau-gelb für Warnungen, rot-orange für Fehler) angezeigt.

Ein neues Problembehandlungstool führt eine detaillierte RBAC-Analyse von Benutzern sowie tief gehende Analysen der Postfächer und Geräte von Benutzern aus, um Fehlerzustände und potenzielle Fehlerbereiche zu erkennen. Alle Cmdlets können in eine Textdatei ausgegeben und gespeichert werden.

In Supportszenarios können durch das Aktivieren eines Diagnosekontrollkästchens in der Konsole die Eigenschaften aller Postfächer auf allen Geräten, die von XenMobile Mail Manager verwaltet werden, gespeichert werden.

In Supportszenarios wird nun die Protokollierung auf Ablaufverfolgungsebene unterstützt.

Authentifizierung

XenMobile Mail Manager unterstützt die Basic-Authentifizierung für lokale Bereitstellungen. So kann XenMobile Mail Manager auch verwendet werden, wenn der XenMobile Mail Manager-Server kein Mitglied der Domäne des Exchange-Servers ist.

Behobene Probleme

Zugriffsregeln

XenMobile Mail Manager wendet lokale Zugriffssteuerungsregeln auf alle Benutzer in Active Directory (AD)-Gruppen an, sogar wenn eine AD-Gruppe über 1000 Benutzer umfasst. In früheren Versionen wendete XenMobile Mail Manager lokale Zugriffssteuerungsregeln nur auf die ersten 1000 Benutzer einer AD-Gruppe an. [#548705]

Die XenMobile Mail Manager-Konsole reagierte gelegentlich nicht, wenn Active Directory-Gruppen mit 1000 oder mehr Benutzern abgefragt wurden. [CXM-11729]

Das LDAP-Konfigurationsfenster zeigt keinen falschen Authentifizierungsmodus mehr an. [CXM-5556]

Snapshots

Benutzernamen mit Apostrophen verursachen keine Fehler bei kleineren Snapshots mehr. [#617549]

In Supportszenarios, in denen Pipelining deaktiviert ist (im Konfigurationsfenster der XenMobile Mail Manager-Konsole ist die Option "Disable Pipelining" aktiviert), schlagen größere Snapshots in lokalen Exchange-Umgebungen nicht mehr fehl. [#586083]

In Supportszenarios, in denen Pipelining deaktiviert ist (im Konfigurationsfenster der XenMobile Mail Manager-Konsole ist die Option "Disable Pipelining" aktiviert), werden Daten für tiefe Snapshots nicht mehr unabhängig davon gesammelt, ob die Umgebung für tiefe oder flache Snapshots konfiguriert wurde. Daten für tiefe Snapshots werden nur gesammelt, wenn die Umgebung für tiefe Snapshots konfiguriert wurde. [#586092]

Beim ersten größeren Snapshot nach der Erstinstallation trat gelegentlich ein Fehler auf, der verhinderte, dass XenMobile Mail Manager

einen weiteren größeren Snapshot ausführen konnte, bis der XenMobile Mail Manager-Dienst neu gestartet wurde. Dieser Fehler tritt nicht mehr auf. [CXM-5536]

Info über XenMobile Mail Manager 10

Info über XenMobile Mail Manager 10.1

Oct 13, 2016

Die folgenden Features sind neu in XenMobile Mail Manager 10.1:

Zugriffsregeln

Im Fenster "Rule Analysis" ist ein Kontrollkästchen, bei dessen Aktivierung nur die Regeln angezeigt werden, die Konflikte, Überschreibungen, Redundanzen oder Ergänzungen sind.

Standardzugriff (Allow, Block oder Unchanged) und ActiveSync-Befehlsmodi (PowerShell oder Simulation) werden für jede in der XenMobile-Bereitstellung konfigurierte Microsoft Exchange-Umgebung separat festgelegt.

Snapshots

Sie können die maximale Anzahl Snapshots konfigurieren, die im Snapshotverlauf angezeigt wird.

Sie können zudem konfigurieren, welche Fehler bei einem größeren Snapshot ignoriert werden. Wenn bei einem größeren Snapshot Fehler zurückgegeben werden, die nicht als ignorierbar konfiguriert sind, werden die Ergebnisse des Snapshots verworfen.

Um Fehler als ignorierbar zu konfigurieren, bearbeiten Sie die Datei config.xml in einem XML-Editor:

- Wenn der Exchange Server Office 365 ist, navigieren Sie zum Knoten /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors und fügen Sie den Text, der mit dem untergeordneten Element übereinstimmen soll, im gleichen Format hinzu wie das vorhandene untergeordnete Fehlerelement. Reguläre Ausdrücke werden unterstützt. Fahren Sie mit Schritt 7 fort.
- Wenn der Exchange Server ein lokaler Server ist, navigieren Sie zum Knoten /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors und fügen Sie den Text, der mit dem untergeordneten Element übereinstimmen soll, im gleichen Format hinzu wie das vorhandene untergeordnete Fehlerelement. Reguläre Ausdrücke werden unterstützt. Fahren Sie mit Schritt 7 fort.
- Wenn mehr als eine Exchange-Umgebung konfiguriert ist, navigieren Sie zum Knoten /ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='ID, die mit der gewünschten Exchange-Umgebung übereinstimmt']/ExchangeServer/Specialists/PowerShell. Fügen Sie dem PowerShell-Knoten einen untergeordneten Knoten namens "IgnorableErrors" hinzu und fügen Sie für jeden Fehler, der ignoriert werden soll, dem Knoten "IgnorableErrors" einen untergeordneten Fehlerknoten hinzu, der den übereinstimmenden Text in einem CDATA-Bereich enthält. Reguläre Ausdrücke werden unterstützt.

Speichern Sie die Datei config.xml und starten Sie den XenMobile Mail Manager-Dienst neu.

PowerShell und Exchange

Basierend auf der verbundenen Exchange-Version bestimmt XenMobile Mail Manager nun dynamisch, welche Cmdlets verwendet werden. Beispielsweise wird für Exchange 2010 **Get-ActiveSyncDevice** verwendet, während für Exchange 2013 und Exchange 2016 **Get-MobileDevice** verwendet wird.

Exchange-Konfiguration

Exchange Server-Konfigurationen können bearbeitet und aktualisiert werden, ohne dass der XenMobile Mail Manager-Dienst neu gestartet werden muss.

Zwei neue Spalten auf der Registerkarte mit der Exchange-Umgebungsübersicht zeigen die Befehlsmodi der Umgebungen an (PowerShell oder Simulation) sowie den Zugriffsmodus (Allow, Block oder Unchanged).

Problembehandlung und Diagnose

PowerShell-Dienstprogramme zur Problembehandlung sind im Order Support\PowerShell verfügbar.

Beim Konnektivitätstest mit dem Exchange-Dienst, den Sie mit der Schaltfläche **Test Connectivity** im Konfigurationsfenster der Konsole starten, werden alle schreibgeschützten Cmdlets ausgeführt, die der Dienst verwendet. Darüber hinaus werden für den konfigurierten Benutzer RBAC-Berechtigungstests auf dem Exchange Server ausgeführt und alle Fehler und Warnungen werden farbkodiert (blau-gelb für Warnungen, rot-orange für Fehler) angezeigt.

Ein neues Problembehandlungstool führt eine detaillierte RBAC-Analyse von Benutzern sowie tief gehende Analysen der Postfächer und Geräte von Benutzern aus, um Fehlerzustände und potenzielle Fehlerbereiche zu erkennen. Alle Cmdlets können in eine Textdatei ausgegeben und gespeichert werden.

In Supportszenarios können durch das Aktivieren eines Diagnosekontrollkästchens in der Konsole die Eigenschaften aller Postfächer auf allen Geräten, die von XenMobile Mail Manager verwaltet werden, gespeichert werden.

In Supportszenarios wird nun die Protokollierung auf Ablaufverfolgungsebene unterstützt.

Authentifizierung

XenMobile Mail Manager unterstützt die Basic-Authentifizierung für lokale Bereitstellungen. So kann XenMobile Mail Manager auch verwendet werden, wenn der XenMobile Mail Manager-Server kein Mitglied der Domäne des Exchange-Servers ist.

Behobene Probleme

Zugriffsregeln

XenMobile Mail Manager wendet lokale Zugriffssteuerungsregeln auf alle Benutzer in Active Directory-Gruppen an, sogar wenn eine Active Directory-Gruppe über 1.000 Benutzer umfasst. In früheren Versionen wendete XenMobile Mail Manager lokale Zugriffssteuerungsregeln nur auf die ersten 1.000 Benutzer einer Active Directory-Gruppe an. [#548705]

Die XenMobile Mail Manager-Konsole reagierte gelegentlich nicht, wenn Active Directory-Gruppen mit 1.000 oder mehr Benutzern abgefragt wurden. [CXM-11729]

Das LDAP-Konfigurationsfenster zeigt keinen falschen Authentifizierungsmodus mehr an. [CXM-5556]

Snapshots

Benutzernamen mit Apostrophen verursachen keine Fehler bei kleineren Snapshots mehr. [#617549]

In Supportszenarios, in denen Pipelining deaktiviert ist (im Konfigurationsfenster der XenMobile Mail Manager-Konsole ist die Option **Disable Pipelining** aktiviert), schlagen größere Snapshots in lokalen Exchange-Umgebungen nicht mehr fehl. [#586083]

In Supportszenarios, in denen Pipelining deaktiviert ist (im Konfigurationsfenster der XenMobile Mail Manager-Konsole ist die Option **Disable Pipelining** aktiviert), werden Daten für tiefe Snapshots nicht mehr unabhängig davon gesammelt, ob die Umgebung für tiefe oder flache Snapshots konfiguriert wurde. Daten für tiefe Snapshots werden nur gesammelt, wenn die Umgebung für tiefe Snapshots konfiguriert wurde. [#586092]

Beim ersten größeren Snapshot nach der Erstinstallation trat gelegentlich ein Fehler auf, der verhinderte, dass XenMobile Mail Manager einen weiteren größeren Snapshot ausführen konnte, bis der XenMobile Mail Manager-Dienst neu gestartet wurde. Dieser Fehler tritt nicht mehr auf. [CXM-5536]

Info über XenMobile Mail Manager 10

Oct 13, 2016

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.
- XenMobile Mail Manager wendet möglicherweise lokale Zugriffssteuerungsregeln nur auf die ersten 1000 Benutzer einer Active Directory-Gruppe an, auch wenn die Gruppe über 1000 Benutzer umfasst.

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.

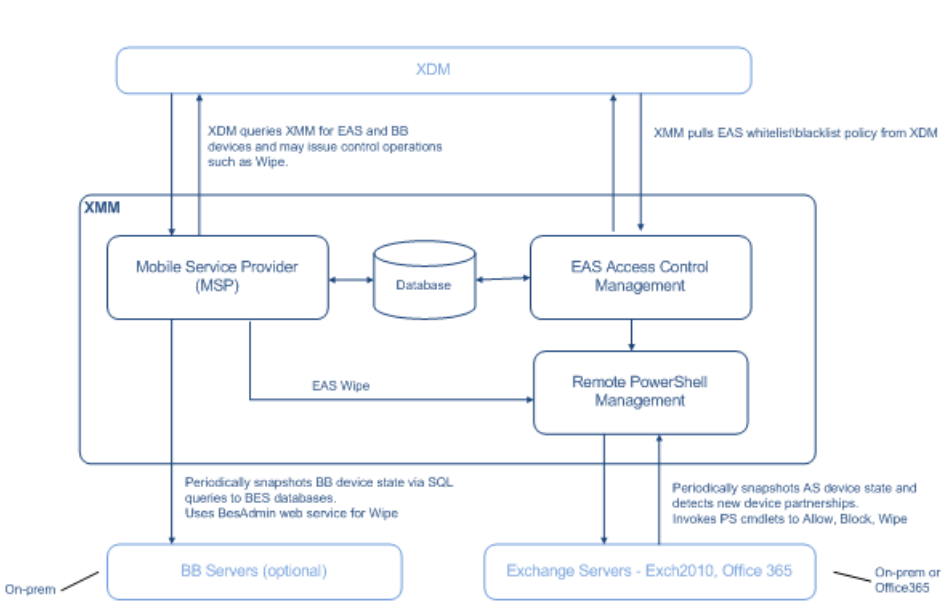
Protokollierung

Von PowerShell zurückgegebene Fehlermeldungen haben jetzt eine GUID. Verwenden Sie diesen Wert, um zu steuern, was auf der Registerkarte mit den Details des Snapshotverlaufs 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.
- Mobilfunkanbieter: 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

Oct 13, 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 2016, 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 2016
- Exchange Server 2013
- Exchange Server 2010 SP2

Voraussetzungen für XenMobile Mail Manager

- Windows Management Framework installiert
  - PowerShell V5, V4 und V3
- 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: Das mit der Konfigurationsbenutzeroberfläche für Exchange festgelegte Konto muss in der Lage sein, eine Verbindung mit Exchange Server herzustellen und vollständigen Zugriff zum Ausführen der folgenden Exchange-spezifischen PowerShell-Cmdlets erhalten:

- **Exchange Server 2010 SP2**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **Exchange Server 2013 und Exchange Server 2016**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment

- 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 Microsoft TechNet-Artikel über Remoteanforderungen müssen die Anmeldeinformationen zum Herstellen einer Remoteverbindung und Ausführen von Remotebefehlen einem Benutzer entsprechen, der auf dem Remotecomputer Administratorrechte hat. Gemäß dem folgenden Blogbeitrag müssen Sie kein Administrator sein, um Remote-PowerShell-Befehle auszuführen: You Don't Have to Be An Administrator to Run Remote PowerShell Commands, 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**: Das mit der Konfigurationsbenutzeroberfläche für Exchange festgelegte Konto muss 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-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- 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

Oct 13, 2016

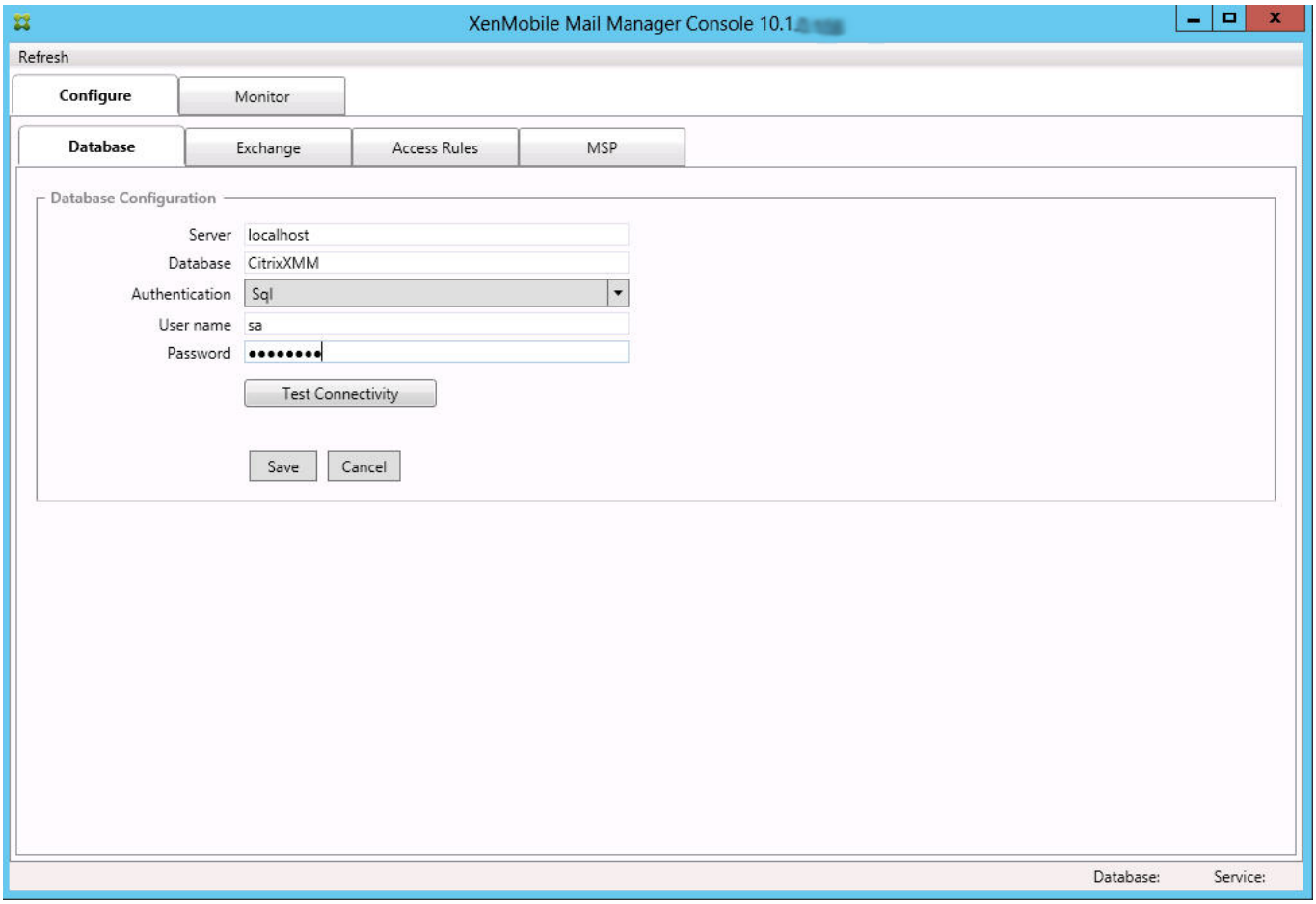
1. Klicken Sie auf die Datei XmmSetup.msi und folgen Sie den Anweisungen des Installers zum Installieren von XenMobile Mail Manager.

2. Lassen Sie die Option zum Starten des Hilfsprogramms für die Konfiguration im letzten Bildschirm des Setupassistenten ausgewählt. Oder öffnen Sie **XenMobile Mail Manager** über das Startmenü.

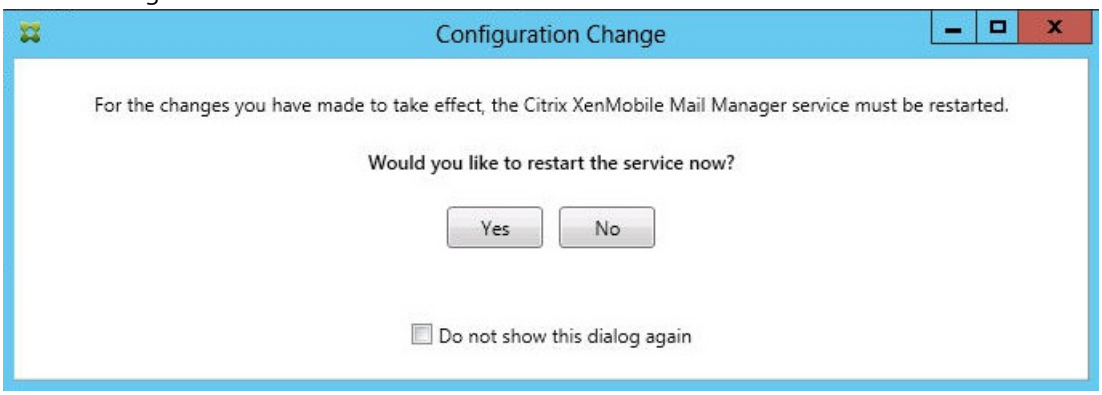
3. Konfigurieren Sie die folgenden Datenbankeigenschaften:
   1. Wählen Sie die Registerkarte **Configure** > **Database**.
   2. Geben Sie den Namen des SQL Server-Computers ein (standardmäßig "localhost").
   3. Behalten Sie den Standarddatenbanknamen "CitrixXmm" bei.
   4. Wählen Sie einen der folgenden 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.

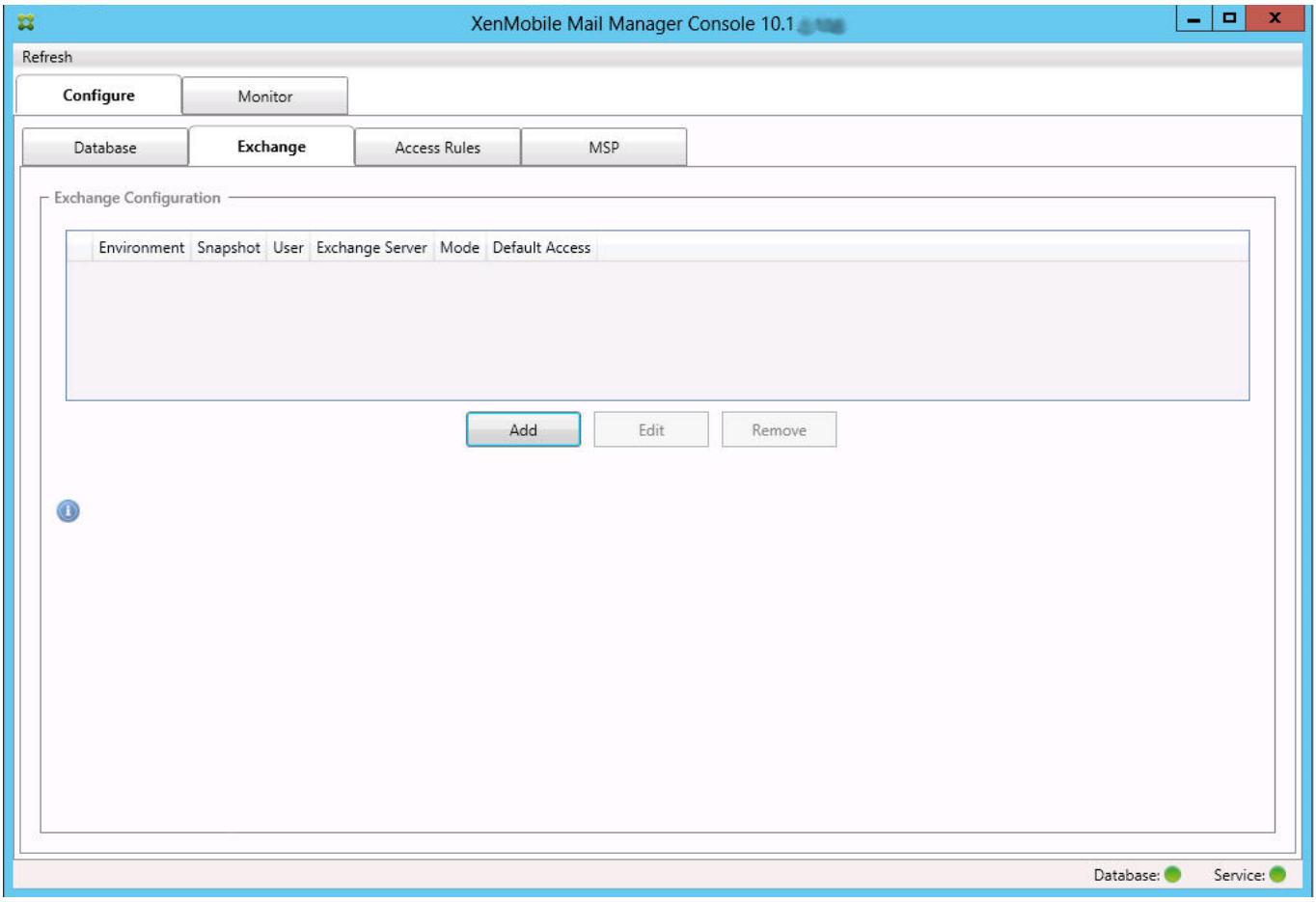
5. Klicken Sie auf **Test Connectivity**, um zu prüfen, ob eine Verbindung mit dem SQL Server hergestellt werden kann, und klicken Sie auf **Save**.



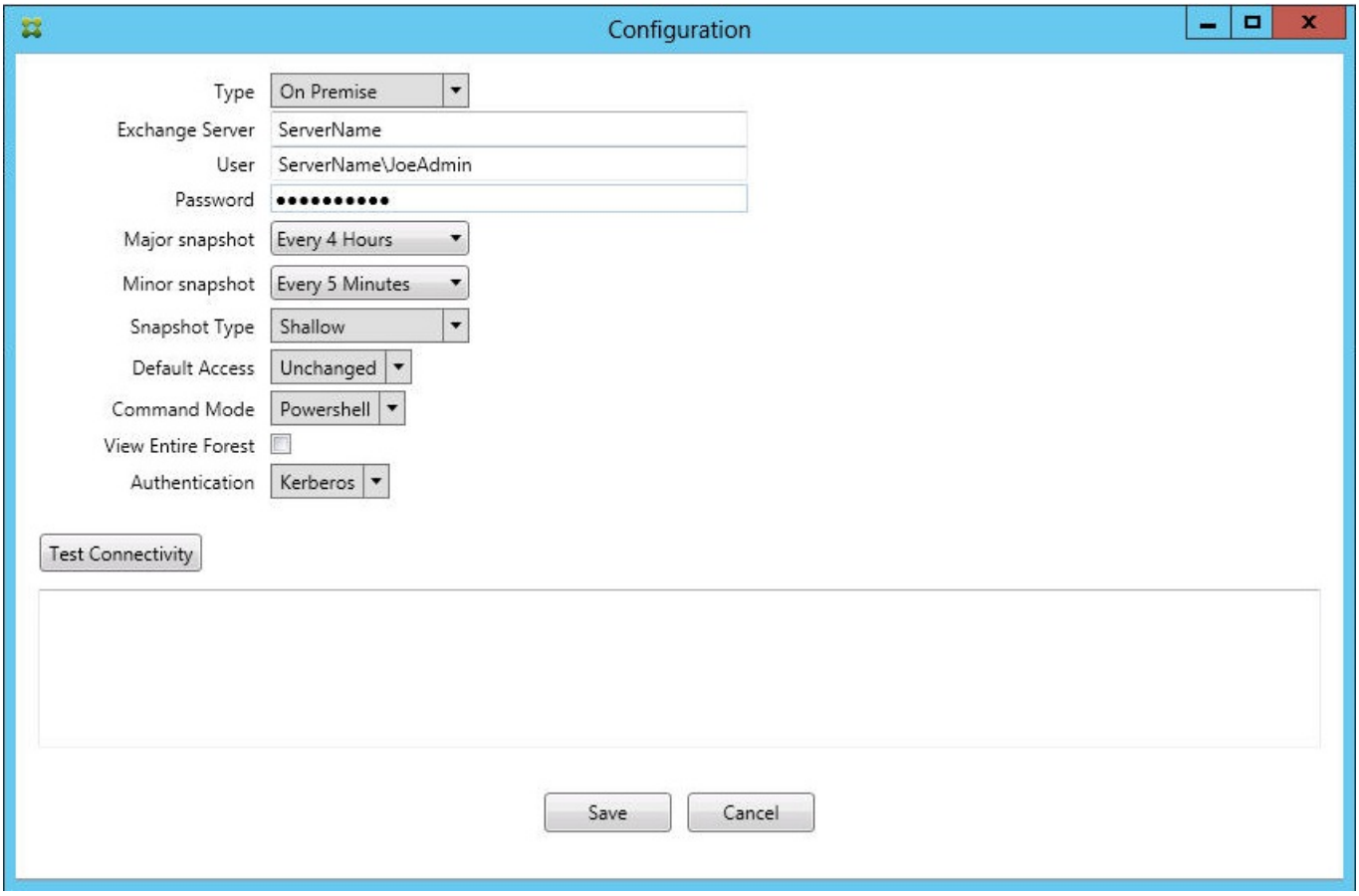
4. Eine Meldung fordert Sie zum Neustarten des Diensts auf. Klicken Sie auf **Yes**.



5. Konfigurieren Sie mindestens einen 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**.



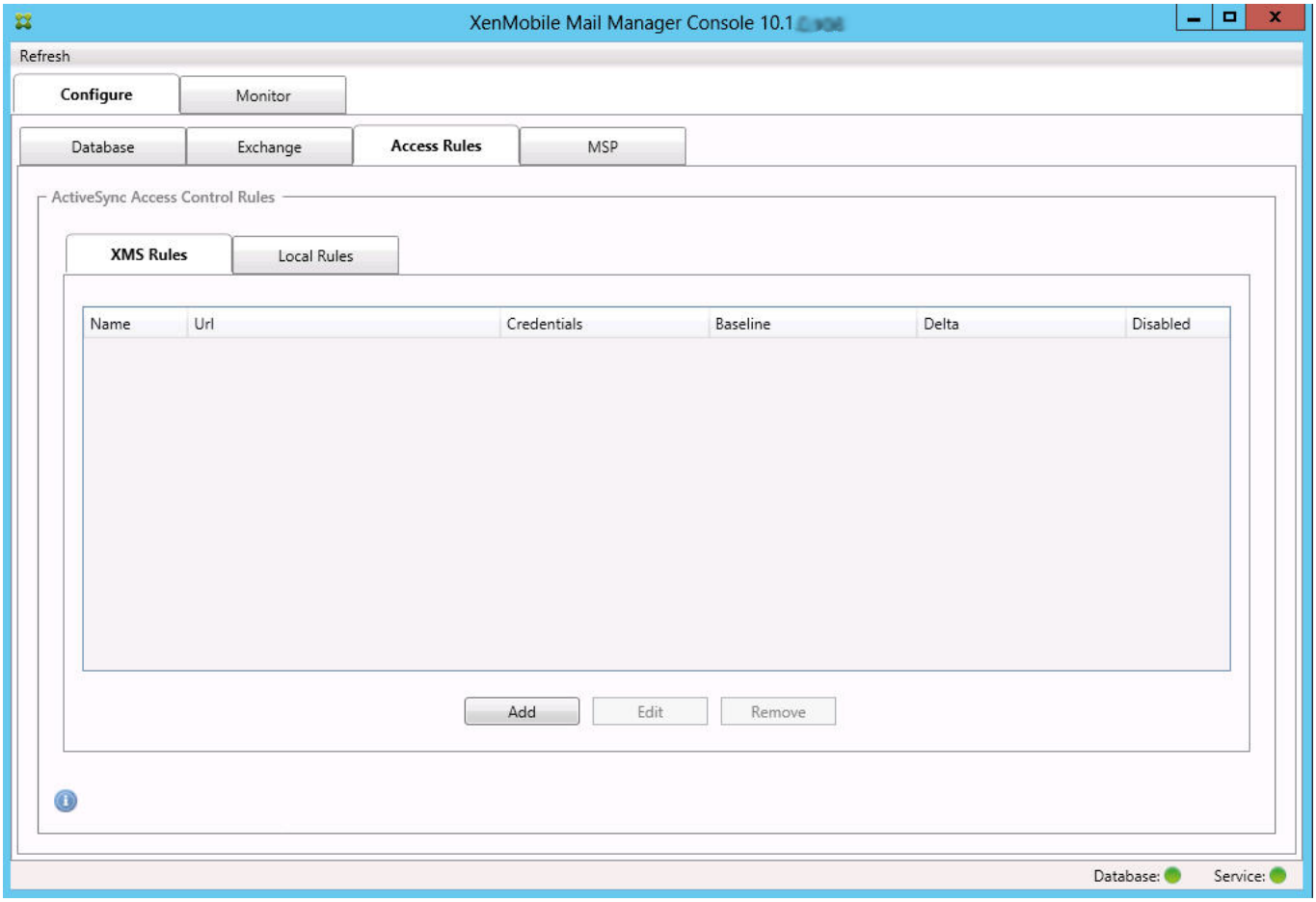
3. Klicken Sie auf **Add**.
4. Wählen Sie den Typ der Exchange Server-Umgebung aus: entweder **On Premise** oder **Office 365**.



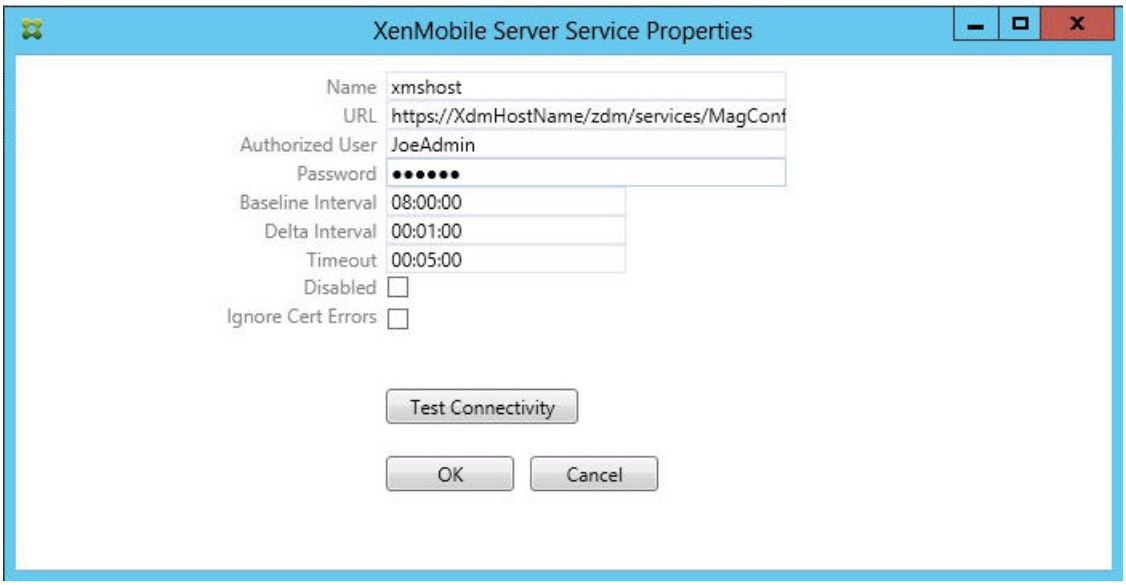
5. Wenn Sie **On Premise** auswählen, geben Sie den Namen des für Remote-PowerShell-Befehle verwendeten Exchange Servers ein.
6. Geben Sie den Benutzernamen einer Windows-Identität ein, die die unter "Anforderungen" aufgeführten Berechtigungen auf dem Exchange Server-Computer hat.
7. Geben Sie für **Password** 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. 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.
12. 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.

13. Wählen Sie **View Entire Forest**, damit XenMobile Mail Manager die gesamte Active Directory-Struktur in der Exchange-Umgebung anzeigt.
14. Wählen Sie das Authentifizierungsprotokoll: **Kerberos** oder **Basic**. XenMobile Mail Manager unterstützt die Basic-Authentifizierung für lokale Bereitstellungen. So kann XenMobile Mail Manager auch verwendet werden, wenn der XenMobile Mail Manager-Server kein Mitglied der Domäne des Exchange-Servers ist.
15. Klicken Sie auf **Test Connectivity**, um zu prüfen, ob eine Verbindung mit dem Exchange Server hergestellt werden kann, und klicken Sie auf **Save**.
16. Eine Meldung fordert Sie zum Neustarten des Diensts auf. Klicken Sie auf **Yes**.

6. Konfigurieren Sie die Zugriffsregeln:
    1. Wählen Sie die Registerkarten **Configure** > **Access Rules**.
    2. Klicken Sie auf die Registerkarte **XDM Rules**.

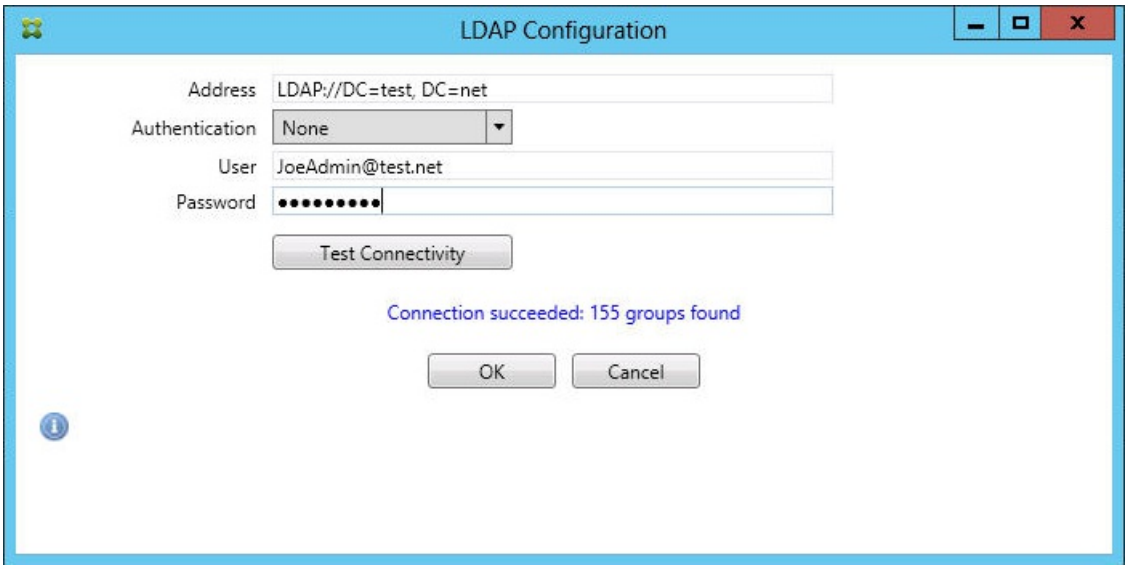


3. Klicken Sie auf **Add**.



4. Geben Sie einen Namen für die XenMobile-Serverregeln ein, z. B. "XdmHost".
5. 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.
6. Geben Sie einen auf dem Server berechtigten Benutzer an.
7. Geben Sie das Kennwort des Benutzers ein.
8. Behalten Sie die Standardwerte für **Baseline Interval**, **Delta Interval** und **Timeout values** bei.
9. 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.
10. Klicken Sie auf **OK**.

7. 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.

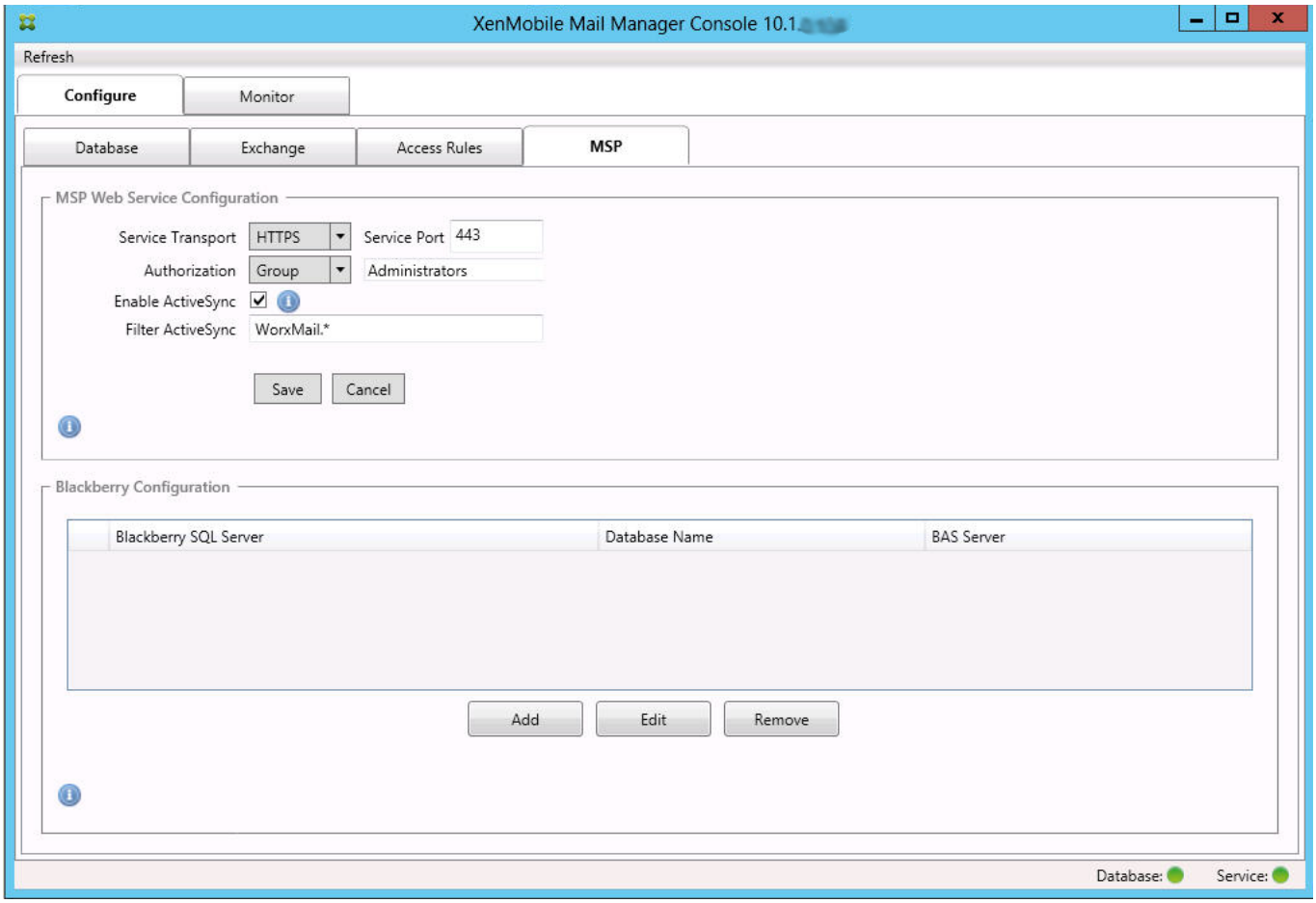


   2. Sie können lokale Regeln basierend auf den Parametern **ActiveSync Device ID**, **Device Type**, **AD Group**, **User** oder **UserAgent** hinzufügen. Wählen Sie in der Liste den geeigneten Schlüssel aus. Weitere Informationen finden Sie unter

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 **Save**.

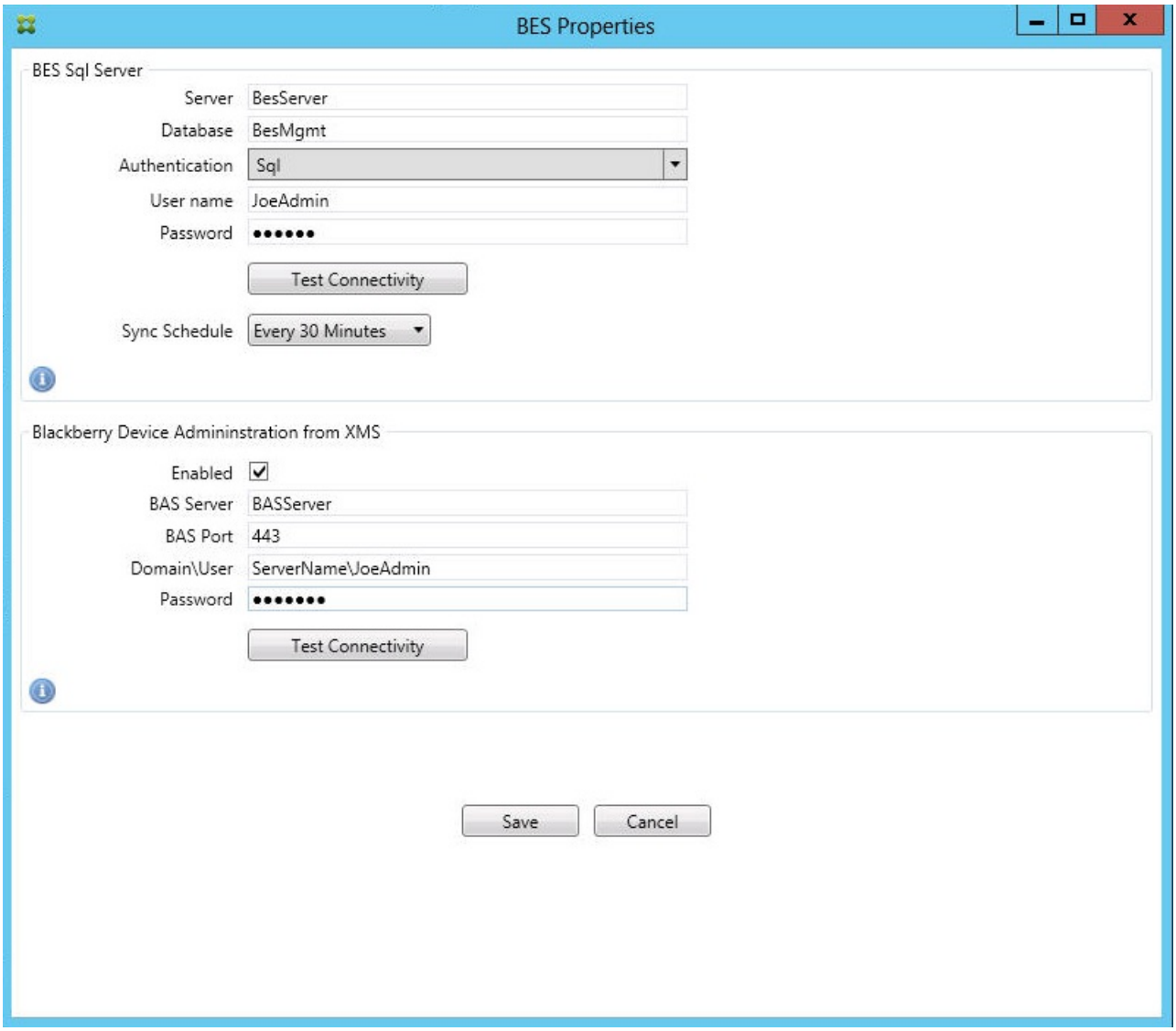
8. Konfigurieren des Mobile Service Provider-Diensts
   Hinweis: Der Mobile Service Provider-Dienst ist optional und nur erforderlich, wenn auch XenMobile für die Verwendung der Mobile Service Provider-Schnittstelle zum Abfragen nicht verwalteter Geräte konfiguriert ist.
   1. Wählen Sie die Registerkarte **Configure** > **MSP**.



   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 zu einer starken Leistungsminderung beim Erstellen von Snapshots führen 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 **Save**.

9. 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.

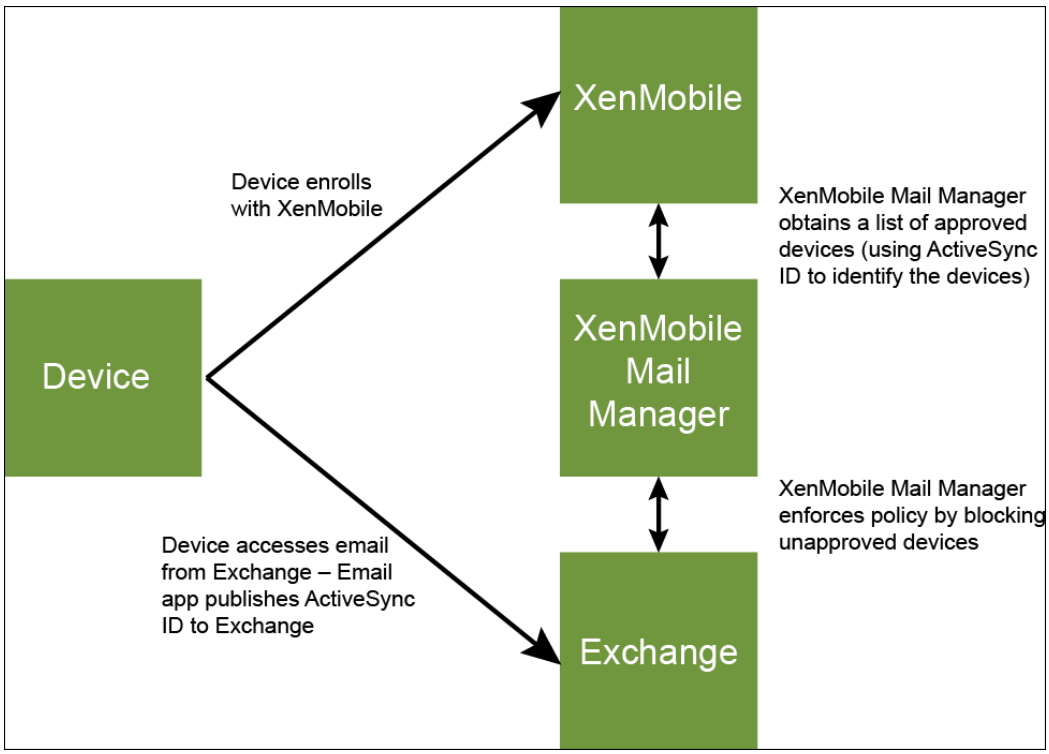
5. Wenn Sie **SQL authentication** auswählen, geben Sie Benutzernamen und Kennwort ein.
6. Legen Sie den Parameter **Sync Schedule** fest. Nach diesem Zeitplan erfolgt eine regelmäßige Verbindung mit dem BES SQL-Server zur Prüfung auf Aktualisierungen an Geräten.
7. Klicken Sie auf **Test Connectivity**, 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 **Save**.

Erzwingen von E-Mail-Richtlinien mit ActiveSync-IDs

Jul 28, 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

Oct 13, 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 durch Klicken auf die Schaltfläche **Cancel** in den Zustand zurückgesetzt werden, den sie beim ersten Öffnen hatte. Wenn Sie nicht auf Schaltfläche **Save** klicken, gehen beim Schließen des Konfigurationstools jegliche Änderungen in diesem Fenster verloren.

XenMobile Mail Manager bietet drei Regeltypen: lokale Regeln, XenMobile-Server-Regeln (auch "XDM-Regeln") und die Standardzugriffsregel.

Lokale Regeln: Diese haben die höchste Priorität, d. h. sobald eine lokale Regel auf einem Gerät zutrifft, wird die Regelauswertung eingestellt. Es werden weder die XenMobile-Server-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.

XenMobile-Server-Regeln: XenMobile-Server-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 XenMobile-Server-Regel zu, wird der gewünschte Zugriffszustand durch die Standardzugriffsregel bestimmt.

- Default Access – Allow: Geräte, auf die weder eine lokale noch eine XenMobile-Server-Regel zutrifft, werden alle zugelassen.
- Default Access – Block: Geräte, auf die weder eine lokale noch eine XenMobile-Server-Regel zutrifft, werden alle blockiert.
- Default Access - Unchanged: Bei Geräten, auf die weder eine lokale noch eine XenMobile-Server-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
- XenMobile-Server-Regeln

Sobald eine Regel zutrifft, wird die Auswertung beendet. Trifft beispielsweise eine lokale Regel auf ein Gerät zu, erfolgt für dieses keine Auswertung der XenMobile-Server-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

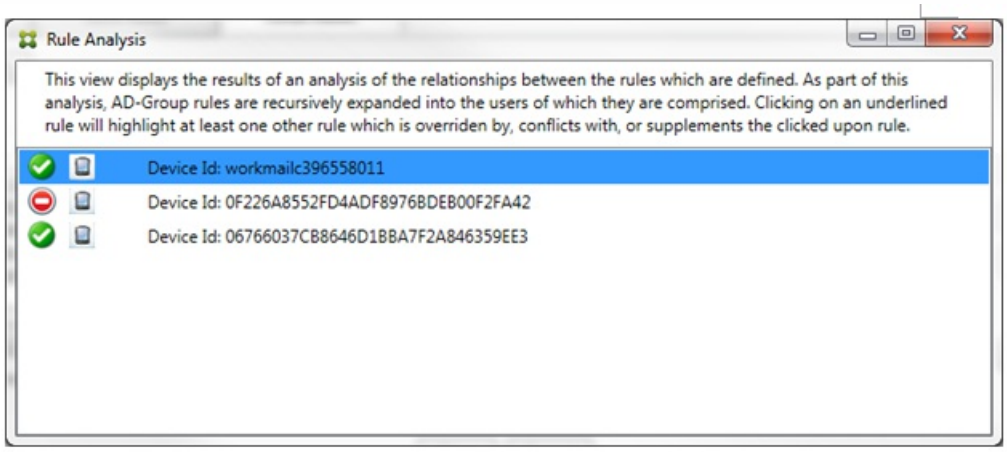
Regel stehen. Ein nach unten weisender Pfeil zeigt an, dass es Nebenregeln gibt, die nach der primären Regel stehen. Es kann immer nur eine primäre Regel aktiv sein.

- **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.

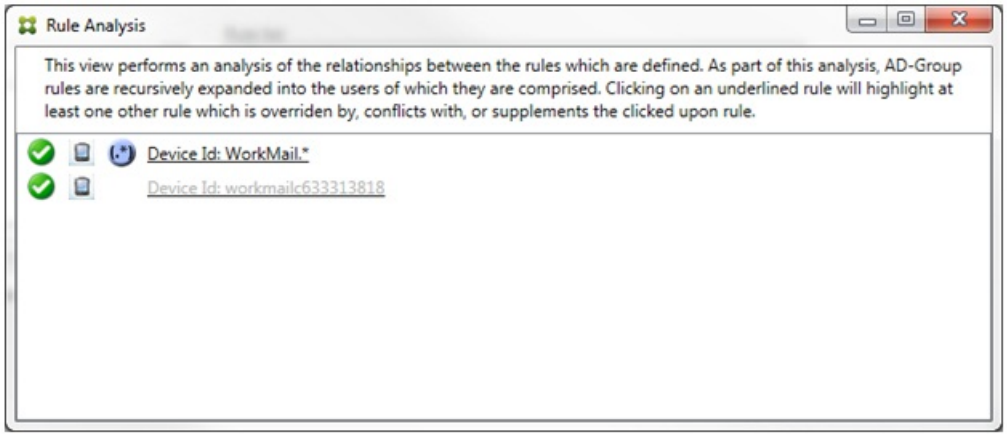
Darstellung des Regeltyps im Dialogfeld zur Regelanalyse

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.

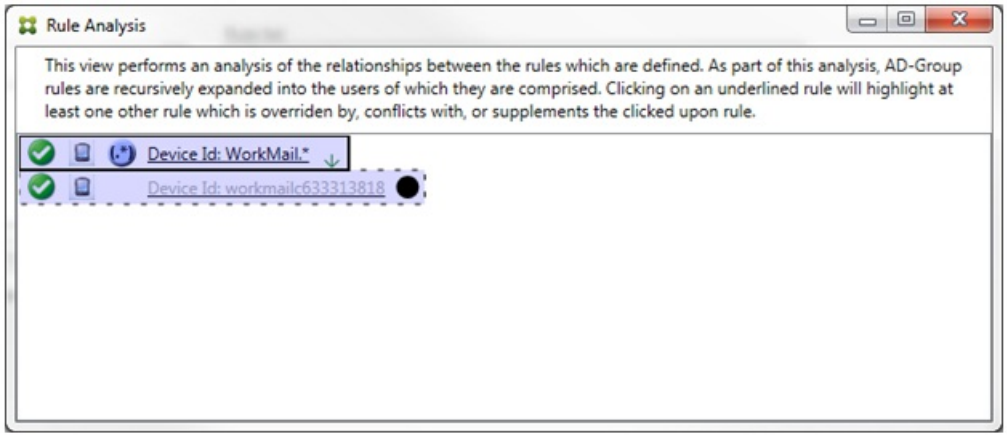
Im Fenster "Rule Analysis" ist ein Kontrollkästchen, bei dessen Aktivierung nur die Regeln angezeigt werden, die Konflikte, Überschreibungen, Redundanzen oder Ergänzungen sind.



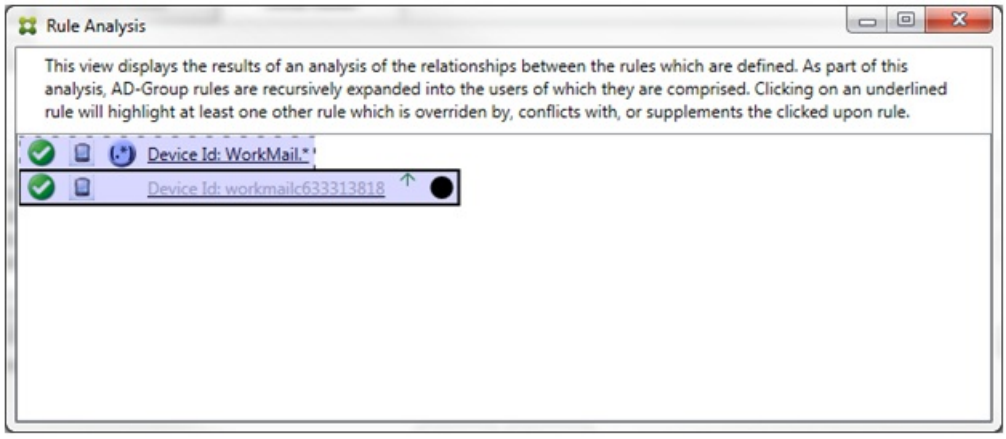
Wenn eine Außerkraftsetzung vorliegt, werden mindestens zwei Regeln unterstrichen dargestellt: die primäre Regel und die Nebenregel(n). Mindestens eine Nebenregel erscheint in einer helleren Schrift, um anzuzeigen, dass sie durch eine höhere Regel außer Kraft gesetzt wird. Sie können auf die außer Kraft 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:

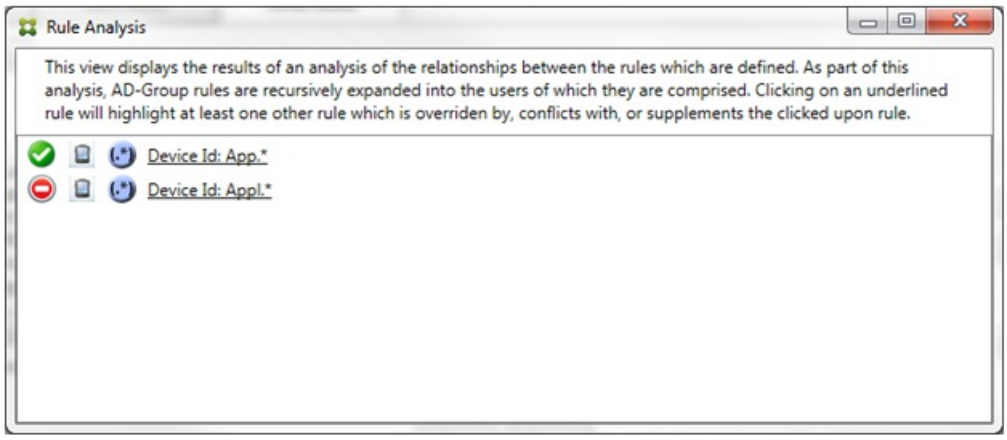


In diesem Beispiel ist die Regel mit regelmäßigen Ausdrücken WorkMail.* die primäre Regel (angezeigt durch den durchgehenden Rahmen) und die normale Regel workmailc633313818 ist eine Nebenregel (angezeigt durch den gestrichelten Rahmen). Der schwarze Punkt neben der Nebenregel weist deutlich darauf hin, 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:

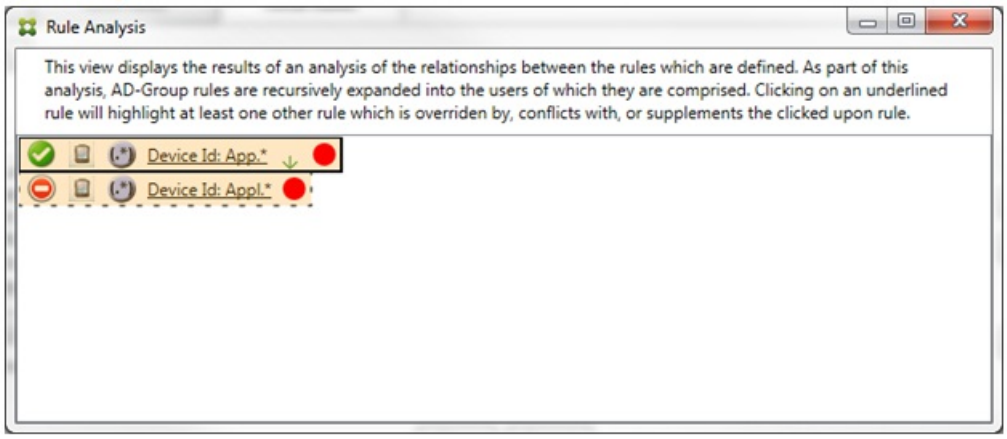


Im vorherigen Beispiel ist die Regel mit regelmäßigen Ausdrücken WorkMail.* die Nebenregel (angezeigt durch den gestrichelten Rahmen) und die normale Regel workmailc633313818 ist eine primäre Regel (angezeigt durch den durchgehenden Rahmen). In diesem einfachen Beispiel ist der Unterschied nicht groß. 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:

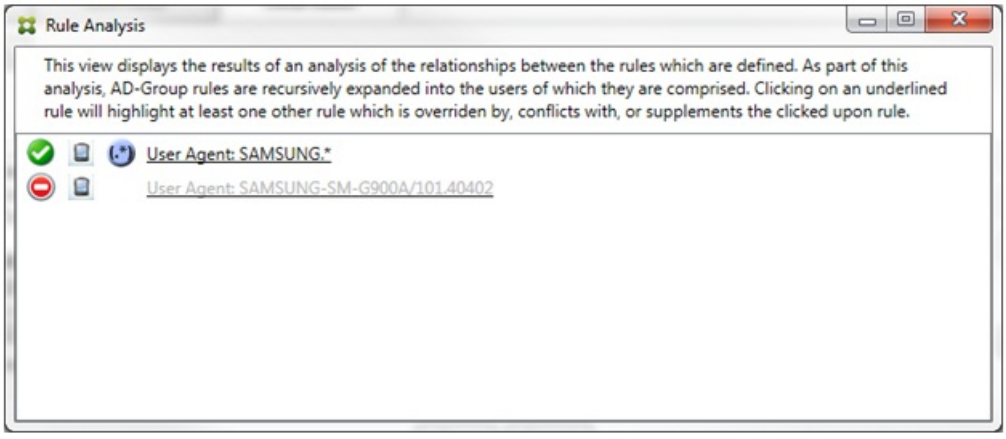


Eine Untersuchung der beiden Regeln mit regelmäßigen Ausdrücken ergibt, dass die erste alle Geräte, deren ID "App" enthält, zulässt und die zweite alle Geräte, deren ID "Appl" enthält, blockiert. Obwohl die zweite Regel alle Geräte, deren ID "Appl" enthält, blockiert, wird kein Gerät, auf das die Regel zutrifft, je blockiert, da die zulassende Regel eine höhere Priorität hat. Nach dem Klicken auf die erste Regel wird das Dialogfeld folgendermaßen angezeigt:



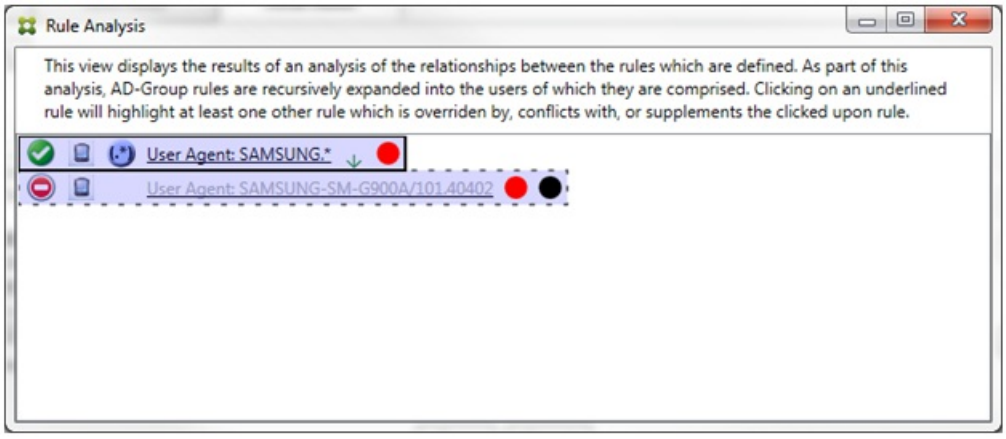
Im vorherigen Szenario wird sowohl die primäre Regel (mit dem regelmäßigen Ausdruck "App.*") und die Nebenregel (mit dem regelmäßigen Ausdruck "Appl.*") gelb markiert angezeigt. Dies ist ein einfacher optischer Warnhinweis auf den Umstand, dass mehrere Regeln mit regelmäßigem Ausdruck für ein einzelnes 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.



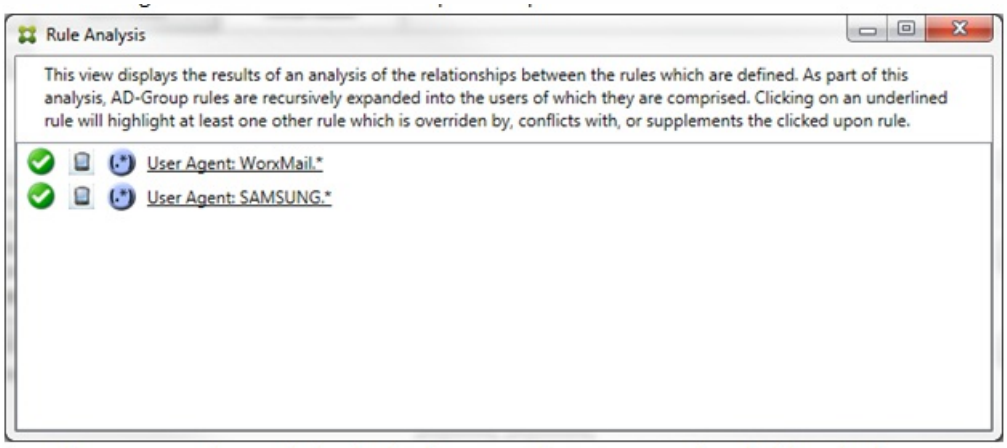
Im vorherigen Beispiel ist leicht zu erkennen, dass die erste Regel (mit dem regelmäßigen Ausdruck SAMSUNG.*) die nächste Regel (normale Regel SAMSUNG-SM-G900A/101.40402) außer Kraft setzt und überdies ein Konflikt beim Zugriffszustand (primäre Regel = Zulassen, Nebenregel = Blockieren) vorliegt. Die 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:

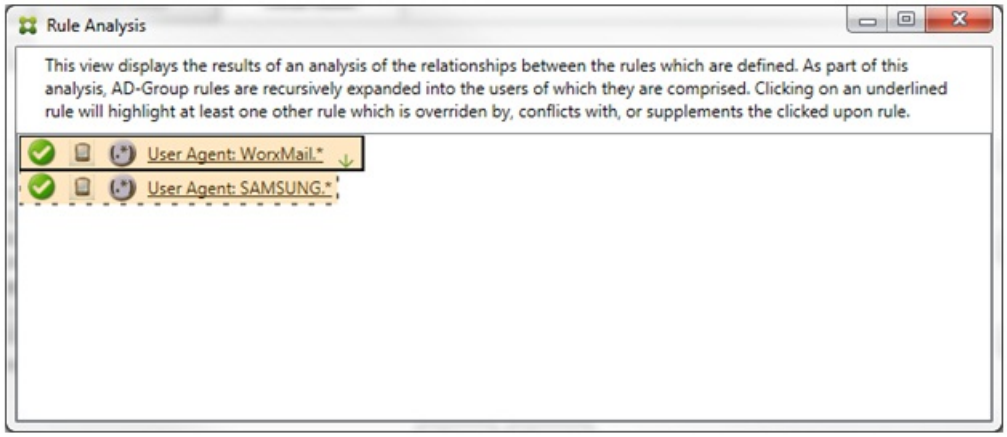


Die primäre Regel (mit dem regelmäßigen Ausdruck SAMSUNG.*) ist mit einem roten Punkt gekennzeichnet, um anzuzeigen, dass ihr Zugriffszustand im Widerspruch mit dem von mindestens einer Nebenregel steht. Die Nebenregel (normale Regel SAMSUNG-SM-G900A/101.40402) ist mit einem roten Punkt gekennzeichnet, 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:



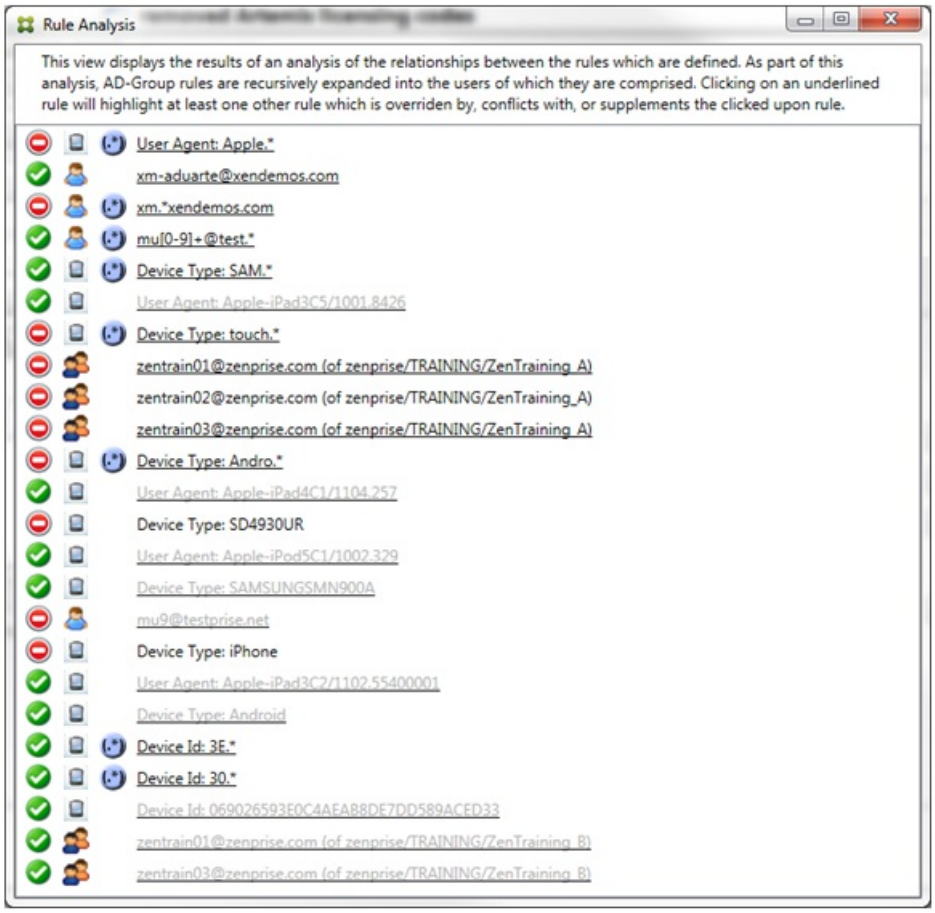
Es ist leicht zu erkennen, dass beide Regeln solche mit regelmäßigen Ausdrücken sind, und beide auf das Feld "ActiveSync device ID" in XenMobile Mail Manager angewendet werden. Nach dem Klicken auf die erste Regel sieht das Dialogfeld folgendermaßen aus:



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

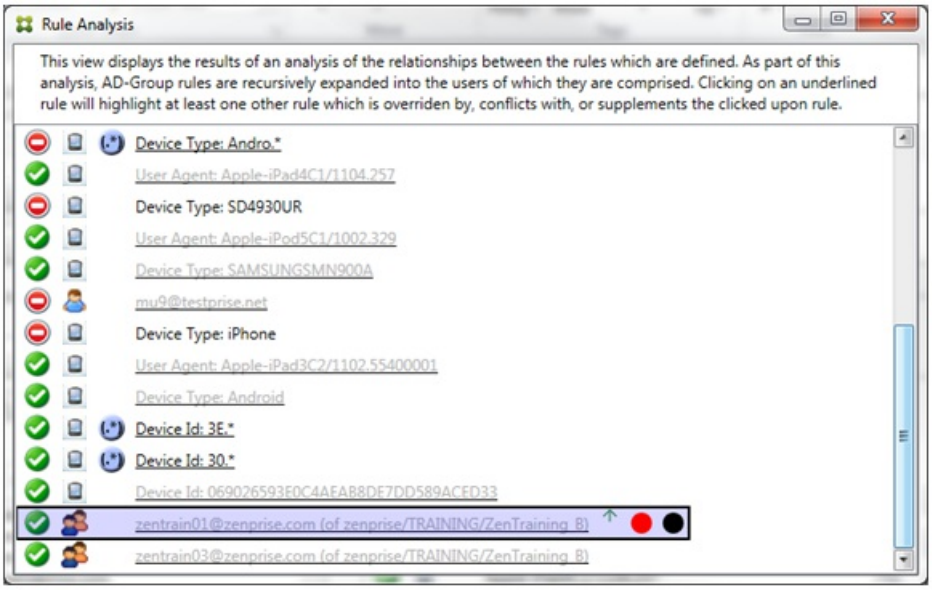
Es sind viele Außerkraftsetzungen, Konflikte oder Ergänzungen möglich, die hier nicht alle mit einem Beispiel vorgestellt werden können. Im Folgenden werden anhand eines Negativbeispiels die immensen Vorzüge des visuellen Konstrukts der Regelanalyse gezeigt. Die meisten Elemente in der folgenden Abbildung 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.

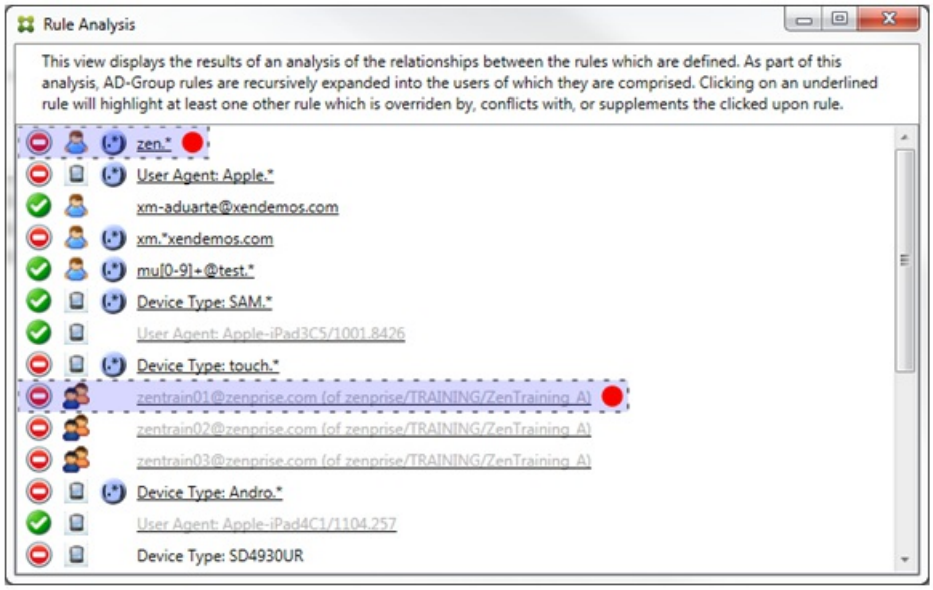
Beispiel 1: In diesem Beispiel wird untersucht, warum zentrain01@zenprise.com außer Kraft gesetzt wurde.



Die primäre Regel (AD-Gruppenregel zenprise/TRAINING/ZenTraining B, bei der zentrain01@zenprise.com Mitglied ist) hat die folgenden Merkmale:

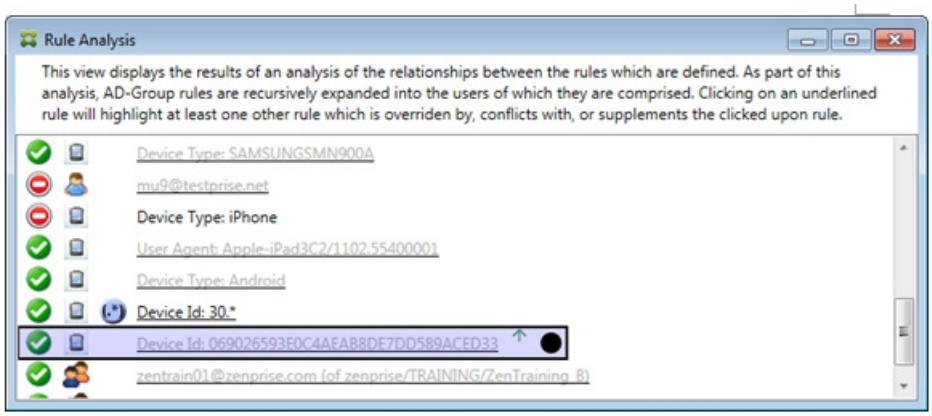
- Sie ist blau unterlegt und wird von einem durchgehenden Rahmen umgeben.
- Sie hat einen nach oben weisenden grünen Pfeil, was anzeigt, dass alle Nebenregeln weiter oben sind.
- Sie ist mit einem roten und einem schwarzen Punkt gekennzeichnet, um anzuzeigen, dass erstens mindestens eine Nebenregel einen 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:



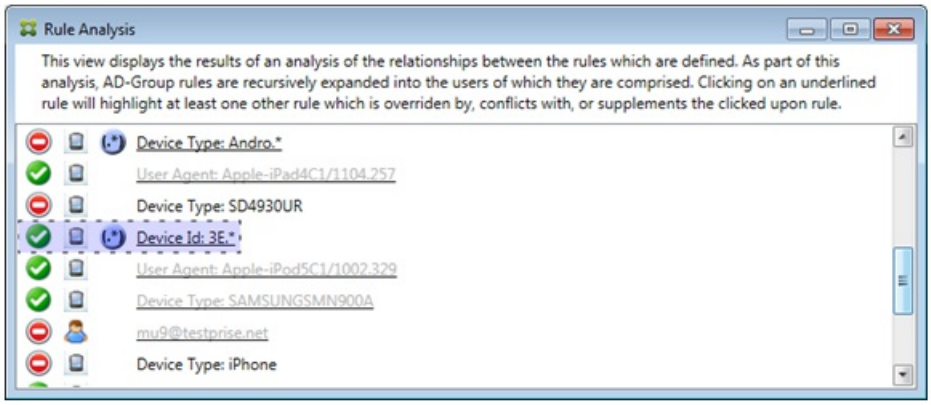
In diesem Fall gibt es zwei Nebenregeln, die die primäre Regel außer Kraft setzen: die Regel mit regelmäßigem Ausdruck zen.* und die normale Regel zentrain01@zenprise.com (von zenprise/TRAINING/ZenTraining A). Bei der letzteren Nebenregel besteht das Problem darin, dass die Active Directory-Gruppenregel 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.

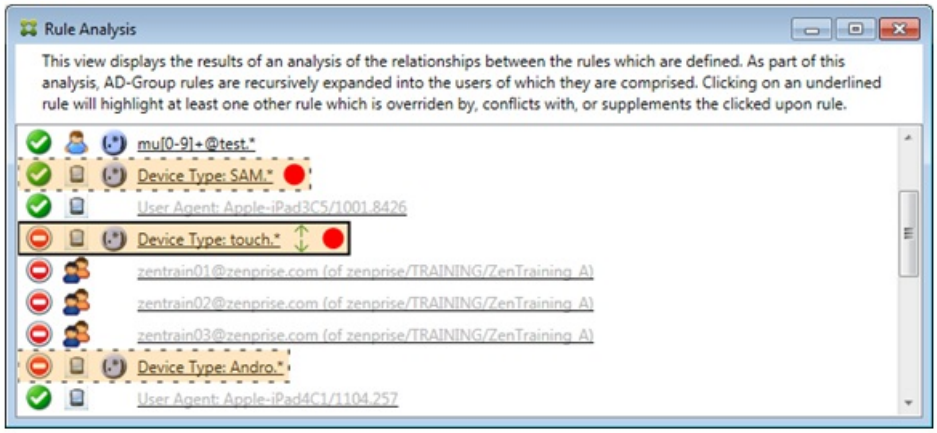
Analysieren einer Ergänzung und eines Konflikts

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

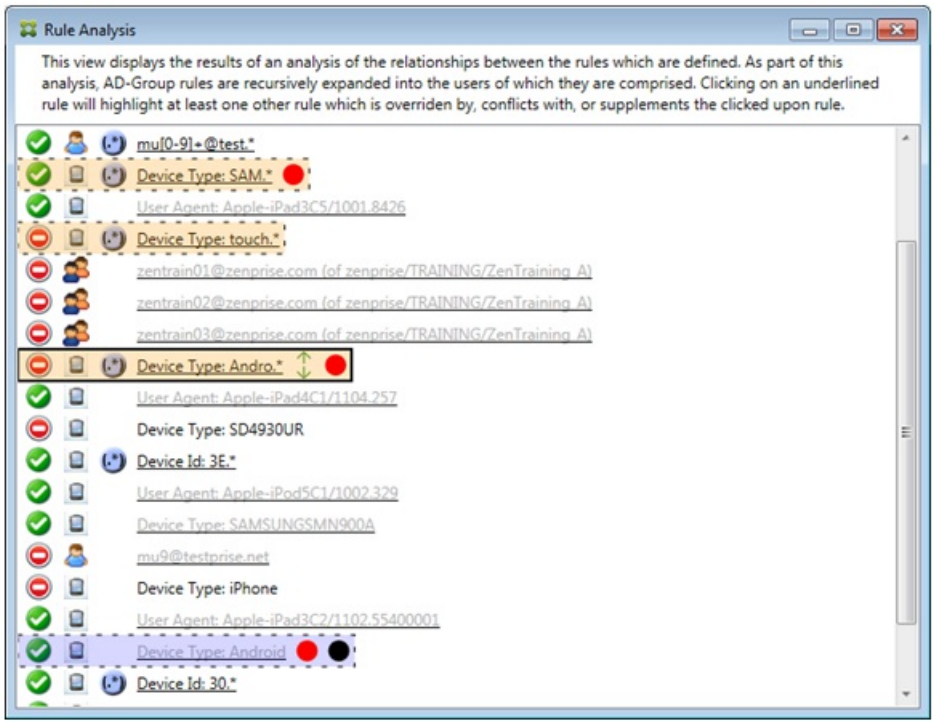
ein Konflikt mit der primären Regel besteht, bei welcher der Zugriffszustand auf Blockieren festgelegt ist.

- 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

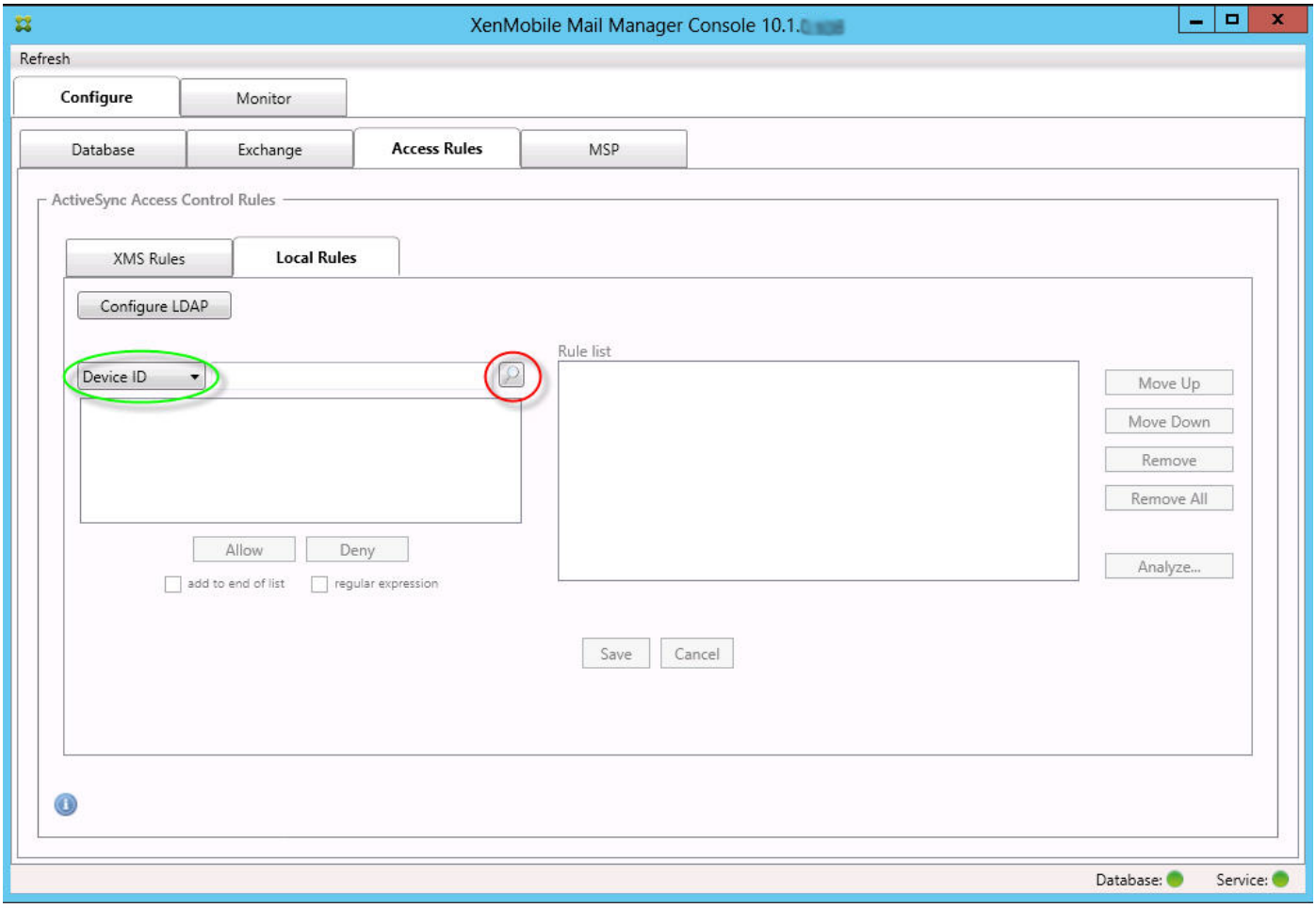
In diesem Beispiel wird demonstriert, dass Regelbeziehungen immer aus der Sicht der primären Regel dargestellt werden. Im vorherigen Beispiel wurde gezeigt, was beim Klicken auf die Gerätetypregel mit dem regelmäßigen Ausdruck touch.* angezeigt wird. Wird auf die Nebenregel Andro.* geklickt, werden andere Nebenregeln markiert.



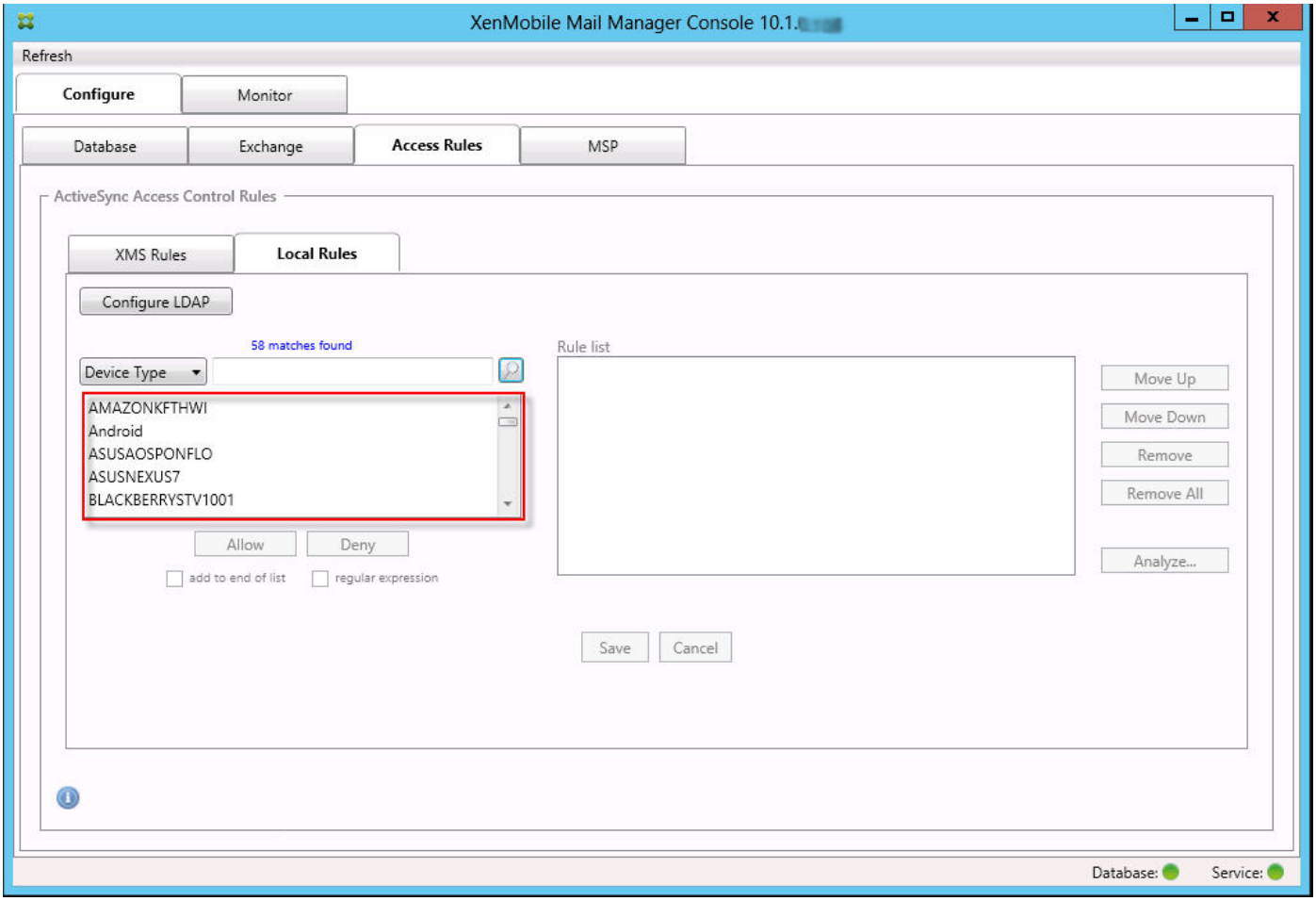
In diesem Beispiel wird eine außer Kraft gesetzte Regel, die Teil der Regelbeziehung ist, gezeigt. Diese Regel ist die normale ActiveSync-Gerätetypregel "Android", die außer Kraft gesetzt ist (sichtbar an der helleren Schrift und dem schwarzen Punkt) und deren Zugriffszustand mit dem der primären ActiveSync-Gerätetypregel 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.

Konfigurieren einer lokalen Regel mit normalem Ausdruck

1. Klicken Sie auf die Registerkarte Access Rules.

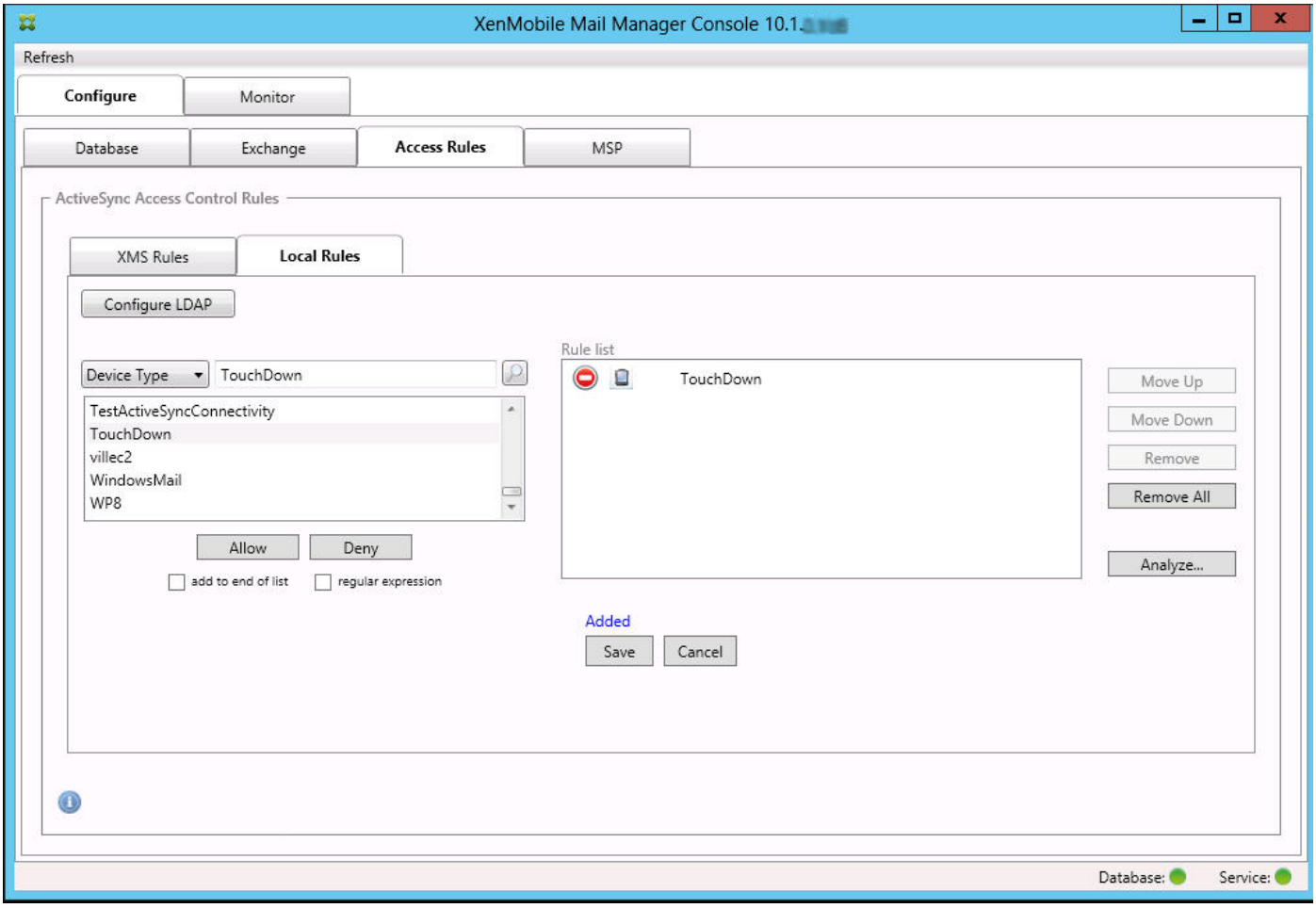


2. Wählen Sie in der Liste Device ID das Feld aus, für das Sie die lokale Regel erstellen möchten.
3. Klicken Sie auf das Lupensymbol, um alle eindeutigen Übereinstimmungen für das ausgewählte Feld einzublenden. In diesem Beispiel wurde das Feld Device Type ausgewählt, die Übereinstimmungen werden unterhalb 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.

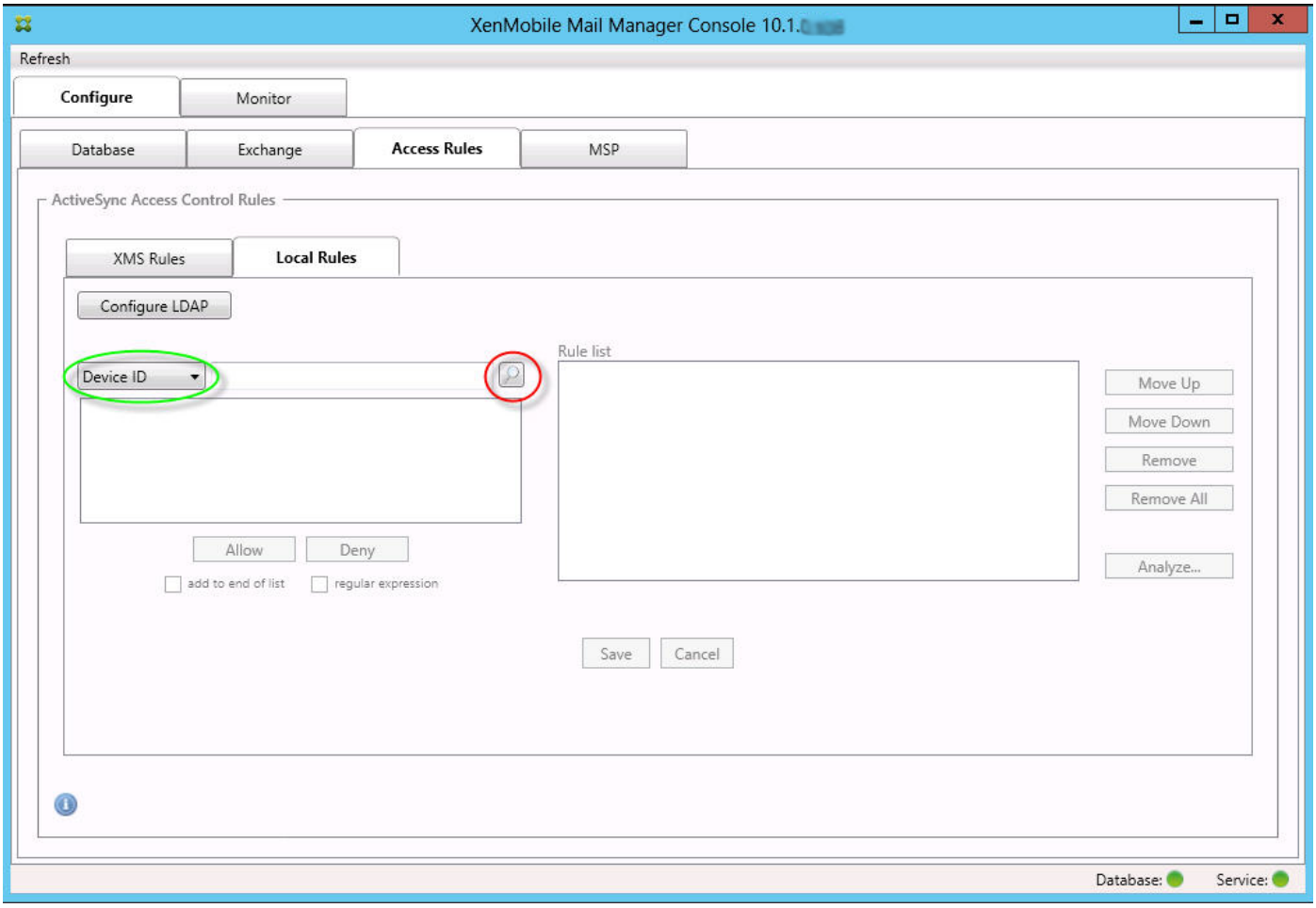


Hinzufügen eines regelmäßigen Ausdrucks

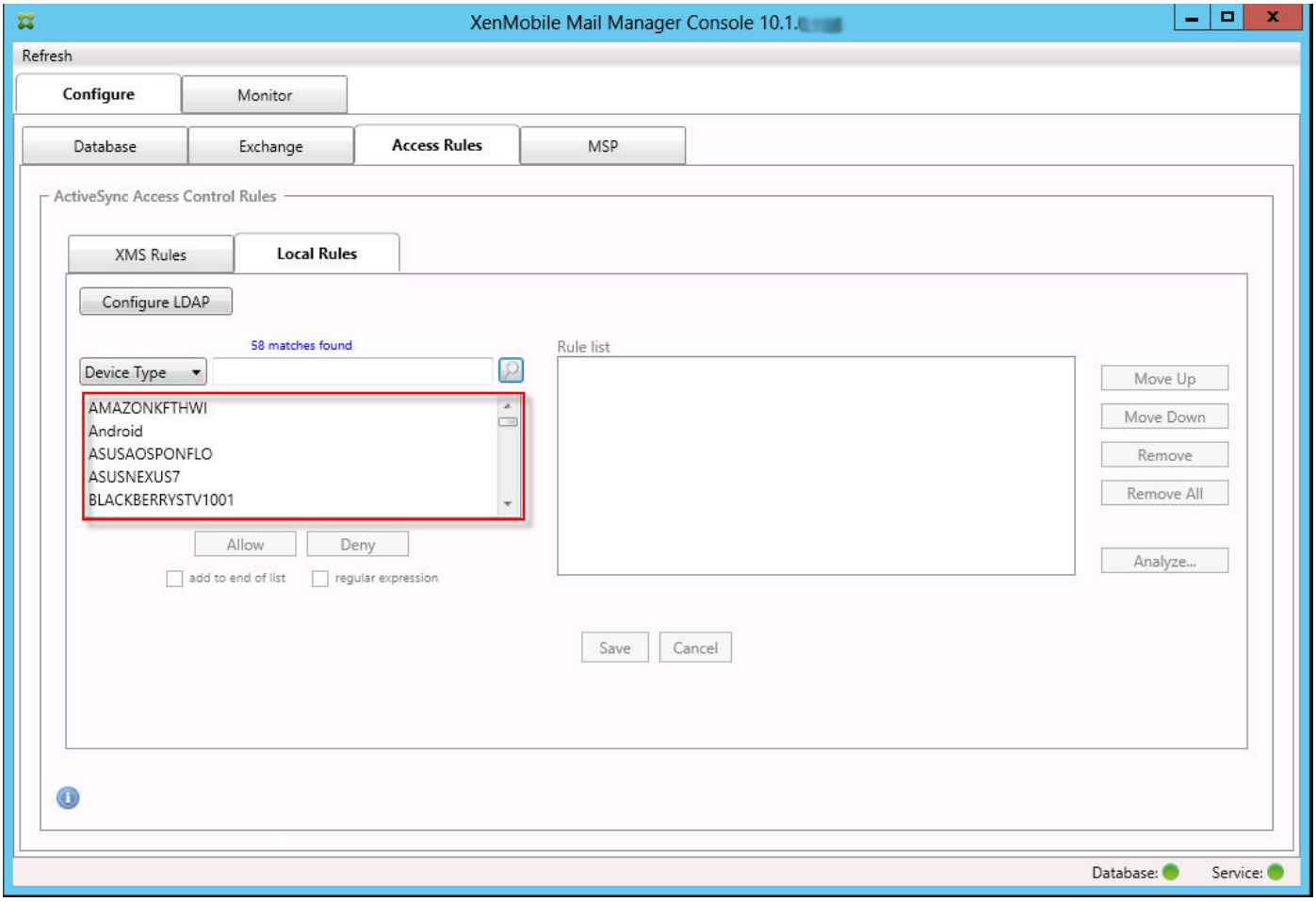
Lokale Regeln mit regelmäßigen Ausdrücken sind an folgendem Symbol zu erkennen: (.*). Zum Hinzufügen einer Regel mit regelmäßigem Ausdruck können Sie entweder einen Wert aus der Ergebnisliste für ein spezifisches Feld als Grundlage verwenden (sofern bereits ein größerer Snapshot durchgeführt wurde) oder den regelmäßigen Ausdruck selbst eingeben.

Erstellen eines regelmäßigen Ausdrucks mit einem vorhandenen Feldwert

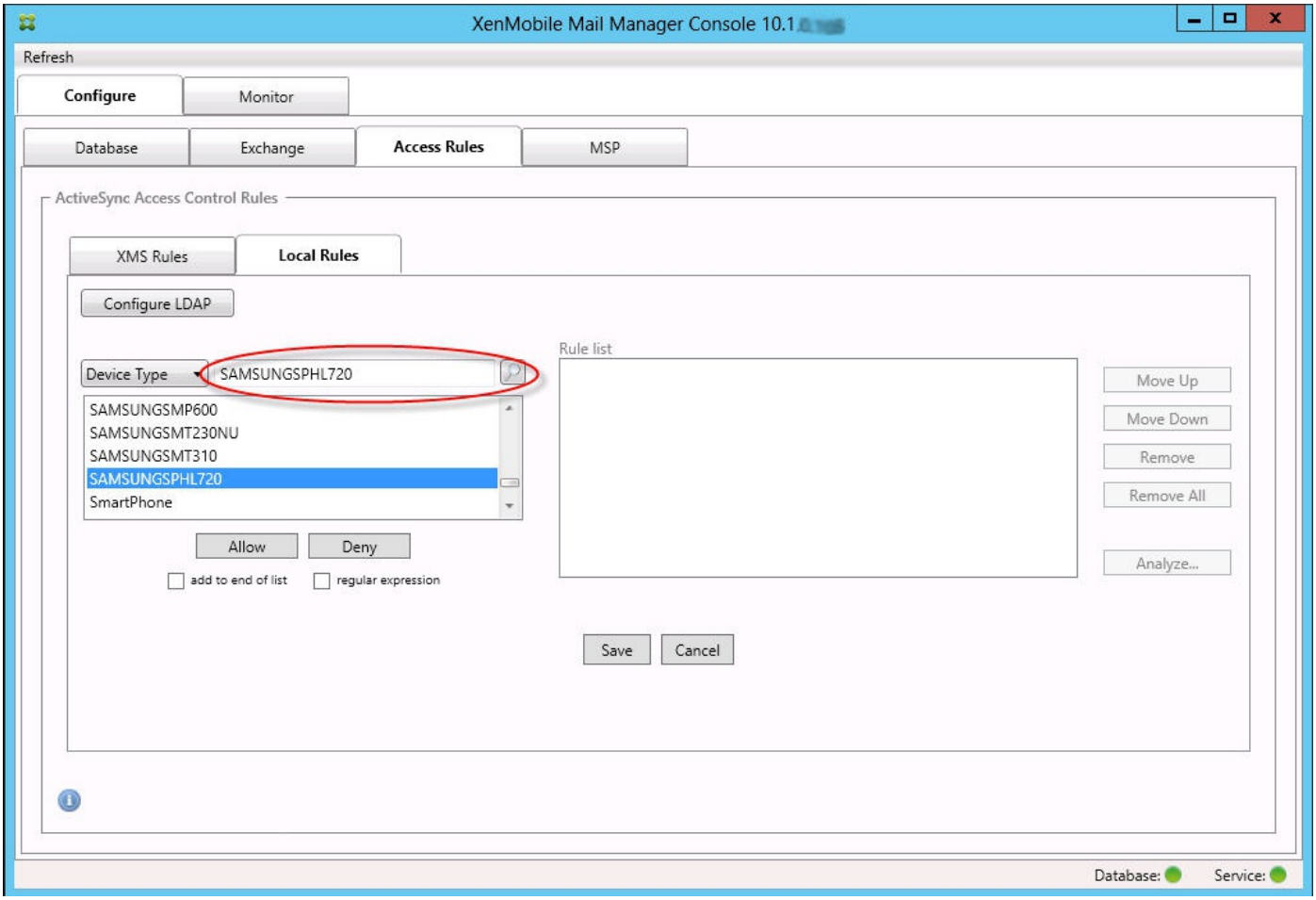
1. Klicken Sie auf die Registerkarte Access Rules.



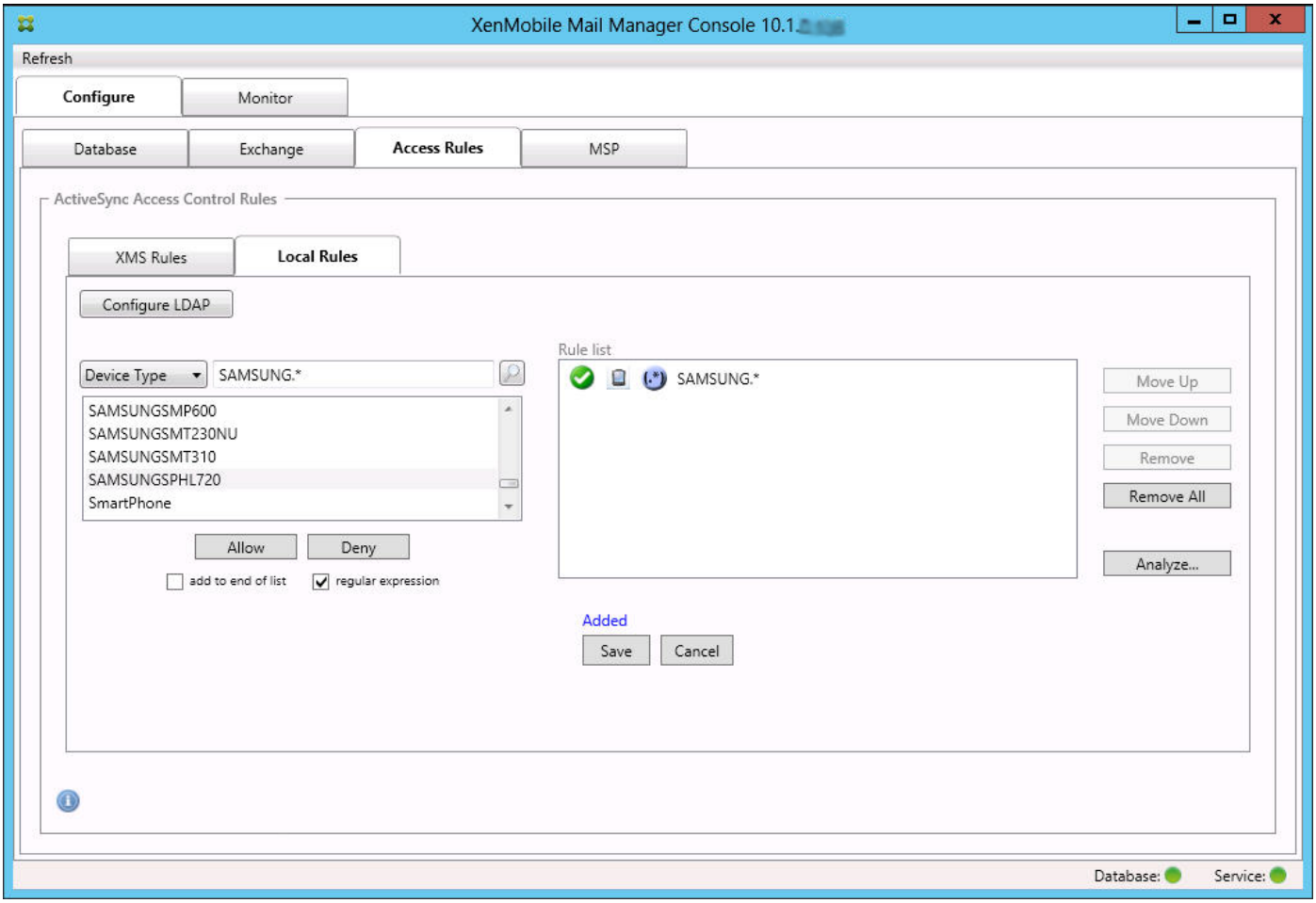
2. Wählen Sie in der Liste Device ID das Feld aus, für das Sie die lokale Regel mit einem regelmäßigen Ausdruck erstellen möchten.
3. Klicken Sie auf das Lupensymbol, um alle eindeutigen Übereinstimmungen für das ausgewählte Feld einzublenden. In diesem Beispiel wurde das Feld Device Type ausgewählt, die Übereinstimmungen werden unterhalb des Listenfelds angezeigt.



4. Klicken Sie auf einen der Einträge in der Ergebnisliste. In diesem Beispiel wurde SAMSUNGSPHL720 ausgewählt und erscheint im Textfeld neben Device Type.

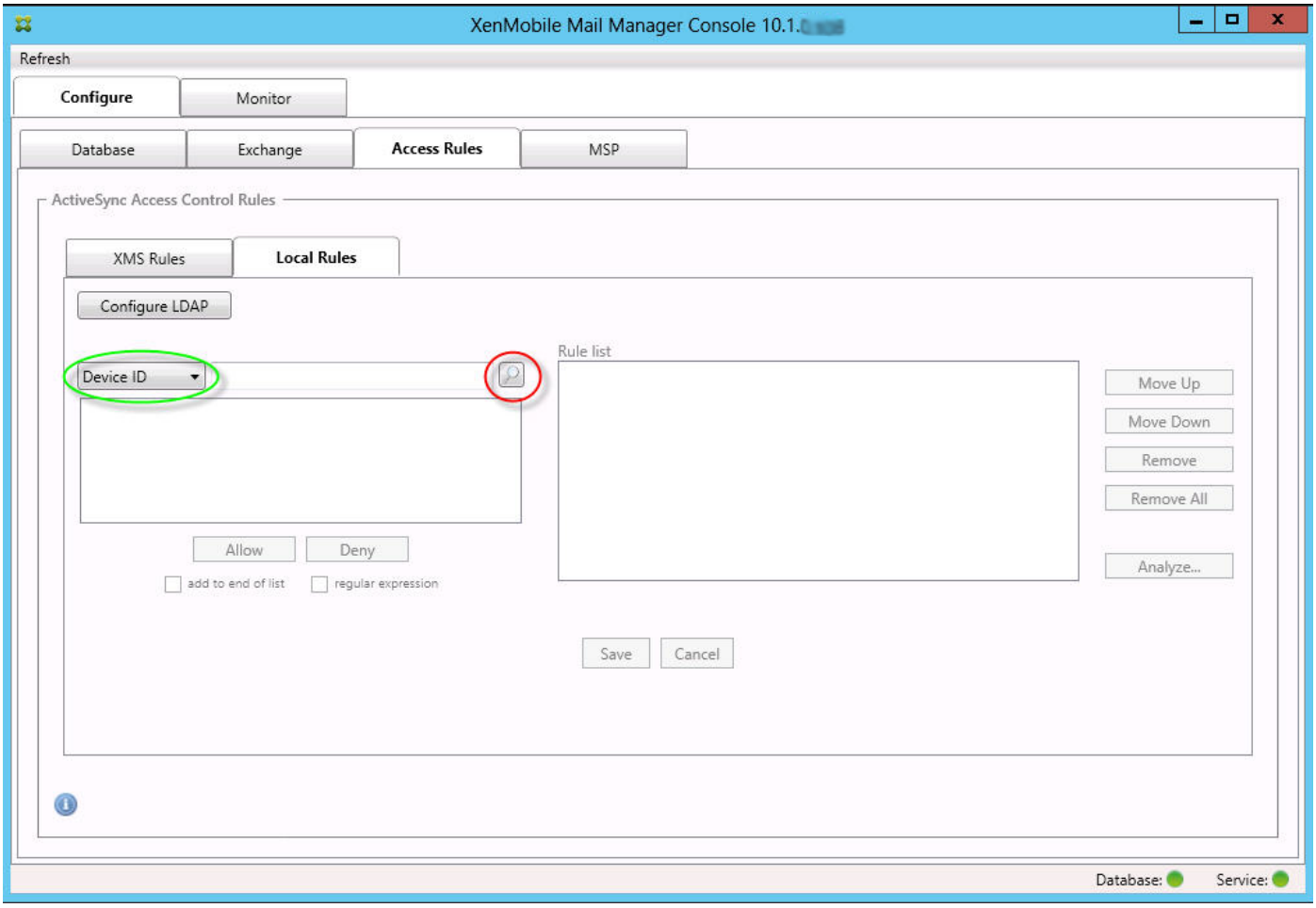


5. Damit alle Gerätetypen, deren Gerätetypwert "Samsung" enthält, zugelassen werden, fügen Sie eine Regel mit regelmäßigem Ausdruck wie folgt hinzu:
   1. Klicken Sie in das Textfeld des ausgewählten Elements.
   2. Ändern Sie den Text SAMSUNGSPHL720 in SAMSUNG.*
   3. Stellen Sie sicher, dass das Kontrollkästchen regular expression aktiviert ist.
   4. Klicken Sie auf Allow.

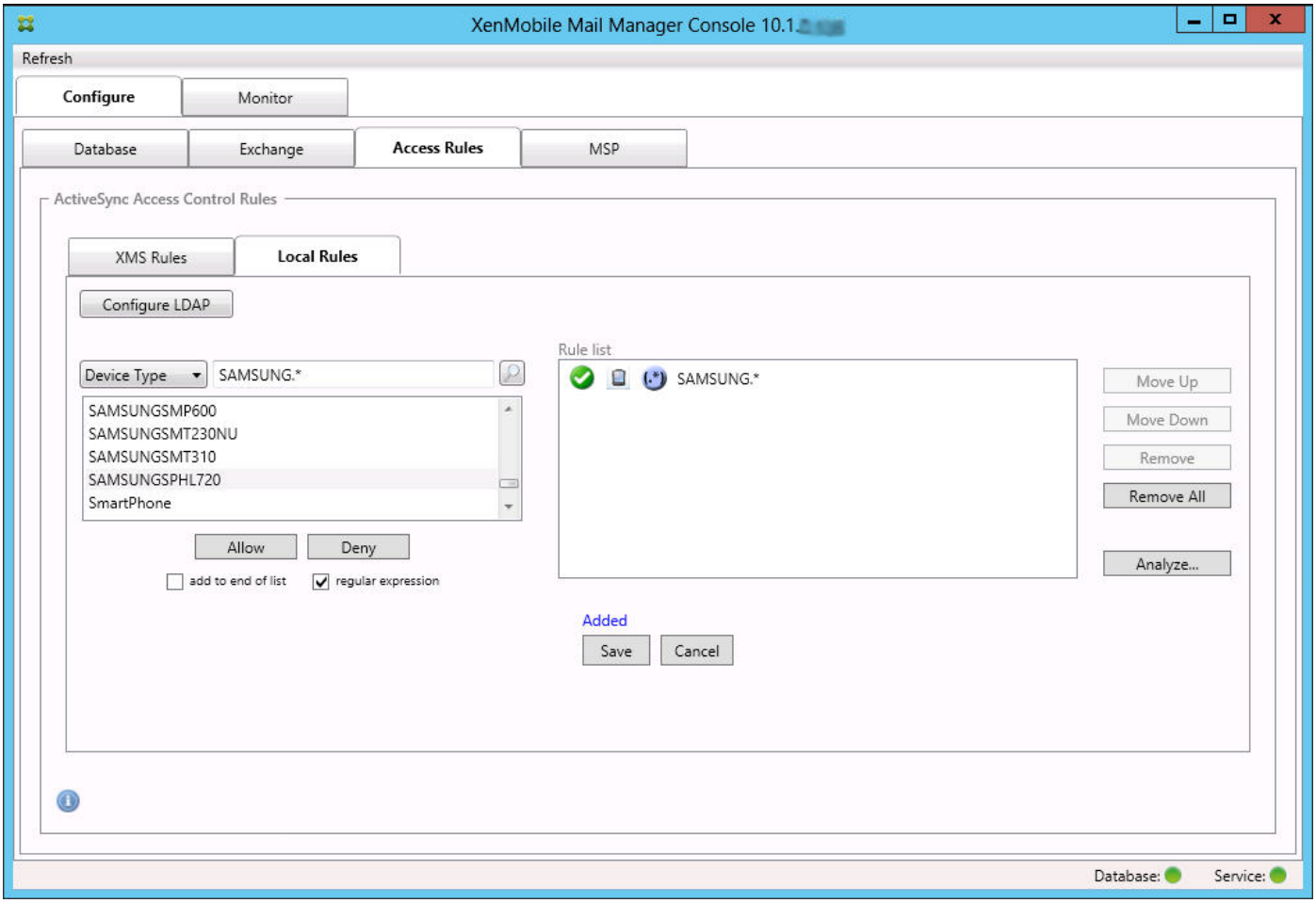


Erstellen einer Zugriffsregel

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.



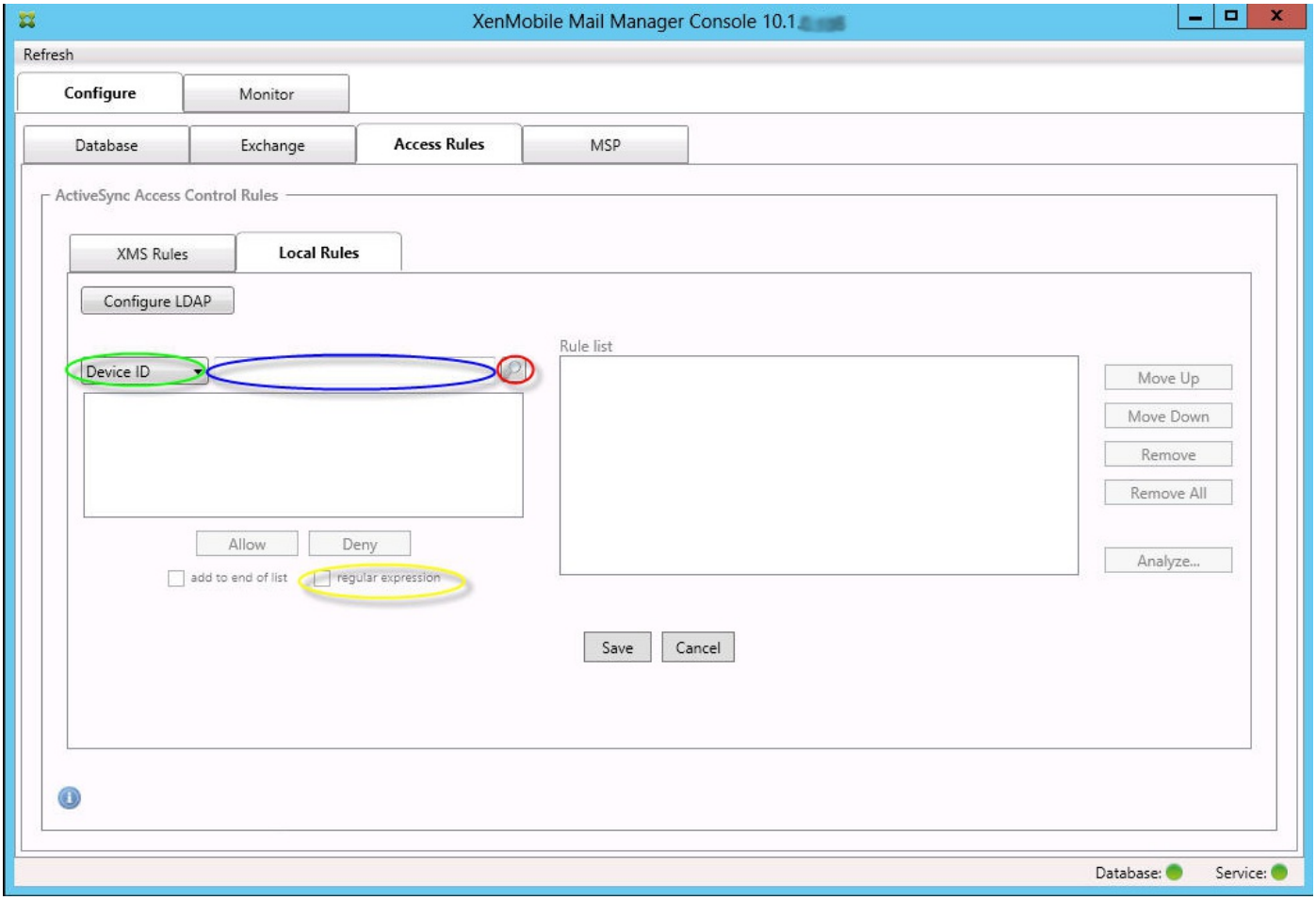
3. Wählen Sie das Feld aus, gegen das der Abgleich stattfinden soll. In diesem Beispiel ist dies Device Type.
4. Geben Sie den regelmäßigen Ausdruck ein. In diesem Beispiel ist diessamsung.*
5. Stellen Sie sicher, dass das Kontrollkästchen regular expression aktiviert ist, und klicken Sie auf Allow oder Deny. In diesem Beispiel lautet die Auswahl Allow und das Endergebnis ist wie folgt:



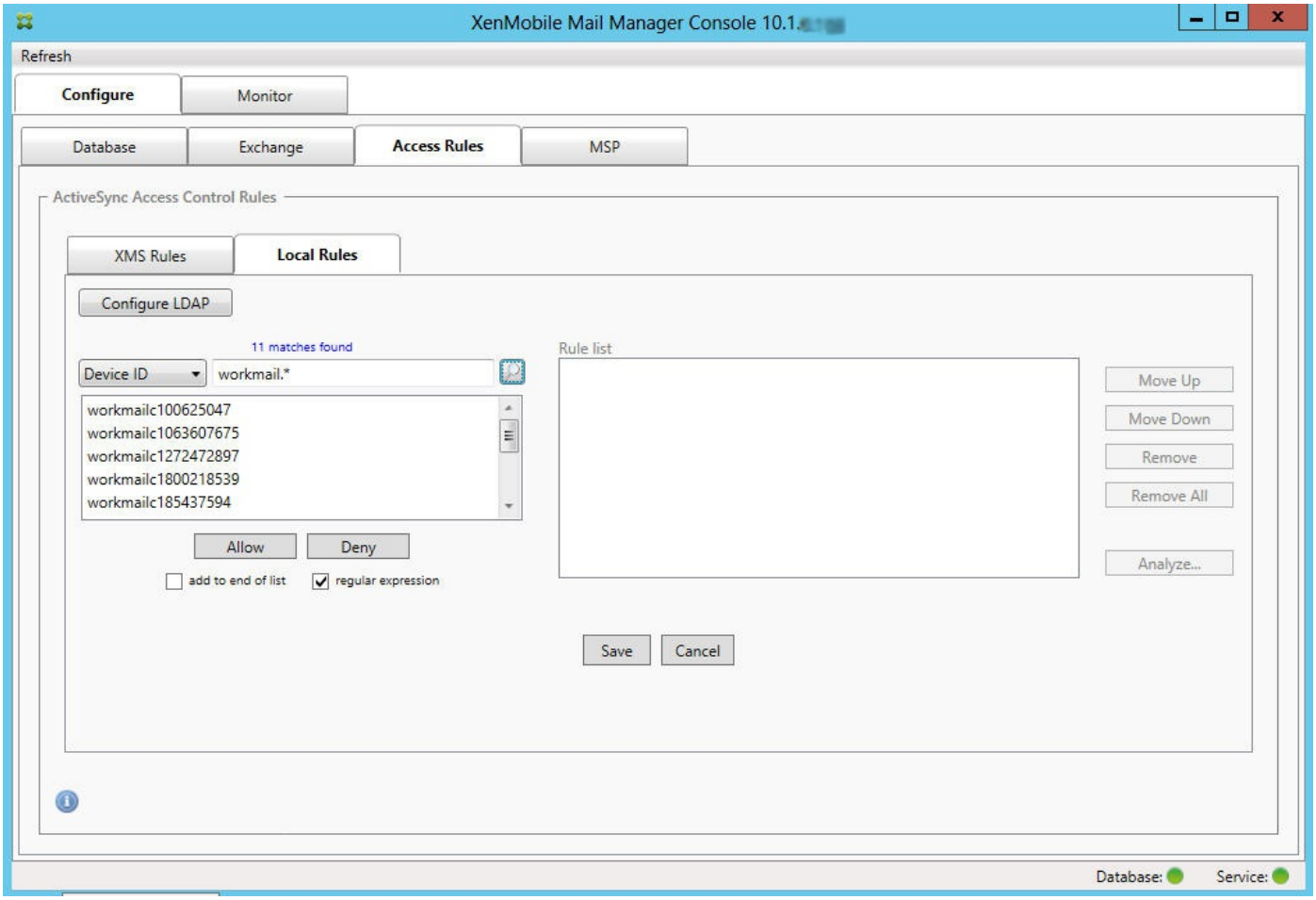
Suchen von Geräten

Durch Aktivieren des Kontrollkästchens "regular expression" können Sie Geräte, die dem angegebenen Ausdruck entsprechen, suchen. Dieses Feature steht nur zur Verfügung, wenn ein größerer Snapshot erfolgreich durchgeführt wurde. Sie können das Feature nutzen, selbst wenn Sie keine Verwendung regelmäßiger Ausdrücke planen. Beispiel: Sie möchten alle Geräte suchen, deren ActiveSync-Geräte-ID den Text "workmail" enthält. Gehen Sie hierfür wie nachfolgend beschrieben vor.

1. Klicken Sie auf die Registerkarte Access Rules.
2. Stellen Sie sicher, dass die Abgleichfeldauswahl auf Device ID (Standardeinstellung) festgelegt ist.



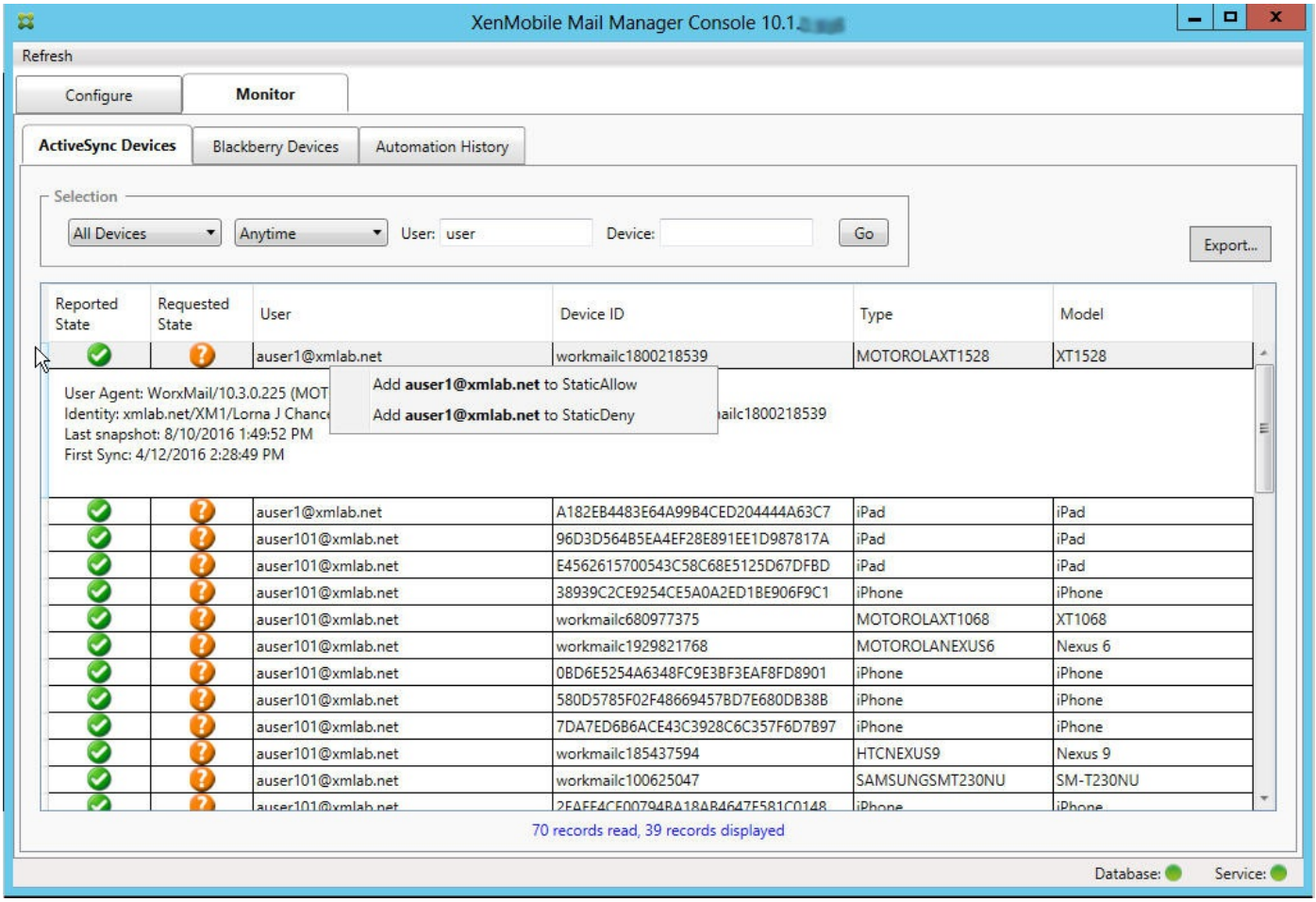
3. Klicken Sie in das Textfeld des ausgewählten Elements (blau in der Abbildung oben) und geben Sieworkmail.*ein.
4. Stellen Sie sicher, dass das Kontrollkästchen regular expression aktiviert ist, und klicken Sie auf das Lupensymbol, damit Übereinstimmungen angezeigt werden (siehe folgende Abbildung).



Hinzufügen eines einzelnen Benutzers, eines einzelnen Geräts oder eines einzelnen Gerätetyps zu einer statischen Regel

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

Jul 28, 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

Oct 13, 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.

Häufige Fehler

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.

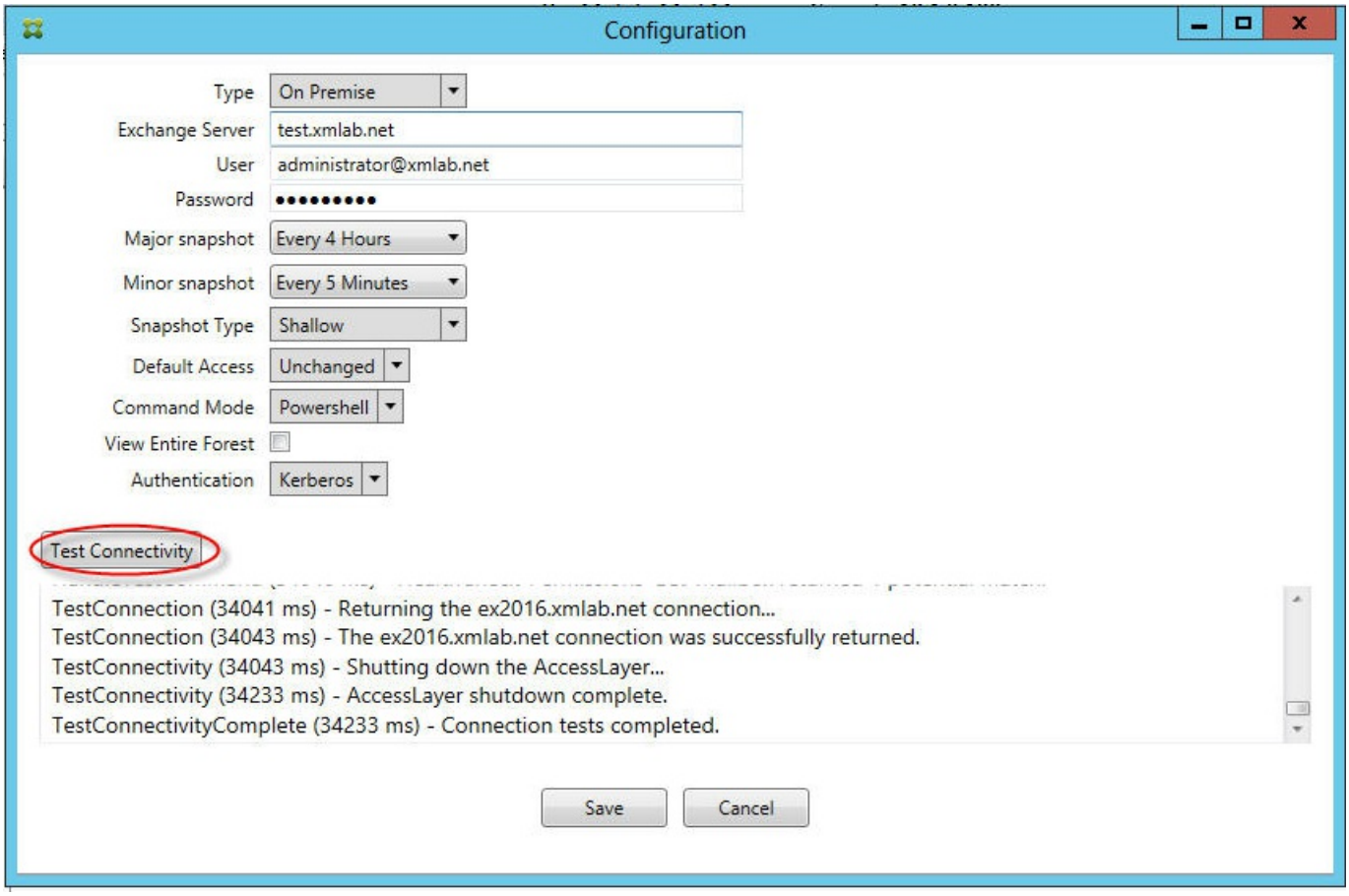
  Wenn die integrierte Windows-Authentifizierung konfiguriert ist, muss das Benutzerkonto von XenMobile Mail Manager als zulässige SQL-Anmeldung konfiguriert sein. Standardmäßig ist das Konto des XenMobile Mail Manager-Diensts das lokale System, es kann aber in jedes beliebige Konto, das über lokale Administratorprivilegien 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 <Installationsordner>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.



Problembehandlungstools

PowerShell-Dienstprogramme zur Problembehandlung sind im Order Support\PowerShell verfügbar.

Ein Problembehandlungstool führt eine gründliche RBAC-Analyse von Benutzern sowie detaillierte Analysen der Postfächer und Geräte von Benutzern aus, um Fehlerzustände und potenzielle Fehlerbereiche zu erkennen. Alle Cmdlets können in eine Textdatei ausgegeben und gespeichert werden.

XenMobile NetScaler Connector

Oct 13, 2016

XenMobile NetScaler Connector bietet einen Authentifizierungsdienst auf Geräteebene für ActiveSync-Clients bei NetScaler, der als Reverseproxy für das Exchange ActiveSync-Protokoll fungiert. Die Autorisierung wird durch eine Kombination von Richtlinien, die Sie in XenMobile definieren, und lokal in XenMobile NetScaler Connector definierten Regeln gesteuert.

Weitere Informationen finden Sie in den folgenden Artikeln:

- XenMobile NetScaler Connector
- ActiveSync Gateway in XenMobile

Ein detailliertes Architekturdiagramm finden Sie im Artikel Reference Architecture for On-Premises Deployments in der XenMobile-Bereitstellungsdokumentation.